Algebra & Number Theory

Volume 8
2014
No. 5

msp

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1045

Polarization estimates for abelian varieties

David Masser and Gisbert Wüstholz

In an earlier paper we showed that an abelian variety over a number field of fixed degree has a polarization whose degree is bounded by a power of its logarithmic Faltings height, provided there are only trivial endomorphisms. Here we greatly relax the endomorphism hypothesis, and we even eliminate it completely when the dimension is at most seven. Our methods ultimately go back to transcendence theory, with the asymmetric geometry of numbers as a new ingredient, together with what we call the Severi–Néron group, a variant of the Néron–Severi group.

1. Introduction

In this paper we address the following question: is the polarization of an abelian variety determined by arithmetical data? More precisely, if A is an abelian variety of fixed dimension defined over a fixed number field, is there necessarily a polarization on A whose degree is bounded in terms of the Faltings height of A?

So formulated, the question has the easy answer, "yes". For a fundamental finiteness result states that, up to isomorphism, there are only finitely many such abelian varieties with a bounded height, and then we can choose a polarization on each of them. However, this argument fails to give any kind of explicit estimate for the degrees of the polarizations.

Taking into account the applications of transcendence theory to abelian varieties in recent years, in particular our papers [Masser and Wüstholz 1993a; 1993b; 1993c; 1994; 1995a; 1995b], one may conjecture that these degrees are bounded by an expression of the form $C \max\{1, h(A)\}^{\pi}$, where $h(A)$ is the absolute logarithmic semistable Faltings height of A (see, for example, [Faltings 1983] or [Bost 1996a]), π depends only on the dimension of A, and C depends only on this dimension together with the degree of the field of definition of A.

The object of the present paper is to establish this conjecture in almost all the cases of interest to algebraists or arithmetic geometers. It was already proved in [Masser and Wüstholz 1995a, Corollary, p. 6] when the endomorphism ring of A is trivial. In general suppose that A is defined over a number field k, and write End A

MSC2010: primary 11G10; secondary 11J95.
Keywords: abelian varieties, estimating polarizations.

for the ring of endomorphisms defined over the algebraic closure $\bar{k}$ of k; this is an order in the algebra $\mathbb{Q} \otimes \mathrm{End}\, A$ over the rational field $\mathbb{Q}$. If A is simple, this algebra is a division algebra whose center is a number field. Our main result can be stated as follows.

Theorem 1.1. *For positive integers n and d there is a constant π depending only on n and a constant C depending only on n and d with the following property. Let A be an abelian variety of dimension n defined over a number field k of degree d. Suppose that A is simple over $\bar{k}$ and that $\mathbb{Q} \otimes \mathrm{End}\, A$ is commutative or its center is totally real. Then A has a polarization over $\bar{k}$ of degree at most $C \max\{1, h(A)\}^{\pi}$.*

In fact the above hypotheses on the endomorphism algebra correspond precisely to the types I, II and III in Albert's famous classification, together with type IV in the commutative case. This remark is already enough to establish the above conjecture for simple abelian varieties in infinitely many dimensions and all abelian varieties, not necessarily simple, in small dimensions. For example, we will deduce the following consequences.

Corollary 1.2. *For a positive squarefree integer n and a positive integer d there is a constant π depending only on n and a constant C depending only on n and d with the following property. Let A be an abelian variety of dimension n defined over a number field k of degree d. Suppose that A is simple over $\bar{k}$. Then A has a polarization over $\bar{k}$ of degree at most $C \max\{1, h(A)\}^{\pi}$.*

Corollary 1.3. *For a positive integer d there is a constant C depending only on d with the following property. Let A be an abelian variety of dimension at most 7 defined over a number field k of degree d. Then A has a polarization over $\bar{k}$ of degree at most $C \max\{1, h(A)\}^{\pi}$, where π is an absolute constant.*

In all of the above results the quantity $C \max\{1, h(A)\}^{\pi}$ can readily be replaced by $C_0 \max\{d, h(A)\}^{\pi}$ with C_0 independent of d; see the remarks in [Masser and Wüstholz 1995a, p. 23]. A more interesting problem is to prove that A has a polarization over k itself of small degree in the above sense, but this seems not to follow from our methods. At any rate we may note that all polarizations of an abelian variety of dimension n defined over a field k of characteristic zero are automatically defined over an extension of k of relative degree at most 3^{16n^4}; see [Masser and Wüstholz 1993a, Lemma 2.3, p. 415].

Our original motivation for estimating polarizations was to extend the isogeny estimates of [Masser and Wüstholz 1993b], for polarized abelian varieties, to unpolarized abelian varieties, simply by providing the latter with explicit polarizations. In fact we solved this isogeny problem in a completely different way in our paper [Masser and Wüstholz 1995a]. Nevertheless we feel that our conjecture has enough independent interest to justify the present paper. And similar problems over finite fields have been studied by Howe [1995].

Actually the proof of our theorem relies heavily on the methods and results of [Masser and Wüstholz 1995a]; in particular we need discriminant estimates and factorization estimates. This paper is based ultimately on the work of [Masser and Wüstholz 1993a], which involves techniques from the theory of transcendental numbers. By contrast, the deduction of our present results from those of [Masser and Wüstholz 1995a] is by purely algebraic methods, together with the geometry of numbers. More precisely, the necessary positive definiteness properties of our polarizations are established using tools from the so-called asymmetric geometry of numbers. For endomorphism algebras of types I, III and IV it suffices to use a theorem of Chalk, but for type II we have to develop what seems to be a new generalization to number fields of a theorem of Blaney. All these results are recorded in Section 2.

In Section 3 we prove some elementary properties of discriminants in quaternion algebras and CM-fields, and in Section 4 we give some analogous results for the cross-discriminants introduced in [Masser and Wüstholz 1995a]. Only instead of considering the full set $\mathrm{Hom}(A, \hat{A})$ of homomorphisms from A into its dual $\hat{A}$, we have to restrict to its subset the Néron–Severi group $\mathrm{NS}(A)$, as well as to a certain complement, which for want of a better name we call the Severi–Néron group $\mathrm{SN}(A)$. Also in this section we record the necessary facts about Albert's classification and the representations of the corresponding endomorphism algebras. Some of this material is borrowed from an article of Shimura [1963].

Then in Sections 5 and 6 we obtain our purely algebraic estimates for polarizations on complex abelian varieties; this enables us to postpone the appeal to [Masser and Wüstholz 1995a] until Section 7, where we establish our theorem and its corollaries.

Of course our results are not quite complete; in fact to prove the full conjecture it remains only to treat simple abelian varieties in the noncommutative case of type IV. We hope to return to this problem in a later paper. For the moment it is perhaps amusing to speculate on whether our conjecture holds with $\pi = 0$; for example, does every abelian variety of dimension 2 defined over $\mathbb{Q}$ have a polarization whose degree is bounded by an absolute constant, say 10^{10}?

And finally we should say something about effectivity. As usual the exponents π in our results are not only effective but also explicitly computable, as already in [Masser and Wüstholz 1993a; 1993b; 1995a]. The effectivity of the coefficients C is known for some time since the work of Bost [1996b]. At any rate the algebraic estimates of our own Sections 2–6 are all completely explicit and it is not until Section 7 that we appeal to [Masser and Wüstholz 1995a].

Some of this work was written up while the first author was visiting Göttingen and Erlangen in 1991 (sic), and he would like to thank S. Patterson and H. Lange for hospitality. Since then the work has been mentioned by Bost in his 1994–95 Séminaire Bourbaki talk [Bost 1996b, p. 126], as well as in [Masser 2006] and [Baker and Wüstholz 2007, p. 164].

Recently É. Gaudron and G. Rémond [2013] sent us a manuscript in which they complete our results. They use the general strategy and methods laid down in our papers [Masser and Wüstholz 1993a; 1993b; 1993c; 1994; 1995a; 1995b], but their details appear to differ from ours. Thus our work is of independent value, not least in our use of the asymmetric geometry of numbers. This topic is relevant to class number problems for quadratic forms over number fields and in our context it brings to the fore some interesting side questions.

2. Asymmetric geometry of numbers

For a positive integer ℓ let Ξ be a lattice in the real Euclidean space $\mathbb{R}^\ell$ with determinant $d(\Xi)$. If $d_1, \dots, d_\ell$ are positive real numbers with $d_1 \cdots d_\ell = d(\Xi)$, Minkowski's theorem in the geometry of numbers (see, for example, [Gruber and Lekkerkerker 1987, Theorem 3, p. 43]) provides nonzero $(\xi_1, \dots, \xi_\ell)$ in Ξ with

$$|\xi_1| \le d_1, \dots, |\xi_\ell| \le d_\ell. \tag{2-1}$$

An asymmetric version of this was established by Chalk; it provides instead $(\xi_1, \dots, \xi_\ell)$ in Ξ with

$$\xi_1 > 0, \dots, \xi_\ell > 0, \quad |\xi_1 \cdots \xi_\ell| \le d(\Xi) \tag{2-2}$$

(see, for example, [Gruber and Lekkerkerker 1987, corollary, p. 598] for a proof of Chalk's original theorem for grids). Note that it is not possible to localize further as in (2-1).

Our first application of these results is as follows. Let K be a totally real number field of degree m, and denote by $\phi_1, \dots, \phi_m$ the different embeddings of K into the real field $\mathbb{R}$. For ξ in K write $N(\xi) = \xi^{\phi_1} \cdots \xi^{\phi_m}$ and $T(\xi) = \xi^{\phi_1} + \cdots + \xi^{\phi_m}$ for the norm and trace, respectively, from K to $\mathbb{Q}$. If $\mathcal{O}$ is an order in K we define in the usual way its discriminant $d(\mathcal{O})$ as the determinant of the matrix with entries $\det T(\xi_i, \xi_j)$, $(1 \le i, j \le m)$, where $\xi_1, \dots, \xi_m$ are elements of any basis of $\mathcal{O}$ over the rational integers $\mathbb{Z}$. Since K is totally real, it is easy to see (for example, as in the proof just below) that $d(\mathcal{O})$ is positive.

Lemma 2.1. *For any nonzero σ in K there exists ξ in $\mathcal{O}$ such that $\sigma\xi$ is totally positive and $|N(\xi)| \le d(\mathcal{O})^{1/2}$.*

Proof. Let $u_1, \dots, u_m$ be the signs of $\sigma^{\phi_1}, \dots, \sigma^{\phi_m}$. As ξ runs over $\mathcal{O}$, the vectors $(u_1\xi^{\phi_1}, \dots, u_m\xi^{\phi_m})$ describe a lattice Ξ in $\mathbb{R}^m$, and it is straightforward to check that its determinant $d(\Xi)$ satisfies $(d(\Xi))^2 = d(\mathcal{O})$. The desired result now follows at once from (2-2). □

Next let n be a positive integer (soon to disappear, so that there is no danger of confusion with $n = \dim A$ in Section 1). Let F be a field (also soon to disappear),

and let Q be a quadratic form on F^n over F. This has a discriminant $d(Q)$ in F defined as the determinant of the matrix with entries $Q(e_i, e_j)$ $(1 \le i, j \le n)$, where Q also denotes the associated bilinear form, and $e_1, \dots, e_n$ are elements of the standard basis of F^n over F.

Suppose for the moment that $K = \mathbb{Q}$ and $F = \mathbb{R}$. If Q is nondegenerate and not negative definite a theorem of Blaney [Gruber and Lekkerkerker 1987, Theorem 4, p. 471] shows how to find small positive values of Q on $\mathbb{Z}^n$. Namely, there exists $(\xi_1, \dots, \xi_n) \in \mathbb{Z}^n$ such that

$$0 < Q(\xi_1, \dots, \xi_n) \le 2^{n-1} |d(Q)|^{1/n}.$$

Our purpose in the rest of this section is to obtain generalizations of this result to arbitrary totally real fields K, with totally positive values of Q on $\mathbb{O}^n$ for some order $\mathbb{O}$ of K. For applications it suffices to restrict ourselves to $n \le 3$ and forms Q defined over K (the latter is not in fact a genuine restriction). In that case the real conjugates $Q^{\phi_1}, \dots, Q^{\phi_m}$ each have a certain signature, and it seems necessary to assume that these are all the same. If this common signature is u, we say that Q has total signature u.

We start with totally positive definite binary forms.

Lemma 2.2. *Let $Q(x, y)$ be a binary quadratic form over K with total signature $(++)$. Then there are ξ, η in $\mathbb{O}$ such that $q = Q(\xi, \eta)$ is totally positive and*

$$N(q) \le 2^m d(\mathbb{O})\, |N(d(Q))|^{1/2}.$$

Proof. Completing the square on each of the positive definite conjugates of Q, we find real numbers a_i, b_i, c_i such that

$$Q^{\phi_i}(x, y) = a_i \big((x - b_i y)^2 + (c_i y)^2\big) \quad (1 \le i \le m). \tag{2-3}$$

In particular

$$d(Q^{\phi_i}) = a_i^2 c_i^2 > 0, \quad a_i > 0 \quad (1 \le i \le m), \tag{2-4}$$

and we can also suppose $c_i > 0$ $(1 \le i \le m)$. Now, as ξ, η run over $\mathbb{O}$, the vectors

$$\big(\xi^{\phi_1} - b_1 \eta^{\phi_1}, \eta^{\phi_1}, \dots, \xi^{\phi_m} - b_m \eta^{\phi_m}, \eta^{\phi_m}\big)$$

describe a lattice Ξ in $\mathbb{R}^{2m}$, and it is easy to see that

$$d(\Xi) = \big(d(\mathbb{O})^{1/2}\big)^2 = d(\mathbb{O}).$$

Define C by

$$C^{2m} = c_1 \cdots c_m d(\mathbb{O}); \tag{2-5}$$

then it follows from (2-1) that we can find ξ, η in $\mathbb{O}$, not both zero, with

$$|\xi^{\phi_i} - b_i \eta^{\phi_i}| \le C, \quad |\eta^{\phi_i}| \le C/c_i \quad (1 \le i \le m).$$

So (2-3) gives

$$0 < Q^{\phi_i}\left(\xi^{\phi_i}, \eta^{\phi_i}\right) \le 2C^2 a_i \quad (1 \le i \le m).$$

Hence $q = Q(\xi, \eta)$ is totally positive and

$$N(q) \le 2^m C^{2m} a_1 \cdots a_m = 2^m d(\mathbb{O})\, |N(d(Q))|^{1/2}$$

by (2-4) and (2-5). This completes the proof. □

The analogue for totally indefinite forms seems to lie a little deeper.

Lemma 2.3. *Let $Q(x, y)$ be a binary quadratic form over K with total signature $(+-)$. Then there are ξ, η in $\mathbb{O}$ such that $q = Q(\xi, \eta)$ is totally positive and*

$$N(q) \le 2^m d(\mathbb{O})\, |N(d(Q))|^{1/2}.$$

Proof. This time we factorize each indefinite conjugate as

$$Q^{\phi_i}(x, y) = a_i(x - b_i y)(x - c_i y) \quad (1 \le i \le m)$$

for real a_i, b_i, c_i; in particular

$$d(Q^{\phi_i}) = -\tfrac{1}{4} a_i^2 (b_i - c_i)^2 < 0 \quad (1 \le i \le m).$$

Now, as ξ, η run over $\mathbb{O}$, the vectors

$$\left(\xi^{\phi_1} - b_1 \eta^{\phi_1}, a_1(\xi^{\phi_1} - c_1 \eta^{\phi_1}), \ldots, \xi^{\phi_m} - b_m \eta^{\phi_m}, a_m(\xi^{\phi_m} - c_m \eta^{\phi_m})\right)$$

describe a lattice Ξ in $\mathbb{R}^{2m}$ with

$$d(\Xi) = |a_1 \cdots a_m|\, |b_1 - c_1| \cdots |b_m - c_m|\, d(\mathbb{O}).$$

So Chalk's theorem (2-2) applied to Ξ gives us in a similar way the desired estimate. This completes the proof. □

To extend these results to ternary forms we need a couple of elementary observations. For an order $\mathbb{O}$ in K recall from [Masser and Wüstholz 1995a, p. 8] the class index $i(\mathbb{O}) = i_1(\mathbb{O})$, which is the smallest positive integer I such that every $\mathbb{O}$-module of rank 1 in $\mathbb{O}$ contains a principal $\mathbb{O}$-module of index at most I.

Lemma 2.4. *Given elements ξ, η in $\mathbb{O}$ there are μ, ν in $\mathbb{O}$ with*

$$0 < |N(\nu)| \le i(\mathbb{O})^3$$

such that

$$\nu M \subseteq \mathbb{O}\mu \subseteq M$$

for $M = \mathbb{O}\xi + \mathbb{O}\eta$.

Proof. Of course μ plays the role of a highest common factor of ξ and η. If ξ and η are both zero then the result is trivial with $\mu = 0$, $\nu = 1$. Otherwise M has rank 1 and so there is $\mu \neq 0$ in M with

$$[M : \mathbb{O}\mu] = I \leq i(\mathbb{O}). \tag{2-6}$$

Let L be the $\mathbb{O}$-module of all λ in $\mathbb{O}$ such that $\lambda M \subseteq \mathbb{O}\mu$. Again there is $\nu \neq 0$ in L with

$$[L : \mathbb{O}\nu] = I' \leq i(\mathbb{O}). \tag{2-7}$$

Now $L = L_\xi \cap L_\eta$, where L_ζ is the set of all λ in $\mathbb{O}$ such that $\lambda\zeta$ is in $\mathbb{O}\mu$. So

$$[\mathbb{O} : L] = [\mathbb{O} : L_\xi][L_\xi : L_\xi \cap L_\eta] \leq [\mathbb{O} : L_\xi][\mathbb{O} : L_\eta]. \tag{2-8}$$

Also for any ζ in M we have

$$[\mathbb{O} : L_\zeta] = [\mathbb{O}\zeta : \mathbb{O}\zeta \cap \mathbb{O}\mu] \leq [M : \mathbb{O}\mu] = I,$$

so (2-8) gives $[\mathbb{O} : L] \leq I^2$. Finally this together with (2-6) and (2-7) leads to

$$[\mathbb{O} : \mathbb{O}\nu] = [\mathbb{O} : L][L : \mathbb{O}\nu] \leq I^2 I' \leq i(\mathbb{O})^3,$$

and since the left-hand side is $|N(\nu)|$ (see, for example, [Reiner 1975, Example 3, p. 231] the proof is complete. □

Next we say that a row vector v in $\mathbb{O}^3$ is $\mathbb{O}$-primitive if every nonzero λ in K with λv in $\mathbb{O}^3$ satisfies $|N(\lambda)| \geq 1$.

Lemma 2.5. *Suppose that v_0 in $\mathbb{O}^3$ is $\mathbb{O}$-primitive. Then there are v_1, v_2 in $\mathbb{O}^3$ such that v_0, v_1, v_2 form a matrix V with*

$$0 < |N(\det V)| \leq i(\mathbb{O})^9.$$

Proof. Let $v_0 = (\xi_0, \eta_0, \zeta_0)$. By Lemma 2.4 there are μ, ν in $\mathbb{O}$ with

$$0 < |N(\nu)| \leq i(\mathbb{O})^3 \tag{2-9}$$

such that

$$\nu M \subseteq \mathbb{O}\mu \subseteq M \tag{2-10}$$

for $M = \mathbb{O}\xi_0 + \mathbb{O}\eta_0$. In particular there exist ξ_1, η_1 in $\mathbb{O}$ with $\mu = \eta_1\xi_0 - \xi_1\eta_0$, and we define $v_1 = (\xi_1, \eta_1, 0)$ in $\mathbb{O}^3$. Again by Lemma 2.4 there are μ', ν' in $\mathbb{O}$ with

$$0 < |N(\nu')| \leq i(\mathbb{O})^3 \tag{2-11}$$

such that

$$\nu' M' \subseteq \mathbb{O}\mu' \subseteq M' \tag{2-12}$$

for $M' = \mathbb{O}\mu + \mathbb{O}\zeta_0$. In particular there exist σ, τ in $\mathbb{O}$ with $\mu' = \sigma\mu + \tau\zeta_0$. By (2-10) the numbers $\xi_2 = -\nu\tau\xi_0/\mu$, $\eta_2 = -\nu\tau\eta_0/\mu$ are in $\mathbb{O}$, and so $v_2 = (\xi_2, \eta_2, \sigma\nu)$ is

in $\mathbb{O}^3$. Now we can quickly check that the rows v_0, v_1, v_2 form a matrix V with $\det V = \nu\mu'$; and this is nonzero since $\mu' = 0$ would imply $v_0 = 0$, contradicting primitivity.

It remains to verify the upper bound for $|N(\det V)|$. But (2-10) and (2-12) show that λv_0 is in $\mathbb{O}^3$ for $\lambda = \nu\nu'/\mu'$, so primitivity gives $|N(\mu')| \le |N(\nu\nu')|$. Therefore

$$|N(\det V)| \le \left|N\left(\nu^2\nu'\right)\right| \le i(\mathbb{O})^9$$

by (2-9) and (2-11); and this completes the proof. □

If $\mathbb{O}$ happens to be a maximal order, a more natural proof of Lemma 2.5 might be obtained using the projectivity of torsion-free $\mathbb{O}$-modules. But this does not seem quite straightforward, since our definition of primitivity does not quite imply that $\mathbb{O}^3/\mathbb{O}v_0$ is torsion-free. Further the extension to nonmaximal orders appears to involve exponents of $i(\mathbb{O})$ depending on $m = [K : \mathbb{Q}]$.

In practice we shall estimate $i(\mathbb{O})$ by $d(\mathbb{O})^{1/2}$, as in the class index lemma of [Masser and Wüstholz 1995a, p. 8] for $e = 1$.

At last we can extend the earlier results of this section to ternary forms.

Lemma 2.6. *Let $Q(x, y, z)$ be a ternary quadratic form over K with total signature $(+--)$. Then there are ξ, η, ζ in $\mathbb{O}$ such that $q = Q(\xi, \eta, \zeta)$ is totally positive and*

$$N(q) \le 2^{2m} d(\mathbb{O})^5 |N(d(Q))|^{1/3}.$$

Proof. We follow closely the method in [Gruber and Lekkerkerker 1987, p. 471]. Since K is dense in $\mathbb{R} \otimes K$ it is easy to see that Q takes totally positive values on K^3 and so also on $\mathbb{O}^3$. The norms of these latter values are rational numbers with bounded denominator and so form a discrete set. Thus we can find $v_0 = (\xi_0, \eta_0, \zeta_0)$ in $\mathbb{O}^3$ at which the value $q_0 = Q(\xi_0, \eta_0, \zeta_0)$ is totally positive with minimal norm, say $N_0 = N(q_0)$. Then v_0 must be $\mathbb{O}$-primitive, otherwise we could find a value with strictly smaller norm. We express the variables x, y, z in terms of new variables x', y', z' using the matrix V of Lemma 2.5. So if the new form Q' is defined by $Q'(x', y', z') = Q(x, y, z)$ we now have $q_0 = Q'(1, 0, 0)$. Completing the square on $q_0^{-1}Q'$ gives

$$q_0^{-1}Q'\left(x', y', z'\right) = \left(x' + \alpha y' + \beta z'\right)^2 + Q_1\left(y', z'\right)$$

for α, β in K and a binary form Q_1 over K. Since q_0 is totally positive and Q' has total signature $(+--)$, it follows that Q_1 has total signature $(--)$. Lemma 2.2 applied to $-Q_1$ gives η', ζ' in $\mathbb{O}$ with $q_1 = Q_1(\eta', \zeta')$ totally negative and

$$|N(q_1)| \le 2^m d(\mathbb{O})\, |N(d(Q_1))|^{1/2}.$$

Now

$$d(Q_1) = q_0^{-3} d(Q'), \quad d(Q') = (\det V)^2 d(Q)$$

and so the estimate of Lemma 2.5 and the class index lemma lead to

$$|N(q_1)| \le 2^m N_0^{-3/2} d(\mathbb{O})^{11/2} |N(d(Q_1))|^{1/2}. \tag{2-13}$$

Next define a third form over K by

$$Q''(x'', y'') = q_0^{-1} Q'(x'', \eta' y'', \zeta' y'') = (x'' + \gamma y'')^2 + q_1 (y'')^2$$

for some γ in K. This has total signature $(+-)$. So Lemma 2.3 gives ξ'', η'' in $\mathbb{O}$ with $q'' = Q''(\xi'', \eta'')$ totally positive and $N(q'') \le 2^m d(\mathbb{O})\, |N(d(Q''))|^{1/2}$. Using the estimate (2-13) for $d(Q'') = q_1$ we find that

$$N(q'') \le 2^{3m/2} N_0^{-3/4} d(\mathbb{O})^{15/4} |N(d(Q_1))|^{1/4}. \tag{2-14}$$

Finally $q = Q'(\xi'', \eta'\eta'', \zeta'\eta'') = q_0 q''$ is a totally positive value of Q' on $\mathbb{O}^3$ and so a totally positive value of Q on $\mathbb{O}^3$. Therefore minimality implies $N_0 \le N(q)$, or $N(q'') \ge 1$. Now (2-14) leads at once to the required upper bound for N_0, and this completes the proof. □

Lemmas 2.2, 2.3, and 2.6 above are all partial generalizations of Blaney's theorem from the rationals to totally real number fields. There is no difficulty in extending the induction argument, as in [Gruber and Lekkerkerker 1987, p. 471], to any number of variables, provided one assumes that Q has a total signature which is not negative definite. But it does not seem straightforward to prove the analogous results under the weaker and more natural hypothesis that no conjugate of Q is negative definite.

3. Quaternion algebras and CM-fields

As in the preceding section, let K be a totally real number field of degree m. Let D be a quaternion algebra over K; that is, a noncommutative algebra over K of dimension 4 with center K. For a finitely generated additive subgroup Γ of D of rank r we define the discriminant $d_1(\Gamma)$ as the determinant of the matrix with entries $T_1(\gamma_i \gamma_j)$ $(1 \le i, j \le r)$, where $\gamma_1, \ldots, \gamma_r$ are elements of any $\mathbb{Z}$-basis for Γ, and T_1 denotes the trace from D to $\mathbb{Q}$ obtained for example through left (or right) regular representations. We also have for all δ in D

$$T_1(\delta) = 2T(\operatorname{tr} \delta), \tag{3-1}$$

where as before T is the trace from K to $\mathbb{Q}$ and now tr is the reduced trace from D to K; see, for example, [Reiner 1975, Example 5, p. 7 and Equation (9.7), p. 116] .

There is a canonical involution ρ_0 on D defined by

$$\rho_0(\delta) = (\operatorname{tr} \delta) - \delta \tag{3-2}$$

for all δ in D. Its fixed space, consisting of all δ with $\rho_0(\delta) = \delta$, is just K; while its antifixed space, consisting of all δ with $\rho_0(\delta) = -\delta$, is a K-vector space E of dimension 3. So $D = K \oplus E$.

The following result specifies the ternary quadratic form to which Lemma 2.6 will eventually be applied. Denote the reduced norm from D to K by

$$\mathrm{nm}\,\delta = \delta\rho_0(\delta) = \rho_0(\delta)\delta,$$

and let N as before be the norm from K to $\mathbb{Q}$.

Lemma 3.1. *If α, β, γ are elements of E linearly independent over K, the quadratic form*

$$Q(x, y, z) = -(x\alpha + y\beta + z\gamma)^2 = \mathrm{nm}(x\alpha + y\beta + z\gamma)$$

satisfies

$$N(d(Q)) = (-1)^m d_1(M) d_1(\mathbb{O})^{-3} \tag{3-3}$$

for any order $\mathbb{O}$ in K, where $M = \mathbb{O}\alpha \oplus \mathbb{O}\beta \oplus \mathbb{O}\gamma$.

Proof. If $\xi_1, \ldots, \xi_m$ are elements of a $\mathbb{Z}$-basis for $\mathbb{O}$, then for any λ in K the matrix with entries $T_1(\xi_i\xi_j\lambda)$ $(1 \le i, j \le m)$ has determinant $d_1(\mathbb{O})N(\lambda)$. We can find a K-basis of E consisting of elements $\alpha_0, \beta_0, \gamma_0$ satisfying the standard quaternion relations

$$\alpha_0^2 = \xi, \quad \beta_0^2 = \eta, \quad \gamma_0 = \alpha_0\beta_0 = -\beta_0\alpha_0$$

for ξ, η in K, and now (3-3) follows after a short calculation with $\alpha_0, \beta_0, \gamma_0$ in place of α, β, γ; in fact both sides have the value $N(\xi\eta)^2$.

Next let α, β, γ in E be such that $M = \mathbb{O}\alpha \oplus \mathbb{O}\beta \oplus \mathbb{O}\gamma$ is a submodule of $M_0 = \mathbb{O}\alpha_0 \oplus \mathbb{O}\beta_0 \oplus \mathbb{O}\gamma_0$, so that α, β, γ are related to $\alpha_0, \beta_0, \gamma_0$ by means of a nonsingular matrix V over $\mathbb{O}$. If we can check that

$$|N(\det V)| = [M_0 : M], \tag{3-4}$$

then both sides of (3-3) change by the square of this quantity on replacing M_0 by M, so (3-3) follows for α, β, γ.

Now (3-4) should be in the literature, but we could not find an exact reference. It can be verified *ad hoc* by picking a $\mathbb{Z}$-basis of $\mathbb{O}$ and for each λ in K writing V_λ for the matrix in the corresponding right regular representation; then if V has entries λ, the index $[M_0 : M]$ is the absolute value of the determinant of the matrix with blocks V_λ. By [Reiner 1975, Example 3, p. 7] this determinant is just $N(\det V)$. See also [Reiner 1975, Example 3, p. 231] for another approach. Or one can compare the maximal exterior powers of M and M_0; these have the shape $\mathcal{P}(\det V)$, $\mathcal{P}$ for an $\mathbb{O}$-module $\mathcal{P}$ of rank 1.

Hence (3-3) is established for any such α, β, γ. Finally the general case can be reduced to this case simply by multiplying by a suitable positive integer; and the proof of the present lemma is thereby complete. □

Notice in this lemma that $d_1(\mathbb{O})$ is not quite the same as the $d(\mathbb{O})$ in Section 2; in fact

$$d_1(\mathbb{O}) = 4^m d(\mathbb{O}) \tag{3-5}$$

due to the differing traces.

Next let K_1 be a CM-field over K; that is, a totally imaginary quadratic extension of K. For a finitely generated additive subgroup Γ of K_1 we define the discriminant $d_1(\Gamma)$ as above using the trace T_1 from K_1 to $\mathbb{Q}$. The analogue of (3-1) is

$$T_1(\delta) = T(\operatorname{tr}\delta), \tag{3-6}$$

where T is the trace from K to $\mathbb{Q}$ and tr is the (reduced) trace from K_1 to K. There is a canonical involution ρ_0 on K_1, which we can identify with complex conjugation, and (3-2) continues to hold. We define as before E as the antifixed space, so that $K_1 = K \oplus E$.

Lemma 3.2. *Let $\mathbb{O}_1$ be an order of either D or K_1. Then*:

(a) $|d_1(K \cap \mathbb{O}_1)| \le 2^{4m} |d_1(\mathbb{O}_1)|$.

(b) $|d_1(E \cap \mathbb{O}_1)| \le 2^{4m} |d_1(\mathbb{O}_1)|$.

Proof. Suppose first that $\mathbb{O}_1$ is a maximal order. If $\mathbb{O}_K$ is the ring of integers of K then $\mathbb{O}_K\mathbb{O}_1$ contains $\mathbb{O}_1$ and so must be $\mathbb{O}_1$. In particular $\mathbb{O}_1$ is an $\mathbb{O}_K$-order containing $\mathbb{O}_K$. So [Reiner 1975, Theorem 10.1, p. 125] shows that $\operatorname{tr}\delta$ is in $\mathbb{O}_K$ for all δ in $\mathbb{O}_1$. In particular $\operatorname{tr}\delta$ is in $\mathbb{O}_1$, and now the identity $2\delta = \operatorname{tr}\delta + (2\delta - \operatorname{tr}\delta)$ leads to

$$2\mathbb{O}_1 \subseteq (K \cap \mathbb{O}_1) \oplus (E \cap \mathbb{O}_1) \subseteq \mathbb{O}_1.$$

Since the summands are perpendicular with respect to the reduced trace, and therefore by (3-1), (3-6) also with respect to T_1, taking discriminants gives

$$2^{4m} |d_1(\mathbb{O}_1)| \ge |d_1(K \cap \mathbb{O}_1)|\, |d_1(E \cap \mathbb{O}_1)| \ge |d_1(\mathbb{O}_1)|.$$

Since all these discriminants are nonzero rational integers, (a) and (b) follow when $\mathbb{O}_1$ is maximal.

In general there is a maximal order $\mathbb{O}_m$ containing $\mathbb{O}_1$, and

$$d_1(\mathbb{O}_1) = [\mathbb{O}_m : \mathbb{O}_1]^2 d_1(\mathbb{O}_m),$$

$$d_1(K \cap \mathbb{O}_1) = [K \cap \mathbb{O}_m : K \cap \mathbb{O}_1]^2 d_1(K \cap \mathbb{O}_m).$$

But the second index above does not exceed the first index, so (a) follows in general; and (b) is established similarly. This completes the proof. □

4. Polarizations and representations

Let A be an abelian variety defined over the field $\mathbb{C}$ of complex numbers. Analytically A is isomorphic to the quotient of the tangent space Lie A at the origin by the period group Per A defined as the kernel of the exponential map from Lie A to A.

We write $\hat{A}$ for the dual abelian variety of A. Then Lie $\hat{A}$ can be identified with the space of all $\mathbb{C}$-antilinear maps from Lie A to $\mathbb{C}$, and Per $\hat{A}$ with the subgroup of all such maps whose imaginary parts are integer-valued on Per A (see [Lange and Birkenhake 1992, pp. 35, 73] or [Mumford 1974, p. 86]). Now a homomorphism f from A to $\hat{A}$ takes an element z of Lie A to an element of Lie $\hat{A}$ which itself takes (antilinearly) an element w of Lie A into an element $R(z, w)$ of $\mathbb{C}$. In this way the group $\mathcal{H} = \mathrm{Hom}(A, \hat{A})$ of all homomorphisms f from A to $\hat{A}$ is identified with the group of sesquilinear forms $R = R(z, w)$ (linear in z and antilinear in w) on Lie $A \times$ Lie A whose imaginary parts are integer-valued on Per $A \times$ Per A. The dual map $\hat{f}$ (corresponding to $\overline{R(w, z)}$) is also in $\mathcal{H}$, and we can identify the Néron–Severi group $\mathcal{N} = \mathrm{NS}(A)$ with the subgroup of all such f satisfying $\hat{f} = f$. These correspond to Hermitian R. We shall also be interested in the complementary group $\mathcal{S} = \mathrm{SN}(A)$ of all f with $\hat{f} = -f$. For example, the sum of $\mathrm{NS}(A)$ and $\mathrm{SN}(A)$ is direct, lying between $2\mathcal{H}$ and $\mathcal{H}$.

Interchanging A and $\hat{A}$, we obtain in a similar way the groups

$$\mathcal{H}' = \mathrm{Hom}(\hat{A}, A), \quad \mathcal{N}' = \mathrm{NS}(\hat{A}), \quad \mathcal{S}' = \mathrm{SN}(\hat{A}).$$

For f in $\mathcal{H}$ and f' in $\mathcal{H}'$ we denote by $f'f$ the composition in the ring End A of endomorphisms of A.

Next let Γ, Γ' be additive subgroups of $\mathcal{H}$, $\mathcal{H}'$, respectively, with the same rank, say r. We define the cross-discriminant $c(\Gamma', \Gamma)$, as in [Masser and Wüstholz 1995a, p. 15], as the square of the determinant of the matrix with entries $T_1(\gamma_i' \gamma_j)$ $(1 \le i, j \le r)$, where $\gamma_1, \dots, \gamma_r$ and $\gamma_1', \dots, \gamma_r'$ are elements of $\mathbb{Z}$-bases of Γ, Γ', respectively, and T_1 is the trace from $\mathbb{Q} \otimes \mathrm{End}\, A$ to $\mathbb{Q}$ obtained through regular representations.

From now on (except briefly in Section 7) we shall assume that A is absolutely simple. The next lemma can be regarded as an analogue of Lemma 3.2.

Lemma 4.1. *Suppose that* End A *has* $\mathbb{Z}$*-rank* ℓ. *Then*:

(a) $1 \le c(\mathcal{N}', \mathcal{N}) \le 2^{4\ell} c(\mathcal{H}', \mathcal{H})$.

(b) $1 \le c(\mathcal{S}', \mathcal{S}) \le 2^{4\ell} c(\mathcal{H}', \mathcal{H})$.

Proof. Since $\mathcal{H}$ contains surjective homomorphisms (for example coming from polarizations as in the discussion below), it is easy to see that both $\mathcal{H}$ and $\mathcal{H}'$ have $\mathbb{Z}$-rank ℓ. Further

$$2\mathcal{H} \subseteq \mathcal{N} \oplus \mathcal{S} \subseteq \mathcal{H}, \quad 2\mathcal{H}' \subseteq \mathcal{N}' \oplus \mathcal{S}' \subseteq \mathcal{H}',$$

and taking cross-discriminants gives

$$2^{4\ell} c(\mathcal{H}', \mathcal{H}) \geq c(\mathcal{N}' \oplus \mathcal{S}', \mathcal{N} \oplus \mathcal{S}) = c(\mathcal{N}', \mathcal{N}) c(\mathcal{S}', \mathcal{S}) \geq c(\mathcal{H}', \mathcal{H}) \tag{4-1}$$

provided we check that $\mathcal{N}$ and $\mathcal{S}'$ (as well as $\mathcal{N}'$ and $\mathcal{S}$) are perpendicular with respect to T_1. But this trace is proportional (see [Masser and Wüstholz 1995a, Equation (4.1), p. 14]) to the rational representation trace coming from homology, which is itself proportional to the real part of the analytic representation trace Tr (see, for example, [Lange and Birkenhake 1992, Proposition 2.3, p. 10]). Now pick basis elements of Lie A and then basis elements of Lie $\hat{A}$ dual with respect to the standard pairing. Then f in $\mathcal{N}$ corresponds to a Hermitian matrix F, and f' in $\mathcal{S}'$ corresponds to an antihermitian matrix F'. With the transposes F^t, F'^t we have

$$\operatorname{Tr}(F'F) = \operatorname{Tr}(FF') = \operatorname{Tr}(F'^t F^t) = -\operatorname{Tr}(\bar{F}'\bar{F})$$

and so the real part of $\operatorname{Tr}(F'F)$ is zero. Hence $\mathcal{N}, \mathcal{S}'$ are indeed perpendicular; and similarly for $\mathcal{N}', \mathcal{S}$. Now [Masser and Wüstholz 1995a, Lemma 5.1(b), p. 17] and the nonvanishing of discriminants implies that $c(\mathcal{H}', \mathcal{H}) \neq 0$. Since all the cross-discriminants in (4-1) are rational integers, the inequalities of the present lemma follow at once, and this completes the proof. □

The next result generalizes [Masser and Wüstholz 1995a, Lemma 4.2, p. 16], at least when $B = \hat{A}$. Note that through composition $\mathcal{H}$ and $\mathcal{H}'$ have natural structures of right and left modules, respectively, over $\operatorname{End} A$. We write $\deg \delta$ for the degree of δ in $\operatorname{End} A$ when it is an isogeny. As in Section 1 let n be the dimension of A.

Lemma 4.2. *Let $\mathbb{O}$ in* $\operatorname{End} A$ *be an order of a division subalgebra of $\mathbb{Q} \otimes \operatorname{End} A$. Suppose that Γ in $\mathcal{H}$ is a right $\mathbb{O}$-module of rank* 1 *and that Γ' in $\mathcal{H}'$ is a left $\mathbb{O}$-module of rank* 1. *Suppose further that $c(\Gamma', \Gamma) \neq 0$ and $f'f$ is in $\mathbb{O}$ for every f in Γ and f' in Γ'. Then there are f in Γ and f' in Γ' such that $f'f$ is an isogeny with*

$$\deg f'f \leq c(\Gamma', \Gamma)^n.$$

Proof. There exists f in Γ with

$$[\Gamma : f\mathbb{O}] = I' \leq i'(\mathbb{O})$$

the right class index of $\mathbb{O}$ (see [ibid., p. 13]). And there exists f' in Γ' with

$$[\Gamma' : \mathbb{O}f'] = I \leq i(\mathbb{O})$$

the left class index. The class index lemma of [ibid., p. 8], together with [ibid., Equation (3.11), p. 14], provides estimates for these class indices in terms of the discriminant of $\mathbb{O}$, which divides the discriminant $d_1(\mathbb{O})$ defined using the present trace T_1 (compare (3-5) above). We get

$$c(\mathbb{O}f', f\mathbb{O}) = I^2 I'^2 c(\Gamma', \Gamma) \leq d_1(\mathbb{O})^2 c(\Gamma', \Gamma). \tag{4-2}$$

On the other hand the left side is the square of the determinant of the matrix with entries $T_1(\xi_i \delta \xi_j)$ $(1 \le i, j \le r)$ for $\delta = f'f$ and elements $\xi_1, \dots, \xi_r$ of a $\mathbb{Z}$-basis of $\mathbb{O}$. Using the left (or right) regular representation of δ in $\mathbb{O}$, we find (much as in the proof of Lemma 3.1) that this determinant is $Nd_1(\mathbb{O})$, where N is the norm of δ from $\mathbb{Q} \otimes \mathbb{O}$ to $\mathbb{Q}$. In particular $N \neq 0$ so δ is an isogeny. Finally comparison of norms (see [Masser and Wüstholz 1995a, Equation (4.2), p. 14]) yields

$$N^{2n} = (\deg \delta)^r \ge \deg \delta,$$

and the present lemma follows from (4-2) after cancellation. This completes the proof. □

The ultimate goal of this paper is to obtain information about the polarizations on A. These may be identified with the subset $\mathrm{Pol}\, A$ of $\mathrm{NS}(A)$ corresponding to positive definite Hermitian forms. Recall that every such polarization f gives rise to its Rosati involution ρ on $\mathbb{Q} \otimes \mathrm{End}\, A$ by the equation

$$\rho(\delta) = f^{-1} \hat{\delta} f. \tag{4-3}$$

It is well known (see, for example, [Lange and Birkenhake 1992, Theorem 1.8, p. 120] or [Mumford 1974, Theorem 1, p. 192]) that ρ is a positive involution in the sense that $T_1(\delta \rho(\delta)) > 0$ for all nonzero δ in $\mathbb{Q} \otimes \mathrm{End}\, A$.

The existence of ρ provides a quick method for calculating $\mathrm{NS}(A)$. For multiplication on the left by f^{-1} gives a (noncanonical) identification of $\mathbb{Q} \otimes \mathrm{Hom}(A, \hat{A})$ with $\mathbb{Q} \otimes \mathrm{End}\, A$, and $\mathbb{Q} \otimes \mathrm{NS}(A)$ corresponds to the fixed space of ρ (see [Lange and Birkenhake 1992, Proposition 2.1(a), p. 122] or [Mumford 1974, p. 190]). Similarly $\mathrm{SN}(A)$ corresponds to the antifixed space. Further, multiplication on the right by f gives an identification of $\mathbb{Q} \otimes \mathrm{Hom}(\hat{A}, A)$ with $\mathbb{Q} \otimes \mathrm{End}\, A$; and now it is $\mathbb{Q} \otimes \mathrm{NS}(\hat{A})$ and $\mathbb{Q} \otimes \mathrm{SN}(\hat{A})$ that correspond to the fixed and antifixed spaces, respectively, of ρ.

Recall that A is absolutely simple. Then $D = \mathbb{Q} \otimes \mathrm{End}\, A$ is a division algebra, and we have the following fundamental classification due to Albert (see, for example, the summaries in [Lange and Birkenhake 1992], [Mumford 1974], [Shimura 1963] or the original papers [Albert 1934a; 1935a; 1934b; 1935b]).

Type I: D is a totally real number field.

Type II: D is a totally indefinite quaternion algebra over a totally real number field.

Type III: D is a totally definite quaternion algebra over a totally real number field.

Type IV: D is a division algebra, of dimension e^2 say, over its center, which is a CM-field.

For each type the underlying totally real number field will be denoted by K, and its degree by m. Let $\phi_1, \ldots, \phi_m$ be the different real embeddings of K as in Section 2. For a field F we denote by $\mathcal{M}_e(F)$ the ring of square matrices of order e over F, and we write $\boldsymbol{U}$ for the subring of $\mathcal{M}_2(\mathbb{C})$ consisting of all $\left(\begin{smallmatrix} x & y \\ -\bar{y} & \bar{x} \end{smallmatrix}\right)$. The operation of complex conjugate transposition defines an involution * on $\mathcal{M}_e(\mathbb{R})$, $\mathcal{M}_e(\mathbb{C})$ and $\boldsymbol{U}$, which we extend to m-fold products in the obvious way. We need the following isomorphisms.

Lemma 4.3. *Fix f in* Pol A *with Rosati involution ρ. Then the above real embeddings induce an isomorphism $\phi = (\phi_1, \ldots, \phi_m)$ from $\mathbb{R} \otimes D$ to one of the following rings* (*corresponding to the above types*):

(I) $\mathbb{R}^m = \mathcal{M}_1(\mathbb{R})^m$,

(II) $\mathcal{M}_2(\mathbb{R})^m$,

(III) $\boldsymbol{U}^m$,

(IV) $\mathcal{M}_e(\mathbb{C})^m$.

Further we have

$$\phi(\rho(\delta)) = \phi(\delta)^* \tag{4-4}$$

for every δ in $\mathbb{R} \otimes D$; and for every σ in K, the matrix $\phi_i(\sigma)$ is the identity multiplied by σ^{ϕ_i} $(1 \le i \le m)$.

Proof. All except the last clause is contained in the discussions in [Lange and Birkenhake 1992, pp. 133–141], [Mumford 1974, pp. 201, 202] or [Shimura 1963, pp. 150–153, 155]. As for $\phi_1(\sigma), \ldots, \phi_m(\sigma)$, they must be in the centers of the appropriate rings and therefore multiples of the identity matrix by some scalars. Further these scalars must have the form $\sigma^{\phi_1'}, \ldots, \sigma^{\phi_m'}$ for $\phi_1', \ldots, \phi_m'$ chosen from $\phi_1, \ldots, \phi_m$. But since ϕ is surjective, $\phi_1', \ldots, \phi_m'$ must be all different, and after a permutation we can assume them to be $\phi_1, \ldots, \phi_m$. This completes the proof. □

We next extend ϕ to an analytic representation of $\mathbb{R} \otimes D$ on the tangent space Lie A. Let $\bar{\phi}_1, \ldots, \bar{\phi}_m$ be the complex conjugates of the coordinates of ϕ. For matrices X in $\mathcal{M}_e(\mathbb{C})$ with entries x_{ij} $(1 \le i, j \le e)$, and Y in $\mathcal{M}_h(\mathbb{C})$, define the Kronecker product $X \otimes Y$ in $\mathcal{M}_{eh}(\mathbb{C})$ as in [Shimura 1963, p. 156] or [Lange and Birkenhake 1992, p. 249] to consist of blocks $x_{ij}Y$ $(1 \le i, j \le e)$. Also for matrices $X_1, \ldots, X_k$ define $\operatorname{diag}(X_1, \ldots, X_k)$ as in this last reference, with blocks $X_1, \ldots, X_k$ "down the main diagonal". Finally write $I(e)$ for the identity in $\mathcal{M}_e(\mathbb{C})$.

Lemma 4.4. *Fix f in* Pol A. *There is a basis of* Lie A *such that the corresponding analytic representation Φ sends δ in $\mathbb{R} \otimes D$ to $\Phi(\delta) = \operatorname{diag}(\Phi_1(\delta), \ldots, \Phi_m(\delta))$, with*

(I) $\Phi_i(\delta) = \phi_i(\delta) \otimes I(n/m) \quad (1 \le i \le m)$,

(II) $\Phi_i(\delta) = \phi_i(\delta) \otimes I(n/2m) \quad (1 \le i \le m)$,

(III) $\Phi_i(\delta) = \phi_i(\delta) \otimes I(n/2m) \quad (1 \le i \le m)$,

(IV) $\Phi_i(\delta) = \operatorname{diag}\big(\phi_i(\delta) \otimes I(r_i), \bar{\phi}_i(\delta) \otimes I(s_i)\big) \quad (1 \le i \le m)$

for nonnegative integers r_i, s_i *with* $r_i + s_i = n/em$ $(1 \le i \le m)$.

Proof. See [Shimura 1963, pp. 156, 157]; of course if $r_i = 0$ or $s_i = 0$ then the corresponding block in case (IV) should be omitted. □

The above result leads to the following for the Riemann form $R(z, w)$ associated with the polarization f, where now $z = (z_1, \dots, z_n)^t$, $w = (w_1, \dots, w_n)^t$ are column vectors of $\mathbb{C}^n$ identified with Lie A by means of the above basis.

Lemma 4.5. *Fix* f *in* Pol A; *then with the basis of* Lie A *constructed above, the Riemann form* $R(z, w)$ *associated with* f *has the shape* $z^t F \bar{w}$ *for*

$$F = \operatorname{diag}(F_1, \dots, F_m)$$

with

(I) F_i *of order* $n/m \quad (1 \le i \le m)$,

(II) $F_i = I(2) \otimes F_i'$ *for* F_i' *of order* $n/2m \quad (1 \le i \le m)$,

(III) $F_i = I(2) \otimes F_i'$ *for* F_i' *of order* $n/2m \quad (1 \le i \le m)$,

(IV) $F_i = \operatorname{diag}(I(e) \otimes G_i, I(e) \otimes H_i)$ *for* G_i, H_i *of orders* r_i, s_i, *respectively* $(1 \le i \le m)$.

Proof. The equation (4-3) of ρ leads to

$$R(z, \Phi(\delta)w) = R(\Phi(\rho(\delta))z, w)$$

for every δ in End A. With $r(z, w) = z^t F \bar{w}$ it follows from (4-4) that $F\bar{\Phi}(\delta) = \bar{\Phi}(\delta)F$ for every such δ, and so also for every δ in $\mathbb{R} \otimes D$. Therefore F commutes with every element of $\bar{\Phi}(\mathbb{R} \otimes D) = \Phi(\mathbb{R} \otimes D)$. The required forms are now easy to work out; see, for example, [Shimura 1963, Formulae (32), (33), pp. 161, 162]. This completes the proof. □

5. Preliminary estimates (i)

In this section we establish preliminary estimates for polarizations on simple abelian varieties with endomorphism algebras of types I, III and the commutative case $e = 1$ of type IV. These cases are especially easy to handle because there is only one positive involution on $D = \mathbb{Q} \otimes \text{End } A$ (see [Lange and Birkenhake 1992, Theorem 5.3, p. 135 and Theorem 5.6, p. 139] or [Mumford 1974, Theorem 2, p. 201]). For type I it is the identity; for type III it is the canonical involution of Section 3; and for type IV it induces complex conjugation on the center, so in the commutative case it is also the canonical involution considered in Section 3.

Therefore the totally real number field K is always the fixed space. For the rest of this section we assume that A is simple corresponding to one of the above cases. We write

$$\mathbb{O}_1 = \operatorname{End} A, \quad \mathbb{O} = K \cap \mathbb{O}_1. \tag{5-1}$$

Lemma 5.1. *Suppose that f is in* Pol A *and ζ is totally positive in $\mathbb{O}$. Then $f\zeta$ is in* Pol A.

Proof. Shimura [1963, Proposition 21, p. 185] gives a short elegant proof of this based on Siegel's theorem that ζ is a sum of squares in K. The following demonstration is more elementary.

By Lemma 4.5 the polarization f corresponds to the form $z^t F \bar{w}$ with

$$F = \operatorname{diag}(F_1, \ldots, F_m)$$

(with respect to a suitable basis). So $f\zeta$ corresponds to the form $z^t F_\zeta \bar{w}$ with $F_\zeta = \Phi(\zeta)^t F$. Now it follows easily from Lemmas 4.3 and 4.4 that

$$\Phi(\zeta)^t = \Phi(\zeta) = \operatorname{diag}(\zeta^{\phi_1} I, \ldots, \zeta^{\phi_m} I)$$

for $I = I(n/m)$, and so

$$F_\zeta = \operatorname{diag}(\zeta^{\phi_1} F_1, \ldots, \zeta^{\phi_m} F_m).$$

Since f is a polarization, F is positive definite Hermitian. Therefore $F_1, \ldots, F_m$ are positive definite Hermitian. Since ζ is totally positive, it follows that $\zeta^{\phi_1} F_1, \ldots, \zeta^{\phi_m} F_m$ are also positive definite Hermitian. Hence F_ζ is positive definite Hermitian, and so $f\zeta$ is indeed a polarization. This completes the proof, which works even for the noncommutative case of type IV. □

Lemma 5.2. *The group $\mathcal{N} = \mathrm{NS}(A)$ is a right $\mathbb{O}$-module of rank* 1; *the group $\mathcal{N}' = \mathrm{NS}(\hat{A})$ is a left $\mathbb{O}$-module of rank* 1; *and $f'f$ is in $\mathbb{O}$ for every f in $\mathcal{N}$ and f' in $\mathcal{N}'$.*

Proof. The claims for $\mathcal{N}$ can be checked by noncanonically identifying $\mathbb{Q} \otimes \mathcal{H}$ with $D = \mathbb{Q} \otimes \mathbb{O}_1$ as described in Section 4; this identification respects the right D-module structure. For type I every Rosati involution is the identity; so $\mathcal{N} = \mathcal{H}$, $\mathcal{S} = \{0\}$ and everything is clear. For type III every Rosati involution ρ is canonical, so $\mathcal{H}$, $\mathcal{N}$, $\mathcal{S}$ have $\mathbb{Z}$-ranks $4m, m, 3m$, respectively. So the asserted $\mathbb{O}$-module structure of $\mathcal{N}$ is obvious because ρ fixes $\mathbb{O}$. For the commutative case of type IV, every Rosati involution is again canonical, so $\mathcal{H}$, $\mathcal{N}$, $\mathcal{S}$ have $\mathbb{Z}$-ranks $2m, m, m$, respectively, and again ρ fixes $\mathbb{O}$.

The claims about $\mathcal{N}'$ can be verified similarly by identifying $\mathbb{Q} \otimes \mathcal{H}'$ with D. Finally let f be in $\mathcal{N}$ and f' in $\mathcal{N}'$. It is easy to see that $\mathbb{Q} \otimes \mathcal{N}$ is generated by polarizations. So in proving that $\delta = f'f$ is in $\mathbb{O}$ we may assume that f is a

polarization. Now using $\hat{f} = f$ and a similar equation for f' we find at once that $f^{-1}\hat{\delta} f = \delta$, so δ is fixed by the Rosati involution. So it lies in K and therefore in $\mathbb{O}$ as desired. This completes the proof. □

We can now give our first preliminary estimate for polarizations. We write $\deg f$ for the degree of f in $\mathcal{H} = \mathrm{Hom}(A, \hat{A})$ when it is an isogeny (that is, when $f \neq 0$).

Proposition 5.3. *Suppose that A is simple and its endomorphism algebra is either commutative or a totally definite quaternion algebra over a totally real number field. Then A has a polarization of degree at most $2^{18mn} c(\mathcal{H}', \mathcal{H})^n |d_1(\mathbb{O}_1)|^n$.*

Proof. From Lemma 4.1(a) we have $c(\mathcal{N}', \mathcal{N}) \neq 0$. Now Lemma 5.2 above allows us to apply Lemma 4.2 with $\Gamma = \mathcal{N}, \Gamma' = \mathcal{N}'$ to find an isogeny $\tilde{f}$ in $\mathcal{N}$ with $\deg \tilde{f} \leq c(\mathcal{N}', \mathcal{N})^n$. Again using Lemma 4.1(a) and the fact that $\ell \leq 4m$ in our situation, we get

$$\deg \tilde{f} \leq 2^{16mn} c(\mathcal{H}', \mathcal{H})^n. \tag{5-2}$$

Now there is certainly some polarization f; so we deduce $\tilde{f} = f\sigma$ for some nonzero σ in K. By Lemma 2.1 there is a ξ in $\mathbb{O}$ with $\xi\sigma$ totally positive and $|N(\xi)| \leq d(\mathbb{O})^{1/2}$. Also Lemma 3.2(a) together with (3-5) gives $d(\mathbb{O}) \leq 2^{2m} |d_1(\mathbb{O}_1)|$, and so we get

$$\deg \xi = |N(\xi)|^{2n/m} \leq N(\xi)^{2n} \leq 2^{2mn} |d_1(\mathbb{O}_1)|^n. \tag{5-3}$$

It is clear from this and (5-2) that our proposition is established as soon as we verify that $\tilde{f}\xi$ is a polarization. But there is a positive integer s such that $\zeta = s\sigma\xi$ is in $\mathbb{O}$; and now it follows from Lemma 5.1 that $s\tilde{f}\xi = f\zeta$ is a polarization. So $\tilde{f}\xi$ is too; and this completes the proof. □

6. Preliminary estimates (ii)

We now deal with type II. This is harder because there are now many positive involutions on $D = \mathbb{Q} \otimes \mathrm{End}\, A$; even worse, the canonical involution ρ_0 is not among them. It is here that we need the considerations of Section 2 on quadratic forms.

But first we recall the isomorphism ϕ from $\mathbb{R} \otimes D$ to $\mathcal{M}_2(\mathbb{R})^m$ constructed in Lemma 4.3 from a given polarization on A. We already have Equation (4-4), where * denotes complex conjugate transposition extended to the m-fold product. We also need the following remarks.

Lemma 6.1. *For any δ in $\mathbb{R} \otimes D$ we have*

$$\phi(\rho_0(\delta)) = \phi(\delta)^a,$$

where $(-)^a$ denotes the adjoint involution extended to the m-fold product.

Proof. The involution ρ_0 on $\mathbb{R}\otimes D$ induces via ϕ an involution i on $\mathcal{M}=\mathcal{M}_2(\mathbb{R})^m$. Since $\delta+\rho_0(\delta)$, $\delta\rho_0(\delta)$ are both fixed by ρ_0, they are in the center for every δ in $\mathbb{R}\otimes D$. It follows that $X+i(X)$, $X\,i(X)$ are both in the center of $\mathcal{M}$ for every X in $\mathcal{M}$. From this we conclude with a simple calculation that $i(X)=X^a$ for every X, which is the assertion of the present lemma. □

For the next remark we recall the decomposition $D=K\oplus E$ of Section 3.

Lemma 6.2. *For any α, β, γ in E linearly independent over K, the quadratic form*

$$Q(x,y,z)=-(x\alpha+y\beta+z\gamma)^2$$

has total signature $(+--)$.

Proof. Fix rational numbers x, y, z; then

$$q=Q(x,y,z)=\pi\rho_0(\pi)$$

for $\pi=x\alpha+y\beta+z\gamma$, so calculating $\phi_i(q)$ from both Lemma 4.3 and 6.1 using $MM^a=(\det M)I(2)$ on $\mathcal{M}_2(\mathbb{R})$ shows that

$$Q^{\phi_i}(x,y,z)=\det\phi_i(\pi)=\det(x\phi_i(\alpha)+y\phi_i(\beta)+z\phi_i(\gamma))\quad(1\le i\le m).$$

Since α, β, γ are linearly independent over K, their images in $\mathbb{R}\otimes D$ are linearly independent over $\mathbb{R}\otimes K$ and so their images by each ϕ_i in $\mathcal{M}_2(\mathbb{R})$ are linearly independent over $\mathbb{R}$. Further their traces are zero, again by Lemma 6.1. But it is easy to check that the determinant function evaluated on the zero trace subspace of $\mathcal{M}_2(\mathbb{R})$ has signature $(+--)$. The assertion of the present lemma is now evident, and this completes the proof. □

Although ρ_0 itself is not positive, it is known that every positive involution ρ on D is defined by

$$\rho(\delta)=\omega^{-1}\rho_0(\delta)\omega, \tag{6-1}$$

where ω is a nonzero element of D with ω^2 in K and totally negative (see, for example, [Lange and Birkenhake 1992, Theorem 5.3, p. 135], [Mumford 1974, Theorem 2, p. 201] or [Shimura 1963, Proposition 2, p. 153]). A simple calculation shows that ω lies in E (not K). Let $\Omega\subseteq E$ be the set of such elements ω. Our first task is to find a small element of Ω in the order $\mathbb{O}_1$. We keep the notation (5-1).

Lemma 6.3. *There exists $\tilde{\omega}$ in $\Omega\cap\mathbb{O}_1$ with*

$$|N(\tilde{\omega})|\le 2^{6m}|d_1(\mathbb{O}_1)|^3.$$

Proof. Write $M_1=E\cap\mathbb{O}_1$. By Lemma 3.2(b) we have

$$|d_1(M_1)|\le 2^{4m}|d_1(\mathbb{O}_1)|. \tag{6-2}$$

Now M_1 is an $\mathbb{O}$-module of rank 3, so by the definition of the generalized class index in [Masser and Wüstholz 1995a, p. 8] it contains a free $\mathbb{O}$-module $M = \mathbb{O}\alpha \oplus \mathbb{O}\beta \oplus \mathbb{O}\gamma$ with index $[M_1 : M] \le i_3(\mathbb{O})$. By the class index lemma we have $i_3(\mathbb{O}) \le d(\mathbb{O})^{3/2}$, and it follows using (3-5) and (6-2) that

$$|d_1(M)| = [M_1 : M]^2 |d_1(M_1)| \le 2^{-2m} d_1(\mathbb{O})^3 |d_1(\mathbb{O}_1)|.$$

So by Lemma 3.1 the quadratic form

$$Q(x, y, z) = -(x\alpha + y\beta + z\gamma)^2$$

satisfies

$$|N(d(Q))| \le 2^{-2m} |d_1(\mathbb{O}_1)|. \tag{6-3}$$

And by Lemma 6.2 it has total signature $(+ - -)$. So Lemma 2.6 provides ξ, η, ζ in $\mathbb{O}$ such that $q = -\tilde{\omega}^2$ is totally positive for $\tilde{\omega} = \xi\alpha + \eta\beta + \zeta\gamma$ in $\mathbb{O}_1$; and by (6-3)

$$N(q) \le 2^{4m/3} d(\mathbb{O})^5 |d_1(\mathbb{O}_1)|^{1/3}.$$

Finally the desired estimate for $|N(\tilde{\omega})| = N(q)^{1/2}$, even with exponent $\frac{8}{3}$, follows from this together with (3-5) and Lemma 3.2(a); the proof is thereby complete. □

We next give an analogue of Lemma 5.1; recall from Section 3 that tr is the reduced trace from D to K.

Lemma 6.4. *Suppose that f in* Pol A *has Rosati involution ρ given by* (6-1) *for some ω in Ω.*

(a) *Then $f_0 = f\omega^{-1}$ is in $\mathbb{Q} \otimes \mathcal{S}$, and we have*

$$f_0^{-1} \hat{\delta} f_0 = \rho_0(\delta) \tag{6-4}$$

for every δ in D.

(b) *Suppose further that ω' is in Ω. Then* $\operatorname{tr} \epsilon \ne 0$ *for $\epsilon = \omega^{-1}\omega'$.*

(c) *Suppose in addition that ϵ is in $\mathbb{O}_1$ with* $\operatorname{tr} \epsilon$ *totally positive. Then $f\epsilon$ is in* Pol A.

Proof. By the definition (4-3) of ρ we have

$$f^{-1} \hat{\delta} f = \omega^{-1} \rho_0(\delta) \omega \tag{6-5}$$

for every δ in D. Put $\delta = \omega$; we get $f^{-1}\hat{\omega} f = -\omega$, and using $\hat{f} = f$ we see easily that the dual of f_0 satisfies $\hat{f}_0 = -f_0$. So f_0 is in $\mathbb{Q} \otimes \mathcal{S}$ as desired. Also the formula (6-4) is immediate from (6-5). This establishes (a).

As for (b), we fix $\phi = (\phi_1, \ldots, \phi_m)$ corresponding to f as in Lemma 4.3, and we start by proving that the matrices

$$E_i = \phi_i(\epsilon) \quad (1 \le i \le m)$$

in $\mathcal{M}_2(\mathbb{R})$ are symmetric. For (4-4) gives the relations

$$\phi_i\big(\omega^{-1}\rho_0(\epsilon)\omega\big) = \phi_i(\epsilon)^t \quad (1 \le i \le m).$$

Also $\rho_0(\epsilon) = \omega'\omega^{-1}$, and we end up with the desired symmetry properties.

Next by Lemma 6.1 we have

$$(\det E_i)I = \phi_i(\epsilon)\phi_i(\rho_0(\epsilon)) = \phi_i\big(\omega^{-1}\omega'\omega'\omega^{-1}\big) \quad (1 \le i \le m)$$

for $I = I(2)$. But $\omega^2 = \sigma$ and $\omega'^2 = \sigma'$ are both totally negative in K; thus $\omega^{-1}\omega'\omega'\omega^{-1} = \sigma^{-1}\sigma'$ is totally positive in K, and the above matrix is $(\sigma^{-1}\sigma')^{\phi_i} I$. We deduce that

$$\det E_i > 0 \quad (1 \le i \le m). \tag{6-6}$$

If t_i is the trace of E_i, then we also have

$$t_i I = \phi_i(\epsilon) + \phi_i(\rho_0(\epsilon)) = 2\phi_i(\tau) = 2\tau^{\phi_i} I \quad (1 \le i \le m) \tag{6-7}$$

with $\tau = \operatorname{tr}\epsilon$ the reduced trace. Now $\tau = 0$ would imply $t_i = 0$ $(1 \le i \le m)$, but the trace of a symmetric matrix in $\mathcal{M}_2(\mathbb{R})$ cannot vanish if its determinant is positive as in (6-6). So indeed $\tau \ne 0$, and this establishes (b).

Lastly, suppose τ is totally positive. We prove that $E_1, \dots, E_m$ are positive definite. For (6-7) now implies that $t_i > 0$ $(1 \le i \le m)$, and it is easy to check that a symmetric matrix in $\mathcal{M}_2(\mathbb{R})$ is positive definite if (and only if) its determinant and trace are both positive. Thus $E_1, \dots, E_m$ are indeed positive definite.

Finally from Lemma 4.5 we know that the polarization f corresponds to the form $z^t F \bar{w}$ with

$$F = \operatorname{diag}(F_1, \dots, F_m),$$

where $F_i = I \otimes F_i'$ for F_i' of order $n/2m$ $(1 \le i \le m)$. As in the proof of Lemma 5.1, the map $f\epsilon$ corresponds to $z^t F_\epsilon \bar{w}$ with $F_\epsilon = \Phi(\epsilon)^t F$, and we have

$$\Phi(\epsilon) = \operatorname{diag}(\Phi_1(\epsilon), \dots, \Phi_m(\epsilon))$$

with $\Phi_i(\epsilon) = E_i \otimes I'$ $(1 \le i \le m)$ for $I' = I(n/2m)$. By symmetry we get

$$\Phi_i(\epsilon)^t F_i = (E_i \otimes I')(I \otimes F_i') = E_i \otimes F_i' \quad (1 \le i \le m),$$

so that

$$F_\epsilon = \operatorname{diag}(E_1 \otimes F_1', \dots, E_m \otimes F_m').$$

Since F is positive definite Hermitian, so are $F_1, \dots, F_m$ and also $F_1', \dots, F_m'$. We have just seen that $E_1, \dots, E_m$ are positive definite Hermitian (and even symmetric). Now it is well known (and almost trivial) that the Kronecker product of two positive definite Hermitian matrices is also positive definite Hermitian. It follows that F_ϵ is

positive definite Hermitian, and so $f\epsilon$ is a polarization. This establishes (c), and so completes the proof of the present lemma. □

The next result is the analogue of Lemma 5.2, but with the Néron–Severi group replaced by the Severi–Néron group.

Lemma 6.5. *The group $\mathcal{S} = \mathrm{SN}(A)$ is a right $\mathbb{O}$-module of rank* 1; *the group $\mathcal{S}' = \mathrm{SN}(\hat{A})$ is a left $\mathbb{O}$-module of rank* 1; *and $f'f$ is in $\mathbb{O}$ for every f in $\mathcal{S}$ and f' in $\mathcal{S}'$.*

Proof. The claims for $\mathcal{S}$ can be checked by noncanonical identification, as in the proof of Lemma 5.2. In fact a Rosati involution of the form (6-1) has antifixed space $K\omega$, since the equation $\rho(\delta\omega) = -\delta\omega$ turns out to be equivalent to $\rho_0(\delta) = \delta$. So $\mathcal{H}, \mathcal{N}, \mathcal{S}$ have $\mathbb{Z}$-ranks $4m, 3m, m$, respectively. The claims for $\mathcal{S}'$ can be verified similarly.

Finally let f be in $\mathcal{S}$ and f' in $\mathcal{S}'$. In showing that $f'f$ is in $\mathbb{O}$ we can assume $f \neq 0$. By Lemma 6.4(a) applied to some polarization (of course not the present f) there is some f_0 in $\mathbb{Q} \otimes \mathcal{S}$ with $f_0^{-1}\hat{\delta} f_0 = \rho_0(\delta)$ for every δ in D. Since $f_0 = f\sigma$ for some σ in K, we deduce also

$$f^{-1}\hat{\delta} f = \rho_0(\delta) \tag{6-8}$$

for every δ in D. With $\delta = f'f$ using $\hat{f} = -f$ and a similar equation for f' leads immediately to $f'f = \rho_0(f'f)$, so $f'f$ is in K and therefore in $\mathbb{O}$ as desired. This completes the proof. □

It is perhaps interesting to note that (6-8) above says that any nonzero f in $\mathcal{S}$ (for type II) determines the canonical involution on D in the same way as a polarization determines its Rosati involution (compare (4-3)).

We now establish our second preliminary estimate for polarizations.

Proposition 6.6. *Suppose that A is simple and its endomorphism algebra is a totally indefinite quaternion algebra over a totally real number field. Then A has a polarization of degree at most*

$$2^{30mn} c(\mathcal{H}', \mathcal{H})^n |d_1(\mathbb{O}_1)|^{7n}.$$

Proof. From Lemma 4.1(b) we have $c(\mathcal{S}', \mathcal{S}) \neq 0$. Lemma 6.5 allows us to apply Lemma 4.2 with $\Gamma = \mathcal{S}$, $\Gamma' = \mathcal{S}'$ to find an isogeny $\tilde{f}$ in $\mathcal{S}$ with $\deg \tilde{f} \leq c(\mathcal{S}', \mathcal{S})^n$. Again using Lemma 4.1(b) and $\ell = 4m$, we get

$$\deg \tilde{f} \leq 2^{16mn} c(\mathcal{H}', \mathcal{H})^n. \tag{6-9}$$

Next by Lemma 6.3 there is $\tilde{\omega}$ in $\Omega \cap \mathbb{O}_1$ with $|N(\tilde{\omega})| \leq 2^{6m} |d_1(\mathbb{O}_1)|^3$, and therefore

$$\deg \tilde{\omega} = |N(\tilde{\omega})|^{2n/m} \leq |N(\tilde{\omega})|^{2n} \leq 2^{12mn} |d_1(\mathbb{O}_1)|^{6n}. \tag{6-10}$$

Now there is certainly some polarization f, and the Rosati involution for f has the form (6-1) for some ω in Ω. By Lemma 6.4(a), $f_0 = f\omega^{-1}$ lies in $\mathbb{Q} \otimes \mathcal{S}$, and therefore $\tilde{f} = f_0\sigma$ for some nonzero σ in K. By Lemma 6.4(b), $\tau = \mathrm{tr}(\omega^{-1}\tilde{\omega})$ is nonzero and so we can use Lemma 2.1 to find ξ in $\mathbb{O}$ such that $\sigma\tau\xi$ is totally positive and $|N(\xi)| \le d(\mathbb{O})^{1/2}$. Exactly as in (5-3) above we find

$$\deg \xi \le 2^{2mn} |d_1(\mathbb{O}_1)|^n.$$

Now it is clear from this and (6-9), (6-10) that the proposition is established as soon as we verify that $\tilde{f}\tilde{\omega}\xi$ is a polarization. But there is a positive integer s such that $\epsilon = \omega^{-1}\omega'$ is in $\mathbb{O}_1$ for $\omega' = s(\tilde{\omega}\sigma\xi)$, and by construction $\mathrm{tr}\,\epsilon = s(\sigma\tau\xi)$ is totally positive. So from Lemma 6.4(c) we see that $f\epsilon = s(\tilde{f}\tilde{\omega}\xi)$ is a polarization. So $\tilde{f}\tilde{\omega}\xi$ is too; and this completes the proof. □

7. Conclusion

We prove the theorem first. Thus let A be a simple abelian variety of dimension n whose endomorphism algebra is commutative or has the property that its center is totally real of degree m. Then we are in the situation of Section 5 or 6, and the appropriate proposition shows that A has a polarization of degree at most

$$2^{30mn} c(\mathcal{H}', \mathcal{H})^n |d_1(\mathbb{O}_1)|^{7n}, \tag{7-1}$$

where $\mathcal{H} = \mathrm{Hom}(A, \hat{A})$, $\mathcal{H}' = \mathrm{Hom}(\hat{A}, A)$ and $\mathbb{O}_1 = \mathrm{End}\, A$.

Now suppose that A is defined over a number field of degree d. We use positive constants $C_1, C_2, \ldots$ depending only on n and d, and we estimate the quantities in (7-1) in terms of $h = \max\{1, h(A)\}$ using Lemma 6.1 of [Masser and Wüstholz 1995a, p. 19]; this says that

$$\max\{c(\mathcal{H}', \mathcal{H}), |d_1(\mathbb{O}_1)|\} \le C_1 h^{\lambda},$$

where $\lambda = \lambda(8n)$ for a certain monotonically increasing function. The inequality of our theorem follows immediately, with exponent $8n\lambda(8n)$.

To prove the first corollary, we note that if A is simple of squarefree dimension n then its endomorphism algebra D is necessarily of the form considered in the theorem. For we only have to rule out the noncommutative case of type IV. In this case D has dimension $e^2 \ge 4$ over its center, which is a CM-field of degree $2m$. Now it is well known that the $\mathbb{Q}$-dimension $2me^2$ of D must divide $2n$ (see [Lange and Birkenhake 1992, Proposition 5.7, p. 141] or [Mumford 1974, p. 182]). This is here impossible and so the first corollary is proved.

Similarly, as preparation for the proof of the second corollary, we note that if A is simple of dimension $n \le 7$ then D is also as in the theorem. Here the only possibility is $e^2 = 4$ and then $m = 1$, $n = 4$.

Now it is a fact that such a case is impossible for simple A, but we could not find a completely satisfactory explicit reference in the literature. Without using this fact, the second corollary would follow only for dimension n at most 3. So we feel obliged to add some remarks about the impossible case.

Everything can be found in Albert's papers [1934a; 1935a], but the reader may well appreciate a more modern exposition. There are two subcases characterized by $r_1 s_1 = 0$ and $r_1 s_1 \neq 0$. The first of these is covered by [Albert 1934a, Theorem 3, p. 13]. A modern treatment (which also implies that A is isogenous to the fourth power of a CM elliptic curve) is given in Shimura [1963, Proposition 14, p. 176]. See [Lange and Birkenhake 1992, Exercise 3, p. 286].

Next if $r_1 s_1 \neq 0$ then $r_1 = s_1 = 1$ by virtue of $r_1 + s_1 = 2$. So this subcase is covered by [Albert 1935a, Theorem 20, p. 391] and also [Shimura 1963, Proposition 19, p. 184]. However Shimura's conclusion that A is isogenous to the square of an abelian surface (of endomorphism type II with $m = 1$) is valid only for what he calls "generic" A; his arguments are definitely moduli-space-theoretic in nature. Our own A is defined over a number field and so unlikely to be generic; on the other hand it is known that specialization only increases the endomorphism ring. Now the generic ring already has rank 16 over $\mathbb{Z}$, whereas the maximum rank for simple A of dimension 4 is only 8 (see above). A general result independent of such considerations is given in [Lange and Birkenhake 1992, Exercise 5, p. 286].

This last subcase $r_1 = s_1 = 1$ can also be treated using only a very elementary specialization argument, paying due attention to the discrepancy between Shimura's analytic concept of generic and the more usual algebraic concept. We omit the details.

We now prove the second corollary. Suppose first that A is an abelian variety of dimension n, not necessarily simple, defined over a number field k of degree d. By [Masser and Wüstholz 1995a, Theorem I, p. 5] there are abelian subvarieties $A_1, \ldots, A_r$ of A, simple over the algebraic closure $\bar{k}$, together with an isogeny g from A to $A' = A_1 \times \cdots \times A_r$ of degree

$$\deg g \leq C_2 h^{\kappa} \tag{7-2}$$

for $\kappa = \kappa(n)$ depending only on n. Also, as in [Masser and Wüstholz 1995a, p. 6], $A_1, \ldots, A_r$ are necessarily defined over an extension of k of relative degree at most C_3. Assume that the endomorphism algebras of $A_1, \ldots, A_r$ are all of the type considered in our theorem. As we have observed, this is automatically true if $n \leq 7$. Then A_i has a polarization f_i of degree at most $C_4 \max\{1, h(A_i)\}^{8n_i\lambda}$, where λ is as above and n_i is the dimension of A_i $(1 \leq i \leq r)$. As in [Masser and Wüstholz 1995a, p. 6] we have $h(A) \leq C_5 h$ $(1 \leq i \leq r)$, and so

$$\deg f_i \leq C_6 h^{8n_i\lambda} \quad (1 \leq i \leq r).$$

Therefore $A' = \prod A_i$ has a polarization f with

$$\deg f = \prod(\deg f_i) \le C_7 h^{8n\lambda}. \tag{7-3}$$

Finally the "pullback" $\hat{g} f g$ is a polarization on A whose degree is $(\deg g)^2(\deg f)$. So by (7-2) and (7-3) this completes the proof of the second corollary, with exponent $8n\lambda(8n) + 2\kappa(n)$.

References

[Albert 1934a] A. A. Albert, "On the construction of Riemann matrices, I", *Ann. of Math.* (2) **35**:1 (1934), 1–28. MR 1503140 Zbl 0010.00304

[Albert 1934b] A. A. Albert, "A solution of the principal problem in the theory of Riemann matrices", *Ann. of Math.* (2) **35**:3 (1934), 500–515. MR 1503176 Zbl 0010.00401

[Albert 1935a] A. A. Albert, "On the construction of Riemann matrices, II", *Ann. of Math.* (2) **36**:2 (1935), 376–394. MR 1503230 Zbl 0011.38904

[Albert 1935b] A. A. Albert, "Involutorial simple algebras and real Riemann matrices", *Ann. of Math.* (2) **36**:4 (1935), 886–964. MR 1503260 Zbl 0012.39102

[Baker and Wüstholz 2007] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, New Mathematical Monographs **9**, Cambridge University Press, 2007. MR 2009e:11001 Zbl 1145.11004

[Bost 1996a] J.-B. Bost, "Intrinsic heights of stable varieties and abelian varieties", *Duke Math. J.* **82**:1 (1996), 21–70. MR 97j:14025 Zbl 0867.14010

[Bost 1996b] J.-B. Bost, "Périodes et isogénies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)", pp. 115–161 in *Séminaire Bourbaki*, Astérisque **237**, Société Mathématique de France, Paris, 1996. MR 98k:11073 Zbl 0936.11042

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026

[Gaudron and Rémond 2013] É. Gaudron and G. Rémond, "Polarisations et isogénies", preprint, 2013, http://math.univ-bpclermont.fr/∼gaudron/art13.pdf.

[Gruber and Lekkerkerker 1987] P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*, 2nd ed., North-Holland Mathematical Library **37**, North-Holland, Amsterdam, 1987. MR 88j:11034 Zbl 0611.10017

[Howe 1995] E. W. Howe, "Bounds on polarizations of abelian varieties over finite fields", *J. Reine Angew. Math.* **467** (1995), 149–155. MR 96i:11064 Zbl 0832.14033

[Lange and Birkenhake 1992] H. Lange and Ch.. Birkenhake, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften **302**, Springer, Berlin, 1992. MR 94j:14001 Zbl 0779.14012

[Masser 2006] D. W. Masser, "From $2^{\sqrt{2}}$ to polarizations on abelian varieties", pp. 37–43 in *Colloquium De Giorgi 2006*, edited by U. Zannier, Colloquia **1**, Edizione della Normale, Pisa, 2006. MR 2008m:14086 Zbl 1231.11081

[Masser and Wüstholz 1993a] D. W. Masser and G. Wüstholz, "Periods and minimal abelian subvarieties", *Ann. of Math.* (2) **137**:2 (1993), 407–458. MR 94g:11040 Zbl 0796.11023

[Masser and Wüstholz 1993b] D. W. Masser and G. Wüstholz, "Isogeny estimates for abelian varieties, and finiteness theorems", *Ann. of Math.* (2) **137**:3 (1993), 459–472. MR 95d:11074 Zbl 0804.14019

[Masser and Wüstholz 1993c] D. W. Masser and G. Wüstholz, "Galois properties of division fields of elliptic curves", *Bull. London Math. Soc.* **25**:3 (1993), 247–254. MR 94d:11036 Zbl 0809.14026

[Masser and Wüstholz 1994] D. W. Masser and G. Wüstholz, "Endomorphism estimates for abelian varieties", *Math. Z.* **215**:4 (1994), 641–653. MR 95b:14032 Zbl 0826.14025

[Masser and Wüstholz 1995a] D. W. Masser and G. Wüstholz, "Factorization estimates for abelian varieties", *Inst. Hautes Études Sci. Publ. Math.* **81** (1995), 5–24. MR 96j:11083 Zbl 0854.11030

[Masser and Wüstholz 1995b] D. W. Masser and G. Wüstholz, "Refinements of the Tate conjecture for abelian varieties", pp. 211–224 in *Abelian varieties* (Egloffstein, 1993), edited by W. Barth et al., de Gruyter, Berlin, 1995. MR 97a:11092 Zbl 0876.14029

[Mumford 1974] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1974. MR 44 #219 Zbl 0223.14022

[Reiner 1975] I. Reiner, *Maximal orders*, London Mathematical Society Monographs **5**, Academic Press, London, 1975. Corrected reprint published by Oxford Univ. Press, 2003. MR 52 #13910 Zbl 0305.16001

[Shimura 1963] G. Shimura, "On analytic families of polarized abelian varieties and automorphic functions", *Ann. of Math.* (2) **78** (1963), 149–192. MR 27 #5934 Zbl 0142.05402

Communicated by John Henry Coates
Received 2013-04-22 Revised 2013-12-13 Accepted 2014-02-15

David.Masser@unibas.ch *Mathematisches Institut, Universität Basel, CH-4051 Basel, Switzerland*

gisbert.wuestholz@math.ethz.ch *Departement für Mathematik, ETH-Zentrum, CH-8092 Zürich, Switzerland*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1071

msp

Compatibility between Satake and Bernstein isomorphisms in characteristic p

Rachel Ollivier

We study the center of the pro-p Iwahori–Hecke ring $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ of a connected split p-adic reductive group G. For k an algebraically closed field of characteristic p, we prove that the center of the k-algebra $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$ contains an affine semigroup algebra which is naturally isomorphic to the Hecke k-algebra $\mathscr{H}(\mathrm{G}, \rho)$ attached to an irreducible smooth k-representation ρ of a given hyperspecial maximal compact subgroup of G. This isomorphism is obtained using the inverse Satake isomorphism defined in our previous work.

We apply this to classify the simple supersingular $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$-modules, study the supersingular block in the category of finite-length $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$-modules, and relate the latter to supersingular representations of G.

1. Introduction

The Iwahori–Hecke ring of a split p-adic reductive group G is the convolution ring of $\mathbb{Z}$-valued functions with compact support in $\mathrm{I}\backslash\mathrm{G}/\mathrm{I}$, where I denotes an Iwahori subgroup of G. It is isomorphic to the quotient of the extended braid group ring associated to G by quadratic relations in the standard generators. If one replaces I by its pro-p Sylow subgroup $\tilde{\mathrm{I}}$, then one obtains the pro-p Iwahori–Hecke ring $\widetilde{\mathrm{H}}_{\mathbb{Z}}$. In this article we study the center of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$. We are motivated by the smooth representation theory of G over an algebraically closed field k with

MSC2010: primary 20C08; secondary 22E50.
Keywords: Hecke algebras, characteristic p, Satake isomorphism, supersingularity.

characteristic p and subsequently will be interested in the k-algebra $\widetilde{\mathrm{H}}_k := \widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$. We construct an isomorphism of k-algebras between a subring of the center of $\widetilde{\mathrm{H}}_k$ and (generalizations of) spherical Hecke k-algebras by means of the inverse mod p Satake isomorphism defined in [Ollivier 2012]. This result is the *compatibility between Bernstein and Satake isomorphisms* referred to in the title of this article. We then explore some consequences of this compatibility. In particular, we study and relate the notions of supersingularity for Hecke modules and k-representations of G.

1A. ***Framework and results.*** Let $\mathfrak{F}$ be a nonarchimedean locally compact field with residue characteristic p and k an algebraic closure of the residue field. We choose a uniformizer ϖ. Let $\mathrm{G} := \mathbf{G}(\mathfrak{F})$ be the group of $\mathfrak{F}$-rational points of a connected reductive group $\mathbf{G}$ over $\mathfrak{F}$, which we assume to be $\mathfrak{F}$-split. In the semisimple building $\mathscr{X}$ of G, we choose and fix a chamber C, which amounts to choosing an Iwahori subgroup I in G, and we denote by $\tilde{\mathrm{I}}$ the pro-p Sylow subgroup of I. The choice of C is unique up to conjugacy by an element of G. We consider the associated pro-p Iwahori–Hecke ring $\widetilde{\mathrm{H}}_{\mathbb{Z}} := \mathbb{Z}[\tilde{\mathrm{I}}\backslash\mathrm{G}/\tilde{\mathrm{I}}]$ of $\mathbb{Z}$-valued functions with compact support in $\tilde{\mathrm{I}}\backslash\mathrm{G}/\tilde{\mathrm{I}}$ under convolution.

Since G is split, C has at least one hyperspecial vertex x_0, and we denote by K the associated maximal compact subgroup of G. Fix a maximal $\mathfrak{F}$-split torus T in G such that the corresponding apartment $\mathscr{A}$ in $\mathscr{X}$ contains C. The set $\mathrm{X}_*(\mathrm{T})$ of cocharacters of T is naturally equipped with an action of the finite Weyl group $\mathfrak{W}$. The choice of x_0 and C induces a natural choice of a positive Weyl chamber of $\mathscr{A}$, that is to say, of a semigroup $\mathrm{X}_*^+(\mathrm{T})$ of dominant cocharacters of T.

1A1. *The complex case.* The structure of the spherical algebra $\mathbb{C}[\mathrm{K}\backslash\mathrm{G}/\mathrm{K}]$ of complex functions compactly supported on $\mathrm{K}\backslash\mathrm{G}/\mathrm{K}$ is understood thanks to the classical Satake isomorphism [1963] (see also [Gross 1998; Haines 2001])

$$s : \mathbb{C}[\mathrm{K}\backslash\mathrm{G}/\mathrm{K}] \xrightarrow{\sim} (\mathbb{C}[\mathrm{X}_*(\mathrm{T})])^{\mathfrak{W}}.$$

On the other hand, the complex Iwahori–Hecke algebra $\mathrm{H}_{\mathbb{C}} := \mathbb{C}[\mathrm{I}\backslash\mathrm{G}/\mathrm{I}]$ of complex functions compactly supported on $\mathrm{I}\backslash\mathrm{G}/\mathrm{I}$ contains a large commutative subalgebra $\mathcal{A}_{\mathbb{C}}$ defined as the image of the *Bernstein map* $\theta : \mathbb{C}[\mathrm{X}_*(\mathrm{T})] \hookrightarrow \mathrm{H}_{\mathbb{C}}$, which depends on the choice of the dominant Weyl chamber (see [Lusztig 1989, Section 3.2]). The algebra $\mathrm{H}_{\mathbb{C}}$ is free of finite rank over $\mathcal{A}_{\mathbb{C}}$ and its center $\mathscr{Z}(\mathrm{H}_{\mathbb{C}})$ is contained in $\mathcal{A}_{\mathbb{C}}$. Furthermore, the map θ yields an isomorphism

$$b : (\mathbb{C}[\mathrm{X}_*(\mathrm{T})])^{\mathfrak{W}} \xrightarrow{\sim} \mathscr{Z}(\mathrm{H}_{\mathbb{C}}).$$

This was proved by Bernstein ([Lusztig 1989, Section 3.5]; see also [Haines 2001, Theorem 2.3]). By [Dat 1999, Corollary 3.1] and [Haines 2001, Proposition 10.1],

the *Bernstein isomorphism* b is compatible with s, in the sense that the composition $(e_{\mathrm{K}} \star \cdot)b$ is an inverse for s, where $(e_{\mathrm{K}} \star \cdot)$ denotes the convolution by the characteristic function of K.

1A2. *Bernstein and Satake isomorphisms in characteristic p.* After defining an integral version of the complex Bernstein map, Vignéras [2005] gave a basis for the center of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ and proved that $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ is noetherian and finitely generated over its center. In the first section of this article, we define a subring $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ of the center of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ over which $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ is still finitely generated. In Proposition 2.8 we prove that $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ is not affected by the choice of another apartment containing C and of another hyperspecial vertex of C, as long as it is conjugate to x_0. In particular, if $\mathbf{G}$ is of adjoint type or $\mathbf{G} = \mathrm{GL}_n$, then $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ depends only on the choice of the uniformizer ϖ.

The natural image of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ in $\widetilde{\mathrm{H}}_k = \widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$ is denoted by $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$, and we prove that it has an affine semigroup algebra structure. More precisely, we have an isomorphism of k-algebras (Proposition 2.10)

$$k[\mathrm{X}_*^+(\mathrm{T})] \xrightarrow{\sim} \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \subseteq \widetilde{\mathrm{H}}_k. \tag{1-1}$$

By the main theorem in [Herzig 2011b] (and in [Ollivier 2012]), this makes $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ isomorphic to the algebra $\mathscr{H}(\mathrm{G}, \rho)$ of any irreducible smooth k-representation ρ of K. Note that when ρ is the k-valued trivial representation $\mathbf{1}_{\mathrm{K}}$ of K, one retrieves the convolution algebra $k[\mathrm{K}\backslash\mathrm{G}/\mathrm{K}] = \mathscr{H}(\mathrm{G}, \mathbf{1}_{\mathrm{K}})$.

In [Ollivier 2012], we constructed an isomorphism

$$\mathcal{T} : k[\mathrm{X}_*^+(\mathrm{T})] \xrightarrow{\sim} \mathscr{H}(\mathrm{G}, \rho). \tag{1-2}$$

Here we prove the following theorem:

Theorem 4.3. *We have a commutative diagram of isomorphisms of k-algebras*

$$\begin{array}{ccc} k[\mathrm{X}_*^+(\mathrm{T})] & \xrightarrow{(1\text{-}1)} & \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \\ \| & & \downarrow \\ k[\mathrm{X}_*^+(\mathrm{T})] & \xrightarrow{\mathcal{T}} & \mathscr{H}(\mathrm{G}, \rho) \end{array} \tag{1-3}$$

where the vertical arrow on the right-hand side is the natural morphism of k-algebras (4-3) *described in Section 4.*

The isomorphism $\mathcal{T}$ was constructed in [Ollivier 2012] by means of generalized integral Bernstein maps, as are the subring $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ and the map (1-1) in the current article. By analogy with the complex case, we can see the map (1-1) as an isomorphism à la Bernstein in characteristic p. The above commutative diagram can then be interpreted as a statement of compatibility between Satake and Bernstein

isomorphisms in characteristic p. Note that under the hypothesis that the derived subgroup of $\mathbf{G}$ is simply connected, it is proved in [Ollivier 2012] that $\mathcal{T}$ is the inverse of the mod p Satake isomorphism defined in [Herzig 2011b]. (The extra hypothesis on $\mathbf{G}$ is probably not necessary).

If we worked with the Iwahori–Hecke algebra $k[\mathrm{I}\backslash\mathrm{G}/\mathrm{I}]$, the analog of $\mathcal{Z}^\circ(\widetilde{\mathrm{H}}_k)$ would actually be the whole center of $k[\mathrm{I}\backslash\mathrm{G}/\mathrm{I}]$. We prove:

Theorem 2.14. *The center of the Iwahori–Hecke k-algebra $k[\mathrm{I}\backslash\mathrm{G}/\mathrm{I}]$ is isomorphic to $k[\mathrm{X}_*^+(\mathrm{T})]$.*

1A3. *Generalized integral Bernstein maps.* One ingredient of the construction of $\mathcal{T}$ in [Ollivier 2012] and of the proof of Theorem 4.3 is the definition of $\mathbb{Z}$-linear injective maps

$$\mathcal{B}_F^\sigma : \mathbb{Z}[\widetilde{\mathrm{X}}_*(\mathrm{T})] \to \widetilde{\mathrm{H}}_\mathbb{Z}$$

defined on the group ring of the (extended) cocharacters $\widetilde{\mathrm{X}}_*(\mathrm{T})$, which are multiplicative when restricted to the semigroup ring of any chosen Weyl chamber of $\widetilde{\mathrm{X}}_*(\mathrm{T})$ (see Section 1B5 for the definition of $\widetilde{\mathrm{X}}_*(\mathrm{T})$). The image of $\mathcal{B}_F^\sigma$ happens to be a commutative subring of $\widetilde{\mathrm{H}}_\mathbb{Z}$, which we denote by $\mathcal{A}_F^\sigma$. The parameter σ is a sign and F is a standard facet (a facet of C containing x_0 in its closure). The choice of F corresponds to the choice of a Weyl chamber in $\mathscr{A}$: for example, if $F = C$ (resp. x_0), then the corresponding Weyl chamber is the dominant (resp. antidominant) one.

The maps $\mathcal{B}_F^\sigma$ are called *integral Bernstein maps* because they are generalizations of the Bernstein map θ mentioned in Section 1A1. In the complex case, it is customary to consider either θ which is constructed using the dominant chamber, or θ^- which is constructed using the antidominant chamber (see the discussion in the introduction of [Haines and Pettet 2002] for example). By a result by Bernstein [Lusztig 1983], a basis for the center of $\mathrm{H}_\mathbb{C}$ is given by the central Bernstein functions

$$\sum_{\lambda' \in \mathcal{O}} \theta(\lambda'),$$

where $\mathcal{O}$ ranges over the $\mathfrak{W}$-orbits in $\mathrm{X}_*(\mathrm{T})$. We refer to [Haines 2001] for the geometric interpretation of these functions. It is natural to ask whether using θ^- instead of θ in the previous formula yields the same central element in $\mathrm{H}_\mathbb{C}$. The answer is yes (see [Haines and Pettet 2002, Section 2.2.2]). The proof is based on [Lusztig 1983, Corollary 8.8] and relies on the combinatorics of the Kazhdan–Lusztig polynomials. Note that there is no theory of Kazhdan–Lusztig polynomials for the complex pro-p Iwahori–Hecke algebra.

Integral (and pro-p) versions of θ and θ^- for the ring $\widetilde{\mathrm{H}}_\mathbb{Z}$ were defined in [Vignéras 2005]. In our language they correspond respectively to $\mathcal{B}_C^+ = \mathcal{B}_{x_0}^-$ and

$\mathcal{B}^+_{x_0} = \mathcal{B}^-_C$. It is also proved there that a $\mathbb{Z}$-basis for the center of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ is given by

$$\sum_{\lambda' \in \mathbb{O}} \mathcal{B}^+_C(\lambda'), \tag{1-4}$$

where $\mathbb{O}$ ranges over the $\mathfrak{W}$-orbits in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. It is now natural to ask whether the element (1-4) is the same if (a) we use $-$ instead of $+$, and if, more generally, (b) we use any standard facet F instead of C, and any sign σ. We prove:

Lemma 3.4. *The element*

$$\sum_{\lambda' \in \mathbb{O}} \mathcal{B}^\sigma_F(\lambda')$$

in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ *does not depend on the choice of the standard facet* F *and of the sign* σ.

To prove the lemma, we first answer positively question (a) above; we then study and exploit the behavior of the integral Bernstein maps upon a process of parabolic induction. In passing we also consider question (a) in the k-algebra $\widetilde{\mathrm{H}}_k$ in the case when G is semisimple, and we suggest a link between such questions and the duality for finite-length $\widetilde{\mathrm{H}}_k$-modules defined in [Ollivier and Schneider 2012] (see Proposition 3.3).

1A4. In Section 5, we define and study a natural topology on $\widetilde{\mathrm{H}}_k$ which depends only on the conjugacy class of x_0. It is the $\mathfrak{I}$-adic topology, where $\mathfrak{I}$ is a natural monomial ideal of the affine semigroup algebra $\mathfrak{X}^\circ(\widetilde{\mathrm{H}}_k)$.

We define the supersingular block of the category of finite length $\widetilde{\mathrm{H}}_k$-modules to be the full subcategory of the modules that are continuous for the $\mathfrak{I}$-adic topology on $\widetilde{\mathrm{H}}_k$ (Proposition-Definition 5.10). A finite length $\widetilde{\mathrm{H}}_k$-module then turns out to be in the supersingular block if and only if all its irreducible constituents are supersingular in the sense of [Vignéras 2005].

In the case when the root system of G is irreducible, we establish the following results. We classify the simple supersingular $\widetilde{\mathrm{H}}_k$-modules (Theorem 5.14 and subsequent corollary). (For example, when G is semisimple simply connected, the simple supersingular modules all have dimension 1.) We prove in passing that even if the ideal $\mathfrak{I}$ does depend on the choices made, the supersingular block is independent of all the choices.

Theorem 5.14 extends Theorem 5 of [Vignéras 2005] and Theorem 7.3 of [Ollivier 2010], which dealt with the case of GL_n and relied on explicit *minimal expressions* for certain Bernstein functions associated to the minuscule coweights. The results of those two papers together proved a "numerical Langlands correspondence for Hecke modules" of $\mathrm{GL}_n(\mathfrak{F})$: there is a bijection between the finite set of all simple n-dimensional supersingular $\widetilde{\mathrm{H}}_k$-modules and the finite set of all irreducible n-dimensional smooth k-representations of the absolute Galois group of $\mathfrak{F}$, where

the action of the uniformizer ϖ on the Hecke modules and the determinant of the Frobenius on the Galois representations are fixed. Recently, Große-Klönne constructed a functor from the category of finite-length $\widetilde{\mathrm{H}}_k$-modules for $\mathrm{GL}_n(\mathbb{Q}_p)$ to the category of étale (φ, Γ)-modules. This functor induces a bijection between the two finite sets above, turning the "numerical" correspondence into a natural and explicit correspondence in the case of $\mathrm{GL}_n(\mathbb{Q}_p)$. In fact, Große-Klönne [2013a] has constructed such a functor (with values in a category of modified étale (φ, Γ)-modules) in the case of a general split group over $\mathbb{Q}_p$. In the case of $\mathrm{SL}_n(\mathfrak{F})$, Koziol [2013] has defined packets of simple supersingular $\widetilde{\mathrm{H}}_k$-modules and built a bijection between the set of packets and a certain set of projective k-representations of the absolute Galois group of $\mathfrak{F}$; if $\mathfrak{F} = \mathbb{Q}_p$, this bijection is proved to be compatible with Große-Klönne's functor and therefore with the explicit Langlands-type correspondence for Hecke modules of $\mathrm{GL}_n(\mathbb{Q}_p)$. This result is a first step towards a mod p principle of functoriality for Hecke modules.

The current article provides, in the case of a general split group, a classification of the objects that one wants to apply Große-Klönne's functor to, in order to investigate the possibility of a Langlands-type correspondence for Hecke modules in general.

1A5. In Section 5F we consider an admissible irreducible smooth k-representation π of G. In the case where the derived subgroup of $\mathbf{G}$ is simply connected, we use the fact that (1-2) is the inverse of the mod p Satake isomorphism to prove that if π is supersingular, then

$$\pi \text{ is a quotient of } \mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1 \,/\, \mathfrak{I}\, \mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1. \tag{1-5}$$

The condition (1-5) is equivalent to saying that $\pi^{\tilde{\mathrm{I}}}$ contains an irreducible supersingular $\widetilde{\mathrm{H}}_k$-module.

When $\mathrm{G} = \mathrm{GL}_n(\mathfrak{F})$ and $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$, we use the classification of the nonsupersingular representations obtained in [Herzig 2011a], the work on generalized special representations in [Große-Klönne 2013b], and our Lemma 3.4 to prove that the condition (1-5) is in fact a characterization of the supersingular representations (Theorem 5.27).

Finally, we comment in Section 5F on the generalization of this characterization to the case of a split group (with simply connected derived subgroup), and on the independence of the characterization of the choices made.

We raise the question of the possibility of a direct proof of this characterization that does not use the classification of the nonsupersingular representations.

1B. ***Notation and preliminaries.*** We choose the valuation $\mathrm{val}_{\mathfrak{F}}$ on $\mathfrak{F}$ normalized by $\mathrm{val}_{\mathfrak{F}}(\varpi) = 1$, where ϖ is the chosen uniformizer. The ring of integers of $\mathfrak{F}$ is denoted by $\mathfrak{O}$ and its residue field by $\mathbb{F}_q$, where q is a power of the prime number p. Recall that k denotes an algebraic closure of $\mathbb{F}_q$. Let $\mathbf{G}_{x_0}$ and $\mathbf{G}_{\boldsymbol{C}}$

denote the Bruhat–Tits group schemes over $\mathfrak{O}$ whose $\mathfrak{O}$-valued points are K and I respectively. Their reductions over the residue field $\mathbb{F}_q$ are denoted by $\overline{\mathbf{G}}_{x_0}$ and $\overline{\mathbf{G}}_{\boldsymbol{C}}$. Note that $\mathrm{G} = \mathbf{G}_{x_0}(\mathfrak{F}) = \mathbf{G}_{\boldsymbol{C}}(\mathfrak{F})$. By [Tits 1979, 3.4.2, 3.7 and 3.8], $\overline{\mathbf{G}}_{x_0}$ is connected reductive and $\mathbb{F}_q$-split. Therefore we have $\mathbf{G}^{\circ}_{\boldsymbol{C}}(\mathfrak{O}) = \mathbf{G}_{\boldsymbol{C}}(\mathfrak{O}) = \mathrm{I}$ and $\mathbf{G}^{\circ}_{x_0}(\mathfrak{O}) = \mathbf{G}_{x_0}(\mathfrak{O}) = \mathrm{K}$. Denote by K_1 the prounipotent radical of K. The quotient K/K_1 is isomorphic to $\overline{\mathbf{G}}_{x_0}(\mathbb{F}_q)$. The Iwahori subgroup I is the preimage in K of the $\mathbb{F}_q$-rational points of a Borel subgroup $\overline{\mathbf{B}}$ with Levi decomposition $\overline{\mathbf{B}} = \overline{\mathbf{T}}\overline{\mathbf{N}}$. The pro-$p$ Iwahori subgroup $\tilde{\mathrm{I}}$ is the preimage in I of $\overline{\mathbf{N}}(\mathbb{F}_q)$. The preimage of $\overline{\mathbf{T}}(\mathbb{F}_q)$ is the maximal compact subgroup T^0 of T. Note that $\mathrm{T}^0/\mathrm{T}^1 = \mathrm{I}/\tilde{\mathrm{I}} = \overline{\mathbf{T}}(\mathbb{F}_q)$, where $\mathrm{T}^1 := \mathrm{T}^0 \cap \tilde{\mathrm{I}}$.

1B1. *Affine root datum.* To the choice of T is attached the root datum

$$(\Phi, \mathrm{X}^*(\mathrm{T}), \check{\Phi}, \mathrm{X}_*(\mathrm{T})).$$

This root system is reduced because the group $\mathbf{G}$ is $\mathfrak{F}$-split. We denote by $\mathfrak{W}$ the finite Weyl group $N_{\mathrm{G}}(\mathrm{T})/\mathrm{T}$, the quotient by T of the normalizer of T. Recall that $\mathscr{A}$ denotes the apartment of the semisimple building attached to T (see [Tits 1979; Schneider and Stuhler 1997, Section I.1], and we follow the notation of [Ollivier 2012, Section 2.2]). We denote by $\langle \cdot, \cdot \rangle$ the perfect pairing $\mathrm{X}_*(\mathrm{T}) \times \mathrm{X}^*(\mathrm{T}) \to \mathbb{Z}$. The elements in $\mathrm{X}_*(\mathrm{T})$ will be called coweights. We identify $\mathrm{X}_*(\mathrm{T})$ with the subgroup T/T^0 of the extended Weyl group $\mathrm{W} = N_{\mathrm{G}}(\mathrm{T})/\mathrm{T}^0$ as in [Tits 1979, I.1] and [Schneider and Stuhler 1997, Section I.1]: to an element $g \in \mathrm{T}$ corresponds the vector $\nu(g) \in \mathbb{R} \otimes_{\mathbb{Z}} \mathrm{X}_*(\mathrm{T})$ defined by

$$\langle \nu(g), \chi \rangle = -\operatorname{val}_{\mathfrak{F}}(\chi(g)) \quad \text{for any } \chi \in \mathrm{X}^*(\mathrm{T}), \tag{1-6}$$

and ν induces the required isomorphism $\mathrm{T}/\mathrm{T}^0 \cong \mathrm{X}_*(\mathrm{T})$. The group T/T^0 acts by translation on $\mathscr{A}$ via ν. The actions of $\mathfrak{W}$ and T/T^0 combine into an action of W on $\mathscr{A}$ as recalled in [Schneider and Stuhler 1997, p. 102]. Since x_0 is a special vertex of the building, W is isomorphic to the semidirect product $\mathfrak{W} \ltimes \mathrm{X}_*(\mathrm{T})$, where we see $\mathfrak{W}$ as the fixator in W of any lift of x_0 in the extended apartment [Tits 1979, 1.9]. A coweight λ will sometimes be denoted by e^{λ} to underline that we see it as an element in W, meaning as a translation on $\mathscr{A}$.

Denote by Φ_{aff} the set of affine roots. The choice of the chamber C implies in particular the choice of the positive affine roots Φ^+_{aff} taking nonnegative values on C. The choice of x_0 as an origin of $\mathcal{A}$ implies that we identify the affine roots taking value zero at x_0 with Φ. We set $\Phi^+ := \Phi^+_{\mathrm{aff}} \cap \Phi$ and $\Phi^- = -\Phi^+$. The affine roots can be described the following way: $\Phi_{\mathrm{aff}} = \Phi \times \mathbb{Z} = \Phi^+_{\mathrm{aff}} \sqcup \Phi^-_{\mathrm{aff}}$, where

$$\Phi^+_{\mathrm{aff}} := \{(\alpha, r) : \alpha \in \Phi, r > 0\} \cup \{(\alpha, 0) : \alpha \in \Phi^+\}.$$

Let Π be the basis for Φ^+ consisting of the set of simple roots. The finite Weyl

group $\mathfrak{W}$ is a Coxeter system with generating set $S := \{s_\alpha : \alpha \in \Pi\}$, where s_α denotes the (simple) reflection at the hyperplane $\langle \cdot, \alpha \rangle = 0$. Denote by $\preceq$ the partial ordering on $\mathrm{X}_*^+(\mathrm{T})$ associated to Π. Let Π_m be the set of roots in Φ that are minimal elements for $\preceq$. Define the set of simple affine roots by $\Pi_{\mathrm{aff}} := \{(\alpha, 0) : \alpha \in \Pi\} \cup \{(\alpha, 1) : \alpha \in \Pi_m\}$. Identifying α with $(\alpha, 0)$, we consider Π a subset of Π_{aff}. For $A \in \Pi_{\mathrm{aff}}$, denote by s_A the following associated reflection: $s_A = s_\alpha$ if $A = (\alpha, 0)$ and $s_A = s_\alpha e^{\check{\alpha}}$ if $A = (\alpha, 1)$. The action of W on the coweights induces an action on the set of affine roots: W acts on Φ_{aff} by $we^\lambda : (\alpha, r) \mapsto (w\alpha, r - \langle \lambda, \alpha \rangle)$, where we denote by $(w, \alpha) \mapsto w\alpha$ the natural action of $\mathfrak{W}$ on Φ. The length on the Coxeter system $(\mathfrak{W}, S)$ extends to W in such a way that the length $\ell(w)$ of $w \in \mathrm{W}$ is the number of affine roots $A \in \Phi_{\mathrm{aff}}^+$ such that $w(A) \in \Phi_{\mathrm{aff}}^-$. It satisfies the following formula, for $A \in \Pi_{\mathrm{aff}}$ and $w \in \mathrm{W}$:

$$\ell(ws_A) = \begin{cases} \ell(w) + 1 & \text{if } w(A) \in \Phi_{\mathrm{aff}}^+, \\ \ell(w) - 1 & \text{if } w(A) \in \Phi_{\mathrm{aff}}^-. \end{cases} \tag{1-7}$$

The affine Weyl group is defined as the subgroup $\mathrm{W}_{\mathrm{aff}}$ of W generated by $S_{\mathrm{aff}} := \{s_A : A \in \Pi_{\mathrm{aff}}\}$. The length function ℓ restricted to $\mathrm{W}_{\mathrm{aff}}$ coincides with the length function of the Coxeter system $(\mathrm{W}_{\mathrm{aff}}, S_{\mathrm{aff}})$ [Bourbaki 1968, V.3.2, Théorème 1(i)]. Recall from [Lusztig 1989, Section 1.5] that $\mathrm{W}_{\mathrm{aff}}$ is a normal subgroup of W: the set Ω of elements with length zero is an abelian subgroup of W and W is the semidirect product $\mathrm{W} = \Omega \ltimes \mathrm{W}_{\mathrm{aff}}$. The length ℓ is constant on the double cosets of W mod Ω. In particular, Ω normalizes S_{aff}.

The extended Weyl group W is equipped with a partial order $\leq$ that extends the Bruhat order on $\mathrm{W}_{\mathrm{aff}}$. By definition, given $w = \omega w_{\mathrm{aff}}$, $w = \omega' w'_{\mathrm{aff}} \in \Omega \ltimes \mathrm{W}_{\mathrm{aff}}$, we have $w \leq w'$ if $\omega = \omega'$ and $w_{\mathrm{aff}} \leq w'_{\mathrm{aff}}$ in the Bruhat order on $\mathrm{W}_{\mathrm{aff}}$ (see for example [Haines 2001, Section 2.1]).

We fix a lift $\hat{w} \in N_{\mathrm{G}}(\mathrm{T})$ for any $w \in \mathrm{W}$. By Bruhat decomposition, G is the disjoint union of all $\mathrm{I}\hat{w}\mathrm{I}$ for $w \in \mathrm{W}$.

1B2. *Orientation character.* The stabilizer of the chamber C in W is Ω. We define as in [Ollivier and Schneider 2012, Section 3.1] the orientation character $\epsilon_C : \Omega \to \{\pm 1\}$ of C by setting $\epsilon_C(\omega) = +1$ (resp. -1) if ω preserves (resp. reverses) a given orientation of C. Since $\mathrm{W}/\mathrm{W}_{\mathrm{aff}} = \Omega$, we can see ϵ_C as a character of W trivial on $\mathrm{W}_{\mathrm{aff}}$. By definition of the Bruhat order on W, we have $\epsilon_C(w) = \epsilon_C(w')$ for $w, w' \in \mathrm{W}$ satisfying $w \leq w'$.

On the other hand, the extended Weyl group acts by affine isometries on the Euclidean space $\mathscr{A}$. We therefore have a determinant map $\det : \mathrm{W} \to \{\pm 1\}$ which is trivial on $\mathrm{X}_*(\mathrm{T})$. An orientation of C is a choice of a cyclic ordering of its set of vertices (in the geometric realization of $\mathscr{A}$). Therefore, $\det(\omega)$ is the signature of the permutation of the vertices of C induced by $\omega \in \Omega$, and $\det(\omega) = \epsilon_C(\omega)$.

Lemma 1.4. (i) *For $w \in \mathrm{W}_{\mathrm{aff}}$, we have $\det(w) = (-1)^{\ell(w)}$.*

(ii) *For $\lambda \in \mathrm{X}_*(\mathrm{T})$, we have $\epsilon_{\boldsymbol{C}}(w) = (-1)^{\ell(e^\lambda)}$ for any $w \in \mathrm{W}$ such that $w \leq e^\lambda$.*

Proof. Part (i) comes from the fact that $\det s = -1$ for $s \in S_{\mathrm{aff}}$. For (ii), by definition of the Bruhat order it is enough to prove that $\epsilon_{\boldsymbol{C}}(e^\lambda) = (-1)^{\ell(e^\lambda)}$ for $\lambda \in \mathrm{X}_*(\mathrm{T})$. Decompose $e^\lambda = \omega w_{\mathrm{aff}}$ with $w \in \mathrm{W}_{\mathrm{aff}}$ and $\omega \in \Omega$. Recall that ω has length zero. Since $\epsilon_{\boldsymbol{C}}$ is trivial on $\mathrm{W}_{\mathrm{aff}}$, we have $\epsilon_{\boldsymbol{C}}(e^\lambda) = \epsilon_{\boldsymbol{C}}(\omega) = \det \omega$. Since e^λ has unit determinant, we get $\det \omega = \det w_{\mathrm{aff}} = (-1)^{\ell(w_{\mathrm{aff}})} = (-1)^{\ell(e^\lambda)}$. □

1B3. *Distinguished cosets representatives.*

Proposition 1.5. (i) *The set $\mathcal{D}$ of all elements $d \in \mathrm{W}$ satisfying $d^{-1}(\Phi^+) \subset \Phi^+_{\mathrm{aff}}$ is a system of representatives of the right cosets $\mathfrak{W}\backslash\mathrm{W}$. It satisfies*

$$\ell(wd) = \ell(w) + \ell(d) \quad \text{for any } w \in \mathfrak{W} \text{ and } d \in \mathcal{D}. \tag{1-8}$$

In particular, d is the unique element with minimal length in $\mathfrak{W}d$.

(ii) *An element $d \in \mathcal{D}$ can be written uniquely as $d = e^\lambda w$, with $\lambda \in \mathrm{X}^+_*(\mathrm{T})$ and $w \in \mathfrak{W}$. We then have $\ell(e^\lambda) = \ell(d) + \ell(w^{-1}) = \ell(d) + \ell(w)$.*

(iii) *For $s \in S_{\mathrm{aff}}$ and $d \in \mathcal{D}$, we are in one of the following situations*:

- *$\ell(ds) = \ell(d) - 1$, in which case $ds \in \mathcal{D}$.*
- *$\ell(ds) = \ell(d) + 1$, in which case either $ds \in \mathcal{D}$ or $ds \in \mathfrak{W}d$.*

Proof. This proposition is proved in [Ollivier 2010, Lemma 2.6, Proposition 2.7] in the case of $\mathrm{G} = \mathrm{GL}_n(\mathfrak{F})$. It is checked in [Ollivier and Schneider 2012, Proposition 4.6] that it remains valid for a general split reductive group (see also [Ollivier 2012, Proposition 2.2] for (ii)), except for point (iii) when $s \in S_{\mathrm{aff}} - S$. We check here that the argument goes through. Let $s \in S_{\mathrm{aff}}$ and A be the corresponding affine root. Let $d \in \mathcal{D}$ and suppose that $ds \notin \mathcal{D}$; then there is $\beta \in \Pi$ such that $(ds)^{-1}\beta \in \Phi^-_{\mathrm{aff}}$ while $d^{-1}\beta \in \Phi^+_{\mathrm{aff}}$. This implies that $d^{-1}\beta = A$, which in particular ensures that $dA \in \Phi^+_{\mathrm{aff}}$ and therefore $\ell(ds) = \ell(d) + 1$. Furthermore, $dsd^{-1} = s_{dA} = s_\beta \in \mathfrak{W}$. □

There is an action of the group G on the semisimple building $\mathscr{X}$ recalled in [Schneider and Stuhler 1997, p. 104] that extends the action of $N_{\mathrm{G}}(\mathrm{T})$ on the standard apartment. For F a standard facet, we denote by $\mathcal{P}^\dagger_{\boldsymbol{F}}$ the stabilizer of F in G.

Proposition 1.6. (i) *The Iwahori subgroup* I *acts transitively on the apartments of $\mathscr{X}$ containing $\boldsymbol{C}$.*

(ii) *The stabilizer $\mathcal{P}^\dagger_{x_0}$ of x_0 acts transitively on the chambers of $\mathscr{X}$ containing x_0 in their closure.*

(iii) *A* G*-conjugate of x_0 in the closure of C is a $\mathcal{P}^\dagger_{\boldsymbol{C}}$-conjugate of x_0.*

Proof. Part (i) is [Bruhat and Tits 1984, 4.6.28]. For (ii), we first consider C' a chamber of $\mathscr{A}$ containing x_0 in its closure. Since the group W acts transitively on the chambers of $\mathscr{A}$, there is $d \in \mathcal{D}$ and $w_0 \in \mathfrak{W}$ such that $C' = w_0 dC$ and C contains $d^{-1}x_0$ in its closure. By [Ollivier and Schneider 2012, Proposition 4.13i.], this implies that $d^{-1}C = C$, and therefore $C' = w_0 C$ or, when considering the action of G on the building, $C' = \hat{w}_0 C$, where $\hat{w}_0 \in \mathrm{K} \cap N_G(\mathrm{T})$ denotes a lift for w_0. Now, let C'' be a chamber of $\mathscr{X}$ containing x_0 in its closure. By [Bruhat and Tits 1972, Corollaire 2.2.6], there is $k \in \mathcal{P}^\dagger_{x_0}$ such that kC'' is in $\mathscr{A}$. Applying the previous observation, C'' is a $\mathcal{P}^\dagger_{x_0}$-conjugate of C. Lastly, let gx_0 (with $g \in \mathrm{G}$) be a conjugate of x_0 in the closure of C. By (ii), the chamber $g^{-1}C$ is of the form kC for $k \in \mathcal{P}^\dagger_{x_0}$, which implies that $gk \in \mathcal{P}^\dagger_C$ and gx_0 is a $\mathcal{P}^\dagger_C$-conjugate of x_0. □

Remark 1.7. By [Ollivier and Schneider 2012, Lemma 4.9], $\mathcal{P}^\dagger_C$ is the disjoint union of all $\mathrm{I}\hat{\omega}\mathrm{I} = \hat{\omega}\mathrm{I}$ for $\omega \in \Omega$. Therefore, a G-conjugate of x_0 in the closure of C is a $\mathcal{P}^\dagger_C \cap N_{\mathrm{G}}(\mathrm{T})$-conjugate of x_0.

1B4. *Weyl chambers.* The set of dominant coweights $\mathrm{X}_*^+(\mathrm{T})$ is the set of all $\lambda \in \mathrm{X}_*(\mathrm{T})$ such that $\langle \lambda, \alpha \rangle \geq 0$ for all $\alpha \in \Phi^+$. It is called the dominant chamber. Its opposite is the antidominant chamber. A coweight λ such that $\langle \lambda, \alpha \rangle > 0$ for all $\alpha \in \Phi^+$ is called strongly dominant. By [Bushnell and Kutzko 1998, Lemma 6.14], strongly dominant elements do exist.

We call a facet F of $\mathscr{A}$ standard if it is a facet of C containing x_0 in its closure. Attached to a standard facet F is the subset Φ_F of all roots in Φ taking value zero on F and the subgroup $\mathfrak{W}_F$ of $\mathfrak{W}$ generated by the simple reflections stabilizing F. Let $\Phi_F^+ := \Phi^+ \cap \Phi_F$ and $\Phi_F^- := \Phi^- \cap \Phi_F$. Define the following Weyl chambers in $\mathrm{X}_*(\mathrm{T})$ as in [Ollivier 2012, Section 4.1.1]:

$$\mathscr{C}^+(F) = \{\lambda \in \mathrm{X}_*(\mathrm{T}) \text{ such that } \langle \lambda, \alpha \rangle \geq 0 \text{ for all } \alpha \in (\Phi^+ - \Phi_F^+) \cup \Phi_F^-\}$$

and its opposite $\mathscr{C}^-(F) = -\mathscr{C}^+(F)$. They are respectively the images of the dominant and antidominant chambers under the longest element w_F in $\mathfrak{W}_F$.

By Gordan's lemma [Kempf et al. 1973, p. 7], a Weyl chamber is finitely generated as a semigroup.

1B5. We follow the notations of [Ollivier 2012, Sections 2.2.2, 2.2.3]. Recall that T^1 is the pro-p Sylow subgroup of T^0. We denote by $\widetilde{\mathrm{W}}$ the quotient of $N_{\mathrm{G}}(\mathrm{T})$ by T^1, and obtain the exact sequence

$$0 \longrightarrow \mathrm{T}^0/\mathrm{T}^1 \longrightarrow \widetilde{\mathrm{W}} \longrightarrow \mathrm{W} \longrightarrow 0.$$

The group $\widetilde{\mathrm{W}}$ parametrizes the double cosets of G modulo $\tilde{\mathrm{I}}$. We fix a lift $\hat{w} \in N_{\mathrm{G}}(\mathrm{T})$ for any $w \in \widetilde{\mathrm{W}}$ and denote by τ_w the characteristic function of the double coset $\tilde{\mathrm{I}}\hat{w}\tilde{\mathrm{I}}$. The set of all $(\tau_w)_{w \in \widetilde{\mathrm{W}}}$ is a $\mathbb{Z}$-basis for $\widetilde{\mathrm{H}}_{\mathbb{Z}}$, which was defined in the introduction

to be the convolution ring of $\mathbb{Z}$-valued functions with compact support in $\tilde{\mathrm{I}}\backslash \mathrm{G}/\tilde{\mathrm{I}}$. For $g \in \mathrm{G}$, we will also use the notation τ_g for the characteristic function of the double coset $\tilde{\mathrm{I}}g\tilde{\mathrm{I}}$.

For Y a subset of W, we denote by $\widetilde{Y}$ its preimage in $\widetilde{\mathrm{W}}$. In particular, we have the preimage $\widetilde{\mathrm{X}}_*(\mathrm{T})$ of $\mathrm{X}_*(\mathrm{T})$. Similarly to those of $\mathrm{X}_*(\mathrm{T})$, its elements will be denoted by λ or e^λ and called coweights. For $\alpha \in \Phi$, we inflate the function $\langle \cdot, \alpha \rangle$ defined on $\mathrm{X}_*(\mathrm{T})$ to $\widetilde{\mathrm{X}}_*(\mathrm{T})$. We still call the elements in the preimage $\widetilde{\mathrm{X}}_*^+(\mathrm{T})$ of $\mathrm{X}_*^+(\mathrm{T})$ *dominant coweights*. For σ a sign and F a standard facet, we consider the preimage of $\mathscr{C}^\sigma(F)$ in $\widetilde{\mathrm{X}}_*(\mathrm{T})$, and we still denote it by $\mathscr{C}^\sigma(F)$.

The length function ℓ on W pulls back to a length function ℓ on $\widetilde{\mathrm{W}}$ [Vignéras 2005, Proposition 1]. For $u, v \in \widetilde{\mathrm{W}}$ we write $u \le v$ (resp. $u < v$) if their projections $\bar{u}$ and $\bar{v}$ in W satisfy $\bar{u} \le \bar{v}$ (resp. $\bar{u} < \bar{v}$).

1B6. We emphasize the following remark which will be important for the definition of the subring $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$ of the center of $\widetilde{\mathrm{H}}_\mathbb{Z}$ in Section 2B.

For $\lambda \in \mathrm{X}_*^+(\mathrm{T})$, the element $\lambda(\varpi^{-1}) \in N_\mathrm{G}(\mathrm{T})$ is a lift for e^λ, viewed in W by our convention (1-6). The map

$$\lambda \in \mathrm{X}_*(\mathrm{T}) \to [\lambda(\varpi^{-1}) \bmod \mathrm{T}^1] \in \widetilde{\mathrm{X}}_*(\mathrm{T}) \tag{1-9}$$

is a $\mathfrak{W}$-equivariant splitting for the exact sequence of abelian groups

$$0 \longrightarrow \mathrm{T}^0/\mathrm{T}^1 \longrightarrow \widetilde{\mathrm{X}}_*(\mathrm{T}) \longrightarrow \mathrm{X}_*(\mathrm{T}) \longrightarrow 0. \tag{1-10}$$

We will identify $\mathrm{X}_*(\mathrm{T})$ with its image in $\widetilde{\mathrm{X}}_*(\mathrm{T})$ via (1-9). Note that this identification depends on the choice of the uniformizer ϖ.

Remark 1.8. We have the decomposition of $\widetilde{\mathrm{W}}$ as the semidirect product $\widetilde{\mathrm{W}} = \widetilde{\mathfrak{W}} \ltimes \mathrm{X}_*(\mathrm{T})$, where $\widetilde{\mathfrak{W}}$ denotes the preimage of $\mathfrak{W}$ in $\widetilde{\mathrm{W}}$.

1B7. *Pro-p Hecke rings.* The product in the generic pro-p Iwahori–Hecke ring $\widetilde{\mathrm{H}}_\mathbb{Z}$ is described in [Vignéras 2005, Theorem 1]. It is given by *quadratic relations* and *braid relations*. Stating the quadratic relations in $\widetilde{\mathrm{H}}_\mathbb{Z}$ requires some more notation. We are only going to use them in $\widetilde{\mathrm{H}}_k$ where they have a simpler form, and we postpone their description to Section 1B8. We recall here the braid relations

$$\tau_{ww'} = \tau_w \tau_{w'} \text{ for } w, w' \in \widetilde{\mathrm{W}} \text{ satisfying } \ell(ww') = \ell(w) + \ell(w'). \tag{1-11}$$

The functions in $\widetilde{\mathrm{H}}_\mathbb{Z}$ with support in the subgroup of G generated by all parahoric subgroups form a subring $\widetilde{\mathrm{H}}_\mathbb{Z}^{\mathrm{aff}}$ called the affine subring. It has $\mathbb{Z}$-basis the set of all τ_w for w in the preimage $\widetilde{\mathrm{W}}_{\mathrm{aff}}$ of $\mathrm{W}_{\mathrm{aff}}$ in $\widetilde{\mathrm{W}}$ (see for example [Ollivier and Schneider 2012, Section 4.5]). It is generated by all τ_s for s in the preimage $\widetilde{S}_{\mathrm{aff}}$ of S_{aff} and all τ_t for $t \in \mathrm{T}^0/\mathrm{T}^1$.

There is an involutive automorphism defined on $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]$ by

$$\iota : \tau_w \mapsto (-q)^{\ell(w)} \tau_{w^{-1}}^{-1} \tag{1-12}$$

[Vignéras 2005, Corollary 2], and it actually yields an involution on $\widetilde{\mathrm{H}}_{\mathbb{Z}}$. Inflating the character $\epsilon_{\boldsymbol{C}} : \mathrm{W} \to \{\pm 1\}$ defined in Section 1B2 to a character of $\widetilde{\mathrm{W}}$, we define a $\mathbb{Z}$-linear involution $\upsilon_{\boldsymbol{C}}$ of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ by

$$\upsilon_{\boldsymbol{C}}(\tau_w) = \epsilon_{\boldsymbol{C}}(w)\tau_w \quad \text{for any } w \in \widetilde{\mathrm{W}}.$$

It is the identity on the affine subring $\widetilde{\mathrm{H}}_{\mathbb{Z}}^{\mathrm{aff}}$. We will consider the following $\mathbb{Z}$-linear involution on $\widetilde{\mathrm{H}}_{\mathbb{Z}}$:

$$\iota_{\boldsymbol{C}} = \iota \circ \upsilon_{\boldsymbol{C}}. \tag{1-13}$$

Remark 1.9. The involution ι fixes all τ_w for $w \in \widetilde{\mathrm{W}}$ with length zero. The involution $\iota_{\boldsymbol{C}}$ fixes all τ_{e^λ} for $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$ with length zero.

1B8. Let R be a ring with unit 1_{R}, containing an inverse for $(q1_{\mathrm{R}}-1)$ and a primitive $(q-1)$-th root of 1_{R}. The group of characters of $\mathrm{T}^0/\mathrm{T}^1 = \overline{\mathbf{T}}(\mathbb{F}_q)$ with values in $\mathrm{R}^\times$ is isomorphic to the group of characters of $\overline{\mathbf{T}}(\mathbb{F}_q)$ with values in $\mathbb{F}_q^\times$, which we denote by $\widehat{\overline{\mathbf{T}}}(\mathbb{F}_q)$. To $\xi \in \widehat{\overline{\mathbf{T}}}(\mathbb{F}_q)$ we attach the idempotent element $\epsilon_\xi \in \widetilde{\mathrm{H}}_{\mathrm{R}}$ as in [Vignéras 2005] (definition recalled in [Ollivier 2012, Section 2.4.3]). For $t \in \mathrm{T}^0$ we have $\epsilon_\xi \tau_t = \tau_t \epsilon_\xi = \xi(t)\epsilon_\xi$. The idempotent elements ϵ_ξ, $\xi \in \widehat{\overline{\mathbf{T}}}(\mathbb{F}_q)$ are pairwise orthogonal and their sum is the identity in $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathrm{R}$.

For $A \in \Pi_{\mathrm{aff}}$, choose the lift $n_A \in \mathrm{G}$ for s_A defined after fixing an épinglage for G as in [Vignéras 2005, Section 1.2]. We refer to [Ollivier 2012, Section 2.2.5] for the definition of the associated subgroup T_A of T^0, which is identified with a subgroup of $\mathrm{T}^0/\mathrm{T}^1$.

For $\xi \in \widehat{\overline{\mathbf{T}}}(\mathbb{F}_q)$, we have in $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathrm{R}$

$$\epsilon_\xi \tau_{n_A}^2 = \begin{cases} \epsilon_\xi((q1_{\mathrm{R}}-1)\tau_{n_A} + q1_{\mathrm{R}}) & \text{if } \xi \text{ is trivial on } \mathrm{T}_A, \\ \text{an element of } q\mathrm{R}^\times \epsilon_\xi & \text{otherwise.} \end{cases} \tag{1-14}$$

The field k is an example of ring R as above. In $\widetilde{\mathrm{H}}_k$ we have

$$\epsilon_\xi \tau_{n_A}^2 = \begin{cases} -\epsilon_\xi \tau_{n_A} & \text{if } \xi \text{ is trivial on } \mathrm{T}_A, \\ 0 & \text{otherwise.} \end{cases} \tag{1-15}$$

Remark 1.10. In $\widetilde{\mathrm{H}}_k$ we have $\tau_{n_A}\iota(\tau_{n_A}) = 0$ for all $A \in S_{\mathrm{aff}}$. Furthermore, $\iota(\tau_{n_A}) + \tau_{n_A}$ lies in the subalgebra of $\widetilde{\mathrm{H}}_k$ generated by all τ_t, $t \in \mathrm{T}^0/\mathrm{T}^1$, or equivalently by all ϵ_ξ, $\xi \in \widehat{\overline{\mathbf{T}}}(\mathbb{F}_q)$. This can be seen using for example [Ollivier 2012, Remark 2.10], which also implies the following:

- If ξ is trivial on T_A, then $\iota(\epsilon_\xi \tau_{n_A}) = \epsilon_\xi \iota(\tau_{n_A}) = -\epsilon_\xi(\tau_{n_A} + 1)$.

- If ξ is not trivial on T_A, then $\iota(\epsilon_\xi \tau_{n_A}) = -\epsilon_\xi \tau_{n_A}$.

1B9. *Parametrization of the weights.* The functions in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ with support in K form a subring $\widetilde{\mathfrak{H}}_{\mathbb{Z}}$. It has $\mathbb{Z}$-basis the set of all τ_w for $w \in \widetilde{\mathfrak{W}}$. Denote by $\widetilde{\mathfrak{H}}_k$ the k-algebra $\widetilde{\mathfrak{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$. The simple modules of $\widetilde{\mathfrak{H}}_k$ are one-dimensional [Sawada 1977, (2.11)].

An irreducible smooth k-representation ρ of K will be called a weight. By [Carter and Lusztig 1976, Corollary 7.5], the weights are in one-to-one correspondence with the characters of $\widetilde{\mathfrak{H}}_k$ via $\rho \mapsto \rho^{\mathrm{I}}$. To a character $\chi : \widetilde{\mathfrak{H}}_k \to k$ is attached the morphism $\bar{\chi} : \mathrm{T}^0/\mathrm{T}^1 \to k^\times$ such that $\bar{\chi}(t) = \chi(\tau_t)$ for all $t \in \mathrm{T}^0/\mathrm{T}^1$ and the set $\Pi_{\bar{\chi}}$ of all simple roots $\alpha \in \Pi$ such that $\bar{\chi}$ is trivial on T_α. We then have $\chi(\tau_{\tilde{s}_\alpha}) = 0$ for all $\alpha \in \Pi - \Pi_{\bar{\chi}}$, where $\tilde{s}_\alpha \in \widetilde{\mathrm{W}}$ is any lift for $s_\alpha \in \mathrm{W}$. We denote by Π_χ the subset of all $\alpha \in \Pi_{\bar{\chi}}$ such that $\chi(\tau_{\tilde{s}_\alpha}) = 0$. The character χ is determined by the data of $\bar{\chi}$ and Π_χ (see also [Ollivier 2012, Section 3.4]).

Remark 1.11. Choosing a standard facet F is equivalent to choosing the subset Π_F of Π of the simple roots taking value zero on F. The standard facet corresponding to Π_χ in the previous discussion will be denoted by F_χ.

2. On the center of the pro-p Iwahori–Hecke algebra in characteristic p

2A. ***Commutative subrings of the pro-p Iwahori–Hecke ring.*** Let σ be a sign and F a standard facet.

2A1. As in [Ollivier 2012, Section 4.1.1], we introduce the multiplicative injective map

$$\Theta_F^\sigma : \widetilde{\mathrm{X}}_*(\mathrm{T}) \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]$$

and the elements $\mathcal{B}_F^\sigma(\lambda) := q^{\ell(e^\lambda)/2}\Theta_F^\sigma(\lambda)$ for all $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$. Recall that $\mathcal{B}_F^\sigma(\lambda) = \tau_{e^\lambda}$ if $\lambda \in \mathscr{C}^\sigma(F)$.

The map $\mathcal{B}_F^\sigma$ does not respect the product in general, but it is multiplicative when restricted to any Weyl chamber (see [ibid., Remark 4.3]). For any coweight $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$, the element $\mathcal{B}_F^\sigma(\lambda)$ lies in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ (see Lemma 2.3 below). Furthermore, combining Lemmas 1.4(ii), 2.3 and [ibid., Lemma 4.4],

$$\iota_C(\mathcal{B}_F^+(\lambda)) = \mathcal{B}_F^-(\lambda). \tag{2-1}$$

Extend Θ_F^σ linearly to an injective morphism of $\mathbb{Z}[q^{\pm 1/2}]$-algebras

$$\mathbb{Z}[q^{\pm 1/2}][\widetilde{\mathrm{X}}_*(\mathrm{T})] \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}].$$

We consider the commutative subring $\mathcal{A}_F^\sigma := \widetilde{\mathrm{H}}_{\mathbb{Z}} \cap \mathrm{Im}(\Theta_F^\sigma)$. By [ibid., Proposition 4.5], it is a free $\mathbb{Z}$-module with basis the set of all $\mathcal{B}_F^\sigma(\lambda)$ for $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$. Since the Weyl chambers (in $\widetilde{\mathrm{X}}_*(\mathrm{T})$) are finitely generated semigroups, $\mathcal{A}_F^\sigma$ is finitely generated as a ring.

Remark 2.1. Note that $\mathcal{B}_C^+ = \mathcal{B}_{x_0}^-$ (resp. $\mathcal{B}_C^- = \mathcal{B}_{x_0}^+$) coincides with the integral Bernstein map E^+ (resp. E) introduced in [Vignéras 2005] and $\mathcal{A}_C^+$ (resp. $\mathcal{A}_C^-$) with the commutative ring denoted by $\mathcal{A}^{+,(1)}$ (resp. $\mathcal{A}^{(1)}$) in Theorem 2 of the same paper.

Identify $\mathrm{X}_*(\mathrm{T})$ with its image in $\widetilde{\mathrm{X}}_*(\mathrm{T})$ via (1-9). We denote by $(\mathcal{A}_F^\sigma)^\circ$ the intersection

$$(\mathcal{A}_F^\sigma)^\circ := \widetilde{\mathrm{H}}_\mathbb{Z} \cap \Theta_F^\sigma(\mathbb{Z}[\mathrm{X}_*(\mathrm{T})]) \subseteq \mathcal{A}_F^\sigma.$$

A $\mathbb{Z}$-basis for $(\mathcal{A}_F^\sigma)^\circ$ is given by all $\mathcal{B}_F^\sigma(\lambda)$ for $\lambda \in \mathrm{X}_*(\mathrm{T})$. It is finitely generated as a ring.

Proposition 2.2. *The commutative $\mathbb{Z}$-algebra $\mathcal{A}_F^\sigma$ is isomorphic to the tensor product of the $\mathbb{Z}$-algebras $\mathbb{Z}[\mathrm{T}^0/\mathrm{T}^1]$ and $(\mathcal{A}_F^\sigma)^\circ$. In particular, $(\mathcal{A}_F^\sigma)^\circ$ is a direct summand of $\mathcal{A}_F^\sigma$ as a $\mathbb{Z}$-module.*

Proof. Since the exact sequence (1-10) splits, $\mathcal{A}_F^\sigma$ is a free $(\mathcal{A}_F^\sigma)^\circ$-module with basis the set of all τ_t for $t \in \mathrm{T}^0/\mathrm{T}^1$. Indeed, recall that

$$\mathcal{B}_F^\sigma(\lambda + t) = \mathcal{B}_F^\sigma(\lambda)\tau_t = \tau_t \mathcal{B}_F^\sigma(\lambda)$$

for all $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$ and $t \in \mathrm{T}^0/\mathrm{T}^1$. □

2A2. The following is a direct consequence of the lemma proved in [Haines 2001, §5] and adapted to the pro-p Iwahori–Hecke algebra in [Vignéras 2005, Lemma 13] (see also [Vignéras 2006, Sections 1.2 and 1.5]).

Lemma 2.3. *Let F be a standard facet and σ a sign. For any $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$, we have*

$$\mathcal{B}_F^\sigma(\lambda) = \tau_{e^\lambda} + \sum_{w < e^\lambda} a_w \tau_w,$$

where $(a_w)_w$ is a family of elements in $\mathbb{Z}$ (depending on σ, F and λ) indexed by the set of $w \in \widetilde{\mathrm{W}}$ such that $w < e^\lambda$. For those w, we have in particular $\ell(w) < \ell(e^\lambda)$.

2A3. In this subsection, we suppose that the root system of G is irreducible. This implies in particular that there is a unique element in Π_m. It can be written $-\alpha_0$, where $\alpha_0 \in \Phi^+$ is the highest root; we have $\beta \preceq \alpha_0$ for all $\beta \in \Phi$ [Bourbaki 1968, VI.1.8]. For any standard facet $F \neq x_0$, we have $\alpha_0 \notin \Phi_F$. Denote by $s_0 \in S_{\mathrm{aff}}$ the simple reflection associated to $(-\alpha_0, 1) \in \Pi_{\mathrm{aff}}$ and $n_0 := n_{(-\alpha_0,1)} \in \mathrm{G}$ the lift for s_0 as chosen in Section 1B8.

Lemma 2.4. *Suppose that $F \neq x_0$ and let $\lambda \in \widetilde{\mathrm{X}}_*^+(\mathrm{T})$ be such that $\ell(e^\lambda) \neq 0$. We have*

$$\mathcal{B}_F^+(\lambda) \in \tau_{n_0} \widetilde{\mathrm{H}}_\mathbb{Z}.$$

Proof. It suffices to check the claim for $\lambda \in \mathrm{X}_*^+(\mathrm{T})$. Let $\mu, \nu \in \mathrm{X}_*(\mathrm{T})$, such that $\lambda = \mu - \nu$ and $w_F\mu, w_F\nu \in \mathrm{X}_*^+(\mathrm{T})$, where w_F denotes the longest element in $\mathfrak{W}_F$. Note that $w_F\alpha_0 \in \Phi^+$ because $F \neq x_0$. Furthermore, $\langle \lambda, \alpha_0 \rangle \geq 1$ because there is $\beta \in \Pi$ such that $\langle \lambda, \beta \rangle \geq 1$ and $\beta \preceq \alpha_0$.

We have $e^\nu(-\alpha_0, 1) = (-\alpha_0, 1 + \langle \nu, \alpha_0 \rangle) = (-\alpha_0, 1 + \langle w_F\nu, w_F\alpha_0 \rangle) \in \Phi^+_{\mathrm{aff}}$. Therefore $\ell(e^\nu n_0) = \ell(e^\nu) + 1$ and $\tau_{e^\nu}\tau_{n_0} = \tau_{e^\nu n_0}$ in $\widetilde{\mathrm{H}}_\mathbb{Z}$. On the other hand, $e^{-\lambda}(-\alpha_0, 1) = (-\alpha_0, 1 - \langle \lambda, \alpha_0 \rangle) \in \Phi^-_{\mathrm{aff}}$, and therefore $\ell(n_0 e^\lambda) = \ell(e^\lambda) - 1$.

We perform the computations in $\widetilde{\mathrm{H}}_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Z}[q^{\pm 1/2}]$, where, by definition, $\mathcal{B}_F^+(\lambda) = q^{\frac{1}{2}(\ell(e^\lambda)+\ell(e^\nu)-\ell(e^\mu))}\tau_{e^\nu}^{-1}\tau_{e^\mu}$. By the previous remarks,

$$\mathcal{B}_F^+(\lambda) = \tau_{n_0} q^{\frac{1}{2}(\ell(n_0 e^\lambda)+\ell(e^\nu n_0)-\ell(e^\mu))}\tau_{e^\nu n_0}^{-1}\tau_{e^\mu},$$

which, by the lemma evoked in Section 2A2, lies in $\tau_{n_0}\widetilde{\mathrm{H}}_\mathbb{Z}$. □

2B. *On the center of the pro-p Iwahori–Hecke ring.*

2B1. The ring $\widetilde{\mathrm{H}}_\mathbb{Z}$ is finitely generated as a module over its center $\mathfrak{Z}(\widetilde{\mathrm{H}}_\mathbb{Z}) = (\mathcal{A}_C^+)^\mathfrak{W}$, and the latter has $\mathbb{Z}$-basis the set of all

$$\sum_{\lambda' \in \mathbb{O}} \mathcal{B}_C^+(\lambda'), \tag{2-2}$$

where $\mathbb{O}$ ranges over the $\mathfrak{W}$-orbits in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. Moreover, $\mathfrak{Z}(\widetilde{\mathrm{H}}_\mathbb{Z})$ is a finitely generated $\mathbb{Z}$-algebra. Those results are proved in [Vignéras 2005, Theorem 4] (the hypothesis of irreducibility of the root system of G made there is not necessary for the statements about the center). One can also find a proof in [Schmidt 2009].

2B2. We denote by $\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$ the intersection of $(\mathcal{A}_C^+)^\circ$ with $\mathfrak{Z}(\widetilde{\mathrm{H}}_\mathbb{Z})$. We have $\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z}) = ((\mathcal{A}_C^+)^\circ)^\mathfrak{W}$. It has $\mathbb{Z}$-basis the set of all

$$z_\lambda := \sum_{\lambda' \in \mathbb{O}(\lambda)} \mathcal{B}_C^+(\lambda') \quad \text{for } \lambda \in \mathrm{X}_*^+(\mathrm{T}), \tag{2-3}$$

where we denote by $\mathbb{O}(\lambda)$ the $\mathfrak{W}$-orbit of λ.

Proposition 2.5. (i) *The left and right $(\mathcal{A}_C^+)^\circ$-modules $\widetilde{\mathrm{H}}_\mathbb{Z}$ are finitely generated.*

(ii) *As a $\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$-module, $\widetilde{\mathrm{H}}_\mathbb{Z}$ is finitely generated.*

(iii) *$\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$ is a finitely generated $\mathbb{Z}$-algebra.*

(iv) *As $\mathbb{Z}$-modules, $\mathfrak{Z}(\widetilde{\mathrm{H}}_\mathbb{Z})$, $\mathcal{A}_C^+$, $\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$ and $(\mathcal{A}_C^+)^\circ$ are direct summands of $\widetilde{\mathrm{H}}_\mathbb{Z}$.*

Proof. Using Proposition 2.2 and [Vignéras 2005, Theorems 3 and 4], which state that $\widetilde{\mathrm{H}}_\mathbb{Z}$ is finitely generated over $\mathcal{A}_C^+$ (see Remark 2.1), we see that $\widetilde{\mathrm{H}}_\mathbb{Z}$ is finitely generated over $(\mathcal{A}_C^+)^\circ$. Statements (ii) and (iii) follow from [Bourbaki 1964, V.1.9, Théorème 2] because $\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$ is the ring of $\mathfrak{W}$-invariants of $(\mathcal{A}_C^+)^\circ$ and $\mathbb{Z}$ is

noetherian. For (iv), we first remark that the $\mathbb{Z}$-module $\mathscr{Z}(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ (resp. $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathbb{Z}})$) is a direct summand of $\mathcal{A}_C^+$ (resp. $(\mathcal{A}_C^+)^{\circ}$) since $\mathscr{Z}(\widetilde{\mathrm{H}}_{\mathbb{Z}}) = (\mathcal{A}_C^+)^{\mathfrak{W}}$ (resp. $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathbb{Z}}) = ((\mathcal{A}_C^+)^{\circ})^{\mathfrak{W}}$). The $\mathbb{Z}$-module $(\mathcal{A}_C^+)^{\circ}$ is a direct summand of $\mathcal{A}_C^+$ by Proposition 2.2. It remains to show that $\mathcal{A}_C^+$ is a direct summand of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$, which can be done by considering the integral Bernstein basis for the whole Hecke ring $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ introduced in [Vignéras 2005]. We recall it later in Section 5A and finish the proof of (iv) in Remark 5.1. □

2B3. Given a ring R with unit 1_{R}, we denote by $\widetilde{\mathrm{H}}_{\mathrm{R}}$ the R-algebra $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathrm{R}$; we identify q with its image in R. By Proposition 2.5(iv), the R-algebras $\mathscr{Z}(\widetilde{\mathrm{H}}_{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathrm{R}$, $\mathcal{A}_C^+ \otimes_{\mathbb{Z}} \mathrm{R}$, $(\mathcal{A}_C^+)^{\circ} \otimes_{\mathbb{Z}} \mathrm{R}$ and $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathrm{R}$ are identified with subalgebras of $\widetilde{\mathrm{H}}_{\mathrm{R}}$, which we denote by $\mathscr{Z}(\widetilde{\mathrm{H}}_{\mathrm{R}})$ $(\mathcal{A}_C^+)_R$, $(\mathcal{A}_C^+)_R^{\circ}$ and $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathrm{R}})$, respectively. By [Schmidt 2009], $\mathscr{Z}(\widetilde{\mathrm{H}}_{\mathrm{R}})$ is not only contained in but is equal to the center of $\widetilde{\mathrm{H}}_{\mathrm{R}}$.

Remark 2.6. Proposition 2.5 remains valid with x_0 instead of C (use the involution ι_C and (2-1)). We introduce the subalgebras $(\mathcal{A}_{x_0}^+)_R$ and $(\mathcal{A}_{x_0}^+)_R^{\circ}$ of $\widetilde{\mathrm{H}}_{\mathrm{R}}$ with the obvious definitions.

For $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$ (resp. $w \in \widetilde{\mathrm{W}}$), we still denote by $\mathcal{B}_F^{\sigma}(\lambda)$ (resp. τ_w) its natural image $\mathcal{B}_F^{\sigma}(\lambda) \otimes 1$ (resp. $\tau_w \otimes 1$) in $\widetilde{\mathrm{H}}_{\mathrm{R}}$. An R-basis for $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathrm{R}})$ is given by the set of all z_λ for $\lambda \in \mathrm{X}_*^+(\mathrm{T})$, where again we identify the element z_λ with its image in $\widetilde{\mathrm{H}}_{\mathrm{R}}$.

From Proposition 2.5 we deduce:

Proposition 2.7. *Let* R *be a field. A morphism of* R*-algebras* $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathrm{R}}) \to \mathrm{R}$ *can be extended to a morphism of* R*-algebras* $\mathscr{Z}(\widetilde{\mathrm{H}}_{\mathrm{R}}) \to \mathrm{R}$.

2B4. In the process of constructing $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathbb{Z}})$, we first fixed a hyperspecial vertex x_0 of C and then an apartment $\mathscr{A}$ containing C.

Proposition 2.8. *The ring* $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ *is not affected by*

- *the choice of another apartment* $\mathscr{A}'$ *containing* C,
- *the choice of another vertex* x_0' *of* C, *provided it is* G*-conjugate to* x_0.

Proof. Let g be in the stabilizer $\mathcal{P}_C^{\dagger}$ of C in G. Let $\mathrm{T}' := g\mathrm{T}g^{-1}$ and $x_0' = gx_0g^{-1}$. The apartment $\mathscr{A}'$ corresponding to T' contains C and x_0' is a hyperspecial vertex of C. Starting from T' and x_0' we proceed to the construction of the corresponding commutative subring $\mathscr{Z}^{\circ}(\widetilde{\mathrm{H}}_{\mathbb{Z}})'$ of the center of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$. Since $g \in \mathcal{P}_C^{\dagger}$, we have $\tilde{\mathrm{I}}g\tilde{\mathrm{I}} = \tilde{\mathrm{I}}\hat{\omega}\tilde{\mathrm{I}} = \tilde{\mathrm{I}}\hat{\omega}$ for some $\omega \in \widetilde{\Omega}$. Since this element ω has length zero, for $\lambda \in \mathrm{X}_*(\mathrm{T})$ the characteristic function of $\tilde{\mathrm{I}}g\lambda(\varpi)g^{-1}\tilde{\mathrm{I}}$ is equal to the product $\tau_g\tau_{\lambda(\varpi)}\tau_g^{-1}$. Therefore, the restriction to $\mathrm{X}_*(\mathrm{T})$ of the new map $(\mathcal{B}_C^+)'$ corresponding to the choice of x_0' and T' is defined by

$$\mathrm{X}_*(\mathrm{T}') \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}}, \quad \lambda \mapsto \tau_g \mathcal{B}_C^+(g^{-1}\lambda g)\tau_g^{-1}.$$

The element $z'_\lambda \in \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})'$ corresponding to the choice of $\lambda \in \mathrm{X}_*^+(\mathrm{T}') = g\mathrm{X}_*^+(\mathrm{T})g^{-1}$ is therefore $\tau_g z_{g^{-1}\lambda g} \tau_g^{-1} = z_\lambda$. We have proved that $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})' = \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$.

By Proposition 1.6(i) and Remark 1.7

- changing $\mathscr{A}$ into another apartment $\mathscr{A}'$ containing C, and
- changing x_0 into another vertex x_0' of C which is G-conjugate to x_0

can be done independently of each other by conjugating by an element of I and of $\mathcal{P}_C^\dagger \cap N_\mathrm{G}(\mathrm{T})$ respectively. We have checked that these changes do not affect $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$. □

If $\mathbf{G}$ is of adjoint type or $\mathbf{G} = \mathrm{GL}_n$, then all hyperspecial vertices are conjugate:

Corollary 2.9 [Tits 1979, Section 2.5]. *If* $\mathbf{G}$ *is of adjoint type or* $\mathbf{G} = \mathrm{GL}_n$, *then* $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathbb{Z})$ *depends only on the choice of the uniformizer* ϖ.

2C. ***An affine semigroup algebra in the center of the pro-p Iwahori–Hecke algebra in characteristic p.*** We will use the following observation several times in this subsection: Let F be a standard facet and σ a sign. For $\mu_1, \mu_2 \in \mathrm{X}_*(\mathrm{T})$, we have in $\widetilde{\mathrm{H}}_k$

$$\mathcal{B}_F^\sigma(\mu_1)\mathcal{B}_F^\sigma(\mu_2) = \begin{cases} \mathcal{B}_F^\sigma(\mu_1+\mu_2) & \text{if } \mu_1 \text{ and } \mu_2 \text{ lie in a common Weyl chamber,} \\ 0 & \text{otherwise.} \end{cases} \tag{2-4}$$

In $\widetilde{\mathrm{H}}_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Z}[q^{\pm 1/2}]$ we have indeed

$$\mathcal{B}_F^\sigma(\mu_1)\mathcal{B}_F^\sigma(\mu_2) = q^{(\ell(e^{\mu_1})+\ell(e^{\mu_2})-\ell(e^{\mu_1+\mu_2}))/2}\mathcal{B}_F^\sigma(\mu_1+\mu_2).$$

If μ_1 and μ_2 lie in a common Weyl chamber, then $\ell(e^{\mu_1}) + \ell(e^{\mu_2}) - \ell(e^{\mu_1+\mu_2})$ is zero; otherwise, there is $\alpha \in \Pi$ satisfying $\langle \mu_1, \alpha\rangle\langle \mu_2, \alpha\rangle < 0$, which implies that this quantity is ≥ 2. This gives the required equality in $\widetilde{\mathrm{H}}_k$.

2C1. *The structure of* $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$.

Proposition 2.10. *The map*

$$k[\mathrm{X}_*^+(\mathrm{T})] \longrightarrow \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k), \quad \lambda \longmapsto z_\lambda, \tag{2-5}$$

is an isomorphism of k*-algebras.*

Proof. We already know that (2-5) maps a k-basis for $k[\mathrm{X}_*^+(\mathrm{T})]$ onto a k-basis for $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$. We have to check that it respects the product. Let $\lambda_1, \lambda_2 \in \mathrm{X}_*^+(\mathrm{T})$, with respective $\mathfrak{W}$-orbits $\mathbb{O}(\lambda_1)$ and $\mathbb{O}(\lambda_2)$. We consider the product

$$z_{\lambda_1} z_{\lambda_2} = \sum_{\substack{\mu_1 \in \mathbb{O}(\lambda_1), \\ \mu_2 \in \mathbb{O}(\lambda_2)}} \mathcal{B}_F^\sigma(\mu_1)\mathcal{B}_F^\sigma(\mu_2) \in \widetilde{\mathrm{H}}_k.$$

A Weyl chamber in $X_*(T)$ is a $\mathfrak{W}$-conjugate of $X_*^+(T)$. Given a Weyl chamber and a coweight (in $X_*(T)$), there is a unique $\mathfrak{W}$-conjugate of the coweight in the chosen Weyl chamber. The map $(\mu_1, \mu_2) \mapsto \mu_1 + \mu_2$ yields a bijection between the set of all $(\mu_1, \mu_2) \in \mathcal{O}(\lambda_1) \times \mathcal{O}(\lambda_2)$ such that μ_1 and μ_2 lie in the same Weyl chamber and the $\mathfrak{W}$-orbit $\mathcal{O}(\lambda_1 + \lambda_2)$ of $\lambda_1 + \lambda_2$: it is indeed surjective, and one checks that the two sets in question have the same size because, λ_1 and λ_2 being both dominant, the stabilizer in $\mathfrak{W}$ of $\lambda_1 + \lambda_2$ is the intersection of the stabilizers of λ_1 and of λ_2. Together with (2-4), this proves that $z_{\lambda_1+\lambda_2} = z_{\lambda_1} z_{\lambda_2}$. □

For a different proof of this proposition, see the remark after Theorem 4.3.

2C2. Since $X_*(T)$ is a free abelian group (of rank $\dim(T)$), the k-algebra $k[X_*(T)]$ is isomorphic to an algebra of Laurent polynomials and has a trivial nilradical. By Gordan's lemma, $X_*^+(T)$ is finitely generated as a semigroup. So, $k[X_*^+(T)]$ is a finitely generated k-algebra and its Jacobson radical coincides with its nilradical.

The Jacobson radical of $\mathcal{Z}^\circ(\widetilde{H}_k)$ is therefore trivial.

Proposition 2.11. *The Jacobson radical of $\mathcal{Z}(\widetilde{H}_k)$ is trivial.*

Proof. Since $\mathcal{Z}(\widetilde{H}_k)$ is a finitely generated k-algebra contained in $(\mathcal{A}_C^+)_k$, it is enough to prove that the nilradical of $(\mathcal{A}_C^+)_k$ is trivial. Using the notation of Section 1B8, it is enough to prove that, for any $\xi \in \widehat{\mathbf{T}}(\mathbb{F}_q)$, the nilradical of the k-algebra $\epsilon_\xi(\mathcal{A}_C^+)_k$ with unit ϵ_ξ is trivial. By Proposition 2.2, the latter algebra is isomorphic to $(\mathcal{A}_C^+)_k^\circ$. It is therefore enough to prove that the nilradical of $(\mathcal{A}_C^+)_k^\circ$ is trivial.

By definition (see the convention in Section 2B3), the image of the k-linear injective map

$$\mathcal{B}_C^+ : k[X_*(T)] \longrightarrow \widetilde{H}_k$$

coincides with $(\mathcal{A}_C^+)_k^\circ$.

Fact i. *Let $\lambda_0 \in X_*^+(T)$ be a strongly dominant coweight. The ideal of $(\mathcal{A}_C^+)_k^\circ$ generated by $\mathcal{B}_C^+(\lambda_0)$ does not contain any nontrivial nilpotent element.*

An element $a \in (\mathcal{A}_C^+)_k^\circ$ is a k-linear combination of elements $\mathcal{B}_C^+(\lambda)$ for $\lambda \in X_*(T)$, and we say that $\lambda \in X_*(T)$ is in the support of a if the coefficient of $\mathcal{B}_C^+(\lambda)$ is nonzero. Suppose that a is nilpotent and nontrivial. After conjugating by an element of $\mathfrak{W}$, we can suppose that there is an element of $X_*^+(T)$ in the support of a. Then, let $\lambda_0 \in X_*^+(T)$ be strongly dominant. The element $a\mathcal{B}_C^+(\lambda_0)$ is nilpotent and by (2-4) it is nontrivial. By Fact i, we have a contradiction. □

Proof of the fact. The restriction of $\mathcal{B}_C^+$ to $k[X_*^+(T)]$ induces an isomorphism of k-algebras $k[X_*^+(T)] \cong \mathcal{B}_C^+(k[X_*^+(T)])$. By (2-4), the ideal $\mathfrak{A}$ of $(\mathcal{A}_C^+)^\circ$ generated by $\mathcal{B}_C^+(\lambda_0)$ coincides with the ideal of $\mathcal{B}_C^+(k[X_*^+(T)])$ generated by $\mathcal{B}_C^+(\lambda_0)$. Since

the k-algebra $k[\mathrm{X}_*^+(\mathrm{T})]$ does not contain any nontrivial nilpotent element, neither does $\mathfrak{A}$. □

Since k is algebraically closed, we have:

Corollary 2.12. *Let $z \in \mathscr{Z}(\widetilde{\mathrm{H}}_k)$. If $\zeta(z) = 0$ for all characters $\zeta : \mathscr{Z}(\widetilde{\mathrm{H}}_k) \to k$, then $z = 0$.*

2C3. *The center of the Iwahori–Hecke algebra in characteristic p.* Let R be a ring containing an inverse for $(q1_\mathrm{R} - 1)$ and a primitive $(q-1)$-th root of 1_R. We can apply the observations of Section 1B8 and consider the algebra

$$\widetilde{\mathrm{H}}_\mathrm{R}(\xi) := \epsilon_\xi \widetilde{\mathrm{H}}_\mathrm{R} \epsilon_\xi.$$

It can be seen as the algebra $\mathscr{H}(\mathrm{G}, \mathrm{I}, \xi^{-1})$ of G-endomorphisms of the representation $\epsilon_\xi \operatorname{ind}_\mathrm{I}^\mathrm{G} \mathbf{1}_\mathrm{R}$, which is isomorphic to the compact induction $\operatorname{ind}_\mathrm{I}^\mathrm{G} \xi^{-1}$ of ξ^{-1} seen as an R-character of I trivial on $\tilde{\mathrm{I}}$: denote by $1_{\mathrm{I},\xi^{-1}} \in \operatorname{ind}_\mathrm{I}^\mathrm{G} \xi^{-1}$ the unique function with support in I and value 1_R at 1_G, and then the map

$$\widetilde{\mathrm{H}}_\mathrm{R}(\xi) \to \mathscr{H}(\mathrm{G}, \mathrm{I}, \xi^{-1}), \quad h \mapsto [1_{\mathrm{I},\xi^{-1}} \mapsto 1_{\mathrm{I},\xi^{-1}} h] \tag{2-6}$$

gives the identification. In particular, when $\xi = \mathbf{1}$ is the trivial character, then the algebra $\widetilde{\mathrm{H}}_\mathrm{R}(\mathbf{1})$ identifies with the usual Iwahori–Hecke algebra $\mathrm{H}_\mathrm{R} = \mathrm{R}[\mathrm{I}\backslash\mathrm{G}/\mathrm{I}]$ with coefficients in R.

Remark 2.13. Let $\xi \in \hat{\bar{\mathbf{T}}}(\mathbb{F}_q)$. We have inclusions

$$\epsilon_\xi \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathrm{R}) \subseteq \epsilon_\xi \mathscr{Z}(\widetilde{\mathrm{H}}_\mathrm{R}) \subseteq \mathscr{Z}(\widetilde{\mathrm{H}}_\mathrm{R}(\xi)),$$

where the latter space is the center of $\widetilde{\mathrm{H}}_\mathrm{R}(\xi)$. The inclusion $\epsilon_\xi \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_\mathrm{R}) \subseteq \mathscr{Z}(\widetilde{\mathrm{H}}_\mathrm{R}(\epsilon_\xi))$ is strict in general. For example if $\mathrm{G} = \mathrm{GL}_2(\mathfrak{F})$, $\mathrm{R} = k$, and ξ is not fixed by the nontrivial element of $\mathfrak{W}$, then $\widetilde{\mathrm{H}}_k(\xi)$ is commutative with a k-basis indexed by the elements in $\mathrm{X}_*(\mathrm{T})$ and contains zero divisors [Barthel and Livné 1994, Proposition 13] while the k-algebra $\epsilon_\xi \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ is isomorphic to $k[\mathrm{X}_*^+(\mathrm{T})]$.

If $\xi = \mathbf{1}$ however, these inclusions are equalities: one easily checks by direct comparison of the basis elements (2-2) and (2-3) that the first inclusion is an equality. The second one comes from the fact that $\epsilon_\mathbf{1}$ is a central idempotent in $\widetilde{\mathrm{H}}_\mathrm{R}$. In particular we have:

Theorem 2.14. *The center of the Iwahori–Hecke k-algebra $k[\mathrm{I}\backslash\mathrm{G}/\mathrm{I}]$ is isomorphic to $k[\mathrm{X}_*^+(\mathrm{T})]$.*

Proof. The map

$$k[\mathrm{X}_*^+(\mathrm{T})] \longrightarrow \epsilon_\mathbf{1} \mathscr{Z}(\widetilde{\mathrm{H}}_k), \quad \lambda \longmapsto \epsilon_\mathbf{1} z_\lambda$$

is surjective by the previous discussion. It is easily checked to be injective using Lemma 2.3 (compare with [Vignéras 2006, (1.6.5)]). □

3. The central Bernstein functions in the pro-p Iwahori–Hecke ring

Let $\mathbb{O}$ be a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. We call the central element of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$

$$z_{\mathbb{O}} := \sum_{\lambda' \in \mathbb{O}} \mathcal{B}_C^+(\lambda') \tag{2-2}$$

the associated central Bernstein function.

3A. ***The support of the central Bernstein functions.*** For $h \in \widetilde{\mathrm{H}}_{\mathbb{Z}}$, the set of all $w \in \widetilde{\mathrm{W}}$ such that $h(\hat{w}) \neq 0$ is called the *support* of h. For $\mathbb{O}$ a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$, we denote by $\ell_{\mathbb{O}}$ the common length of all the coweights in $\mathbb{O}$.

Lemma 3.1. *Let $\mathbb{O}$ be a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. The support of $z_{\mathbb{O}}$ contains the set of all e^{μ} for $\mu \in \mathbb{O}$: more precisely, the coefficient of $\tau_{e^{\mu}}$ in the decomposition of $z_{\mathbb{O}}$ is equal to* 1. *Any other element in the support of $z_{\mathbb{O}}$ has length $< \ell_{\mathbb{O}}$. The same is true with $\iota_C(z_{\mathbb{O}})$ instead of $z_{\mathbb{O}}$.*

Proof. This is a consequence of Lemma 2.3 (and of (2-1)). □

Proposition 3.2. *The involution ι_C fixes the elements in the center $\mathfrak{Z}(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$. In particular, for $\mathbb{O}$ a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$, the element $\sum_{\lambda' \in \mathbb{O}} \mathcal{B}_C^{\sigma}(\lambda') \in \widetilde{\mathrm{H}}_{\mathbb{Z}}$ does not depend on the sign σ.*

Proof. We prove that ι_C fixes $z_{\mathbb{O}}$ by induction on $\ell_{\mathbb{O}}$.

If $\ell_{\mathbb{O}} = 0$, we conclude using Remark 1.9. Let $\mathbb{O}$ be a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$ such that $\ell_{\mathbb{O}} > 0$. The element $\iota_C(z_{\mathbb{O}})$ is central in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$. Recall that a $\mathbb{Z}$-basis for $\mathfrak{Z}(\widetilde{\mathrm{H}}_{\mathbb{Z}})$ is given by the central Bernstein functions $z_{\mathbb{O}}$, where $\mathbb{O}$ ranges over the $\mathfrak{W}$-orbits in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. Lemma 3.1 implies that $\iota_C(z_{\mathbb{O}})$ decomposes as a sum

$$\iota_C(z_{\mathbb{O}}) = z_{\mathbb{O}} + \sum_{\mathbb{O}'} a_{\mathbb{O}'} z_{\mathbb{O}'},$$

where $\mathbb{O}'$ ranges over a finite set of $\mathfrak{W}$-orbits in $\widetilde{\mathrm{X}}_*(\mathrm{T})$ such that $\ell_{\mathbb{O}'} < \ell_{\mathbb{O}}$ and $a_{\mathbb{O}'} \in \mathbb{Z}$. By induction and applying the involution ι_C, we get

$$z_{\mathbb{O}} = \iota_C(z_{\mathbb{O}}) + \sum_{\mathbb{O}'} a_{\mathbb{O}'} z_{\mathbb{O}'}$$

and $2(\iota(z_{\mathbb{O}}) - z_{\mathbb{O}}) = 0$. Since $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ has no $\mathbb{Z}$-torsion, $\iota(z_{\mathbb{O}}) = z_{\mathbb{O}}$. The second statement follows from (2-1). □

If G is semisimple, the projection in $\widetilde{\mathrm{H}}_k$ of the equality proved in Proposition 3.2 can be obtained independently, using the duality for finite-length $\widetilde{\mathrm{H}}_k$-modules defined in [Ollivier and Schneider 2012]:

Proposition 3.3. *Suppose that* G *is semisimple. The element $\sum_{\lambda' \in \mathbb{O}} \mathcal{B}_C^{\sigma}(\lambda') \in \widetilde{\mathrm{H}}_k$ is fixed by the involution ι_C and therefore does not depend on the sign σ.*

Proof. Suppose that G is semisimple. Let $\mathbb{O}$ be a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. We want to prove, without using Proposition 3.2, that in $\widetilde{\mathrm{H}}_k$ we have $z_{\mathbb{O}} = \iota_C(z_{\mathbb{O}})$.

Let $\zeta : \mathscr{Z}(\widetilde{\mathrm{H}}_k) \to k$ be a character and $M = \widetilde{\mathrm{H}}_k \otimes_{\mathscr{Z}(\widetilde{\mathrm{H}}_k)} \zeta$ the induced $\widetilde{\mathrm{H}}_k$-module. It is finite dimensional over k and therefore by [Ollivier and Schneider 2012, Corollary 6.12] we have an isomorphism of right $\widetilde{\mathrm{H}}_k$-modules

$$\mathrm{Ext}^d_{\widetilde{\mathrm{H}}_k}(M, \widetilde{\mathrm{H}}_k) = \mathrm{Hom}_k(\iota_C^* M, k),$$

where d is the semisimple rank of G and $\iota_C^* M$ denotes the left $\widetilde{\mathrm{H}}_k$-module M with action twisted by the involution ι_C defined by (1-13). The category of left $\widetilde{\mathrm{H}}_k$-modules is naturally a $\mathscr{Z}(\widetilde{\mathrm{H}}_k)$-linear category, and therefore, for X and Y two left $\widetilde{\mathrm{H}}_k$-modules, $\mathrm{Ext}^d_{\widetilde{\mathrm{H}}_k}(X, Y)$ inherits the structure of a central $\mathscr{Z}(\widetilde{\mathrm{H}}_k)$-bimodule. Hence, the right $\widetilde{\mathrm{H}}_k$-module $\mathrm{Ext}^d_{\widetilde{\mathrm{H}}_k}(M, \widetilde{\mathrm{H}}_k)$ has a central character equal to ζ. On the other hand, $\mathrm{Hom}_k(\iota_C^* M, k)$ has $\zeta \circ \iota_C$ as a central character. Therefore, $\zeta(z_{\mathbb{O}}) = \zeta \circ \iota_C(z_{\mathbb{O}})$. By Corollary 2.12, we have the required equality $z_{\mathbb{O}} = \iota_C(z_{\mathbb{O}})$. □

3B. ***Independence lemma.*** The following lemma will be proved in Section 3C3.

Lemma 3.4. *For $\mathbb{O}$ a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$, the element*

$$\sum_{\lambda \in \mathbb{O}} \mathcal{B}_F^\sigma(\lambda)$$

in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ does not depend on the choice of the standard facet F and of the sign σ.

Corollary 3.5. *The center of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ is contained in the intersection of all the commutative rings $\mathcal{A}_F^\sigma$ for F a standard facet and σ a sign.*

3C. ***Inducing the generalized integral Bernstein functions.*** We study the behavior of the integral Bernstein maps upon parabolic induction and subsequently prove Lemma 3.4.

3C1. Let F be a standard facet, Π_F the associated set of simple roots and P_F the corresponding standard parabolic subgroup, with Levi decomposition $\mathrm{P}_F = \mathrm{M}_F \mathrm{N}_F$. The root datum attached to the choice of the split torus T in M_F is $(\Phi_F, \mathrm{X}^*(\mathrm{T}), \check{\Phi}_F, \mathrm{X}_*(\mathrm{T}))$ (notation in Section 1B4). The extended Weyl group of M_F is $\mathrm{W}_F = (N_{\mathrm{G}}(\mathrm{T}) \cap \mathrm{M}_F)/\mathrm{T}^0$. It is isomorphic to the semidirect product $\mathfrak{W}_F \ltimes \mathrm{X}_*(\mathrm{T})$, where $\mathfrak{W}_F$ is the finite Weyl group $(N_{\mathrm{G}}(\mathrm{T}) \cap \mathrm{M}_F)/\mathrm{T}$ (also defined in Section 1B4). We denote by ℓ_F its length function and by $\leq_F$ the Bruhat order on W_F.

Set $\widetilde{\mathrm{W}}_F = (N_{\mathrm{G}}(\mathrm{T}) \cap \mathrm{M}_F)/\mathrm{T}^1$. It is a subgroup of $\widetilde{\mathrm{W}}$. The double cosets of M_F modulo its pro-p Iwahori subgroup $\tilde{\mathrm{I}} \cap \mathrm{M}_F$ are indexed by the elements in $\widetilde{\mathrm{W}}_F$. For $w \in \mathrm{W}_F$, we denote by τ_w^F the characteristic function of the double coset containing the lift $\hat{w}$ for w (which lies in $N_{\mathrm{G}}(\mathrm{T}) \cap \mathrm{M}_F$). The set of all τ_w^F

for $w \in \mathrm{W}_F$ is a basis for the pro-p Iwahori–Hecke ring $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$ of $\mathbb{Z}$-valued functions with compact support in $(\tilde{\mathrm{I}} \cap \mathrm{M}_F)\backslash \mathrm{M}_F / (\tilde{\mathrm{I}} \cap \mathrm{M}_F)$. The ring $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$ does not inject in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ in general.

An element in $w \in \mathrm{W}_F$ is called F-positive if $w^{-1}(\Phi^+ - \Phi_F^+) \subset \Phi_{\mathrm{aff}}^+$. For example, for $\lambda \in \mathrm{X}_*(\mathrm{T})$, the element e^λ is F-positive if and only if $\langle \lambda, \alpha \rangle \geq 0$ for all $\alpha \in \Phi^+ - \Phi_F^+$. In this case, we will say that the coweight λ itself is F-positive. If furthermore $\langle \lambda, \alpha \rangle > 0$ for $\alpha \in \Phi^+ - \Phi_F^+$ and $\langle \lambda, \alpha \rangle = 0$ for $\alpha \in \Phi_F^+$, then it is called strongly F-positive. The F-positive coweights are the $\mathfrak{W}_F$-conjugates of the dominant coweights. The C-positive (resp. strongly C-positive) coweights are the dominant (resp. strongly dominant) coweights. An element in W_F is F-positive if and only if it belongs to $e^\lambda \mathfrak{W}_F$ for some F-positive coweight $\lambda \in \mathrm{X}_*(\mathrm{T})$. If μ and $\nu \in \mathrm{X}_*(\mathrm{T})$ are F-positive coweights such that $\mu - \nu$ is also F-positive, then we have the equality (see [Ollivier 2012, Section 1.2] for example)

$$\ell(e^{\mu-\nu}) + \ell(e^\nu) - \ell(e^\mu) = \ell_F(e^{\mu-\nu}) + \ell_F(e^\nu) - \ell_F(e^\mu). \tag{3-1}$$

An element in $\widetilde{\mathrm{W}}_F$ will be called F-positive if its projection in W_F is F-positive.

The subspace of $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$ generated over $\mathbb{Z}$ by all τ_w^F for F-positive $w \in \widetilde{\mathrm{W}}_F$ is denoted by $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)^+$. It is in fact a ring, and there is an injection of rings

$$j_F^+ : \widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)^+ \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}}, \quad \tau_w^F \longmapsto \tau_w$$

which extends to an injection of $\mathbb{Z}[q^{\pm 1/2}]$-algebras

$$j_F : \widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}] \to \widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}].$$

This is a classical result for complex Hecke algebras [Bushnell and Kutzko 1998, (6.12)]. The argument is valid over $\mathbb{Z}[q^{\pm 1/2}]$.

Remark 3.6. An element $w \in \widetilde{\mathrm{W}}_F$ is called F-negative (resp. strongly F-negative) if w^{-1} is F-positive (resp. strongly F-positive), and, as before, $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$ contains as a subring the space $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)^-$ generated over $\mathbb{Z}$ by all τ_w^F for F-negative $w \in \widetilde{\mathrm{W}}_F$. There is an injection of rings $j_F^- : \widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)^- \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}}, \tau_w^F \longmapsto \tau_w$.

Fact ii. *Let $v \in \mathrm{W}_F$, such that $v \leq_F e^\lambda$ for $\lambda \in \mathrm{X}_*(\mathrm{T})$ an F-positive coweight. Then v is F-positive.*

Proof. Suppose first that λ is dominant. Then the claim is Lemma 2.9(ii) of [Ollivier 2012]. In general, λ is a $\mathfrak{W}_F$-conjugate of a dominant coweight λ_0: there is $u \in \mathfrak{W}_F$ such that $e^\lambda = u e^{\lambda_0} u^{-1}$. We argue by induction on $\ell_F(u)$. Let s be a simple reflection in $\mathfrak{W}_F$ such that $\ell_F(su) = \ell_F(u) - 1$. By the properties of the Bruhat order (see [Haines 2001, Lemma 4.3] for example), one of v, vs, sv, svs is $\leq_F se^\lambda s$, and by induction this element is F-positive, which implies that v is F-positive. □

3C2. Let $F' \subseteq \overline{C}$ be another facet containing x_0 in its closure, such that $F \subseteq \overline{F}'$. This implies that $\Phi_{F'} \subseteq \Phi_F$ and $\Phi^+_{F'} \subseteq \Phi^+_F$. Let ${}_F\Theta^+_{F'}$ be the map constructed as in Section 2A with respect to the root data attached to M_F:

$$ {}_F\Theta^+_{F'} : \mathbb{Z}[q^{\pm 1/2}][\widetilde{\mathrm{X}}_*(\mathrm{T})] \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]. $$

The corresponding $\mathbb{Z}$-linear integral map is denoted by ${}_F\mathcal{B}^+_{F'} : \mathbb{Z}[\widetilde{\mathrm{X}}_*(\mathrm{T})] \longrightarrow \widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$ and defined by ${}_F\mathcal{B}^+_{F'}(\lambda) = q^{\ell_F(e^\lambda)/2}\, {}_F\Theta^+_{F'}(\lambda)$ for all $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$. It satisfies ${}_F\mathcal{B}^+_{F'}(\lambda) = \tau^F_{e^\lambda}$ if $\langle \lambda, \alpha \rangle \geq 0$ for all $\alpha \in (\Phi^+_F - \Phi^+_{F'}) \cup \Phi^-_{F'}$.

Remark 3.7. If $F = x_0$ then ${}_{x_0}\mathcal{B}^+_{F'} = \mathcal{B}^+_{F'}$.

Lemma 3.8. *Let $\lambda \in \widetilde{\mathrm{X}}_*(\mathrm{T})$ be an F-positive coweight. Then ${}_F\mathcal{B}^+_{F'}(\lambda)$ lies in $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)^+$ and*

$$ j^+_F({}_F\mathcal{B}^+_{F'}(\lambda)) = \mathcal{B}^+_{F'}(\lambda). \tag{3-2} $$

Proof. Decompose $\lambda = \mu - \nu$ with $\mu, \nu \in \mathscr{C}^+(F')$. Then in $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]$ we have ${}_F\mathcal{B}^+_{F'}(\lambda) = q^{(\ell_F(e^\lambda) + \ell_F(e^\nu) - \ell_F(e^\mu))/2} \tau^F_{e^\mu} (\tau^F_{e^\nu})^{-1}$. By Lemma 2.3 applied to the pro-p Iwahori–Hecke algebra $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$, this element decomposes in $\widetilde{\mathrm{H}}_{\mathbb{Z}}(\mathrm{M}_F)$ into a linear combination of $\tau^F_{\tilde{w}}$ for $\tilde{w} \in \widetilde{\mathrm{W}}_F$, where the projection w of $\tilde{w}$ in W_F satisfies $w \leq_F e^\lambda$. Fact ii ensures that these w (and $\tilde{w}$) are F-positive. Now, j_F respects the product and

$$ j^+_F({}_F\mathcal{B}^+_{F'}(\lambda)) = j_F({}_F\mathcal{B}^+_{F'}(\lambda)) = q^{(\ell_F(e^\lambda) + \ell_F(e^\nu) - \ell_F(e^\mu))/2} \tau_{e^\mu} (\tau_{e^\nu})^{-1} $$

because μ and ν are in particular F-positive. Apply (3-1) to finish the proof. □

3C3. We prove Lemma 3.4. Let $\mathbb{O}$ be a $\mathfrak{W}$-orbit in $\widetilde{\mathrm{X}}_*(\mathrm{T})$. Since $\mathcal{B}^+_{x_0} = \mathcal{B}^-_C$, and using (2-1), it is enough to prove

$$ \sum_{\lambda \in \mathbb{O}} \mathcal{B}^+_F(\lambda) = \sum_{\lambda \in \mathbb{O}} \mathcal{B}^+_C(\lambda) \tag{3-3} $$

for any standard facet F. If $F = x_0$ then the result is given by Proposition 3.2. Let F be a standard facet, such that $F \neq x_0$.

(1) Let $\mu \in \widetilde{\mathrm{X}}_*(\mathrm{T})$ be an F-positive coweight with $\mathfrak{W}_F$-orbit $\mathbb{O}_F$. We have the following identity:

$$ \sum_{\mu' \in \mathbb{O}_F} \mathcal{B}^+_F(\mu') = \sum_{\mu' \in \mathbb{O}_F} j^+_F({}_F\mathcal{B}^+_F(\mu')) = \sum_{\mu' \in \mathbb{O}_F} j^+_F({}_F\mathcal{B}^+_C(\mu')) = \sum_{\mu' \in \mathbb{O}_F} \mathcal{B}^+_C(\mu'), $$

where the first and third equalities come from (3-2) and the second one from Proposition 3.2 applied to M_F.

(2) Choose ν a strongly F-positive coweight such that $\lambda + \nu$ is F-positive for all $\lambda \in \mathbb{O}$. Decompose the $\mathfrak{W}$-orbit $\mathbb{O}$ into the disjoint union of $\mathfrak{W}_F$-orbits $\mathbb{O}^i_F$

for $i \in \{1, \dots, r\}$. Since ν lies in both $\widetilde{\mathrm{X}}^+_*(\mathrm{T})$ and $\mathscr{C}^+(F)$, we have $\mathcal{B}^+_F(-\nu) = \mathcal{B}^+_C(-\nu) = \iota_C(\tau_{e^{-\nu}})$.

Let $i \in \{1, \dots, r\}$ and $\lambda \in \mathbb{O}^i_F$. We have in $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]$ that

$$\mathcal{B}^+_F(\lambda) = q^{\frac{1}{2}(\ell(e^\lambda) - \ell(e^{\lambda+\nu}) - \ell(e^\nu))} \mathcal{B}^+_F(\lambda+\nu)\mathcal{B}^+_F(-\nu).$$

Note that $\ell(e^\lambda) - \ell(e^{\lambda+\nu}) - \ell(e^\nu)$ does not depend on $\lambda \in \mathbb{O}^i_F$: since $\langle \nu, \alpha \rangle = 0$ for all $\alpha \in \Phi^+_F$, this quantity is equal to $\sum_{\alpha \in \Phi^+ - \Phi^+_F} |\langle \lambda, \alpha \rangle| - |\langle \lambda + \nu, \alpha \rangle| - |\langle \nu, \alpha \rangle|$, which does not depend on the choice of $\lambda \in \mathbb{O}^i_F$ because $\Phi^+ - \Phi^+_F$ is invariant under the action of $\mathfrak{W}_F$. Therefore, if we pick a representative $\lambda_i \in \mathbb{O}^i_F$, we have

$$\begin{aligned}\sum_{\lambda \in \mathbb{O}^i_F} \mathcal{B}^+_F(\lambda) &= q^{\frac{1}{2}(\ell(e^{\lambda_i}) - \ell(e^{\lambda_i+\nu}) - \ell(e^\nu))} \sum_{\lambda \in \mathbb{O}^i_F} \mathcal{B}^+_F(\lambda+\nu)\mathcal{B}^+_C(-\nu). \\ &= q^{\frac{1}{2}(\ell(e^{\lambda_i}) - \ell(e^{\lambda_i+\nu}) - \ell(e^\nu))} \sum_{\lambda \in \mathbb{O}^i_F} \mathcal{B}^+_C(\lambda+\nu)\mathcal{B}^+_C(-\nu) = \sum_{\lambda \in \mathbb{O}^i_F} \mathcal{B}^+_C(\lambda)\end{aligned}$$

(where the second equality follows from (1) applied to the $\mathfrak{W}_F$-orbit of $\lambda + \nu$), which proves that $\sum_{\lambda \in \mathbb{O}} \mathcal{B}^+_F(\lambda) = \sum_{\lambda \in \mathbb{O}} \mathcal{B}^+_C(\lambda)$.

4. Compatibility between Satake and Bernstein isomorphisms in characteristic p

In this section all the algebras have coefficients in k.

Let (ρ, V) be a weight and v a chosen nonzero $\tilde{\mathrm{I}}$-fixed vector. Let $\chi : \widetilde{\mathfrak{H}}_k \to k$ be the associated character and F_χ the corresponding standard facet (Remark 1.11). We consider the compact induction $\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho$ and its k-algebra of G-endomorphisms $\mathscr{H}(\mathrm{G}, \rho)$. The $\tilde{\mathrm{I}}$-invariant subspace $(\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho)^{\tilde{\mathrm{I}}}$ is naturally a right $\widetilde{\mathrm{H}}_k$-module. Let $\mathbf{1}_{\mathrm{K},v} \in \mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho$ be the ($\tilde{\mathrm{I}}$-invariant) function with support K and value v at 1.

The map

$$\mathscr{Z}(\widetilde{\mathrm{H}}_k) \longrightarrow \mathrm{Hom}_{\widetilde{\mathrm{H}}_k}((\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho)^{\tilde{\mathrm{I}}}, (\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho)^{\tilde{\mathrm{I}}}), \quad z \longmapsto [f \mapsto fz], \tag{4-1}$$

defines a morphism of k-algebras. On the other hand, by [Ollivier 2012, Corollary 3.14], passing to $\tilde{\mathrm{I}}$-invariants yields an isomorphism of k-algebras

$$\mathscr{H}(\mathrm{G}, \rho) = \mathrm{Hom}_{\mathrm{G}}(\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho, \mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho) \xrightarrow{\sim} \mathrm{Hom}_{\widetilde{\mathrm{H}}_k}((\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho)^{\tilde{\mathrm{I}}}, (\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho)^{\tilde{\mathrm{I}}}). \tag{4-2}$$

Composing (4-1) with the inverse of (4-2) therefore gives a morphism of k-algebras $\mathscr{Z}(\widetilde{\mathrm{H}}_k) \to \mathscr{H}(\mathrm{G}, \rho)$, and we consider its restriction to $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$:

$$\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \longrightarrow \mathscr{H}(\mathrm{G}, \rho), \quad z \longmapsto [\mathbf{1}_{\mathrm{K},v} \mapsto \mathbf{1}_{\mathrm{K},v} z]. \tag{4-3}$$

For $\lambda \in \mathrm{X}_*^+(\mathrm{T})$, we denote by $\mathcal{T}'_\lambda \in \mathscr{H}(\mathrm{G}, \rho)$ the image under (4-3) of the central Bernstein function z_λ defined by (2-3).

On the other hand, recall that we have the isomorphism of k-algebras [Ollivier 2012, Theorem 4.11]

$$\mathcal{T} : k[\mathrm{X}_*^+(\mathrm{T})] \xrightarrow{\sim} \mathscr{H}(\mathrm{G}, \rho), \tag{4-4}$$

where $\mathcal{T}_\lambda$ for $\lambda \in \mathrm{X}_*^+(\mathrm{T})$ is defined by

$$\mathcal{T}_\lambda : \mathbf{1}_{\mathrm{K},v} \mapsto \mathbf{1}_{\mathrm{K},v} \mathcal{B}^+_{F_\chi}(\lambda). \tag{4-5}$$

Proposition 4.1. *We have $\mathcal{T}'_\lambda = \mathcal{T}_\lambda$ for all $\lambda \in \mathrm{X}_*^+(\mathrm{T})$.*

Proof. It is enough to check that these operators coincide on $\mathbf{1}_{\mathrm{K},v}$. If λ has length zero, then $\mathcal{B}^+_{F_\chi}(\lambda) = z_\lambda = \tau_{e^\lambda}$ and the claim is true. Otherwise λ has length > 0; recall that $\mathbb{O}(\lambda)$ denotes the $\mathfrak{W}$-orbit of λ.

(a) Let $\lambda' \in \mathbb{O}(\lambda)$ and suppose that $\lambda' \neq \lambda$. By (2-4), we have $\mathcal{B}^+_{F_\chi}(\lambda')\mathcal{B}^+_{F_\chi}(\lambda) = \mathcal{B}^+_{F_\chi}(\lambda)\mathcal{B}^+_{F_\chi}(\lambda') = 0$ in $\widetilde{\mathrm{H}}_k$. This implies that $\mathcal{T}_\lambda(\mathbf{1}_{\mathrm{K},v}\mathcal{B}^+_{F_\chi}(\lambda')) = 0$ and therefore that $\mathbf{1}_{\mathrm{K},v}\mathcal{B}^+_{F_\chi}(\lambda') = 0$ by [Herzig 2011a, Corollary 6.5], which claims that $\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}}\rho$ is a torsion-free $\mathscr{H}(\mathrm{G}, \rho)$-module.

(b) By Lemma 3.4, we have

$$\begin{aligned}\mathcal{T}'_\lambda(\mathbf{1}_{\mathrm{K},v}) &= \mathbf{1}_{\mathrm{K},v}\mathcal{B}^+_{F_\chi}(\lambda) + \sum_{\substack{\lambda' \in \mathbb{O}(\lambda),\\ \lambda' \neq \lambda}} \mathbf{1}_{\mathrm{K},v}\mathcal{B}^+_{F_\chi}(\lambda') = \mathcal{T}_\lambda(\mathbf{1}_{\mathrm{K},v}) + \sum_{\substack{\lambda' \in \mathbb{O}(\lambda),\\ \lambda' \neq \lambda}} \mathbf{1}_{\mathrm{K},v}\mathcal{B}^+_{F_\chi}(\lambda')\\ &= \mathcal{T}_\lambda(\mathbf{1}_{\mathrm{K},v}),\end{aligned}$$

where the last equality follows from (a). □

Remark 4.2. By [Ollivier 2012, Lemma 3.6], the map

$$\chi \otimes_{\widetilde{\mathfrak{H}}_k} \widetilde{\mathrm{H}}_k \cong (\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}}\rho)^{\tilde{\mathrm{I}}}, \quad 1 \otimes 1 \mapsto \mathbf{1}_{\mathrm{K},v}, \tag{4-6}$$

induces an $\widetilde{\mathrm{H}}_k$-equivariant isomorphism. Proposition 4.1, combined with (4-6), proves that for $\lambda \in \mathrm{X}_*^+(\mathrm{T})$, the right actions of z_λ and of $\mathcal{B}^+_{F_\chi}(\lambda)$ on $1 \otimes 1 \in \chi \otimes_{\widetilde{\mathfrak{H}}_k} \widetilde{\mathrm{H}}_k$ coincide. This remark will be important for the classification of the simple supersingular $\widetilde{\mathrm{H}}_k$-modules in Section 5D.

Proposition 4.1 implies:

Theorem 4.3. *The diagram*

$$\begin{array}{ccc} k[\mathrm{X}_*^+(\mathrm{T})] & \xrightarrow{(2\text{-}5)} & \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \\ \| & & \downarrow{\scriptstyle (4\text{-}3)} \\ k[\mathrm{X}_*^+(\mathrm{T})] & \xrightarrow{\mathcal{T}} & \mathscr{H}(\mathrm{G}, \rho) \end{array} \tag{4-7}$$

is a commutative diagram of isomorphisms of k-algebras.

We remark that we have not used the fact that (2-5) is multiplicative. We proved this fact beforehand in Proposition 2.10, but it can also be seen as a consequence of the commutativity of the diagram.

5. Supersingularity

We turn to the study of the $\widetilde{\mathrm{H}}_k$-modules with finite length. We consider right modules unless otherwise specified. Recall that k is algebraically closed with characteristic p.

5A. ***A basis for the pro-p Iwahori–Hecke ring.*** We recall the $\mathbb{Z}$-basis for $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ defined in [Vignéras 2005]. It is indexed by $w \in \widetilde{\mathrm{W}}$ and is denoted by $(E_w)_{w\in\widetilde{\mathrm{W}}}$ there. We will call it $(\mathcal{B}^+_{x_0}(w))_{w\in\widetilde{\mathrm{W}}}$ because it coincides on $\widetilde{\mathrm{X}}_*(\mathrm{T})$ with the definition introduced in Section 2A (see also Remark 2.1). Recall that we have a decomposition of $\widetilde{\mathrm{W}}$ as the semidirect product

$$\widetilde{\mathrm{W}} = \mathrm{X}_*(\mathrm{T}) \rtimes \widetilde{\mathfrak{W}}.$$

For $w_0 \in \widetilde{\mathfrak{W}}$, set $\mathcal{B}^+_{x_0}(w_0) = \tau_{w_0}$ and for $w = e^\lambda w_0 \in \mathrm{X}_*(\mathrm{T}) \rtimes \widetilde{\mathfrak{W}}$, define in $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]$

$$\mathcal{B}^+_{x_0}(w) = q^{(\ell(w)-\ell(w_0)-\ell(e^\lambda))/2}\mathcal{B}^+_{x_0}(\lambda)\mathcal{B}^+_{x_0}(w_0) = q^{(\ell(w)-\ell(w_0))/2}\Theta^+_{x_0}(\lambda)\tau_{w_0}.$$

By [Vignéras 2005, Theorem 2 and Proposition 8], this element lies in $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ and the set of all $(\mathcal{B}^+_{x_0}(w))_{w\in\widetilde{\mathrm{W}}}$ is a $\mathbb{Z}$-basis for $\widetilde{\mathrm{H}}_{\mathbb{Z}}$.

Remark 5.1. As a $\mathbb{Z}$-module, $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ is the direct sum of $\mathcal{A}^+_{x_0}$ and of the $\mathbb{Z}$-module with basis $(\mathcal{B}^+_{x_0}(e^\lambda w_0))$, where λ ranges over $\mathrm{X}_*(\mathrm{T})$ and w_0 over the set of elements in $\widetilde{\mathfrak{W}}$ the projection of which in $\mathfrak{W}$ is nontrivial. Applying (2-1), we obtain that the $\mathbb{Z}$-module $\mathcal{A}^+_C$ is a direct summand of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ as well.

Remark 5.2. Let $d \in \mathcal{D}$ and $\tilde{d} \in \widetilde{\mathrm{W}}$ be a lift for d. Write $\tilde{d} = e^\lambda w_0$ with $w_0 \in \widetilde{\mathfrak{W}}$, $\lambda \in \mathrm{X}^+_*(\mathrm{T})$ and $\ell(e^\lambda) = \ell(d) + \ell(w_0)$ (Proposition 1.5).

Then in $\widetilde{\mathrm{H}}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[q^{\pm 1/2}]$, we have

$$\mathcal{B}^+_{x_0}(\tilde{d}) = q^{(\ell(\tilde{d})-\ell(w_0)+\ell(e^\lambda))/2}\tau^{-1}_{e^{-\lambda}}\tau_{w_0} = q^{\ell(\tilde{d})}\tau^{-1}_{\tilde{d}^{-1}} = (-1)^{\ell(d)}\iota(\tau_{\tilde{d}}). \quad (5\text{-}1)$$

5B. ***Topology on the pro-p Iwahori–Hecke algebra in characteristic p.*** We consider the (finitely generated) ideal $\mathfrak{I}$ of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ generated by all z_λ for $\lambda \in \mathrm{X}^+_*(\mathrm{T})$ such that $\ell(e^\lambda) > 0$, and the associated ring filtration of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$. A $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$-module M can be endowed with the $\mathfrak{I}$-adic topology induced by the filtration

$$M \supseteq M\mathfrak{I} \supseteq M\mathfrak{I}^2 \supseteq \cdots.$$

An example of such a module is $\widetilde{\mathrm{H}}_k$ itself. We define on $\widetilde{\mathrm{H}}_k$ another decreasing filtration $(F_n\widetilde{\mathrm{H}}_k)_{n\in\mathbb{N}}$ by k-vector spaces, where

$$F_n\widetilde{\mathrm{H}}_k := \text{the } k\text{-vector space generated by } \mathcal{B}^+_{x_0}(w),\ w\in\widetilde{\mathrm{W}} \text{ with } \ell(w)\geq n. \quad (5\text{-}2)$$

Lemma 5.3. *The filtration* (5-2) *is a filtration of* $\widetilde{\mathrm{H}}_k$ *as a left* $\mathcal{A}^+_{x_0}$*-module. In particular, it is a filtration of* $\widetilde{\mathrm{H}}_k$ *as a (left and right)* $\mathfrak{Z}^\circ(\widetilde{\mathrm{H}}_k)$*-module. It is compatible with the* $\mathfrak{I}$*-filtration: for all* $n\in\mathbb{N}$*, we have*

$$(F_n\widetilde{\mathrm{H}}_k)\mathfrak{I} = \mathfrak{I}\,(F_n\widetilde{\mathrm{H}}_k)\ \subseteq F_{n+1}\widetilde{\mathrm{H}}_k.$$

Proof. Let $\lambda\in\widetilde{\mathrm{X}}_*(\mathrm{T})$ and $w\in\widetilde{\mathrm{W}}$. From the definition of $\mathcal{B}^+_{x_0}$, we see that

$$\mathcal{B}^+_{x_0}(\lambda)\mathcal{B}^+_{x_0}(w) = q^{(\ell(e^\lambda)+\ell(w)-\ell(e^\lambda w))/2}\mathcal{B}^+_{x_0}(e^\lambda w)$$

and therefore in $\widetilde{\mathrm{H}}_k$ we have $\mathcal{B}^+_{x_0}(\lambda)\mathcal{B}^+_{x_0}(w)=0$ if $\ell(e^\lambda)+\ell(w)>\ell(e^\lambda w)$ and $\mathcal{B}^+_{x_0}(\lambda)\mathcal{B}^+_{x_0}(w)=\mathcal{B}^+_{x_0}(e^\lambda w)$ if $\ell(w)+\ell(e^\lambda)=\ell(e^\lambda w)$. This proves the claims. □

Proposition 5.4. *The* $\mathfrak{I}$*-adic topology on* $\widetilde{\mathrm{H}}_k$ *is equivalent to the topology on* $\widetilde{\mathrm{H}}_k$ *induced by the filtration* $(F_n\widetilde{\mathrm{H}}_k)_{n\in\mathbb{N}}$*. In particular, it is independent of the choice of the uniformizer* ϖ*.*

Proof. We have to prove that given $m\in\mathbb{N}$, $m\geq 1$, there is $n\in\mathbb{N}$ such that $F_n\widetilde{\mathrm{H}}_k\subseteq\mathfrak{I}^m\widetilde{\mathrm{H}}_k$.

Fact iii. *For* $\lambda\in\mathrm{X}_*(\mathrm{T})$ *such that* $\ell(e^\lambda)>0$ *and* $m\geq 1$*, we have* $\mathcal{B}^+_{x_0}((m+1)\lambda)\in\mathfrak{I}^m\widetilde{\mathrm{H}}_k$.

Proof. We check that for $m\in\mathbb{N}$ we have $\mathcal{B}^+_{x_0}((m+1)\lambda)=z_\lambda^m\mathcal{B}^+_{x_0}(\lambda)$. Notice that $\mathcal{B}^+_{x_0}(2\lambda)=\mathcal{B}^+_{x_0}(\lambda)\mathcal{B}^+_{x_0}(\lambda)=z_\lambda\mathcal{B}^+_{x_0}(\lambda)$ by (2-4) and Lemma 3.4. Now let $m\geq 2$. We have $\mathcal{B}^+_{x_0}((m+1)\lambda)=\mathcal{B}^+_{x_0}(m\lambda)\mathcal{B}^+_{x_0}(\lambda)=z_\lambda^m\mathcal{B}^+_{x_0}(\lambda)$ by induction. □

Fact iv. *Let* $m\geq 1$*. There is* $A_m\in\mathbb{N}$ *such that for any* $\lambda\in\mathrm{X}_*(\mathrm{T})$*, if* $\ell(e^\lambda)>A_m$ *then* $\mathcal{B}^+_{x_0}(\lambda)\in\mathfrak{I}^m\widetilde{\mathrm{H}}_k$.

Proof. Let $\{z_{\lambda_1},\dots,z_{\lambda_r}\}$ be a system of generators of $\mathfrak{I}$ with $\lambda_1,\dots,\lambda_r\in\mathrm{X}_*^+(\mathrm{T})$. Let $A_m:=m\sum_{i=1}^r\ell(e^{\lambda_i})$. Let $\lambda\in\mathrm{X}_*(\mathrm{T})$ such that $\ell(e^\lambda)>0$. This is $\mathfrak{W}$-conjugate to an element $\lambda_0\in\mathrm{X}_*^+(\mathrm{T})$, and one can write $\lambda=w_0.\lambda_0$ with $w_0\in\mathfrak{W}$ and $\lambda_0=\sum_{i=1}^r a_i\lambda_i$ with $a_i\in\mathbb{N}$ (not all equal to zero). If $\ell(e^\lambda)=\ell(e^{\lambda_0})>A_m$, then there is $i_0\in\{1,\dots,r\}$ such that $a_{i_0}>m$ and $\mathcal{B}^+_{x_0}(\lambda)=\prod_{i=1}^r\mathcal{B}^+_{x_0}(a_i(w_0.\lambda_i))\in\mathcal{B}^+_{x_0}((m+1)(w_0.\lambda_{i_0}))\widetilde{\mathrm{H}}_k\subseteq\mathfrak{I}^m\widetilde{\mathrm{H}}_k$ by Fact iii. □

We now turn to the proof of the proposition. Let $m\geq 1$. To any $w_0\in\mathfrak{W}$ corresponds, by [Vignéras 2006, (1.6.3)], a finite set $\mathrm{X}(w_0)$ of elements in $\mathrm{X}_*(\mathrm{T})$ such that

$$\text{for all } \lambda\in\mathrm{X}_*(\mathrm{T}) \text{ there is } \mu\in\mathrm{X}(w_0) \text{ such that } \ell(e^\lambda w_0)=\ell(e^{\lambda-\mu})+\ell(e^\mu w_0).$$

Let $\tilde{w} \in \widetilde{\mathrm{W}}$ with image w_0 under the projection $\widetilde{\mathrm{W}} \to \mathfrak{W}$. Its image w under $\widetilde{\mathrm{W}} \to \mathrm{W}$ has the form $w = e^{\lambda} w_0 \in \mathrm{X}_*(\mathrm{T}) \rtimes \mathfrak{W}$, and there is $\mu \in \mathrm{X}(w_0)$ such that $\ell(w) = \ell(e^{\lambda-\mu}) + \ell(e^{\mu} w_0)$. Choose lifts $\widetilde{e}^{\mu} w_0$ and $\widetilde{e}^{\lambda-\mu}$ in $\widetilde{\mathrm{W}}$ for $e^{\mu} w_0$ and $e^{\lambda-\mu}$. The product $\widetilde{e}^{\lambda-\mu}\widetilde{e}^{\mu} w_0$ differs from $\tilde{w}$ by an element in $\mathrm{T}^0/\mathrm{T}^1$ (which has length zero). Therefore, $\mathcal{B}^+_{x_0}(\tilde{w}) \in \mathcal{B}^+_{x_0}(\lambda-\mu)\widetilde{\mathrm{H}}_k$ (see the proof of Lemma 5.3, for example). If $\ell(\tilde{w}) > A_m(w_0) := A_m + \max\{\ell(e^{\mu'} w_0),\ \mu' \in \mathrm{X}(w_0)\}$ then $\ell(e^{\lambda-\mu}) > A_m$ and $\mathcal{B}^+_{x_0}(\tilde{w}) \in \mathfrak{I}^m \widetilde{\mathrm{H}}_k$ by Fact iv.

We have proved that $n > \max\{A_m(w_0), w_0 \in \mathfrak{W}\}$ implies $F_n \widetilde{\mathrm{H}}_k \subseteq \mathfrak{I}^m \widetilde{\mathrm{H}}_k$. □

5C. ***The category of modules of finite length over the pro-p Iwahori–Hecke algebra in characteristic p.*** We consider the abelian category $\mathrm{Mod}_{fg}(\widetilde{\mathrm{H}}_k)$ of all $\widetilde{\mathrm{H}}_k$-modules with finite length.

For an $\widetilde{\mathrm{H}}_k$-module, having finite length is equivalent to being finite-dimensional as a k-vector space (see [Vignéras 2007, Section 5.3] or [Ollivier and Schneider 2012, Lemma 6.9]). Therefore, any irreducible $\widetilde{\mathrm{H}}_k$-module is finite dimensional and has a central character, and any module in $\mathrm{Mod}_{fg}(\widetilde{\mathrm{H}}_k)$ decomposes uniquely into a direct sum of indecomposable modules.

5C1. *The category of finite-dimensional $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$-modules.* Let $\mathrm{Mod}_{fd}(\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k))$ denote the category of finite-dimensional $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$-modules. For $\mathfrak{M}$ a maximal ideal of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$, we consider the full subcategory

$$\mathfrak{M}\text{-}\,\mathrm{Mod}_{fd}(\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k))$$

of modules M of $\mathfrak{M}$-torsion, that is, such that there is $e \in \mathbb{N}$ satisfying $M\mathfrak{M}^e = 0$. The category $\mathrm{Mod}_{fd}(\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k))$ decomposes into the direct sum

$$\bigoplus_{\mathfrak{M}} \mathfrak{M}\text{-}\,\mathrm{Mod}_{fd}(\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)),$$

where $\mathfrak{M}$ ranges over the maximal ideals of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$.

5C2. *Blocks of $\widetilde{\mathrm{H}}_k$-modules with finite length.* For $\mathfrak{M}$ a maximal ideal of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$, we say that an $\widetilde{\mathrm{H}}_k$-module with finite length is an $\mathfrak{M}$-torsion module if its restriction to a $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$-module lies in the subcategory $\mathfrak{M}\text{-}\,\mathrm{Mod}_{fd}(\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k))$. We denote by

$$\mathfrak{M}\text{-}\,\mathrm{Mod}_{fg}(\widetilde{\mathrm{H}}_k) \tag{5-3}$$

the full subcategory of $\mathrm{Mod}_{fg}(\widetilde{\mathrm{H}}_k)$ whose objects are the $\mathfrak{M}$-torsion modules.

Lemma 5.5. *Let $\mathfrak{M}$ and $\mathfrak{N}$ be two maximal ideals of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$. If there is a nonzero $\mathfrak{M}$-torsion module M and a nonzero $\mathfrak{N}$-torsion module N such that $\mathrm{Ext}^r_{\widetilde{\mathrm{H}}_k}(M, N) \neq 0$ for some $r \geq 0$, then $\mathfrak{M} = \mathfrak{N}$.*

Proof. For any $\widetilde{\mathrm{H}}_k$-modules X and Y, the natural morphisms of algebras $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \to \mathrm{End}_{\widetilde{\mathrm{H}}_k}(X)$ and $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \to \mathrm{End}_{\widetilde{\mathrm{H}}_k}(Y)$ equip $\mathrm{Hom}_{\widetilde{\mathrm{H}}_k}(X, Y)$ with the structure of a

central $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$-bimodule. The space $\mathrm{Ext}^r_{\widetilde{\mathrm{H}}_k}(M,N)$ is therefore naturally a central $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$-bimodule. It is an $\mathfrak{M}$-torsion module and an $\mathfrak{N}$-torsion module; it is zero unless $\mathfrak{M}=\mathfrak{N}$. □

Since $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ is a central finitely generated subalgebra of $\widetilde{\mathrm{H}}_k$, an indecomposable $\widetilde{\mathrm{H}}_k$-module with finite length is an $\mathfrak{M}$-torsion module for some maximal ideal $\mathfrak{M}$ of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$.

Remark 5.6. An $\widetilde{\mathrm{H}}_k$-module with finite length M lies in the block corresponding to some maximal ideal $\mathfrak{M}$ if and only if all the characters of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ contained in M have kernel $\mathfrak{M}$.

Remark 5.7. The blocks (5-3) are not indecomposable. They can for example be further decomposed via the idempotents introduced in Section 1B8.

5C3. *The supersingular block.*

Definition 5.8. We call a maximal ideal $\mathfrak{M}$ of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ supersingular if it contains the ideal $\mathfrak{I}$ defined in Section 5B. A character of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ is called supersingular if its kernel is a supersingular maximal ideal of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$.

Given a character ω of the connected center Z of G, there is a unique supersingular character ζ_ω of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ satisfying $\zeta_\omega(z_\lambda)=\omega(\lambda(\varpi))$ for any $\lambda\in \mathrm{X}_*^+(\mathrm{T})$ with length zero. A character of the center of $\widetilde{\mathrm{H}}_k$ is called "null" in [Vignéras 2005] if it takes value zero at all central elements (2-2) for all $\mathfrak{W}$-orbits $\mathbb{O}$ in $\widetilde{\mathrm{X}}_*(\mathrm{T})$ containing a coweight with nonzero length.

Lemma 5.9. *A character $\mathscr{Z}(\widetilde{\mathrm{H}}_k)\to k$ is null if and only if its restriction to $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ is a supersingular character in the sense of Definition 5.8.*

Proof. Consider a character $\zeta:\mathscr{Z}(\widetilde{\mathrm{H}}_k)\to k$ whose restriction to $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ is supersingular. We want to prove that ζ is null. Since the $\widetilde{\mathrm{H}}_k$-module $\widetilde{\mathrm{H}}_k\otimes_{\mathscr{Z}(\widetilde{\mathrm{H}}_k)}\zeta$ is finite dimensional, it contains a character $\hat{\zeta}$ for the commutative finitely generated k-algebra $(\mathcal{A}^+_{x_0})_k$ and the restriction of $\hat{\zeta}$ to $\mathscr{Z}(\widetilde{\mathrm{H}}_k)$ coincides with ζ.

Let $\lambda\in \mathrm{X}_*^+(\mathrm{T})$ with $\ell(e^\lambda)\neq 0$; by (2-4), there is at most one $\mathfrak{W}$-conjugate λ' of λ such that $\hat{\zeta}(\mathcal{B}^+_{x_0}(\lambda'))\neq 0$, and if there exists such a λ', then $\hat{\zeta}(z_\lambda)=\zeta(z_\lambda)\neq 0$, which is a contradiction; we have proved that $\hat{\zeta}(\mathcal{B}^+_{x_0}(\lambda'))=0$ for all $\lambda'\in \mathrm{X}_*(\mathrm{T})$ with $\ell(e^{\lambda'})\neq 0$, which implies that this is also the case for $\lambda'\in\widetilde{\mathrm{X}}_*(\mathrm{T})$ with $\ell(e^{\lambda'})\neq 0$. Therefore, ζ is null. □

A finite-dimensional $\widetilde{\mathrm{H}}_k$-module M with central character is called supersingular in [Vignéras 2005] if this central character is null. We extend this definition:

Proposition-Definition 5.10. *A finite-length $\widetilde{\mathrm{H}}_k$-module is in the supersingular block and is called* supersingular *if and only if, equipped with the discrete topology, it is a continuous module for the $\mathfrak{I}$-adic topology on $\widetilde{\mathrm{H}}_k$ or, equivalently, for the topology induced by the filtration* (5-2).

Proof. An indecomposable $\widetilde{\mathrm{H}}_k$-module M with finite length is in the supersingular block if and only if there is $m \geq 1$ such that $M\mathfrak{I}^m = \{0\}$. Then use Proposition 5.4. □

5D. ***Classification of the simple supersingular modules over the pro-p Iwahori–Hecke algebra in characteristic p.*** We establish this classification in the case where the root system of G is irreducible, which we will suppose in Section 5D4. Until then the results are valid without further assumption on the root system.

5D1. Denote by $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ the natural image in $\widetilde{\mathrm{H}}_k$ of the affine Hecke subring $\widetilde{\mathrm{H}}_{\mathbb{Z}}^{\mathrm{aff}}$ of $\widetilde{\mathrm{H}}_{\mathbb{Z}}$ defined in Section 1B7. We generalize [Ollivier 2010, Theorem 7.3]:

Proposition 5.11. *A finite-length $\widetilde{\mathrm{H}}_k$-module in the supersingular block contains a character for the affine Hecke subalgebra $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$.*

Proof. Let M be an $\widetilde{\mathrm{H}}_k$-module with finite length in the supersingular block. By Proposition-Definition 5.10, there is $n \in \mathbb{N}$ such that for any $w \in \widetilde{\mathrm{W}}$, if $\ell(w) > n$ then $M\mathcal{B}_{x_0}^+(w) = 0$. Let $x \in M$, and suppose that it supports a character for $\widetilde{\mathfrak{H}}_k$ (see Section 1B9) and let $d \in \mathcal{D}$ with maximal length such that $x\mathcal{B}_{x_0}^+(\tilde{d}) \neq 0$, where $\tilde{d} \in \widetilde{\mathrm{W}}$ denotes a lift for d (the property $x\mathcal{B}_{x_0}^+(\tilde{d}) \neq 0$ does not depend on the choice of the lift $\tilde{d}$). As in the proof of [Ollivier 2010, Theorem 7.3], we prove that $x' := x\mathcal{B}_{x_0}^+(\tilde{d})$ supports a character for $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ which is the k-algebra generated by all τ_t and all $\tau_{\tilde{s}}$ for $t \in \mathrm{T}^0/\mathrm{T}^1$ and $s \in S_{\mathrm{aff}}$ with chosen lift $\tilde{s} \in \widetilde{\mathrm{W}}$ (see paragraph Section 1B7). From the relations (1-11) we get that $x'\tau_t = x\tau_{dtd^{-1}}\mathcal{B}_{x_0}^+(\tilde{d})$ is proportional to x'. Now let $s \in S_{\mathrm{aff}}$. If $\ell(ds) = \ell(d) - 1$, then $ds \in \mathcal{D}$ by Proposition 1.5 and, by (5-1), the element x' is equal to $x\iota(\tau_{\tilde{d}\tilde{s}})\iota(\tau_{\tilde{s}})$ (up to an invertible element in k), so $x'\tau_{\tilde{s}} = 0$ by Remark 1.10. If $\ell(ds) = \ell(d) + 1$ and $ds \in \mathcal{D}$, then $x\mathcal{B}_{x_0}^+(\tilde{d}\tilde{s})$ is equal to zero on one side and, by (5-1), to $x'\iota(\tau_{\tilde{s}})$ (up to an invertible element in k) on the other side. This proves that $x'\tau_{\tilde{s}}$ is proportional to x' by Remark 1.10. If $\ell(ds) = \ell(d) + 1$ and $ds \notin \mathcal{D}$ then there is $s' \in S$ such that $ds = s'd$ by Proposition 1.5, and $x'\iota(\tau_{\tilde{s}})$ is proportional to $x\iota(\tau_{\tilde{s}'})\mathcal{B}_{x_0}^+(\tilde{d})$ and therefore to x' because $\iota(\tau_{\tilde{s}'}) \in \widetilde{\mathfrak{H}}_k$. We conclude that $x'\tau_{\tilde{s}}$ is proportional to x' by Remark 1.10. □

5D2. *Characters of* $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$. We call a morphism of k-algebras $\widetilde{\mathrm{H}}_k^{\mathrm{aff}} \to k$ a character of $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$. A character $\mathcal{X}$ of $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ is completely determined by:

- The unique $\xi \in \widehat{\overline{\mathbf{T}}}(\mathbb{F}_q)$ such that $\mathcal{X}(\epsilon_\xi) = 1$ (see notation in Section 1B8). This ξ is defined by $\xi(t) = \mathcal{X}(\tau_t)$, where $t \in \mathrm{T}^0/\mathrm{T}^1 = \overline{\mathbf{T}}(\mathbb{F}_q)$, and we call ξ the restriction of $\mathcal{X}$ to $k[\mathrm{T}^0/\mathrm{T}^1]$.
- The values $\mathcal{X}(\tau_{n_A})$ for all $A \in S_{\mathrm{aff}}$, which, by the quadratic relations (1-15) satisfy $\mathcal{X}(\tau_{n_A}) \in \{0, -1\}$, if ξ is trivial on T_A, and $\mathcal{X}(\tau_{n_A}) = 0$ otherwise.

Conversely, one checks that any such datum of $\xi \in \hat{\tilde{\mathbf{T}}}(\mathbb{F}_q)$ and values $\mathcal{X}(\tau_{n_A})$ for all $A \in S_{\mathrm{aff}}$ satisfying the above conditions defines a character $\mathcal{X}$ of $\tilde{\mathrm{H}}_k^{\mathrm{aff}}$.

Example. The pro-p Iwahori–Hecke ring $\tilde{\mathrm{H}}_{\mathbb{Z}}$ is endowed with two natural morphisms of rings $\tilde{\mathrm{H}}_{\mathbb{Z}} \to \mathbb{Z}$ defined by

$$\tau_w \mapsto q^{\ell(w)} \quad \text{and} \quad \tau_w \mapsto (-1)^{\ell(w)}.$$

We denote by $\mathcal{X}_{\mathrm{triv}}$ and $\mathcal{X}_{\mathrm{sign}}$ the characters of $\tilde{\mathrm{H}}_k$ that they respectively induce, as well as their restrictions to characters of $\tilde{\mathrm{H}}_k^{\mathrm{aff}}$. The former can be described by $\xi = \mathbf{1}$ and $\mathcal{X}_{\mathrm{triv}}(\tau_{n_A}) = 0$ for all $A \in S_{\mathrm{aff}}$, the latter by $\xi = \mathbf{1}$ and $\mathcal{X}_{\mathrm{sign}}(\tau_{n_A}) = -1$ for all $A \in S_{\mathrm{aff}}$.

Let $\mathcal{X}$ be a character of $\tilde{\mathrm{H}}_k^{\mathrm{aff}}$ and ξ the corresponding element in $\hat{\tilde{\mathbf{T}}}(\mathbb{F}_q)$.

- Let $\xi_0 \in \hat{\tilde{\mathbf{T}}}(\mathbb{F}_q)$, and suppose that ξ_0 is trivial on T_α for all $\alpha \in \Pi$. Then one can consider the twist $(\xi_0)\mathcal{X}$ of $\mathcal{X}$ by ξ_0 in the obvious way. The restriction of $(\xi_0)\mathcal{X}$ to $k[\mathrm{T}^0/\mathrm{T}^1]$ is the product $\xi_0\xi$, and $(\xi_0)\mathcal{X}$ coincides with $\mathcal{X}$ on the elements of type τ_{n_A} for $A \in S_{\mathrm{aff}}$. By a *twist of the character* $\mathcal{X}$, we mean from now on a twist of $\mathcal{X}$ by an element in $\hat{\tilde{\mathbf{T}}}(\mathbb{F}_q)$ that is trivial on T_α for all $\alpha \in \Pi$.
- The involution ι_C extends to an involution of the k-algebra $\tilde{\mathrm{H}}_k$. The composition $\mathcal{X} \circ \iota_C$ is then also a character for $\tilde{\mathrm{H}}_k^{\mathrm{aff}}$. Note that $\mathcal{X}$ and $\mathcal{X} \circ \iota_C$ have the same restriction to $k[\mathrm{T}^0/\mathrm{T}^1]$ (Remark 1.9). Furthermore, if $\mathcal{X}(\tau_{n_A}) = -1$ for some $A \in S_{\mathrm{aff}}$, then $\mathcal{X} \circ \iota_C(\tau_{n_A}) = 0$ (use Remark 1.10). For example, $\mathcal{X}_{\mathrm{triv}} = \mathcal{X}_{\mathrm{sign}} \circ \iota_C$.
- There is an action of $\tilde{\Omega}$ by conjugacy on $\tilde{\mathrm{W}}_{\mathrm{aff}}$. Since the elements in $\tilde{\Omega}$ have length zero, this yields an action of $\tilde{\Omega}$ on $\tilde{\mathrm{H}}_k^{\mathrm{aff}}$ and its characters. For $\omega \in \tilde{\Omega}$, we denote by $\omega.\mathcal{X}$ the character $\mathcal{X}(\tau_{\omega^{-1}} \,.\, \tau_\omega)$.

Lemma 5.12. *A simple $\tilde{\mathrm{H}}_k$-module containing a twist of the character $\mathcal{X}_{\mathrm{triv}}$ or of the character $\mathcal{X}_{\mathrm{sign}}$ of $\tilde{\mathrm{H}}_k^{\mathrm{aff}}$ is not supersingular.*

Proof. Let M be a simple $\tilde{\mathrm{H}}_k$-module. Suppose that it contains a twist of the character $\mathcal{X}_{\mathrm{sign}}$ supported by the nonzero vector $m \in M$. In particular, m supports the character of $\tilde{\mathfrak{H}}_k$ parametrized by (a twist of) the trivial character of $\hat{\tilde{\mathbf{T}}}(\mathbb{F}_q)$ and by the facet C (see Section 1B9). By Remark 4.2, we have

$$m z_\lambda = m\mathcal{B}_C^+(\lambda)$$

for all $\lambda \in X_*^+(\mathrm{T})$. There are $\omega \in \tilde{\Omega}$ and $w \in \tilde{\mathrm{W}}_{\mathrm{aff}}$ such that $\lambda(\varpi^{-1}) \mod \mathrm{T}^1$ corresponds to $w\omega \in \tilde{\mathrm{W}}$. Since $\mathcal{B}_C^+(\lambda) = \tau_{\lambda(\varpi^{-1})}$, the element $m\mathcal{B}_C^+(\lambda)$ is equal to $(-1)^{\ell(w)} m\tau_\omega$ (up to multiplication by an element in $k^\times$), and we recall that τ_ω is invertible in $\tilde{\mathrm{H}}_k$. We have proved that $m.z_\lambda \neq 0$ and M is not supersingular.

Now if M contains a twist of the character $\mathcal{X}_{\text{triv}}$, then $\iota_C^* M$ contains a twist of the character $\mathcal{X}_{\text{sign}}$ and is not supersingular (notation in the proof of Proposition 3.3). By Proposition 3.2, this implies that M is not supersingular either. □

5D3. Consider the image of $\widetilde{\Omega}$ in $\widetilde{\mathrm{H}}_k$ via $\omega \mapsto \tau_\omega$. For $\mathcal{X}$ a character of $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$, denote by $\widetilde{\Omega}_{\mathcal{X}}$ its fixator under the action of $\widetilde{\Omega}$; obviously $\widetilde{\Omega}_{\mathcal{X}}$ contains $\mathrm{T}^0/\mathrm{T}^1$ as a subgroup. We consider the set $\mathcal{P}$ of pairs $(\mathcal{X}, \sigma)$ where $\mathcal{X}$ is a character of $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ and $(\sigma, \mathrm{V}_\sigma)$ an irreducible finite-dimensional k-representation of $\widetilde{\Omega}_{\mathcal{X}}$ (up to isomorphism) whose restriction to $\mathrm{T}^0/\mathrm{T}^1$ coincides with the inverse of the restriction of $\mathcal{X}$; for any $t \in \mathrm{T}^0/\mathrm{T}^1$ and $v \in \mathrm{V}_\sigma$, we have $\sigma(t)v = \mathcal{X}(\tau_{t^{-1}})v$.

The set $\mathcal{P}$ is naturally endowed with an action of $\widetilde{\Omega}$: for $(\mathcal{X}, \sigma) \in \mathcal{P}$ and $\omega \in \widetilde{\Omega}$, denote by $\omega.\sigma$ the representation of $\widetilde{\Omega}_{\omega.\mathcal{X}} = \omega \widetilde{\Omega}_{\mathcal{X}} \omega^{-1}$ naturally obtained by conjugating σ; then $\omega.(\mathcal{X}, \sigma) := (\omega.\mathcal{X}, \omega.\sigma) \in \mathcal{P}$.

Let $(\mathcal{X}, \sigma) \in \mathcal{P}$. Consider the subalgebra $\widetilde{\mathrm{H}}_k(\mathcal{X})$ of $\widetilde{\mathrm{H}}_k$ generated by $k[\widetilde{\Omega}_{\mathcal{X}}]$ and $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$. It is isomorphic to the twisted tensor product of algebras

$$\widetilde{\mathrm{H}}_k(\mathcal{X}) \simeq k[\widetilde{\Omega}_{\mathcal{X}}] \otimes_{k[\mathrm{T}^0/\mathrm{T}^1]} \widetilde{\mathrm{H}}_k^{\mathrm{aff}},$$

where the product is given by $(\omega \otimes h)(\omega' \otimes h') = \omega\omega' \otimes \tau_{\omega'}^{-1} h \tau_{\omega'} h'$. As a left $\widetilde{\mathrm{H}}_k(\mathcal{X})$-module, $\widetilde{\mathrm{H}}_k$ is free with basis the set of all τ_ω, where ω ranges over a set of representatives of the right cosets $\widetilde{\Omega}_{\mathcal{X}} \backslash \widetilde{\Omega}$. The tensor product $\sigma \otimes \mathcal{X}$ is naturally a right $\widetilde{\mathrm{H}}_k(\mathcal{X})$-module: the right action of $\omega \otimes h$ on $v \in \mathrm{V}_\sigma$ is given by $\mathcal{X}(h)\sigma(\omega^{-1})v$. The right $\widetilde{\mathrm{H}}_k(\mathcal{X})$-module $\sigma \otimes \mathcal{X}$ is irreducible. As an $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$-module, it is isomorphic to a direct sum of copies of $\mathcal{X}$.

Lemma 5.13. *The isomorphism classes of the simple $\widetilde{\mathrm{H}}_k$-modules containing a character for $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ are represented by the induced modules*

$$\mathfrak{m}(\mathcal{X}, \sigma) := (\sigma \otimes \mathcal{X}) \otimes_{\widetilde{\mathrm{H}}_k(\mathcal{X})} \widetilde{\mathrm{H}}_k,$$

where $(\mathcal{X}, \sigma)$ ranges over the set of orbits in $\mathcal{P}$ under the action of $\widetilde{\Omega}$.

Proof. First note that for any $\omega \in \widetilde{\Omega}$, the $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \omega.\mathcal{X})$-isotypic component of $\mathfrak{m}(\mathcal{X}, \sigma)$ is isomorphic to $\omega.\sigma \otimes \omega\mathcal{X}$ as a right $\widetilde{\mathrm{H}}_k(\omega.\mathcal{X})$-module.

(1) We check that an $\widetilde{\mathrm{H}}_k$-module of the form $\mathfrak{m}(\mathcal{X}, \sigma)$ is irreducible. Restricted to $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$, it is semisimple and isomorphic to a direct sum of $\mathcal{X}$ and of its conjugates. Therefore, a submodule $\mathfrak{m}$ of $\mathfrak{m}(\mathcal{X}, \sigma)$ contains a nonzero $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \omega.\mathcal{X})$-isotypic vector for some $\omega \in \widetilde{\Omega}$, and, after translating by $\tau_{\omega^{-1}}$, we see that $\mathfrak{m}$ contains a nonzero $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \mathcal{X})$-isotypic vector. But the $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \mathcal{X})$-isotypic component in $\mathfrak{m}(\mathcal{X}, \sigma)$ supports the irreducible representation σ of $k[\widetilde{\Omega}_{\mathcal{X}}]$. Therefore $\mathfrak{m} = \mathfrak{m}(\mathcal{X}, \sigma)$.

(2) Let $\mathfrak{m}$ be a simple $\widetilde{\mathrm{H}}_k$-module containing the character $\mathcal{X}$ of $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$. Its $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \mathcal{X})$-isotypic component contains an irreducible (finite-dimensional) representation σ of

$k[\widetilde{\Omega}_{\mathcal{X}}]$ which coincides with the inverse of $\mathcal{X}$ on $k[\mathrm{T}^0/\mathrm{T}^1]$. Therefore, using (1), $\mathfrak{m} \simeq (\sigma \otimes \mathcal{X}) \otimes_{\widetilde{\mathrm{H}}_k(\mathcal{X})} \widetilde{\mathrm{H}}_k$.

(3) Let $\omega \in \widetilde{\Omega}$ and $(\mathcal{X}, \sigma) \in \mathcal{P}$. The $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \mathcal{X})$-isotypic component of $\mathfrak{m}(\omega.(\mathcal{X}, \sigma))$ contains the representation σ of $k[\widetilde{\Omega}_{\mathcal{X}}]$. The simple $\widetilde{\mathrm{H}}_k$-module $\mathfrak{m}(\omega.(\mathcal{X}, \sigma))$ is therefore isomorphic to $\mathfrak{m}(\mathcal{X}, \sigma)$ by (2).

(4) Let $(\mathcal{X}, \sigma)$ and $(\mathcal{X}', \sigma')$ be in $\mathcal{P}$ and suppose that they induce isomorphic $\widetilde{\mathrm{H}}_k$-modules. Looking at the restriction of the latter to $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$, we see that there is $\omega \in \widetilde{\Omega}$ such that $\mathcal{X}' = \omega.\mathcal{X}$.

Therefore, by (3), $\mathfrak{m}(\mathcal{X}, \omega^{-1}\sigma')$ and $\mathfrak{m}(\mathcal{X}, \sigma)$ are isomorphic, and looking at the restriction to the $(\widetilde{\mathrm{H}}_k^{\mathrm{aff}}, \mathcal{X})$-isotypic component shows that $\sigma' \simeq \omega.\sigma$. Therefore, $(\mathcal{X}', \sigma')$ and $(\mathcal{X}, \sigma)$ are conjugate. □

5D4. *Classification of the simple supersingular $\widetilde{\mathrm{H}}_k$-modules when the root system of* G *is irreducible.* We generalize [Vignéras 2005, Theorem 5(1)] and [Ollivier 2010, Theorem 7.3].

Theorem 5.14. *Suppose that the root system of* G *is irreducible. A simple $\widetilde{\mathrm{H}}_k$-module is supersingular if and only if it contains a character for $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ that is different from a twist of $\mathcal{X}_{\mathrm{triv}}$ or $\mathcal{X}_{\mathrm{sign}}$.*

Remark 5.15. This proves in particular (if the root system of G is irreducible) that the notion of supersingularity for Hecke modules does not depend on any of the choices made.

Proof of Theorem 5.14. We already proved in Proposition 5.11 (without restriction on the root system of G) that a simple supersingular module contains a character for $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$, and by Lemma 5.12 we know that this character is not a twist of $\mathcal{X}_{\mathrm{triv}}$ or $\mathcal{X}_{\mathrm{sign}}$.

Conversely, let $\mathfrak{m}$ be a simple $\widetilde{\mathrm{H}}_k$-module containing the character $\mathcal{X}$ for $\widetilde{\mathrm{H}}_k^{\mathrm{aff}}$ and suppose that $\mathcal{X}$ is not a twist of $\mathcal{X}_{\mathrm{triv}}$ or $\mathcal{X}_{\mathrm{sign}}$. We want to prove that $\mathfrak{m}$ is supersingular. Since, by Proposition 3.2, this is equivalent to showing that $\iota_C^*\mathfrak{m}$ is supersingular (notation in the proof of Proposition 3.3), we can suppose (see the discussion before Lemma 5.12) that $\mathcal{X}(\tau_{n_0}) = 0$, where n_0 was introduced in Section 2A3.

Let $m \in \mathfrak{m}$ be a nonzero vector supporting $\mathcal{X}$. Let χ be the restriction of $\mathcal{X}$ to $\widetilde{\mathfrak{H}}_k$ and F_χ the associated standard facet. Suppose that $F_\chi = x_0$; then $\Pi_{\bar{\chi}} = \Pi_\chi = \Pi$ (notation in Section 1B9) and $\mathcal{X}(\tau_{n_\alpha}) = 0$ for all $\alpha \in \Pi$. Since, by hypothesis, we also have $\mathcal{X}(\tau_{n_0}) = 0$, the character $\mathcal{X}$ is equal to $\mathcal{X}_{\mathrm{triv}}$ up to twist. Therefore, $F_\chi \neq x_0$. Let $\lambda \in \mathrm{X}_*^+(\mathrm{T})$ with $\ell(e^\lambda) > 0$. By Remark 4.2,

$$m.z_\lambda = m.\mathcal{B}^+_{F_\chi}(\lambda),$$

and, since $F_\chi \neq x_0$, we have $m.z_\lambda = 0$ by Lemma 2.4. We have proved that $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ acts on m and therefore on $\mathfrak{m}$ by a supersingular character. □

Let $\mathcal{P}^*$ denote the subsets of pairs $(\mathcal{X}, \sigma)$ in $\mathcal{P}$ such that $\mathcal{X}$ is different from a twist of $\mathcal{X}_{\mathrm{triv}}$ or $\mathcal{X}_{\mathrm{sign}}$. It is stable under the action of $\widetilde{\Omega}$. Lemma 5.13 and Theorem 5.14 together give the following:

Corollary 5.16. *Suppose that the root system of* G *is irreducible. The map*

$$(\mathcal{X}, \sigma) \mapsto \mathfrak{m}(\mathcal{X}, \sigma)$$

induces a bijection between the $\widetilde{\Omega}$*-orbits of pairs* $(\mathcal{X}, \sigma) \in \mathcal{P}^*$ *and a system of representatives of the isomorphism classes of the simple supersingular* $\widetilde{\mathrm{H}}_k$*-modules.*

5E. *Pro-p Iwahori invariants of parabolic inductions and of special representations.*

5E1. In this section, $\mathbf{k}$ is an arbitrary field. Let F be a standard facet, Π_F the associated set of simple roots and P_F the group of $\mathfrak{F}$-points of the corresponding standard parabolic subgroup, with Levi decomposition $\mathrm{P}_F = \mathrm{M}_F\mathrm{N}_F$. We use the same notation as in Section 3C1. The unipotent subgroup N_F is generated by all the root subgroups $\mathcal{U}_\alpha$ for $\alpha \in \Phi^+ - \Phi_F^+$. Let N_F^- denote the opposite unipotent subgroup of G. The pro-p Iwahori subgroup $\tilde{\mathrm{I}}$ has the decomposition

$$\tilde{\mathrm{I}} = \tilde{\mathrm{I}}_F^+ \, \tilde{\mathrm{I}}_F^0 \, \tilde{\mathrm{I}}_F^-,$$

where

$$\tilde{\mathrm{I}}_F^+ := \tilde{\mathrm{I}} \cap \mathrm{N}_F, \quad \tilde{\mathrm{I}}_F^0 := \tilde{\mathrm{I}} \cap \mathrm{M}_F, \quad \tilde{\mathrm{I}}_F^- := \tilde{\mathrm{I}} \cap \mathrm{N}_F^-.$$

By Remark 3.6, the subspace $\widetilde{\mathrm{H}}_{\mathbf{k}}(\mathrm{M}_F)^-$ of $\widetilde{\mathrm{H}}_{\mathbf{k}}(\mathrm{M}_F)$ generated over $\mathbf{k}$ by τ_w^F for F-negative $w \in \widetilde{\mathrm{W}}_F$ is identified with a sub-$\mathbf{k}$-algebra of $\widetilde{\mathrm{H}}_{\mathbf{k}}$ via the injection

$$j_F^- : \widetilde{\mathrm{H}}_{\mathbf{k}}(\mathrm{M}_F)^- \longrightarrow \widetilde{\mathrm{H}}_{\mathbf{k}}, \quad \tau_w^F \longmapsto \tau_w.$$

This endows $\widetilde{\mathrm{H}}_k$ with the structure of left module over $\widetilde{\mathrm{H}}_{\mathbf{k}}(\mathrm{M}_F)^-$.

Proposition 5.17. *Let* $(\sigma, \mathrm{V}_\sigma)$ *be a smooth* $\mathbf{k}$*-representation of* M_F*. Consider the parabolic induction* $\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma$ *and its* $\tilde{\mathrm{I}}$*-invariant subspace* $(\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}}$*. There is a surjective morphism of right* $\widetilde{\mathrm{H}}_{\mathbf{k}}$*-modules*

$$\sigma^{\tilde{\mathrm{I}}_F^0} \otimes_{\widetilde{\mathrm{H}}_{\mathbf{k}}(\mathrm{M}_F)^-} \widetilde{\mathrm{H}}_{\mathbf{k}} \longrightarrow (\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}} \tag{5-4}$$

sending $v \otimes 1$ *to the unique* $\tilde{\mathrm{I}}$*-invariant function with support in* $\mathrm{P}_F\tilde{\mathrm{I}}$ *and value* v *at* 1_{G}.

Remark 5.18. In the cases $\mathbf{G} = \mathrm{PGL}_n$ or GL_n, Proposition 5.2 in [Ollivier 2010] implies that (5-4) is an isomorphism. This result should be true for a general (split) $\mathbf{G}$, but we will only use the surjectivity here.

The proposition follows from the discussion below. All the lemmas are proved in the next section.

Lemma 5.19. *Let* $\mathcal{D}_F = \{d \in \mathfrak{W} : d^{-1}\Phi_F^+ \subseteq \Phi^+\}$.

(i) *For* $d \in \mathcal{D}_F$, *we have* $\mathrm{P}_F \tilde{\mathrm{I}}\, \hat{d}\, \tilde{\mathrm{I}} = \mathrm{P}_F \hat{d}\, \tilde{\mathrm{I}}$.

(ii) *The set of all* $\hat{d} \in \mathrm{G}$ *for* $d \in \mathcal{D}_F$ *is a system of representatives of the double cosets* $\mathrm{P}_F \backslash \mathrm{G} / \tilde{\mathrm{I}}$.

(iii) *For* $d \in \mathcal{D}_F$, *let* $\tilde{\mathrm{I}}\, \hat{d}\, \tilde{\mathrm{I}} = \bigsqcup_y \tilde{\mathrm{I}}\, \hat{d}\, y$ *be a decomposition into right cosets. Then*

$$\mathrm{P}_F \hat{d}\, \tilde{\mathrm{I}} = \bigsqcup_y \mathrm{P}_F \tilde{\mathrm{I}}\, \hat{d}\, y.$$

(iv) *Let* $d \in \mathcal{D}_F$. *Under the projection* $\mathrm{P}_F \twoheadrightarrow \mathrm{M}_F$, *the image of* $\mathrm{P}_F \cap \hat{d}\tilde{\mathrm{I}}\hat{d}^{-1}$ *is* $\tilde{\mathrm{I}}_F^0$.

An element $m \in \mathrm{M}_F$ contracts $\tilde{\mathrm{I}}_F^+$ and dilates $\tilde{\mathrm{I}}_F^-$ if it satisfies the conditions

$$m\tilde{\mathrm{I}}_F^+ m^{-1} \subseteq \tilde{\mathrm{I}}_F^+, \quad m^{-1}\tilde{\mathrm{I}}_F^- m \subseteq \tilde{\mathrm{I}}_F^- \tag{5-5}$$

(see [Bushnell and Kutzko 1998, (6.5)]).

Remark 5.20. This property of an element $m \in \mathrm{M}_F$ only depends on the double coset $\tilde{\mathrm{I}}_F^0 m \tilde{\mathrm{I}}_F^0$. Furthermore, if $m \in \mathrm{K} \cap \mathrm{M}_F$ then $m\tilde{\mathrm{I}}_F^+ m^{-1} = \tilde{\mathrm{I}}_F^+$ and $m^{-1}\tilde{\mathrm{I}}_F^- m = \tilde{\mathrm{I}}_F^-$.

Lemma 5.21. *Let* $w \in \widetilde{\mathrm{W}}_F$. *The element* $\hat{w}$ *satisfies* (5-5) *if and only if* w *is* F*-negative.*

Let $(\sigma, \mathrm{V}_\sigma)$ be as in the proposition. Let $v \in \mathrm{V}_\sigma^{\tilde{\mathrm{I}}_F^0}$ and $d \in \mathcal{D}_F$. By (ii) and (iv) of Lemma 5.19, the $\tilde{\mathrm{I}}$-invariant function

$$f_{d,v} \in (\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}}$$

with support in $\mathrm{P}_F \hat{d}\, \tilde{\mathrm{I}}$ and value v at $\hat{d}$ is well defined, and the set of all $f_{d,v}$ form a basis of $(\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}}$, where d ranges over $\mathcal{D}_F$ and v over a basis of $\mathrm{V}_\sigma^{\tilde{\mathrm{I}}_F^0}$.

Lemma 5.22. (i) *If* w *is an* F*-negative element in* $\widetilde{\mathrm{W}}_F$, *then* $f_{1,v}.\tau_w = f_{1,v.\tau_w^F}$.

(ii) *We have* $f_{1,v}.\tau_{\hat{d}} = f_{d,v}$.

5E2. *Proof of the lemmas.* Recall that given $\alpha \in \Phi$, the root subgroup $\mathcal{U}_\alpha$ is endowed with a filtration $\mathcal{U}_{(\alpha,k)}$ for $k \in \mathbb{Z}$ (see for example [Schneider and Stuhler 1997, Section I.1] or [Ollivier and Schneider 2012, Section 4.2]) and that the product map

$$\prod_{\alpha \in \Phi^-} \mathcal{U}_{(\alpha,1)} \times \mathrm{T}^1 \times \prod_{\alpha \in \Phi^+} \mathcal{U}_{(\alpha,0)} \xrightarrow{\sim} \tilde{\mathrm{I}} \tag{5-6}$$

induces a bijection, where the products on the left side are ordered in some arbitrary

chosen way [Schneider and Stuhler 1997, Proposition I.2.2]. The subgroup $\tilde{\mathrm{I}}_F^+$ of $\tilde{\mathrm{I}}$ is generated by the image of $\prod_{\alpha\in\Phi^+-\Phi_F^+}\mathcal{U}_{(\alpha,0)}$, while $\tilde{\mathrm{I}}_F^-$ is generated by that of $\prod_{\alpha\in\Phi^--\Phi_F^-}\mathcal{U}_{(\alpha,1)}$. The subgroup $\tilde{\mathrm{I}}_F^0$ is generated by the image of

$$\prod_{\alpha\in\Phi_F^-}\mathcal{U}_{(\alpha,1)}\times\mathrm{T}^1\times\prod_{\alpha\in\Phi_F^+}\mathcal{U}_{(\alpha,0)}.$$

Proof of Lemma 5.19. (i) We have $\mathrm{P}_F\tilde{\mathrm{I}}\,\hat{d}\tilde{\mathrm{I}}=\mathrm{P}_F\tilde{\mathrm{I}}_F^-\hat{d}\tilde{\mathrm{I}}$. But for $\alpha\in\Phi^+$, we have $\hat{d}^{-1}\mathcal{U}_{(-\alpha,1)}\hat{d}=\mathcal{U}_{(-d^{-1}\alpha,1)}\subseteq\tilde{\mathrm{I}}$, so $\tilde{\mathrm{I}}_F^-\hat{d}\subseteq\hat{d}\tilde{\mathrm{I}}$ and $\mathrm{P}_F\tilde{\mathrm{I}}\,\hat{d}\tilde{\mathrm{I}}=\mathrm{P}_F\hat{d}\tilde{\mathrm{I}}$. Point (ii) follows by Bruhat decomposition for K and Iwasawa decomposition for G. For (iii), we first recall that the image of $\mathrm{P}_F\cap\mathrm{K}$ under the reduction $\mathrm{red}\,\mathrm{K}\to\bar{\mathbf{G}}_{x_0}(\mathbb{F}_q)$ modulo K_1 is a parabolic subgroup $\bar{\mathbf{P}}_F(\mathbb{F}_q)$ containing $\bar{\mathbf{B}}(\mathbb{F}_q)$ (notation in Section 1B).

Recall that the Weyl group of $\bar{\mathbf{G}}_{x_0}(\mathbb{F}_q)$ is $\mathfrak{W}$; for $w\in\mathfrak{W}$ we will still denote by w a chosen lift in $\bar{\mathbf{G}}_{x_0}(\mathbb{F}_q)$. The set $\mathcal{D}_F$ is a system of representatives of $\bar{\mathbf{P}}_F(\mathbb{F}_q)\backslash\bar{\mathbf{G}}_{x_0}(\mathbb{F}_q)/\bar{\mathbf{N}}(\mathbb{F}_q)$. For $d\in\mathcal{D}_F$ we have, using [Carter 1985, 2.5.12],

$$\bar{\mathbf{P}}_F(\mathbb{F}_q)\cap d\bar{\mathbf{N}}(\mathbb{F}_q)d^{-1}\subset\bar{\mathbf{N}}(\mathbb{F}_q).$$

We deduce that the image of $\mathrm{P}_F\cap\tilde{\mathrm{I}}_F^-\hat{d}\tilde{\mathrm{I}}\,\hat{d}^{-1}$ by red is contained in $\bar{\mathbf{N}}(\mathbb{F}_q)$ and therefore $\mathrm{P}_F\cap\tilde{\mathrm{I}}_F^-\hat{d}\tilde{\mathrm{I}}\,\hat{d}^{-1}$ is contained in $\tilde{\mathrm{I}}$.

Now let $d\in\mathcal{D}_F$ and $y\in\tilde{\mathrm{I}}$. By the previous observations, $\hat{d}\in\mathrm{P}_F\tilde{\mathrm{I}}\hat{d}\,y=\mathrm{P}_F\tilde{\mathrm{I}}_F^-\hat{d}\,y$ implies $\hat{d}\in\tilde{\mathrm{I}}\,\hat{d}\,y$. This proves (iii). In passing we proved that $\mathrm{P}_F\cap\hat{d}\tilde{\mathrm{I}}\,\hat{d}^{-1}$ is contained in $\mathrm{P}_F\cap\tilde{\mathrm{I}}=\tilde{\mathrm{I}}_F^0\tilde{\mathrm{I}}_F^+$. Since $\tilde{\mathrm{I}}_F^0$ is contained in $\mathrm{P}_F\cap\hat{d}\tilde{\mathrm{I}}\,\hat{d}^{-1}$ by definition of $\mathcal{D}_F$, this proves (iv). □

Proof of Lemma 5.21. By Remark 5.20, it is enough to prove the result for $w=e^\lambda\in\mathrm{X}_*(\mathrm{T})$. A lift for e^λ is given by $\lambda(\varpi^{-1})$. The element $\lambda(\varpi^{-1})$ satisfies (5-5) if

$$\begin{aligned}\text{for all }\alpha\in\Phi^+-\Phi_F^+\text{ we have }&\lambda(\varpi^{-1})\,\mathcal{U}_{(\alpha,0)}\lambda(\varpi)\subseteq\tilde{\mathrm{I}}_F^+\\ &\text{and }\lambda(\varpi)\mathcal{U}_{(-\alpha,1)}\lambda(\varpi^{-1})\subseteq\tilde{\mathrm{I}}_F^-.\end{aligned}\tag{5-7}$$

By [Ollivier and Schneider 2012, Remark 4.1(1)] for example,

$$\lambda(\varpi^{-1})\mathcal{U}_{(\alpha,0)}\lambda(\varpi)=\mathcal{U}_{(\alpha,-\langle\alpha,\lambda\rangle)}\quad\text{and}\quad\lambda(\varpi)\mathcal{U}_{(-\alpha,1)}\lambda(\varpi^{-1})=\mathcal{U}_{(-\alpha,1-\langle\alpha,\lambda\rangle)}.$$

Condition (5-7) is satisfied if and only if λ is F-negative (definition in Section 3C1). □

Proof of Lemma 5.22. (i) Let w be an F-negative element in $\tilde{\mathrm{W}}_F$. The function $f_{1,v}.\tau_w$ has support in $\mathrm{P}_F\tilde{\mathrm{I}}_F^-\hat{w}\tilde{\mathrm{I}}$. Since $\hat{w}$ satisfies (5-5), we have $\mathrm{P}_F\tilde{\mathrm{I}}_F^-\hat{w}\tilde{\mathrm{I}}=\mathrm{P}_F\hat{w}\tilde{\mathrm{I}}=\mathrm{P}_F\tilde{\mathrm{I}}$. It remains to compute the value of $f_{1,v}.\tau_w$ at 1_G (we choose the unit element 1_G of G as a lift for $1\in\mathcal{D}_F$). The proof goes through exactly as in [Ollivier 2010, Section 6A.3], where it is written up in the case of $\mathbf{G}=\mathrm{GL}_n$.

(ii) Let $d \in \mathcal{D}_F$. By Lemma 5.19(i), the $\tilde{\mathrm{I}}$-invariant function $f_{1,v} \,.\, \tau_d$ has support in $\mathrm{P}_F \hat{d} \tilde{\mathrm{I}}$, and it follows from Lemma 5.19(iii) that it takes value v at $\hat{d}$. □

5E3. Here we consider again representations with coefficients in an algebraically closed field k with characteristic p. We draw corollaries from Proposition 5.17.

Corollary 5.23. *Let $F \neq x_0$ be a standard facet. If σ is an admissible k-representation of M_F with a central character, then $(\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}}$ is a finite-dimensional $\tilde{\mathrm{H}}_k$-module whose irreducible subquotients are not supersingular.*

Proof. That $(\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}}$ is finite-dimensional is a consequence of the admissibility of σ. Let $\lambda \in \mathrm{X}_*(\mathrm{T})$ be a strongly F-negative coweight (see Remark 3.6) and $\lambda_0 \in \mathrm{X}_*^+(\mathrm{T})$ the unique dominant coweight in its $\mathfrak{W}$-orbit $\mathbb{O}(\lambda)$. By Lemma 3.4,

$$z_{\lambda_0} = \sum_{\lambda' \in \mathbb{O}(\lambda)} \mathcal{B}_F^-(\lambda').$$

We compute the action of z_{λ_0} on an element of the form $v \otimes 1 \in \sigma^{\tilde{\mathrm{I}}_F^0} \otimes_{\tilde{\mathrm{H}}_k(\mathrm{M}_F)^-} \tilde{\mathrm{H}}_k$. We have $\mathcal{B}_F^-(\lambda) = \tau_{e^\lambda}$ and therefore

$$(v \otimes 1)\mathcal{B}_F^-(\lambda) = v \otimes \tau_{e^\lambda} = v \otimes j_F^-(\tau_{e^\lambda}^F) = (v\tau_{e^\lambda}^F) \otimes 1.$$

Recall that $\tau_{e^\lambda}^F = \tau_{\lambda(\varpi^{-1})}^F$ and that $\lambda(\varpi^{-1})$ is a central element in M_F. Therefore, $v\tau_{e^\lambda}^F = \omega(\lambda(\varpi))v$, where ω denotes the central character of σ. By (2-4), this implies in particular that $(v \otimes 1)\mathcal{B}_F^-(\lambda') = 0$ for $\lambda' \in \mathbb{O}(\lambda)$ distinct from λ. We have proved that z_{λ_0} acts by multiplication by $\omega(\lambda(\varpi)) \neq 0$ on $\sigma^{\tilde{\mathrm{I}}_F^0} \otimes_{\tilde{\mathrm{H}}_k(\mathrm{M}_F)^-} \tilde{\mathrm{H}}_k$, and therefore on $(\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} \sigma)^{\tilde{\mathrm{I}}}$ by Proposition 5.17. This proves the claim. □

Corollary 5.24. *Let F be a standard facet. Let Sp_F be the generalized special k-representation of* G

$$\mathrm{Sp}_F = \frac{\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} 1}{\sum_{F' \neq F \subset \overline{F}} \mathrm{Ind}_{\mathrm{P}_{F'}}^{\mathrm{G}} 1},$$

where F' ranges over the set of standard facets $\neq F$ contained in the closure of F. The $\tilde{\mathrm{I}}$-invariant subspace of Sp_F is a finite-dimensional $\tilde{\mathrm{H}}_k$-module whose irreducible subquotients are not supersingular.

Proof. Suppose first that $F \neq x_0$. By [Große-Klönne 2013b, (18)] (which is valid with no restriction on the split group G), $(\mathrm{Sp}_F)^{\tilde{\mathrm{I}}}$ is a quotient of $(\mathrm{Ind}_{\mathrm{P}_F}^{\mathrm{G}} 1)^{\tilde{\mathrm{I}}}$. Apply Corollary 5.23. If $F = x_0$, then the special representation in question is the trivial character of G, whose $\tilde{\mathrm{I}}$-invariant subspace is isomorphic to the trivial character of $\tilde{\mathrm{H}}_k$ and is not supersingular (see the example in Section 5D2 and Lemma 5.12). □

5F. ***On supersingular representations.*** Let ρ be a weight of K. By (4-7), there is a correspondence between the k-characters of $\mathscr{H}(\mathrm{G},\rho)$ and the k-characters of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$, and we will use the letter ζ for each of the two characters paired up by (4-7). With this notation, by the work in Section 4 we have a surjective morphism of representations of G:

$$\zeta \otimes_{\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)} \mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1 \longrightarrow \zeta \otimes_{\mathscr{H}(\mathrm{G},\rho)} \mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho. \tag{5-8}$$

For ω a character of the connected center of G, let ζ_ω the supersingular character of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ as in Section 5C3. We remark that the representation $\zeta_\omega \otimes_{\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)} \mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1$ of G has central character ω.

From now on we suppose that the derived group of G is simply connected and that $\mathfrak{F}$ is a finite extension of $\mathbb{Q}_p$.

Lemma 5.25. *A character $\mathscr{H}(\mathrm{G},\rho) \to k$ is parametrized by the pair (G,ω) in the sense of* [Herzig 2011a, Proposition 4.1] *if and only if it corresponds to the supersingular character ζ_ω of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$ via* (4-7)*.*

Proof. In this proof we denote by $\psi : \mathscr{H}(\mathrm{G},\rho) \to k$ and $\zeta : \mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k) \to k$ a pair of characters corresponding to each other by (4-7). Recall that $\mathcal{T}$ denotes the inverse Satake isomorphism (4-4). By [ibid., Corollary 4.2] (see also Corollary 2.19 there), the character $\psi : \mathscr{H}(\mathrm{G},\rho) \to k$ is parametrized by the pair (G,ω) if and only if $\psi \circ \mathcal{T}(\lambda) = 0$ for all $\lambda \in \mathrm{X}_*^+(\mathrm{T})$ such that $\ell(e^\lambda) \neq 0$ and if $\psi \otimes_{\mathscr{H}(\mathrm{G},\rho)} \mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho$ has central character equal to ω (see Lemma 4.4 and its proof there). Since for all $\lambda \in \mathrm{X}_*^+(\mathrm{T})$ we have $\zeta(z_\lambda) = \psi \circ \mathcal{T}(\lambda)$ and since $\psi \otimes_{\mathscr{H}(\mathrm{G},\rho)} \mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho$ is a quotient of $\zeta \otimes_{\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)} \mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1$, we have proved (using the remark before the statement of this lemma) that ψ is parametrized by the pair (G,ω) if and only if $\zeta = \zeta_\omega$. □

A smooth irreducible admissible k-representation of G has a central character. A smooth irreducible admissible k-representation π with central character $\omega : Z \to k^\times$ is called supersingular with respect to $(\mathrm{K},\mathrm{T},\mathrm{B})$ [ibid., Definition 4.7] if for all weights ρ of K, any map $\mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho \to \pi$ factors through

$$\zeta_\omega \otimes_{\mathscr{H}(\mathrm{G},\rho)} \mathrm{ind}_{\mathrm{K}}^{\mathrm{G}} \rho \longrightarrow \pi.$$

Note that if the first map is zero, then the condition is trivial. By (5-8), a supersingular representation with central character $\omega : Z \to k^\times$ is therefore a quotient of $\zeta_\omega \otimes_{\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)} \mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1$ and, by Definition 5.8, of

$$\mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1 \,/\, \mathcal{I}\, \mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1.$$

Remark 5.26. (i) The representation $\mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1 \,/\, \mathcal{I}\, \mathrm{ind}_{\widetilde{\mathrm{I}}}^{\mathrm{G}} 1$ depends only on the conjugacy class of x_0. It is independent of any choices if $\mathbf{G}$ is of adjoint type or $\mathbf{G} = \mathrm{GL}_n$.

(ii) An irreducible admissible representation π of G is a quotient of $\mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1 / \mathfrak{I}\,\mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1$ if and only if $\pi^{\tilde{\mathrm{I}}}$ contains a supersingular $\widetilde{\mathrm{H}}_k$-module. Recall that when the root system of G is irreducible, we have proved that the notion of supersingularity for $\widetilde{\mathrm{H}}_k$-modules is independent of all the choices made.

Theorem 5.27. *If* $\mathrm{G} = \mathrm{GL}_n(\mathfrak{F})$ *or* $\mathrm{PGL}_n(\mathfrak{F})$, *a smooth irreducible admissible* k*-representation* π *is supersingular if and only if* $\pi^{\tilde{\mathrm{I}}}$ *contains a supersingular* $\widetilde{\mathrm{H}}_k$*-module*; *that is to say*, *if and only if* π *is a quotient of*

$$\mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1 / \mathfrak{I}\,\mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1. \tag{5-9}$$

Proof. Let π be a smooth irreducible admissible k-representation of G with central character ω. If it is a quotient of $\mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1 / \mathfrak{I}\,\mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1$, then it is a quotient of $\zeta_\omega \otimes_{\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)} \mathrm{ind}_{\tilde{\mathrm{I}}}^{\mathrm{G}} 1$, and $\pi^{\tilde{\mathrm{I}}}$ contains the supersingular character ζ_ω of $\mathscr{Z}^\circ(\widetilde{\mathrm{H}}_k)$. Therefore it contains a supersingular $\widetilde{\mathrm{H}}_k$-module. By Corollaries 5.23 and 5.24, this implies that π is neither a representation induced from a strict parabolic subgroup of G nor (a twist by a character of G of) a generalized special representation. By [Herzig 2011a, Theorem 1.1], which classifies all smooth irreducible admissible k-representation of G, we conclude by elimination that the representation π is supersingular. □

The results of [Herzig 2011a] have been generalized to the case of an $\mathfrak{F}$-split connected reductive group G in [Abe 2013]: the classification of the smooth irreducible admissible representations of G is quite similar to the case of $\mathrm{GL}_n(\mathfrak{F})$ (expect for a certain subtlety when the root system of G is not irreducible). Based on this classification and on Corollaries 5.23 and 5.24, N. Abe confirmed that the space of $\tilde{\mathrm{I}}$-invariant vectors of a nonsupersingular representation does not contain any supersingular $\widetilde{\mathrm{H}}_k$-module. Therefore, Theorem 5.27 is true for a general split group with simply connected derived subgroup.

References

[Abe 2013] N. Abe, "On a classification of irreducible admissible modulo p representations of a p-adic split reductive group", *Compos. Math.* **149**:12 (2013), 2139–2168. MR 3143708 Zbl 06250165 arXiv 1103.2525

[Barthel and Livné 1994] L. Barthel and R. Livné, "Irreducible modular representations of GL_2 of a local field", *Duke Math. J.* **75**:2 (1994), 261–292. MR 95g:22030 Zbl 0826.22019

[Bourbaki 1964] N. Bourbaki, Actualités Scientifiques et Industrielles **1308**, Hermann, Paris, 1964. Translated in *Commutative algebra: chapters* 1–7, Springer, 1989. MR 33 #2660 Zbl 0205.34302

[Bourbaki 1968] N. Bourbaki, *Groupes et algébres de Lie: chapitres 4 à 6*, Actualités Scientifiques et Industrielles **1337**, Hermann, Paris, 1968. Translated as *Lie groups and Lie algebras, chapters 4–6*, Springer, Berlin, 2002. French original reprinted by Springer, Berlin, 2007. MR 39 #1590 Zbl 0186.33001

[Bruhat and Tits 1972] F. Bruhat and J. Tits, "Groupes réductifs sur un corps local, I: Données radicielles valuées", *Inst. Hautes Études Sci. Publ. Math.* **41** (1972), 5–251. MR 48 #6265 Zbl 0254.14017

[Bruhat and Tits 1984] F. Bruhat and J. Tits, "Groupes réductifs sur un corps local, II: Schémas en groupes. Existence d'une donnée radicielle valuée", *Inst. Hautes Études Sci. Publ. Math.* **60** (1984), 5–184. MR 86c:20042 Zbl 0597.14041

[Bushnell and Kutzko 1998] C. J. Bushnell and P. C. Kutzko, "Smooth representations of reductive p-adic groups: structure theory via types", *Proc. London Math. Soc.* (3) **77**:3 (1998), 582–634. MR 2000c:22014 Zbl 0911.22014

[Carter 1985] R. W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley, New York, 1985. MR 87d:20060 Zbl 0567.20023

[Carter and Lusztig 1976] R. W. Carter and G. Lusztig, "Modular representations of finite groups of Lie type", *Proc. London Math. Soc.* (3) **32**:2 (1976), 347–384. MR 53 #592 Zbl 0338.20013

[Dat 1999] J.-F. Dat, "Caractères à valeurs dans le centre de Bernstein", *J. Reine Angew. Math.* **508** (1999), 61–83. MR 2000f:22021 Zbl 0938.22016

[Gross 1998] B. H. Gross, "On the Satake isomorphism", pp. 223–238 in *Galois representations in arithmetic algebraic geometry* (Durham, 1996), edited by A. J. Scholl and R. L. Taylor, London Math. Soc. Lecture Note Ser. **254**, Cambridge University Press, 1998. MR 2000e:22008 Zbl 0996.11038

[Große-Klönne 2013a] E. Große-Klönne, "From pro-p Iwahori–Hecke modules to (φ, Γ)-modules, I", preprint, 2013, http://www.math.hu-berlin.de/~zyska/Grosse-Kloenne/iwahecgal.pdf.

[Große-Klönne 2013b] E. Große-Klönne, "On special representations of p-adic reductive groups", preprint, 2013, http://www.math.hu-berlin.de/~zyska/Grosse-Kloenne/spec.pdf.

[Haines 2001] T. J. Haines, "The combinatorics of Bernstein functions", *Trans. Amer. Math. Soc.* **353**:3 (2001), 1251–1278. MR 2002j:20012 Zbl 0962.14018

[Haines and Pettet 2002] T. J. Haines and A. Pettet, "Formulae relating the Bernstein and Iwahori–Matsumoto presentations of an affine Hecke algebra", *J. Algebra* **252**:1 (2002), 127–149. MR 2003f:20012 Zbl 1056.20003

[Herzig 2011a] F. Herzig, "The classification of irreducible admissible mod p representations of a p-adic GL_n", *Invent. Math.* **186**:2 (2011), 373–434. MR 2845621 Zbl 1235.22030

[Herzig 2011b] F. Herzig, "A Satake isomorphism in characteristic p", *Compos. Math.* **147**:1 (2011), 263–283. MR 2012c:22020 Zbl 1214.22004

[Kempf et al. 1973] G. Kempf, F. Knudsen, D. Mumford, and B. Saint-Donat, *Toroidal embeddings, I*, Lecture Notes in Math. **339**, Springer, Berlin, 1973. MR 49 #299 Zbl 0271.14017

[Koziol 2013] K. Koziol, "Restriction of pro-p-Iwahori–Hecke modules", preprint, 2013. arXiv 1308.6239

[Lusztig 1983] G. Lusztig, "Singularities, character formulas, and a q-analog of weight multiplicities", pp. 208–229 in *Analyse et topologie sur les espaces singuliers, II, III* (Luminy, 1981), edited by A. A. Beilinson et al., Astérisque **101**, Soc. Math. France, Paris, 1983. MR 85m:17005 Zbl 0561.22013

[Lusztig 1989] G. Lusztig, "Affine Hecke algebras and their graded version", *J. Amer. Math. Soc.* **2**:3 (1989), 599–635. MR 90e:16049 Zbl 0715.22020

[Ollivier 2010] R. Ollivier, "Parabolic induction and Hecke modules in characteristic p for p-adic GL_n", *Algebra Number Theory* **4**:6 (2010), 701–742. MR 2012c:20007 Zbl 1243.22017

[Ollivier 2012] R. Ollivier, "An inverse Satake isomorphism in characteristic p", preprint, 2012. arXiv 1207.5557

[Ollivier and Schneider 2012] R. Ollivier and P. Schneider, "Pro-p Iwahori–Hecke algebras are Gorenstein", preprint, 2012. arXiv 1207.3769

[Satake 1963] I. Satake, "Theory of spherical functions on reductive algebraic groups over p-adic fields", *Inst. Hautes Études Sci. Publ. Math.* **18** (1963), 5–69. MR 33 #4059 Zbl 0122.28501

[Sawada 1977] H. Sawada, "A characterization of the modular representations of finite groups with split (B, N)-pairs", *Math. Z.* **155**:1 (1977), 29–41. MR 56 #8679 Zbl 0345.20009

[Schmidt 2009] N. A. Schmidt, *Generische pro-p Hecke-Algebren*, thesis, Humboldt University, Berlin, 2009, http://www2.mathematik.hu-berlin.de/~schmidtn/hecke.pdf.

[Schneider and Stuhler 1997] P. Schneider and U. Stuhler, "Representation theory and sheaves on the Bruhat–Tits building", *Inst. Hautes Études Sci. Publ. Math.* **85** (1997), 97–191. MR 98m:22023 Zbl 0892.22012

[Tits 1979] J. Tits, "Reductive groups over local fields", pp. 29–69 in *Automorphic forms, representations and L-functions, Part 1* (Corvallis, OR, 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979. MR 80h:20064 Zbl 0415.20035

[Vignéras 2005] M.-F. Vignéras, "Pro-p-Iwahori Hecke ring and supersingular $\overline{\mathbf{F}}_p$-representations", *Math. Ann.* **331**:3 (2005), 523–556. [Erratum at ibid. **333**:3 (2005), 699–701]. MR 2005m:22020 Zbl 1107.22011

[Vignéras 2006] M.-F. Vignéras, "Algèbres de Hecke affines génériques", *Represent. Theory* **10** (2006), 1–20. MR 2006i:20005 Zbl 1134.22014

[Vignéras 2007] M.-F. Vignéras, "Représentations irréductibles de GL(2, F) modulo p", pp. 548–563 in *L-functions and Galois representations*, edited by D. Burns et al., London Math. Soc. Lecture Note Ser. **320**, Cambridge University Press, 2007. MR 2009h:11084 Zbl 1172.11017

Communicated by Marie-France Vignéras
Received 2013-04-25 Revised 2013-12-27 Accepted 2014-02-27

ollivier@math.columbia.edu *Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027, United States*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1113

The final log canonical model of $\overline{\mathcal{M}}_6$

Fabian Müller

We describe the birational model of $\overline{\mathcal{M}}_6$ given by quadric hyperplane sections of the degree-5 del Pezzo surface. In the spirit of the genus-4 case treated by Fedorchuk, we show that it is the last nontrivial space in the log minimal model program for $\overline{\mathcal{M}}_6$. We also obtain a new upper bound for the moving slope of the moduli space.

1. Introduction

A general smooth curve C of genus 6 has five planar sextic models with four nodes in general linear position. Blowing up these four points and embedding the resulting surface in $\mathbb{P}^5$ via its complete anticanonical linear series, one finds that the canonical model of C is a quadric hyperplane section of a degree-5 del Pezzo surface S. As any four general points in $\mathbb{P}^2$ are projectively equivalent, this surface is unique up to isomorphism. Its automorphism group is finite and isomorphic to the symmetric group S_5 (see, e.g., [Shepherd-Barron 1989]). The surface S contains ten (-1)-curves, which are the four exceptional divisors of the blowup, together with the proper transforms of the six lines through pairs of the points. There are five ways of choosing four nonintersecting (-1)-curves on S, inducing five blowdown maps $S \to \mathbb{P}^2$, and restricting to the five g^2_6's on C. Residual to the latter are five g^1_4's, which can be seen in each planar model as the projection maps from the four nodes, together with the map that is induced on C by the linear system of conics passing through the nodes.

This description gives rise to a birational map

$$\varphi : \overline{\mathcal{M}}_6 \dashrightarrow X_6 := |-2K_S|/\mathrm{Aut}(S),$$

which is well defined and injective on the sublocus $(\mathcal{M}_6 \cup \Delta_0^{\mathrm{irr}}) \setminus \overline{\mathcal{GP}}_6$. Here Δ_0^{irr} denotes the locus of irreducible singular stable curves, and $\overline{\mathcal{GP}}_6$ is the closure of the Gieseker–Petri divisor of curves having fewer than five g^1_4's (or residually, g^2_6's). These have planar sextic models in which the nodes fail to be in general linear position, which forces the anticanonical image of the blown-up $\mathbb{P}^2$ to become

MSC2010: primary 14H10; secondary 14E30, 14H45.
Keywords: moduli space of curves, genus 6, log canonical model, moving slope.

singular. In the generic case, exactly three of the nodes become collinear, and the line through them is a (-2)-curve that gets contracted to an A_1 singularity. The class of the Gieseker–Petri divisor is computed in [Eisenbud and Harris 1987b] as

$$\left[\overline{\mathcal{GP}}_6\right] = 94\lambda - 12\delta_0 - 50\delta_1 - 78\delta_2 - 88\delta_3.$$

It is an extremal effective divisor of minimal slope on $\overline{\mathcal{M}}_6$ [Chang and Ran 1991].

The aim of this article is to study the birational model X_6, determine its place within the log minimal model program of $\overline{\mathcal{M}}_6$, and use it to derive an upper bound on the moving slope of this space. In order to do so, we will start in Section 2 by determining explicitly the way in which φ extends to the generic points of the divisors Δ_i for $i = 1, 2, 3$ and of $\overline{\mathcal{GP}}_6$. The divisors Δ_1 and Δ_2 are shown to be contracted by 1 and 4 dimensions as the low-genus components are replaced by a cusp and an A_5 singularity, respectively. The image of Δ_3 is at most one-dimensional, and $\overline{\mathcal{GP}}_6$ turns out to be contracted to a point. The curves parametrized by the latter two are shown to be mapped to the classes of certain nonreduced degree-10 curves on S.

In Section 3, we will then construct test families along which φ is defined and determine their intersection numbers with the standard generators of $\mathrm{Pic}(\overline{\mathcal{M}}_6)$ as well as with $\varphi^*\mathcal{O}_{X_6}(1)$. Having enough of those enables us in Section 4 to finally compute the class of the latter. This computation is then used to establish the upper bound $s'(\overline{\mathcal{M}}_6) \leq \frac{102}{13}$ for the moving slope of $\overline{\mathcal{M}}_6$ as well as to show that the log canonical model $\overline{\mathcal{M}}_6(\alpha)$ is isomorphic to X_6 for $\frac{16}{47} < \alpha \leq \frac{35}{102}$ and becomes trivial below this point.

2. Defining φ in codimension 1

In this section, we will see how φ is defined on the generic points of the codimension-one subloci of $\overline{\mathcal{M}}_6$ parametrizing curves whose canonical image does not lie on S. As mentioned in the introduction, these are the divisors Δ_i, $i = 1, 2, 3$, as well as $\overline{\mathcal{GP}}_6$, and they will turn out to constitute exactly the exceptional locus of φ.

Proposition 2.1. *A curve $C = C_1 \cup_p C_2 \in \Delta_1$ with p not a Weierstraß point on $C_2 \in \mathcal{M}_5$ is mapped to the class of a cuspidal curve whose pointed normalization is $(C_2,\ p)$. In particular, the map φ contracts Δ_1 by one dimension.*

Proof. This follows readily from the existence of a moduli space for pseudostable curves [Schubert 1991]. More concretely, let $\pi : \mathcal{C} \to B$ be a flat family of genus-6 curves whose general fiber is smooth and Gieseker–Petri general and with special fiber C. Then the twisted linear system $|\omega_\pi(C_1)|$ maps $\mathcal{C}$ to a flat family of curves in $|-2K_S|$. It restricts to $\mathcal{O}_{C_1}$ on C_1 and to $\omega_{C_2}(2p)$ on C_2, so it contracts C_1 and maps C_2 to a cuspidal curve of arithmetic genus 6, which lies on a smooth del Pezzo surface. □

Proposition 2.2. *Let $C = C_1 \cup_p C_2 \in \Delta_2$ be a curve such that*

- *the component $C_2 \in \mathcal{M}_4$ is Gieseker–Petri general and*
- *p is not a Weierstraß point on either component.*

Then C is mapped to the class of a curve consisting of C_2 together with a line that is 3-tangent to it at p. In particular, the map φ restricted to Δ_2 has 4-dimensional fibers.

Proof. Let $\mathscr{C} \to B$ be a flat family of genus-6 curves whose general fiber is smooth and Gieseker–Petri general and with special fiber C. Blow up the hyperelliptic conjugate $\tilde{p} \in C_1$ of p, and let $\pi : \mathscr{C}' \to B$ be the resulting family with central fiber C' and exceptional divisor R. Then the twisted line bundle $\mathscr{L} := \omega_\pi(2C_1)$ restricts to $\omega_{C_2}(3p)$, $\mathbb{O}_{C_1}$, and $\mathbb{O}_R(1)$ on the respective components of C'. By a detailed analysis, one can see that the family of linear systems $(\mathscr{L}, \pi_*\omega_\pi)$ restricts to $|\omega_{C_2}(3p)|$ on C_2 and maps R to the 3-tangent line at p while contracting C_1. A similar but harder analysis of this kind is carried out in Lemma 2.5 for the case of Δ_3, to which we refer.

In order to see that the central fiber lies on S as a section of $-2K_S$, it suffices to observe that a generic pointed curve $(C_2, p) \in \mathcal{M}_{4,1}$ has three quintic planar models with a flex at p. Each such model has two nodes, projecting from which gives the two g^1_3's. The 3-tangent line R at p meets C_2 at two other points, so $C_2 \cup R$ is a plane curve of degree 6 with four nodes (and an A_5 singularity). Blowing up the four nodes, which for generic (C_2, p) will be in general linear position, gives the claim.

For showing that the flat limit is unique, it suffices by [Fedorchuk 2012, Lemma 3.10] to show that, if C' is any curve in a small punctured neighborhood of $R \cup_p C_2$ inside $|-2K_S|$, then C is not the stable reduction of C' in any family in which it occurs as the central fiber. If C' is smooth, this is obviously satisfied, so assume it is still singular. If C' retains an A_5 singularity, then its genus-4 component must be different from (C_2, p) since C_2 has only a finite number of g^2_5's with a flex at p. Thus, its stable reduction cannot be isomorphic to C. If on the other hand the type of singularity changes, it can only become an A_k singularity with $1 \le k \le 4$. In case $k \le 3$, any irreducible component arising in the stable reduction has genus at most 1 while for $k = 4$ the stable tail is always a genus-2 curve attached at a Weierstraß point [Hassett 2000, Section 6]. Thus, the stable reduction cannot be isomorphic to C in these cases either. □

Proposition 2.3. *Let $C = C_1 \cup_p C_2 \in \Delta_3$ be a curve such that, on both components,*

- *p is not a Weierstraß point and*
- *p is not in the support of any odd theta characteristic (in particular, neither component is hyperelliptic).*

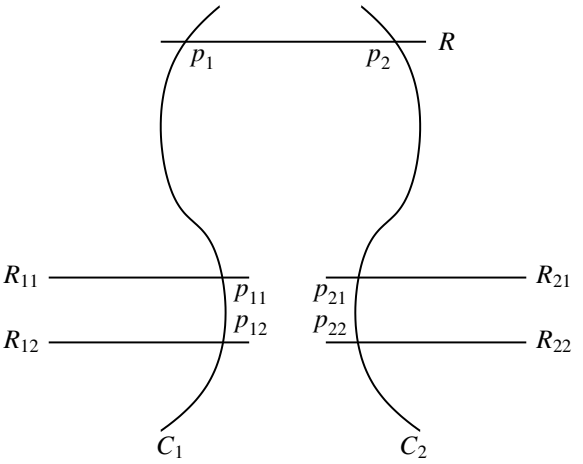


Figure 1. The central curve C'.

Then C is mapped to the class of two times a twisted cubic on S together with two (possibly reducible) conics meeting it tangentially. In particular, the image of Δ_3 under φ is at most 1-dimensional.

Proof. Let $\mathscr{C} \to B$ be a flat family of genus-6 curves whose general fiber is smooth and Gieseker–Petri general and with special fiber C. By assumption, the two base points of $|\omega_{C_i}(-2p)|$ are distinct from each other and from p for $i = 1, 2$. Blow up the total space $\mathscr{C}$ at p and at these four base points. Let $\pi : \mathscr{C}' \to B$ denote the resulting family with central fiber $C' = C_1 + C_2 + R + \sum R_{ij}$, where C_i are the proper transforms of the genus-3 components and R and R_{ij} are the exceptional divisors over p and the base points, respectively. For $i, j = 1, 2$, denote by p_{ij} the point of intersection of C_i with R_{ij} and by p_i the point of intersection of C_i with R (see Figure 1).

Consider the twisted sheaf $\mathscr{L} := \omega_\pi\big(3(C_1 + C_2) + \sum R_{ij}\big)$ on $\mathscr{C}'$. On the various components of C', it restricts to $\mathbb{O}_{C_i}$, $\mathbb{O}_R(6)$, and $\mathbb{O}_{R_{ij}}(1)$, respectively. The push-forward $\pi_*\mathscr{L}$ is not locally free (the central fiber has dimension 7 instead of 6), but it contains $\pi_*\omega_\pi$ as a locally free rank-6 subsheaf. The central fiber V of the image of this sheaf in $\pi_*\mathscr{L}$ is described in Lemma 2.5. The induced linear system $(\mathscr{L}|_{C'}, V)$ maps C' to the curve $C'' = R + 2R_1 + 2R_2 \subseteq \mathbb{P}^5$, which consists of the middle rational component R embedded as a degree-6 curve together with twice the tangent lines R_1 and R_2 at p_1 and p_2. The genus-3 components C_i are contracted to the points p_i. If one introduces coordinates $[x_0 : \cdots : x_5]$ in $\mathbb{P}^5$ corresponding to the basis of V given in Lemma 2.5, the image curve lies on the variety

$$\widetilde{S}_{2,3} = \bigcup_{[\lambda:\mu]\in\mathbb{P}^1} \overline{\varphi_1([\lambda : \mu])\varphi_2([\lambda : \mu])},$$

where

$$\varphi_1([\lambda:\mu]) := [\lambda^3 : 0 : \lambda^2\mu : \lambda\mu^2 : 0 : \mu^3],$$
$$\varphi_2([\lambda:\mu]) := [0 : \lambda^2 : 0 : 0 : \mu^2 : 0],$$

which is a projection of the rational normal scroll $S_{2,3} \subseteq \mathbb{P}^6$ from a point in the plane of the directrix. This surface is among the possible degenerations of the degree-5 del Pezzo surface investigated in [Coskun 2006, Proposition 3.2] and has the same Betti diagram. In equations, it is given by

$$\widetilde{S}_{2,3} = \left\{ \operatorname{rk} \begin{pmatrix} x_0 & x_1 & x_2 \\ x_3 & x_4 & x_5 \end{pmatrix} \le 1 \right\} \cap \left\{ \operatorname{rk} \begin{pmatrix} x_0 & x_2 & x_3 \\ x_2 & x_3 & x_5 \end{pmatrix} \le 1 \right\},$$

and C'' is a quadric section cut out for example by $x_1x_4 - x_0x_5$. When restricted to the directrix, the image of the projection is the line $\tilde{L} = \{x_0 = x_2 = x_3 = x_5 = 0\}$, which is the singular locus of $\widetilde{S}_{2,3}$. The two branch points q_i of this restriction are the intersection points of the double lines R_i with $\tilde{L}$.

The image of $\mathscr{C}'$ under the family of linear systems $(\mathscr{L}, \pi_*\omega_\pi)$ lies on a flat family of surfaces $\mathscr{S} \subseteq \mathbb{P}^5 \times B$ with general fiber S and special fiber $\widetilde{S}_{2,3}$. We will construct a birational modification of $\mathscr{S}$ whose central fiber is isomorphic to S. Let $\pi' : \mathscr{S}' \to B$ be the family obtained by blowing up $\tilde{L}$ and $S' \subseteq \mathscr{S}'$ the exceptional divisor. The proper transform of $\widetilde{S}_{2,3}$ in $\mathscr{S}'$ is $S_{2,3}$, and the intersection curve $L = S_{2,3} \cap S'$ is its directrix.

We want to show that $S' \cong S$. The ten (-1)-curves of the generic fiber cannot all specialize to points in the central limit since then the whole surface S would be contracted, contradicting flatness. Any exceptional curve that is not contracted must go to $\tilde{L}$ in the limit since it is the only curve on $\widetilde{S}_{2,3}$ having a normal sheaf of negative degree. By a chase around the intersection graph of the (-1)-curves on S, one can see that, if one of them is mapped dominantly to $\tilde{L}$, then at least four of them are. Since the graph is connected, the rest of them get mapped to points that lie on $\tilde{L}$. Using a base change ramified over 0 if necessary, we may assume that limits of noncontracted curves get separated in $\mathscr{S}'$ while the contracted ones are blown up to lines. Thus, there are ten distinct (-1)-curves on S', which by the list of possible limits in [Coskun 2006] forces it to be isomorphic to S (note that there are at most seven (-1)-curves on a singular degree-5 del Pezzo surface [Coray and Tsfasman 1988, Proposition 8.5]).

It remains to see what happens to the curve C'' in the process. Denote by $\psi : \mathscr{S}' \to \mathbb{P}^5 \times B$ the map induced by the family of linear systems $(\omega_{\pi'}^\vee(S_{2,3}), \pi'_*\omega_{\pi'}^\vee)$. This restricts to $-K_{S'}$ on S' and to a subsystem of $|3F|$ on $S_{2,3}$. Thus, the map ψ contracts the latter and has degree 3 on L. This implies that $\mathbb{O}_{S'}(L) = \rho^*\mathbb{O}_{\mathbb{P}^2}(1)$ for one of the five maps $\rho : S' \to \mathbb{P}^2$, and there are exactly four exceptional curves $E_1, \ldots, E_4 \subseteq S'$ that do not meet L. The blowdown fibration on S' is given

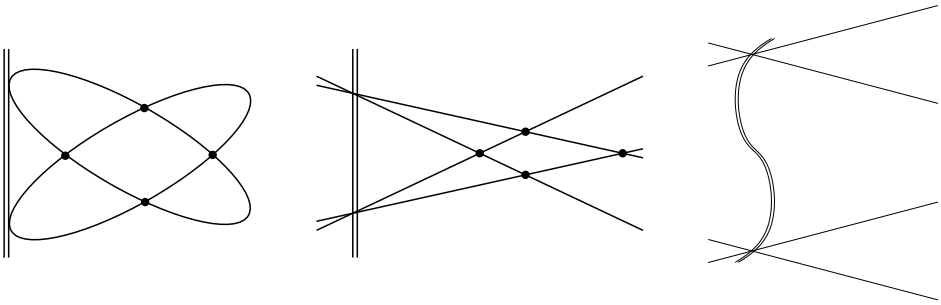


Figure 2. Two possibilities for the image of C under φ and the proper transform of the latter after blowing up the nodes.

by $\left|2L - \sum E_i\right|$, and it contains exactly 3 reducible conics. The flat pullback of C'' to $\mathcal{S}'$ contains the two conics in the fibration that meet L at the ramification points of the map $L \to \tilde{L}$, and the map ψ restricted to C'' contracts the two double lines R_i to the points q_i and maps R doubly onto L. Thus, the flat limit of C'' consists of twice the line L together with the two conics in the fibration which are tangent to L at the points q_i. Up to automorphisms, such a configuration has a 1-dimensional family of moduli, so the image of Δ_3 under φ is at most 1-dimensional. □

Remark 2.4. The image curve $\varphi(C)$ has two possible kinds of nonreduced planar singularities shown in Figure 2. The one on the left with local equation $y^2(y-x^2)=0$ appears in the proof of Proposition 2.3 in the curve C''. For the second one with equation $y^2(y^2-x^2)=0$, one can see directly using an appropriate family that it has the generic smooth genus 3 curve in its variety of stable tails. We will use this construction in the proof of Lemma 3.5.

Lemma 2.5. *Let $\mathscr{C}'$ and $\mathscr{L}$ be constructed as in the proof of Proposition 2.3, and let V be the central fiber of the image of $\pi_*\omega_\pi \hookrightarrow \pi_*\mathscr{L}$. Choose coordinates $[s:t]$ on each rational component such that on R_{1j} the coordinate t is centered at p_{1j}, on R_{2j} the coordinate s is centered at p_{2j} $(j=1,2)$, and on R the coordinate s is centered at p_1 and t at p_2. Then V is spanned by the following sections (on C_i the sections are constants and not listed in the table)*:

R_{11}	R_{12}	R	R_{21}	R_{22}
0	0	s^6	t	t
0	0	s^5t	s	s
0	0	s^4t^2	0	0
0	0	s^2t^4	0	0
t	t	st^5	0	0
s	s	t^6	0	0

Proof. Let $\ell_R = (\mathcal{L}_R, V_R)$ be the R-aspect of the unique limit canonical series on the central fiber of $\mathscr{C}'$. By [Eisenbud and Harris 1987a, Theorem 2.2], we have that

$$\mathcal{L}_R = \omega_\pi\big(5(C_1 + C_2) + 4\textstyle\sum R_{ij}\big)\big|_R = \mathbb{O}_R(10)$$

and ℓ_R has vanishing sequence $a^\ell_R(p_i) = (2, 3, 4, 6, 7, 8)$ at both p_i, so

$$V_R = s^2t^2\langle s^6, s^5t, s^4t^2, s^2t^4, st^5, t^6\rangle.$$

Since on R the inclusion $\mathcal{L}|_R \hookrightarrow \mathcal{L}_R$ restricts to $\mathbb{O}_R(6) \hookrightarrow \mathbb{O}_R(10)$, $\sigma \mapsto s^2t^2\sigma$, we have that $s^2t^2V|_R \subseteq V_R$. Since the dimensions match, the claim for the central column follows. By dimension considerations, it is clear that $\mathcal{L}$ must restrict to the complete linear series $|\mathbb{O}_{R_{ij}}(1)|$ on R_{ij}.

It remains to show that, if a section $\sigma \in V$ fulfills $\operatorname{ord}_{p_i}(\sigma|_R) \geq 2$, then $\sigma|_{R_{ij}} = 0$ for $j = 1, 2$. For this, let $\sigma_{C_i} \in H^0(C, \mathbb{O}_{\mathscr{C}'}(C_i)|_C)$ be the restriction of a generating section, and let $\varphi_i : H^0(C, \mathcal{L}(-C_i)|_C) \to H^0(C, \mathcal{L}|_C)$ be the map given by $\sigma \mapsto \sigma_{C_i} \cdot \sigma$. For a divisor D on $\mathscr{C}'$ and $k \in \mathbb{N}$, introduce the subspaces

$$V_{i,k}(D) := \big\{\sigma \in H^0(C, \mathcal{L} \otimes \mathbb{O}_{\mathscr{C}'}(D)|_C) \;\big|\; \operatorname{ord}_{p_i}(\sigma|_R) \geq k\big\},$$
$$V_{i,k} := V_{i,k}(0).$$

Since $\mathcal{L}|_{C_i} = \mathbb{O}_{C_i}$, we have that $\operatorname{im}(\varphi_i) = V_{i,1}$. Moreover, we certainly have the inclusion $\varphi_i(V_{i,1}(-C_i)) \subseteq V_{i,2}$ and

$$\begin{aligned}\operatorname{codim}(\varphi_i(V_{i,1}(-C_i)), V_{i,1}) &\leq \operatorname{codim}(V_{i,1}(-C_i), H^0(C, \mathcal{L}(-C_i)|_C)) \\ &\leq 1.\end{aligned}$$

From the description of the sections on R, it is apparent that $V_{i,2} \subsetneq V_{i,1}$, so we have in fact $\varphi_i(V_{i,1}(-C_i)) = V_{i,2}$. Thus, we get

$$\begin{aligned}V_{i,2} &= \varphi_i(V_{i,1}(-C_i)) \\ &= \varphi_i\big(\big\{\sigma \in H^0(C, \mathcal{L}(-C_i)|_C) \;\big|\; \sigma|_{R_{ij}} = 0 \text{ for } j = 1, 2\big\}\big) \\ &\subseteq \big\{\sigma \in H^0(C, \mathcal{L}|_C) \;\big|\; \sigma|_{R_{ij}} = 0 \text{ for } j = 1, 2\big\}.\end{aligned}$$

□

Proposition 2.6. *Let C be a smooth Gieseker–Petri special curve whose canonical image lies on a singular del Pezzo surface with a unique A_1 singularity but not passing through that singularity. Then φ maps C to a nonreduced degree-10 curve on S consisting of four times a line together with two times each of the three lines meeting it. In particular, φ contracts $\overline{\mathcal{GP}}_6$ to a point.*

Proof. This can be done by a geometric construction similar to [Fedorchuk 2012, Theorem 3.13]. Here we follow a simpler approach from [Jensen 2013]. A curve C as above has a planar sextic model with three collinear nodes, so the map $\mathcal{G}^1_4 \to \mathcal{M}_6$ is simply ramified over C. Thus, a neighborhood of the ramification point will map

a (double cover of a) neighborhood of C to a family of $(4,4)$-curves on $\mathbb{P}^1 \times \mathbb{P}^1$. The image of the general fiber will be an irreducible curve with three nodes while the special fiber goes to four times the diagonal. Blowing up the nodes gives a flat family on S with central fiber as described. □

Remark 2.7. A pencil of antibicanonical curves on a singular del Pezzo surface as above has slope $\frac{47}{6}$ like in the smooth case (for which see Lemma 3.1). This would seem to contradict the fact that φ contracts the Gieseker–Petri divisor, which has the same slope, to a point. However, any such pencil will contain a curve C having a node at the singular point. The normalization of such a curve is a trigonal curve of genus 5 since blowing up the node and blowing down four disjoint (-1)-curves gives a planar quintic model of C together with a line. Using this model, one can show that φ maps C to a configuration consisting of three times a line on S together with three lines and two conics meeting it. This arrangement obviously has moduli, so we deduce that φ is not defined on $\Delta_0^{\mathrm{trig}} := \{C \in \Delta_0 \mid C \text{ has a trigonal normalization}\}$, which is a component of $\Delta_0 \cap \overline{\mathcal{GP}}_6$.

3. Test families

In order to compute the class of $\varphi^* \mathbb{O}_{X_6}(1)$, we now construct some test families and record their intersection numbers with the standard generators of $\mathrm{Pic}(\overline{\mathcal{M}}_6)$ and with $\varphi^* \mathbb{O}_{X_6}(1)$. Those numbers not mentioned in the statements of the lemmas are implied to be 0.

Lemma 3.1. *A generic pencil T_1 of quadric hyperplane sections of S has intersection numbers*

$$T_1 \cdot \lambda = 6, \quad T_1 \cdot \delta_0 = 47, \quad T_1 \cdot \varphi^* \mathbb{O}_{X_6}(1) = 1.$$

Proof. Since all members of T_1 are irreducible, it suffices to show that $\varphi_* \lambda = \mathbb{O}_V(6)$ and $\varphi_* \delta = \mathbb{O}_V(47)$ on $V := |-2K_S| \cong \mathbb{P}^{15}$. This is completely parallel to the computation in [Fedorchuk 2012, Proposition 3.2]. If $Y := S \times V$ and $\mathscr{C} \subseteq Y$ denotes the universal curve, we have $\mathbb{O}_Y(\mathscr{C}) = \mathbb{O}_Y(-2K_S, 1)$, so by adjunction, $\omega_{\mathscr{C}/V} = \mathbb{O}_{\mathscr{C}}(-K_S, 1)$. Applying π_{2*} to the exact sequence

$$0 \to \mathbb{O}_Y(K_S, 0) \to \mathbb{O}_Y(-K_S, 1) \to \omega_{\mathscr{C}/V} \to 0,$$

we find that

$$\pi_{2*} \omega_{\mathscr{C}/V} \cong \pi_{2*} \mathbb{O}_Y(-K_S, 1) \cong H^0(S, -K_S) \otimes \mathbb{O}_V(1)$$

since $\pi_{2_*} \mathbb{O}_Y(K_S, 0) = R^1 \pi_{2*} \mathbb{O}_Y(K_S, 0) = 0$ by Kodaira vanishing. Therefore, we obtain that $\varphi_* \lambda = \det \pi_{2*} \omega_{\mathscr{C}/V} = \mathbb{O}_V(6)$.

We also find that

$$\varphi_* \kappa = \pi_{2*}(\omega_{\mathscr{C}/V}^2) = \pi_{2*}((-2K_S, 1) \cdot (-K_S, 1)^2) = \mathbb{O}_V(25),$$

and from $\kappa = 12\lambda - \delta$, we deduce that $\varphi_*\delta = \mathbb{O}_V(47)$. □

Lemma 3.2. *Let T_2 be the family obtained by attaching a fixed genus-5 curve to a base point of a general pencil of plane cubics. Then T_2 has intersection numbers*

$$T_2 \cdot \lambda = 1, \quad T_2 \cdot \delta_0 = 12, \quad T_2 \cdot \delta_1 = -1, \quad T_2 \cdot \varphi^* \mathbb{O}_{X_6}(1) = 0.$$

Proof. The first three intersection numbers are standard. By Proposition 2.1, φ is defined on T_2 and contracts it to a point. □

Lemma 3.3. *There is a family T_3 of stable genus-6 curves having intersection numbers*

$$T_3 \cdot \lambda = 3, \quad T_3 \cdot \delta_0 = 30, \quad T_3 \cdot \delta_2 = -1, \quad T_3 \cdot \varphi^* \mathbb{O}_{X_6}(1) = 0.$$

Proof. In [Alper et al. 2011, Example 6.1], the authors construct for all $k \geq 2$ a complete family B_k of stable hyperelliptic curves of genus k with two marked points that are conjugate under the hyperelliptic involution. It is obtained by taking a double cover of the Hirzebruch surface $\mathbb{F}_1$ (considered as a $\mathbb{P}^1$-bundle over $\mathbb{P}^1$), branched along $2k+2$ general sections of self-intersection 1. The markings are given as the preimage of the unique (-1)-curve, which does not meet the branch locus. The covering map to $\mathbb{F}_1$ restricts to the hyperelliptic g^1_2 on every fiber, and since the two markings are always distinct, they are never Weierstraß points.

From the family B_2, we construct our family T_3 by forgetting one marking and attaching at the other a fixed 1-pointed curve of genus 4. Then the first three intersection numbers directly carry over from the computation in [Alper et al. 2011, Example 6.1] (note that $T_3 \cdot \delta_2 = -B_2 \cdot \psi_1$). The last one follows by Proposition 2.2 since φ is defined on T_3 and contracts it to a point. □

The following computation is used in the proof of Lemma 3.5:

Lemma 3.4. *Let X be a smooth threefold, $\mathscr{C} \subseteq X$ a surface with an ordinary k-fold point p, $\pi : \widetilde{X} \to X$ the blowup at p, and $\widetilde{\mathscr{C}}$ the proper transform of $\mathscr{C}$. Then $\chi(\mathbb{O}_{\widetilde{\mathscr{C}}}) = \chi(\mathbb{O}_{\mathscr{C}}) - \binom{k}{3}$.*

Proof. Let $E \subseteq \widetilde{X}$ be the exceptional divisor and $C = E \cap \widetilde{\mathscr{C}}$. By adjunction,

$$\begin{aligned} K_{\widetilde{\mathscr{C}}} &= (K_{\widetilde{X}} + \widetilde{\mathscr{C}})|_{\widetilde{\mathscr{C}}} \\ &= (\pi^* K_X + 2E + \pi^* \mathscr{C} - kE)|_{\widetilde{\mathscr{C}}} \\ &= \pi^* K_{\mathscr{C}} - (k-2)C, \end{aligned}$$

so Riemann–Roch for surfaces gives

$$\begin{aligned} \chi(\mathbb{O}_{\widetilde{\mathscr{C}}}) &= \chi(\mathbb{O}_{\widetilde{\mathscr{C}}}(-kC)) - kC^2 \\ &= \chi(\mathbb{O}_{\widetilde{\mathscr{C}}}(-kC)) + k^2. \end{aligned}$$

From the exact sequence

$$0 \to \mathcal{O}_X(-\mathscr{C}) \to \mathcal{O}_{\widetilde{X}}(-kE) \to \mathcal{O}_{\widetilde{\mathscr{C}}}(-kC) \to 0,$$

we get that

$$\chi(\mathcal{O}_{\widetilde{\mathscr{C}}}(-kC)) = \chi(\mathcal{O}_{\widetilde{X}}(-kE)) - \chi(\mathcal{O}_X) + \chi(\mathcal{O}_{\mathscr{C}}).$$

Finally, using induction on the exact sequence

$$0 \to \mathcal{O}_{\widetilde{X}}(-(i+1)E) \to \mathcal{O}_{\widetilde{X}}(-iE) \to \mathcal{O}_{\mathbb{P}^2}(i) \to 0$$

for $i = 0, \dots, k-1$, we conclude that

$$\chi(\mathcal{O}_{\widetilde{X}}(-kE)) = \chi(\mathcal{O}_X) - \sum_{i=0}^{k-1} \frac{i^2+3i+2}{2} = \chi(\mathcal{O}_X) - \frac{k^3+3k^2+2k}{6}.$$

Putting these three equations together gives the result. □

Lemma 3.5. *There is a family T_4 of stable genus-6 curves having intersection numbers*

$$T_4 \cdot \lambda = 16, \quad T_4 \cdot \delta_0 = 118, \quad T_4 \cdot \delta_3 = 1, \quad T_4 \cdot \varphi^* \mathcal{O}_{X_6}(1) = 4.$$

Proof. Let X be the blowup of $\mathbb{P}^2 \times \mathbb{P}^1$ at four constant sections of the second projection, and let $\mathscr{C}, \mathscr{C}' \subseteq X$ denote the proper transforms of degree-4 families of plane sextic curves with assigned nodes at the blown-up points. Suppose $\mathscr{C}$ is chosen in such a way that it contains the curve pictured in Figure 2 on the right as a member and that the fourfold points of this fiber are also ordinary fourfold points of the total space while away from this special fiber the family is smooth and all singular fibers are irreducible nodal. The stable reduction of the special fiber is then a Δ_3-curve, which we furthermore assume to lie in the locus where the map φ is defined. The family $\mathscr{C}'$ is chosen generically so that all its members are irreducible stable curves.

Let $\pi : \widetilde{X} \to X$ be the blowup of X at the two fourfold points of $\mathscr{C}$; denote by $\widetilde{\mathscr{C}}$ the proper transform of $\mathscr{C}$ and by $E_1, E_2 \subseteq \widetilde{X}$ the exceptional divisors of π. Then $\widetilde{\mathscr{C}} = \pi^*\mathscr{C} - 4E_1 - 4E_2$ and $K_{\widetilde{X}} = \pi^* K_X + 2E_1 + 2E_2$, so

$$\begin{aligned} K_{\widetilde{\mathscr{C}}}^2 &= (K_{\widetilde{X}} + \widetilde{\mathscr{C}})^2 \widetilde{\mathscr{C}} \\ &= (\pi^*(K_X + \mathscr{C}) - 2(E_1+E_2))^2 (\pi^*\mathscr{C} - 4(E_1+E_2)) \\ &= (K_X + \mathscr{C}')^2 \mathscr{C}' - 16(E_1^3 + E_2^3) = K_{\mathscr{C}'}^2 - 32. \end{aligned}$$

By Lemma 3.4, we find that

$$\chi(\mathcal{O}_{\widetilde{\mathscr{C}}}) = \chi(\mathcal{O}_{\mathscr{C}}) - 2\tbinom{4}{3} = \chi(\mathcal{O}_{\mathscr{C}'}) - 8,$$

so $c_2(\widetilde{\mathscr{C}}) = c_2(\mathscr{C}') - 64$ by Noether's formula. If T_4 and T_4' denote the families in $\overline{\mathcal{M}}_6$ induced by $\widetilde{\mathscr{C}}$ and $\mathscr{C}'$, respectively, we find that $T_4 \cdot \lambda = T_4' \cdot \lambda - 8 = 4 \cdot 6 - 8 = 16$ (note that T_4' is numerically equivalent to $4T_1$, where T_1 is the pencil described in Lemma 3.1). Moreover, the difference in topological Euler characteristics between a general (smooth) fiber and the special (blown-up) fiber of $\widetilde{\mathscr{C}}$ is 6; thus, we find $T_4 \cdot \delta_0 = T_4' \cdot \delta_0 - 64 - 6 = 4 \cdot 47 - 70 = 118$. Finally, T_4 is constructed in such a way that $T_4 \cdot \delta_3 = 1$ and $T_4 \cdot \varphi^* \mathbb{O}_{X_6}(1) = 4$. □

Lemma 3.6. *There is a family T_5 of stable genus-6 curves having intersection numbers*

$$T_5 \cdot \lambda = 21, \quad T_5 \cdot \delta_0 = 164, \quad T_5 \cdot \varphi^* \mathbb{O}_{X_6}(1) = 10.$$

Proof. In order to construct T_5, we take a family of quadric hyperplane sections of a family of generically smooth anticanonically embedded del Pezzo surfaces with special fibers having A_1 singularities. More concretely, let $\widetilde{\mathscr{S}}$ be the blowup of $\mathbb{P}^2 \times \mathbb{P}^1$ along the four sections

$$\begin{aligned}
\Sigma_1 &= ([1:0:0], [\lambda:\mu]),\\
\Sigma_2 &= ([0:1:0], [\lambda:\mu]),\\
\Sigma_3 &= ([0:0:1], [\lambda:\mu]),\\
\Sigma_4 &= ([\lambda+\mu:\lambda:\mu], [\lambda:\mu]),
\end{aligned}$$

where $[\lambda:\mu] \in \mathbb{P}^1$ is the base parameter. We map $\widetilde{\mathscr{S}}$ into $\mathbb{P}^7 \times \mathbb{P}^1$ by taking a system of eight $(3,1)$-forms that span the space of anticanonical forms in every fiber as given for example by

$$\begin{aligned}
f([x_0:x_1:x_2]) = \big[& x_0x_1(\lambda x_0 - (\lambda+\mu)x_1) : x_0^2(\mu x_1 - \lambda x_2)\\
& : x_0x_2(\mu x_0 - (\lambda+\mu)x_2) : x_0x_2(\mu x_1 - \lambda x_2)\\
& : x_0x_1(\mu x_1 - \lambda x_2) \qquad\quad : x_1^2(\mu x_0 - (\lambda+\mu)x_2)\\
& : x_1x_2(\mu x_1 - \lambda x_2) \qquad\quad : x_2^2(\lambda x_0 - (\lambda+\mu)x_1)\big].
\end{aligned}$$

This maps every fiber anticanonically into a 5-dimensional subspace of $\mathbb{P}^7$ that depends on $[\lambda:\mu] \in \mathbb{P}^1$. The image of the blown-up $\mathbb{P}^2$ is isomorphic to S except for the parameter values $[\lambda:\mu] = [1:0]$, $[0:1]$, and $[1:-1]$, where three base points lie on a line that gets contracted to an A_1 singularity under the anticanonical embedding.

Denote the image of f by $\mathscr{S}$; let H_1 and H_2 be the generators of $\mathrm{Pic}(\mathbb{P}^7 \times \mathbb{P}^1)$ and $\widetilde{H}_1$, $\widetilde{H}_2$, $E_1, \ldots, E_4$ those of $\mathrm{Pic}(\widetilde{\mathscr{S}})$. Note that $f^*H_1 = 3\widetilde{H}_1 - \sum E_i + \widetilde{H}_2$ and $f^*H_2 = \widetilde{H}_2$. We claim that

$$\mathscr{S} \equiv 5H_1^5 + 9H_1^4H_2 \in A^*(\mathbb{P}^7 \times \mathbb{P}^1).$$

Indeed, the first coefficient is just the degree in a fiber while the second one is computed as

$$\begin{aligned}\mathcal{S}\cdot H_1^3 &= \left(3\widetilde{H}_1 - \sum_{i=1}^{4} E_i + \widetilde{H}_2\right)^3 = 27\widetilde{H}_1^2\widetilde{H}_2 + 3\sum_{i=1}^{4}\widetilde{H}_2 E_i^2 - E_4^3 + 9\widetilde{H}_1 E_4^2\\ &= 27 - 12 + 3 - 9 = 9.\end{aligned}$$

Here we have used that $\widetilde{H}_2 E_i^2 = -1$ for $i = 1, \dots, 4$ as it is just the self-intersection of the exceptional $\mathbb{P}^1$ in a fiber. Moreover, by the normal bundle exact sequence,

$$E_i^3 = K_{\mathbb{P}^2\times\mathbb{P}^1}\cdot\Sigma_i - \deg K_{\Sigma_i} = (-3\widetilde{H}_1 - 2\widetilde{H}_2)\widetilde{H}_1^2 + 2 = 0$$

for $i = 1, 2, 3$, and similarly,

$$E_4^3 = (-3\widetilde{H}_1 - 2\widetilde{H}_2)(\widetilde{H}_1^2 + \widetilde{H}_1\widetilde{H}_2) + 2 = -3.$$

Finally, $\widetilde{H}_1$ and $\widetilde{H}_2$ both restrict to the same thing on E_4 (namely the class of a fiber of the fibration $E_4 \to \Sigma_4$), so $\widetilde{H}_1 E_4^2 = \widetilde{H}_2 E_4^2 = -1$.

Let $\mathcal{C}$ be the family cut out on $\mathcal{S}$ by a generic hypersurface of bidegree $(2, 2)$ so that $\mathcal{C} \equiv 10H_1^6 + 28H_1^5 H_2$. Since $K_{\widetilde{\mathcal{S}}} = \mathbb{O}_{\widetilde{\mathcal{S}}}(-3\widetilde{H}_1 + \sum E_i - 2\widetilde{H}_2)$, we find that $K_{\mathcal{S}} = \mathbb{O}_{\mathcal{S}}(-H_1 - H_2)$. Thus, $\omega_{\mathcal{S}/\mathbb{P}^1} = \mathbb{O}_{\mathcal{S}}(-H_1 + H_2)$, and by adjunction, $\omega_{\mathcal{C}/\mathbb{P}^1} = \mathbb{O}_{\mathcal{C}}(H_1 + 3H_2)$. If T_5 denotes the family induced in $\overline{\mathcal{M}}_6$ by $\mathcal{C}$, we then find that

$$T_5\cdot\kappa = \omega_{\mathcal{C}/\mathbb{P}^1}^2 = (H_1 + 3H_2)^2\cdot(10H_1^6 + 28H_1^5 H_2) = 88.$$

Next we note that $\mathbb{O}_{\mathcal{S}}(-\mathcal{C}) = 2K_{\mathcal{S}}$, so applying the Riemann–Roch theorem for threefolds to the short exact sequence $0 \to 2K_{\mathcal{S}} \to \mathbb{O}_{\mathcal{S}} \to \mathbb{O}_{\mathcal{C}} \to 0$, we get

$$\begin{aligned}\chi(\mathbb{O}_{\mathcal{C}}) &= \chi(\mathbb{O}_{\mathcal{S}}) - \chi(2K_{\mathcal{S}})\\ &= -\tfrac{1}{2}K_{\mathcal{S}}^3 + 4\chi(\mathbb{O}_{\mathcal{S}})\\ &= -\tfrac{1}{2}(-H_1 - H_2)^3(5H_1^5 + 9H_1^4 H_2) + 4\\ &= 16,\end{aligned}$$

where we used that $\chi(\mathbb{O}_{\mathcal{S}}) = 1$ because $\mathcal{S}$ is rational. Hence, if C denotes a generic fiber of $\mathcal{C}$, we get that $T_5\cdot\lambda = \chi(\mathbb{O}_{\mathcal{C}}) - (g(\mathbb{P}^1) - 1)(g(C) - 1) = 21$. Finally, by Mumford's relation, we obtain $T_5\cdot\delta_0 = 12\cdot 21 - 88 = 164$.

For computing $T_5\cdot\varphi^*\mathbb{O}_{X_6}(1)$, we note that we can also construct $\mathcal{S}$ as follows: blow up $\mathbb{P}^2\times\mathbb{P}^1$ at $[1:0:0]$, $[0:1:0]$, $[0:0:1]$, and $[1:1:1]$, embed it into $\mathbb{P}^7\times\mathbb{P}^1$ via

$$\begin{aligned}f'([x_0:x_1:x_2]) = \big[&x_0x_1(x_0 - x_1) : x_0^2(x_1 - x_2) : x_0x_2(x_0 - x_2) : x_0x_2(x_1 - x_2)\\ &: x_0x_1(x_1 - x_2) : x_1^2(x_0 - x_2) : x_1x_2(x_1 - x_2) : x_2^2(x_0 - x_1)\big],\end{aligned}$$

and take the proper transform of this constant family under the birational map $\psi : \mathbb{P}^7 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^7 \times \mathbb{P}^1$ given by

$$\begin{aligned}\psi([y_0 : \cdots : y_7]) = \big[&\lambda^2(\lambda+\mu)^2 y_0 \ : \lambda\mu(\lambda+\mu)^2 y_1 : \mu^2(\lambda+\mu)^2 y_2 : \lambda\mu^2(\lambda+\mu) y_3 \\ &: \lambda^2\mu(\lambda+\mu) y_4 : \lambda^2\mu(\lambda+\mu) y_5 : \lambda^2\mu^2 y_6 \qquad : \lambda\mu^2(\lambda+\mu) y_7\big].\end{aligned}$$

Denoting by $\mathcal{S}' \cong S \times \mathbb{P}^1$ the image of f', the intersection number $T_5 \cdot \varphi^* \mathbb{O}(1)$ is given by the number of curves in T_5 passing through a general fixed point of S. Since two general hyperplane sections cut out five general points on S, we compute that

$$T_5 \cdot \varphi^* \mathbb{O}_{X_6}(1) = \tfrac{1}{5} \mathbb{O}_{\mathcal{S}'}(H_1)^2 \cdot \psi^* \mathbb{O}_{\mathcal{G}}(\mathcal{C}) = \tfrac{1}{5} H_1^5 \cdot H_1^2 \cdot (2H_1 + 10H_2) = 10. \quad \square$$

4. The moving slope of $\overline{\mathcal{M}}_6$

Proposition 4.1. *The moving slope of $\overline{\mathcal{M}}_6$ fulfills $\frac{47}{6} \le s'(\overline{\mathcal{M}}_6) \le \frac{102}{13}$.*

Proof. The lower bound is the slope of the effective cone of $\overline{\mathcal{M}}_6$ and was known before [Farkas 2010]. Using the test families T_1 through T_5 described in Section 3, we get that

$$\varphi^* \mathbb{O}_{X_6}(1) = 102\lambda - 13\delta_0 - 54\delta_1 - 84\delta_2 - 94\delta_3.$$

Since $\mathbb{O}_{X_6}(1)$ is ample on X_6 and φ is a rational contraction, this is a moving divisor on $\overline{\mathcal{M}}_6$, which gives the upper bound on the moving slope. $\square$

Remark 4.2. Note that $\frac{102}{13} \approx 7.846$ is strictly smaller than $\frac{65}{8} = 8.125$, which was the upper bound previously obtained in [Farkas 2010]. However, since our families T_4 and T_5 are not covering families for divisors contracted by φ, we cannot argue as in [Fedorchuk 2012, Corollary 3.7]. In particular, the actual moving slope may be lower than the upper bound given here.

Proposition 4.3. *The log canonical model $\overline{\mathcal{M}}_6(\alpha)$ is isomorphic to X_6 whenever $\frac{16}{47} < \alpha \le \frac{35}{102}$. It is a point for $\alpha = \frac{16}{47}$, and empty for $\alpha < \frac{16}{47}$.*

Proof. This is completely analogous to [Fedorchuk 2012, Corollary 3.6]. Since

$$\begin{aligned}(K_{\overline{\mathcal{M}}_6} + \alpha\delta) - \varphi^* \varphi_* (K_{\overline{\mathcal{M}}_6} + \alpha\delta) \\ &= (13\lambda - (2-\alpha)\delta) - \varphi^* \varphi_* (13\lambda - (2-\alpha)\delta) \\ &= \big(\tfrac{35}{2} - 51\alpha\big)\big[\overline{\mathcal{GP}}_6\big] + (9 - 11\alpha)\delta_1 + (19 - 29\alpha)\delta_2 + (34 - 96\alpha)\delta_3\end{aligned}$$

is an effective exceptional divisor for φ as long as $\alpha \le \frac{35}{102}$, the upper bound follows. Moreover, $\varphi_*(13\lambda - (2-\alpha)\delta) = \mathbb{O}_{X_6}(47\alpha - 16)$, which gives the lower bound. $\square$

Acknowledgements

This work is part of my PhD thesis. I am very grateful to my advisor Gavril Farkas for suggesting the problem and providing many helpful insights. I would also like to thank Florian Geiß for several enlightening discussions as well as an anonymous referee for some constructive criticism. I am supported by the DFG Priority Project SPP 1489.

References

[Alper et al. 2011] J. Alper, M. Fedorchuk, and D. Smyth, "Singularities with $\mathbb{G}_m$-action and the log minimal model program for $\overline{M}_g$", preprint, 2011. arXiv 1010.3751v2

[Chang and Ran 1991] M.-C. Chang and Z. Ran, "On the slope and Kodaira dimension of $\overline{M}_g$ for small g", *J. Differential Geom.* **34**:1 (1991), 267–274. MR 92h:14015 Zbl 0780.14014

[Coray and Tsfasman 1988] D. F. Coray and M. A. Tsfasman, "Arithmetic on singular Del Pezzo surfaces", *Proc. London Math. Soc.* (3) **57**:1 (1988), 25–87. MR 89f:11083 Zbl 0653.14018

[Coskun 2006] I. Coskun, "The enumerative geometry of Del Pezzo surfaces via degenerations", *Amer. J. Math.* **128**:3 (2006), 751–786. MR 2007i:14053 Zbl 1099.14029

[Eisenbud and Harris 1987a] D. Eisenbud and J. Harris, "Existence, decomposition, and limits of certain Weierstrass points", *Invent. Math.* **87**:3 (1987), 495–515. MR 88a:14028b Zbl 0606.14014

[Eisenbud and Harris 1987b] D. Eisenbud and J. Harris, "The Kodaira dimension of the moduli space of curves of genus ≥ 23", *Invent. Math.* **90**:2 (1987), 359–387. MR 88g:14027 Zbl 0631.14023

[Farkas 2010] G. Farkas, "Rational maps between moduli spaces of curves and Gieseker–Petri divisors", *J. Algebraic Geom.* **19**:2 (2010), 243–284. MR 2011b:14060 Zbl 1210.14029

[Fedorchuk 2012] M. Fedorchuk, "The final log canonical model of the moduli space of stable curves of genus 4", *Int. Math. Res. Not.* **2012**:24 (2012), 5650–5672. MR 3006172 Zbl 1258.14032

[Hassett 2000] B. Hassett, "Local stable reduction of plane curve singularities", *J. Reine Angew. Math.* **520** (2000), 169–194. MR 2001d:14029 Zbl 0962.14019

[Jensen 2013] D. Jensen, "Birational contractions of $\overline{M}_{3,1}$ and $\overline{M}_{4,1}$", *Trans. Amer. Math. Soc.* **365**:6 (2013), 2863–2879. MR 3034451 Zbl 06185190

[Schubert 1991] D. Schubert, "A new compactification of the moduli space of curves", *Compositio Math.* **78**:3 (1991), 297–313. MR 92d:14018 Zbl 0735.14022

[Shepherd-Barron 1989] N. I. Shepherd-Barron, "Invariant theory for S_5 and the rationality of M_6", *Compositio Math.* **70**:1 (1989), 13–25. MR 90b:14058 Zbl 0704.14044

Communicated by Ravi Vakil
Received 2013-06-17 Revised 2014-04-06 Accepted 2014-05-19

muellerf@math.hu-berlin.de *Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1127

msp

Poisson structures and star products on quasimodular forms

François Dumas and Emmanuel Royer

We construct and classify all Poisson structures on quasimodular forms that extend the one coming from the first Rankin–Cohen bracket on the modular forms. We use them to build formal deformations on the algebra of quasimodular forms.

1. Introduction

Henri Cohen [1975, Theorem 7.1] defined a collection of bidifferential operators on modular forms. Let n be a positive integer, f a modular form of weight k, and g a modular form of weight ℓ. The n-th Rankin–Cohen bracket of f and g is the modular form of weight $k+\ell+2n$ defined by

$$\mathrm{RC}_n(f,g)=\sum_{r=0}^{n}(-1)^r\binom{k+n-1}{n-r}\binom{\ell+n-1}{r}\mathrm{D}^r f\,\mathrm{D}^{n-r}g \quad \left(\mathrm{D}=\frac{1}{2\pi\mathrm{i}}\frac{\mathrm{d}}{\mathrm{d}z}\right).$$

The algebraic structure of these brackets has been studied in the seminal [Zagier 1994]. That Rankin–Cohen brackets define a formal deformation of the algebra of modular forms has been widely studied. Important contributions are [Unterberger and Unterberger 1996; Cohen et al. 1997; Yao 2007; Bieliavsky et al. 2007; Pevzner 2012; Kobayashi and Pevzner 2013].

In this paper, we construct formal deformations of the algebra $\mathcal{M}_*^{\leq\infty}$ of quasimodular forms. This algebra is generated over $\mathbb{C}$ by the three Eisenstein series E_2, E_4 and E_6. The algebra $\mathcal{M}_*$ of modular forms is the subalgebra generated by E_4 and E_6. As a first step, we classify the admissible Poisson structures of $\mathcal{M}_*^{\leq\infty}$. A Poisson bracket $\{\,,\}$ on $\mathcal{M}_*^{\leq\infty}$ is admissible if

(i) the restriction of $\{\,,\}$ to the algebra $\mathcal{M}_*$ of modular forms is the first Rankin–Cohen bracket RC_1 and

We thank François Martin and Anne Pichereau for many fruitful discussions.
MSC2010: primary 17B63; secondary 11F25, 11F11, 16W25.
Keywords: quasimodular forms, Poisson brackets, Rankin–Cohen brackets, formal deformation, Eholzer product, star product.

(ii) it satisfies $\{\mathcal{M}_k^{\leq s}, \mathcal{M}_\ell^{\leq t}\} \subset \mathcal{M}_{k+\ell+2}^{\leq s+t}$ for any even integers k, ℓ and any integers s and t,

where $\mathcal{M}_k^{\leq s}$ is the vector space of quasimodular forms of weight k and depth less than s. The vector space of parabolic modular forms of weight 12 is one-dimensional. We choose $\Delta = \mathrm{E}_4^3 - \mathrm{E}_6^2$ a generator.

Proposition A (first family of Poisson brackets). *For any $\lambda \in \mathbb{C}^*$, there exists an admissible Poisson bracket $\{\,,\,\}_\lambda$ on the algebra of quasimodular forms defined by the following values on the generators*:

$$\begin{aligned}\{\mathrm{E}_4, \mathrm{E}_6\}_\lambda &= -2\Delta,\\ \{\mathrm{E}_2, \mathrm{E}_4\}_\lambda &= -\tfrac{1}{3}(2\mathrm{E}_6\mathrm{E}_2 - \lambda\mathrm{E}_4^2),\\ \{\mathrm{E}_2, \mathrm{E}_6\}_\lambda &= -\tfrac{1}{2}(2\mathrm{E}_4^2\mathrm{E}_2 - \lambda\mathrm{E}_4\mathrm{E}_6).\end{aligned}$$

Moreover:

(i) *For any $\lambda \in \mathbb{C}^*$, the Poisson bracket $\{\,,\,\}_\lambda$ is not unimodular.*

(ii) *The Poisson algebras $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_\lambda)$ and $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_{\lambda'})$ are Poisson modular isomorphic for all λ and λ' in $\mathbb{C}^*$.*

(iii) *For any $\lambda \in \mathbb{C}^*$, the Poisson centre of $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_\lambda)$ is $\mathbb{C}$.*

Remark. A Poisson isomorphism φ on $\mathcal{M}_*^{\leq\infty}$ is modular if $\varphi(\mathcal{M}_*) \subset \mathcal{M}_*$.

Thanks to (ii) in Proposition A, we restrict to the bracket $\{\,,\,\}_1$. Following [Zagier 1994, Equation (38)], we consider the derivation w on $\mathcal{M}_*^{\leq\infty}$ defined by

$$\mathrm{w}(f) = \frac{\{\Delta, f\}_1}{12\Delta}.$$

A derivation δ on $\mathcal{M}_*^{\leq\infty}$ is complex-like if $\delta(\mathcal{M}_k^{\leq s}) \subset \mathcal{M}_{k+2}^{\leq s+1}$ for any k and s. The set of complex-like derivations δ such that $kf\delta(g) - \ell g\delta(f) = 0$ for any $f \in \mathcal{M}_k^{\leq s}$ and $g \in \mathcal{M}_\ell^{\leq t}$, for any k, ℓ, s, t, is a one-dimensional vector space over $\mathbb{C}$. Let π be a generator. The following theorem provides a first family of formal deformations of the algebra $\mathcal{M}_*^{\leq\infty}$.

Theorem B. *For any $a \in \mathbb{C}$, let d_a be the derivation on $\mathcal{M}_*^{\leq\infty}$ defined by $\mathrm{d}_a = a\pi + \mathrm{w}$.*

(i) *For all quasimodular forms f and g of respective weights k and ℓ, we have*

$$\{f, g\}_1 = kf\,\mathrm{d}_a(g) - \ell g\,\mathrm{d}_a(f).$$

(ii) *More generally, for any $a \in \mathbb{C}$, the brackets defined for any integer $n \geq 0$ by*

$$[f, g]_{\mathrm{d}_a,n} = \sum_{r=0}^{n} (-1)^r \binom{k+n-1}{n-r}\binom{\ell+n-1}{r} \mathrm{d}_a^r(f)\mathrm{d}_a^{n-r}(g) \qquad (f \in \mathcal{M}_k^{\leq\infty}, g \in \mathcal{M}_\ell^{\leq\infty})$$

satisfy

$$[\mathcal{M}_k^{\leq\infty}, \mathcal{M}_\ell^{\leq\infty}]_{\mathrm{d}_a,n} \subset \mathcal{M}_{k+\ell+2n}^{\leq\infty}$$

and define a formal deformation of $\mathcal{M}_*^{\leq\infty}$.

(iii) *Moreover,* $[\mathcal{M}_k^{\leq s}, \mathcal{M}_\ell^{\leq t}]_{\mathrm{d}_a,n} \subset \mathcal{M}_{k+\ell+2n}^{\leq s+t}$ *for all* n, s, t, k, ℓ *if and only if* $a = 0$.

Remark. A generator π is defined by linear extension of $\pi(f) = kf\mathrm{E}_2$ for f any quasimodular form of weight k. For this choice, the derivation d_a is defined on the generators by

$$\mathrm{d}_a\mathrm{E}_2 = 2a\mathrm{E}_2^2 - \tfrac{1}{12}\mathrm{E}_4, \quad \mathrm{d}_a\mathrm{E}_4 = 4a\mathrm{E}_4\mathrm{E}_2 - \tfrac{1}{3}\mathrm{E}_6, \quad \mathrm{d}_a\mathrm{E}_6 = 6a\mathrm{E}_6\mathrm{E}_2 - \tfrac{1}{2}\mathrm{E}_4^2.$$

Proposition C (second family of Poisson brackets). *For any* $\alpha \in \mathbb{C}$, *there exists an admissible Poisson bracket* $(\,,\,)_\alpha$ *on the algebra of quasimodular forms defined by the following values on the generators*:

$$(\mathrm{E}_4, \mathrm{E}_6)_\alpha = -2\Delta, \quad (\mathrm{E}_2, \mathrm{E}_4)_\alpha = \alpha\mathrm{E}_6\mathrm{E}_2, \quad (\mathrm{E}_2, \mathrm{E}_6)_\alpha = \tfrac{3}{2}\alpha\mathrm{E}_4^2\mathrm{E}_2.$$

Moreover:

(i) *For any* $\alpha \in \mathbb{C} \setminus \{4\}$, *the Poisson bracket* $(\,,\,)_\alpha$ *is not unimodular. For* $\alpha = 4$, *the Poisson bracket* $(\,,\,)_4$ *is Jacobian* (*and hence unimodular*) *of potential* $k_0 = -2\Delta\mathrm{E}_2$.

(ii) *The Poisson algebras* $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$ *and* $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_{\alpha'})$ *are Poisson modular isomorphic if and only if* $\alpha = \alpha'$.

(iii) *For any* $\alpha \in \mathbb{C}$,

  (a) *if* $\alpha \notin \mathbb{Q}$, *the Poisson centre of* $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$ *is* $\mathbb{C}$;

  (b) *if* $\alpha = 0$, *the Poisson centre of* $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$ *is* $\mathbb{C}[\mathrm{E}_2]$;

  (c) *if* $\alpha = p/q$ *with* $p \in \mathbb{Z}^*$ *and* $q \in \mathbb{N}^*$, p *and* q *coprimes*, *the Poisson centre of* $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$ *is*

$$\begin{cases} \mathbb{C} & \text{if } p < 0, \\ \mathbb{C}[\Delta^p\mathrm{E}_2^{4q}] & \text{if } p \geq 1 \text{ is odd}, \\ \mathbb{C}[\Delta^u\mathrm{E}_2^{2q}] & \text{if } p = 2u \text{ for odd } u \geq 1, \\ \mathbb{C}[\Delta^v\mathrm{E}_2^{q}] & \text{if } p = 4v \text{ with } v \geq 1. \end{cases}$$

Remark. The bracket $(\,,\,)_0$ is the trivial bracket.

This second family provides a new set of formal deformations of the algebra of quasimodular forms. Following [Zagier 1994, Equation (38)], we consider the derivation v defined on $\mathcal{M}_*^{\leq\infty}$ by

$$\mathrm{v}(f) = \frac{(\Delta, f)_\alpha}{12\Delta}.$$

Let us define $\mathcal{H}_\alpha : \mathcal{M}_*^{\leq\infty} \to \mathbb{C}$ by setting $\mathcal{H}_\alpha(f) = k - (3\alpha+2)s$ if f has weight k and depth s. The set of complex-like derivations δ such that

$$\mathcal{H}_\alpha(f) f\delta(g) - \mathcal{H}_\alpha(g) g\delta(f) = 0$$

for any $f \in \mathcal{M}_k^{\leq s}$ and $g \in \mathcal{M}_\ell^{\leq t}$, for any k, ℓ, s, t, is a one-dimensional vector space over $\mathbb{C}$. Let π_α be a generator. We define

$$\mathcal{M}_k^s = \mathcal{M}_{k-2s}\mathrm{E}_2^s.$$

Theorem D. *Let $\alpha \in \mathbb{C}$. For any $b \in \mathbb{C}$, let $\delta_{\alpha,b}$ be the derivation on $\mathcal{M}_*^{\leq\infty}$ defined by $\delta_{\alpha,b} = b\pi_\alpha + \mathrm{v}$.*

(i) *For all $f \in \mathcal{M}_k^s$ and $g \in \mathcal{M}_\ell^t$, we have*

$$(f, g)_\alpha = (k - (3\alpha+2)s) f\delta_{\alpha,b}(g) - (\ell - (3\alpha+2)t) g\delta_{\alpha,b}(f)$$

for any $f \in \mathcal{M}_k^s$ and $g \in \mathcal{M}_\ell^t$.

(ii) *Moreover, the brackets defined for any integer $n \geq 0$ by*

$$[f, g]^{\mathcal{H}_\alpha}_{\delta_{\alpha,b},n} = \sum_{r=0}^{n} (-1)^r \binom{k-(3\alpha+2)s+n-1}{n-r} \binom{\ell-(3\alpha+2)t+n-1}{r} \delta_{\alpha,b}^r(f) \delta_{\alpha,b}^{n-r}(g)$$

for any $f \in \mathcal{M}_k^s$ and $g \in \mathcal{M}_\ell^t$ define a formal deformation of $\mathcal{M}_*^{\leq\infty}$ satisfying

$$[\mathcal{M}_k^{\leq s}, \mathcal{M}_\ell^{\leq t}]^{\mathcal{H}_\alpha}_{\delta_{\alpha,b},n} \subset \mathcal{M}_{k+\ell+2n}^{\leq s+t}$$

for all k, ℓ in $2\mathbb{N}$ and s, t in $\mathbb{N}$ if and only if $b = 0$.

Remark. A generator π_α is defined by linear extension of

$$\pi_\alpha(f) = [k - (3\alpha+2)s] f\mathrm{E}_2 \quad (f \in \mathcal{M}_k^s).$$

For this choice, the derivation $\delta_{\alpha,b}$ is defined on the generators by

$$\delta_{\alpha,b}\mathrm{E}_2 = -3b\alpha\mathrm{E}_2^2, \quad \delta_{\alpha,b}\mathrm{E}_4 = 4b\mathrm{E}_4\mathrm{E}_2 - \tfrac{1}{3}\mathrm{E}_6, \quad \delta_{\alpha,b}\mathrm{E}_6 = 6b\mathrm{E}_6\mathrm{E}_2 - \tfrac{1}{2}\mathrm{E}_4^2.$$

To complete the classification of Poisson structures, we introduce a third family of Poisson brackets. We note, however, that when $\mu \neq 0$ this third family does not lead to a formal deformation of $\mathcal{M}_*^{\leq\infty}$ with the shape of Rankin–Cohen brackets (see Section 4.3).

Proposition E (third family of Poisson brackets). *For any $\mu \in \mathbb{C}$, there exists an admissible Poisson bracket $\langle\,,\,\rangle_\mu$ on the algebra of quasimodular forms defined by*

the following values on the generators:

$$\langle \mathrm{E}_4, \mathrm{E}_6\rangle_\mu = -2\Delta,$$
$$\langle \mathrm{E}_2, \mathrm{E}_4\rangle_\mu = 4\mathrm{E}_6\mathrm{E}_2 + \mu\mathrm{E}_4^2,$$
$$\langle \mathrm{E}_2, \mathrm{E}_6\rangle_\mu = 6\mathrm{E}_4^2\mathrm{E}_2 - 2\mu\mathrm{E}_4\mathrm{E}_6.$$

Moreover:

(i) *This Poisson bracket is Jacobian with potential*

$$k_\mu = -2\Delta\mathrm{E}_2 + \mu\mathrm{E}_4^2\mathrm{E}_6.$$

(ii) *The Poisson algebras* $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_\mu)$ *and* $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_{\mu'})$ *are Poisson modular isomorphic for all* μ *and* μ' *in* $\mathbb{C}^*$.

(iii) *For any* $\mu \in \mathbb{C}$, *the Poisson centre of* $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_\mu)$ *is the polynomial algebra* $\mathbb{C}[k_\mu]$.

Remark. We note that $\langle\,,\,\rangle_0 = (\,,\,)_4$.

Finally, the following result implies that our classification is complete.

Theorem F. *Up to Poisson modular isomorphism, the only distinct admissible Poisson brackets on the algebra of quasimodular forms are* $\{\,,\,\}_1$, $\langle\,,\,\rangle_1$ *and the family* $(\,,\,)_\alpha$ *for any* $\alpha \in \mathbb{C}$.

Remark. We could endow the algebra of modular forms with another Poisson structure b. If we require $\mathrm{b}(\mathcal{M}_k, \mathcal{M}_\ell) \subset \mathcal{M}_{k+\ell+2}$, then b is necessarily defined by $\mathrm{b}(\mathrm{E}_4, \mathrm{E}_6) = \alpha\mathrm{E}_4^3 + \beta\mathrm{E}_6^2$ for some complex numbers α and β. If $\alpha\beta \neq 0$, then $(\mathcal{M}_*, \mathrm{b})$ is Poisson isomorphic to $(\mathcal{M}_*, \mathrm{RC}_1)$ and is indeed studied by this work. If $\alpha\beta = 0$, the Poisson algebras are no longer Poisson isomorphic (they do not have the same group of automorphisms). This degenerate case deserves another study.

Remark. From an algebraic point of view, classifications of Poisson structures and associated (co)homology for polynomial algebras in two variables appear in [Monnier 2002; Pichereau 2006a; Roger and Vanhaecke 2002] for a Poisson bracket on $\mathbb{C}[x, y]$ defined by $\{x, y\} = \varphi(x, y)$ with φ a homogeneous or square-free weight-homogeneous polynomial in $\mathbb{C}[x, y]$. The algebra of modular forms $\mathcal{M}_* = \mathbb{C}[\mathrm{E}_4, \mathrm{E}_6]$ with the Poisson bracket defined by RC_1 is the case A_2 in the classification theorem 3.8 in [Monnier 2002]. Applying Propositions 4.10 and 4.11 of [Pichereau 2006a], or Theorems 4.6 and 4.11 of [Monnier 2002], we can deduce that the Poisson cohomology spaces $\mathrm{HP}^1(\mathcal{M}_*)$ and $\mathrm{HP}^2(\mathcal{M}_*)$ are of respective dimensions 1 and 2. In three variables, the Poisson structures on the algebra $\mathcal{M}_*^{\leq\infty} = \mathbb{C}[\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6]$ of quasimodular forms arising from Theorem F do not fall under the classification of [Dufour and Haraki 1991] since they are not quadratic. The (co)homological study of Pichereau [2006a; 2006b] does not apply to the brackets $\{\,,\,\}_1$ and $(\,,\,)_\alpha$, since

they are not Jacobian, or to the Jacobian bracket $\langle\,,\,\rangle_1$, because its potential k_1 does not admit an isolated singularity at the origin.

2. Number theoretic and algebraic background

2.1. ***Quasimodular forms.*** The aim of this section is to provide the necessary background on quasimodular forms. For details, the reader is advised to refer to [Zagier 2008] or [Martin and Royer 2005]. On $\mathrm{SL}(2,\mathbb{Z})$, a modular form of weight $k \in 2\mathbb{N}$, $k \neq 2$, is a holomorphic function on the Poincaré upper half-plane $\mathcal{H} = \{z \in \mathbb{C} : \Im z > 0\}$ satisfying

$$(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = f(z)$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ and having Fourier expansion

$$f(z) = \sum_{n\geq 0} \widehat{f}(n) \mathrm{e}^{2\pi i n z}.$$

We denote by $\mathcal{M}_k$ the finite-dimensional space of modular forms of weight k. The algebra of modular forms is defined as the graded algebra

$$\mathcal{M}_* = \bigoplus_{\substack{k\in 2\mathbb{N} \\ k\neq 2}} \mathcal{M}_k.$$

Let $k \geq 2$ be even. We define the Eisenstein series of weight k by

$$\mathrm{E}_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{+\infty} \sigma_{k-1}(n) \mathrm{e}^{2\pi i n z}.$$

Here the rational numbers B_k are defined by their exponential generating series

$$\sum_{n=0}^{+\infty} B_n \frac{t^n}{n!} = \frac{t}{\mathrm{e}^t - 1}$$

and σ_{k-1} is the divisor function defined by

$$\sigma_{k-1}(n) = \sum_{\substack{d\,|\,n \\ d>0}} d^{k-1} \quad (n \in \mathbb{N}^*).$$

If $k \geq 4$, the Eisenstein series E_k is a modular form of weight k and $\mathcal{M}_*$ is the polynomial algebra in the two algebraically independent Eisenstein series E_4 and E_6. In other words,

$$\mathcal{M}_* = \mathbb{C}[\mathrm{E}_4, \mathrm{E}_6], \quad \mathcal{M}_k = \bigoplus_{\substack{(i,j)\in\mathbb{N}^2 \\ 4i+6j=k}} \mathbb{C}\mathrm{E}_4^i \mathrm{E}_6^j.$$

However, the Eisenstein series E_2 is not a modular form. It satisfies

$$(cz+d)^{-2}\mathrm{E}_2\left(\frac{az+b}{cz+d}\right) = \mathrm{E}_2(z) + \frac{6}{\pi \mathrm{i}}\frac{c}{cz+d} \quad (z \in \mathscr{H})$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Moreover, the algebra of modular forms is not stable by the normalised complex derivation

$$\mathrm{D} = \frac{1}{2\pi \mathrm{i}}\frac{\mathrm{d}}{\mathrm{d}z}.$$

For example, we have the Ramanujan differential equations

$$\mathrm{D}\mathrm{E}_2 = \tfrac{1}{12}(\mathrm{E}_2^2 - \mathrm{E}_4), \quad \mathrm{D}\mathrm{E}_4 = \tfrac{1}{3}(\mathrm{E}_4\mathrm{E}_2 - \mathrm{E}_6), \quad \mathrm{D}\mathrm{E}_6 = \tfrac{1}{2}(\mathrm{E}_6\mathrm{E}_2 - \mathrm{E}_4^2).$$

To account for these observations, and using the fact that E_2, E_4 and E_6 are algebraically independent, we introduce the algebra $\mathscr{M}_*^{\leq\infty}$ of quasimodular forms defined as the polynomial algebra

$$\mathscr{M}_*^{\leq\infty} = \mathbb{C}[\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6] = \mathscr{M}_*[\mathrm{E}_2].$$

More intrinsically, if for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ we define

$$\mathrm{X}(\gamma) = z \mapsto \frac{c}{cz+d}$$

and

$$f|_k\gamma = z \mapsto (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right),$$

then a quasimodular form of weight $k \in 2\mathbb{N}$ and depth $s \in \mathbb{N}$ is a holomorphic function f on $\mathscr{H}$ such that there exist holomorphic functions $f_0, \ldots, f_s$ ($f_s \neq 0$) satisfying

$$f|_k\gamma = \sum_{j=0}^{s} f_j \mathrm{X}(\gamma)^j$$

for any $\gamma \in \mathrm{SL}(2,\mathbb{Z})$. Moreover, it is required that any f_j have a Fourier expansion

$$f_j(z) = \sum_{n\geq 0} \widehat{f}_j(n)\mathrm{e}^{2\pi \mathrm{i} n z} \quad (z \in \mathscr{H}).$$

The zero function is supposed to have arbitrary weight and depth 0. We write $\mathscr{M}_k^{\leq\infty}$ for the space of quasimodular forms of weight k and $\mathscr{M}_k^{\leq s}$ for the space of quasimodular forms of weight k and depth less than or equal to s. We have $\mathscr{M}_k^{\leq 0} = \mathscr{M}_k$ and

$$\mathscr{M}_k^{\leq s} = \bigoplus_{j=0}^{s} \mathscr{M}_{k-2j}\mathrm{E}_2^j, \quad \mathscr{M}_*^{\leq\infty} = \bigoplus_{k\in 2\mathbb{N}} \mathscr{M}_k^{\leq k/2}.$$

Moreover, $\mathrm{D}\mathcal{M}_k^{\leq s} \subset \mathcal{M}_{k+2}^{\leq s+1}$. Since the depth of a quasimodular form is nothing but its degree as a polynomial in E_2 with modular coefficients, we note that

$$\mathcal{M}_k^{\leq s} = \bigoplus_{t=0}^{s} \mathcal{M}_k^t, \quad \mathcal{M}_*^{\leq \infty} = \bigoplus_{k\in 2\mathbb{N}} \bigoplus_{t=0}^{k/2} \mathcal{M}_k^t,$$

where

$$\mathcal{M}_k^t = \mathcal{M}_{k-2t}\mathrm{E}_2^t = \bigoplus_{\substack{(i,j)\in\mathbb{N}^2 \\ 4i+6j=k-2t}} \mathbb{C}\mathrm{E}_4^i\mathrm{E}_6^j\mathrm{E}_2^t.$$

An important element in our study will be the discriminant function $\Delta = \mathrm{E}_4^3 - \mathrm{E}_6^2$. We note that $\mathrm{D}\Delta = \Delta\mathrm{E}_2$.

Let n be a nonnegative integer, f a modular form of weight k, and g a modular form of weight ℓ. The n-th Rankin–Cohen bracket of f and g is

$$\mathrm{RC}_n(f,g) = \sum_{r=0}^{n} (-1)^r \binom{k+n-1}{n-r} \binom{\ell+n-1}{r} \mathrm{D}^r f\, \mathrm{D}^{n-r} g.$$

This is a modular form of weight $k+\ell+2n$. If f and g are quasimodular forms of respective weights k and ℓ and respective depths s and t, their n-th Rankin–Cohen bracket is defined in [Martin and Royer 2009] by

$$\mathrm{RC}_n(f,g) = \sum_{r=0}^{n} (-1)^r \binom{k-s+n-1}{n-r} \binom{\ell-t+n-1}{r} \mathrm{D}^r f\, \mathrm{D}^{n-r} g. \tag{1}$$

This is a quasimodular form of weight $k+\ell+2n$ and minimal depth (that is $s+t$).

2.2. ***Poisson algebra.*** The aim of this section is to give a brief account of what is needed about Poisson algebra. For more details, the reader is advised to refer to [Laurent-Gengoux et al. 2013]. A commutative $\mathbb{C}$-algebra A is a Poisson algebra if there exists a bilinear skew-symmetric map $\mathrm{b} : A \times A \to A$ satisfying the two conditions

- (Leibniz rule) $\mathrm{b}(fg,h) = f\mathrm{b}(g,h) + \mathrm{b}(f,h)g$ and
- (Jacobi identity) $\mathrm{b}(f,\mathrm{b}(g,h)) + \mathrm{b}(g,\mathrm{b}(h,f)) + \mathrm{b}(h,\mathrm{b}(f,g)) = 0$

for all f, g and h in A. The bilinear map b is given the name of Poisson bracket. If A is a finitely generated algebra with generators $x_1,\dots,x_N$, a Poisson bracket b is entirely determined by its values $\mathrm{b}(x_i,x_j)$ for $i<j$, where A is generated by $x_1,\dots,x_N$. More precisely, we have

$$\mathrm{b}(f,g) = \sum_{0\leq i<j\leq N} \left(\frac{\partial f}{\partial x_i}\frac{\partial g}{\partial x_j} - \frac{\partial g}{\partial x_i}\frac{\partial f}{\partial x_j} \right) \mathrm{b}(x_i,x_j) \tag{2}$$

for f and g expressed as polynomials in $x_1,\dots,x_N$.

If $A = \mathbb{C}[x, y]$, any $p \in A$ determines a Poisson bracket satisfying $\mathrm{b}(x, y) = p$. However, if $A = \mathbb{C}[x, y, z]$, for any p, q and r in A, there exists a Poisson bracket on A defined by

$$\mathrm{b}(x, y) = r, \quad \mathrm{b}(y, z) = p \quad \text{and} \quad \mathrm{b}(z, x) = q$$

if and only if

$$\mathrm{curl}(p, q, r) \cdot (p, q, r) = 0, \tag{3}$$

where

$$\mathrm{curl}(p, q, r) = \left(\frac{\partial r}{\partial y} - \frac{\partial q}{\partial z}, \frac{\partial p}{\partial z} - \frac{\partial r}{\partial x}, \frac{\partial q}{\partial x} - \frac{\partial p}{\partial y} \right).$$

If condition (3) is satisfied, then (p, q, r) is called a Poissonian triple. A particular case is obtained if there exists $k \in \mathbb{C}[x, y, z]$ such that $\mathrm{curl}(p, q, r) = (p, q, r) \wedge \mathrm{grad}\, k$. The bracket b is said then to be unimodular. Among unimodular brackets are the Jacobian brackets. A bracket b is Jacobian if $(p, q, r) = \mathrm{grad}\, k$ for some polynomial k. The bracket b then satisfies

$$\mathrm{b}(f, g) = \mathrm{jac}(f, g, k) \quad (f, g \in A).$$

In this case, $\mathbb{C}[x, y, z]$ is said to have a Jacobian Poisson structure of potential (or Casimir function) k. The Poissonian triple (p, q, r) is said then to be exact.

The Poisson centre (or zeroth Poisson cohomology group) of a Poisson algebra A is the Poisson subalgebra

$$\mathrm{HP}^0(A) = \{g \in A : \mathrm{b}(f, g) = 0, \ \forall f \in A\}.$$

The Poisson centre is contained in the Poisson centraliser of any element in the algebra: let $f \in A$; its Poisson centraliser is $\{g \in A : \mathrm{b}(f, g) = 0\}$. The following lemma computes the Poisson centre of polynomial algebras in three variables equipped with a Jacobian Poisson structure. It allows one to recover, for example, Proposition 4.2 of [Pichereau 2006b] in the particular case where the potential is a weight-homogeneous polynomial with an isolated singularity. A polynomial $h \in \mathbb{C}[x, y, z]$ is indecomposable if there is no polynomial $p \in \mathbb{C}[x]$ with $\deg p \geq 2$ such that $h = p \circ \ell$ for some $\ell \in \mathbb{C}[x, y, z]$.

Lemma 1. *Let $\mathbb{C}[x, y, z]$ be endowed with a Jacobian Poisson structure of nonconstant potential k. Its Poisson centre is $\mathbb{C}[k]$ if and only if k is indecomposable.*

Proof. Assume that k is not indecomposable: $k = p \circ \ell$ with $p \in \mathbb{C}[x]$, $\deg p = 2$. Then $\mathrm{jac}(\ell, g, k) = (p' \circ \ell)\, \mathrm{jac}(\ell, g, \ell)$, and hence ℓ is in the Poisson centre, but not in $\mathbb{C}[k]$. Assume conversely that k is indecomposable. Let f be in the Poisson centre; then the rank of the Jacobian matrix of (f, g, k) is at most 2 for any g. If it is 1 for any g then $\mathrm{grad}\, f$ and $\mathrm{grad}\, k$ are zero, which contradicts the fact that k is not constant. Hence, for some g, the rank is 2. It follows (see, for example,

[Gutierrez and Sevilla 2006, Theorem 6]) that there exist $q \in \mathbb{C}[x, y, z]$, $F \in \mathbb{C}[x]$ and $K \in \mathbb{C}[x]$ such that $f = F \circ q$ and $k = K \circ q$. Since k is indecomposable and nonconstant, we have $\deg K = 1$, and hence q and f are polynomials in k. □

If A and B are two Poisson algebras with respective Poisson brackets b_A and b_B, a map $\varphi : A \to B$ is a morphism of Poisson algebras when it is a morphism of algebras that satisfies

$$\varphi(\mathrm{b}_A(f, g)) = \mathrm{b}_B(\varphi(f), \varphi(g))$$

for any f and g in A. Two Poisson-isomorphic Poisson algebras have isomorphic Poisson centres.

We detail now a canonical way to extend a Poisson structure from an algebra A to a polynomial algebra $A[x]$. This construction is due to Sei-Qwon Oh [2006]. A Poisson derivation of A is a derivation σ of A satisfying

$$\sigma(\mathrm{b}(f, g)) = \mathrm{b}(\sigma(f), g) + \mathrm{b}(f, \sigma(g))$$

for all f and g in A. If σ is a Poisson derivation of A, a Poisson σ-derivation is a derivation δ of A such that

$$\delta(\mathrm{b}(f, g)) = \mathrm{b}(\delta(f), g) + \mathrm{b}(f, \delta(g)) + \sigma(f)\delta(g) - \delta(f)\sigma(g)$$

for all f and g in A.

Theorem 2 [Oh 2006]. *Let (A, b_A) be a Poisson algebra. Let σ and δ be linear maps on A. The polynomial ring $A[x]$ becomes a Poisson algebra with Poisson brackets* b *defined by*

$$\mathrm{b}(f, g) = \mathrm{b}_A(f, g), \quad \mathrm{b}(x, f) = \sigma(f)x + \delta(f)$$

for all f and g in A if and only if σ is a Poisson derivation and δ is a Poisson σ-derivation. In this case, the Poisson algebra $A[x]$ is said to be a Poisson–Ore extension of A. It is denoted by $A[x]_{\sigma,\delta}$.

We describe also a general process to obtain Poisson brackets from a pair of derivations. A pair (δ, d) of two derivations of A is solvable if there exists some scalar α such that $\delta \circ \mathrm{d} - \mathrm{d} \circ \delta = \alpha \mathrm{d}$. In particular, a solvable pair (δ, d) is abelian when $\alpha = 0$.

Proposition 3. *Let A be a commutative algebra, and* d *and δ two derivations of A. Let* $\mathrm{b} : A \times A \to A$ *be defined by*

$$\mathrm{b}(f, g) = \delta(f)\mathrm{d}(g) - \mathrm{d}(f)\delta(g) \quad (f, g \in A).$$

Then:

(i) *The map* b *is bilinear skew-symmetric and satisfies the Leibniz rule.*

(ii) *If* (δ, d) *is solvable, then* b *satisfies the Jacobi identity and so becomes a Poisson bracket.*

(iii) *If* (δ, d) *is solvable, then* d *is a Poisson derivation for* b.

Proof. Point (i) is immediate. Point (ii) is a consequence of the following computation. If (δ, d) is solvable with $\delta\mathrm{d} - \mathrm{d}\delta = \alpha\mathrm{d}$ and if $\mathrm{B} : A \otimes A \otimes A \to A$ is defined by $\mathrm{B}(f, g, h) = \mathrm{b}(f, \mathrm{b}(g, h))$, then

$$\mathrm{B} = \alpha(\mathrm{d}\otimes\mathrm{d}\otimes\delta - \mathrm{d}\otimes\delta\otimes\mathrm{d}) + \big(\delta\otimes(\mathrm{d}\circ\delta)\otimes\mathrm{d} - \mathrm{d}\otimes\delta\otimes(\mathrm{d}\circ\delta)\big)$$
$$+\big(\mathrm{d}\otimes(\mathrm{d}\circ\delta)\otimes\delta - \delta\otimes\mathrm{d}\otimes(\mathrm{d}\circ\delta)\big) + (\delta\otimes\delta\otimes\mathrm{d}^2 - \delta\otimes\mathrm{d}^2\otimes\delta) + (\mathrm{d}\otimes\mathrm{d}\otimes\delta^2 - \mathrm{d}\otimes\delta^2\otimes\mathrm{d}).$$

Point (iii) is obtained by direct computation. □

A direct consequence of this proposition is the following corollary. If $A = \bigoplus_{n\geq 0} A_n$ is a commutative graded algebra, a map $\kappa : A \to \mathbb{C}$ is graded-additive if for any $f \in A_k$ and $g \in A_\ell$ (for any k and ℓ) we have $\kappa(fg) = \kappa(f) + \kappa(g)$.

Corollary 4. *Let* $A = \bigoplus_{n\geq 0} A_n$ *be a commutative graded algebra. Let* $\kappa : A \to \mathbb{C}$ *be a graded-additive map. Let* d *be a homogeneous derivation of* A (*there exists* $e \geq 0$ *such that* $\mathrm{d}A_n \subset A_{n+e}$ *for any* $e \geq 0$). *Then the bracket defined on* A *by the bilinear extension of*

$$\mathrm{b}(f, g) = \kappa(f) f\,\mathrm{d}(g) - \kappa(g) g\,\mathrm{d}(f) \quad (f \in A_k,\ g \in A_\ell)$$

is a Poisson bracket for which d *is a Poisson derivation.*

We turn to formal deformations of a commutative $\mathbb{C}$-algebra A. Assume we have a family $\mu = (\mu_i)_{i\in\mathbb{N}}$ of bilinear maps $\mu_i : A \times A \to A$ such that μ_0 is the product. Let $A[\![\hbar]\!]$ be the commutative algebra of formal power series in one variable $\hbar$ with coefficients in A. The family μ is a formal deformation of A if the noncommutative product on $A[\![\hbar]\!]$ defined by extension of

$$f * g = \sum_{j\geq 0} \mu_j(f, g)\hbar^j \quad (f, g \in A)$$

is associative. This condition is equivalent to

$$\sum_{r=0}^{n} \mu_{n-r}(\mu_r(f, g), h) = \sum_{r=0}^{n} \mu_{n-r}(f, \mu_r(g, h)) \quad (\text{for all } f, g, h \in A) \qquad (4)$$

for all $n \geq 0$. In this case, the product $*$ is called a star product. If μ is a formal deformation and if moreover μ_1 is skew-symmetric and μ_2 is symmetric, then (A, μ_1) is a Poisson algebra.

2.3. ***Problems at issue.*** The first Rankin–Cohen bracket

$$\mathrm{RC}_1(f,g) = kf\,\mathrm{D}(g) - \mathrm{D}(f)\ell g \quad (f \in \mathcal{M}_k,\ g \in \mathcal{M}_\ell)$$

gives $\mathcal{M}_*$ a structure of Poisson algebra. This is a consequence of Corollary 4. Cohen, Manin and Zagier [Cohen et al. 1997] and Yao [2007] (see also Rochberg, Tang and Yao [Rochberg et al. 2011]) proved that the family of Rankin–Cohen brackets is a formal deformation of $\mathcal{M}_*$. In this case, the star product is called the Eholzer product. This subject has been widely studied. See for example [Olver and Sanders 2000; Pevzner 2008].

Can we construct formal deformations of $\mathcal{M}_*^{\leq\infty}$? In other words, can we construct suitable families $(\mu_n)_{n\in\mathbb{N}}$ of bilinear maps on $\mathcal{M}_*^{\leq\infty}$ that increase the weight by $2n$, preserve the depth and define an analogue of the Eholzer product? The brackets defined in (1) do not lead to a solution since RC_1 does not even provide $\mathcal{M}_*^{\leq\infty}$ with a Poisson structure. Our first step is to obtain admissible Poisson brackets on $\mathcal{M}_*^{\leq\infty}$ with the following definition.

Definition 5. A Poisson bracket b on $\mathcal{M}_*^{\leq\infty}$ is admissible if

(1) $\mathrm{b}(f,g) = \mathrm{RC}_1(f,g)$ if f and g are in $\mathcal{M}_*$;

(2) it satisfies $\mathrm{b}(\mathcal{M}_k^{\leq s}, \mathcal{M}_\ell^{\leq t}) \subset \mathcal{M}_{k+\ell+2}^{\leq s+t}$ for all k, ℓ, s, t.

Remark. We could have replaced condition (2) by the following one: there exists $e \geq 0$ such that $\mathrm{b}(\mathcal{M}_k^{\leq s}, \mathcal{M}_\ell^{\leq t}) \subset \mathcal{M}_{k+\ell+e}^{\leq s+t}$ for all k, ℓ, s, t. However, condition (1) implies that necessarily $e = 2$.

Equivalently, a Poisson bracket b on $\mathcal{M}_*^{\leq\infty}$ is admissible if and only if

$$\begin{aligned}
&\mathrm{b}(\mathrm{E}_4, \mathrm{E}_6) = -2\Delta,\\
&\mathrm{b}(\mathrm{E}_2, \mathrm{E}_4) \in \mathcal{M}_8^{\leq\infty}, \quad \mathrm{b}(\mathrm{E}_2, \mathrm{E}_6) \in \mathcal{M}_{10}^{\leq\infty},\\
&\mathrm{b}(\mathrm{E}_2, \mathcal{M}_*) \subset \mathcal{M}_*\mathrm{E}_2 + \mathcal{M}_*.
\end{aligned}$$

In order to classify the admissible Poisson brackets, we introduce the notion of Poisson modular isomorphism.

Definition 6. A Poisson isomorphism $\varphi : (\mathcal{M}_*^{\leq\infty}, \mathrm{b}_1) \to (\mathcal{M}_*^{\leq\infty}, \mathrm{b}_2)$ is called a Poisson modular isomorphism if $\varphi(\mathcal{M}_*) \subset \mathcal{M}_*$.

Indeed, if φ is a Poisson modular isomorphism, then its restriction to the subalgebra $\mathcal{M}_*$ is the identity. This is a consequence of the following proposition.

Proposition 7. *The group of Poisson automorphisms of Poisson algebra* $(\mathcal{M}_*, \mathrm{RC}_1)$ *is trivial.*

Proof. Let φ be a Poisson automorphism of $\mathcal{M}_*$. There exist two polynomials s and t in $\mathbb{C}[x, y]$ such that $\varphi(\mathrm{E}_4) = s(\mathrm{E}_4, \mathrm{E}_6)$ and $\varphi(\mathrm{E}_6) = t(\mathrm{E}_4, \mathrm{E}_6)$. By (2), we have

$$\mathrm{RC}_1(\varphi(\mathrm{E}_4), \varphi(\mathrm{E}_6)) = \mathrm{jac}(s, t)(\mathrm{E}_4, \mathrm{E}_6) \cdot \mathrm{RC}_1(\mathrm{E}_4, \mathrm{E}_6).$$

Since φ is an automorphism, $\mathrm{jac}(s, t)$ is a nonzero scalar, say λ. We get

$$\varphi(\mathrm{RC}_1(\mathrm{E}_4, \mathrm{E}_6)) = \lambda\, \mathrm{RC}_1(\mathrm{E}_4, \mathrm{E}_6) \quad \text{and hence} \quad s^3 - t^2 = \lambda(x^3 - y^2) \quad \text{in } \mathbb{C}[x, y]. \tag{5}$$

We develop s and t into homogeneous components with respect to the weight:

$$s = \sum_{\substack{i=0 \\ i \neq 1}}^{m} s_{2i} \quad \text{and} \quad t = \sum_{\substack{i=0 \\ i \neq 1}}^{n} t_{2i},$$

where

$$s_{2i} = \sum_{\substack{(a,b) \in \mathbb{N}^2 \\ 2a+3b=i}} \sigma_{a,b} x^a y^b \quad \text{and} \quad t_{2i} = \sum_{\substack{(a,b) \in \mathbb{N}^2 \\ 2a+3b=i}} \tau_{a,b} x^a y^b \quad (\sigma_{a,b}, \tau_{a,b} \in \mathbb{C})$$

for all i (where $m = 0$ or $m \geq 2$ and $n = 0$ or $n \geq 2$). Equation (5) implies that $t(\mathrm{E}_4, \mathrm{E}_6)^2 - s(\mathrm{E}_4, \mathrm{E}_6)^3$ has weight 12. Then only three cases are possible.

(1) If $3m > 2n$ then $m = 2$ and so $n \in \{0, 2\}$. This implies that $s = \sigma_{00} + \sigma_{10} x$ and $t = \tau_{00} + \tau_{10} x$. This contradicts $\mathrm{jac}(s, t) \neq 0$.

(2) If $3m < 2n$ then $n = 3$ and $m = 0$. This contradicts $\mathrm{jac}(s, t) \neq 0$.

(3) If $3m = 2n$, we differentiate (5) with respect to x and y and get

$$3s^2 \frac{\partial s}{\partial x} - 2t \frac{\partial t}{\partial x} = 3\lambda x^2, \quad 3s^2 \frac{\partial s}{\partial y} - 2t \frac{\partial t}{\partial y} = -2\lambda y.$$

This implies

$$2t = 3x^2 \frac{\partial s}{\partial y} + 2y \frac{\partial s}{\partial x}, \quad 3s^2 = 3x^2 \frac{\partial t}{\partial y} + 2y \frac{\partial t}{\partial x}. \tag{6}$$

From the first differential equation of (6) we have

$$2t(\mathrm{E}_4, \mathrm{E}_6) = 3\mathrm{E}_4^2 \frac{\partial s}{\partial y}(\mathrm{E}_4, \mathrm{E}_6) + 2\mathrm{E}_6 \frac{\partial s}{\partial x}(\mathrm{E}_4, \mathrm{E}_6).$$

The highest weight of the right-hand side is less than or equal to $2m + 2$. This implies $n \leq m + 1$. From the second differential equation of (6), we have

$$3s^2(\mathrm{E}_4, \mathrm{E}_6) = 3\mathrm{E}_4^2 \frac{\partial t}{\partial y}(\mathrm{E}_4, \mathrm{E}_6) + 2\mathrm{E}_6 \frac{\partial t}{\partial x}(\mathrm{E}_4, \mathrm{E}_6);$$

hence $2m \leq n+1$. We deduce $(m, n) \in \{(0, 0), (2, 3)\}$. Since $n = m = 0$ would imply $\mathrm{jac}(s, t) = 0$, we have $n = 3$ and $m = 2$. Then $s = \sigma_{00} + \sigma_{10} x$ and $t = \tau_{00} + \tau_{10} x + \tau_{01} y$. The first differential equation in (6) implies that $\tau_{00} = \tau_{10} = 0$ and $\tau_{01} = \sigma_{10}$, whereas

the second one implies that $\sigma_{00} = 0$ and $\sigma_{10} = 1$. Finally, $\varphi(\mathrm{E}_4) = s(\mathrm{E}_4, \mathrm{E}_6) = \mathrm{E}_4$ and $\varphi(\mathrm{E}_6) = s(\mathrm{E}_4, \mathrm{E}_6) = \mathrm{E}_6$. □

Since $\mathrm{RC}_1(\Delta, f) = (12\mathrm{D}(f) - kf\mathrm{E}_2)\Delta$ for any $f \in \mathcal{M}_k$, the first Rankin–Cohen bracket defines a derivation on $\mathcal{M}_*$ called Serre's derivative by linear extension of

$$\vartheta f = \frac{\mathrm{RC}_1(\Delta, f)}{12\Delta} = \mathrm{D}(f) - \frac{k}{12} f\mathrm{E}_2 \quad (f \in \mathcal{M}_k). \tag{7}$$

This derivation is characterised by its values on the generators

$$\vartheta \mathrm{E}_4 = -\tfrac{1}{3}\mathrm{E}_6, \quad \vartheta \mathrm{E}_6 = -\tfrac{1}{2}\mathrm{E}_4^2.$$

We shall need the following result.

Proposition 8. *The kernel of Serre's derivative is the Poisson centraliser of* Δ *for the first Rankin–Cohen bracket. This is* $\mathbb{C}[\Delta]$.

Proof. If $f \in \mathcal{M}_k$ is in $\ker \vartheta$ then $kf\mathrm{D}(\Delta) = 12\Delta\mathrm{D}(f)$. Solving the differential equation, we find that 12 divides k and that $f \in \mathbb{C}\Delta^{k/12}$. □

We note that for any $g \in \mathcal{M}_\ell$ we have

$$\mathrm{RC}_1(\Delta^m, g) = m\Delta^m(12\mathrm{D}(g) - \ell g\mathrm{E}_2)$$

and deduce that for any $f \in \mathbb{C}[\Delta]$ and $g \in \mathcal{M}_*$ we have

$$\mathrm{RC}_1(f, g) = 12\xi(f)\vartheta(g), \tag{8}$$

where ξ is the Eulerian derivative on $\mathbb{C}[\Delta]$ defined by $\xi = \Delta\dfrac{\partial}{\partial\Delta}$.

3. Poisson structures on quasimodular forms

3.1. ***First family.*** This section is devoted to the proof of Proposition A.

We fix $\lambda \in \mathbb{C}^*$ and introduce in $\mathbb{C}[x, y, z]$ the three polynomials

$$\begin{aligned} r(x, y, z) &= \tfrac{1}{3}(\lambda y^2 - 2xz), \\ p(x, y, z) &= -2(y^3 - z^2), \\ q(x, y, z) &= -\tfrac{1}{2}(\lambda yz - 2xy^2). \end{aligned}$$

Since $(p, q, r) \cdot \mathrm{curl}(p, q, r) = 0$, we define a Poisson bracket on $\mathcal{M}_*^{\leq\infty}$ if we set

$$\begin{aligned} \{\mathrm{E}_4, \mathrm{E}_6\}_\lambda &= p(\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6), \\ \{\mathrm{E}_2, \mathrm{E}_4\}_\lambda &= r(\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6), \\ \{\mathrm{E}_6, \mathrm{E}_2\}_\lambda &= q(\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6). \end{aligned}$$

Let us prove that $\{\,,\,\}_\lambda$ is not unimodular. If it were, we would have $k \in \mathbb{C}[x, y, z]$ such that $\operatorname{curl}(p, q, r) = (p, q, r) \wedge \operatorname{grad} k$. Identifying the first components would lead to

$$\frac{7}{6}\lambda y = \frac{1}{2}(-\lambda yz + 2y^2 x)\frac{\partial k}{\partial z} - \frac{1}{3}(\lambda y^2 - 2zx)\frac{\partial k}{\partial y},$$

which has no solution in $\mathbb{C}[x, y, z]$.

A Poisson modular isomorphism φ_λ between $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_\lambda)$ and $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_1)$ is determined by

$$\varphi_\lambda(\mathrm{E}_2) = \lambda \mathrm{E}_2, \quad \varphi_\lambda(\mathrm{E}_4) = \mathrm{E}_4, \quad \varphi_\lambda(\mathrm{E}_6) = \mathrm{E}_6.$$

Finally, we determine the Poisson centre of the Poisson algebra $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_1)$. Let us define a derivation on $\mathcal{M}_*$ by $\sigma = 2\vartheta$ (see (7)) and a derivation on $\mathcal{M}_*$ by linear extension of

$$\delta(f) = \frac{k}{12} f \mathrm{E}_4 \quad (f \in \mathcal{M}_k).$$

We note that $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_1)$ is the Poisson–Ore extension $\mathbb{C}[\mathrm{E}_4, \mathrm{E}_6][\mathrm{E}_2]_{\sigma,\delta}$. Now consider any $f \in \mathcal{M}_*^{\leq\infty}$ written as

$$f = \sum_{i=0}^{s} f_i \mathrm{E}_2^i \quad (f_i \in \mathcal{M}_*).$$

We compute

$$\{\mathrm{E}_2, f\}_1 = \delta(f_0) + \sum_{i=1}^{s} (\sigma(f_{i-1}) + \delta(f_i))\mathrm{E}_2^i + \sigma(f_s)\mathrm{E}_2^{s+1}.$$

If $\{\mathrm{E}_2, f\}_1 = 0$ then $\delta(f_0) = 0$, and hence $f_0 \in \mathbb{C}$ and $\sigma(f_0) = 0$. We obtain inductively that $f_i \in \mathbb{C}$ for all $0 \leq i \leq s$, so the Poisson centraliser of E_2 is $\mathbb{C}[\mathrm{E}_2]$. Suppose that the Poisson centre contains a nonscalar element. Then it is in the Poisson centraliser of E_2 and can be written

$$f = \sum_{j=0}^{p} \alpha_j \mathrm{E}_2^j \quad (p \geq 1,\ \alpha_j \in \mathbb{C},\ \alpha_p \neq 0).$$

We compute

$$\{\mathrm{E}_4, f\}_1 = \sum_{j=0}^{p} j\alpha_j \mathrm{E}_2^{j-1} \cdot \{\mathrm{E}_4, \mathrm{E}_2\}_1$$

and find that the coefficient of E_2^p is nonzero. It follows that f is not in the Poisson centre.

3.2. ***Second family.*** This section is devoted to the proof of Proposition C. We fix $\alpha \in \mathbb{C}$ and introduce in $\mathbb{C}[x, y, z]$ the three polynomials

$$\begin{aligned} r(x, y, z) &= \alpha xz, \\ p(x, y, z) &= -2(y^3 - z^2), \\ q(x, y, z) &= -\tfrac{3}{2}\alpha xy^2. \end{aligned}$$

Since $(p, q, r) \cdot \operatorname{curl}(p, q, r) = 0$, we define a Poisson bracket on $\mathcal{M}_*^{\leq\infty}$ if we set

$$\begin{aligned} (\mathrm{E}_4, \mathrm{E}_6)_\alpha &= p(\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6), \\ (\mathrm{E}_2, \mathrm{E}_4)_\alpha &= r(\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6), \\ (\mathrm{E}_6, \mathrm{E}_2)_\alpha &= q(\mathrm{E}_2, \mathrm{E}_4, \mathrm{E}_6). \end{aligned}$$

Assume $\alpha \neq 4$. Let us prove that $(\,,\,)_\alpha$ is not unimodular. If it were, we would have $k \in \mathbb{C}[x, y, z]$ such that $\operatorname{curl}(p, q, r) = (p, q, r) \wedge \operatorname{grad} k$. Identifying the second components would lead to

$$(4 - \alpha)z = \alpha xz \frac{\partial k}{\partial x} + 2(y^3 - z^2)\frac{\partial k}{\partial z},$$

which has no solution in $\mathbb{C}[x, y, z]$.

If $\alpha = 4$, then $(p, q, r) = \operatorname{grad} k_0$, where $k_0 = -2(y^3 - z^2)x$. As a consequence, the bracket $(\,,\,)_4$ provides $\mathcal{M}_*^{\leq\infty}$ with a Jacobian Poisson structure of potential $k_0 = -2\Delta\mathrm{E}_2 = -2\mathrm{D}(\Delta)$.

If $\varphi : (\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha) \to (\mathcal{M}_*^{\leq\infty}, (\,,\,)_{\alpha'})$ is a Poisson modular isomorphism, let us prove that $\alpha = \alpha'$. By Proposition 7, we have $\varphi(\mathrm{E}_4) = \mathrm{E}_4$ and $\varphi(\mathrm{E}_6) = \mathrm{E}_6$. By surjectivity, it follows that $\varphi(\mathrm{E}_2) = \eta\mathrm{E}_2 + F$ for some $\eta \in \mathbb{C}^*$ and $F \in \mathcal{M}_*$. We compute

$$\varphi((\mathrm{E}_2, \mathrm{E}_4)_\alpha) = \alpha\eta\mathrm{E}_6\mathrm{E}_2 + \alpha\mathrm{E}_6 F$$

and

$$(\varphi(\mathrm{E}_2), \varphi(\mathrm{E}_4))_{\alpha'} = \alpha'\eta\mathrm{E}_6\mathrm{E}_2 + (F, \mathrm{E}_4)_{\alpha'}.$$

Since $(F, \mathrm{E}_4)_{\alpha'} \in \mathcal{M}_*$ we get $\alpha' = \alpha$.

Finally, we determine the Poisson centre of the Poisson algebra $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$. We note that $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$ is the Poisson–Ore extension $\mathbb{C}[\mathrm{E}_4, \mathrm{E}_6][\mathrm{E}_2]_{\sigma,\delta}$, where $\sigma = -3\alpha\vartheta$ (see (7)) and $\delta = 0$. Let

$$f = \sum_{j=0}^{s} f_j \mathrm{E}_2^j \quad (f_j \in \mathcal{M}_*).$$

We have

$$(\mathrm{E}_2, f)_\alpha = \sum_{j=0}^{s} \sigma(f_j)\mathrm{E}_2^{j+1},$$

and hence f is in the Poisson centraliser of E_2 if and only if each f_j is in the Poisson centraliser of Δ for RC_1. By Proposition 8, we deduce that the centraliser of E_2 is $\mathbb{C}[\Delta, E_2]$. Let

$$f = \sum_{j=0}^{s} f_j(\Delta) E_2^j \in \mathbb{C}[\Delta, E_2].$$

We use (8) to compute

$$(f, E_4)_\alpha = \sum_{j=0}^{s} (-4\xi(f_j) + j\alpha f_j) E_6 E_2^j,$$

$$(f, E_6)_\alpha = \tfrac{3}{2} \sum_{j=0}^{s} (-4\xi(f_j) + j\alpha f_j) E_4^2 E_2^j.$$

We deduce that f is in the Poisson centre of $(\,,\,)_\alpha$ if and only if

$$\xi(f_j) = \frac{j\alpha}{4} f_j$$

for all j, that is, if and only if any f_j is of the form $f_j = \lambda_j \Delta^{m_j}$ for some $\lambda_j \in \mathbb{C}$ and $m_j \in \mathbb{N}$ such that $j\alpha = 4m_j$. If $\alpha \notin \mathbb{Q}$ or if $\alpha < 0$ then $j = 0$ and $m_j = 0$, and hence $f = f_0 \in \mathbb{C}$. If $\alpha = p/q$ with $p \geq 1$, $q \geq 1$ and $(p, q) = 1$, then $\lambda \Delta^{m_j} E_2^j$ is in the Poisson centre if and only if $pj = 4qm_j$. The result follows by obvious arithmetical consideration. Finally, if $\alpha = 0$, then $(\,,\,)_0$ is the trivial bracket and its Poisson centre is $\mathbb{C}[E_2]$.

3.3. ***Third family.*** In this section, we study the third family, that is, we prove Proposition E.

For any $\mu \in \mathbb{C}$, let us introduce

$$k_\mu = -2\Delta E_2 + \mu E_4^2 E_6.$$

Then

$$\mathrm{jac}(E_4, E_6, k_\mu) = \frac{\partial k_\mu}{\partial E_2} = -2E_4^3 + 2E_6^2,$$

$$\mathrm{jac}(E_2, E_4, k_\mu) = \frac{\partial k_\mu}{\partial E_6} = 4E_6 E_2 + \mu E_4^2,$$

$$\mathrm{jac}(E_2, E_6, k_\mu) = -\frac{\partial k_\mu}{\partial E_4} = 6E_4^2 E_2 - 2\mu E_4 E_6.$$

The third family of Poisson brackets is then defined by $\langle f, g\rangle_\mu = \mathrm{jac}(f, g, k_\mu)$. With the notation of Proposition C, we have in particular $\langle f, g\rangle_0 = (f, g)_4$.

For any $\mu \in \mathbb{C}^*$, define a Poisson modular isomorphism φ_μ between $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_\mu)$ and $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_1)$ by setting $\varphi_\mu(E_2) = \mu E_2$, $\varphi_\mu(E_4) = E_4$ and $\varphi_\mu(E_6) = E_6$.

Since the degree in E_2 of k_μ as a polynomial in E_2, E_4, E_6 is 1, Lemma 1 implies that the Poisson centre of $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_\mu)$ is $\mathbb{C}[k_\mu]$.

3.4. ***Classification.*** This section is devoted to the proof of Theorem F.

Let $\{\,,\,\}$ be an admissible bracket on $\mathcal{M}_*^{\leq\infty}$. By Definition 5 and Theorem 2, there exist a Poisson derivation σ of $\mathcal{M}_*$ and a Poisson σ-derivation δ of $\mathcal{M}_*$ such that

$$\{E_2, f\} = \sigma(f)E_2 + \delta(f) \quad (f \in \mathcal{M}_*).$$

By definition, $\sigma(\mathcal{M}_k) \subset \mathcal{M}_{k+2}$ and $\delta(\mathcal{M}_k) \subset \mathcal{M}_{k+4}$ for any k. The admissible bracket $\{\,,\,\}$ is then defined by the four scalars α, β, γ and ε such that

$$\sigma(E_4) = \alpha E_6, \quad \delta(E_4) = \beta E_4^2, \quad \sigma(E_6) = \gamma E_4^2 \quad \text{and} \quad \delta(E_6) = \varepsilon E_4 E_6.$$

The condition that σ is a Poisson derivation imposes the condition

$$\{\sigma(E_4), E_6\} + \{E_4, \sigma(E_6)\} = -2\sigma(E_4^3 - E_6^2),$$

or equivalently, $3\alpha = 2\gamma$. The condition that δ is a Poisson σ-derivation imposes

$$\delta(\{E_4, E_6\}) = (2\beta + \varepsilon)E_4\{E_4, E_6\} + \alpha\varepsilon E_4 E_6^2 - \beta\gamma E_4^4,$$

or equivalently,

$$\begin{cases} 4\beta + (\alpha - 2)\varepsilon = 0, \\ (3\alpha - 4)\beta + 4\varepsilon = 0. \end{cases}$$

Either $\beta = \varepsilon = 0$ is the only solution, or $\alpha \in \left\{-\frac{2}{3}, 4\right\}$ and $\varepsilon = \dfrac{4}{2-\alpha}\beta$.

- The case $\beta = \varepsilon = 0$ leads to the second family: $\{\,,\,\} = (\,,\,)_\alpha$.
- The case $\alpha = -\frac{2}{3}$ and $\varepsilon = 3\beta/2 \neq 0$ leads to the first family: $\{\,,\,\} = \{\,,\,\}_{3\beta}$.
- The case $\alpha = 4$ and $\varepsilon = -2\beta \neq 0$ leads to the third family: $\{\,,\,\} = \langle\,,\,\rangle_\beta$.

Using Propositions C and E, we conclude that the only admissible Poisson brackets, up to Poisson modular isomorphisms, are $\{\,,\,\}_1$, $\langle\,,\,\rangle_1$ and $(\,,\,)_\alpha$ for any $\alpha \in \mathbb{C}$. Looking at the centres, it is clear that the Poisson algebras $(\mathcal{M}_*^{\leq\infty}, \langle\,,\,\rangle_1)$ and $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_1)$ are not Poisson modular isomorphic. Suppose that there exists a Poisson modular isomorphism φ from $(\mathcal{M}_*^{\leq\infty}, (\,,\,)_\alpha)$ to $(\mathcal{M}_*^{\leq\infty}, \{\,,\,\}_1)$. We know (see Section 3.2) that

$$\varphi(E_4) = E_4, \quad \varphi(E_6) = E_6 \quad \text{and} \quad \varphi(E_2) = \eta E_2 + F$$

for some $\eta \in \mathbb{C}^*$ and $F \in \mathcal{M}_*$. From $\varphi((E_2, E_4)_\alpha) = \{\varphi(E_2), \varphi(E_4)\}_1$ we obtain

$$\alpha\eta E_6 E_2 + \alpha F E_6 = -\frac{2}{3}\eta E_6 E_2 + \frac{1}{3}\eta E_4^2 + \{F, E_4\}_1,$$

and hence

$$\alpha = -\frac{2}{3}, \quad \frac{1}{3}\eta E_4^2 = -\frac{2}{3}F E_6 - \{F, E_4\}_1 = -\frac{2}{3}F E_6 + 2(E_4^3 - E_6^2)\frac{\partial F}{\partial E_6}$$

by (2). We get a contradiction. Replacing $\{\,,\,\}_1$ by $\langle\,,\,\rangle_1$, we get

$$\alpha = 4, \quad \eta \mathrm{E}_4^2 = 4F\mathrm{E}_6 - 2(\mathrm{E}_4^3 - \mathrm{E}_6^2)\frac{\partial F}{\partial \mathrm{E}_6},$$

and again we get a contradiction.

4. Star products on quasimodular forms

4.1. ***Extension of the first family.*** This section is devoted to proving Theorem B. We will use the following result of Zagier [1994, Example 1]. Let $A = \bigoplus A_k$ be a commutative graded algebra with a derivation d homogeneous of degree 2 (that is, $\mathrm{d}(A_k) \subset A_{k+2}$). Let us define, for any $f \in A_k$, $g \in A_\ell$, $r \geq 0$:

$$[f, g]_{d,r} = \sum_{i=0}^{r} (-1)^i \binom{k+r-1}{r-i} \binom{\ell+r-1}{i} \mathrm{d}^i(f)\mathrm{d}^{r-i}(g) \in A_{k+\ell+2r}. \tag{9}$$

Then A equipped with these brackets is a Rankin–Cohen algebra, which means that all algebraic identities satisfied by the usual Rankin–Cohen brackets on modular forms are also satisfied, in particular those expressing the associativity of the corresponding star product. We obtain the following result.

Theorem 9. *The star product defined by*

$$f \# g = \sum_{n \geq 0} [f, g]_{\mathrm{d},n} \hbar^n$$

defines a formal deformation on A.

In particular, we recover the fact, given by Corollary 4, that $[\,,\,]_{\mathrm{d},1}$ is a Poisson bracket. Note also that this theorem can be obtained from Connes and Moscovici's result cited below (see Section 4.2).

Let $a \in \mathbb{C}$ and d_a be the homogeneous derivation of degree 2 on $\mathcal{M}_*^{\leq\infty}$ defined by

$$\mathrm{d}_a(\mathrm{E}_2) = 2a\mathrm{E}_2^2 - \tfrac{1}{12}\mathrm{E}_4, \quad \mathrm{d}_a(\mathrm{E}_4) = 4a\mathrm{E}_4\mathrm{E}_2 - \tfrac{1}{3}\mathrm{E}_6, \quad \mathrm{d}_a(\mathrm{E}_6) = 6e\mathrm{E}_6\mathrm{E}_2 - \tfrac{1}{2}\mathrm{E}_4^2.$$

A direct computation proves that the two Poisson brackets $[\,,\,]_{\mathrm{d}_a,1}$ and $\{\,,\,\}_1$ coincide on generators and hence are equal on $\mathcal{M}_*^{\leq\infty}$.

Remark. A derivation d on $\mathcal{M}_*^{\leq\infty}$ is complex-like if $\mathrm{d}\mathcal{M}_k^{\leq s} \subset \mathcal{M}_{k+2}^{\leq s+1}$ for all k and s. Let π be the derivation on $\mathcal{M}_*^{\leq\infty}$ defined by linear extension of $\pi(f) = kf\mathrm{E}_2$ for all $f \in \mathcal{M}_k^{\leq\infty}$. The set of complex-like derivations d such that $[\,,\,]_{\mathrm{d},1} = 0$ is the vector space of dimension 1 over $\mathbb{C}$ generated by π. Let us define w on $\mathcal{M}_*^{\leq\infty}$ by

$$\mathrm{w}(f) = \frac{\{\Delta, f\}_1}{12\Delta}.$$

Then

$$\mathrm{d}_a = \mathrm{w} + a\delta.$$

This implies in particular that if a complex-like derivation d satisfies $[\,,\,]_{\mathrm{d},1} = \{\,,\,\}_1$, then $\mathrm{d} = \mathrm{d}_a$ for some $a \in \mathbb{C}$.

Point (ii) of Theorem B is obtained by a direct application of Theorem 9. We prove now (iii). The term of highest degree with respect to E_2 in $[\mathrm{E}_2, \mathrm{E}_4]_{\mathrm{d}_a,2}$ is $8a^2\mathrm{E}_4\mathrm{E}_2^3$. This forces $a = 0$. Conversely, if $a = 0$, then $\mathrm{d}_0\mathcal{M}_*^{\leq\infty} \subset \mathcal{M}_*$. For any $f = f_i\mathrm{E}_2^i$ with $f_i \in \mathcal{M}_*$, we have

$$\mathrm{d}_0(f) = \mathrm{d}_0(f_i)\mathrm{E}_2^i - \tfrac{1}{12} i f_i \mathrm{E}_4 \mathrm{E}_2^{i-1},$$

and hence $\deg_{\mathrm{E}_2} \mathrm{d}_0(f) \leq \deg_{\mathrm{E}_2} f$ and $\deg_{\mathrm{E}_2} \mathrm{d}_0^j(f) \leq \deg_{\mathrm{E}_2} f$ for any $f \in \mathcal{M}_*^{\leq\infty}$ and $j \geq 0$. This implies that

$$[\mathcal{M}_k^{\leq s}, \mathcal{M}_\ell^{\leq t}]_{\mathrm{d}_0,n} \subset \mathcal{M}_{k+\ell+2n}^{\leq s+t}.$$

4.2. ***Extension of the second family.*** The aim of this section is to prove Theorem D. The proof of (i) is similar to the proof of (i) in Theorem B. Let $\mathcal{H} : \mathcal{M}_*^{\leq\infty} \to \mathbb{C}$ be a graded-additive map. For any integer $n \geq 0$, we define a bilinear application $[\,,\,]_{\mathrm{d},n}^{\mathcal{H}}$ by bilinear extension of

$$[f, g]_{\mathrm{d},n}^{\mathcal{H}} = \sum_{r=0}^{n} (-1)^r \binom{\mathcal{H}(f)+n-1}{n-r} \binom{\mathcal{H}(g)+n-1}{r} \mathrm{d}^r f\, \mathrm{d}^{n-r} g.$$

By Corollary 4, we know that $[f, g]_{\mathrm{d},1}^{\mathcal{H}}$ is a Poisson bracket.

Let us fix $\mathcal{H}_\alpha$ to be the linear extension on $\mathcal{M}_*^{\leq\infty} = \bigoplus_k \bigoplus_s \mathcal{M}_k^s$ of

$$\mathcal{H}_\alpha(f) = (k - (3\alpha + 2)s) \quad (f \in \mathcal{M}_k^s). \tag{10}$$

Let π_α be the derivation on $\mathcal{M}_*^{\leq\infty}$ defined by $\pi_\alpha(f) = \mathcal{H}_\alpha(f) f \mathrm{E}_2$ for all $f \in \mathcal{M}_*^{\leq\infty}$. The set of complex-like derivations such that $[\,,\,]_{\mathrm{d},1}^{\mathcal{H}_\alpha} = 0$ is the vector space of dimension 1 over $\mathbb{C}$ generated by π_α. Define derivations v and $\delta_{\alpha,b}$ on $\mathcal{M}_*^{\leq\infty}$ by

$$\mathrm{v}(f) = \frac{(\Delta, f)_\alpha}{12\Delta}$$

and

$$\delta_{\alpha,b} = \mathrm{v} + b\pi_\alpha.$$

Note that v does not depend on α. By comparing the values on the generators, it is immediate that $(\,,\,)_\alpha = [\,,\,]_{\delta_{\alpha,b},1}^{\mathcal{H}_\alpha}$.

Remark. Direct computations show that if d is a homogeneous derivation of degree 2 and $\mathcal{H}$ is such that $(\,,\,)_\alpha = [\,,\,]_{\mathrm{d},1}^{\mathcal{H}}$, then we necessarily have $\mathcal{H} = \mathcal{H}_\alpha$ and $\mathrm{d} = \delta_{\alpha,b}$ for some $b \in \mathbb{C}$.

The condition that $[\mathrm{E}_4, \mathrm{E}_6]_{\delta_{\alpha,b},2}^{\mathcal{H}}$ has to be a modular form implies $b = 0$ or $\alpha = -\frac{1}{3}$. For $\alpha = -\frac{1}{3}$, condition (4) for $\mu_r = [\,,\,]_{\delta_{\alpha,b},r}^{\mathcal{H}}$ and $n = 3$ is not satisfied

(this can be shown with computer assistance, for example with Sage [Stein et al. 2013]). We assume then that $b = 0$.

Connes and Moscovici [2004, Remark 14] (see also [Yao 2007, §II.2] for a nice presentation of this result) proved that if E and H are two derivations of an algebra R such that $HE - EH = E$, then the applications $\mu_n : R \times R \to R$ defined by

$$\mu_n(f,g) = \sum_{r=0}^{n} \frac{(-1)^r}{r!(n-r)!} [E^r \circ (2H+r)^{\langle n-r\rangle}(f)] \cdot [E^{n-r} \circ (2H+n-r)^{\langle r\rangle}(g)] \quad (11)$$

define a formal deformation on R with the notation

$$F^{\langle m\rangle} = F \circ (F+1) \circ (F+2) \circ \cdots \circ (F+m-1).$$

Let ϖ be the derivation defined on $\mathcal{M}_*^{\leq\infty}$ by $\varpi(f) = \mathcal{H}(f) f$. Then we have

$$\varpi \circ \delta_{\alpha,0} - \delta_{\alpha,0} \circ \varpi = 2\delta_{\alpha,0}.$$

We use Connes and Moscovici's result with $E = \delta_{\alpha,0}$ and $H = \varpi/2$ to obtain

$$\mu_n(f,g) = \sum_{r=0}^{n} (-1)^r \binom{k-(3\alpha+2)s+n-1}{n-r} \binom{\ell-(3\alpha+2)t+n-1}{r} \delta_{\alpha,0}^r(f) \delta_{\alpha,0}^{n-r}(g).$$

This implies Theorem D.

Remark. We could have applied Connes and Moscovici's result to extend the first family. Indeed Zagier's result is a consequence of Connes and Moscovici's. Let d be a derivation homogeneous of degree 2 of the commutative graded algebra $A = \bigoplus A_k$. It is obvious that the linear map defined on each A_k by $H(f) = (k/2) f$ is a derivation of A. It is also clear that it satisfies $H \circ d - d \circ H = d$. In particular, for any $f \in A_k$ and $g \in A_\ell$ we calculate

$$(2H+r)^{\langle n-r\rangle}(f) = \frac{(k+n-1)!}{(k+r-1)!} f,$$
$$(2H+(n-r))^{\langle r\rangle}(g) = \frac{(\ell+n-1)!}{(\ell+n-r-1)!} g.$$

Hence a direct application of formula (11) gives formula (9).

4.3. ***Extension of the third family.*** We do not extend the third family, since for $\mu \neq 0$, the bracket $\langle\,,\,\rangle_\mu$ does not have the shape of a Rankin–Cohen bracket. More precisely, if there exist a function $\kappa : \mathcal{M}_*^{\leq\infty} \to \mathbb{C}$ and a complex-like derivation δ of $\mathcal{M}_*^{\leq\infty}$ such that

$$\langle f, g\rangle_\mu = \kappa(f) f \delta(g) - \kappa(g) g \delta(f)$$

for all f and g in $\mathcal{M}_*^{\leq\infty}$, then $\mu = 0$. Indeed, assume κ and δ exist; then

$$\begin{cases} \delta(\mathrm{E}_2) = A\mathrm{E}_2^2 + B\mathrm{E}_4, \\ \delta(\mathrm{E}_4) = C\mathrm{E}_4\mathrm{E}_2 + D\mathrm{E}_6, \\ \delta(\mathrm{E}_6) = E\mathrm{E}_6\mathrm{E}_2 + F\mathrm{E}_4^2 \end{cases}$$

for some complex numbers A, B, C, D, E and F. Since we know the values of $\langle\,,\rangle_\mu$ on the generators, we get a system depending on A, B, C, D, E, F, $\kappa(\mathrm{E}_2)$, $\kappa(\mathrm{E}_4)$ and $\kappa(\mathrm{E}_6)$. It is not difficult to prove that this system has a solution if and only if $\mu = 0$.

References

[Bieliavsky et al. 2007] P. Bieliavsky, X. Tang, and Y.-J. Yao, "Rankin–Cohen brackets and formal quantization", *Adv. Math.* **212**:1 (2007), 293–314. MR 2008f:53125 Zbl 1123.53049

[Cohen 1975] H. Cohen, "Sums involving the values at negative integers of L-functions of quadratic characters", *Math. Ann.* **217**:3 (1975), 271–285. MR 52 #3080 Zbl 0311.10030

[Cohen et al. 1997] P. B. Cohen, Y. Manin, and D. Zagier, "Automorphic pseudodifferential operators", pp. 17–47 in *Algebraic aspects of integrable systems: in memory of Irene Dorfman*, edited by A. S. Fokas and I. M. Gelfand, Progr. Nonlinear Differential Equations Appl. **26**, Birkhäuser, Boston, 1997. MR 98e:11054 Zbl 1055.11514

[Connes and Moscovici 2004] A. Connes and H. Moscovici, "Rankin–Cohen brackets and the Hopf algebra of transverse geometry", *Mosc. Math. J.* **4**:1 (2004), 111–130. MR 2005f:11079b Zbl 1122.11024

[Dufour and Haraki 1991] J.-P. Dufour and A. Haraki, "Rotationnels et structures de Poisson quadratiques", *C. R. Acad. Sci. Paris Sér. I Math.* **312**:1 (1991), 137–140. MR 92a:53045 Zbl 0719.58001

[Gutierrez and Sevilla 2006] J. Gutierrez and D. Sevilla, "Computation of unirational fields", *J. Symbolic Comput.* **41**:11 (2006), 1222–1244. MR 2007g:12003 Zbl 1149.12001

[Kobayashi and Pevzner 2013] T. Kobayashi and M. Pevzner, "Rankin–Cohen operators for symmetric pairs", preprint, 2013. arXiv 1301.2111

[Laurent-Gengoux et al. 2013] C. Laurent-Gengoux, A. Pichereau, and P. Vanhaecke, *Poisson structures*, Grundlehren der Mathematischen Wissenschaften **347**, Springer, Heidelberg, 2013. MR 2906391 Zbl 1271.53074

[Martin and Royer 2005] F. Martin and E. Royer, "Formes modulaires et périodes", pp. 1–117 in *Formes modulaires et transcendance* (Marseille, 2003), edited by S. Fischler et al., Sémin. Congr. **12**, Soc. Math. France, Paris, 2005. MR 2007a:11065 Zbl 1104.11017

[Martin and Royer 2009] F. Martin and E. Royer, "Rankin–Cohen brackets on quasimodular forms", *J. Ramanujan Math. Soc.* **24**:3 (2009), 213–233. MR 2011d:11094 Zbl 1206.11052

[Monnier 2002] P. Monnier, "Poisson cohomology in dimension two", *Israel J. Math.* **129** (2002), 189–207. MR 2003h:53117 Zbl 1077.17018

[Oh 2006] S.-Q. Oh, "Poisson polynomial rings", *Comm. Algebra* **34**:4 (2006), 1265–1277. MR 2007g:17021 Zbl 1135.17012

[Olver and Sanders 2000] P. J. Olver and J. A. Sanders, "Transvectants, modular forms, and the Heisenberg algebra", *Adv. in Appl. Math.* **25**:3 (2000), 252–283. MR 2001j:11016 Zbl 1041.11026

[Pevzner 2008] M. Pevzner, "Rankin–Cohen brackets and associativity", *Lett. Math. Phys.* **85**:2-3 (2008), 195–202. MR 2010i:53176 Zbl 1167.53075

[Pevzner 2012] M. Pevzner, "Rankin–Cohen brackets and representations of conformal Lie groups", *Ann. Math. Blaise Pascal* **19**:2 (2012), 455–484. MR 3025141 Zbl 1283.11072

[Pichereau 2006a] A. Pichereau, *(Co)homologie de Poisson et singularités isolées en petites dimensions, avec une application en théorie des déformations*, thesis, Université de Poitiers, Poitiers, 2006, Available at http://dossier.univ-st-etienne.fr/pa11405h/www/PagePersoAP/These_files/fichier.pdf.

[Pichereau 2006b] A. Pichereau, "Poisson (co)homology and isolated singularities", *J. Algebra* **299**:2 (2006), 747–777. MR 2007k:17026 Zbl 1113.17009

[Rochberg et al. 2011] R. Rochberg, X. Tang, and Y.-J. Yao, "A survey on Rankin–Cohen deformations", pp. 133–151 in *Perspectives on noncommutative geometry* (Toronto, ON, 2008), edited by M. Khalkhali and G. Yu, Fields Inst. Commun. **61**, Amer. Math. Soc., Providence, RI, 2011. MR 2838685 Zbl 05994726

[Roger and Vanhaecke 2002] C. Roger and P. Vanhaecke, "Poisson cohomology of the affine plane", *J. Algebra* **251**:1 (2002), 448–460. MR 2003g:17031 Zbl 0998.17023

[Stein et al. 2013] W. A. S. Stein et al., "Sage mathematics software", The Sage Development Team, 2013, Available at http://www.sagemath.org. Version 5.6.

[Unterberger and Unterberger 1996] A. Unterberger and J. Unterberger, "Algebras of symbols and modular forms", *J. Anal. Math.* **68** (1996), 121–143. MR 97i:11044 Zbl 0857.43015

[Yao 2007] Y.-J. Yao, *Autour des déformations de Rankin–Cohen*, thesis, École Polytechnique, Centre de Mathématiques Laurent Schwartz, Paris, 2007, Available at http://pastel.archives-ouvertes.fr/pastel-00002414.

[Zagier 1994] D. Zagier, "Modular forms and differential operators", *Proc. Indian Acad. Sci. Math. Sci.* **104**:1 (1994), 57–75. MR 95d:11048 Zbl 0806.11022

[Zagier 2008] D. Zagier, "Elliptic modular forms and their applications", pp. 1–103 in *The 1-2-3 of modular forms*, edited by K. Ranestad, Springer, Berlin, 2008. MR 2010b:11047 Zbl 1259.11042

Communicated by Yuri Manin
Received 2013-07-26 Revised 2014-01-20 Accepted 2014-03-24

francois.dumas@math.univ-bpclermont.fr
Clermont Université, Université Blaise Pascal, Laboratoire de mathématiques, BP 10448, F-63000 Clermont-Ferrand, France

Current address: *Université Blaise Pascal, Laboratoire de mathématiques, Les Cézeaux, BP 80026, F-63171 Aubière, France*

emmanuel.royer@math.univ-bpclermont.fr
Clermont Université, Université Blaise Pascal, Laboratoire de mathématiques, BP 10448, F-63000 Clermont-Ferrand, France

Current address: *Université Blaise Pascal, Laboratoire de mathématiques, Les Cézeaux, BP 80026, F-63171 Aubière, France*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1151

msp

Affinity of Cherednik algebras on projective space

Gwyn Bellamy and Maurizio Martino

We give sufficient conditions for the affinity of Etingof's sheaves of Cherednik algebras on projective space. To do this, we introduce the notion of pullback of modules under certain flat morphisms.

1. Introduction

1.1. In a seminal paper, Etingof and Ginzburg [2002] introduced the family of rational Cherednik algebras associated to a complex reflection group. Since their introduction, rational Cherednik algebras have been intensively studied, and found to be related to several other areas of mathematics. Their definition was vastly generalized in [Etingof 2004]. Given any smooth variety X and finite group W acting on X, Etingof defines a family of sheaves[1] of algebras $\mathscr{H}_{\omega,\mathbf{c}}(X, W)$ on X which are flat deformations of the skew group ring $\mathscr{D}_X \rtimes W$. Being sheaves of algebras, one would like to be able to use standard geometric techniques such as pullback and pushforward to study their representation theory. This paper is a small first step in developing these techniques. As motivation, we consider the question of affinity for these algebras when $X = \mathbb{P}(V)$.

MSC2010: primary 20C08; secondary 16S80.
Keywords: rational Cherednik algebras, localization theory.

[1] Here, one must take the W-equivariant Zariski topology on X. See Section 2.1.

1.2. If V is a finite-dimensional vector space and W acts linearly on V, then there is an induced action of W on $\mathbb{P}(V)$. Thus, Etingof's construction gives us a sheaf of algebras $\mathscr{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ on $\mathbb{P}(V)$. In trying to understand the representation theory of these algebras, one would like to know when they are affine, i.e., for which ω and $\mathbf{c}$ does the global sections functor give us an equivalence between the category of modules for $\mathscr{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ and the category of modules for its global sections $\mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$. Our main result is an explicit combinatorial criterion on ω and $\mathbf{c}$ which guarantees that the corresponding Cherednik algebra is affine. We associate to ω, $\mathbf{c}$ and $\lambda \in \operatorname{Irr} W$ a pair of scalars a_λ, b_λ; see Section 5.5.

Theorem 1.2.1. *The sheaf of algebras $\mathscr{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ is affine provided $a_\lambda \notin \mathbb{Z}_{\geq 0}$ and $b_\lambda \notin \mathbb{Z}_{>0}$ for all $\lambda \in \operatorname{Irr} W$.*

In order to prove this result, we introduce two key pieces of machinery. The first is the notion of pullback of $\mathscr{H}_{\omega,\mathbf{c}}$-modules under certain well-behaved maps (which we call melys). The second is to establish an equivalence between the category of (twisted) T-equivariant $\mathscr{H}_{\mathbf{c}}$-modules on a principal T-bundle $Y \to X$ and the category of modules for a Cherednik algebra $\mathscr{H}_{\omega,\mathbf{c}}$ on the base X of the bundle. With this machinery in place, the proof of the main result is essentially the same as for sheaves of twisted differential operators on $\mathbb{P}(V)$; see [Hotta et al. 2008, Theorem 1.6.5].

1.3. Being able to pull back D-modules is an extremely useful tool in studying the representation theory of sheaves of differential operators. Therefore, one would like to be able to do the same for Cherednik algebras. We show that this is possible, at least for some morphisms. A W-equivariant map $\varphi : Y \to X$ between smooth varieties is said to be *melys* if it is flat and, for all reflections (w, Z) in X, $\varphi^{-1}(Z)$ is contained in the fixed point set Y^w of w.

Theorem 1.3.1. *If $\varphi : Y \to X$ is melys, then pullback is an exact functor*

$$\varphi^* : \mathscr{H}_{\omega,\mathbf{c}}(X, W)\text{-Mod} \longrightarrow \mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)\text{-Mod}.$$

The pullback functor is particularly well behaved when φ is étale. We define the melys site over X, a certain modification of the usual étale site over X. Using Theorem 1.3.1, we show that the Cherednik algebra forms a sheaf on this site.

One particularly rich source of melys morphisms is when $\pi : Y \to X$ is a principal T-bundle, where T is a torus acting on Y with the action commuting with the action of W. In this situation, one can perform quantum Hamiltonian reduction of the Cherednik algebra $\mathscr{H}_{\mathbf{c}}(Y, W)$ on Y to get a sheaf $\mathscr{H}_{\beta(\chi),\mathbf{c}}(X, W)$ of Cherednik algebras on X. As a consequence, one gets an equivalence between the category of (χ-twisted) T-equivariant $\mathscr{H}_{\mathbf{c}}(Y, W)$-modules on Y and the category of $\mathscr{H}_{\beta(\chi),\mathbf{c}}(X, W)$-modules on X.

Theorem 1.3.2. *Let $\chi \in \mathfrak{t}^*$. We have an isomorphism of sheaves of algebras on X*

$$\mathscr{H}_{\beta(\chi),\mathbf{c}}(X, W) \simeq (\pi_\bullet \mathscr{H}_{\mathbf{c}}(Y, W))^T / \langle \{t - \chi(t) \mid t \in \mathfrak{t}\} \rangle,$$

and the functor

$$(\mathscr{H}_{\mathbf{c}}(X, W), T, \chi)\text{-Mod} \longrightarrow \mathscr{H}_{\beta(\chi),\mathbf{c}}(Y, W)\text{-Mod}$$

given by $\mathcal{M} \mapsto (\pi_\bullet \mathcal{M})^T$ is an equivalence of categories, with quasi-inverse $\mathcal{N} \mapsto \pi^* \mathcal{N}$.

1.4. We also study a natural generalization of the Knizhnik–Zamolodchikov connection. The question of whether the Knizhnik–Zamolodchikov connection is flat is closely related to the issue of presenting the Cherednik algebra. In the appendix, we summarize for the reader unfamiliar with sheaves of twisted differential operators (TDOs) those basic properties that we require.

2. Sheaves of Cherednik algebras

In this section we introduce sheaves of Cherednik algebras on a smooth variety.

2.1. ***Conventions.*** Throughout, all our spaces will be equipped with the action of a finite group W. We do not assume that this action is effective. The morphisms $\varphi : Y \to X$ that we will consider will always be assumed to be W-equivariant. Since we wish to deal with objects such as $\mathbb{O}_X \rtimes W$, we work throughout with the *W-equivariant Zariski topology*: a subset $U \subset X$ is an open subset in this topology if and only if it is open in the Zariski topology and W-stable. Then, $\mathbb{O}_X \rtimes W$ becomes a sheaf on X. If $w \in W$, then X^w denotes the set of all points fixed under the automorphism w. The sheaf of vector fields (resp. one-forms) on a smooth variety X is denoted by Θ_X (resp. Ω^1_X).

2.2. Let X be a smooth, connected, quasiprojective variety over $\mathbb{C}$. Let Z be a smooth subvariety of X of codimension one. Locally, the ideal defining Z is principal, generated by one section, f_Z say. Then, the element

$$d \log f_Z := \frac{df_Z}{f_Z}$$

is a section of $\Omega^1_X(Z) = \Omega^1_X \otimes \mathbb{O}_X(Z)$. Contraction defines a pairing

$$\Theta_X \otimes \Omega^1_X(Z) \to \mathbb{O}_X(Z), \quad (\nu, \omega) \mapsto i_\nu(\omega).$$

Let $\Omega^{1,2}_X$ be the two-term subcomplex $\Omega^1_X \xrightarrow{d} (\Omega^2_X)^{\mathrm{cl}}$, concentrated in degrees 1 and 2, of the algebraic de Rham complex of X, where $(\Omega^2_X)^{\mathrm{cl}}$ denotes the subsheaf of closed forms in Ω^2_X. As noted in the appendix, sheaves of twisted differential operators on X are parametrized, up to isomorphism, by the second hypercohomology

group $\mathbb{H}^2(X, \Omega_X^{1,2})$. Given $\omega \in \mathbb{H}^2(X, \Omega_X^{1,2})$, the corresponding sheaf of differential operators is denoted by $\mathcal{D}_X^{\omega}$.

2.3. *Dunkl–Opdam operators.* Let W be a finite group acting on X. Let $\mathcal{S}(X)$ be the set of pairs (w, Z) where $w \in W$ and Z is a connected component of X^w of codimension one. Any such Z is smooth. A pair (w, Z) in $\mathcal{S}(X)$ will be referred to as a *reflection* of (X, W). The group W acts on $\mathcal{S}(X)$, and we fix $\mathbf{c} : \mathcal{S}(X) \to \mathbb{C}$ to be a W-equivariant function, where W acts trivially on $\mathbb{C}$. A Picard algebroid $\mathcal{P}$ on X is said to be W-equivariant if there are isomorphisms $\psi_w : w^*(\mathcal{P}) \xrightarrow{\sim} \mathcal{P}$ of algebroids satisfying the usual cocycle condition such that the inclusion $\mathcal{O}_X \to \mathcal{P}$ and anchor map $\sigma : \mathcal{P} \to \Theta_X$ are W-equivariant. Since W acts rationally on $\mathbb{H}^2(X, \Omega_X^{1,2})$, each class $[\omega] \in \mathbb{H}^2(X, \Omega_X^{1,2})^W$ can be represented by an invariant 2-cocycle ω. The corresponding Picard algebroid $\mathcal{P}^{\omega}$ is W-equivariant. We fix one such W-equivariant Picard algebroid $\mathcal{P}^{\omega}$. Fix also an open affine, W-stable covering $\{U_i\}$ of X such that $\mathrm{Pic}(U_i) = 0$ for all i. Then, we can choose functions $f_{Z,i}$ defining $U_i \cap Z$. The union of all the Z is denoted by D. If $j : X - D \hookrightarrow X$ is the inclusion, then write $\mathcal{P}^{\omega}(D)$ for the sheaf $j_*(\mathcal{P}^{\omega}|_{X-D})$.

Definition 2.3.1. For each $v \in \Gamma(U_i, \mathcal{P}^{\omega})$, the associated Dunkl–Opdam operator is

$$D_v = v + \sum_{(w,Z)\in\mathcal{S}(X)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} i_{\sigma(v)}(d \log f_{Z,i})(w - 1), \tag{2.3.2}$$

where $\lambda_{w,Z}$ is the eigenvalue of w on each fiber of the conormal bundle of Z in X.

The operator D_v is a section of $\mathcal{P}^{\omega}(D) \rtimes W$ over U_i. The $\Gamma(U_i, \mathcal{O}_X \rtimes W)$-submodule of $\mathcal{P}^{\omega}(D) \rtimes W$ generated by $\Gamma(U_i, \mathcal{O}_X \rtimes W)$ and all the Dunkl–Opdam operators $\{D_v \mid v \in \Gamma(U_i, \mathcal{P}^{\omega})\}$ is denoted by $\Gamma(U_i, \mathcal{F}^1_{\omega,\mathbf{c}}(X, W))$. Though the definition of the Dunkl–Opdam operator D_v depends on the choice of functions $f_{Z,i}$, it is easy to see that the submodule $\Gamma(U_i, \mathcal{F}^1_{\omega,\mathbf{c}}(X, W))$ of $\Gamma(U_i, \mathcal{P}^{\omega}(D) \rtimes W)$ is independent of any choices. The modules $\Gamma(U_i, \mathcal{F}^1_{\omega,\mathbf{c}}(X, W))$ glue to form a sheaf $\mathcal{F}^1_{\omega,\mathbf{c}}(X, W)$ in the W-equivariant Zariski topology on X. As noted in the remark after Theorem 2.11 of [Etingof 2004], a calculation in each formal neighborhood of $x \in X$ shows that $[D_{v_1}, D_{v_2}] \in \mathcal{F}^1_{\omega,\mathbf{c}}(X, W)$ for all $v_1, v_2 \in \mathcal{P}^{\omega}$. However, there is *no* natural bracket on $\mathcal{F}^1_{\omega,\mathbf{c}}(X, W)$. The anchor map $\sigma : \mathcal{P}^{\omega}(D) \otimes W \to \Theta_X(D) \otimes W$ restricts to a map $\mathcal{F}^1_{\omega,\mathbf{c}}(X, W) \to \Theta_X \otimes W$ which fits into a short exact sequence

$$0 \longrightarrow \mathcal{O}_X \rtimes W \longrightarrow \mathcal{F}^1_{\omega,\mathbf{c}}(X, W) \xrightarrow{\sigma} \Theta_X \otimes W \longrightarrow 0. \tag{2.3.3}$$

Definition 2.3.4. We call the subsheaf of algebras of $j_*(\mathcal{D}^{\omega}_{X-D} \rtimes W)$ generated by $\mathcal{F}^1_{\omega,\mathbf{c}}(X, W)$ the *sheaf of Cherednik algebras* associated to W, ω and $\mathbf{c}$. It is denoted $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$.

The global sections of $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ are denoted $\mathsf{H}_{\omega,\mathbf{c}}(X, W)$.

2.4. There is a natural order filtration $\mathcal{F}^{\bullet}_{\omega,\mathbf{c}}(X, W)$ on $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$, defined in one of two ways. Either one defines $\mathcal{F}^{\bullet}_{\omega,\mathbf{c}}(X, W)$ to be the restriction to $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ of the order filtration on $j_{\bullet}(\mathcal{D}^{\omega}_{X-D} \rtimes W)$, or, equivalently, one gives elements in $\mathcal{F}^{1}_{\omega,\mathbf{c}}(X, W)$ degree at most one, with $D \in \mathcal{F}^{1}_{\omega,\mathbf{c}}(X, W)$ having degree one if and only if $\sigma(D) \neq 0$, and then defines the filtration inductively by setting $\mathcal{F}^{i}_{\omega,\mathbf{c}}(X, W) = \mathcal{F}^{1}_{\omega,\mathbf{c}}(X, W)\mathcal{F}^{i-1}_{\omega,\mathbf{c}}(X, W)$. By definition, the filtration is exhaustive. Let $\pi : T^*X \to X$ be the projection map. Etingof [2004, Theorem 2.11] has shown that the algebras $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ are a flat deformation of $\mathcal{D}_X \rtimes W$. Equivalently, the PBW property holds for Cherednik algebras:

Theorem 2.4.1. *We have* $\mathrm{gr}_{\mathcal{F}} \mathcal{H}_{\omega,\mathbf{c}}(X, W) \simeq \pi_{\bullet}\mathcal{O}_{T^*X} \rtimes W$.

We note for later use that Theorem 2.4.1 implies that for any affine W-stable open set $U \subset X$, the algebra $\Gamma(U, \mathcal{H}_{\omega,\mathbf{c}}(X, W))$ has finite global dimension; its global dimension is bounded by $2 \dim X$.

2.5. Throughout, an $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-module will always mean an $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-module that is quasicoherent over $\mathcal{O}_X$. The category of all $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-modules is denoted by $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-Mod and the full subcategory of all modules coherent over $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ is denoted by $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-mod. A module $\mathcal{M} \in \mathcal{H}_{\omega,\mathbf{c}}(X, W)$-Mod is called *lisse* if it is coherent over $\mathcal{O}_X$.

3. Pullback of sheaves

In this section we show that modules for sheaves of Cherednik algebras can be pulled back under morphisms that are "melys" for the parameter $\mathbf{c}$.

3.1. Let $\varphi : Y \to X$ be a W-equivariant morphism between smooth, connected, quasiprojective varieties. As explained in the appendix, given a Picard algebroid $\mathcal{P}^{\omega}_X$ on X, there is a φ-morphism $\mathcal{P}^{\varphi^*\omega}_Y \to \varphi^*\mathcal{P}^{\omega}_X$. This implies that the sheaf $\varphi^*\mathcal{D}^{\omega}_X$ is a left $\mathcal{D}^{\varphi^*\omega}_Y$-module. We give conditions on the map φ so that there exist a sheaf of Dunkl operators $\mathcal{F}^{1}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$ on Y and morphism of $\mathcal{O}_Y \rtimes W$-modules $\mathcal{F}^{1}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W) \to \varphi^*\mathcal{F}^{1}_{\omega,\mathbf{c}}(X, W)$. As a consequence $\varphi^*\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ becomes a left $\mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$-module and we can pullback $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-modules to $\mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$-modules.

3.2. If the morphism φ is flat of relative dimension r, then there is a good notion of pullback of algebraic cycles, namely, $\varphi^* : C_k(X) \to C_{k+r}(Y)$, where $C_k(X)$ is the abelian group of k-dimensional algebraic cycles on X. See [Fulton 1998, Section 1.7]. The class in $C_k(X)$ of a k-dimensional subscheme Z of X is denoted by $[Z]$.

Lemma 3.2.1. *Let $\varphi : Y \to X$ be flat and $(w, Z) \in \mathcal{S}(X)$. Write $\varphi^*[Z] = \sum_i n_i[Z_i]$, where each Z_i is an irreducible subvariety of Y. Then, w permutes the $[Z_i]$.*

Moreover, if $\varphi^{-1}(Z)$ is set-theoretically contained in Y^w, then each irreducible component of $\varphi^{-1}(Z)$ is a connected component of Y^w of codimension one.

Proof. The first claim follows from the fact that, set-theoretically, $\varphi^{-1}(Z) = \bigcup_{n_i \neq 0} Z_i$. Since $\varphi^{-1}(Z)$ is a union of closed subvarieties of Y of codimension one and Y is assumed to be irreducible, it suffices for the second claim to show that $Y^w \neq Y$. Assume otherwise. Then, since φ is flat, $\varphi(Y^w) = \varphi(Y)$ is open in X, but is also contained in the closed subvariety X^w. Hence $X^w = X$. This contradicts the fact that Z is an irreducible component of X^w. □

3.3. Let $\mathcal{S}_{\mathbf{c}}(X)$ denote the set of all pairs $(w, Z) \in \mathcal{S}(X)$ such that $\mathbf{c}(w, Z) \neq 0$.

Definition 3.3.1. The morphism $\varphi : Y \to X$ is *melys* with respect to $\mathbf{c}$ if:

(1) φ is flat.

(2) For all $(w, Z) \in \mathcal{S}_{\mathbf{c}}(X)$, set-theoretically $\varphi^{-1}(Z) \subset Y^w$.

If φ is melys with respect to $\mathbf{c}$ then we define $\varphi^*\mathbf{c}$ on $\mathcal{S}(Y)$ by

$$(\varphi^*\mathbf{c})(w, Z') = \sum_{(w,Z)\in\mathcal{S}(X)} n_{Z,Z'}\, \mathbf{c}(w, Z),$$

where $\varphi^*[Z] = \sum_{Z'} n_{Z,Z'}[Z']$. Let $E = \bigcup_{\mathbf{c}(w,Z)\neq 0} Z$ and $D = \varphi^{-1}(E)$. Since φ is flat, each irreducible component of D has codimension one in X. Let $j : U := X - D \hookrightarrow X$ and $k : V = Y - E \hookrightarrow Y$; these are affine morphisms. For any quasicoherent sheaf $\mathcal{F}$ on X (resp. on Y), we denote by $\mathcal{F}(D)$ the sheaf $j_\bullet(\mathcal{F}|_U)$ (resp. by $\mathcal{F}(E)$ the sheaf $k_\bullet(\mathcal{F}|_V)$).

Lemma 3.3.2. *The sheaf $\varphi^*\mathcal{D}_Y^\omega(E) \rtimes W$ on X is a $\mathcal{D}_X^{\varphi^*\omega}(D) \rtimes W$-module, and there exists a morphism*

$$\gamma : \mathcal{D}_X^{\varphi^*\omega}(D) \rtimes W \longrightarrow \varphi^*\mathcal{D}_Y^\omega(E) \rtimes W$$

of $\mathcal{D}_X^{\varphi^*\omega}(D) \rtimes W$-modules.

Proof. The map φ restricts to a flat morphism $\Phi : U \to V$. By Lemma A.2.2, we have

$$\mathcal{P}_U^{\Phi^*\omega} \xrightarrow{\sim} \Phi^*\mathcal{P}_V^\omega \times_{\Phi^*\Theta_V} \Theta_U.$$

This induces a morphism $\gamma : \mathcal{D}_U^{\Phi^*\omega} \to \Phi^*\mathcal{D}_V^\omega$ of $\mathcal{D}_U^{\Phi^*\omega}$-modules. Since ω was chosen to be W-invariant, this extends to a morphism $\gamma : \mathcal{D}_U^{\Phi^*\omega} \rtimes W \to \Phi^*\mathcal{D}_V^\omega \rtimes W$ of $\mathcal{D}_U^{\Phi^*\omega} \rtimes W$-modules. Since $j_\bullet\mathcal{P}_U^{\Phi^*\omega} = \mathcal{P}_X^{\varphi^*\omega}(D)$, we have $j_\bullet(\mathcal{D}_U^{\Phi^*\omega} \rtimes W) =$

$\mathscr{D}_X^{\varphi^*\omega}(D) \rtimes W$. The diagram

$$\begin{array}{ccc} U & \xrightarrow{j} & X \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ V & \xrightarrow{k} & Y \end{array}$$

is Cartesian. Therefore, by flat base change, $j_\bullet \Phi^* \mathscr{P}_V^\omega \rtimes W = \varphi^* \mathscr{P}_Y^\omega(E) \rtimes W$ and hence $j_\bullet(\Phi^* \mathscr{D}_V^\omega \rtimes W) = \varphi^* \mathscr{D}_Y^\omega(E) \rtimes W$. □

3.4. By analogy with φ-morphisms (see Lemma A.2.2) we have:

Proposition 3.4.1. *There is a morphism*

$$\gamma : \mathscr{H}_{\varphi^*\omega, \varphi^*\mathbf{c}}(Y, W) \longrightarrow \varphi^* \mathscr{H}_{\omega, \mathbf{c}}(X, W)$$

of $\mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$-modules that induces an isomorphism of $\mathbb{O}_Y \rtimes W$-modules

$$\psi : \mathscr{F}^1_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W) \xrightarrow{\sim} \varphi^* \mathscr{F}^1_{\omega,\mathbf{c}}(X, W) \times_{\varphi^*\Theta_X \otimes W} \Theta_Y \otimes W.$$

Proof. The algebra $\mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$ is a subalgebra of $\mathscr{D}_Y^{\varphi^*\omega}(E) \rtimes W$, whereas $\varphi^* \mathscr{H}_{\omega,\mathbf{c}}(X, W)$ is a subalgebra of $\varphi^* \mathscr{D}_X^\omega(D) \rtimes W$. Let $\gamma : \mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W) \to \varphi^* \mathscr{D}_X^\omega(D) \rtimes W$ be the restriction of the morphism $\gamma : \mathscr{D}_Y^{\varphi^*\omega}(E) \rtimes W \to \varphi^* \mathscr{D}_X^\omega(D) \rtimes W$ of Lemma 3.3.2. We claim that it suffices to show that the image of γ is contained in $\varphi^* \mathscr{H}_{\omega,\mathbf{c}}(X, W)$. Assuming this, the action of $\mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$ on $\varphi^* \mathscr{H}_{\omega,\mathbf{c}}(X, W)$ will just be the restriction of the action of $\mathscr{D}_Y^{\varphi^*\omega}(E) \rtimes W$ on $\varphi^* \mathscr{D}_X^\omega(D) \rtimes W$. Therefore, it is given by

$$a \cdot (g \otimes p) = \gamma([a, g]) \cdot (1 \otimes p) + g(\gamma(a) \cdot (1 \otimes p)),$$

where $a \in \mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$, $g \in \mathbb{O}_Y$ and $p \in \varphi^{-1}\mathscr{H}_{\omega,\mathbf{c}}(X, W)$. Here $[a, g]$ is thought of as an element of $\mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$. If $\gamma(a)$ is contained in $\varphi^* \mathscr{H}_{\omega,\mathbf{c}}(X, W)$ and $p \in \varphi^{-1}\mathscr{H}_{\omega,\mathbf{c}}(X, W)$, then $\gamma(a) \cdot (1 \otimes p)$ belongs to $\varphi^* \mathscr{H}_{\omega,\mathbf{c}}(X, W)$. Thus, it suffices to show that the image of γ is contained in $\varphi^* \mathscr{H}_{\omega,\mathbf{c}}(X, W)$ as claimed.

Since $\mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$ is generated as an algebra by $\mathscr{F}^1_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$, it will suffice to show that the image of $\mathscr{F}^1_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$ is contained in $\varphi^* \mathscr{F}^1_{\omega,\mathbf{c}}(X, W)$. This is a local calculation. Therefore, we may assume that both X and Y are affine and that the subvarieties Z of X with $(w, Z) \in \mathscr{S}_\mathbf{c}(X)$ are defined by the vanishing of functions f_Z. Let $p \in \mathscr{P}_Y^{\varphi^*\omega}$, and denote by D_p the associated Dunkl–Opdam operator given by (2.3.2). Let $\gamma(p) = \sum_i g^i \otimes q^i$ in $\varphi^* \mathscr{P}_X^\omega$. Then,

$$\gamma(D_p) = \sum_i g^i \otimes q^i + \sum_{(w,Z')} \frac{2(\varphi^*\mathbf{c})(w, Z')}{1 - \lambda_{w,Z'}} i_{\sigma_Y(p)}(d \log f_{Z'}) \otimes (w - 1).$$

If $\varphi^{-1}(Z) = Z'_1 \cup \cdots \cup Z'_l$ set-theoretically and $\varphi^*[Z] = \sum_{i=1}^{l} n_i [Z'_i]$, then $\varphi^* f_Z = u \prod_i f_{Z'_i}^{n_i}$, for some unit u, and scheme-theoretically $\varphi^{-1}(Z)$ is defined by the vanishing of the function $\prod_i f_{Z'_i}^{n_i}$. Therefore, by definition of the parameter $\varphi^*\mathbf{c}$,

$$\frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} \varphi^* d \log f_Z = \sum_{Z' \subset \varphi^{-1}(Z)} \frac{2(\varphi^*\mathbf{c})(w, Z')}{1 - \lambda_{w,Z'}} d \log f_{Z'} + h, \tag{3.4.2}$$

where $h \in \mathbb{O}_Y \rtimes W$. Hence, up to a term in $\varphi^*\mathbb{O}_X \rtimes W$,

$$\begin{aligned}
&\sum_{(w,Z')} \frac{2(\varphi^*\mathbf{c})(w, Z')}{1 - \lambda_{w,Z'}} i_{\sigma_Y(p)}(d \log f_{Z'}) \otimes (w - 1) \\
&\qquad = \sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} i_{\sigma_Y(p)}(d \log \varphi^* f_Z) \otimes (w - 1) \\
&\qquad = \sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} \frac{\sigma_Y(p)(\varphi^* f_Z)}{\varphi^* f_Z} \otimes (w - 1) \\
&\qquad = \sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} \frac{1}{\varphi^* f_Z} \left(\sum_i g^i \varphi^*(\sigma_X(q^i)(f_Z)) \right) \otimes (w - 1) \\
&\qquad = \sum_i g^i \otimes \left(\sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} \frac{\sigma_X(q^i)(f_Z)}{f_Z} (w - 1) \right) \\
&\qquad = \sum_i g^i \otimes \left(\sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} i_{\sigma_X(q^i)}(d \log f_Z)(w - 1) \right).
\end{aligned}$$

Thus, $\gamma(D_p) = \sum_i g^i \otimes D_{q^i}$, which lies in $\varphi^* \mathscr{F}^1_{\omega,\mathbf{c}}(X, W)$.

Finally, we show that the morphism γ induces the isomorphism ψ, as stated. Since φ is flat, pulling back the sequence (2.3.3) gives a short exact sequence

$$0 \longrightarrow \mathbb{O}_Y \rtimes W \longrightarrow \varphi^* \mathscr{F}^1_{\omega,\mathbf{c}}(X, W) \longrightarrow \varphi^* \Theta_X \otimes W \longrightarrow 0.$$

Using the fact that $\mathbb{O}_Y \rtimes W \times_{\varphi^*\Theta_X \otimes W} \Theta_Y \otimes W = \mathbb{O}_Y \rtimes W$, where $\mathbb{O}_Y \rtimes W \to \varphi^*\Theta_X \otimes W$ is the zero map, and the fact that $\varphi^*\Theta_X \otimes W \times_{\varphi^*\Theta_X \otimes W} \Theta_Y \otimes W = \Theta_Y \otimes W$, we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{O}_Y \rtimes W & \longrightarrow & \mathscr{F}^1_{\varphi^*\omega, \varphi^*\mathbf{c}}(Y, W) & \xrightarrow{\sigma} & \Theta_Y \otimes W & \longrightarrow & 0 \\
 & & \| & & \downarrow \psi & & \| & & \\
0 & \longrightarrow & \mathbb{O}_Y \rtimes W & \longrightarrow & \varphi^* \mathscr{F}^1_{\omega,\mathbf{c}}(X, W) \times_{\varphi^*\Theta_X \otimes W} \Theta_Y \otimes W & \longrightarrow & \Theta_Y \otimes W & \longrightarrow & 0
\end{array}$$

By the five lemma, ψ is an isomorphism. □

3.5. The morphism γ allows us to define an action of $\mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$ on $\varphi^*\mathcal{M}$ for any $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-module $\mathcal{M}$.

Corollary 3.5.1. *Assume that φ is melys with respect to $\mathbf{c}$. Then pullback is an exact functor*

$$\varphi^* : \mathcal{H}_{\omega,\mathbf{c}}(X, W)\text{-Mod} \longrightarrow \mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)\text{-Mod}$$

extending the usual pullback $\varphi^* : \mathsf{QCoh}(X) \longrightarrow \mathsf{QCoh}(Y)$.

Proof. Proposition 3.4.1 implies that

$$\varphi^*\mathcal{M} = \varphi^*\mathcal{H}_{\omega,\mathbf{c}}(X, W) \otimes_{\varphi^{-1}\mathcal{H}_{\omega,\mathbf{c}}(X,W)} \varphi^{-1}\mathcal{M}$$

is naturally an $\mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$-module. Since φ is flat, pullback of quasicoherent $\mathcal{O}_X$-modules is an exact functor. □

It is clear by definition that φ^* maps $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-mod to $\mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$-mod and lisse $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-modules to lisse $\mathcal{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$-modules.

3.6. ***Étale morphisms.*** In this section we consider étale morphisms. Fix X, ω, W and $\mathbf{c}$ as above. Let $(X, \mathbf{c})_{\mathrm{mel}}$ be the full subcategory of $\mathrm{Sch}\,/X$ (schemes over X) consisting of all morphisms $Y \to X$ that are étale and melys with respect to $\mathbf{c}$. Then, one can easily check that $(X, \mathbf{c})_{\mathrm{mel}}$ is a site over X; see, e.g., [Milne 1980, Section II.1] for details on sites. We call $(X, \mathbf{c})_{\mathrm{mel}}$ the melys site over X. The following result is closely related to [Wilcox 2011, Proposition 2.3].

Proposition 3.6.1. *The sheaf $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ is a sheaf of algebras on the melys site $(X, \mathbf{c})_{\mathrm{mel}}$.*

Proof. Let $\varphi : Y \to X$ be an étale map, melys with respect to $\mathbf{c}$. We begin by showing that $\varphi^*\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ is a sheaf of algebras and the morphism γ of Proposition 3.4.1 is an isomorphism of algebras.

As in Section 3.3, let $D = \bigcup Z$, $E = \varphi^{-1}(D)$, $U = X - D$ and $V = Y - E$. Since $\Phi : V \to U$ is étale, it is flat, and hence $\Phi^{-1}\mathcal{D}_U^\omega \rtimes W$ is a subsheaf of $\Phi^*\mathcal{D}_U^\omega \rtimes W$. As noted in Remark A.2.4, the natural map $\gamma : \mathcal{D}_V^{\Phi^*\omega} \rtimes W \to \Phi^*\mathcal{D}_U^\omega \rtimes W$ is an algebra isomorphism such that the restriction of γ^{-1} to $\Phi^{-1}\mathcal{D}_U^\omega \rtimes W$ is an algebra morphism $\Phi^{-1}\mathcal{D}_U^\omega \rtimes W \to \mathcal{D}_V^{\Phi^*\omega} \rtimes W$. Therefore, using flat base change as in the proof of Lemma 3.3.2, we get an algebra morphism $\gamma^{-1} : \varphi^{-1}\mathcal{D}_X^\omega(D) \rtimes W \to \mathcal{D}_Y^{\varphi^*\omega}(E) \rtimes W$. This morphism induces an algebra isomorphism

$$\gamma^{-1} : \varphi^*\mathcal{D}_X^\omega(D) \rtimes W \xrightarrow{\sim} \mathcal{D}_Y^{\varphi^*\omega}(E) \rtimes W,$$

where the multiplication in $\varphi^*\mathcal{D}_X^\omega(D) \rtimes W$ is given by

$$(g_1 \otimes q_1) \cdot (g_2 \otimes q_2) = (g_1 \otimes 1)u(q_1, g_2)(1 \otimes q_2),$$

with $u(q, g) := \gamma([\gamma^{-1}(q), g]) \in \Phi^*\mathcal{D}_X^\omega(D) \rtimes W$, for all $q, q_1, q_2 \in \varphi^{-1}\mathcal{D}_X^\omega(D) \rtimes W$

and all $g, g_1, g_2 \in \mathbb{O}_Y$. By Proposition 3.4.1, γ^{-1} restricts to an algebra morphism $\varphi^{-1}\mathscr{H}_{\omega,\mathbf{c}}(X, W) \to \mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$, inducing an isomorphism $\varphi^*\mathscr{H}_{\omega,\mathbf{c}}(X, W) \xrightarrow{\sim} \mathscr{H}_{\varphi^*\omega,\varphi^*\mathbf{c}}(Y, W)$. Let

$$\begin{array}{ccc} Y_1 & \xrightarrow{\vartheta} & Y_2 \\ & {\scriptstyle\varphi_1}\searrow \quad \swarrow{\scriptstyle\varphi_2} & \\ & X & \end{array}$$

be a morphism in $(X, \mathbf{c})_{\mathrm{mel}}$. Then, Y_1 and Y_2 are smooth varieties and, by [Milne 1980, I, Corollary 3.6], ϑ is an étale morphism. Lemma 3.2.1 implies that it is also melys. Thus, the above computations show that $\mathscr{H}_{\omega,\mathbf{c}}(X, W)$ forms a presheaf on $(X, \mathbf{c})_{\mathrm{mel}}$.

To check that it is in fact a sheaf, it suffices to do so locally; see the proof of [Borho and Brylinski 1989, Proposition 0]. Therefore, we assume that X is affine and that we are given an étale, W-equivariant, affine covering $(i_\alpha : Y_\alpha \to X)$ of X; i.e., each Y_α is affine and the union of the images of the maps i_α cover X. Then we must prove that the sequence

$$0 \longrightarrow \mathsf{H}_{\omega,\mathbf{c}}(X, W) \longrightarrow \bigoplus_\alpha \mathsf{H}_{i_\alpha^*\omega, i_\alpha^*\mathbf{c}}(Y_\alpha, W) \longrightarrow \bigoplus_{\alpha,\beta} \mathsf{H}_{i_{\alpha,\beta}^*\omega, i_{\alpha,\beta}^*\mathbf{c}}(Y_\alpha \times_X Y_\beta, W)$$

is exact. Let $U, V_\alpha, \ldots$ be the usual open subsets of $X, Y_\alpha, \ldots$. Then, we have a commutative diagram

$$\begin{array}{ccccc} 0 \longrightarrow \mathsf{H}_{\omega,\mathbf{c}}(X, W) & \xrightarrow{j} & \bigoplus_\alpha \mathsf{H}_{i_\alpha^*\omega, i_\alpha^*\mathbf{c}}(Y_\alpha, W) & \xrightarrow{k} & \bigoplus_{\alpha,\beta} \mathsf{H}_{i_{\alpha,\beta}^*\omega, i_{\alpha,\beta}^*\mathbf{c}}(Y_\alpha \times_X Y_\beta, W) \\ \downarrow & & \downarrow & & \downarrow \\ 0 \longrightarrow \Gamma(U, \mathscr{D}_U^\omega \rtimes W) & \longrightarrow & \bigoplus_\alpha \Gamma\big(V_\alpha, \mathscr{D}_{V_\alpha}^{i_\alpha^*\omega} \rtimes W\big) & \longrightarrow & \bigoplus_{\alpha,\beta} \Gamma\big(V_\alpha \times_U V_\beta, \mathscr{D}^{i_{\alpha,\beta}^*\omega} \rtimes W\big) \end{array}$$

The bottom row is exact because $\mathscr{D}_U^\omega \rtimes W$ is a sheaf on the melys site. Since the diagram commutes, j is injective and the image of j is contained in the kernel of k. Therefore, we just need to show that the image of j is exactly the kernel of k. The sequence on the bottom row is strictly filtered with respect to the order filtration and, as noted in Section 2.4, the Cherednik algebra inherits its natural filtration by restriction of the order filtration on $\mathscr{D}_U^\omega \rtimes W$. Therefore, the top row will be exact if and only if the corresponding sequence of associated graded objects is exact. But this sequence is also the associated graded of the analogous sequence for $\mathscr{D}_X \rtimes W$, which we know is exact. □

3.7. ***The*** **KZ*-functor.*** Assume that W acts freely on the open sets $V \subset Y$ and $U \subset X$, and let $\omega = 0$. The proof of Proposition 3.4.1 makes it clear that pullback of

$\mathcal{H}_{\mathbf{c}}(X, W)$-modules is compatible with the KZ-functor. Denote by $\mathcal{H}_{\mathbf{c}}(X, W)$-Reg the full subcategory of $\mathcal{H}_{\mathbf{c}}(X, W)$-mod consisting of all lisse $\mathcal{H}_{\mathbf{c}}(X, W)$-modules whose restriction to U is an integrable connection with regular singularities. Let DR be the de Rham functor that maps integrable connections with regular singularities on U/W to representations of the fundamental group $\pi_1(U/W)$. The KZ-functor is defined by

$$\mathsf{KZ}_X(\mathcal{M}) = \mathsf{DR}\big([\rho_\bullet(\mathcal{M}|_U)]^W\big).$$

Then φ^* maps $\mathcal{H}_{\mathbf{c}}(X, W)$-Reg into $\mathcal{H}_{\varphi^*\mathbf{c}}(Y, W)$-Reg. Therefore, since the de Rham functor behaves well with respect to pullback [Hotta et al. 2008, Theorem 7.1.1], the following diagram commutes

$$\begin{array}{ccc} \mathcal{H}_{\mathbf{c}}(X, W)\text{-Reg} & \xrightarrow{\varphi^*} & \mathcal{H}_{\varphi^*\mathbf{c}}(Y, W)\text{-Reg} \\ \Big\downarrow{\scriptstyle \mathsf{KZ}_X} & & \Big\downarrow{\scriptstyle \mathsf{KZ}_Y} \\ \pi_1(U/W)\text{-mod} & \xrightarrow{\Phi^*} & \pi_1(V/W)\text{-mod} \end{array}$$

The image of the KZ-functor is contained in the full subcategory of $\pi_1(U/W)$-mod consisting of all modules for a certain "Hecke" quotient of $\mathbb{C}\pi_1(U/W)$; see [Etingof 2004, Proposition 3.4].

3.8. ***Pushforward.*** It is also possible to define (derived) pushforward of modules under melys maps. Let $\varphi : Y \to X$ be melys with respect to $\mathbf{c}$, and denote by Mod-$\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$ the category of right $\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$-modules. Then, the derived pushforward functor

$$\mathbb{R}\varphi_* : D^b(\text{Mod-}\mathcal{H}_{\omega,\mathbf{c}}(Y, W)) \longrightarrow D^b(\text{Mod-}\mathcal{H}_{\omega,\mathbf{c}}(X, W))$$

is given by

$$\mathbb{R}\varphi_*(\mathcal{M}) = \mathbb{R}\varphi_\bullet\big(\mathcal{M} \otimes^{\mathbb{L}}_{\mathcal{H}_{\omega,\mathbf{c}}(Y,W)} \varphi^*\mathcal{H}_{\omega,\mathbf{c}}(X, W)\big).$$

Let us justify the fact that the image of $\mathbb{R}\varphi_*$ is contained in $D^b(\text{Mod-}\mathcal{H}_{\omega,\mathbf{c}}(X, W))$. First, as noted in Section 2.4, the PBW theorem implies that the sheaf $\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$ has good homological properties. Since we have assumed that Y is quasiprojective, this implies that each $\mathcal{M} \in \text{Mod-}\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$ has a finite resolution by locally projective $\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$-modules; see [Hotta et al. 2008, Section 1.4]. Hence, for $\mathcal{M} \in D^b(\text{Mod-}\mathcal{H}_{\omega,\mathbf{c}}(Y, W))$, the complex $\mathcal{M} \otimes^{\mathbb{L}}_{\mathcal{H}_{\omega,\mathbf{c}}(Y,W)} \varphi^*\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ belongs to $D^b(\text{Mod-}\varphi^{-1}\mathcal{H}_{\omega,\mathbf{c}}(Y, W))$. That $\mathbb{R}\varphi_*(\mathcal{M})$ belongs to $D^b(\text{Mod-}\mathcal{H}_{\omega,\mathbf{c}}(X, W))$ then follows, for instance, from [Hotta et al. 2008, Proposition 1.5.4].

We will also require pushforwards of left $\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$-modules under open embeddings $j : Y \hookrightarrow X$. The following is standard; see, e.g., [Hotta et al. 2008, Proposition 1.5.4].

Lemma 3.8.1. *For $\mathcal{M} \in \mathcal{H}_{\omega,\mathbf{c}}(Y, W)$-Mod, the sheaves $\mathbb{R}^i j_\bullet(\mathcal{M})$, $i \geq 0$, belong to $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-Mod.*

It would be interesting to develop a notion of duality for Cherednik algebras, which would allow one to define pushforwards of left $\mathcal{H}_{\omega,\mathbf{c}}(Y, W)$-modules along arbitrary melys morphisms.

4. Twisted equivariant modules

In this section we define (twisted) G-equivariant $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-modules.

4.1. Let X be a smooth W-variety, and $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ a sheaf of Cherednik algebras on X. Assume that a *connected* algebraic group G also acts on X such that this action commutes with the action of W. Write $p, a : G \times X \longrightarrow X$ for the projection and action maps. Let $\mathcal{M}$ be an $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-module. Clearly, $p^*\mathcal{M}$ is an $\mathcal{H}_{\omega,\mathbf{c}}(G \times X, W) = \mathcal{D}_G \boxtimes \mathcal{H}_{\omega,\mathbf{c}}(X, W)$-module.

Lemma 4.1.1. *The action map a is melys for any $\mathbf{c}$, and therefore $a^*\mathcal{M}$ is an $\mathcal{H}_{\omega,\mathbf{c}}(G \times X, W)$-module.*

Proof. The action map a is smooth and hence flat. Let $(w, Z) \in \mathcal{S}(X)$. Since the action of G commutes with the action of W, X^w is G-stable. Moreover, the fact that G and Z are connected implies that Z itself is G-stable. Thus, $a^{-1}(Z) = G \times Z$ is contained in $(G \times X)^w = G \times X^w$. □

4.2. The Lie algebra of G is denoted by $\mathfrak{g}$. Let $m : G \times G \to G$ the multiplication map and $s : X \to G \times X$ be defined by $s(x) = (e, x)$. Choose $\chi \in (\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}])^*$, and let $\mathbb{O}_G^\chi$ be the $\mathcal{D}_G$-module $\mathcal{D}_G/\mathcal{D}_G\{v - \chi(v) \mid v \in \mathfrak{g}\}$, where we have identified $\mathfrak{g}$ with right-invariant vector fields on G. It is an irreducible integrable connection on G.

Definition 4.2.1. The module $\mathcal{M} \in \mathcal{H}_{\omega,\mathbf{c}}(X, W)$-Mod is called (G, χ)-monodromic if there exists an isomorphism $\theta : \mathbb{O}_G^\chi \boxtimes \mathcal{M} \xrightarrow{\sim} a^*\mathcal{M}$ of $\mathcal{H}_{\omega,\mathbf{c}}(G \times X, W)$-modules such that $s^*\theta = \mathrm{id}_{\mathcal{M}}$ and the diagram

$$\begin{array}{ccc}
\mathbb{O}_G^\chi \boxtimes \mathbb{O}_G^\chi \boxtimes \mathcal{M} & \xrightarrow{\mathrm{id}_G \times \theta} & \mathbb{O}_G^\chi \boxtimes a^*\mathcal{M} \\
= \downarrow & & \downarrow = \\
(m \times \mathrm{id})^*(\mathbb{O}_G^\chi \boxtimes \mathcal{M}) & & (\mathrm{id}_G \times a)^*(\mathbb{O}_G^\chi \boxtimes \mathcal{M}) \\
{\scriptstyle (m \times \mathrm{id}_X)^*\theta} \downarrow & \swarrow {\scriptstyle (\mathrm{id}_G \times a)^*\theta} & \\
(m \times \mathrm{id}_X)^* a^*\mathcal{M} & \xrightarrow{=} & (\mathrm{id}_G \times a)^* a^*\mathcal{M}
\end{array} \tag{4.2.2}$$

is commutative: $\mathcal{M}$ satisfies the *cocycle condition*.

We will denote the category of (G, χ)-monodromic $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$-modules by $(\mathcal{H}_{\omega,\mathbf{c}}(X, W), G, \chi)$-Mod.

4.3. *T-monodromic modules.* Let T be a torus, i.e., a product of copies of the multiplicative group $\mathbb{C}^\times$. The Lie algebra of T is denoted by $\mathfrak{t}$. Let $\pi : Y \to X$ be a principal T-bundle, with X smooth. We assume that the finite group W acts on Y, the action commuting with the action of T. This implies that W also acts on X and that the map π is T-equivariant. Let $\mathcal{H}_{\mathbf{c}}(Y, W)$ be a sheaf of Cherednik[2] algebras on Y.

Lemma 4.3.1. *There is a morphism of Lie algebras $\mu_{\mathbf{c}} : \mathfrak{t} \to \mathcal{F}^1_{\mathbf{c}}(Y, W)$ such that the composite $\sigma \circ \mu_{\mathbf{c}}$ equals the usual moment map $\mu : \mathfrak{t} \to \Theta_Y \otimes W$.*

Proof. Since the action of T commutes with the action of W, the open set $V = Y - E$ is T-stable. Differentiating the action of T on U, there is a map $\mu' : \mathfrak{t} \to \mathcal{D}_Y(E) \rtimes W$. It is clear that $\sigma \circ \mu' = \mu$. Therefore, we just need to show that the image of μ' is contained in the subsheaf $\mathcal{F}^1_{\mathbf{c}}(Y, W)$. This is a local computation. Hence we may assume that $Y = X \times T$, in which case $\mathcal{H}_{\mathbf{c}}(Y, W) = \mathcal{H}_{\mathbf{c}}(X, W) \boxtimes \mathcal{D}_T$. Now the claim is clear. □

The group T acts on $\mathcal{H}_{\mathbf{c}}(Y, W)$ and the map $\mu_{\mathbf{c}}$ is T-equivariant. Moreover, a local computation (using the fact that the bundle $Y \to X$ is locally trivial) shows that the image of $\mathfrak{t}$ is central in $(\pi_\bullet \mathcal{H}_{\mathbf{c}}(Y, W))^T$, and hence we may perform quantum Hamiltonian reduction. Recall that we define the map $\beta : \mathfrak{t}^* \to \mathbb{H}^2(X, \Omega^{1,2}_X)$ in (A.3.2).

Proposition 4.3.2. *Let $\chi \in \mathfrak{t}^*$. We have an isomorphism of sheaves of algebras on X*

$$\mathcal{H}_{\beta(\chi),\mathbf{c}}(X, W) \simeq (\pi_\bullet \mathcal{H}_{\mathbf{c}}(Y, W))^T / \langle \{\mu_{\mathbf{c}}(t) - \chi(t) \mid t \in \mathfrak{t}\} \rangle.$$

Proof. As in the proof of Proposition 3.4.1, let $D = \bigcup_{\mathbf{c}(w,Z)\neq 0} Z$, $U = X - D$, $E = \pi^{-1}(D)$ and $V = Y - E$. Then the restriction of π to V is a principal T-bundle $\Pi : V \to U$ and we have a Cartesian diagram

$$\begin{array}{ccc} V & \xrightarrow{j} & Y \\ {\scriptstyle\Pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ U & \xrightarrow{k} & X \end{array}$$

Proposition A.3.3 implies that there is an isomorphism

$$(\Pi_\bullet \mathcal{D}_V \rtimes W)^T / \langle \{\mu'(t) - \chi(t) \mid t \in \mathfrak{t}\} \rangle \xrightarrow{\sim} \mathcal{D}_U^{\beta(\chi)} \rtimes W. \tag{4.3.3}$$

[2]We assume, for simplicity, that the twist ω is zero. Presumably one can also deal with nontrivial twists.

Recall that $\mathcal{D}_X^{\beta(\chi)}(D) \rtimes W = k_\bullet(\mathcal{D}_U^{\beta(\chi)} \rtimes W)$. Since

$$k_\bullet(\Pi_\bullet \mathcal{D}_V \rtimes W)^T = (k_\bullet(\Pi_\bullet \mathcal{D}_V \rtimes W))^T = (\pi_\bullet(j_\bullet \mathcal{D}_V \rtimes W))^T$$

and $(\pi_\bullet \mathcal{H}_{\mathbf{c}}(Y, W))^T$ is a subalgebra of $(\pi_\bullet j_\bullet \mathcal{D}_V \rtimes W)^T$, we have a morphism of sheaves $\tau : (\pi_\bullet \mathcal{H}_{\mathbf{c}}(Y, W))^T \to \mathcal{D}_X^{\beta(\chi)}(D) \rtimes W$. The isomorphism (4.3.3) implies that $\langle \{\mu_{\mathbf{c}}(t) - \chi(t) \mid t \in \mathfrak{t}\} \rangle$ is contained in the kernel of τ. Therefore it suffices to show that $\langle \{\mu_{\mathbf{c}}(t) - \chi(t) \mid t \in \mathfrak{t}\} \rangle$ is precisely the kernel of τ and that the image of τ is $\mathcal{H}_{\beta(\chi),\mathbf{c}}(X, W)$. Both of these statements are local. Thus, we may assume without loss of generality that $Y = X \times T$. In this case, both statements reduce to the statement $\mathcal{D}(T)^T / \langle \{t - \chi(t) \mid t \in \mathfrak{t}\} \rangle \simeq \mathbb{C}$, which is clear. □

4.4. As for differential operators on principal T-bundles — see Section 2.5 of [Beilinson and Bernstein 1993]) — Proposition 4.3.2 implies an equivalence of categories:

Theorem 4.4.1. *The functor*

$$(\mathcal{H}_{\mathbf{c}}(X, W), T, \chi)\text{-Mod} \to \mathcal{H}_{\beta(\chi),\mathbf{c}}(Y, W)\text{-Mod}, \quad \mathcal{M} \mapsto (\pi_\bullet \mathcal{M})^T$$

is an equivalence of categories with quasi-inverse $\mathcal{N} \mapsto \pi^* \mathcal{N}$.

The above theorem can be extended in the obvious way to the category of weakly T-equivariant $\mathcal{H}_{\mathbf{c}}(X, W)$-modules with generalized central character $\overline{\chi} \in \mathfrak{t}^*/\mathbb{X}(T)$, as in [Beilinson and Bernstein 1993]. We leave the details to the interested reader.

5. Affinity of Cherednik algebras on projective space

In this section we prove the main result, which is a criterion for the affinity of Cherednik algebras on $\mathbb{P}(V)$.

5.1. Let V be a vector space and $W \subset \mathrm{GL}(V)$ a finite group. For each $(s, H) \in \mathcal{S}(V)$ and $(s, H^*) \in \mathcal{S}(V^*)$, we fix $\alpha_H \in V^*$ and $\alpha_H^\vee \in V$ such that $H = \operatorname{Ker} \alpha_H$ and $H^* = \operatorname{Ker} \alpha_H^\vee$, normalized so that $\alpha_H(\alpha_H^\vee) = 2$. Let $V^o = V - \{0\}$ and $\pi : V^o \to \mathbb{P}(V)$ be the quotient map. The map π is a principal T-bundle, where $T = \mathbb{C}^\times$ acts on V by dilations; i.e., $t \cdot v = t^{-1} v$ for $t \in T$ and $v \in V$. Since W acts on V it also acts on $\mathbb{P}(V)$. For each $s \in W$, $\operatorname{codim} \mathbb{P}(V)^s = 1$ if and only if s is a reflection, in which case $\mathbb{P}(V)^s = \mathbb{P}(H) \cup \mathbb{C} \cdot \alpha_H^\vee$.

Lemma 5.1.1. *We have* $\mathbb{H}^2(\mathbb{P}(V), \Omega_{\mathbb{P}}^{1,2}) \simeq \mathbb{C}$, *and the morphism* β *of* (A.3.2) *is an isomorphism.*

Proof. For each $n \in \mathbb{Z}$, let λ_n be the character of $\mathbb{C}^\times$ given by $t \mapsto t^n$. Then, $(\pi_\bullet \mathcal{O}_{V^o})^{\lambda_n} \simeq \mathcal{O}(n)$. This implies that β is injective. Therefore, it suffices to show that $\dim \mathbb{H}^2(\mathbb{P}(V), \Omega_{\mathbb{P}}^{1,2}) = 1$. Since $\mathbb{P}(V)$ can be covered by open sets isomorphic to $\mathbb{A}^{n-1}$, and $H_{\mathrm{DR}}^i(\mathbb{A}^{n-1}) = 0$ for $i \neq 0$, the algebraic de Rham complex is acyclic.

This implies that the map $d\mathcal{O}_{\mathbb{P}}[-1] \to \Omega^{1,2}_{\mathbb{P}}$ is a quasi-isomorphism. Therefore, the map $H^1(\mathbb{P}(V), d\mathcal{O}_{\mathbb{P}}) = \mathbb{H}^2(\mathbb{P}(V), d\mathcal{O}_{\mathbb{P}}[-1]) \to \mathbb{H}^2(\mathbb{P}(V), \Omega^{1,2}_{\mathbb{P}})$ is an isomorphism. The long exact sequence associated to the short exact sequence

$$0 \longrightarrow \mathbb{C}_{\mathbb{P}} \longrightarrow \mathcal{O}_{\mathbb{P}} \longrightarrow d\mathcal{O}_{\mathbb{P}} \longrightarrow 0$$

shows that $H^1(\mathbb{P}(V), d\mathcal{O}_{\mathbb{P}}) \simeq H^2(\mathbb{P}(V), \mathbb{C}_{\mathbb{P}})$ is one-dimensional. □

Lemma 5.1.1 implies the well-known fact that twisted differential operators on projective space are locally isomorphic, in the Zariski topology, to the usual differential operators. We identify $\mathbb{H}^2(\mathbb{P}(V), \Omega^{1,2}_{\mathbb{P}})$ with $\mathbb{C}$ so that if $\omega = n \in \mathbb{Z}$, then $\mathcal{D}^{\omega}_{\mathbb{P}(V)}$ acts on $\mathcal{O}(n)$. The action of W on $\mathbb{H}^2(\mathbb{P}(V), \Omega^{1,2}_{\mathbb{P}})$ is trivial; therefore the sheaf $\mathcal{D}^{\omega}_{\mathbb{P}(V)}$ is W-equivariant for all ω.

5.2. When $X = V$, the *rational Cherednik algebra* $\mathsf{H}_{\mathbf{c}}(V, W)$, as introduced by Etingof and Ginzburg, can be described as an algebra given by generators and relations. Namely, it is the quotient of the skew group algebra $T(V \oplus V^*) \rtimes W$ by the ideal generated by the relations

$$[x, x'] = 0, \quad [y, y'] = 0, \quad [y, x] = x(y) - \sum_{s \in \mathcal{S}} \mathbf{c}(s) \alpha_H(y) x(\alpha_H^{\vee}) s \qquad (5.2.1)$$

for all $x, x' \in V^*$ and $y, y' \in V$. Let $x_1, \ldots, x_n$ be a basis of V^* and $y_1, \ldots, y_n \in V$ the dual basis. The Euler element is

$$\mathbf{h} = \sum_{i=1}^{n} x_i y_i - \sum_{s \in \mathcal{S}} \frac{2\mathbf{c}(s)}{1 - \lambda_s} s = \sum_{i=1}^{n} y_i x_i - n + \sum_{s \in \mathcal{S}} 2\mathbf{c}(s) \left(1 - \frac{1}{1 - \lambda_s}\right) s.$$

One can easily check that $[\mathbf{h}, x] = x$, $[\mathbf{h}, y] = -y$ and $[\mathbf{h}, w] = 0$ for all $x \in V^*$, $y \in V$ and $w \in W$. The element $\mathbf{h}$ defines an internal grading on $\mathsf{H}_{\mathbf{c}}(V, W)$, where $\deg(x) = 1$, $\deg(y) = -1$ and $\deg(w) = 0$. The m-th graded piece of $\mathsf{H}_{\mathbf{c}}(V, W)$ is denoted by $\mathsf{H}_{\mathbf{c}}(V, W)_m$.

5.3. ***Dunkl embedding.*** The open subset $U = V - D$ of V is the complement to the zero locus of $\prod_{s \in \mathcal{S}} \alpha_H$. For $y \in V$, thought of as a constant coefficient differential operator, the corresponding Dunkl operator D_y equals

$$\partial_y + \sum_{s \in \mathcal{S}} \frac{2\mathbf{c}(s)}{1 - \lambda_s} \frac{\alpha_H(y)}{\alpha_H} (s - 1) \in \Gamma(U, \mathcal{D}_U \rtimes W).$$

The presentation of $\mathsf{H}_{\mathbf{c}}(V, W)$ given above is identified with the Cherednik algebra, defined in terms of Dunkl operators, via the injective algebra homomorphism

$$\mathsf{H}_{\mathbf{c}}(V, W) \hookrightarrow \Gamma(U, \mathcal{D}_U \rtimes W), \quad w \mapsto w,\ x \mapsto x,\ y \mapsto D_y$$

for all $w \in W$, $x \in V^*$ and $y \in V$. The image of $\mathbf{h}$ under the Dunkl embedding is

$$\mathbf{h} = \sum_{i=1}^{n} x_i \frac{\partial}{\partial x_i} - \sum_{s \in \mathcal{S}} \frac{2\mathbf{c}(s)}{1-\lambda_s}. \tag{5.3.1}$$

5.4. ***The sheaf of Cherednik algebras on*** $\mathbb{P}(V)$**.** Set $\rho_{\mathbf{c}} = \sum_{s \in \mathcal{S}} 2\mathbf{c}(s)/(1-\lambda_s)$. As noted in Example 2.20 of [Etingof 2004], the global sections of $\mathcal{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ are related to $\mathsf{H}_{\mathbf{c}}(V, W)$ as follows:

Lemma 5.4.1. *The space* $\mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ *of global sections equals*

$$\mathsf{H}_{\mathbf{c}}(V, W)_0/(\mathbf{h} + \rho_{\mathbf{c}} - \omega).$$

Proof. By Proposition 4.3.2, we have a morphism

$$\mathsf{H}_{\mathbf{c}}(V, W)_0 = \mathsf{H}_{\mathbf{c}}(V, W)^T \to \mathsf{H}_{\mathbf{c}}(V^o, W)^T \to \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W).$$

Equation (5.3.1) implies that the operator $\mathbf{h} + \rho_{\mathbf{c}} - \omega$ is in the kernel of this map because it is in the kernel of the composite

$$\mathsf{H}_{\mathbf{c}}(V, W)_0 \to \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W) \to \mathcal{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W) \hookrightarrow \mathcal{D}^{\omega}_{\mathbb{P}(V)}(D) \rtimes W.$$

To prove that $\mathsf{H}_{\mathbf{c}}(V, W)_0/(\mathbf{h} + \rho_{\mathbf{c}} - \omega) \to \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ is an isomorphism, we consider the associated graded morphism. We have

$$\mathrm{gr}_{\mathscr{F}} \mathsf{H}_{\mathbf{c}}(V, W)_0 = \mathbb{C}[x_i y_j \mid i, j = 1, \ldots, n] \rtimes W.$$

We claim that

$$\begin{aligned}\mathrm{gr}_{\mathscr{F}} \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W) &= \Gamma(\mathbb{P}(V), \pi_{\bullet}\mathcal{O}_{T^*\mathbb{P}(V)} \rtimes W) \\ &= \left(\mathbb{C}[x_i y_j \mid i, j = 1, \ldots, n] \Big/ \left(\sum_{i=1}^{n} x_i y_i\right)\right) \rtimes W.\end{aligned}$$

The second equality just follows from the usual description of $T^*\mathbb{P}(V)$ as the Hamiltonian reduction of $T^*V^o = V^o \times V^*$ with respect to the induced action of T. The first equality follows from Theorem 2.4.1, once one takes into account that the short exact sequences

$$0 \longrightarrow \mathscr{F}^{m-1}_{\omega,\mathbf{c}}(\mathbb{P}(V), W) \longrightarrow \mathscr{F}^{m}_{\omega,\mathbf{c}}(\mathbb{P}(V), W) \longrightarrow (\mathrm{Sym}^m \Theta_{\mathbb{P}(V)}) \otimes W \longrightarrow 0$$

imply by induction that $\mathbb{R}^i\Gamma(\mathscr{F}^{m}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)) = 0$ for $i > 0$. Therefore, the filtered morphism $\mathsf{H}_{\mathbf{c}}(V, W)_0 \to \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ is surjective, and hence so too is $\mathsf{H}_{\mathbf{c}}(V, W)_0/(\mathbf{h} + \rho_{\mathbf{c}} - \omega) \to \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$. On the other hand, the associated graded algebra of $\mathsf{H}_{\mathbf{c}}(V, W)_0/(\mathbf{h} + \rho_{\mathbf{c}} - \omega)$ is a quotient of the algebra

$$\left(\mathbb{C}[x_i y_j \mid i, j = 1, \ldots, n] / \left(\sum_{i=1}^{n} x_i y_i\right)\right) \rtimes W. \qquad \square$$

5.5. Let $\operatorname{Irr} W$ be the set of all isomorphism classes of irreducible W-modules. The element

$$\mathbf{z} := \sum_{s \in \mathcal{S}} 2\mathbf{c}(s)\left(1 - \frac{1}{1-\lambda_s}\right)s = -\mathbf{z}_0 + \sum_{s \in \mathcal{S}} 2\mathbf{c}(s)s$$

belongs to the center of $\mathbb{C}W$. For each $\lambda \in \operatorname{Irr} W$, let c_λ be the scalar by which $\mathbf{z}$ acts on λ and d_λ the scalar by which $\mathbf{z}_0$ acts on λ. Set

$$a_\lambda := \rho_{\mathbf{c}} + c_\lambda - n - \omega, \quad b_\lambda := \rho_{\mathbf{c}} - d_\lambda - \omega.$$

The sheaf of algebras $\mathcal{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ is said to be *affine* if the global sections functor Γ induces an equivalence of categories

$$\Gamma : \mathcal{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)\text{-Mod} \xrightarrow{\sim} \mathsf{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)\text{-Mod}.$$

Theorem 5.5.1. *Let a_λ and b_λ be as above.*

(1) *The functor Γ is exact, provided $a_\lambda \notin \mathbb{Z}_{\geq 0}$ for all $\lambda \in \operatorname{Irr} W$.*

(2) *The functor Γ is conservative, provided $b_\lambda \notin \mathbb{Z}_{>0}$ for all $\lambda \in \operatorname{Irr} W$.*

Hence, the sheaf of algebras $\mathcal{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$ is affine, provided $a_\lambda \notin \mathbb{Z}_{\geq 0}$ and $b_\lambda \notin \mathbb{Z}_{>0}$ for all $\lambda \in \operatorname{Irr} W$.

Our proof of Theorem 5.5.1 follows that of Theorem 1.6.5 in [Hotta et al. 2008].

Proof. The category of finitely generated $\mathsf{H}_c(V, W)$-modules supported on $\{0\} \subset V$ is denoted by $\mathcal{O}_-$. It is the category $\mathcal{O}$ for the rational Cherednik algebra as studied in [Ginzburg et al. 2003]. We use basic results from this article without reference. The element $\mathbf{h}$ acts locally finitely on modules in $\mathcal{O}_-$. The generalized eigenvalues of $\mathbf{h}$ on $M \in \mathcal{O}_-$ are the *weights* of M. Let $\Delta(\lambda)$, for $\lambda \in \operatorname{Irr} W$, denote the Verma modules in $\mathcal{O}_-$. It is isomorphic to $(\operatorname{Sym} V) \otimes \lambda$ as a $\operatorname{Sym} V \rtimes (\mathbb{C}W \otimes \mathbb{C}[\mathbf{h}])$-module. The weights of $\Delta(\lambda)$ are $c_\lambda - n - \mathbb{Z}_{\geq 0}$. If $M \in \mathcal{O}_-$, then there exist a projective module $P \in \mathcal{O}_-$ and a surjection $P \twoheadrightarrow M$. The fact that the module P has a Verma flag implies that the weights of M are contained in $\bigcup_{\lambda \in \operatorname{Irr} W} c_\lambda - n - \mathbb{Z}_{\geq 0}$. Therefore, zero is not a generalized eigenvalue of $\mathbf{h} + \rho_{\mathbf{c}} - \omega$ on M, provided $c_\lambda + \rho_{\mathbf{c}} - r - \omega - n \neq 0$ for all $r \in \mathbb{Z}_{\geq 0}$, i.e., provided $a_\lambda \notin \mathbb{Z}_{\geq 0}$.

Let $0 \to \mathcal{M}_1 \to \mathcal{M}_2 \to \mathcal{M}_3 \to 0$ be a short exact sequence in $\mathcal{H}_{\omega,\mathbf{c}}(\mathbb{P}(V), W)$-mod. By Theorem 4.4.1, the terms of the sequence $0 \to \pi^*\mathcal{M}_1 \to \pi^*\mathcal{M}_2 \to \pi^*\mathcal{M}_3 \to 0$ belong to $(\mathcal{H}_{\mathbf{c}}(V^o, W), T, \omega)$-mod. Moreover, the sequence is exact because π is smooth. Let $j : V^o \hookrightarrow V$. As noted in Lemma 3.8.1, the sheaves $\mathbb{R}^i j_\bullet(\pi^*\mathcal{M}_k)$ for $i \geq 0$ and $k = 1, 2, 3$ are $\mathsf{H}_{\omega,\mathbf{c}}(V, W)$-modules. The modules $\mathbb{R}^i j_\bullet(\pi^*\mathcal{M}_k)$ are supported on $\{0\}$ for all $i > 0$. Therefore, they belong to the ind-category $\operatorname{Ind} \mathcal{O}_-$. The global sections $\Gamma(\mathbb{P}(V), \mathcal{M}_k)$ are the element of the $\Gamma(V, j_\bullet\pi^*\mathcal{M}_k)^T$. Therefore

the long exact sequence

$$0 \longrightarrow \Gamma(V, j_\bullet \pi^* \mathcal{M}_1) \longrightarrow \Gamma(V, j_\bullet \pi^* \mathcal{M}_2) \longrightarrow \Gamma(V, j_\bullet \pi^* \mathcal{M}_3) \longrightarrow \Gamma(V, \mathbb{R}^1 j_\bullet (\pi^* \mathcal{M}_1)) \longrightarrow \cdots$$

gives rise to

$$0 \longrightarrow \Gamma(\mathbb{P}(V), \mathcal{M}_1) \longrightarrow \Gamma(\mathbb{P}(V), \mathcal{M}_2) \longrightarrow \Gamma(\mathbb{P}(V), \mathcal{M}_3) \longrightarrow \Gamma(V, \mathbb{R}^1 j_\bullet (\pi^* \mathcal{M}_1))^T \longrightarrow \cdots .$$

The space $\Gamma(V, \mathbb{R}^1 j_\bullet (\pi^* \mathcal{M}_1))^T$ can be identified with the space of generalized $\mathbf{h}$-eigenvectors in $\Gamma(V, \mathbb{R}^1 j_\bullet (\pi^* \mathcal{M}_1))$ with eigenvalue $\omega - \rho_{\mathfrak{c}}$. But if $a_\lambda \notin \mathbb{Z}_{\geq 0}$ for all λ, then this space is necessarily zero. Hence the sequence $0 \to \Gamma(\mathbb{P}(V), \mathcal{M}_1) \to \Gamma(\mathbb{P}(V), \mathcal{M}_2) \to \Gamma(\mathbb{P}(V), \mathcal{M}_3) \to 0$ is exact.

Next we need to show if $b_\lambda \notin \mathbb{Z}_{>0}$ for all $\lambda \in \operatorname{Irr} W$, then Γ is conservative; i.e., $\Gamma(\mathbb{P}(V), \mathcal{M}) = 0$ implies that $\mathcal{M} = 0$. Assume that $\mathcal{M} \neq 0$. Since π is smooth and surjective, it is faithfully flat and $\pi^* \mathcal{M} = 0$ implies that $\mathcal{M} = 0$. Hence $\pi^* \mathcal{M} \neq 0$. Since $\pi^* \mathcal{M}$ is (T, ω)-monodromic, the Euler element $\mathbf{h}$ acts semisimply on $\Gamma(V, j_\bullet \pi^* \mathcal{M})$, hence it decomposes as

$$\Gamma(V, j_\bullet \pi^* \mathcal{M}) = \bigoplus_{\alpha \in \mathbb{Z}} \Gamma(V, j_\bullet \pi^* \mathcal{M})_{\alpha + \omega - \rho_{\mathfrak{c}}}.$$

There is some $\alpha \in \mathbb{Z}$ for which $\Gamma(V, j_\bullet \pi^* \mathcal{M})_{\alpha+\omega-\rho_{\mathfrak{c}}} \neq 0$. We first assume that $\alpha > 0$. Choose $0 \neq m \in \Gamma(V, j_\bullet \pi^* \mathcal{M})_{\alpha+\omega-\rho_{\mathfrak{c}}}$. Since the space $\Gamma(V, j_\bullet \pi^* \mathcal{M})_{\alpha+\omega-\rho_{\mathfrak{c}}}$ is a W-module, we may assume that m lies in some irreducible W-isotypic component (of type λ say) of $\Gamma(V, j_\bullet \pi^* \mathcal{M})_{\alpha+\omega-\rho_{\mathfrak{c}}}$. We claim that there is some y such that $y \cdot m \neq 0$. Assume not; then $\mathbf{h} \cdot m = -d_\lambda m$. Hence $-d_\lambda = \alpha + \omega - \rho_{\mathfrak{c}}$; i.e., $b_\lambda = \rho_{\mathfrak{c}} - d_\lambda - \omega = \alpha \in \mathbb{Z}_{>0}$, contradicting our assumption on b_λ. Thus $y \cdot m \neq 0$. But $y \cdot m \in \Gamma(V, j_\bullet \pi^* \mathcal{M})_{\alpha-1+\omega-\rho_{\mathfrak{c}}}$, so eventually we get a nonzero vector in $\Gamma(V, j_\bullet \pi^* \mathcal{M})_{\omega-\rho_{\mathfrak{c}}}$ as required. Now, assume that $\alpha < 0$. If $m \in \Gamma(V^o, \pi^* \mathcal{M})_{\alpha+\omega-\rho_{\mathfrak{c}}}$ is a nonzero section, then the support of m is not contained in $\{0\}$. On the other hand, if $x \cdot m = 0$ for all $x \in V^*$, then $\operatorname{Supp}(m) \subset \{0\}$ and hence $m = 0$. Hence $m \neq 0$ implies that there exists some $x \in V^*$ such that $x \cdot m \neq 0$. Repeating this argument, we eventually conclude that $\Gamma(V^o, \pi^* \mathcal{M})_{\omega-\rho_{\mathfrak{c}}} \neq 0$. □

When W is trivial, Theorem 5.5.1 says that $\mathbb{P}(V)$ is $\mathscr{D}^\omega$-affine provided $\omega \notin \{-n, -n-1, \dots\}$, which equals the set of all $\omega \in \mathscr{A} \cup \mathscr{C}$ of [Van den Bergh 1991, Theorem 6.1.3].

Remark 5.5.2. The action of W on V induces an action of W on all the partial flag manifolds $\mathrm{GL}(V)/P$, where P is a parabolic of $\mathrm{GL}(V)$. However, one can check that there are reflections in $(\mathrm{GL}(V)/P, W)$ if and only if $\mathrm{GL}(V)/P = \mathbb{P}(V)$ or $\mathrm{GL}(V)/P$ is the Grassmannian of codimension-one subspaces in V.

5.6. ***Abelianization of W.*** In this section we assume that (V, W) is a complex reflection group. Pullback of melys morphisms can be used to relate the representation theory of $\mathsf{H}_{\mathbf{c}}(V, W)$ with that of $\mathsf{H}_{\mathbf{c}}(\Gamma)$, where Γ is a cyclic quotient of W. Let $\mathscr{A}$ denote the set of reflecting hyperplanes in V and, for each $H \in \mathscr{A}$, fix s_H a generator of the cyclic group $W_H = \{w \in W \mid w(H) = H\}$. Let $W_{\mathrm{ab}} = W/[W, W]$, and let $\chi_0, \ldots, \chi_{k-1}$ denote the linear characters of W, where $k = |W_{\mathrm{ab}}|$. For each i and $H \in \mathscr{A}$ we let $a_{i,H}$ be the least positive integer such that $\chi_i(s_H) = (\det s_H)^{a_{i,H}}$. We write $\mathbb{N}(W_{\mathrm{ab}})$ for the free semigroup generated by $\chi_0, \ldots, \chi_{k-1}$. Then there is an evaluation map $\mathbb{N}(W_{\mathrm{ab}}) \to \{\chi_0, \ldots, \chi_{k-1}\}$ which sends $\underline{\chi} = \sum_{i=0}^{k-1} n_i \chi_i$ to $\mathrm{ev}(\underline{\chi}) = \prod_{i=0}^{k-1} \chi_i^{n_i}$. For each $\underline{\chi} = \sum_{i=0}^{k-1} n_i \chi_i$, define

$$m_H = \sum_{i=0}^{k-1} n_i a_{i,H} \quad \text{and} \quad f_{\underline{\chi}} = \prod_{H \in \mathscr{A}} \alpha_H^{m_H} \in \mathbb{C}[V].$$

Then it follows from Stanley's results [1977] on W-semi-invariants that

$$w \cdot f_{\underline{\chi}} = \mathrm{ev}(\underline{\chi})(w) f_{\underline{\chi}} \quad \text{for all } w \in W.$$

Fix $\underline{\chi} \in \mathbb{N}(W_{\mathrm{ab}})$. The one-dimensional space spanned by $f_{\underline{\chi}}$ in $\mathbb{C}[V]$ is denoted by $\mathfrak{t}^*$. Inclusion $\mathfrak{t}^* \hookrightarrow \mathbb{C}[V]$ defines a W-equivariant morphism $\varphi : V \to \mathfrak{t}$. It is melys for any parameter $\mathbf{c}$ associated to $(\mathfrak{t}, W)$. Define $\mathbf{c}' : \mathscr{S}(V) \to \mathbb{C}$ by $\mathbf{c}'(s, H) = m_H\, \mathbf{c}(s, \{0\})$ for all (s, H) such that $(s, \{0\}) \in \mathscr{S}(\mathfrak{t})$, and $\mathbf{c}'(s, H) = 0$ otherwise. Corollary 3.5.1 implies:

Proposition 5.6.1. *Pullback by φ defines an exact functor*

$$\mathsf{H}_{\mathbf{c}}(\mathfrak{t}, W)\text{-Mod} \to \mathsf{H}_{\mathbf{c}'}(V, W)\text{-Mod}.$$

One can check that (3.4.2) implies that φ^* maps a module $M \in \mathbb{O}_{\mathbf{c}}(\mathfrak{t}, W)$ to $\varphi^* M \in \mathbb{O}_{\mathbf{c}'}(V, W)$, since the term h of (3.4.2) will be zero in this case. Moreover, for any such M, we have $\mathrm{GK\text{-}dim}(\varphi^* M) = \mathrm{GK\text{-}dim}(M) + \dim V - 1$. Let Γ be the cyclic group $W/\operatorname{Ker} \mathrm{ev}(\underline{\chi})$. Representations of the rational Cherednik algebra $\mathsf{H}_{\mathbf{c}}(\mathfrak{t}, W)$ can be viewed as W-equivariant representations of $\mathsf{H}_{\mathbf{c}}(\mathfrak{t}, \Gamma)$; see [Chmutova 2005].

Remark 5.6.2. More generally, if $\mathfrak{t}^* \subset \mathbb{C}[V]$ is an irreducible W-module, then we get a morphism $\varphi : V \to \mathfrak{t}$. It seems likely that one can use the theory developed in [Bessis et al. 2002] to classify all $\mathfrak{t}$ such that φ is melys. However, there do not seem to be many examples where $\dim \mathfrak{t} > 1$.

6. A local presentation of the Cherednik algebra

In this section we give a local presentation of the sheaf of Cherednik algebras.

6.1. In this section only, we make the following assumptions:

- For each $(w, Z) \in \mathcal{S}(X)$, there exists a globally defined function f_Z such that $Z = V(f_Z)$.
- All Picard algebroids considered can be trivialized in the Zariski topology.

We fix a choice of functions f_Z.

6.2. ***The* KZ*-connection.*** Recall that $U = X - \bigcup_{(w,Z)} Z$, where the union is over all (w, Z) in $\mathcal{S}(X)$. Since we have fixed a choice of defining equations of the hypersurfaces Z, it is possible to write down a KZ-connection on U.

Definition 6.2.1. The Knizhnik–Zamolodchikov connection on U, with values in $\mathcal{O}_U \otimes \mathbb{C}W$, is defined to be

$$\omega_{X,\mathbf{c}} = \sum_{(w,Z)\in\mathcal{S}(X)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} (d \log f_Z) \otimes s.$$

The KZ-connection behaves well under melys morphisms:

Lemma 6.2.2. *Let $\varphi : Y \to X$ be a surjective morphism, melys for* $\mathbf{c}$. *Then,* $\varphi^* \omega_{Y,\mathbf{c}} = \omega_{X,\varphi^*\mathbf{c}}$.

Proof. The fact that φ is surjective implies that $\varphi^* f_Z$ is not a unit for all $(w, Z) \in \mathcal{S}_{\mathbf{c}}(X)$. Then, the lemma follows from (3.4.2), since the term h there can be chosen to be zero. □

6.3. Fix $\omega \in \mathbb{H}^2(X, \Omega_X^{1,2})^W$, trivializable in the Zariski topology. For $(w, Z) \in \mathcal{S}(X)$ and $\nu_1, \nu_2 \in \mathcal{P}^\omega$, define

$$\Xi_Z^w(\nu_1, \nu_2) := i_{\sigma(\nu_1)}(d \log f_Z)(w(\nu_2) - \nu_2) - i_{\sigma(\nu_2)}(d \log f_Z)(w(\nu_1) - \nu_1)$$

in $\mathcal{P}^\omega(D)$.

Lemma 6.3.1. *Let $(w, Z) \in \mathcal{S}(X)$, $g \in \mathcal{O}_X$ and $\nu_1, \nu_2 \in \mathcal{P}^\omega$. Then,*

$$i_{\sigma(\nu)}(d \log f_Z)(w(g) - g) \in \mathcal{O}_X \quad \textit{and} \quad \Xi_Z^w(\nu_1, \nu_2) \in \mathcal{P}^\omega.$$

Proof. If $g \in \mathcal{O}_X$ and $\nu \in \mathcal{P}^\omega$, then $i_{\sigma(\nu)}(d \log f_Z)(w(g) - g) \in \mathcal{O}_X$ because $w(g) - g \in I(Z)$. The second claim is that

$$\frac{\sigma(\nu_1)(f_Z)}{f_Z}(w(\nu_2) - \nu_2) - \frac{\sigma(\nu_2)(f_Z)}{f_Z}(w(\nu_1) - \nu_1) \in \mathcal{P}^\omega.$$

The statement is local and is clearly true in a neighborhood of any point of $X - Z$. Therefore, we may assume that we have fixed a point $x \in Z$. Choose a small, affine w-stable open subset U of X with coordinate system $x_1, \ldots, x_n$ such that $w(x_1) = \zeta x_1$ and $w(x_i) = x_i$ for $i \neq 1$. Moreover, since we have assumed that the Picard algebroid $\mathcal{P}^\omega$ trivializes in the Zariski topology, we may assume that

$\mathcal{P}^\omega|_U = \mathcal{O}_U \oplus \Theta_U$. There exists some unit $u \in \Gamma(U, \mathcal{O}_X)$ such that $f_Z = ux_1$. The statement is clear if either ν_1 or ν_2 is in $\Gamma(U, \mathcal{O}_X)$. Thus, without loss of generality, $\nu_1, \nu_2 \in \Gamma(U, \Theta_X)$. Expanding,

$$\Xi_Z^w(\nu_1, \nu_2) = \frac{\nu_1(x_1)}{x_1}(w(\nu_2) - \nu_2) - \frac{\nu_2(x_1)}{x_1}(w(\nu_1) - \nu_1) + h$$

for some $h \in \Gamma(U, \Theta_X)$. There are $f_i, g_i \in \Gamma(U, \mathcal{O}_X)$ such that $\nu_1 = \sum_{i=1}^n f_i(\partial/\partial x_i)$ and $\nu_2 = \sum_{i=1}^n g_i(\partial/\partial x_i)$. We have

$$\begin{aligned}
\frac{\nu_1(x_1)}{x_1}(w(\nu_2) - \nu_2) &= \sum_{i,j=1}^n f_i x_1^{-1} \frac{\partial x_1}{\partial x_i}\left(w(g_j)\frac{\partial}{\partial w(x_j)} - g_j\frac{\partial}{\partial x_j}\right) \\
&= \sum_{j=1}^n f_1 x_1^{-1}\left(w(g_j)\frac{\partial}{\partial w(x_j)} - g_j\frac{\partial}{\partial x_j}\right) \\
&= \sum_{j=1}^n f_1 x_1^{-1}\left((w(g_j) - g_j)\frac{\partial}{\partial w(x_j)} + g_j\left(\frac{\partial}{\partial w(x_j)} - \frac{\partial}{\partial x_j}\right)\right) \\
&= f_1 g_1 x_1^{-1}(\zeta - 1)\frac{\partial}{\partial x_1} + \sum_{j=1}^n f_1 x_1^{-1}\left((w(g_j) - g_j)\frac{\partial}{\partial w(x_j)}\right).
\end{aligned}$$

Thus, if we define

$$h_1 = \sum_{j=1}^n f_1 x_1^{-1}\left((w(g_j) - g_j)\frac{\partial}{\partial w(x_j)}\right), \quad h_2 = \sum_{j=1}^n g_1 x_1^{-1}\left((w(f_j) - f_j)\frac{\partial}{\partial w(x_j)}\right),$$

which belong to $\Gamma(U, \mathcal{P}^\omega)$, we have

$$\begin{aligned}
&\frac{\nu_1(x_1)}{x_1}(w(\nu_2) - \nu_2) - \frac{\nu_2(x_1)}{x_1}(w(\nu_1) - \nu_1) \\
&\qquad = f_1 g_1 x_1^{-1}(\zeta - 1)\frac{\partial}{\partial x_1} + h_1 - f_1 g_1 x_1^{-1}(\zeta - 1)\frac{\partial}{\partial x_1} - h_2 = h_1 - h_2,
\end{aligned}$$

which belongs to $\Gamma(U, \Theta_X)$. □

6.4. We define the sheaf of algebras $\mathcal{U}_{\omega,\mathbf{c}}(X, W)$ to be the quotient of $T\mathcal{P}^\omega \rtimes W$ by the relations

$$\nu \otimes g - g \otimes \nu = \sigma(\nu)(g) + \sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} i_{\sigma(\nu)}(d \log f_Z)(w(g) - g)w, \quad (6.4.1)$$

$$\nu_1 \otimes \nu_2 - \nu_2 \otimes \nu_1 = [\nu_1, \nu_2] + \sum_{(w,Z)} \frac{2\mathbf{c}(w, Z)}{1 - \lambda_{w,Z}} \Xi_Z^w(\nu_1, \nu_2)w \quad (6.4.2)$$

for all $\nu, \nu_1, \nu_2 \in \mathcal{P}_X^\omega$ and $g \in \mathbb{O}_X$, and the relation[3] $1_{\mathcal{P}} = 1$.

Remark 6.4.3. When $X = V$ is a vector space and $\nu_1, \nu_2 \in V$ are constant coefficient vector fields, the right-hand side of (6.4.2) is zero and we get the usual relations of the rational Cherednik algebra.

Proposition 6.4.4. *The map $\nu \mapsto D_\nu$, $w \mapsto w$ for $\nu \in \mathcal{P}^\omega$ and $w \in W$ defines an isomorphism $\mathcal{U}_{\omega,\mathbf{c}}(X, W) \xrightarrow{\sim} \mathcal{H}_{\omega,\mathbf{c}}(X, W)$ if and only if the* KZ*-connection is flat.*

Proof. The proof is a direct calculation. It is straightforward to see that relation (6.4.1) always holds in $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$. Therefore, we just need to check that relation (6.4.2) holds for Dunkl operators in $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ if and only if the KZ-connection is flat. Let $\nu_1, \nu_2 \in \mathcal{P}_X^\omega$, and D_{ν_1}, D_{ν_2} the corresponding Dunkl operators. We need to calculate the right-hand side of

$$[D_{\nu_1}, D_{\nu_2}]$$
$$= \left[\nu_1 + \sum_{(w,Z)} \frac{2\mathbf{c}(w,Z)}{1-\lambda_{w,Z}} \frac{\sigma(\nu_1)(f_Z)}{f_Z}(w-1),\ \nu_2 + \sum_{(w,Z)} \frac{2\mathbf{c}(w,Z)}{1-\lambda_{w,Z}} \frac{\sigma(\nu_2)(f_Z)}{f_Z}(w-1) \right].$$

We have

$$\left[\frac{\sigma(\nu_1)(f_Z)}{f_Z}(w-1), \nu_2 \right] = \frac{\sigma(\nu_2)\circ\sigma(\nu_1)(f_Z)}{f_Z}(w-1) - \frac{\sigma(\nu_1)(f_Z)\sigma(\nu_2)(f_Z)}{f_Z^2}(w-1) + \frac{\sigma(\nu_1)(f_Z)}{f_Z}(w(\nu_2)-\nu_2)w,$$

and hence

$$\sum_{(w,Z)} \frac{2\mathbf{c}(w,Z)}{1-\lambda_{w,Z}} \left(\left[\frac{\nu_1(f_Z)}{f_Z}(w-1), \nu_2 \right] + \left[\nu_1, \frac{\nu_2(f_Z)}{f_Z}(w-1) \right] \right)$$

equals

$$\sum_{(w,Z)} \frac{2\mathbf{c}(w,Z)}{1-\lambda_{w,Z}} \left(\frac{[\nu_1,\nu_2](f_Z)}{f_Z}(w-1) + \frac{\nu_1(f_Z)}{f_Z}(w(\nu_2)-\nu_2)w - \frac{\nu_2(f_Z)}{f_Z}(w(\nu_1)-\nu_1)w \right).$$

Also,

$$\left[-\frac{\nu_1(f_Z)}{f_Z}w_1, \frac{\nu_2(f_{Z'})}{f_{Z'}} \right] + \left[\frac{\nu_1(f_Z)}{f_Z}, -\frac{\nu_2(f_{Z'})}{f_{Z'}}w_2 \right] + \left[\frac{\nu_1(f_Z)}{f_Z}w_1, \frac{\nu_2(f_{Z'})}{f_{Z'}}w_2 \right]$$

[3] Recall from Definition A.1.1 that $1_{\mathcal{P}}$ is defined to be the image of $1 \in \mathbb{O}_X$ under the map $i : \mathbb{O}_X \to \mathcal{P}$.

equals

$$-\frac{\nu_1(f_Z)}{f_Z}w_1\left(\frac{\nu_2(f_{Z'})}{f_{Z'}}\right)(w_1-1)+\frac{\nu_2(f_{Z'})}{f_{Z'}}w_2\left(\frac{\nu_1(f_Z)}{f_Z}\right)(w_2-1)$$
$$+\frac{\nu_1(f_Z)}{f_Z}w_1\left(\frac{\nu_2(f_{Z'})}{f_{Z'}}\right)w_1w_2-\frac{\nu_2(f_{Z'})}{f_{Z'}}w_2\left(\frac{\nu_1(f_Z)}{f_Z}\right)w_2w_1.$$

Combining the above equations, one sees that relation (6.4.2) holds for Dunkl operators in $\mathcal{H}_{\omega,\mathbf{c}}(X, W)$ if and only if

$$\sum_{\substack{(w_1,Z)\\(w_2,Z')}}\frac{4\mathbf{c}(w_1,Z)\mathbf{c}(w_2,Z')}{(1-\lambda_{w_1,Z})(1-\lambda_{w_2,Z'})}\left(\frac{\nu_2(f_Z)}{f_Z}\frac{\nu_1(f_{Z'})}{f_{Z'}}-\frac{\nu_1(f_Z)}{f_Z}\frac{\nu_2(f_{Z'})}{f_{Z'}}\right)w_1w_2=0.$$

Since the left-hand side equals

$$\left(\sum_{\substack{(w_1,Z)\\(w_2,Z')}}\frac{4\mathbf{c}(w_1,Z)\mathbf{c}(w_2,Z')}{(1-\lambda_{w_1,Z})(1-\lambda_{w_2,Z'})}(d\log f_Z\wedge d\log f_{Z'})\otimes w_1w_2\right)(\nu_2,\nu_1),$$

it will be zero for all ν_1, ν_2 if and only if the meromorphic two-form inside the bracket is zero. But this two-form is the curvature $\omega_{X,\mathbf{c}}\wedge\omega_{X,\mathbf{c}}$ of the KZ-connection. □

Proposition 6.4.4 implies that when the KZ-connection is flat, the algebra $\mathcal{U}_{\omega,\mathbf{c}}(X, W)$ is, up to isomorphism, independent of the choice of functions f_Z.

Appendix: TDOs

In the appendix we summarize the facts we need about twisted differential operators, following [Beilinson and Bernstein 1993] and [Kashiwara 1989].

A.1. ***Twisted differential operators.*** It is most natural to realize a sheaf of algebras of twisted differential operators as a quotient of the enveloping algebra of a Picard algebroid.

Definition A.1.1. An $\mathbb{O}_X$-module $\mathcal{L}$ is called a *Lie algebroid* if there exists a bracket $[-,-]:\mathcal{L}\otimes_{\mathbb{C}_X}\mathcal{L}\to\mathcal{L}$ and morphism of $\mathbb{O}_X$-modules $\sigma:\mathcal{L}\to\Theta_X$ (the anchor map) such that $(\mathcal{L},[-,-])$ is a sheaf of Lie algebras with the anchor map being a morphism of Lie algebras, and, for $l_1, l_2\in\mathcal{L}$ and $f\in\mathbb{O}_X$,

$$[l_1, fl_2]=f[l_1,l_2]+\sigma(l_1)(f)l_2.$$

If, moreover, there exists a map $i:\mathbb{O}_X\to\mathcal{L}$ of $\mathbb{O}_X$-modules such that the sequence

$$0\longrightarrow\mathbb{O}_X\longrightarrow\mathcal{L}\longrightarrow\Theta_X\longrightarrow 0$$

is exact and $i(1):=1_{\mathcal{L}}$ is central in $\mathcal{L}$, then $\mathcal{L}$ is called a *Picard algebroid*.

As in [Beilinson and Bernstein 1993], we denote by $\Omega_X^{1,2}$ the two-term subcomplex $\Omega_X^1 \xrightarrow{d} (\Omega_X^2)^{\mathrm{cl}}$, concentrated in degrees 1 and 2, of the algebraic de Rham complex of X.

Proposition A.1.2. *The Picard algebroids on X are parametrized up to isomorphism by $\mathbb{H}^2(X, \Omega_X^{1,2})$.*

Given $\omega \in \mathbb{H}^2(X, \Omega_X^{1,2})$, the corresponding Picard algebroid is denoted by $\mathcal{P}_X^\omega$. Associated to $\mathcal{P}_X^\omega$ is $\mathcal{D}_X^\omega$, the sheaf of differential operators on X with twist ω. It is the quotient of the enveloping algebra $\mathcal{U}(\mathcal{P}_X^\omega)$ of $\mathcal{P}_X^\omega$ by the ideal generated by $1_{\mathcal{P}_X^\omega} - 1$.

Definition A.1.3. A module for the Picard algebroid $\mathcal{P}$ is a quasicoherent $\mathcal{O}_X$-module $\mathcal{M}$ together with a map $- \cdot - : \mathcal{P} \otimes_{\mathcal{O}_X} \mathcal{M} \to \mathcal{M}$ such that $i(f) \cdot m = fm$ and $[p, q] \cdot m = p \cdot (q \cdot m) - q \cdot (p \cdot m)$ for all $p, q \in \mathcal{P}$, $m \in \mathcal{M}$ and $f \in \mathcal{O}_X$.

There is a natural equivalence between the category of $\mathcal{P}^\omega$-modules and the category of $\mathcal{D}^\omega$-modules.

A.2. ***Functoriality.*** We recall from Section 2.2 of [Beilinson and Bernstein 1993] the functoriality properties of Picard algebroids and twisted differential operators. Fix a morphism $\varphi : Y \to X$. Let $\mathcal{P}_X$ be a Picard algebroid on X and $\mathcal{P}_Y$ a Picard algebroid on Y.

Definition A.2.1. A φ-morphism $\gamma : \mathcal{P}_Y \to \mathcal{P}_X$ is an $\mathcal{O}_Y$-linear map $\gamma : \mathcal{P}_Y \to \varphi^* \mathcal{P}_X$ such that for any section $p \in \mathcal{P}_Y$ and $\gamma(p) = \sum_i g^i \otimes q^i$ with $g_i \in \mathcal{O}_Y$ and $q_i \in \varphi^{-1}\mathcal{P}_X$, we have

$$\gamma([p_1, p_2]) = \sum_{i,j} g_1^i g_2^j \otimes [q_1^i, q_2^j] + \sum_j \sigma(p_1)(g_2^j) \otimes q_2^j - \sum_i \sigma(p_2)(g_1^i) \otimes q_1^i$$

and $\sigma(n)(f^* g) = \sum_i g^i \varphi^*(\sigma(q^i)(g))$ for all $g \in \varphi^{-1}\mathcal{O}_X$.

The first fundamental theorem on differential forms [Matsumura 1989, Theorem 25.1] implies that there is a morphism of sheaves $\varphi^{-1}\Omega_X^1 \to \Omega_Y^1$. This extends to a morphism of complexes $\varphi^{-1}\Omega_X^\bullet \to \Omega_Y^\bullet$ and $\varphi^{-1}\Omega_X^{1,2} \to \Omega_Y^{1,2}$. By functoriality of hypercohomology, we get a map $\varphi^* : \mathbb{H}^2(X, \Omega_X^{1,2}) \to \mathbb{H}^2(Y, \Omega_Y^{1,2})$. For $\omega \in \mathbb{H}^2(X, \Omega_X^{1,2})$, let $\mathcal{P}_X^\omega$ be the corresponding Picard algebroid and $\mathcal{P}_Y$ the fiber product $\varphi^* \mathcal{P}_X^\omega \times_{\varphi^* \Theta_X} \Theta_Y$, where $\varphi^* \mathcal{P}_X^\omega \to \varphi^* \Theta_X$ is the anchor map and $\Theta_Y \to \varphi^* \Theta_X$ is $d\varphi$.

Lemma A.2.2. *The sheaf $\mathcal{P}_Y$ is a Picard algebroid, $\psi : \mathcal{P}_Y \to \varphi^* \mathcal{P}_X$ is a φ-morphism and we have an isomorphism of Picard algebroids $\mathcal{P}_Y \simeq \mathcal{P}_Y^{\varphi^* \omega}$.*

Thus, by definition, the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_Y & \longrightarrow & \mathcal{P}_Y^{\varphi^*\omega} & \xrightarrow{\sigma_Y} & \Theta_Y & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow & & \\ & & \mathcal{O}_Y = \varphi^*\mathcal{O}_X & \longrightarrow & \varphi^*\mathcal{P}_X^{\omega} & \xrightarrow{\sigma_X} & \varphi^*\Theta_X & & \end{array}$$

commutes. The projection $\mathcal{P}_Y^{\varphi^*\omega} \to \varphi^*\mathcal{P}_X^{\omega}$ extends to a morphism $\mathcal{D}_Y^{\varphi^*\omega} \to \varphi^*\mathcal{D}_X^{\omega}$, making $\varphi^*\mathcal{D}_X^{\omega}$ a left $\mathcal{D}_Y^{\varphi^*\omega}$-module. Let $\mathcal{M}$ be a left $\mathcal{D}_X^{\omega}$-module. Since $\varphi^*\mathcal{M} = \varphi^*\mathcal{D}_X^{\omega} \otimes_{\varphi^{-1}\mathcal{D}_X^{\omega}} \varphi^{-1}\mathcal{M}$, we have:

Proposition A.2.3. *For any $\mathcal{M} \in \mathcal{D}_X^{\omega}$-Mod, the sheaf $\varphi^*\mathcal{M}$ is a $\mathcal{D}_Y^{\varphi^*\omega}$-module.*

Remark A.2.4. If φ is étale, then $d\varphi : \Theta_Y \to \varphi^*\Theta_X$ is an isomorphism. Therefore, the projection $\mathcal{P}_Y^{\varphi^*\omega} \to \varphi^*\mathcal{P}_X^{\omega}$ is also an isomorphism and, in this case, the isomorphism $\gamma : \mathcal{D}_Y^{\varphi^*\omega} \to \varphi^*\mathcal{D}_X^{\omega}$ of left $\mathcal{D}_Y^{\varphi^*\omega}$-modules is actually an algebra isomorphism (in particular, $\varphi^*\mathcal{D}_X^{\omega}$ is a sheaf of algebras).

A.3. ***Monodromic $\mathcal{D}$-modules.*** Let T be a torus, i.e., a product of copies of the multiplicative group $\mathbb{C}^\times$. The Lie algebra of T is denoted by $\mathfrak{t}$. Let $\pi : Y \to X$ be a principal T-bundle, with X smooth. A common way of constructing sheaves of twisted differential operators on X is by quantum Hamiltonian reduction. Let $\mu : \mathfrak{t} \to \mathcal{D}_Y$ be the differential of the action of T on Y. Since $\mathcal{D}_Y$ is a T-equivariant sheaf, there is a stalkwise action of T on $\pi_\bullet\mathcal{D}_Y$. The map μ is T-equivariant and, since T acts trivially on $\mathfrak{t}$, μ descends to a map $\mathfrak{t} \to (\pi_\bullet\mathcal{D}_Y)^T$. The image of μ is central. Given a character $\chi : \mathfrak{t} \to \mathbb{C}$, let

$$\mathcal{D}_{X,\chi} := (\pi_\bullet\mathcal{D}_Y)^T / \langle \{\mu(t) - \chi(t) \mid t \in \mathfrak{t}\} \rangle. \tag{A.3.1}$$

Let $\mathbb{X}(T)$ be the lattice of characters of T. By differentiation, we may identify $\mathbb{X}(T)$ with a lattice in $\mathfrak{t}^*$ such that $\mathbb{X}(T) \otimes_{\mathbb{Z}} \mathbb{C} = \mathfrak{t}^*$. Given $\lambda \in \mathbb{X}(T)$, the sheaf of λ-semi-invariant sections $(\pi_\bullet\mathcal{O}_Y)^\lambda$ is a line bundle on X. Thus, we have a map $\mathbb{X}(T) \to H^1(X, \mathcal{O}_X^\times)$. Composing this with the map $\mathcal{O}_X^\times \xrightarrow{d\log} \mathrm{Ker}(d : \Omega_X^1 \to \Omega_X^2) \subset \Omega_X^{1,2}$ gives a map

$$\beta_{\mathbb{Z}} : \mathbb{X}(T) \longrightarrow H^1(X, \mathcal{O}_X^\times) \xrightarrow{d\log} \mathbb{H}^2(X, \Omega_X^{1,2})$$

of $\mathbb{Z}$-modules. Extending scalars, we get a map

$$\beta : \mathfrak{t}^* \to \mathbb{H}^2(X, \Omega_X^{1,2}). \tag{A.3.2}$$

Proposition A.3.3. *The sheaf of algebras $\mathcal{D}_{X,\chi}$ is a sheaf of twisted differential operators, isomorphic to $\mathcal{D}_X^{\beta(\chi)}$.*

Sketch of proof. Let $\lambda \in \mathbb{X}(T)$ and $\mathscr{L} := (\pi_\bullet \mathcal{O}_Y)^\lambda$ be the corresponding line bundle on X. If χ is the differential of λ, then (A.3.1) implies that $\mathscr{D}_{X,\chi}$ acts on $\mathscr{L}$. As explained in [Beilinson and Bernstein 1993, Section 2.1.12], this implies that $\mathscr{D}_{X,\chi} \simeq \mathscr{D}_X^{\beta_{\mathbb{Z}}(\chi)}$. The fact that this extends to an isomorphism $\mathscr{D}_{X,\chi} \simeq \mathscr{D}_X^{\beta(\chi)}$ for all $\chi \in \mathfrak{t}^*$ follows from the Baer sum construction, as explained in [ibid., Section 2.1.3]. □

Acknowledgments

The authors would like to thank Colin Ingalls, Anne Shepler and Cédric Bonnafé for fruitful discussions. The first author is supported by the EPSRC grant EP-H028153.

References

[Beilinson and Bernstein 1993] A. Beilinson and J. Bernstein, "A proof of Jantzen conjectures", pp. 1–50 in *I. M. Gel'fand Seminar*, edited by S. Gel'fand and S. Gindikin, Adv. Soviet Math. **16**, Amer. Math. Soc., Providence, RI, 1993. MR 95a:22022 Zbl 0790.22007

[Van den Bergh 1991] M. Van den Bergh, "Differential operators on semi-invariants for tori and weighted projective spaces", pp. 255–272 in *Topics in invariant theory* (Paris, 1989–1990), edited by M.-P. Malliavin, Lecture Notes in Math. **1478**, Springer, Berlin, 1991. MR 93h:16046 Zbl 0802.13005

[Bessis et al. 2002] D. Bessis, C. Bonnafé, and R. Rouquier, "Quotients et extensions de groupes de réflexion", *Math. Ann.* **323**:3 (2002), 405–436. MR 2003g:20066 Zbl 1053.20037

[Borho and Brylinski 1989] W. Borho and J.-L. Brylinski, "Differential operators on homogeneous spaces, II: Relative enveloping algebras", *Bull. Soc. Math. France* **117**:2 (1989), 167–210. MR 90j:17023 Zbl 0702.22019

[Chmutova 2005] T. Chmutova, "Twisted symplectic reflection algebras", preprint, 2005. arXiv math/0505653

[Etingof 2004] P. Etingof, "Cherednik and Hecke algebras of varieties with a finite group action", preprint, 2004. arXiv math/0406499v3

[Etingof and Ginzburg 2002] P. Etingof and V. Ginzburg, "Symplectic reflection algebras, Calogero–Moser space, and deformed Harish-Chandra homomorphism", *Invent. Math.* **147**:2 (2002), 243–348. MR 2003b:16021 Zbl 1061.16032

[Fulton 1998] W. Fulton, *Intersection theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics **2**, Springer, Berlin, 1998. MR 99d:14003 Zbl 0885.14002

[Ginzburg et al. 2003] V. Ginzburg, N. Guay, E. Opdam, and R. Rouquier, "On the category $\mathcal{O}$ for rational Cherednik algebras", *Invent. Math.* **154**:3 (2003), 617–651. MR 2005f:20010 Zbl 1071.20005

[Hotta et al. 2008] R. Hotta, K. Takeuchi, and T. Tanisaki, *D-modules, perverse sheaves, and representation theory*, Progress in Mathematics **236**, Birkhäuser, Boston, 2008. MR 2008k:32022 Zbl 1136.14009

[Kashiwara 1989] M. Kashiwara, "Representation theory and D-modules on flag varieties", pp. 55–109 in *Orbites unipotentes et représentations, III: Orbites et faisceaux pervers*, Astérisque **173-174**, Soc. Math. France, Paris, 1989. MR 90k:17029 Zbl 0705.22010

[Matsumura 1989] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1989. MR 90i:13001 Zbl 0666.13002

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980. MR 81j:14002 Zbl 0433.14012

[Stanley 1977] R. P. Stanley, "Relative invariants of finite groups generated by pseudoreflections", *J. Algebra* **49**:1 (1977), 134–148. MR 57 #477 Zbl 0383.20029

[Wilcox 2011] S. J. Wilcox, *Representations of the rational Cherednik algebra*, thesis, Harvard University, Cambridge, MA, 2011, http://search.proquest.com/docview/878131539. MR 2941903 arXiv 1012.2585v2

Communicated by J. Toby Stafford
Received 2013-07-29 Revised 2014-02-17 Accepted 2014-03-31

gwyn.bellamy@glasgow.ac.uk *School of Mathematics and Statistics, University of Glasgow, 15 University Gardens, Glasgow, G12 8QW, United Kingdom*

ohmymo@googlemail.com

msp

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1179

Cosemisimple Hopf algebras are faithfully flat over Hopf subalgebras

Alexandru Chirvasitu

The question of whether or not a Hopf algebra H is faithfully flat over a Hopf subalgebra A has received positive answers in several particular cases: when H (or more generally, just A) is commutative, cocommutative, or pointed, or when K contains the coradical of H. We prove the statement in the title, adding the class of cosemisimple Hopf algebras to those known to be faithfully flat over all Hopf subalgebras. We also show that the third term of the resulting "exact sequence" $A \to H \to C$ is always a cosemisimple coalgebra, and that the expectation $H \to A$ is positive when H is a CQG algebra.

Introduction

The issue of faithful flatness of a Hopf algebra (always over a field) over its Hopf subalgebras arises quite naturally in several ways. One direction is via the so-called Kaplansky conjecture [1975], which initially asked whether or not Hopf algebras are free over Hopf subalgebras (as an analogue to the Lagrange theorem for finite groups). The answer was known to be negative, with a counterexample appearing in [Oberst and Schneider 1974], but it is true in certain particular cases: using the notation in the abstract, H is free over A whenever H is finite-dimensional (the Nichols–Zoeller theorem [Montgomery 1993, Theorem 3.1.5]), or pointed [Radford 1977b], or A contains the coradical of H [Radford 1977a, Corollary 2.3].

Montgomery then naturally asks whether one can get a positive result by requiring only faithful flatness of a Hopf algebra over an arbitrary Hopf subalgebra [1993,

MSC2010: primary 16T20; secondary 16T15, 16T05, 20G42.

Keywords: cosemisimple Hopf algebra, CQG algebra, faithfully flat, right coideal subalgebra, quotient left module coalgebra, expectation.

Question 3.5.4]. Again, this turns out not to work in general (see [Schauenburg 2000] and also [Chirvasitu 2010], where the same problem is considered in the context of whether or not epimorphisms of Hopf algebras are surjective), but one has positive results in several important cases, such as when A is commutative [Arkhipov and Gaitsgory 2003, Proposition 3.12] or H is cocommutative ([Takeuchi 1972, Theorem 3.2], which also takes care of the case when H is commutative). The most recent version of the question, asked in [Schauenburg 2000], seems to be whether or not a Hopf algebra with bijective antipode is faithfully flat over Hopf subalgebras with bijective antipode.

Another way to get to the faithful flatness issue is via the problem of constructing quotients of affine group schemes. We recall briefly how this goes.

Let $A \to H$ be an inclusion of commutative Hopf algebras; in scheme language, A and H are affine groups, and the inclusion means that $\operatorname{spec}(A)$ is a quotient group scheme of $\operatorname{spec}(H)$. The Hopf-algebraic analogue of the kernel of this epimorphism is the quotient Hopf algebra $\pi : H \to C = H/HA^+$, where A^+ stands for the kernel of the counit of A. The map π is then *normal*, in the sense of [Andruskiewitsch and Devoto 1995, Definition 1.1.5]:

$$\mathrm{LKER}(\pi) = \{a \in A \mid (\pi \otimes \mathrm{id}) \circ \Delta(a) = 1_C \otimes a\}$$

equals its counterpart

$$\mathrm{RKER}(\pi) = \{a \in A \mid (\mathrm{id} \otimes \pi) \circ \Delta(a) = a \otimes 1_C\}.$$

This means precisely that $\operatorname{spec}(C)$ is a normal affine subgroup scheme of $\operatorname{spec}(A)$ [Takeuchi 1972, Lemma 5.1]. This gives a map $A \mapsto C$ from quotient affine group schemes of H to normal subgroup schemes. One naturally suspects that this is probably a bijective correspondence, and this is indeed true (see [Takeuchi 1972, Theorem 4.3] and also [Demazure and Gabriel 1970, III §3, 7.2]). In Takeuchi's paper, faithful flatness is crucial in proving half of this result, namely, the injectivity of the map $A \mapsto C$: one recovers A as $\mathrm{LKER}(\pi)$.

Many of the technical arguments and constructions appearing in this context go through in the noncommutative setting, so one might naturally be led to the faithful flatness issue by trying to mimic the algebraic group theory in a more general setting, where Hopf algebras are viewed as function algebras on a "quantum" group. This is, for example, the point of view taken in the by now very rich and fruitful theory of compact quantum groups, first introduced and studied by Woronowicz: the main characters are certain C^* algebras A with a comultiplication $A \to A \underline{\otimes} A$ (the minimal C^* tensor product), imitating the algebras of continuous functions on compact groups (we refer the reader to [Klimyk and Schmüdgen 1997, Chapter 11] or Woronowicz's landmark papers [1987; 1988] for details).

These objects are not quite Hopf algebras, but for any compact quantum group A as above, one can introduce a genuine Hopf algebra $\mathcal{A}$, imitating the algebra of *representative* functions on a compact group (i.e., the linear span of matrix coefficients of finite-dimensional unitary representations), and which contains all the relevant information on the representation theory of the quantum group in question. The abstract properties of such Hopf $(*)$-algebras have been axiomatized, and they are usually referred to as compact quantum group (CQG) algebras (see [Klimyk and Schmüdgen 1997, Section 11.3] or the original paper [Dijkhuizen and Koornwinder 1994], where the term was coined). They are always cosemisimple (as an analogue of Peter–Weyl theory for representations of compact groups), which is why we hope that despite the seemingly restrictive hypothesis of cosemisimplicity, the results in the present paper might be useful apart from any intrinsic interest, at least in dealing with Hopf-algebraic issues arising in the context of compact quantum groups.

We now describe the contents of the paper.

In the first section we introduce the conventions and notation to be used throughout the rest of the paper, and also develop the tools needed to prove the main results. In Section 1A we set up a Galois correspondence between the set of right coideal subalgebras of a Hopf algebra H and the set of quotient left module coalgebras of H. We then recall basic results on categories of objects imitating Sweedler's Hopf modules: These have both a module and a comodule structure, one of them over a Hopf algebra H, and the other one over a right coideal subalgebra or a quotient left module coalgebra of H. These categories are used extensively in the subsequent discussion.

Section 2 is devoted to the main results. We provide sufficient conditions for faithful flatness over Hopf subalgebras in Theorem 2.1 and Corollary 2.4. We also investigate the case of cosemisimple H further, proving in Theorem 2.5 that for any Hopf subalgebra A, the quotient left H-module coalgebra $C = H/HA^+$ is always cosemisimple. This quotient is the third term of the "exact sequence" which completes the inclusion $A \to H$, and the question of whether or not C is cosemisimple arises naturally in the course of the proof of Theorem 2.1, which shows immediately that the answer is affirmative when HA^+ happens to be an ideal (both left *and* right).

Finally, in Section 3 we show that when the ambient Hopf algebra H is CQG, the "expectation" $H \to A$ that plays a crucial role in the preceding section is positive. In the course of the proof we use a sort of "A-relative" Fourier transform from H to C^* (whereas ordinary Fourier transforms, as in, say, [Podleś and Woronowicz 1990], are roughly speaking more like maps from H to the dual H^*). This construction has some of the familiar properties from harmonic analysis, such as intertwining products and "convolution products" (Proposition 3.11(1)), playing well with $*$ structures (Proposition 3.11(2)), and satisfying a Plancherel-type condition Remark 3.12.

1. Preliminaries

In this section we make the preparations necessary to prove the main results. Throughout, we work over a fixed field k, so all algebras and coalgebras are to be taken over k. The reader should feel free to assume k to be algebraically closed whenever convenient, as most results are invariant under scalar extension. In Section 3 we specialize to characteristic zero.

We assume basic familiarity with coalgebra and Hopf algebra theory, for example as presented in [Montgomery 1993]. We will make brief use of the notion of coring over a (not necessarily commutative) k-algebra; we refer to [Brzezinski and Wisbauer 2003] for basic properties and results.

The notation is standard: Δ_C and ε_C stand for comultiplication and the counit of the coalgebra C respectively, and we will allow ourselves to drop the subscript when it is clear which coalgebra is being discussed. Similarly, S_H or S stands for the antipode of the Hopf algebra H, 1_A (or just 1) will be the unit of the algebra A, etc. Sweedler notation for comultiplication is used throughout: $\Delta(h) = h_1 \otimes h_2$, as well as for left or right coactions: if $\rho : N \to N \otimes C$ ($\rho : N \to C \otimes N$) is a right (left) C-comodule structure, we write $n_0 \otimes n_1$ ($n_{\langle -1\rangle} \otimes n_{\langle 0\rangle}$) for $\rho(n)$. We sometimes adorn the indices with parentheses, as in $\Delta(c) = c_{(1)} \otimes c_{(2)}$.

We will also be working extensively with categories of (co)modules over (co)algebras, as well as categories of objects admitting both a module and a comodule structure, compatible in some sense that will be made precise below (see Section 1A). These categories are always denoted by the letter $\mathcal{M}$, with left (right) module structures appearing as left (right) subscripts, and left (right) comodule structures appearing as left (right) superscripts. All such categories are abelian (and in fact Grothendieck), and the forgetful functor from each of them to vector spaces is exact. The one exception from this notational convention is the category of k-vector spaces, which we simply call VEC.

Recall that the category $\mathcal{M}_f^H$ of finite-dimensional right comodules over a Hopf algebra is monoidal left rigid: every object V has a left dual V^* (at the level of vector spaces it is just the usual dual vector space), and one has adjunctions $(\otimes V, \otimes V^*)$ and $(V^* \otimes, V \otimes)$ (the left-hand member of the pair is the left adjoint) on $\mathcal{M}_f^H$.

We also use the correspondence between subcoalgebras of a Hopf algebra H and finite-dimensional (right) comodules over H: for such a comodule V, there is a smallest subcoalgebra $D = \mathrm{COALG}(V) \leq H$ such that the structure map $V \to V \otimes H$ factors through $V \to V \otimes D$. Conversely, if $D \leq H$ is a simple subcoalgebra, then we denote by V_D the simple right D-comodule, viewed as a right H-comodule. Then, for simple subcoalgebras $D, E \leq H$, the product ED will be precisely $\mathrm{COALG}(V_E \otimes V_D)$, while $S(D)$ is $\mathrm{COALG}(V^*)$.

For a coalgebra C, the symbol $\widehat{C}$ denotes the set of isomorphism classes of simple (right, unless specified otherwise) C-comodules.

1A. ***Descent data and adjunctions.*** We will be dealing with the kind of situation studied extensively in [Takeuchi 1979]: H will be a Hopf algebra, and for most of this section (and in fact the paper), $\iota : A \to H$ will be a right coideal subalgebra, while $\pi : H \to C$ will be a quotient left H-module coalgebra. Recall that this means that A is a right coideal of H ($\Delta_H(A) \leq A \otimes H$) as well as a subalgebra, and so the induced map $A \to A \otimes H$ is an algebra map; similarly, C is the quotient of H by a left ideal as well as a coalgebra, and the induced map $H \otimes C \to C$ is supposed to be a coalgebra map.

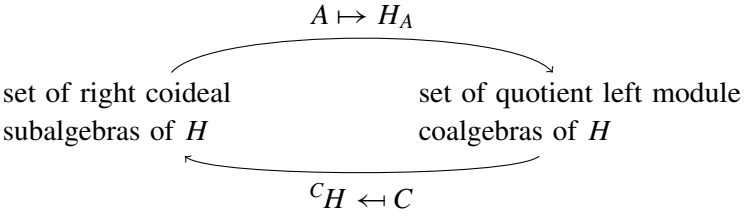
Given a coalgebra map $\pi : H \to C$, we write $\bar{h}$ for $\pi(h)$, $h \in H$. In this situation, H will naturally be both a left and a right C-comodule (via the structure maps $(\pi \otimes \mathrm{id}) \circ \Delta_H$ and $(\mathrm{id} \otimes \pi) \circ \Delta_H$ respectively), while C has a distinguished grouplike element $\bar{1}$, where $1 \in H$ is the unit. Write

$$ {}^{\pi}H = {}^{C}H\{h \in H \mid \overline{h_1} \otimes h_2 = \bar{1} \otimes h\}, \quad H^{\pi} = H^{C} = \{h \in H \mid h_1 \otimes \overline{h_2} = h \otimes \bar{1}\}. $$

These are what were called $\mathrm{LKER}(\pi)$ and $\mathrm{RKER}(\pi)$ back in the introduction, following the notation in [Andruskiewitsch and Devoto 1995]. They are the spaces of $\bar{1}$-coinvariants under the left and right coaction of C on H respectively, in the sense of [Brzezinski and Wisbauer 2003, Section 28.4].

Dually, let $\iota : A \to H$ be an algebra map, and set $A^+ = \iota^{-1}(\ker \varepsilon_H)$. Write $H_\iota = H_A$ for the left H-module $H/H\iota(A^+)$, and similarly, ${}_\iota H = {}_A H = H/\iota(A^+)H$.

It is now an easy exercise to check that if $\iota : A \to H$ is a right coideal subalgebra, then H_A is a quotient left module coalgebra, and, vice versa, if $\pi : H \to C$ is the projection on a quotient left module coalgebra, then ${}^{C}H$ is a right coideal subalgebra of H.



In the above diagram, the maps are order-reversing with respect to the obvious poset structures on the two sets (whose partial orders we write as $\preceq$)

Remark 1.1. Note that the two order-reversing maps form a *Galois connection* in the sense of [Mac Lane 1998, Section IV.5] between the poset of right coideal subalgebras and the poset of left module quotient coalgebras.

Definition 1.2. Let $\iota : A \to H$ be a right coideal subalgebra and $\pi : H \to C$ a quotient left module coalgebra. We call $\pi : H \to H_A$ (or H_A itself) the *right reflection* of $\iota : A \to H$ or of A, and $\iota : {}^C H \to H$ (or ${}^C H$ itself) the *left reflection* of $\pi : H \to C$. We also write $r(A)$ and $r(C)$ for H_A and ${}^C H$.

Using this language, recall from [Andruskiewitsch and Devoto 1995, Proposition 1.2.3]:

Definition 1.3. Let H be a Hopf algebra. For a right coideal subalgebra $A \to H$ and a quotient left module coalgebra $H \to C$, we say that $k \to A \to H \to C \to k$ is *exact* if A and C are each other's reflections.

We usually drop the k and talk just about exact sequences $A \to H \to C$.

If H is a Hopf algebra and C is a left H-module coalgebra, then ${}^C_H\mathcal{M}$ will be the category of left H-modules endowed with a left C-comodule structure which is a left H-module map from M to $C \otimes M$ (where the latter has the left H-module structure induced by the comultiplication on H). Similarly, if A is a right H-comodule algebra, then $\mathcal{M}_A^H$ is the category of right H-comodules with a right A-module structure such that $M \otimes A \to M$ is a map of right H-comodules. The morphisms in each of these categories are required to preserve both structures.

Let $\iota : A \to H$ be a right coideal subalgebra and $\pi : H \to C$ a quotient left module coalgebra such that $\pi \circ \iota$ factors through $A \ni a \mapsto \varepsilon(a)\bar{1} \in C$ (this is equivalent to saying that $A \preceq r(C)$, or $C \preceq r(A)$, in the two posets discussed before Definition 1.2). Then, there is an adjunction between the categories ${}_A\mathcal{M}$ and ${}^C_H\mathcal{M}$, and dually, an adjunction between $\mathcal{M}_A^H$ and $\mathcal{M}^C$. We will recall briefly how these are defined, omitting most of the proofs, which are routine.

Let $M \in {}_A\mathcal{M}$. The vector space $H \otimes_A M$ then has a left H-module structure, as well as a left C-comodule structure inherited from the left C-coaction on H (checking this is where the condition $A \preceq r(C)$ is needed). This defines a functor $L : {}_A\mathcal{M} \to {}^C_H\mathcal{M}$. To go in the other direction, for $N \in {}^C_H\mathcal{M}$, let

$$R(N) = \{n \in N \mid n_{\langle -1 \rangle} \otimes n_{\langle 0 \rangle} = \bar{1} \otimes n\}. \tag{1}$$

This defines a functor, and, as the notation suggests, L is a left adjoint to R.

For the other adjunction, given $M \in \mathcal{M}_A^H$, define $L'(M) = M/MA^+$. This is a functor (with the obvious definition on morphisms), and it is left adjoint to $R' : \mathcal{M}^C \to \mathcal{M}_A^H$ defined by $R'(N) = N \,\square_C\, H$; the latter has a right H-comodule structure obtained by making H coact on itself, as well as a right A-module structure obtained from the right A-action on H.

Let us now focus on the adjunction ${}_A\mathcal{M} \longleftrightarrow {}^C_H\mathcal{M}$. In [Takeuchi 1979], the same discussion is carried out in a slightly less general situation: the adjunction described above is considered in the case $A = r(C)$. On the other hand, we remark that when $C = r(A)$, the category ${}^C_H\mathcal{M}$ introduced above is nothing but the category of

descent data for the ring extension $A \to H$. Recall from [Brzezinski and Wisbauer 2003, Proposition 25.4] that in our case this would be the category ${}^{H\otimes_A H}\mathcal{M}$ of left comodules over the canonical H-coring $H \otimes_A H$ associated to the algebra extension $A \to H$. This means left H-modules M with an appropriately coassociative and counital left H-module map $\rho : M \mapsto (H \otimes_A H) \otimes_H M \cong H \otimes_A M$.

The usual bijection

$$H \otimes H \cong H \otimes H, \quad h \otimes k \mapsto h_1 \otimes h_2 k$$

is easily seen to descend to a bijection $H \otimes_A H \cong r(A) \otimes H$. Hence, we see that a map ρ as above is the same thing as a map $\psi : M \mapsto r(A) \otimes M$. The other properties of ρ, namely, being a coassociative, counital, left H-module map, precisely translate to ψ being coassociative, counital, and a left H-module map, respectively. Taking into account this equivalence ${}^{r(A)}_{H}\mathcal{M} \simeq {}^{H\otimes_A H}\mathcal{M}$, the adjunction $(L, R) : {}_A\mathcal{M} \longleftrightarrow {}^{r(A)}_{H}\mathcal{M}$ is an equivalence as soon as H is right faithfully flat over A (this is the faithfully flat descent theorem; see [Nuss 1997, Theorem 3.8]).

Apart from faithful flatness, other criteria are known to ensure (L, R) is an equivalence. To state one such, we recall some notation from [Mesablishvili 2006].

For a ring A, consider the contravariant endofunctor ${}_AC_A$ on the category of A-bimodules defined by

$${}_AC_A(M) = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z});$$

these are homomorphisms of abelian groups, with the usual A-bimodule structure induced from that on M. Then, [ibid., Theorem 8.1] (very slightly rephrased) reads:

Theorem. *If $\iota : A \to H$ is a map of rings such that ${}_AC_A(\iota) : {}_AC_A(H) \to {}_AC_A(A)$ is a split epimorphism, then $H\otimes_A$ is an equivalence between ${}_A\mathcal{M}$ and ${}^{H\otimes_A H}\mathcal{M}$.*

Since we have just observed that in our case the functor $H\otimes_A$ from the statement of the theorem can be identified with $L : {}_A\mathcal{M} \to {}^{r(A)}_{H}\mathcal{M}$, we get the following result as a consequence:

Proposition 1.4. *With the previous notation, $(L, R) : {}_A\mathcal{M} \longleftrightarrow {}^{r(A)}_{H}\mathcal{M}$ is an equivalence if the inclusion $\iota : A \to H$ splits as an A-bimodule map.* □

Remark 1.5. The paper [Mesablishvili 2006] deals with rings rather than Hopf algebras. To deduce Proposition 1.4 one uses the noted identification ${}^{r(A)}_{H}\mathcal{M} \simeq {}^{H\otimes_A H}\mathcal{M}$ to turn the problem into the usual formulation of descent for arbitrary rings. Sections 7 and 8 of [ibid.] spell this out.

As a kind of converse to the faithfully flat descent theorem, (L, R) being an equivalence implies that H is right A-faithfully flat. Indeed, $H\otimes_A$ is then exact on ${}_A\mathcal{M}$. Note that we are using the fact that ${}^{r(A)}_{H}\mathcal{M}$ is abelian, with the same exact sequences as VEC. All in all, this proves:

Proposition 1.6. *Let $\iota : A \to H$ be a right coideal subalgebra. The adjunction*

$$(L,\, R) : {}_A\mathcal{M} \longleftrightarrow {}^{r(A)}_{H}\mathcal{M}$$

is an equivalence if and only if H is right A-faithfully flat. □

Remark 1.7. This result is very similar in spirit to the equivalence (5) $\iff$ (3) in [Schneider 1990, Theorem I], or to (1) $\iff$ (2) in [Schauenburg and Schneider 2005, Lemma 1.7]. These can all be deduced from much more general, coring-flavored descent theorems that are now available, such as, say, [Caenepeel et al. 2007, Theorem 2.7].

1B. ***CQG algebras.*** For background, we rely mainly on [Klimyk and Schmüdgen 1997, 11.3–11.4] or the paper [Dijkhuizen and Koornwinder 1994], where these objects were originally introduced. Recall briefly that these Hopf algebras are meant to have just enough structure to imitate algebras of representative functions on compact groups. This means they are complex $*$-algebras (they possess conjugate-linear involutive multiplication-reversing automorphisms $*$) as well as Hopf algebras, and the two structures are compatible in the sense that the comultiplication and the counit are both $*$-algebra homomorphisms.

In addition, CQG algebras are required to have *unitarizable* comodules. This is a condition we will not spell out in any detail, but it says essentially that every finite-dimensional comodule has an inner product compatible with the coaction in some sense (once more imitating the familiar situation for compact groups, where invariant inner products on representations can be constructed by averaging against the Haar measure). In particular, CQG algebras are automatically cosemisimple, and hence fit comfortably into the setting of Section 2.

Not all $*$-algebras have enveloping C^*-algebras, but CQG algebras do. See, e.g., [Klimyk and Schmüdgen 1997, Section 11.3.3]. Such a completion is a so-called *full*, or *universal*, C^*-algebraic compact quantum group, in the sense that it is a (unital) C^*-algebra A endowed with coassociative C^*-algebra homomorphism $A \to A \otimes A$ (minimal C^* tensor product) with additional conditions ([Klimyk and Schmüdgen 1997, Section 11.3.3, Proposition 32] or [Dijkhuizen and Koornwinder 1994, §4–5]).

On the very few occasions when tensor product C^*-algebras come up, $\otimes$ always denotes the smallest C^* tensor product (as treated in [Wegge-Olsen 1993, T.5], for instance). The term *completely positive map* between C^*-algebras will also make brief appearances. Recall that a linear map $T : A \to B$ between C^*-algebras is said to be positive if for each $x \in A$ we have $T(x^*x) = y^*y$ for some $y \in B$, and completely positive [Takesaki 2002, Section IV.3] if the maps

$$\mathrm{id} \otimes T : M_n \otimes A \to M_n \otimes B$$

between matrix algebras are all positive.

2. Main results

We now prove the statement from the title of the paper:

Theorem 2.1. *A cosemisimple Hopf algebra is faithfully flat over all its Hopf subalgebras.*

Proof. Let H be cosemisimple, and $\iota : A \to H$ an inclusion of a Hopf subalgebra. Combining Propositions 1.6 and 1.4, it suffices to show that ι splits as an A-bimodule map. In fact, one can even find a subcoalgebra $B \leq H$ with $H = A \oplus B$ as A-bimodules.

Let I be the set of simple subcoalgebras of H, and J the subset of I consisting of subcoalgebras contained in A. One then has $H = \bigoplus_I D$ and $A = \bigoplus_J D$. Define $B = \bigoplus_{I \setminus J} D$; in other words, B is the direct sum of those simple subcoalgebras of H which are not in A. Clearly, B is a subcoalgebra and $H = A \oplus B$, and we now only need to check that B is invariant under (either left or right) multiplication by A.

Let $D \in J$ and $E \in I \setminus J$ be simple subcoalgebras of A and B respectively. The product ED inside H is then $\mathrm{COALG}(V_E \otimes V_D)$ (see last paragraph above Section 1A). Now assume $F \in J$ is a summand of ED. This means $V_F \leq V_E \otimes V_D$, so $V_E^* \leq V_D \otimes V_F^*$. This is absurd: V_E^* is a B-comodule, while $V_D \otimes V_F^*$ is an A-comodule. □

Remark 2.2. This proves the first part of [Wang 2009, Conjecture 1]; the second part, stating the faithful coflatness of a CQG algebra over quotient CQG algebras, follows immediately from the cosemisimplicity of CQG algebras.

Remark 2.3. Examples of cosemisimple Hopf algebras which are not faithfully coflat over *quotient* Hopf algebras abound, at least in characteristic zero.

Indeed, let G be a reductive complex algebraic group and B a Borel subgroup. Denoting by $\mathbb{O}(\bullet)$ "regular functions on the variety $\bullet$", the Hopf algebra $H = \mathbb{O}(G)$ is cosemisimple (e.g., [Fogarty 1969, p. 178]), and it surjects onto $C = \mathbb{O}(B)$.

If the surjection $H \to C$ were to be faithfully coflat, then, by [Takeuchi 1979, Theorem 2], we could reconstruct C as H/HA^+ for $A = r(C)$. But A is simply the algebra of global regular functions on the projective variety G/B, and hence consists only of constants; this provides the contradiction.

In fact, the result can be strengthened slightly. Recall that the *coradical* C_0 of a coalgebra C is the sum of all its simple subcoalgebras.

Corollary 2.4. *A Hopf algebra H whose coradical H_0 is a Hopf subalgebra is faithfully flat over its cosemisimple Hopf subalgebras.*

Proof. Any cosemisimple Hopf subalgebra $A \leq H$ will automatically be contained in the coradical H_0. By the previous corollary, H_0 is faithfully flat over A. On the

other hand, Hopf algebras are faithfully flat (and indeed free) over sub-bialgebras which contain the coradical [Radford 1977b, Corollary 1]; in particular, in this case, H is faithfully flat over H_0. The conclusion follows. □

Now let us place ourselves in the setting of Theorem 2.1, assuming in addition that the Hopf subalgebra $A \to H$ is *conormal* in the language of [Andruskiewitsch and Devoto 1995]. This simply means that $HA^+ = A^+H$, and is equivalent to $C = r(A)$ being a quotient Hopf algebra of H rather than just a quotient coalgebra [Andruskiewitsch and Devoto 1995, Definition 1.1.9]. Recalling the decomposition $H = A \oplus B$ as a direct sum of subcoalgebras, C breaks up as the direct sum of the coalgebras $k = k\bar{1}$ and B/BA^+. In other words, the coalgebra spanned by the unit of the Hopf algebra C has a coalgebra complement in C. It follows from the equivalence of (c) and (f) in [Sweedler 1969, Theorem 14.0.3] that C is a cosemisimple Hopf algebra. Our aim in the rest of this section is to extend this result to the general case covered by Theorem 2.1:

Theorem 2.5. *If $\iota : A \to H$ is a Hopf subalgebra of a cosemisimple Hopf algebra H, then the coalgebra $C = r(A)$ is cosemisimple.*

Proof. We know from Theorem 2.1 that H is right A-faithfully flat, and hence also left faithfully flat (just flip everything by means of the bijective antipode). This then implies, for example by [Takeuchi 1979, Theorem 1], that the second adjunction we introduced above, $(L', R') : \mathcal{M}_A^H \longleftrightarrow \mathcal{M}^C$, is an equivalence. It is then enough to show that all objects of the category $\mathcal{M}_A^H$ are projective, and this is precisely what the next two results do. □

Definition 2.6. An object of $\mathcal{M}_A^H$ is said to be *A-projective* if it is projective as an A-module.

Proposition 2.7. *Under the hypotheses of Theorem 2.5, every object of $\mathcal{M}_A^H$ is A-projective.*

Proof. Let $M \in \mathcal{M}_A^H$ be an arbitrary object. Endow $M \otimes H$ with a right H-comodule structure by making H coact on itself, and also a right A-module structure by the diagonal right action (i.e., $M \otimes H$ is the tensor product in the monoidal category $\mathcal{M}_A$). It is easy to check that these are compatible in the sense that they make $M \otimes H$ into an object of $\mathcal{M}_A^H$, and the map $\rho : m \mapsto m_{\langle 0 \rangle} \otimes m_{\langle 1 \rangle} \in M \otimes H$ giving M its right H-comodule structure is actually a morphism in $\mathcal{M}_A^H$. Similarly, $\mathrm{id} \otimes \varepsilon_H : M \otimes H \to M$ is a morphism in $\mathcal{M}_A$, and it splits the inclusion ρ. It follows that it is enough to show that the object $M \otimes H \in \mathcal{M}_A^H$ described above is A-projective.

Theorem 2.1 says that H is A-faithfully flat, and it follows from [Masuoka and Wigner 1994, Corollary 2.9] that it is then (left and right) A-projective. This means that $M \otimes H$ can be split embedded (in the category $\mathcal{M}_A$) into a direct sum of copies

of $M \otimes A$ with the diagonal right action of A. But

$$M \otimes A \to M \otimes A, \quad m \otimes a \mapsto ma_1 \otimes a_2$$

exhibits an isomorphism from $M \otimes A$ with the right A-action on the right tensorand to $M \otimes A$ with the diagonal A-action (its inverse is $m \otimes a \mapsto mS(a_1) \otimes a_2$). This means that in $\mathcal{M}_A$, $M \otimes H$ is a direct summand of a direct sum of copies of A, thus projective. □

Proposition 2.8. *Under the hypotheses of Theorem 2.5, A-projective objects of $\mathcal{M}_A^H$ are projective.*

Before going into the proof, we need some preparation, including additional notation to keep track of the several A-module or H-comodule structures that might exist on the same object.

As in the proof of Theorem 2.1, denote by I and $J \subseteq J$ the sets of simple right comodules over H and A, respectively. Recall that these are also in one-to-one correspondence with the simple subcoalgebras of H and A, respectively. We will henceforth denote by $\varphi : H \to A$ the map which is the identity on A and sends every simple subcoalgebra $D \in I \setminus J$ to 0.

Notice now that A acts on H (as well as on itself) not just by the usual right regular action, but also by the right adjoint action: $h \triangleleft a = S(a_1)ha_2$ ($h \in H$, $a \in A$). This gives H and A a second structure as objects in $\mathcal{M}_A^H$. When working with this structure rather than the obvious one, we denote these objects by H_{ad} and A_{ad}.

Lemma 2.9. (a) *For any object $M \in \mathcal{M}_A^H$, $M \otimes H_{\mathrm{ad}}$ becomes an object of $\mathcal{M}_A^H$ when endowed with the diagonal A-action* (*where A acts on $M \in \mathcal{M}_A^H$ and on H by the right adjoint action*) *and the diagonal H-coaction.*

(b) *Similarly, $M \otimes A_{\mathrm{ad}} \in \mathcal{M}_A^H$.*

(c) $\mathrm{id} \otimes \varphi : M \otimes H_{\mathrm{ad}} \to M \otimes A_{\mathrm{ad}}$ *respects the structures from* (a) *and* (b), *and hence is a morphism in $\mathcal{M}_A^H$.*

Proof. We will only prove (a); (b) is entirely analogous, while (c) follows immediately, since φ clearly preserves both the right H-coaction and the adjoint A-action.

Proving (a) amounts to checking that the diagram

$$\begin{array}{ccc} M \otimes H_{\mathrm{ad}} \otimes A & \longrightarrow & M \otimes H_{\mathrm{ad}} \\ \downarrow & & \downarrow \\ M \otimes H_{\mathrm{ad}} \otimes H \otimes A & \longrightarrow & M \otimes H_{\mathrm{ad}} \otimes H \end{array}$$

is commutative. The path passing through the upper horizontal line is

$$m \otimes h \otimes a \longmapsto ma_1 \otimes S(a_2)ha_3 \longmapsto m_0a_1 \otimes S(a_4)h_1a_5 \otimes m_1a_2S(a_3)h_2a_6,$$

while the other composition is

$$m \otimes h \otimes a \longmapsto m_0 \otimes h_1 \otimes m_1h_2 \otimes a \longmapsto m_0a_1 \otimes S(a_2)h_1a_3 \otimes m_1h_2a_4.$$

Using the properties of the antipode and counit in a Hopf algebra, we have

$$\begin{aligned} m_0a_1 \otimes S(a_4)h_1a_5 \otimes m_1a_2S(a_3)h_2a_6 &= m_0a_1 \otimes S(\varepsilon(a_2)a_3)h_1a_4 \otimes m_1h_2a_5 \\ &= m_0a_1 \otimes S(a_2)h_1a_3 \otimes m_1h_2a_4, \end{aligned}$$

concluding the proof. □

Now denote by $(M \otimes H)^r \in \mathcal{M}_A^H$ the object from the proof of Proposition 2.7: the A-action is diagonal, while H coacts on the right tensorand alone. The upper r is meant to remind the reader of this.

Lemma 2.10. *For $M \in \mathcal{M}_A^H$, the map $\psi_M : M \otimes H \to M \otimes H$ defined by*

$$m \otimes h \longmapsto m_0 \otimes S(m_1)h$$

is a morphism in $\mathcal{M}_A^H$ from $(M \otimes H)^r$ to $M \otimes H_{\mathrm{ad}}$.

Proof. We only check compatibility with the A-actions, leaving H-coactions to the reader. The composition $(M \otimes H)^r \otimes A \longrightarrow (M \otimes H)^r \longrightarrow M \otimes H_{\mathrm{ad}}$ is

$$m \otimes h \otimes a \longmapsto ma_1 \otimes ha_2 \overset{\psi_M}{\longmapsto} m_0a_1 \otimes S(m_1a_2)ha_3,$$

while the other relevant composition is

$$m \otimes h \otimes a \overset{\psi_M \otimes \mathrm{id}}{\longmapsto} m_0 \otimes S(m_1)h \otimes a \longmapsto m_0a_1 \otimes S(a_2)S(m_1)ha_3.$$

Since S is an algebra antimorphism, they are equal. □

Finally, we have:

Lemma 2.11. *Let $M \in \mathcal{M}_A^H$. The map $M \otimes A \to M$ giving M its A-module structure is a morphism $M \otimes A_{\mathrm{ad}} \to M$ in $\mathcal{M}_A^H$.*

Proof. Compatibility with the H-coactions is built into the definition of the category $\mathcal{M}_A^H$, so one only needs to check that the map is a morphism of A-modules. In other words, we must show that the diagram

$$\begin{array}{ccc} M \otimes A_{\mathrm{ad}} \otimes A & \longrightarrow & M \otimes A_{\mathrm{ad}} \\ \downarrow & & \downarrow \\ M \otimes A & \longrightarrow & M \end{array}$$

is commutative. The right-down composition is

$$m \otimes a \otimes b \longmapsto mb_1 \otimes S(b_2)ab_3 \longmapsto mb_1 S(b_2)ab_3,$$

while the other composition is

$$m \otimes a \otimes b \longmapsto ma \otimes b \longmapsto mab;$$

they are thus equal. □

Lemma 2.12. *For $M \in \mathcal{M}_A^H$, the composition*

$$t_M : (M \otimes H)^r \xrightarrow{\psi_M} M \otimes H_{\mathrm{ad}} \xrightarrow{\mathrm{id}\otimes\varphi} M \otimes A_{\mathrm{ad}} \longrightarrow M,$$

where the last arrow gives M its A-module structure, is a natural transformation from the $\mathcal{M}_A^H$-endofunctor $(\bullet \otimes H)^r$ to the identity functor, and it exhibits the latter as a direct summand of the former.

Proof. The fact that t_M is a map in $\mathcal{M}_A^H$ follows from Lemmas 2.9, 2.10 and 2.11. Naturality is immediate (one simply checks that it holds for each of the three maps), as is the fact that t_M is a left inverse of the map $M \to (M \otimes H)^r$ giving M its H-comodule structure. □

We are now ready to prove the result we were after:

Proof of Proposition 2.8. Let $P \in \mathcal{M}_A^H$ be an A-projective object. We must show that $\mathcal{M}_A^H(P, \bullet)$ is an exact functor. Embedding the identity functor as a direct summand into $(\bullet \otimes H)^r$ (Lemma 2.12), it suffices to show that $\mathcal{M}_A^H(P, (\bullet \otimes H)^r)$ is exact.

The functor $(\bullet \otimes H)^r : \mathcal{M}_A \to \mathcal{M}_A^H$ is right adjoint to forget : $\mathcal{M}_A^H \to \mathcal{M}_A$ (as $\mathcal{M}_A^H$ is the category of coalgebras for the comonad $\bullet \otimes H$ on $\mathcal{M}_A$; see [Mac Lane 1998, Theorem VI.2.1]), so $\mathcal{M}_A^H(P, (\bullet \otimes H)^r)$ is naturally isomorphic to $\mathcal{M}_A(P, \bullet)$, which is exact by our assumption that P is A-projective. □

Remark 2.13. In the above proof, the forgetful functor forget : $\mathcal{M}_A^H \to \mathcal{M}_A$ has been suppressed in several places, in order to streamline the notation; we trust that this has not caused any confusion.

Remark 2.14. The proof of Proposition 2.7 is essentially a rephrasing of the usual proof that Hopf algebras H with a (right, say) integral sending 1_H to 1 are cosemisimple [Sweedler 1969, §14.0]; we will call such integrals unital. The map $\varphi : H \to A$ introduced in Lemma 2.9 might be referred to as an *A-valued right integral* (by which we mean a map preserving both the right H-comodule structure and the right adjoint action of A), and specializes to a unital integral when $A = k$. In conclusion, one way of stating Proposition 2.8 would be:

If the inclusion $\iota : A \to H$ of a right coideal subalgebra is split by an A-valued right integral, then the forgetful functor $\mathcal{M}_A^H \to \mathcal{M}_A$ reflects projectives.

Remark 2.15. Propositions 2.7 and 2.8 can both be traced back to work by Y. Di, but we have included proofs for completeness. Proposition 2.7, for instance, is a consequence of [Doi 1983, Theorem 4]. Similarly, Proposition 2.8 follows from [Doi 1990, Theorem 1]. I thank the referee for pointing this out.

3. Expectations on CQG subalgebras are positive

We now move the entire $A \to H \to C$ setting over to the case when H is a CQG algebra. We take for granted the preceding sections, and in particular the fact that C is cosemisimple (Theorem 2.5). The inclusion $\iota : A \to H$ is now one of $*$-algebras, and we follow the operator-algebraists' convention of referring to its left inverse $p : H \to A$ from the proof of Theorem 2.1 as the *expectation* of H on A (in accordance with a view of A and H as consisting of random variables on noncommutative measure spaces). Positivity here means the following:

Think of H as embedded in its universal C^* completion H_u (Section 1B), and complete A to A_u with the subspace norm. Then, p extends to a completely positive map $H_u \to A_u$. Equivalently, the self-map $\iota \circ p : H \to H$ lifts to a completely positive self-map of H_u.

Note that a functional $\psi \in H^*$ with $\psi(1) = 1$ extends to a state on the C^* completion H_u if and only if it is positive in the usual sense; i.e., $\psi(x^*x) \geq 0$ for every $x \in H$.

The main result of the section is this:

Theorem 3.1. *Let $\iota : A \to H$ be an inclusion of CQG algebras. Then, the expectation $p : H \to A$ is positive in the above sense.*

Remark 3.2. So-called *expected* C^*-subalgebras of (locally) compact quantum groups have featured prominently in the literature (see [Tomatsu 2007; Salmi and Skalski 2012] and references therein). The techniques used in the proof of Theorem 3.1 will be applied elsewhere to characterize all right coideal $*$-subalgebras A of a CQG algebra H which are expected in the sense of admitting a positive splitting of the inclusion as an A-bimodule, right H-comodule map, where positivity is understood as in Theorem 3.1.

Let us first reformulate the theorem slightly. Denote the unique unital (left and right) integral of C by h_C, and the composition $h_C \circ \pi$ by φ (where $\pi : H \to C$ is the surjection we start out with). The expectation decomposes as $(\varphi \otimes \mathrm{id}) \circ \Delta : H \to A$. This follows easily from the decomposition $H = A \oplus B$ as a direct sum of subcoalgebras used in the proof of Theorem 2.1, and the fact that $\varphi|_A$ equals ε_A and $\varphi|_B$ is the zero map.

Remark 3.3. Let us note in passing that φ is self-adjoint as a functional, in the sense that $\varphi(x^*)$ is the complex conjugate of $\varphi(x)$ for any $x \in H$. This follows

immediately from $\varphi|_A = \varepsilon_A$ and $\varphi|_B = 0$, the fact that A and B are closed under $*$, and the fact that ε is a $*$-homomorphism.

This observation is needed in the proof of item (2) in Proposition 3.11, for instance.

Lemma 3.4. *The conclusion of Theorem 3.1 holds if and only if the functional $\varphi \in H^*$ is positive.*

Proof. Note that φ equals $\varepsilon \circ p$ (more pedantically, in this expression ε is the restriction of ε_H to A). If p is positive then so is φ, given that ε is a $*$-algebra map $A \to \mathbb{C}$ which lifts to A_u.

Conversely, if φ is positive (and hence lifts to a state on H_u), then both maps in the composition $(\varphi \otimes \mathrm{id}) \circ \Delta : H \to H$ lift to completely positive maps on the appropriate C^* completions (Δ lifts to a C^*-algebra map $H_u \to H_u \otimes H_u$, while $\varphi \otimes \mathrm{id} : H_u \otimes H_u \to H_u$ will also be completely positive). But that composition is precisely $\iota \circ p$, as noted above. □

Remark 3.5. The identity $\varphi = \varepsilon \circ p$, in particular, shows that $\varphi \circ S = \varphi$. This is needed below.

We are going to take what looks like a detour to make the necessary preparations.

For a cosemisimple coalgebra D over an algebraically closed field, denote by $D^\bullet$ its *restricted dual*: the direct sum of the matrix algebras dual to the matrix subcoalgebras of D. In general, $D^\bullet$ is a nonunital algebra. In our case, the full dual H^* is in addition a (unital) $*$-algebra, with $*$ operation defined by

$$f^*(x) = f((Sx)^*)^* \quad \text{for all } x \in H, \tag{2}$$

where the outer $*$ means complex conjugation of a number (see, e.g., [Van Daele 1998, Proposition 4.3]). Furthermore, $C^\bullet \leq H^*$ is a $*$-subalgebra.

Finally, again for a cosemisimple coalgebra D, we will talk about its completion $\bar{D}$; this is by definition the direct product of the matrix subcoalgebras comprising D. Equivalently, $\bar{D}$ is the (ordinary, vector space) dual of $D^\bullet$. The module structure $H \otimes C \to C$ extends to an action of H on $\bar{C}$.

Remark 3.6. This extension of the H-module structure to $\bar{C}$ is a simple enough observation, but there is some content to it. The claim is that for $x \in H$ and some simple subcoalgebra $C_\alpha \leq C$ (for $\alpha \in \widehat{C}$), there are only finitely many simple comodules $\beta \in \widehat{C}$ such that xC_β intersects C_α nontrivially.

Although $\mathcal{M}^C$ is not monoidal, $V \otimes W$ can be made sense of as a C-comodule for any H-comodule V and C-comodule W. This makes $\mathcal{M}^C$ into a *module category* over the monoidal category $\mathcal{M}^H$. Upon rephrasing the claim using the correspondence $W \mapsto \mathrm{COALG}(W)$ between comodules and subcoalgebras, it reads: for each finite-dimensional H-comodule V and each $\alpha \in \widehat{C}$, there are only finitely many $\beta \in \widehat{C}$

such that (identifying α, β with the corresponding comodules) $\mathrm{Hom}_{\mathcal{M}^C}(\alpha, V\otimes\beta)$ is nonzero. But just as in a rigid monoidal category, $V\otimes : \mathcal{M}^C \to \mathcal{M}^C$ is right adjoint to $V^*\otimes$, and hence we're saying only finitely many β satisfy $\mathrm{Hom}(V^*\otimes\alpha, \beta) \neq 0$. This is clear simply because $V^*\otimes\alpha$ is some finite direct sum of irreducibles.

First, a preliminary result:

Lemma 3.7. *The squared antipode S^2 of H descends to an automorphism of every simple subcoalgebra C_α of C. Moreover, the resulting automorphism on the C^*-algebra C_α^* is conjugation by an invertible positive operator.*

Proof. That S^2 descends to $C = H/HA^+$ is clear from the fact that it acts on A. We move the action over to duals by precomposition: $S^2 f = f(S^2\cdot)$ for $f \in H^*$.

Now let $D \leq H$ be a simple subcoalgebra, and $\bigoplus_{\alpha\in I} C_\alpha$, $I \subset \widehat{C}$ the image of D through $H \to C$. The squared antipode acts on D^* as conjugation by a positive operator F [Klimyk and Schmüdgen 1997, Chapter 11, Lemma 30 and Proposition 34], and, by the previous paragraph, preserves the subalgebra $B = \bigoplus_{\alpha\in I} C_\alpha^*$. In particular, conjugation by F permutes the $|I|$ minimal nonzero projections p_α, $\alpha \in I$ in the center of B. I claim that this permutation action is in fact trivial, which would finish the proof.

To check the claim, consider the unique (up to isomorphism) simple $*$-representation of D^* on a Hilbert space $\mathcal{H}$. If $Fp_\alpha F^{-1}$ were equal to some p_β with $\beta \neq \alpha \in I$, then F would map the range of p_α onto the range of p_β. Denoting by $\langle\ ,\ \rangle$ the inner product on $\mathcal{H}$, this implies that $\langle Fx, x\rangle$ vanishes for any x in the range of p_α. This cannot happen for nonzero x, as F is both positive and invertible. □

We now establish the existence of a kind of "relative Haar measure" on $C^\bullet$.

Proposition 3.8. *There is an element $\theta \in \overline{C}$ satisfying the following conditions*:

(a) *Writing θ as a formal sum of elements in the simple subcoalgebras of C, its component in $\mathbb{C}\overline{1} \leq C$ is $\overline{1}$.*

(b) *It is H-invariant, in the sense that $x\theta = \varepsilon(x)\theta$ for $x \in H$.*

(c) *It is positive as a functional on the $*$-algebra $C^\bullet$.*

Sketch of proof. Let e_i, e^i, $i \in I$ be dual bases in C and $C^\bullet$ respectively, compatible with the decomposition of C into simple subcoalgebras. We distinguish an element $0 \in I$ such that $e_0 = \overline{1}$. Since the automorphism S^2 of H descends to $C = H/HA^+$, the definition

$$\theta = \sum_{i\in I} e^i(S^2 e_{i(2)})e_{i(1)}$$

makes sense as an element of $\overline{C}$, and clearly satisfies (a). Moreover, the definition does not depend on the choice of bases.

The calculation proving H-invariance can simply be lifted, e.g., from [Van Daele 1997, Proposition 1.1]. Even though that result is about finite-dimensional Hopf algebras, it works verbatim in the present setting.

Finally, let us prove positivity, this time imitating [Van Daele 1996]. Let $\alpha \in \widehat{C}$, and $u \in C_\alpha^* \leq C^\bullet$ an element. We can assume harmlessly that the bases e_i, e^i are organized as matrix (co)units; i.e., those e_i in the matrix coalgebra C_α form a matrix counit e_{pq}, and e^i will then be the dual matrix unit $e^{pq} \in C_\alpha^*$.

Now note that e_{pq}, regarded as a functional on C_α^*, can be written as $\mathrm{tr}_\alpha(\,\cdot\, e^{qp})$, where tr_α is the trace on the matrix algebra $C_\alpha^* \cong M_n$, so that $\mathrm{tr}_\alpha(1) = n$. In conclusion, the component of θ in C_α, regarded as a functional on C_α^*, is

$$\theta_\alpha = \sum_{p,q} \mathrm{tr}_\alpha(\,\cdot\, S^2(e^{pq})e^{qp}). \tag{3}$$

If $Q \in C_\alpha^*$ is a positive operator such that conjugation by Q equals S^2 on C_α^* (Lemma 3.7), then, suppressing summation over $p, q = 1, \ldots, n$,

$$S^2(e^{pq})e^{qp} = Qe^{pq}Q^{-1}e^{qp} = \mathrm{tr}_\alpha(Q^{-1})Q.$$

This is a positive operator, and the conclusion follows. □

Remark 3.9. The expression (3), the invariance of θ with respect to bases, and the fact that $S^2(e^{pq})$ are again matrix units make it clear that $\theta \circ S^2 = \theta$. In fact θ is unique, but we do not need this stronger fact.

Definition 3.10. Keeping the previous notation, the *φ-relative Fourier transform* $\mathcal{F} : H \to C^\bullet$ is defined as

$$H \ni x \mapsto \varphi(Sx\,\cdot\,).$$

There is a slight abuse of notation in the definition: although a priori φ is a functional on H, it descends to one on $C = H/HA^+$. The map $\mathcal{F}$ is a relative analogue to the usual Fourier transform [Podleś and Woronowicz 1990, §2], and enjoys similar properties. Let us record some of them:

Proposition 3.11. *The map $\mathcal{F} : H \to C^\bullet$ introduced above satisfies the following relations*:

(1) $\mathcal{F}(x \triangleleft \mathcal{F}y) = \mathcal{F}x\mathcal{F}y$ *for all* $x, y \in H$, *where the right action* $\triangleleft$ *of* H^* *on* H *is defined by* $x \triangleleft f = f(x_1)x_2$.

(2) $\mathcal{F}(x)^* = S^2\mathcal{F}((Sx)^*)$, *where the* $*$ *structure on* $C^\bullet$ *is defined in* (2), *and* S^2 *acts on* H^* *by precomposition, as in the proof of Lemma 3.7.*

(3) $\varepsilon(x \triangleleft \mathcal{F}y) = \varphi(Syx)$.

(4) $\theta\mathcal{F} = \varepsilon$, *where* θ *is the functional on* $C^\bullet$ *from Proposition 3.8.*

(5) $\mathcal{F}S^2 = S^{-2}\mathcal{F}$.

Proof. Most of this consists of simple computations, so let us only prove the first and fourth items.

Applying both sides of (1) to $z \in H$, we have to prove

$$\varphi(Sy\, x_1)\varphi(Sx_2\, z) = \varphi(Sx\, z_1)\varphi(Sy\, z_2).$$

Substituting y for Sy, z for Sz, and using $\varphi \circ S = \varphi$ (Remark 3.5), this turns into

$$\varphi(yx_1)\varphi(zx_2) = \varphi(z_2x)\varphi(ySz_1).$$

Now make the substitution $yx_1 \otimes x_2 = a \otimes b$, which in turn means $y \otimes x = aSb_1 \otimes b_2$. The target identity turns into

$$\varphi(a)\varphi(zb) = \varphi(aSb_1Sz_1)\varphi(z_2b_2).$$

Writing $zb = c$, it transforms further into

$$\varphi(a)\varphi(c) = \varphi(aSc_1)\varphi(c_2).$$

Finally, the substitution of c for $S^{-1}c$ and again $\varphi \circ S = \varphi$ turn this into

$$\varphi(a)\varphi(c) = \varphi(ac_2)\varphi(c_1).$$

To prove this last equality, it suffices to split into two cases, according to whether c is in A or the complementary A-bimodule, right H-comodule $\ker(p)$.

In the latter case, both $\varphi(c)$ and $\varphi(c_1)$ vanish. In the former, the left-hand side is $\varphi(a)\varepsilon(c)$, while the right-hand side is $\varphi(ac)$ (since $\varphi(c_1) = \varepsilon(c_1)$). These two expressions are equal because $\varphi = \varepsilon p$ and p is an A-bimodule map.

We now check (4). Applying its left-hand side to $x \in H$, we get $\theta(\varphi(Sx\,\cdot)) = \varphi(Sx\,\theta)$, where this time θ is thought of as an element of $\overline{C}$, $Sx\,\theta$ is the action of Sx on it (Remark 3.6), and φ is regarded naturally as a functional on $\overline{C}$. By the H-invariance of θ (Proposition 3.8(b)), the expression is $\varepsilon(x)\varphi(\theta) = \varepsilon(x)$ by Proposition 3.8(a). □

All of the ingredients are now in place.

Proof of Theorem 3.1. According to Lemma 3.4, it suffices to show that $\varphi(x^*x) \geq 0$ for all $x \in H$. We do this through a string of equalities based on the preliminary results of this section.

Let $x, y \in H$. Then, we have

$$\begin{aligned}\theta((\mathcal{F}y)^*\mathcal{F}x) &\overset{(2)}{=} \theta(S^2\mathcal{F}((Sy)^*)\mathcal{F}x) = \theta(S^2\mathcal{F}((Sy)^*)\mathcal{F}(S^2x))\\ &\overset{(1)}{=} \theta\mathcal{F}((Sy)^* \triangleleft \mathcal{F}(S^2x)) \overset{(4)}{=} \varepsilon((Sy)^* \triangleleft \mathcal{F}(S^2x))\\ &\overset{(3)}{=} \varphi(S^3x(Sy)^*) = \varphi(S^3xS(S^2y)^*) = \varphi((S^2y)^*S^2x),\end{aligned}$$

where the numbers above the equal signs refer to the items in Proposition 3.11, the second equality follows from (5) and the fact that $\theta S^2 = \theta$ (Remark 3.9), the next-to-last one is a simple manipulation valid in any Hopf $*$-algebra, and the last equality is based on $\varphi S = \varphi$ (Remark 3.5). Since the left-hand side is nonnegative when $x = y$, so is the right-hand side. This concludes the proof of the theorem. □

Remark 3.12. The equality obtained in the course of the proof should be thought of as a Plancherel theorem [Rudin 1991, 7.9, p. 188], to the effect that the relative Fourier transform is an isometry with respect to the "inner products" induced by φ and θ.

Acknowledgements

I would like to thank Akira Masuoka and Issan Patri for useful references, conversations and comments on the contents of the paper. I am also grateful to the anonymous referee for bringing to my attention the references [Doi 1983; 1990], and for numerous other suggestions that have helped considerably with improving the manuscript.

References

[Andruskiewitsch and Devoto 1995] N. Andruskiewitsch and J. Devoto, "Extensions of Hopf algebras", *Algebra i Analiz* **7**:1 (1995), 22–61. MR 96f:16044 Zbl 0857.16032

[Arkhipov and Gaitsgory 2003] S. Arkhipov and D. Gaitsgory, "Another realization of the category of modules over the small quantum group", *Adv. Math.* **173**:1 (2003), 114–143. MR 2004e:17010 Zbl 1025.17004

[Brzezinski and Wisbauer 2003] T. Brzezinski and R. Wisbauer, *Corings and comodules*, London Mathematical Society Lecture Note Series **309**, Cambridge University Press, 2003. MR 2004k:16093 Zbl 1035.16030

[Caenepeel et al. 2007] S. Caenepeel, E. De Groot, and J. Vercruysse, "Galois theory for comatrix corings: descent theory, Morita theory, Frobenius and separability properties", *Trans. Amer. Math. Soc.* **359**:1 (2007), 185–226. MR 2007e:16042 Zbl 1115.16017

[Chirvasitu 2010] A. Chirvasitu, "On epimorphisms and monomorphisms of Hopf algebras", *J. Algebra* **323**:5 (2010), 1593–1606. MR 2011f:16075 Zbl 1198.16030

[Demazure and Gabriel 1970] M. Demazure and P. Gabriel, *Groupes algébriques, I: Géométrie algébrique, généralités, groupes commutatifs*, Masson, Paris, 1970. MR 46 #1800 Zbl 0203.23401

[Dijkhuizen and Koornwinder 1994] M. S. Dijkhuizen and T. H. Koornwinder, "CQG algebras: a direct algebraic approach to compact quantum groups", *Lett. Math. Phys.* **32**:4 (1994), 315–330. MR 95m:16029 Zbl 0861.17005

[Doi 1983] Y. Doi, "On the structure of relative Hopf modules", *Comm. Algebra* **11**:3 (1983), 243–255. MR 84a:16014 Zbl 0502.16009

[Doi 1990] Y. Doi, "Hopf extensions of algebras and Maschke type theorems", *Israel J. Math.* **72**:1-2 (1990), 99–108. MR 92b:16078 Zbl 0731.16025

[Fogarty 1969] J. Fogarty, *Invariant theory*, W. A. Benjamin, New York, 1969. MR 39 #1458 Zbl 0191.51701

[Kaplansky 1975] I. Kaplansky, *Bialgebras*, University of Chicago, 1975. MR 55 #8087

[Klimyk and Schmüdgen 1997] A. Klimyk and K. Schmüdgen, *Quantum groups and their representations*, Springer, Berlin, 1997. MR 99f:17017 Zbl 0891.17010

[Mac Lane 1998] S. Mac Lane, *Categories for the working mathematician*, 2nd ed., Graduate Texts in Mathematics **5**, Springer, New York, 1998. MR 2001j:18001 Zbl 0906.18001

[Masuoka and Wigner 1994] A. Masuoka and D. Wigner, "Faithful flatness of Hopf algebras", *J. Algebra* **170**:1 (1994), 156–164. MR 95i:16040 Zbl 0820.16034

[Mesablishvili 2006] B. Mesablishvili, "Monads of effective descent type and comonadicity", *Theory Appl. Categ.* **16**:1 (2006), 1–45. MR 2006m:18002 Zbl 1085.18003

[Montgomery 1993] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics **82**, American Mathematical Society, Providence, RI, 1993. MR 94i:16019 Zbl 0793.16029

[Nuss 1997] P. Nuss, "Noncommutative descent and non-abelian cohomology", *K-Theory* **12**:1 (1997), 23–74. MR 99d:16001 Zbl 0884.18015

[Oberst and Schneider 1974] U. Oberst and H.-J. Schneider, "Untergruppen formeller Gruppen von endlichem Index", *J. Algebra* **31** (1974), 10–44. MR 50 #13057 Zbl 0304.14028

[Podleś and Woronowicz 1990] P. Podleś and S. L. Woronowicz, "Quantum deformation of Lorentz group", *Comm. Math. Phys.* **130**:2 (1990), 381–431. MR 91f:46100 Zbl 0703.22018

[Radford 1977a] D. E. Radford, "Operators on Hopf algebras", *Amer. J. Math.* **99**:1 (1977), 139–158. MR 55 #10505 Zbl 0369.16011

[Radford 1977b] D. E. Radford, "Pointed Hopf algebras are free over Hopf subalgebras", *J. Algebra* **45**:2 (1977), 266–273. MR 55 #10506 Zbl 0354.16004

[Rudin 1991] W. Rudin, *Functional analysis*, 2nd ed., McGraw-Hill, New York, 1991. MR 92k:46001 Zbl 0867.46001

[Salmi and Skalski 2012] P. Salmi and A. Skalski, "Idempotent states on locally compact quantum groups", *Q. J. Math.* **63**:4 (2012), 1009–1032. MR 2999995 Zbl 1263.46055

[Schauenburg 2000] P. Schauenburg, "Faithful flatness over Hopf subalgebras: counterexamples", pp. 331–344 in *Interactions between ring theory and representations of algebras* (Murcia, 1998), edited by F. Van Oystaeyen and M. Saorin, Lecture Notes in Pure and Appl. Math. **210**, Dekker, New York, 2000. MR 2001d:16061 Zbl 0977.16019

[Schauenburg and Schneider 2005] P. Schauenburg and H.-J. Schneider, "On generalized Hopf Galois extensions", *J. Pure Appl. Algebra* **202**:1-3 (2005), 168–194. MR 2006e:16069 Zbl 1081.16045

[Schneider 1990] H.-J. Schneider, "Principal homogeneous spaces for arbitrary Hopf algebras", *Israel J. Math.* **72**:1-2 (1990), 167–195. MR 92a:16047 Zbl 0731.16027

[Sweedler 1969] M. E. Sweedler, *Hopf algebras*, W. A. Benjamin, New York, 1969. MR 40 #5705 Zbl 0194.32901

[Takesaki 2002] M. Takesaki, *Theory of operator algebras, I*, Encyclopaedia of Mathematical Sciences **124**, Springer, Berlin, 2002. MR 2002m:46083 Zbl 0990.46034

[Takeuchi 1972] M. Takeuchi, "A correspondence between Hopf ideals and sub-Hopf algebras", *Manuscripta Math.* **7** (1972), 251–270. MR 48 #328 Zbl 0238.16011

[Takeuchi 1979] M. Takeuchi, "Relative Hopf modules: equivalences and freeness criteria", *J. Algebra* **60**:2 (1979), 452–471. MR 82m:16006 Zbl 0492.16013

[Tomatsu 2007] R. Tomatsu, "A characterization of right coideals of quotient type and its application to classification of Poisson boundaries", *Comm. Math. Phys.* **275**:1 (2007), 271–296. MR 2008j:46058 Zbl 1130.46042

[Van Daele 1996] A. Van Daele, "Discrete quantum groups", *J. Algebra* **180**:2 (1996), 431–444. MR 97a:16076 Zbl 0864.17012

[Van Daele 1997] A. Van Daele, "The Haar measure on finite quantum groups", *Proc. Amer. Math. Soc.* **125**:12 (1997), 3489–3500. MR 98b:16036 Zbl 0888.16023

[Van Daele 1998] A. Van Daele, "An algebraic framework for group duality", *Adv. Math.* **140**:2 (1998), 323–366. MR 2000g:16045 Zbl 0933.16043

[Wang 2009] S. Wang, "Simple compact quantum groups, I", *J. Funct. Anal.* **256**:10 (2009), 3313–3341. MR 2011c:46150 Zbl 1176.46063

[Wegge-Olsen 1993] N. E. Wegge-Olsen, *K-theory and C*-algebras: a friendly approach*, Clarendon, New York, 1993. MR 95c:46116 Zbl 0780.46038

[Woronowicz 1987] S. L. Woronowicz, "Compact matrix pseudogroups", *Comm. Math. Phys.* **111**:4 (1987), 613–665. MR 88m:46079 Zbl 0627.58034

[Woronowicz 1988] S. L. Woronowicz, "Tannaka–Krein duality for compact matrix pseudogroups. Twisted $SU(N)$ groups", *Invent. Math.* **93**:1 (1988), 35–76. MR 90e:22033 Zbl 0664.58044

Communicated by Susan Montgomery
Received 2013-08-11 Revised 2014-03-06 Accepted 2014-04-21

chirvasitua@gmail.com *Department of Mathematics, University of Washington, Box 354350, Seattle, WA 98195-4350, United States*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1201

msp

Tetrahedral elliptic curves and the local-global principle for isogenies

Barinder S. Banwait and John E. Cremona

We study the failure of a local-global principle for the existence of l-isogenies for elliptic curves over number fields K. Sutherland has shown that over $\mathbb{Q}$ there is just one failure, which occurs for $l = 7$ and a unique j-invariant, and has given a classification of such failures when K does not contain the quadratic subfield of the l-th cyclotomic field. In this paper we provide a classification of failures for number fields which do contain this quadratic field, and we find a new "exceptional" source of such failures arising from the exceptional subgroups of $\mathrm{PGL}_2(\mathbb{F}_l)$. By constructing models of two modular curves, $X_s(5)$ and $X_{S_4}(13)$, we find two new families of elliptic curves for which the principle fails, and we show that, for quadratic fields, there can be no other exceptional failures.

1. Introduction

Let E be an elliptic curve defined over a number field K, and l a prime. It is easy to show that if E possesses a K-rational l-isogeny, then the reduction $\widetilde{E}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$, for all primes $\mathfrak{p}$ of K of good reduction and not dividing l, likewise possesses an $\mathbb{F}_{\mathfrak{p}}$-rational l-isogeny.

Andrew Sutherland [2012] asked a converse question: if $\widetilde{E}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$-rational l-isogeny for a density-one set of primes $\mathfrak{p}$, then does E/K admit a K-rational l-isogeny? Sutherland showed that while the answer to this question is usually "yes", there nevertheless exist pairs $(E/K, l)$ for which the answer is "no".

Whether an elliptic curve over a field possesses a rational l-isogeny or not depends only on its j-invariant, provided that the j-invariant is neither 0 nor 1728; thus, if the answer is "no" for one elliptic curve E/K for the prime l, it is also "no" for every elliptic curve over K with the same j-invariant $j(E)$ (with the same exceptions). Following Sutherland, we thus define a pair (l, j_0), consisting of a prime l and an element $j_0 \neq 0, 1728$ of a number field K, to be *exceptional for* K if there exists an elliptic curve E over K, with $j(E) = j_0$, such that the answer to

The first author was supported by an EPSRC Doctoral Training Award at the University of Warwick.
MSC2010: primary 11G05; secondary 11G18.
Keywords: elliptic curves, local-global, isogeny, exceptional modular curves.

the above question at l is "no". We will refer to the prime in the exceptional pair as an *exceptional prime for* K, and any elliptic curve E over K with $j(E) = j_0$ as a *Hasse at* l *curve over* K.

Sutherland gives a necessary condition for the existence of an exceptional pair, under a certain assumption. To state Sutherland's result, recall that the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on the l-torsion subgroup $E(\overline{K})[l]$, yielding the mod-l representation

$$\bar{\rho}_{E,l} : G_K \to \mathrm{GL}_2(\mathbb{F}_l),$$

whose image $G_{E,l} := \mathrm{Im}\,\bar{\rho}_{E,l}$ is well-defined up to conjugacy; we refer to $G_{E,l}$ as *the mod-*l *image of* E. We let $H_{E,l} := G_{E,l}$ modulo scalars, and observe that $H_{E,l}$ depends only upon $j(E)$, provided that $j(E) \neq 0$ or 1728; we refer to $H_{E,l}$ as *the projective mod-*l *image of* E.

It is easy to show that $l = 2$ is not an exceptional prime for any number field, so henceforth we assume that l is odd. We now define $l^* := \pm l$, where the plus sign is taken if $l \equiv 1 \pmod 4$, and the minus sign otherwise.

Sutherland's result may now be stated as follows; by D_{2n} we mean the dihedral group of order $2n$:

Proposition 1.1 (Sutherland). *Assume* $\sqrt{l^*} \notin K$. *If* (l, j_0) *is exceptional for* K, *then for all elliptic curves* E/K *with* $j(E) = j_0$:

(1) *The projective mod-*l *image of* E *is isomorphic to* D_{2n}, *where* $n > 1$ *is an odd divisor of* $(l-1)/2$.

(2) $l \equiv 3 \pmod 4$.

(3) *The mod-*l *image of* E *is contained in the normaliser of a split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_l)$.

(4) E *obtains a rational* l*-isogeny over* $K(\sqrt{l^*})$.

(In fact, the converse is also true, as may be shown by applying the proof of the converse part of Proposition 1.3 below; see Section 7.)

Sutherland used this result for $K = \mathbb{Q}$ to determine the exceptional pairs for $\mathbb{Q}$ (where the assumption $\sqrt{l^*} \notin \mathbb{Q}$ is trivially satisfied for all l). If $(l, j(E))$ is exceptional for $\mathbb{Q}$, then (3) above says that E corresponds to a $\mathbb{Q}$-point on the modular curve $X_{\mathrm{s}}(l)$. By the recent work of Bilu, Parent and Rebolledo [Bilu et al. 2013], it follows that l must be 2, 3, 5, 7 or 13. Of these, only 3 and 7 are 3 (mod 4), and 3 can easily be ruled out as a possible exceptional prime (for all number fields). Thus, 7 is the only possible exceptional prime for $\mathbb{Q}$, and (1) above tells us that the projective mod-7 image of a Hasse at 7 curve over $\mathbb{Q}$ must be isomorphic to D_6, the dihedral group of order 6. The modular curve parametrising elliptic curves with this specific level-7 structure turns out to be the rational elliptic curve with

label 49a3 in [Cremona 1997], which has precisely two noncuspidal rational points. Evaluating j at these points yields the same value, and hence gives Sutherland's second result.

Theorem 1.2 [Sutherland 2012, Theorem 2]. *The only exceptional pair for $\mathbb{Q}$ is*

$$\left(7, \tfrac{2268945}{128}\right).$$

In this paper we would like to investigate what happens in the case where $\sqrt{l^*} \in K$. In Section 7 we will prove the following using Sutherland's methods:

Proposition 1.3. *Assume $\sqrt{l^*} \in K$. Then (l, j_0) is exceptional for K if and only if one of the following holds for elliptic curves E/K with $j(E) = j_0$:*

- *$H_{E,l} \cong A_4$ and $l \equiv 1 \pmod{12}$.*
- *$H_{E,l} \cong S_4$ and $l \equiv 1 \pmod{24}$.*
- *$H_{E,l} \cong A_5$ and $l \equiv 1 \pmod{60}$.*
- *$H_{E,l} \cong D_{2n}$ and $l \equiv 1 \pmod 4$, where $n > 1$ is a divisor of $(l-1)/2$, and $G_{E,l}$ lies in the normaliser of a split Cartan subgroup.*

Thus, in the case $\sqrt{l^*} \in K$, there are two sorts of exceptional pairs: the *dihedral ones* and the *nondihedral ones*.

Let us now consider each of these two cases over $K = \mathbb{Q}(\sqrt{l^*})$, the smallest field containing $\sqrt{l^*}$. Regarding the dihedral pairs, we may ask the following question:

Question 1.4. For which $l \equiv 1 \pmod 4$ is there an elliptic curve E over $\mathbb{Q}(\sqrt{l})$ such that $H_{E,l} \cong D_{2n}$, for $n > 1$ a divisor of $(l-1)/2$?

A positive answer to the Serre uniformity problem for number fields would imply that there should be only finitely many such l, but we are unable to prove this. Instead, we show that the set of l asked for by the above question is not empty; $l = 5$ gives a positive answer.

Theorem 1.5. *An elliptic curve E over $\mathbb{Q}(\sqrt{5})$ has $H_{E,5} \cong D_4$ if and only if its j-invariant is given by the formula*

$$j(E) = \frac{\left((s+5)(s^2-5)(s^2+5s+10)\right)^3}{(s^2+5s+5)^5} \tag{1-1}$$

for some $s \in \mathbb{Q}(\sqrt{5})$, together with the condition that $s^2 - 20$ is not a square in $\mathbb{Q}(\sqrt{5})$ for all $s \in \mathbb{Q}(\sqrt{5})$ satisfying (1-1).

Thus, the exceptional pairs at 5 over $\mathbb{Q}(\sqrt{5})$ are given by $(5, j(E))$ for $j(E)$ as above, and, in particular, there are infinitely many exceptional pairs at 5 over $\mathbb{Q}(\sqrt{5})$.

The proof of this theorem considers the modular curve $X_s(5)$ corresponding to the normaliser of a split Cartan subgroup, whose $\mathbb{Q}(\sqrt{5})$-points (as we will see) correspond to elliptic curves E over $\mathbb{Q}(\sqrt{5})$ with $H_{E,5} \subseteq D_4$. This curve is defined over $\mathbb{Q}$ and has genus 0; writing the j-map

$$X_s(5) \xrightarrow{j} X(1)$$

as a rational function yields the parametrisation (1-1); the further condition stated in the theorem is needed to force the corresponding elliptic curve to have $H_{E,5} \cong D_4$ (and not merely a subgroup of D_4); see Section 3 for the full proof.

Regarding the nondihedral pairs, we prove the following in Section 8:

Proposition 1.6. *The only nondihedral exceptional prime l over any quadratic field is* 13 *over* $\mathbb{Q}(\sqrt{13})$, *where the projective mod-*13 *image is isomorphic to* A_4.

This leads to the following question:

Question 1.7. Find all elliptic curves E over $\mathbb{Q}(\sqrt{13})$ such that $H_{E,13} \cong A_4$.

By Proposition 1.6, such elliptic curves are the only nondihedral Hasse curves over quadratic fields.

We take a similar approach to this question as we did for Theorem 1.5, by studying the relevant modular curve $X_{S_4}(13)$; this is the modular curve over $\mathbb{Q}$ corresponding to the pullback to $\mathrm{GL}_2(\mathbb{F}_{13})$ of $S_4 \subset \mathrm{PGL}_2(\mathbb{F}_{13})$; the earliest reference to this curve we are aware of is in [Mazur 1977b]. This modular curve is geometrically connected, and over the complex numbers has the description $\Gamma_{A_4}(13)\backslash\mathcal{H}^*$, where $\Gamma_{A_4}(13)$ is the pullback to $\mathrm{PSL}_2(\mathbb{Z})$ of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$. A $\mathbb{Q}$-point on $X_{S_4}(13)$ corresponds to an elliptic curve $E/\mathbb{Q}$ such that $H_{E,13} \subseteq S_4$. A $\mathbb{Q}(\sqrt{13})$-point corresponds to an elliptic curve $E/\mathbb{Q}(\sqrt{13})$ such that $H_{E,13} \subseteq A_4$. Thus, the elliptic curves we seek in Question 1.7 correspond to certain $\mathbb{Q}(\sqrt{13})$-points on the modular curve $X_{S_4}(13)$.

Theorem 1.8. *The modular curve $X_{S_4}(13)$ is a genus-*3 *curve, whose canonical embedding in $\mathbb{P}^2_{\mathbb{Q}}$ has the model*

$$\begin{aligned}\mathscr{C} : 4X^3Y - 3X^2Y^2 + 3XY^3 - X^3Z + 16X^2YZ - 11XY^2Z \\ +5Y^3Z + 3X^2Z^2 + 9XYZ^2 + Y^2Z^2 + XZ^3 + 2YZ^3 = 0.\end{aligned}$$

On this model, the j-map $X_{S_4}(13) \xrightarrow{j} X(1)$ is given by

$$j(X,Y,Z) = \frac{n(X,Y,Z)}{d(X,Y,Z)^{13}},$$

where

$$\begin{aligned}d(X,Y,Z) = 5X^3 - 19X^2Y - 6XY^2 + 9Y^3 + X^2Z \\ -23XYZ - 16Y^2Z + 8XZ^2 - 22YZ^2 + 3Z^3\end{aligned}$$

and $n(X, Y, Z)$ is an explicit degree-39 polynomial.

The proof of this theorem will occupy Sections 4 and 5 of the paper.

We have not been able to provably determine the $\mathbb{Q}(\sqrt{13})$-points on the curve. The method of Chabauty does not apply in this case, and this is likely to be a difficult problem; see Section 9 for more about the Jacobian of $\mathscr{C}$ and the difficulty of determining the $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{13})$-rational points.

We have, however, the following six points[1] in $\mathscr{C}(\mathbb{Q}(\sqrt{13}))$, four of which are in $\mathscr{C}(\mathbb{Q})$:

$$\{(1:3:-2),\ (0:0:1),\ (0:1:0),\ (1:0:0),\ (3\pm\sqrt{13}:0:2)\}.$$

By evaluating the j-map at these points, we obtain the j-invariants of elliptic curves over $\mathbb{Q}(\sqrt{13})$ whose projective mod-13 image is contained in A_4; in fact, apart from $(0:0:1)$, whose corresponding j-invariant is 0, these points have projective mod-13 image isomorphic to A_4.

Corollary 1.9. *Elliptic curves over $\mathbb{Q}$ with j-invariants*

$$\frac{11225615440}{1594323} = \frac{2^4\cdot 5\cdot 13^4\cdot 17^3}{3^{13}},$$

$$-\frac{160855552000}{1594323} = -\frac{2^{12}\cdot 5^3\cdot 11\cdot 13^4}{3^{13}},$$

$$\frac{9061636498563792450559037262 1162077487104}{19765049735370209430857055664 0625} = \frac{2^{18}\cdot 3^3\cdot 13^4\cdot 127^3\cdot 139^3\cdot 157^3\cdot 283^3\cdot 929}{5^{13}\cdot 61^{13}}$$

have projective mod-13 images isomorphic to S_4. Elliptic curves over $\mathbb{Q}(\sqrt{13})$ with these j-invariants have projective mod-13 images isomorphic to A_4, as do elliptic curves over $\mathbb{Q}(\sqrt{13})$ with j-invariant

$$j = \frac{4096000}{1594323}(15996230 \pm 4436419\sqrt{13}).$$

Thus, elliptic curves over $\mathbb{Q}(\sqrt{13})$ with these j-invariants are Hasse at 13 curves over $\mathbb{Q}(\sqrt{13})$.

Remark 1.10. It is known that, for $l > 13$, there are no elliptic curves E over $\mathbb{Q}$ with $H_{E,l} \cong S_4$; in fact, Serre proved that $X_{S_4}(l)(\mathbb{Q})$ is empty for $l > 13$. Mazur [1977a, p. 36] reports that Serre has constructed a $\mathbb{Q}$-point on $X_{S_4}(13)$ corresponding to elliptic curves with complex multiplication by $\sqrt{-3}$; this point that Serre found corresponds to the point $(0:0:1)$ on the curve $\mathscr{C}$ above.

[1] These are all the points in $\mathscr{C}(\mathbb{Q}(\sqrt{13}))$ of logarithmic height less than 5.24, according to [Turner 2013].

Remark 1.11. The rational points on $X_{S_4}(l)$ for $l \leq 11$ have already been determined. The most interesting case is $l = 11$, where Ligozat [1977] proved that the curve $X_{S_4}(11)$ is the elliptic curve with Cremona label 121c1.

We conclude this introduction by considering the following problem, which we would like to solve at least for every quadratic field. This may be viewed as a generalisation of Sutherland's theorem 2 (see 1.2).

Problem 1.12. Fix a number field K. Find all exceptional pairs over K.

Samuele Anni [2014] has proved that there can be only finitely many exceptional primes for a given number field K. In the quadratic case, his result gives the following:

Proposition 1.13 (Anni). *A quadratic field K admits at most* 3 *exceptional primes. If $K = \mathbb{Q}(\sqrt{l})$ for l a prime $\equiv 1 \pmod 4$, then the only possible exceptional primes are* 7, 11, *and l. If $K \neq \mathbb{Q}(\sqrt{l})$, then only* 7 *and* 11 *are possible exceptional primes.*

It is straightforward to determine, for a given quadratic field K, the exceptional pairs of the form $(7, j_0)$; in principle all one needs to do is determine the j-invariants of the K-points on the elliptic curve 49a3.

In the case where $K = \mathbb{Q}(\sqrt{l})$ and the prime is l, Problem 1.12 reduces to Question 1.4 above, which essentially asks for quadratic points on the modular curves $X_s(l)$; this is known to be a difficult problem.

Regarding 11 as a possible exceptional prime, we make the following conjecture:

Conjecture 1.14. 11 is not an exceptional prime for any quadratic field.

In Section 10, we will explain our evidence for this conjecture.

2. Preliminaries

Let l be an odd prime. We define $\mathrm{PSL}_2(\mathbb{F}_l)$ to be the kernel of the map det : $\mathrm{PGL}_2(\mathbb{F}_l) \to \mathbb{F}_l^*/(\mathbb{F}_l^*)^2 \cong \{\pm 1\}$. It is isomorphic to $\mathrm{SL}_2(\mathbb{F}_l)/\{\pm I\}$. By $\mathrm{GL}_2^+(\mathbb{F}_l)$ we mean the subgroup of matrices with square determinant.

Lemma 2.1. *Let E/K be an elliptic curve. The following are equivalent*:

(1) $H_{E,l} \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$.

(2) $\sqrt{l^*} \in K$.

(3) $G_{E,l} \subseteq \mathrm{GL}_2^+(\mathbb{F}_l)$.

Proof. The equivalence of (1) and (3) is clear. The equivalent of (2) and (3) follows from standard Galois theory upon observing that the determinant of $\bar{\rho}_{E,l}$ is equal to the mod-l cyclotomic character over K. □

In particular, if $E/\mathbb{Q}$ is an elliptic curve with $H_{E,13} \cong S_4$, then after base-changing to $\mathbb{Q}(\sqrt{13})$ the projective image is intersected with $\mathrm{PSL}_2(\mathbb{F}_{13})$, and becomes isomorphic to A_4. This argument uses the fact that $13 \equiv 5 \pmod 8$.

We would like to briefly mention the Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_l)$; for a complete treatment see [Lang 2002, Chapter XVIII, §12]. There are two sorts of Cartan subgroup, *split* and *nonsplit*. A split Cartan subgroup is conjugate to the group of diagonal matrices, and hence is isomorphic to $\mathbb{F}_l^* \times \mathbb{F}_l^*$. Its normaliser is then conjugate to the group C_{s}^+ of diagonal and antidiagonal matrices. A nonsplit Cartan subgroup is isomorphic to $\mathbb{F}_{l^2}^*$, and is conjugate to the group C_{ns} defined as follows:

$$C_{\mathrm{ns}} = \left\{ \begin{pmatrix} x & \delta y \\ y & x \end{pmatrix} : x, y \in \mathbb{F}_l,\ (x, y) \neq (0, 0) \right\},$$

where δ is any fixed quadratic nonresidue in $\mathbb{F}_l^*$. It also has index two in its normaliser C_{ns}^+.

Associated to the groups C_{s}^+ and C_{ns}^+ are modular curves $X_{\mathrm{s}}(l)$ and $X_{\mathrm{ns}}(l)$ respectively; these serve as coarse moduli spaces for elliptic curves E whose mod-l Galois image $G_{E,l}$ is contained in (a conjugate of) C_{s}^+ and C_{ns}^+ respectively. Both curves are geometrically connected and defined over $\mathbb{Q}$. Over the complex numbers each curve has the description of being the quotient of the extended upper half-plane $\mathcal{H}^*$ by an appropriate congruence subgroup. The curve $X_{\mathrm{s}}(l)$ is $\mathbb{Q}$-isomorphic to the quotient $X_0^+(l^2)$ of the modular curve $X_0(l^2)$ by the Fricke involution. Over $\mathbb{C}$, this isomorphism is established by mapping τ on $X_0^+(l^2)$ to $l\tau$ on $X_{\mathrm{s}}(l)$.

One of Sutherland's insights was that the notion of Hasse at l curve E over K depends only on the projective mod-l image $H_{E,l}$. Given a subgroup H of $\mathrm{PGL}_2(\mathbb{F}_l)$, we say that H is *Hasse* if its natural action on $\mathbb{P}^1(\mathbb{F}_l)$ satisfies the following two properties:

- Every element $h \in H$ fixes a point in $\mathbb{P}^1(\mathbb{F}_l)$.
- There is no point in $\mathbb{P}^1(\mathbb{F}_l)$ fixed by the whole of H.

Proposition 2.2 (Sutherland). *An elliptic curve E/K is Hasse at l if and only if $H_{E,l}$ is Hasse.*

This allows us to reduce the study of exceptional pairs largely to group theory.

3. Proof of Theorem 1.5

Throughout this proof, $K = \mathbb{Q}(\sqrt{5})$.

Let E/K have $H_{E,5} \cong D_4$. It follows from Dickson's classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_l)$ [1901] that $G_{E,5}$ is contained in the normaliser of a Cartan subgroup. If this Cartan subgroup were nonsplit, then $G_{E,5}$ would be contained in $C_{\mathrm{ns}}^+ \cap \mathrm{GL}_2^+(\mathbb{F}_5)$ (we take the intersection by Lemma 2.1), and so $H_{E,5}$ would be contained in

$(C_{\mathrm{ns}}^+ \cap \mathrm{GL}_2^+(\mathbb{F}_5))/\text{scalars}$, which is a group of size 6, and hence cannot contain a subgroup isomorphic to D_4; thus $G_{E,5} \subseteq C_{\mathrm{s}}^+$, and so E/K corresponds to a K-point on $X_{\mathrm{s}}(5)$. The converse is not quite true; a K-point on $X_{\mathrm{s}}(5)$ corresponds to an elliptic curve E' over K with $H_{E',5} \subseteq D_4$, but not necessarily equal to D_4.

We now give an expression for the j-map $X_{\mathrm{s}}(5) \xrightarrow{j} X(1)$. Since $X_0^+(25)$ is isomorphic to $X_{\mathrm{s}}(5)$ under the map $\tau \mapsto 5\tau$, it suffices to write down the function $j(5\tau)$ in terms of a Hauptmodul s for $X_0^+(25)$.

Let t_N be a Hauptmodul for $X_0(N)$. Klein found the following formula in 1879:

$$j(5\tau) = \frac{(t_5^2 + 250t_5 + 3125)^3}{t_5^5}.$$

We can look up an expression for t_5 in terms of t_{25} from [Maier 2009]:

$$t_5 = t_{25}(t_{25}^4 + 5t_{25}^3 + 15t_{25}^2 + 25t_{25} + 25).$$

We also know that the Fricke involution w_{25} maps t_{25} to $5/t_{25}$. Hence a Hauptmodul for $X_0^+(25)$ is $s := t_{25} + 5/t_{25}$. It follows that

$$j(5\tau) = \frac{((s+5)(s^2-5)(s^2+5s+10))^3}{(s^2+5s+5)^5}.$$

Inserting a K-value for s in this expression yields the j-invariant of an elliptic curve E over K with $H_{E,5} \subseteq D_4$. The condition on $s^2 - 20$ in the statement of the theorem ensures that we have equality here, by ensuring that the image is not contained in any one of the three subgroups of order 2 in D_4, as we now demonstrate.

Let E be a curve in $X_{\mathrm{s}}(5)(K)$ corresponding to a choice of s in K, so that $H_{E,5} \subseteq D_4$. The following statements are readily seen to be equivalent to $H_{E,5} \neq D_4$:

- $H_{E,5}$ is cyclic.
- $G_{E,5}$ is contained in (a conjugate of) $C_{\mathrm{s}}(\mathbb{F}_5)$.
- E has a pair of independent K-rational 5-isogenies.
- E pulls back to a K-point on $X_0(25)$.
- $t_{25} \in K$.

Since t_{25} is a root of the polynomial $x^2 - sx + 5$ of discriminant $s^2 - 20$, we have $t_{25} \in K$ if and only if $s^2 - 20$ is a square in K. Thus the statement that $s^2 - 20$ is not a square in K is equivalent to $H_{E,5}$ not being cyclic, and hence $H_{E,5} \cong D_4$.

We have, however, overlooked an issue above. For a given $j = j(E) \in K$ satisfying (1-1), there are two other values of $s \in K$ also satisfying (1-1). This is because the field extension $K(s)/K(j)$, which has degree 15 and is not Galois, has

automorphism group of order 3, generated by $s \mapsto ((\sqrt{5}-5)s-20)/(2s+5+\sqrt{5})$. We must ensure that for none of the Galois conjugate values is s^2-20 square in K, so that $H_{E,5}$ is not contained in any of the three cyclic subgroups of D_4. This explains the final condition in the statement of the theorem.

Example 3.1. To illustrate this theorem, we input $s = 3\sqrt{5}+1$ to obtain

$$j = \frac{337876318862280\sqrt{5}+741305345279328}{41615795893};$$

we check that s^2-20 is not a square for the other two values of $s \in K$, namely $(\sqrt{5}-15)/7$ and $(-22\sqrt{5}-30)/19$, and hence any elliptic curve over $\mathbb{Q}(\sqrt{5})$ with this j has $H_{E,5} \cong D_4$. Equivalently, the pair $(5, j)$ is exceptional for $\mathbb{Q}(\sqrt{5})$.

However, if we input $s = (3\sqrt{5}-80)/41$, we get

$$j = \frac{277374956280053760\sqrt{5}+622630488102469632}{18658757027251},$$

and whilst $(3\sqrt{5}-80)/41$ does satisfy s^2-20 not being a square, this is not the case for $s = 3\sqrt{5}+2$, which yields the same j-value. One therefore has to be careful of these "pretenders", hence the last paragraph of the above proof.

We can even insert rational values of s, such as $s = 1$, to obtain elliptic curves over $\mathbb{Q}$ whose base-change to $\mathbb{Q}(\sqrt{5})$ are Hasse at 5, e.g.,

$$j = \frac{-56623104}{161051}.$$

4. Proof of Theorem 1.8: the model

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for some N, and consider the modular curve $X_G(N)$ over $\mathbb{Q}$; let us assume $\det G = (\mathbb{Z}/N\mathbb{Z})^*$, so that this curve is geometrically connected. As a curve over $\mathbb{C}$, the curve depends only on the intersection of G with $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Therefore, if $N = 13$, and G is the pullback to $\mathrm{GL}_2(\mathbb{F}_{13})$ of $S_4 \subset \mathrm{PGL}_2(\mathbb{F}_{13})$, then the modular curve $X_{S_4}(13) := X_G(13)$, when considered over $\mathbb{C}$, depends only on $G \cap \mathrm{SL}_2(\mathbb{F}_{13})$, which modulo scalar matrices becomes $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$, and has the description $\Gamma_{A_4}(13)\backslash\mathscr{H}^*$, where $\Gamma_{A_4}(13)$ is the pullback of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$ to $\mathrm{PSL}_2(\mathbb{Z})$, and $\mathscr{H}^*$ is the extended upper half-plane.

Steven Galbraith [1996, Chapter 3] has described a method to compute the canonical model of any modular curve $X(\Gamma)$, provided one can compute explicitly and to some precision the q-expansions of a basis of $S_2(\Gamma)$, the weight-2 cuspforms of level Γ (a congruence subgroup). Hence, to compute the desired equation, we are reduced to computing explicitly a basis of the finite-dimensional $\mathbb{C}$-vector space $S_2(\Gamma_{A_4}(13))$. A standard application of the Riemann–Hurwitz genus formula gives

that the genus of the desired curve is 3; this is also the dimension of $S_2(\Gamma_{A_4}(13))$. We will proceed with the exposition in a series of steps.

Step 1. *Identifying our desired space as the set of invariant vectors of a representation.* Since $\Gamma(13) \subset \Gamma_{A_4}(13)$, we obtain

$$S_2(\Gamma_{A_4}(13)) \subset S_2(\Gamma(13)),$$

a 3-dimensional subspace of a 50-dimensional space. On this latter 50-dimensional space there is a right action — the "weight 2 slash operator" — of $\mathrm{PSL}_2(\mathbb{Z})$ (since $\Gamma(13)$ is normal in $\mathrm{PSL}_2(\mathbb{Z})$) which, by definition of $S_2(\Gamma(13))$, factors through the quotient $\mathrm{PSL}_2(\mathbb{F}_{13})$, which we recall contains a unique (up to conjugacy) subgroup isomorphic to A_4. Our desired 3-dimensional space is then the subspace of $S_2(\Gamma(13))$ fixed by A_4:

$$S_2(\Gamma_{A_4}(13)) = S_2(\Gamma(13))^{A_4},$$

that is, the A_4-invariant subspace of the $\mathrm{PSL}_2(\mathbb{F}_{13})$-representation $S_2(\Gamma(13))$.

When we carry out the computation, we will work with an explicit subgroup of $\mathrm{PSL}_2(\mathbb{F}_{13})$ isomorphic to A_4, namely that generated by the two matrices

$$A = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -2 & -2 \\ -3 & 3 \end{pmatrix}.$$

A different choice of A_4 will yield an isomorphic space of cuspforms, which for our application (in computing an equation for $X_{S_4}(13)$) makes no difference. However, the present choice of A_4 is favourable for computational reasons, since it is normalised by the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$; the congruence subgroup is then said to be of *real type* (see [Cremona 1997, Section 2.1.3]).

Step 2. *The conjugate representation.* Given a congruence subgroup Γ of level 13, denote by $\widetilde{\Gamma}$ the conjugate subgroup of level 13^2:

$$\widetilde{\Gamma} := \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix} \supseteq \Gamma_0(13^2) \cap \Gamma_1(13).$$

In general, $\widetilde{\Gamma}$ has level 13^2; in particular we have

$$\widetilde{\Gamma(13)} = \Gamma_0(13^2) \cap \Gamma_1(13).$$

Then we have the important isomorphism

$$\begin{aligned} S_2(\Gamma) &\to S_2(\widetilde{\Gamma}), \\ f(z) &\mapsto f(13z), \end{aligned}$$

which on q-expansions takes $q := e^{2\pi iz}$ to q^{13}. The point is that we may work with $S_2(\widetilde{\Gamma})$ instead of $S_2(\Gamma)$ if we like, as we can easily pass between the two; the two spaces are only superficially different.

This is exactly our plan for $\Gamma(13) \subset \Gamma_{A_4}(13)$. We have $S_2(\widetilde{\Gamma_{A_4}(13)}) \subset S_2(\widetilde{\Gamma(13)})$. This latter space is also a representation of $\mathrm{PSL}_2(\mathbb{F}_{13})$; for $g \in \mathrm{PSL}_2(\mathbb{F}_{13})$, we let γ be a pullback to $\mathrm{PSL}_2(\mathbb{Z})$ of g, and define, for $F \in S_2(\widetilde{\Gamma(13)})$,

$$g \cdot F := F|_2\tilde{\gamma} := F|_2 \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \gamma \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}.$$

We then obtain

$$S_2(\widetilde{\Gamma_{A_4}(13)}) = S_2(\widetilde{\Gamma(13)})^{A_4}.$$

Working inside the conjugated space $S_2(\widetilde{\Gamma(13)})$ is better, since its alternative description as $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ is more amenable to the explicit computations we wish to carry out using the computer algebra systems Sage and Magma.

Step 3. *The three relevant subrepresentations.* Inside $S_2(\Gamma_0(169) \cap \Gamma_1(13))$, we have $S_2(\Gamma_0^+(169))$, the subspace of w_{169}-invariants of $S_2(\Gamma_0(169))$. We can compute this space explicitly in Sage. Let $q := e^{2\pi iz}$, $\zeta_7 := e^{2\pi i/7}$, $\zeta_7^+ := \zeta_7 + \zeta_7^{-1}$, and σ a nontrivial Galois automorphism of the field $\mathbb{Q}(\zeta_7^+) = \mathbb{Q}(\zeta_7)^+$. Then an explicit Sage computation yields

$$S_2(\Gamma_0^+(169)) = \langle g, g^\sigma, g^{\sigma^2} \rangle,$$

where

$$g(z) = q - (\zeta_7^+ + 1)q^2 + (1 - \zeta_7^{+2})q^3 + (\zeta_7^{+2} + 2\zeta_7^+ - 1)q^4 + \cdots.$$

These three forms are Galois-conjugate newforms. We will denote by a_n the Fourier coefficients of g.

For each $r \in \mathbb{F}_{13}^*$, define the *isotypical component* g_r *of* g as

$$g_r := \sum_{j \equiv r \bmod 13} a_j q^j,$$

and consider the $\mathbb{C}$-span V_0 of these components. Similarly define V_1 and V_2 by replacing g with g^σ and g^{σ^2} respectively. We will show in the coming sections that each V_i is a 12-dimensional subrepresentation of $S_2(\widetilde{\Gamma(13)})$ which is irreducible as $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{13})]$-module. We may focus on these three subrepresentations, because, as we compute later, each one contains a unique (up to scaling) A_4-invariant cuspform.

Since we already know that we are looking for three forms, we need not concern ourselves with the other irreducible components of $S_2(\widetilde{\Gamma(13)})$. In fact, the sum $V_0 \oplus V_1 \oplus V_2$, of dimension 36, is the subspace of $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ spanned by the Galois conjugates of the newform g together with their twists by characters

of conductor 13. The complementary subspace of dimension 14 is spanned by oldforms from level 13 and their twists. Each of these two subspaces is the base-change of a vector space over $\mathbb{Q}$ which is irreducible as a $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{13})]$-module, while the 36-dimensional piece splits as a $\mathbb{Q}(\zeta_7^+)[\mathrm{PSL}_2(\mathbb{F}_{13})]$-module into three irreducible 12-dimensional subspaces.

Although we discovered these facts computationally, there is an alternative representation-theoretic explanation of these spaces in [Baran 2013], whose Propositions 3.6 and 5.2 show that the spaces V_i are irreducible cuspidal representations of $\mathrm{PSL}_2(\mathbb{F}_{13})$.

Step 4. *Computing the action of* $\mathrm{PSL}_2(\mathbb{F}_{13})$ *on each subrepresentation.* $\mathrm{PSL}_2(\mathbb{F}_{13})$ is generated by the two matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

However, since we have conjugated the congruence subgroup, the action we need to consider must also be conjugated by the matrix $\left(\begin{smallmatrix} 13 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Hence, $\mathrm{PSL}_2(\mathbb{F}_{13})$ acts on $S_2(\widetilde{\Gamma(13)})$ via the matrices $\widetilde{S}$ and $\widetilde{T}$:

$$\widetilde{S} = \frac{1}{13}\begin{pmatrix} 0 & -1 \\ 169 & 0 \end{pmatrix} \quad \text{and} \quad \widetilde{T} = \begin{pmatrix} 1 & 1/13 \\ 0 & 1 \end{pmatrix}.$$

Observe that the action of $\widetilde{S}$ is, up to a scaling that we may ignore, the same as the Fricke involution w_{169}.

Thus, to describe the action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ on each V_i, we will express the action of $\widetilde{S}$ and $\widetilde{T}$ on each V_i, explicitly as 12×12 matrices.

Step 5. *Computing the action of* $\widetilde{S}$ *and* $\widetilde{T}$. We fix $i = 0$; the other two cases are completely analogous and can be obtained by Galois conjugation (see Lemma 4.4 below).

To compute the action of $\widetilde{T}$ on V_0, we use the definition directly:

$$\left(g|_2 \begin{pmatrix} 1 & 1/13 \\ 0 & 1 \end{pmatrix}\right)(z) = g\left(z + \tfrac{1}{13}\right).$$

Recall that a_i is the i-th coefficient of g. We then get

$$g\left(z + \tfrac{1}{13}\right) = \zeta_{13} q - (\zeta_7^+ + 1)\zeta_{13}^2 q^2 + \cdots,$$

which we can rearrange as

$$\zeta_{13}(a_1 q + a_{14} q^{14} + a_{27} q^{27} + \cdots) + \zeta_{13}^2 (a_2 q^2 + a_{15} q^{15} + \cdots) + \cdots.$$

Thus, in the isotypical basis for V_0, the action of $\widetilde{T}$ is given simply by the 12×12 diagonal matrix

$$\begin{pmatrix} \zeta & & & \\ & \zeta^2 & & \\ & & \ddots & \\ & & & \zeta^{12} \end{pmatrix},$$

where we write ζ for ζ_{13}. In particular, this shows that V_0 is indeed invariant under the action of $\widetilde{T}$.

Computing $\widetilde{S}$ directly on the isotypical basis is not so easy, so what we do is change to a basis upon which we can compute it. Instead of the isotypical basis, we take the *twist basis*

$$\langle g \otimes \chi^j : 0 \le j \le 11 \rangle,$$

where $\chi : 2 \mapsto \zeta_{12}$ is a fixed generator of the group of Dirichlet characters of conductor 13, and $g \otimes \chi$ denotes the usual twist of g by χ. Note that this twist basis consists entirely of newforms (see [Atkin and Li 1978]). Since twisting by χ preserves V_0 and the change of basis matrix is $(\chi^j(i))$ (for $0 \le j \le 11$ and $1 \le i \le 12$), which has nonzero determinant, we have shown the following:

Lemma 4.1. *Both the isotypical and twist bases are $\mathbb{C}$-bases for the 12-dimensional subspace V_0 of $S_2(\widetilde{\Gamma(13)})$:*

$$\langle g \otimes \chi^j : 0 \le j \le 11 \rangle = \langle g_j : 1 \le j \le 12 \rangle.$$

Recall that the action of $\widetilde{S}$ is the same as the Fricke involution w_{169}. It is known (see [loc. cit.]) that w_N acts on newforms F of level N as

$$F|_2 w_N = \lambda_N(F) \cdot \overline{F},$$

where $\overline{F}$ is the newform obtained from the Fourier expansion of F by complex conjugation, and $\lambda_N(F)$ is the Atkin–Lehner pseudoeigenvalue, an algebraic number of absolute value 1 [loc. cit., Theorem 1.1]. In our twist basis, we have

$$\overline{g \otimes \chi^j} = g \otimes \chi^{12-j},$$

so we only need to compute the pseudoeigenvalues associated to $g \otimes \chi^j$ for $0 \le j \le 6$; the others may be obtained from these by complex conjugation. Also, the pseudoeigenvalues for $j = 0$ and $j = 6$ are actually eigenvalues, and may be computed directly (for example in Sage); we find that the eigenvalue for $j = 0$ is $+1$, and for $j = 6$ is -1.

Step 6. *Computing the Atkin–Lehner pseudoeigenvalues.* In order to stay consistent with the notation of [Atkin and Li 1978], we relabel g to F, and we let $q = 13$. By $a(q)$ we mean the q-th Fourier coefficient of F, which we may check is 0. We may also check that F is not a twist of an oldform of $S_2(\widetilde{\Gamma(13)})$; thus, in the language of [loc. cit.], F is *13-primitive*. We let χ_0 be the trivial character modulo 13, so $\chi_0 = \chi^0$, and we write $\lambda(\chi)$ for the Atkin–Lehner pseudoeigenvalue of $F \otimes \chi$, for χ any character. We let $g(\chi)$ be the Gauss sum of the character χ, with the convention that $g(\chi_0) = -1$.

The main tool to compute $\lambda(\chi^j)$, for $0 \le j \le 11$, is this:

Theorem 4.2 (special case of Theorem 4.5 of [Atkin and Li 1978]). *With the above notation and assumptions, we have, for* $0 \le j \le 11$,

$$(-1)^j 12 g(\chi^{12-j})\lambda(\chi^j) = \sum_{k=0}^{11} g(\chi^k) g(\chi^{j+k}) \overline{\lambda(\chi^k)}.$$

This theorem gives us, for each $0 \le j \le 11$, a linear relation among the $\lambda(\chi^k)$. Although there are twelve $\lambda(\chi^k)$, we have in the previous paragraph computed two of them, leaving us with ten. But actually, we have $\lambda(\chi^j) = \overline{\lambda(\chi^{12-j})}$ for $0 \le j \le 5$, so we really only have five independent unknowns. However, our strategy is, at first, to consider that we indeed have ten unknowns (namely, $\lambda(\chi^j)$ for $1 \le j \le 5$ and $7 \le j \le 11$) and use the theorem to derive as many linear relations between these ten unknowns as we can.

Doing this yields six independent equations, whose coefficients lie in $\mathbb{Q}(\zeta_{156})$ (the field over which the Gauss sums are defined). One is, however, able to obtain two more independent equations, by applying Theorem 4.5 of Atkin and Li starting not with $F = g$ (as we did previously), but rather with $F = g \otimes \chi^6$. Thus we get:

Theorem 4.3 (another special case of Theorem 4.5 of [Atkin and Li 1978]). *For* $0 \le j \le 11$, *we have*

$$(-1)^{j+1} 12 g(\chi^{12-j})\lambda(\chi^{6+j}) = \sum_{k=0}^{11} g(\chi^k) g(\chi^{j+k}) \overline{\lambda(\chi^{6+k})}.$$

As previously stated, this yields two more independent equations, giving us a linear system of eight independent equations in ten unknowns.

Let $x = \lambda(\chi)$ and $y = \lambda(\chi^2)$. We obtain the following two linear equations in the unknowns $x, \bar{x}, y, \bar{y}$:

$$c_1\bar{y} + c_2 y + c_3 x + c_4 \bar{x} = c_5, \tag{4-1}$$

$$c_6 y + c_7 x + c_8 \bar{x} = c_9; \tag{4-2}$$

here the c_i are explicit elements of $\mathbb{Q}(\zeta_{156})$. We now use the relations $x\bar{x} = y\bar{y} = 1$. We use (4-2) to eliminate y and $\bar{y}$ from (4-1) to obtain a linear relation between

x and $\bar{x}$; now, using $x\bar{x} = 1$, we obtain a quadratic in x. This quadratic has no root in $\mathbb{Q}(\zeta_{156})$; we need to adjoin $\sqrt{-7}$, so in fact we work in the field $\mathbb{Q}(\zeta_{1092})$; this might seem excessive, but the coefficients of g are anyway in $\mathbb{Q}(\zeta_7)^+$. This quadratic in x tells us that x is one of two values, and x determines all other $\lambda(\chi^j)$.

In order to determine which of the two values x really is, we computed two competing $\widetilde{S}$ matrices, and took the one which satisfied the correct relations with $\widetilde{T}$ to be the generators of $\mathrm{PSL}_2(\mathbb{F}_{13})$, namely,

$$\widetilde{S}^2 = \widetilde{T}^{13} = (\widetilde{S}\widetilde{T})^3 = 1.$$

Step 7. *The cuspforms.* We now have matrices giving the action of $\widetilde{S}$ on the twist basis, and the action of $\widetilde{T}$ on the isotypical basis; a change of basis matrix applied to either of these gives the action of both matrices in terms of the same basis. Write $\rho(S)$ and $\rho(T)$ for the 12×12 matrices giving the action of $\widetilde{S}$ and $\widetilde{T}$ respectively with respect to the twist basis.

We now compute the A_4-invariant subspace of V_0. Recall that our generators of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$ are

$$A = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -2 & -2 \\ -3 & 3 \end{pmatrix}.$$

Writing each generator as a word in S and T,

$$A = T^5 S T^{-2} S T^2 S T^3 S T^{-5},$$
$$B = T^4 S T^3 S T^{-3} S,$$

the action of A_4 on $S_2(\widetilde{\Gamma(13)})$ is given by the same words in the matrices $\widetilde{S}, \widetilde{T}$:

$$\widetilde{A} = \widetilde{T}^5 \widetilde{S} \widetilde{T}^{-2} \widetilde{S} \widetilde{T}^2 \widetilde{S} \widetilde{T}^3 \widetilde{S} \widetilde{T}^{-5},$$
$$\widetilde{B} = \widetilde{T}^4 \widetilde{S} \widetilde{T}^3 \widetilde{S} \widetilde{T}^{-3} \widetilde{S}.$$

The action of $\widetilde{A}$ and $\widetilde{B}$ on our vector space V_0 is given by taking the same words as above, but in $\rho(S)$ and $\rho(T)$; we call the resulting matrices $\rho(A)$ and $\rho(B)$.

The intersection of the kernels of $\rho(A) - I$ and $\rho(B) - I$ is one-dimensional, spanned by a vector of the coefficients, in the twist basis, of an A_4-invariant cuspform in V_0. These coefficients lie in the degree-9 field $\mathbb{Q}(\zeta_7^+, \zeta_{13}^{++})$, where by $\mathbb{Q}(\zeta_{13}^{++})$ we denote the unique cubic subfield of $\mathbb{Q}(\zeta_{13})$. We call this A_4-invariant form f.

We do not have to repeat the calculation for V_1 and V_2, because of the following fact. Here we regard V_i as $\overline{\mathbb{Q}}[\mathrm{PSL}_2(\mathbb{F}_{13})]$-modules.

Lemma 4.4. *Let γ be an element of* $\mathrm{PSL}_2(\mathbb{F}_{13})$. *The following diagram commutes*:

$$\begin{array}{ccc} V_0 & \xrightarrow{\sigma} & V_1 \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma} \\ V_0 & \xrightarrow{\sigma} & V_1 \end{array}$$

Proof. Each V_i admits a twist basis, corresponding to g^{σ^i} and its twists under powers of χ. Fixing this twist basis for each V_i, we find that the actions of $\widetilde{S}$ and $\widetilde{T}$ are exactly the same; this is because the coefficients in $\widetilde{S}$ and $\widetilde{T}$ we found for V_0 are invariant under the action of σ. □

The lemma allows us to conclude that for $i = 0, 1, 2$, the conjugate f^{σ^i} spans the A_4-invariant subspace of V_i, and hence that $\{f, f^\sigma, f^{\sigma^2}\}$ is a basis of $S_2(\widetilde{\Gamma_{A_4}(13)})$. Next we replace this basis with one defined over a smaller field, namely $\mathbb{Q}(\zeta_{13}^{++})$.

Write f as

$$f = F + \zeta_7^+ G + \zeta_7^{+2} H,$$

where F, G, H have coefficients in $\mathbb{Q}(\zeta_{13}^{++})$. The forms F, G, H form a basis for the same space, with coefficients in the smaller field:

Lemma 4.5. *The following two* $\mathbb{C}$*-spans are the same*:

$$\langle f, f^\sigma, f^{\sigma^2}\rangle = \langle F, G, H\rangle.$$

Proof. We have

$$\begin{pmatrix} f \\ f^\sigma \\ f^{\sigma^2} \end{pmatrix} = \begin{pmatrix} 1 & \zeta_7^+ & \zeta_7^{+2} \\ 1 & \sigma(\zeta_7^+) & \sigma(\zeta_7^{+2}) \\ 1 & \sigma^2(\zeta_7^+) & \sigma^2(\zeta_7^{+2}) \end{pmatrix} \begin{pmatrix} F \\ G \\ H \end{pmatrix},$$

where the matrix has nonzero determinant. □

As a final flourish, we apply the nonsingular transformation

$$\begin{pmatrix} 1 & 4 & 3 \\ -4 & -3 & 1 \\ 6 & -2 & 5 \end{pmatrix}$$

to obtain the following cuspforms (where again $\zeta = \zeta_{13}$), which are a basis for $S_2(\widetilde{\Gamma_{A_4}(13)})$:

$$\begin{aligned} f = {} & -q \\ & + (-\zeta^{11} - \zeta^{10} - \zeta^3 - \zeta^2) q^2 \\ & + (\zeta^{11} + \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 + \zeta^3 + \zeta^2 - 2) q^3 + \cdots, \end{aligned}$$

$$\begin{aligned} g = {} & (-\zeta^{11}-\zeta^{10}-\zeta^9-\zeta^7-\zeta^6-\zeta^4-\zeta^3-\zeta^2-1)q \\ & + (-\zeta^{11}-\zeta^{10}-\zeta^9-\zeta^7-\zeta^6-\zeta^4-\zeta^3-\zeta^2-2)q^2 \\ & \qquad + (-\zeta^{11}-\zeta^{10}-\zeta^3-\zeta^2-1)q^3 + \cdots, \\ h = {} & (\zeta^{11}+\zeta^{10}+\zeta^3+\zeta^2+3)q \\ & + (-\zeta^{11}-\zeta^{10}-\zeta^9-\zeta^7-\zeta^6-\zeta^4-\zeta^3-\zeta^2-3)q^2 \\ & \qquad + q^3 + \cdots. \end{aligned}$$

The final transformation was chosen retrospectively, solely for cosmetic reasons; it moves three of the rational points on the curve to $[1:0:0]$, $[0:1:0]$, $[0:0:1]$.

Having obtained the q-expansions, we may proceed with the canonical embedding algorithm of Galbraith, to obtain the smooth quartic equation for the model $\mathscr{C}$ given in the introduction. In practice this simply amounts to finding a linear relation between the q-expansions of the fifteen monomials of degree 4 in f, g, h. Although these q-expansions have coefficients defined over a cubic field (and there is no basis with rational q-expansions), the relation we find has rational coefficients.

Remark 4.6. Burcu Baran [2013] uses a different method to compute the equation of the modular curve $X_{\mathrm{ns}}(13)$; her method would also work for the present curve $X_{S_4}(13)$; one would need an analogue of her Proposition 6.1 for the subgroup at hand, which can be proved using her formulae in §3.

Remark 4.7. We also implemented a variation of the approach detailed here, using a modular symbol space of level 169, dual to the spaces V_i above. This second approach saved us from having to find the pseudoeigenvalues, since the matrices of both S and T on modular symbols are easily computed. This variation is also easy to adapt to find models for the curves $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$. Full details (including the cases $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$) may be found in the annotated Sage code [Banwait and Cremona 2013] and Sage worksheet [Cremona 2014].

5. Proof of Theorem 1.8: the j-map

In this section we explicitly determine the j-map

$$X_{S_4}(13) \xrightarrow{j} X(1) \cong \mathbb{P}^1_{\mathbb{Q}}$$

as a rational function on $X_{S_4}(13)$. This is a function of degree 91, which we seek to express in the form

$$j(X,Y,Z) = \frac{n(X,Y,Z)}{d_0(X,Y,Z)},$$

where n and d_0 are polynomials of the same degree over $\mathbb{Q}$. We first find a suitable denominator $d_0(X,Y,Z)$. The poles of j are all of order 13 and are at the seven cusps of $X_{S_4}(13)$, so we will find these, as $\overline{\mathbb{Q}}$-rational points on $X_{S_4}(13)$. Then

we find a cubic d in $\mathbb{Q}[X, Y, Z]$ which passes through these seven points (there is no quadratic which does), and set $d_0 = d^{13}$. Having found d_0 we determine the numerator n using linear algebra on q-expansions.

Remark 5.1. It would also be possible, in principal, to follow [Baran 2013] by computing the zeros of j numerically to sufficient precision to be able to recognise them as algebraic points, as then we would have the full divisor of the function j from which j itself could be recovered using an explicit Riemann–Roch space computation. Our method has the advantage of not requiring any numerical approximations.

We first need to find which points on our model $\mathscr{C}$ for $X_{S_4}(13)$ are the seven cusps. It turns out that there are three which are defined and conjugate over the degree-3 subfield $\mathbb{Q}(\alpha)$ of $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_{13}$ and $\alpha = \zeta + \zeta^5 + \zeta^8 + \zeta^{12}$, and the other four are defined and conjugate over the degree-4 subfield $\mathbb{Q}(\beta)$ of $\mathbb{Q}(\zeta)$, where $\beta = \zeta + \zeta^3 + \zeta^9$.

Proposition 5.2. *On the model $\mathscr{C}$ for $X_{S_4}(13)$, the seven cusps are given by the three Galois conjugates of*

$$[-3\alpha^2 - 7\alpha + 1 : 4\alpha^2 + 11\alpha - 3 : 5]$$

and the four conjugates of

$$[3\beta^3 + 6\beta^2 + 6\beta - 15 : \beta^3 + \beta^2 - 4\beta - 4 : 9],$$

where α and β have minimal polynomials x^3+x^2-4x+1 and $x^4+x^3+2x^2-4x+3$ respectively.

The degree-3 cusps are easy to obtain; the cusp corresponding to the point $i\infty$ on the extended upper half-plane $\mathscr{H}^*$ has coordinates given by the leading coefficients of the three basis cuspforms f, g, h; denoting by φ the map

$$\begin{aligned} \varphi : \Gamma_{A_4}(13)\backslash\mathscr{H}^* &\xrightarrow{\sim} X_{S_4}(13), \\ \Gamma_{A_4}(13)\cdot z &\longmapsto [f(z) : g(z) : h(z)], \end{aligned}$$

we see that $\varphi(i\infty) = [a_1(f) : a_1(g) : a_1(h)]$. Expressing these coordinates in terms of α gives the degree-3 cusp given in the proposition.

It is possible to determine in advance the Galois action on the cusps, as in the following lemma. However, note that in practice our method to compute the cusps algebraically, given below, does not require this knowledge.

Lemma 5.3. *The absolute Galois group of $\mathbb{Q}$ acts on the seven cusps with two orbits, of sizes* 3 *and* 4.

Proof. We know *a priori* that the cusps are all defined over $\mathbb{Q}(\zeta_{13})$. Theorem 1.3.1 in [Stevens 1982] explains how to compute the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$ on the cusps of a modular curve X of level N, provided that the field of rational functions on X is generated by rational functions whose q-expansions have rational coefficients. This does not apply here, since the field of modular functions for $\Gamma_{A_4}(13)$ is not generated by functions with rational q-expansions, but rather by functions with q-expansions in the cubic field $\mathbb{Q}(\alpha)$. But following Stevens' method we can compute the action of the absolute Galois group of $\mathbb{Q}(\alpha)$, which acts through the cyclic subgroup of order 4 of $(\mathbb{Z}/13\mathbb{Z})^*$ fixing α. We find that it fixes three cusps (which we already know from above, as they are defined over $\mathbb{Q}(\alpha)$), and permutes the remaining four cyclically. It follows that the other four cusps are also permuted cyclically by the full Galois group, and hence have degree 4 as claimed. □

It remains to find the coordinates of one cusp of degree 4.

Let $c \in \Gamma_{A_4}(13)\backslash\mathbb{P}^1(\mathbb{Q})$ be any cusp. Then there exists $\gamma \in \mathrm{PSL}_2(\mathbb{Z})\backslash\Gamma_{A_4}(13)$ such that $\gamma(c) = \infty$, and hence,

$$\alpha(c) = [a_1(f|\gamma) : a_1(g|\gamma) : a_1(h|\gamma)].$$

Since we already computed in the previous section the action of $\mathrm{PSL}_2(\mathbb{Z})$ on the cuspforms f, g, h, we can compute the right-hand side of this equation for any γ. With some work one can show that the cubic cusps are obtained using $c = \infty, 1$ and $7/6$, while the quartic cusps are obtained from $c = 2, 3, 6$ and 9; or we can simply choose random $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ until we find a point which is not one of the three conjugates we already have. This proves Proposition 5.2.

Next we find a cubic curve passing through these seven points.

Proposition 5.4. *The following cubic passes through the seven cusps*:

$$5X^3 - 19X^2Y - 6XY^2 + 9Y^3 + X^2Z - 23XYZ - 16Y^2Z + 8XZ^2 - 22YZ^2 + 3Z^3.$$

Proof. The full linear system of degree 3 associated to $\mathcal{O}_{\mathbb{P}^2}(1)$ has dimension 10, and the subsystem passing though the seven cusps has dimension 3 with a basis in $\mathbb{Q}[X, Y, Z]$. Using LLL-reduction we found a short element which does not pass through any rational points on $\mathcal{C}$ (to simplify the evaluation of the j-map at these points later). □

Since all cusps have ramification degree 13 under the j-map, a possible choice for the denominator of the j-map is to take the thirteenth power $d_0 = d^{13}$ of this cubic.

Next we turn to the numerator $n(X, Y, Z)$, which is a polynomial of degree 39. The idea is to consider an arbitrary degree-39 polynomial in the q-expansions of the cusp forms f, g, h, and compare it with the known q-expansion of $j \cdot d(f, g, h)^{13}$. This gives a system of linear equations which can be solved.

The full linear system of degree 39 has dimension 820, but modulo the defining quartic polynomial for $\mathscr{C}$ we can reduce the number of monomials needing to be considered to only 154. We chose those monomials in which either X does not occur, or else Y does not occur and X has exponent 1 or 2, but this is arbitrary.

Now we consider the equation

$$n(X,Y,Z) - j(X,Y,Z)\cdot d(X,Y,Z)^{13} = 0$$

as a q-expansion identity after substituting f, g, h for X, Y, Z. Using 250 terms in the q-expansions (giving a margin to safeguard against error) and comparing coefficients gives 250 equations for the unknown coefficients of $n(X,Y,Z)$. There is a unique solution, which has rational coefficients. Although we have apparently only shown that the equation holds modulo q^{250}, it must hold identically, since we know that there is exactly one solution.

The expression for $n(X,Y,Z)$ we obtain this way is too large to display here (it has 151 nonzero integral coefficients of between 46 and 75 digits), but can easily be used to evaluate the j-map at any given point on the curve $\mathscr{C}$. For the sake of completeness, however, we give here explicitly the zeros of the j-map from which (together with the poles) it may be recovered; the complete expression may be seen in [Cremona 2014].

The 91 zeros of j consist of 29 points with multiplicity 3 and four with multiplicity 1, all defined over the number field $M = \mathbb{Q}(\delta)$, where δ has minimal polynomial

$$x^8 - 9x^6 + 32x^4 - 9x^2 + 1,$$

which is Galois with group D_8. This field is the splitting field of the polynomial $P(t)$ defined in the next section, so is also the field of definition of the points in the fibre over $j = 0$ of the covering map $X_0(13) \to X(1)$. Some of the 33 zeros are defined over the quartic subfields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, where α and β have minimal polynomials $x^4 + 13x^2 - 39$ and $x^4 - 13x^2 + 52$ respectively. Their coordinates are as follows (together with all Galois conjugates): with multiplicity 1 we have

$$[3\beta^3 + 2\beta^2 - 15\beta - 14 : -3\beta^3 + 4\beta^2 + 29\beta - 22 : -3\beta^3 - 4\beta^2 + 25\beta + 46],$$

and with multiplicity 3 we have the rational point $[1:0:0]$, the degree-4 points

$$[2(-\alpha^2 + 5\alpha - 4) : -\alpha^3 - \alpha^2 + \alpha + 6 : \alpha^3 + 14\alpha - 35],$$
$$[\beta^3 - 2\beta^2 - 9\beta + 14 : 2(\beta^2 - \beta - 2) : 2(-\beta^3 - 2\beta^2 + 7\beta + 16)],$$
$$[4(\beta - 1) : \beta^3 - 7\beta - 10 : 2(\beta^3 + 2\beta^2 - 7\beta - 12)],$$

and the degree-8 points

$$[\delta^7+2\delta^6-8\delta^5-8\delta^4+36\delta^3+12\delta^2-5\delta-2 : 8(\delta^3+\delta^2) : -\delta^7-2\delta^6+4\delta^5-28\delta^3-8\delta^2+5\delta+2]$$

and

$$[2(-\delta^6+4\delta^5-10\delta^3+4\delta-1) : -3\delta^7+2\delta^6+28\delta^5-32\delta^4-52\delta^3+16\delta^2+7\delta-2 : \delta^7-2\delta^6-4\delta^5+4\delta^4+4\delta^3+8\delta^2-9\delta+2].$$

6. Proof of Corollary 1.9

Evaluating the j-map at the six points in $\mathscr{C}(\mathbb{Q}(\sqrt{13}))$ exhibited in the introduction yields the five j-invariants listed in the statement of Corollary 1.9, together with $j=0$, which is the image of $[1:0:0]$. We know that any elliptic curve E over $\mathbb{Q}(\sqrt{13})$ with one of these six j-invariants has $H_{E,13}\subseteq A_4$. Any elliptic curve with $j=0$ has complex multiplication, with mod-13 image contained in a split Cartan subgroup (split since $13\equiv 1 \pmod 3$). Hence what remains to prove in this section is that $H_{E,13}\cong A_4$ for the five nonzero j-invariants listed.

Lemma 6.1. *Let l be a prime for which $X_0(l)$ has genus 0 (that is, $l=2,3,5,7,13$). There is an explicit polynomial $F_l(X,Y)\in\mathbb{Z}[X,Y]$ such that, if E/K is an elliptic curve over a number field, then*

$$H_{E,l}\cong \mathrm{Gal}\big(F_l(X,j(E))\big).$$

Proof. The function field of $X_0(l)$ is generated by a single modular function t (the so-called "Hauptmodul"), and classically there is a canonical choice of such, for each l. The j-function is a rational function of t of degree $l+1$ of the form $P(t)/t$, where P is an explicit integral polynomial of degree $l+1$.

Define $F_l(X,Y)=P(X)-YX\in\mathbb{Z}[X,Y]$. Let E/K be an elliptic curve over a number field, and consider the set of roots of $F_l(X,j(E))\in K[X]$ over $\overline{\mathbb{Q}}$. As a set, this is in bijection with the set of preimages t of $j(E)$ under the j-map $X_0(l)\to X(1)$ (which is unramified away from $j=0$ and $j=1728$), and hence is in Galois-equivariant bijection with the l-isogenies on E. Hence the Galois action on the set of $l+1$ isogenies is isomorphic to the Galois action on the roots of $F_l(X,j(E))$. □

For $l=13$, we have

$$P(t)=(t^2+5t+13)\cdot(t^4+7t^3+20t^2+19t+1)^3,$$

and hence

$$F_{13}(X,Y)=(X^2+5X+13)\cdot(X^4+7X^3+20X^2+19X+1)^3-XY.$$

For each j-invariant listed in Corollary 1.9 we may verify that $F_{13}(X, j)$ has Galois group isomorphic to A_4 over $\mathbb{Q}(\sqrt{13})$, and for the rational j-values, isomorphic to S_4 over $\mathbb{Q}$.

7. Proof of Proposition 1.3

By Proposition 2.2 and Lemma 2.1, Proposition 1.3 is equivalent to the following purely group-theoretic statement.

Proposition 7.1. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$. Then H is Hasse if and only if one of the following holds*:

(1) $H \cong A_4$ *and* $l \equiv 1 \pmod{12}$.

(2) $H \cong S_4$ *and* $l \equiv 1 \pmod{24}$.

(3) $H \cong A_5$ *and* $l \equiv 1 \pmod{60}$.

(4) $H \cong D_{2n}$ *and* $l \equiv 1 \pmod 4$, *where* $n > 1$ *is a divisor of* $(l-1)/2$, *and the pullback of* H *to* $\mathrm{GL}_2(\mathbb{F}_l)$ *is contained in the normaliser of a split Cartan subgroup.*

We begin the forward implication of this Proposition by quoting the following lemma of Sutherland, which is a small piece of his Lemma 1.

Lemma 7.2 (Sutherland). *If $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ is Hasse, then $l \nmid |H|$.*

We may now invoke the following classical result (see [Lang 1976, Theorem XI.2.3]).

Fact 7.3. *Let H be a subgroup of $\mathrm{PGL}_2(\mathbb{F}_l)$ with $l \nmid |H|$, and let G denote its pullback to $\mathrm{GL}_2(\mathbb{F}_l)$. Then one of the following occurs*:

- *H is cyclic, and G is contained in a Cartan subgroup.*
- *H is dihedral, and G is contained in the normaliser of a Cartan subgroup.*
- *H is isomorphic to A_4, S_4 or A_5.*

Clearly H being cyclic is incompatible with H being Hasse, so either $H \cong D_{2n}$ for $n > 1$, or H is one of A_4, S_4 or A_5.

Lemma 7.4. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ be Hasse, and let $h \in H$. Then the order of h must divide $(l-1)/2$.*

Proof. Write $H' := \langle h \rangle$, a cyclic group of order r say, prime to l. By Fact 7.3, the pullback G' of H' to $\mathrm{GL}_2(\mathbb{F}_l)$ is contained in a Cartan subgroup. If this Cartan subgroup were nonsplit, then the elements of G' would *not* be diagonalisable, and hence h would not fix an element of $\mathbb{P}^1(\mathbb{F}_l)$, contradicting the Hasse assumption. Thus the Cartan subgroup must be split, so the elements of G' are diagonalisable,

and thus h has two fixed points; the same is true for every nonidentity element of H'. We now apply the orbit counting lemma to H':

$$s := |\mathbb{P}^1(\mathbb{F}_l)/H| = 2 + \frac{l-1}{r}. \tag{7-1}$$

Note that this formula says that there are $(l-1)/r$ nontrivial orbits of $\mathbb{P}^1(\mathbb{F}_l)$ under h (a trivial orbit being a fixed point). The sizes of these $(l-1)/r$ nontrivial orbits all divide r and sum to $l-1$, and hence they are all equal to r.

We claim that s must be even. This is clear if r is odd, by (7-1). If r is even, then

$$\operatorname{sign}(h) = (-1)^{s-2} = (-1)^s,$$

where sign means the sign as a permutation. The key observation, which proves the claim, is that $\operatorname{sign}(h)$ must be 1, because it coincides with $\det h$.

As s must be even, we look finally at (7-1) to conclude that r must divide $l-1$ with even quotient, and the lemma is proved. □

A part of the previous proof is worth framing, for it explains why the pullback of the dihedral group D_{2n} is contained in the normaliser of a *split* Cartan subgroup.

Lemma 7.5. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ be Hasse, and let $h \in H$. Let $H' := \langle h \rangle$, and let G' be the pullback of H' to $\mathrm{GL}_2(\mathbb{F}_l)$. Then G' is contained in a split Cartan subgroup.*

Lemma 7.4 implies that the n in D_{2n} divides $(l-1)/2$, and also the congruence restrictions for A_4, S_4 and A_5; indeed, since A_4 contains elements of order 1, 2 and 3, we must have that 2 and 3 divide $(l-1)/2$, or equivalently, $l \equiv 1 \pmod{12}$; the same argument works for S_4 and A_5. This proves the forward implication of the group-theoretic proposition above.

We now prove the converse; that is, if H is isomorphic to one of the four subgroups listed above, then it satisfies the Hasse condition.

The easier thing to prove is that every element h in H fixes a point of $\mathbb{P}^1(\mathbb{F}_l)$, so we address this first. Suppose, for a contradiction, that we have $h \in H$ which fixes no point of $\mathbb{P}^1(\mathbb{F}_l)$, let r be the order of this h, and let $s := |\mathbb{P}^1(\mathbb{F}_l)/h|$ be the number of orbits. Proposition 2 of [Sutherland 2012] says that $\operatorname{sign}(h) = (-1)^s$; in particular, s must be even. Applying the orbit counting lemma to the action of $\langle h \rangle$ on $\mathbb{P}^1(\mathbb{F}_l)$ yields the formula $s = (l+1)/r$, and hence r must divide $(l+1)/2$. We now do a case-by-case elimination. Suppose first that $H \cong D_{2n}$ with all the other conditions expressed above. The order of any element of this group must divide $(l-1)/2$. Since $(l-1)/2$ and $(l+1)/2$ are coprime, we obtain the desired contradiction. The argument in the other cases is similar.

We are left with proving that, in the four cases, no point of $\mathbb{P}^1(\mathbb{F}_l)$ is fixed by the whole of H. This follows from the following well-known fact from group theory; see for example Theorem 80.27 in [Curtis and Reiner 1987].

Lemma 7.6. *Let G be a group, S a transitive left G-set, and H a subgroup of G. Denote by $H\backslash S$ the set of orbits of S under H. Let B denote the G-stabiliser of any point of S. Then we have an isomorphism of H-sets*

$$S \cong \bigsqcup_g H/(H \cap B^g),$$

where g runs over a set of double coset representatives for $H\backslash G/B$; here we regard the S on the left as an H-set.

This allows us to prove that, in the four cases, there is no point of $\mathbb{P}^1(\mathbb{F}_l)$ fixed by all of H. We apply the lemma with $G = \mathrm{PSL}_2(\mathbb{F}_l)$, $S = \mathbb{P}^1(\mathbb{F}_l)$, and B the stabiliser of ∞, that is, the Borel subgroup. By the lemma, an orbit of size 1 corresponds to a double coset representative g for which $H \subseteq B^g$. But this inclusion is impossible, since each H contains D_4 and B does not. This finishes the proof.

8. Proof of Proposition 1.6

Let $E/\mathbb{Q}(\sqrt{l})$ be a nondihedral Hasse at l curve. Then $l \equiv 1 \pmod{12}$, $\pmod{24}$ or $\pmod{60}$, according as the projective image of $\bar{\rho}_{E,l}$ is A_4, S_4 or A_5, by Proposition 7.1. However, there is the following general result of David regarding the projective mod-p image, which we are grateful to Nicolas Billerey for bringing to our attention. For F a number field, and p a prime, let

$$e_p := \max_{\mathfrak{p}}\{e_{\mathfrak{p}}\},$$

where $e_{\mathfrak{p}}$ denotes the ramification index of the prime $\mathfrak{p} \mid p$.

Fact 8.1 [David 2011, Lemme 2.4]. *For an elliptic curve defined over a number field F, the projective mod-p image contains an element of order at least $(p-1)/(4e_p)$.*

Applying this with $F = \mathbb{Q}(\sqrt{l})$ and $p = l$, we see that:

- A_4 can occur only when $l \leq 25$ and $l \equiv 1 \pmod{12}$, so only for $l = 13$.
- S_4 can occur only when $l \leq 33$ and $l \equiv 1 \pmod{24}$, so cannot occur.
- A_5 can occur only when $l \leq 41$ and $l \equiv 1 \pmod{60}$, so cannot occur.

Thus only A_4 is possible, for the prime $l = 13$.

9. The Jacobian of $X_{S_4}(13)$

Over the complex numbers, there are precisely three modular curves of level 13 and genus 3; they are $X_{\mathrm{s}}(13)$, $X_{\mathrm{ns}}(13)$, and $X_{S_4}(13)$; see for example the table of

[Cummins and Pauli 2003]. Observe that all of these curves are defined over $\mathbb{Q}$ and are geometrically connected.

Baran [2013; 2012] proved in two different ways that the curves $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$ are in fact $\mathbb{Q}$-isomorphic. Her first proof [2013] was computational; she computed models of both curves and showed that they give isomorphic curves. Her second proof was more conceptual, establishing that the Jacobians $J_{\mathrm{s}}(13)$ and $J_{\mathrm{ns}}(13)$ are isomorphic, with an isomorphism preserving the canonical polarisation of both Jacobians; the Torelli theorem then gives the result.

The $\mathbb{Q}$-points on $X_{\mathrm{s}}(13)$ have not yet been determined; in fact, as discussed in the final section of [Bilu et al. 2013], $p = 13$ is the *only* prime p for which the $\mathbb{Q}$-points on $X_{\mathrm{s}}(p)$ have *not* yet been determined, and Baran's result, linking $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$, may give some reason for why this $p = 13$ case is so difficult: the determination of $\mathbb{Q}$-points on $X_{\mathrm{ns}}(p)$ is known to be a difficult problem.

Another reason for this difficulty is that $J_{\mathrm{s}}(13)(\mathbb{Q})$ is likely to have Mordell–Weil rank 3, which equals the genus, so the method of Chabauty to determine the rational points does not apply. By likely, we mean that the analytic rank of this Jacobian is 3, so under the Birch–Swinnerton-Dyer conjecture, we would have that the Mordell–Weil rank is also 3.

The curves $X_{\mathrm{s}}(13)$ and $X_{S_4}(13)$ are *not* isomorphic, even over $\mathbb{C}$; this may be verified using the explicit models of both curves, by computing certain invariants of genus-3 curves and observing that they are different — we are grateful to Jeroen Sijsling for carrying out this computation.

Nevertheless, their Jacobians are isogenous:

Proposition 9.1. *The Jacobians $J_{\mathrm{s}}(13)$ and $J_{S_4}(13)$ of the modular curves $X_{\mathrm{s}}(13)$ and $X_{S_4}(13)$ are $\mathbb{Q}$-isogenous.*

Proof. Let $G = \mathrm{GL}_2(\mathbb{F}_{13})$, B the Borel subgroup of G, and for K any subgroup of $\mathrm{PGL}_2(\mathbb{F}_{13})$, denote by $\pi^{-1}(K)$ the pullback of K to G. One first verifies (for example in Magma) that there is a $\mathbb{Q}[G]$-module isomorphism as follows:

$$2\mathbb{Q}[G/C_{\mathrm{s}}^{+}] \oplus \mathbb{Q}[G/\pi^{-1}(C_{13} \ltimes C_3)] \oplus \mathbb{Q}[G/\pi^{-1}(C_{13} \ltimes C_4)] \cong 2\mathbb{Q}[G/\pi^{-1}(S_4)] \oplus \mathbb{Q}[G/\pi^{-1}(D_{26})] \oplus \mathbb{Q}[G/B]. \quad (9\text{-}1)$$

For R any $\mathbb{Q}$-algebra, apply the contravariant functor $\mathrm{Hom}_{\mathbb{Q}[G]}(-, J(13)(R))$ to this formula; this yields, by a well-known method of Kani and Rosen ([1989], but see also [de Smit and Edixhoven 2000]), the following $\mathbb{Q}$-isogeny between Jacobians of modular curves of level 13:

$$J_{S_4}^2 \oplus J_{\pi^{-1}(D_{26})} \oplus J_B \quad \longrightarrow \quad J_{\mathrm{s}}^2 \oplus J_{\pi^{-1}(C_{13} \ltimes C_3)} \oplus J_{\pi^{-1}(C_{13} \ltimes C_4)}; \quad (9\text{-}2)$$

here we have, for simplicity, denoted the Jacobian of the modular curve $X_H(13)$ simply as J_H.

However, as may be checked by computing genera of these curves, most of these terms are zero, leaving us with a $\mathbb{Q}$-isogeny $J_{S_4}^2 \to J_{\mathrm{s}}^2$. Restricting this isogeny to the first component yields an isogeny between J_{S_4} and its image in J_{s}^2. This image must have dimension 3, and since J_{s} is simple over $\mathbb{Q}$ (as shown in Section 2 of [Baran 2012]), the image is isogenous to J_{s}. □

Remark 9.2. One may still wonder whether J_{s} is isomorphic to J_{S_4} or not. They are indeed not isomorphic; for if they were, then the arguments in Section 3 of [Baran 2012] would apply, and we would conclude that the curves X_{s} and X_{S_4} were isomorphic, which we know is not true.

Remark 9.3. With additional work one may show that there is a $\mathbb{Q}$-isogeny between J_{s} and J_{S_4} of degree a power of 13, and furthermore that 13 must divide the degree of any isogeny.

10. The evidence for Conjecture 1.14

There can be no Hasse at 11 curve over $\mathbb{Q}(\sqrt{-11})$, because 11 is not congruent to 1 (mod 4) (see Proposition 1.3). Thus, we let K be any other quadratic field. Sutherland's result (Proposition 1.1) tells us that, if E/K is a Hasse at 11 curve over K, then it corresponds to a K-point on the modular curve $X_{\mathrm{s}}(11)$. A model for this curve, as well as an expression for the j-map $X_{\mathrm{s}}(11) \to X(1)$, may be computed along the lines of that for $X_{S_4}(13)$; we obtain a singular projective model

$$X_{\mathrm{s}}(11) : y^2 = 4X^6 - 4X^4 - 2X^3 + 2X^2 + \tfrac{3}{2}X + \tfrac{1}{4}.$$

We used Magma to search for K-points on this curve, for every quadratic field with absolute discriminant up to 10^7, and evaluated the j-map at these points, giving many potential j-invariants of Hasse at 11 curves over quadratic fields.

Given such a j-invariant $j_0 \in K$, we considered the polynomial $\Phi_{11}(X, j_0) \in K[X]$, that is, the classical modular polynomial at 11, evaluated at $Y = j_0$.

Proposition 10.1. *The pair* $(11, j_0)$ *is exceptional for* K *if and only if the polynomial* $\Phi_{11}(X, j_0) \in K[X]$

- *has no linear factor over* K, *and*
- *modulo every prime* $\mathfrak{p}$ *in a density-one set, it has a linear factor.*

Proof. This is a direct consequence of the fact, proved in [Igusa 1959], that, for an elliptic curve E over any field F, and an integer N with $\mathrm{char}\, F \nmid N$, the existence of a cyclic F-rational N-isogeny on E is equivalent to $\Phi_N(X, j(E)) \in F[X]$ having a linear factor. □

We found that, for all of our potential j-invariants, $\Phi_{11}(X, j_0)$ had many reductions with no linear factor — too many to be of density zero. This suggested to us that Conjecture 1.14 should be true.

The results of [Serre 1972] imply the following.

Proposition 10.2. *Let K be a quadratic field. If E/K is Hasse at* 11, *then either* 11 *ramifies in K, or E has additive reduction at all places v of K dividing* 11.

Proof. If 11 is unramified in K and E has a place v of good or multiplicative reduction above 11, then the results of [Serre 1972] (see in particular Section 4) give the image of the inertia subgroup at v of G_K under $\bar{\rho}_{E,11}$, which in all cases is incompatible with the projective image being isomorphic with D_{10}. □

We can also say, by part (a) of Proposition 1.1, that E/K is Hasse at 11 if and only if $H_{E,11} \cong D_{10}$, and so corresponds to a K-point on the modular curve $X_{D_{10}}(11)$ parametrising such elliptic curves. This modular curve is the $\mathbb{Q}(\sqrt{-11})$-twist of the more usual modular curve $X_0(121)$, which, by Theorem 4.9 of [Bars 2012], has only finitely many quadratic points. Thus, we can say that there are only finitely many quadratic fields over which a Hasse at 11 curve might exist. If we could determine exactly which quadratic fields K arise for the twist $X_{D_{10}}(11)$ of $X_0(121)$, we could prove the conjecture by determining the K-points on $X_{\mathrm{s}}(11)$, find the finite list of potential j-invariants, and show that none of them yield $H_{E,5} \cong D_{10}$ (this last step can be established by recent work of Sutherland, who has implemented an algorithm to determine the mod-p Galois image of any elliptic curve over any number field). The methods of Freitas, Le Hung and Siksek [Freitas et al. 2013] for determining the quadratic points on $X_0(N)$ for certain N may be of use here.

Acknowledgements

We are grateful to Jeroen Sijsling for helping us with the computation of the j-function in Theorem 1.8, as well as verifying that the genus-3 curves in Section 9 are not isomorphic. We would like to thank Damiano Testa for making interesting observations and suggestions regarding the curve $X_{S_4}(13)$ and its rational and quadratic points, Tim and Vladimir Dokchitser for their comments and suggestions regarding Theorem 1.5, Alex Bartel for finding the isomorphism (9-1), Martin Orr for communicating to us results about subvarieties of products of abelian varieties, and Andrew Sutherland for verifying the mod-13 Galois images of the elliptic curves in Corollary 1.9. Finally, we thank the anonymous referees for their careful reading and comments, and for verifying our results.

All computations in this paper were carried out using either Sage (see [Sage 2013]) or Magma (see [Bosma et al. 1997]), or both. Annotated Sage code which reproduces the computations in this paper concerning $X_{S_4}(13)$, together with similar computations for $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$, is available (see [Banwait and Cremona 2013]), as well as a Sage worksheet with the complete computation (see [Cremona 2014]).

References

[Anni 2014] S. Anni, "A local-to-global principle for isogenies of prime degree over number fields", *J. London Math. Soc.* **89**:3 (2014), 745–761.

[Atkin and Li 1978] A. O. L. Atkin and W. C. W. Li, "Twists of newforms and pseudo-eigenvalues of W-operators", *Invent. Math.* **48**:3 (1978), 221–243. MR 80a:10040 Zbl 0369.10016

[Banwait and Cremona 2013] B. Banwait and J. Cremona, "Computing the modular curves $X_{sp}(13)$, $X_{ns}(13)$ and $X_{A_4}(13)$ using modular symbols in Sage (annotated Sage code)", preprint, 2013, http://arxiv.org/src/1306.6818v3/anc/X13.pdf.

[Baran 2012] B. Baran, "An exceptional isomorphism between modular curves of level 13 via Torelli's theorem", preprint, 2012, http://www-personal.umich.edu/~bubaran/torelli.pdf.

[Baran 2013] B. Baran, "An exceptional isomorphism between modular curves of level 13", preprint, 2013, http://www-personal.umich.edu/~bubaran/bbaran.pdf.

[Bars 2012] F. Bars, "On quadratic points of classical modular curves", preprint, 2012, http://mat.uab.es/~francesc/surveyMomose.pdf.

[Bilu et al. 2013] Y. Bilu, P. Parent, and M. Rebolledo, "Rational points on $X_0^+(p^r)$", *Ann. Inst. Fourier* (*Grenoble*) **63**:3 (2013), 957–984. MR 3137477 Zbl 06227477

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Cremona 1997] J. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. MR 99e:11068 Zbl 0872.14041

[Cremona 2014] J. Cremona, "*X13* (Sage worksheet)", 2014, http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/X13.sws.

[Cummins and Pauli 2003] C. J. Cummins and S. Pauli, "Congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus less than or equal to 24", *Experiment. Math.* **12**:2 (2003), 243–255. MR 2004i:11037 Zbl 1060.11021

[Curtis and Reiner 1987] C. W. Curtis and I. Reiner, *Methods of representation theory, II: With applications to finite groups and orders*, Wiley, New York, 1987. MR 88f:20002 Zbl 0616.20001

[David 2011] A. David, "Borne uniforme pour les homothéties dans l'image de Galois associée aux courbes elliptiques", *J. Num. Theory* **131**:11 (2011), 2175–2191. MR 2012k:11075 Zbl 1246.11116

[Dickson 1901] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, B. G. Teubner, Leipzig, 1901. JFM 32.0128.01

[Freitas et al. 2013] N. Freitas, B. V., L. Hung, and S. Siksek, "Elliptic curves over real quadratic fields are modular", preprint, 2013. arXiv 1310.7088

[Galbraith 1996] S. Galbraith, *Equations for modular curves*, Ph.D. thesis, University of Oxford, 1996, https://www.math.auckland.ac.nz/~sgal018/thesis.pdf.

[Igusa 1959] J.-i. Igusa, "Kroneckerian model of fields of elliptic modular functions", *Amer. J. Math.* **81** (1959), 561–577. MR 21 #7214 Zbl 0093.04502

[Kani and Rosen 1989] E. Kani and M. Rosen, "Idempotent relations and factors of Jacobians", *Math. Ann.* **284**:2 (1989), 307–327. MR 90h:14057 Zbl 0652.14011

[Lang 1976] S. Lang, *Introduction to modular forms*, Grundlehren Math. Wiss. **222**, Springer, New York, 1976. MR 55 #2751 Zbl 0344.10011

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001

[Ligozat 1977] G. Ligozat, "Courbes modulaires de niveau 11", pp. 149–237 in *Modular functions of one variable, V* (Bonn, 1976), edited by J. P. Serre and D. B. Zagier, Lecture Notes in Math. **601**, Springer, Berlin, 1977. MR 57 #3079 Zbl 0357.14006

[Maier 2009] R. S. Maier, "On rationally parametrized modular equations", *J. Ramanujan Math. Soc.* **24**:1 (2009), 1–73. MR 2010f:11060 Zbl 1214.11049

[Mazur 1977a] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186. MR 80c:14015 Zbl 0394.14008

[Mazur 1977b] B. Mazur, "Rational points on modular curves", pp. 107–148 in *Modular functions of one variable, V* (Bonn, 1976), edited by J. P. Serre and D. B. Zagier, Lecture Notes in Math. **601**, Springer, Berlin, 1977. MR 56 #8579 Zbl 0357.14005

[Sage 2013] The Sage Development Team, Sage Mathematics Software (Version 5.10), 2013, http://www.sagemath.org.

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[de Smit and Edixhoven 2000] B. de Smit and B. Edixhoven, "Sur un résultat d'Imin Chen", *Math. Res. Lett.* **7**:2-3 (2000), 147–153. MR 2001j:11043 Zbl 0968.14024

[Stevens 1982] G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics **20**, Birkhäuser, Boston, 1982. MR 87b:11050 Zbl 0529.10028

[Sutherland 2012] A. V. Sutherland, "A local-global principle for rational isogenies of prime degree", *J. Théor. Nombres Bordeaux* **24**:2 (2012), 475–485. MR 2950703 Zbl 1276.11095

[Turner 2013] C. L. Turner, *Lattice methods for finding rational points on varieties over number fields*, Ph.D. thesis, University of Warwick, 2013, http://webcat.warwick.ac.uk/record=b2715884~S1.

Communicated by Joseph Silverman
Received 2013-09-03 Revised 2014-03-25 Accepted 2014-04-26

Barinder.Banwait@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux, Université de Bordeaux I, 351 Cours de la Libération, 33405 Talence, France

J.E.Cremona@warwick.ac.uk *Mathematics Institute, University of Warwick, Zeeman Building, Coventry CV4 7AL, United Kingdom*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1231

Local cohomology with support in generic determinantal ideals

Claudiu Raicu and Jerzy Weyman

To the memory of Andrei Zelevinsky

For positive integers $m \geq n \geq p$, we compute the $\mathrm{GL}_m \times \mathrm{GL}_n$-equivariant description of the local cohomology modules of the polynomial ring $S = \mathrm{Sym}(\mathbb{C}^m \otimes \mathbb{C}^n)$ with support in the ideal of $p \times p$ minors of the generic $m \times n$ matrix. Our techniques allow us to explicitly compute all the modules $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$, for $\underline{x}$ a partition and $I_{\underline{x}}$ the ideal generated by the irreducible subrepresentation of S indexed by $\underline{x}$. In particular we determine the regularity of the ideals $I_{\underline{x}}$, and we deduce that the only ones admitting a linear free resolution are the powers of the ideal of maximal minors of the generic matrix, as well as the products between such powers and the maximal ideal of S.

1. Introduction

Given positive integers $m \geq n$ and a field $\mathbb{K}$ of characteristic zero, we consider the space $\mathbb{K}^{m\times n}$ of $m \times n$ matrices and the ring S of polynomial functions on this space. For each $p = 1, \ldots, n$ we define the ideal $I_p \subset S$ generated by the polynomial functions in S that compute the $p \times p$ minors of the matrices in $\mathbb{K}^{m\times n}$. The goal of this paper is to describe for each p the local cohomology modules $H^\bullet_{I_p}(S)$ of S with support in the ideal I_p. The case $p = n$ was previously analyzed by the authors in joint work with Emily Witt [Raicu et al. 2014]. There is a natural action of the group $\mathrm{GL}_m \times \mathrm{GL}_n$ on $\mathbb{K}^{m\times n}$ and hence on S, and this action preserves each of the ideals I_p. This makes the $H^\bullet_{I_p}(S)$ into $\mathrm{GL}_m \times \mathrm{GL}_n$-representations, and our results describe the characters of these representations explicitly. Our methods also allow us to determine explicitly the characters of all the modules $\mathrm{Ext}^\bullet_S(S/I, S)$, where I is an ideal of S generated by an irreducible $\mathrm{GL}_m \times \mathrm{GL}_n$-subrepresentation of S, and in particular to determine the regularity of such ideals. It is an interesting problem to determine the minimal free resolutions of such ideals I, which unfortunately has

MSC2010: primary 13D45; secondary 14M12.
Keywords: local cohomology, determinantal ideals, regularity.

only been answered in a small number of cases. We hope that our results will help shed some light on this problem in the future.

We will adopt a basis-independent notation throughout the paper, writing F (resp. G) for a $\mathbb{K}$-vector space of dimension m (resp. n), and thinking of $F^* \otimes G^*$ as the space $\mathbb{K}^{m\times n}$ of $m \times n$ matrices and of $S = \mathrm{Sym}(F \otimes G)$ as the ring of polynomial functions on this space. S is graded by degree, with the space of linear forms $F \otimes G$ sitting in degree 1. The *Cauchy formula* [Weyman 2003, Corollary 2.3.3]

$$S = \bigoplus_{\underline{x}=(x_1\geq\cdots\geq x_n\geq 0)} S_{\underline{x}}F \otimes S_{\underline{x}}G \tag{1-1}$$

describes the decomposition of S into a sum of irreducible $\mathrm{GL}(F) \times \mathrm{GL}(G)$-representations, indexed by partitions $\underline{x}$ with at most n parts ($S_{\underline{x}}$ denotes the *Schur functor* associated to $\underline{x}$). This decomposition respects the grading, the term corresponding to $\underline{x}$ being of degree $|\underline{x}| = x_1 + \cdots + x_n$. We denote by $I_{\underline{x}}$ the ideal generated by $S_{\underline{x}}F \otimes S_{\underline{x}}G$. If we write (1^p) for the partition $\underline{x}$ with $x_1 = \cdots = x_p = 1$ and $x_i = 0$ for $i > p$, then $I_{(1^p)}$ is just another notation for the ideal I_p of $p \times p$ minors. Our first result gives an explicit formula for the regularity of the ideals $I_{\underline{x}}$:

Theorem 5.1 (regularity of equivariant ideals). *For a partition $\underline{x}$ with at most n parts, letting $x_{n+1} = -1$, we have the following formula for the regularity of the ideal $I_{\underline{x}}$:*

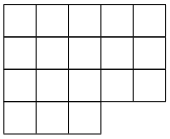
$$\mathrm{reg}(I_{\underline{x}}) = \max_{\substack{p=1,\ldots,n\\ x_p > x_{p+1}}} (n \cdot x_p + (p-2)\cdot(n-p)).$$

In particular, the only ideals $I_{\underline{x}}$ which have a linear resolution are those for which $x_1 = \cdots = x_n$ (i.e., powers $I_n^{x_1}$ of the ideal I_n of maximal minors) or $x_1 - 1 = x_2 = \cdots = x_n$ (i.e., $I_n^{x_1-1} \cdot I_1$).

The minimal free resolutions of the powers of I_n have been computed in [Akin et al. 1981, Theorem 5.4]. Together with the fact that $I \cdot \mathfrak{m}$ has a linear resolution whenever I has a linear resolution and $\mathfrak{m}$ is the maximal homogeneous ideal, this implies that the ideals $I_{\underline{x}}$ have a linear resolution when $x_2 = \cdots = x_n = x_1$ (or $x_1 - 1$). The fact that no other $I_{\underline{x}}$ has a linear resolution is, to the best of our knowledge, new.

The theorem on the regularity of equivariant ideals is a consequence of the explicit description of the modules $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$ that we obtain in Theorem 4.3. This description is somewhat involved, so we avoid stating it for the moment. A key point is that the modules $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$ *grow* as we append new columns to the *end* of the partition $\underline{x}$. More precisely, we can identify a partition $\underline{x}$ with its pictorial realization as a *Young diagram* consisting of left-justified rows of boxes,

with x_i boxes in the i-th row; for example, $\underline{x} = (5, 5, 5, 3)$ corresponds to



and adding two columns of size 2 and three columns of size 1 to the end of $\underline{x}$ yields $\underline{y} = (10, 7, 5, 3)$.

Theorem 4.2 (the growth of Ext modules). *Let $d \geq 0$ and consider partitions $\underline{x}$, $\underline{y}$, where $\underline{x}$ consists of the first d columns of $\underline{y}$; i.e., $x_i = \min(y_i, d)$ for all $i = 1, \ldots, n$. The natural quotient map $S/I_{\underline{y}} \twoheadrightarrow S/I_{\underline{x}}$ induces injective maps*

$$\mathrm{Ext}^i_S(S/I_{\underline{x}}, S) \hookrightarrow \mathrm{Ext}^i_S(S/I_{\underline{y}}, S)$$

for all $i = 0, 1, \ldots, m \cdot n$.

We warn the reader that the naive generalization of the statement above fails: if $\underline{y}$ is a partition containing $\underline{x}$ (i.e., $y_i \geq x_i$ for all i), then it is not always the case that the induced maps $\mathrm{Ext}^i_S(S/I_{\underline{x}}, S) \to \mathrm{Ext}^i_S(S/I_{\underline{y}}, S)$ are injective. In fact, a general partition $\underline{x}$ has the property that most modules $\mathrm{Ext}^i_S(S/I_{\underline{x}}, S)$ are nonzero, but it is always contained in some partition $\underline{y}$ with $y_1 = \cdots = y_n$; for such a $\underline{y}$, all but n of the modules $\mathrm{Ext}^i_S(S/I_{\underline{y}}, S)$ will vanish.

We next give the explicit description of $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$, which requires some notation. We write $\mathfrak{R}$ for the representation ring of the group $\mathrm{GL}(F) \times \mathrm{GL}(G)$. Given a $\mathbb{Z}$-graded S-module $M = \bigoplus_{i \in \mathbb{Z}} M_i$ admitting an action of $\mathrm{GL}(F) \times \mathrm{GL}(G)$ compatible with the natural one on S, we define its *character* $\chi_M(z)$ to be the element in the Laurent power series ring $\mathfrak{R}((z))$ given by

$$\chi_M(z) = \sum_{i \in \mathbb{Z}} [M_i] \cdot z^i,$$

where $[M_i]$ denotes the class in $\mathfrak{R}$ of the $\mathrm{GL}(F) \times \mathrm{GL}(G)$-representation M_i. We will often work with doubly graded modules M_i^j, where the second grading (in j) is a cohomological one and $M_\bullet^j \neq 0$ for only finitely many values of j; for us they will be either Ext modules or local cohomology modules. We define the character of such an M to be the element $\chi_M(z, w) \in \mathfrak{R}((z))[w^{\pm 1}]$ given by

$$\chi_M(z, w) = \sum_{i,j \in \mathbb{Z}} [M_i^j] \cdot z^i \cdot w^j.$$

We will refer to an r-tuple $\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathbb{Z}^r$ (for $r = m$ or n) as a *weight*. We say that λ is dominant if $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$, and denote by $\mathbb{Z}^r_{\mathrm{dom}}$ the set of dominant weights. Note that a partition is just a dominant weight with nonnegative entries. We will usually use the notation $\underline{x}$, $\underline{y}$, $\underline{z}$, etc. to refer to partitions indexing

the subrepresentations of S, and λ, μ, etc. to denote the weights describing the characters of other equivariant modules (Ext modules or local cohomology modules).

For $\lambda \in \mathbb{Z}^n_{\mathrm{dom}}$ and $0 \le s \le n$, we define

$$\lambda(s) = \big(\lambda_1, \dots, \lambda_s, \underbrace{s-n, \dots, s-n}_{m-n}, \lambda_{s+1} + (m-n), \dots, \lambda_n + (m-n)\big) \in \mathbb{Z}^m. \quad (1\text{-}2)$$

(Note that in [Raicu et al. 2014] this was called $\lambda(n-s)$.)

Theorem 4.3 (the characters of Ext Modules). *With the above notation, the character of the doubly graded module* $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$ *is given by*

$$\chi_{\mathrm{Ext}^\bullet_S(S/I_{\underline{x}},S)}(z,w) = \sum_{\substack{1\le p\le n \\ 0\le s\le t_1\le\cdots\le t_{n-p}\le p-1 \\ \lambda\in W'(\underline{x},p;\underline{t},s)}} [S_{\lambda(s)}F \otimes S_\lambda G] \cdot z^{|\lambda|} \cdot w^{m\cdot n+1-p^2-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-p} t_j)},$$

where $W'(\underline{x}, p; \underline{t}, s)$ *is the set of dominant weights* $\lambda \in \mathbb{Z}^n$ *satisfying*

$$\begin{cases} \lambda_n \ge p - x_p - m, \\ \lambda_{t_j+j} \le t_j - x_{n+1-j} - m \quad \text{for } j = 1, \dots, n-p, \\ \lambda_s \ge s-n \text{ and } \lambda_{s+1} \le s-m. \end{cases}$$

Our proof of this theorem starts with the observation in [de Concini et al. 1980] that even though the algebraic set defined by $I_{\underline{x}}$ is somewhat simple (it is the set of matrices of rank smaller than the number of nonzero parts of $\underline{x}$), its scheme-theoretic structure is more complicated: it is generally nonreduced, and has embedded components supported on I_p for each size p of some column of $\underline{x}$. Our approach is then to filter $S/I_{\underline{x}}$ with subquotients $J_{\underline{z},p}$ (defined in Section 2B) whose scheme-theoretic support is the (reduced) space of matrices of rank at most p, which are therefore less singular and easier to resolve. In fact, each $J_{\underline{z},p}$ is the push-forward of a locally free sheaf on some product of flag varieties, which allows us to compute $\mathrm{Ext}^\bullet_S(J_{\underline{z},p}, S)$ via duality theory. Solving the extension problem to deduce the formulas for $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$ turns out to be then trivial, due to the restrictions imposed by the equivariant structure of the modules.

We end this introduction with our main theorem on local cohomology modules, whose statement needs some more notation. For $0 \le s \le n$, we define (with the convention $\lambda_0 = \infty$, $\lambda_{n+1} = -\infty$)

$$h_s(z) = \sum_{\substack{\lambda\in\mathbb{Z}^n_{\mathrm{dom}} \\ \lambda_s\ge s-n \\ \lambda_{s+1}\le s-m}} [S_{\lambda(s)}F \otimes S_\lambda G] \cdot z^{|\lambda|}, \quad (1\text{-}3)$$

so that $h_n(z)$ is just the character of S. The other $h_s(z)$'s are characters of local cohomology modules with support in I_n (in the case when $m > n$). More precisely, for $p = 1, \ldots, n$ we write $H_p(z, w)$ for the character of the doubly graded module $H^\bullet_{I_p}(S)$. In [Raicu et al. 2014] we proved that for $m > n$

$$H_n(z, w) = \sum_{s=0}^{n-1} h_s(z) \cdot w^{(n-s)\cdot(m-n)+1},$$

and it is easy to see that the same formula holds for $m = n$ (in this case, the only nonzero local cohomology module is $H^1_{I_n}(S) = S_{\det}/S$, where det denotes the determinant of the generic $n \times n$ matrix, and $S_{\det}$ is the localization of S at det).

We write $p(a, b; c)$ for the number of partitions of c contained in an $a \times b$ rectangle, and define the *Gauss polynomial* $\binom{a+b}{b}(w)$ to be the generating function for the sequence $p(a, b; c)_{c\geq 0}$:

$$\binom{a+b}{a}(w) = \sum_{c\geq 0} p(a, b; c) \cdot w^c = \sum_{b\geq t_1\geq t_2\geq\cdots\geq t_a\geq 0} w^{t_1+\cdots+t_a}. \tag{1-4}$$

Gauss polynomials have previously appeared in [Akin and Weyman 2007] in connection to the closely related problem of understanding the minimal free resolutions of the ideals $I_{(p^d)}$.

Theorem 6.1 (local cohomology with support in generic determinantal ideals). *With the above notation, we have, for each* $p = 1, \ldots, n$,

$$H_p(z, w) = \sum_{s=0}^{p-1} h_s(z) \cdot w^{(n-p+1)^2+(n-s)\cdot(m-n)} \cdot \binom{n-s-1}{p-s-1}(w^2).$$

The theorem implies that the maximal cohomological index for which $H^\bullet_{I_p}(S)$ is nonzero (the *cohomological dimension* of the ideal I_p) is obtained for $s = 0$ and is equal to

$$(n - p + 1)^2 + n \cdot (m - n) + (p - 1) \cdot (n - p) = m \cdot n - p^2 + 1.$$

This was first observed in [Bruns and Schwänzl 1990]. Using the fact that once we invert one of the entries of a generic $m \times n$ matrix, I_p becomes I_{p-1} for a generic $(m - 1) \times (n - 1)$ matrix, it follows easily from the above that

$$H^j_{I_p}(S) \neq 0 \quad \text{for } j = (m - s) \cdot (n - s) - (p - s)^2 + 1,\ s = 0, 1, \ldots, p - 1. \tag{1-5}$$

For maximal minors ($p = n$) this nonvanishing result is sharp, as explained in [Witt 2012]. Our next result, which is a direct consequence of Theorem 6.1, says that *many more* of the local cohomology modules $H^j_{I_p}(S)$ are nonzero when $p < n$, namely:

Theorem (nonvanishing of local cohomology with determinantal support). *If $p \leq n \leq m$ then $H^j_{I_p}(S) \neq 0$ precisely when*

$$j = (n-p+1)^2 + (n-s)\cdot(m-n) + 2\cdot k \quad \text{for } 0 \leq s \leq p-1,\ 0 \leq k \leq (p-s-1)\cdot(n-p).$$

The nonvanishing statement (1-5) *is obtained for $k = (p-s-1)\cdot(n-p)$.*

This result contrasts with the positive characteristic situation, where the only nonvanishing local cohomology module appears in degree $j = (m-p+1)\cdot(n-p+1)$ (see [Hochster and Eagon 1971, Corollary 4] or [Bruns and Vetter 1988, Corollary 5.18], where it is shown that I_p is perfect, and [Peskine and Szpiro 1973, Proposition 4.1], where a local cohomology vanishing result for perfect ideals in positive characteristic is proved). For determinantal ideals over arbitrary rings one can't expect such explicit results as Theorem 6.1; for the latest advances in this general context, the reader should consult [Lyubeznik et al. 2013] and the references therein.

Our paper is organized as follows: In Section 2 we give some representation-theoretic preliminaries: in Section 2A we fix some notation for Schur functors, weights and partitions; in Section 2B we recall from [de Concini et al. 1980] some properties of the ideals $I_{\underline{x}}$ and introduce certain associated subquotients $J_{\underline{x},p}$ that will play an important role in the sequel; in Section 2C we recall the definition of flag varieties and formulate some consequences of Bott's theorem in a form that will be useful to us; we also recall in Section 2D a method described in [Raicu et al. 2014] for computing extension groups for certain modules that arise as push-forwards of vector bundles with vanishing higher cohomology. In Section 3 we compute explicitly the characters of the modules $\mathrm{Ext}^\bullet_S(J_{\underline{x},p}, S)$, and in Section 4 we use this calculation to deduce the main result about the characters of the modules $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$ for all partitions $\underline{x}$. In Section 5 we derive the formulas for the regularity of the ideals $I_{\underline{x}}$, while in Section 6 we describe the characters of the local cohomology modules with support in determinantal varieties.

2. Preliminaries

2A. ***Representation theory*** [Fulton and Harris 1991; Weyman 2003, Chapter 2]. Throughout the paper, $\mathbb{K}$ will denote a field of characteristic 0. If W is a $\mathbb{K}$-vector space of dimension $\dim(W) = N$, a choice of basis determines an isomorphism between $\mathrm{GL}(W)$ and $\mathrm{GL}_N(\mathbb{K})$. We will refer to N-tuples $\lambda = (\lambda_1, \ldots, \lambda_N) \in \mathbb{Z}^N$ as *weights* of the corresponding maximal torus of diagonal matrices. We say that λ is a *dominant weight* if $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. Irreducible (rational) representations of $\mathrm{GL}(W)$ are in one-to-one correspondence with dominant weights λ. We denote by $S_\lambda W$ the irreducible representation associated to λ, often referred to as the *Schur functor*. We write (a^N) for the weight with all parts equal to a, and define

the *determinant* of W by $\det(W) = S_{(1^N)}W = \bigwedge^N W$. We have $S_\lambda W \otimes \det(W) = S_{\lambda+(1^N)}W$ and $S_\lambda W^* = S_{(-\lambda_N,\dots,-\lambda_1)}W$. We write $|\lambda|$ for the total size $\lambda_1+\cdots+\lambda_N$ of λ.

When $\underline{x}$ is a dominant weight with $x_N \geq 0$, we say that $\underline{x}$ is a *partition* of $r = |\underline{x}|$. Note that when we're dealing with partitions we often omit the trailing zeros, so $\underline{x} = (5, 2, 1)$ is the same as $\underline{x} = (5, 2, 1, 0, 0, 0)$. If $\underline{y}$ is another partition, we write $\underline{x} \subset \underline{y}$ to indicate that $x_i \leq y_i$ for all i.

2B. ***The ideals $I_{\underline{x}}$ and the subquotients $J_{\underline{x},p}$.*** Recall the Cauchy formula (1-1) and the definition of the ideals $I_{\underline{x}} \subset S = \mathrm{Sym}(F \otimes G)$ as the ideals generated by subrepresentations $S_{\underline{x}}F \otimes S_{\underline{x}}G$ of S. It is shown in [de Concini et al. 1980] that

$$I_{\underline{x}} = \bigoplus_{\underline{x}\subset\underline{y}} S_{\underline{y}}F \otimes S_{\underline{y}}G, \tag{2-1}$$

and in particular $I_{\underline{y}} \subset I_{\underline{x}}$ if and only if $\underline{x} \subset \underline{y}$. More generally, for arbitrary partitions $\underline{x}, \underline{y}$, we let $\underline{z} = \max(\underline{x}, \underline{y})$ be defined by $z_i = \max(x_i, y_i)$ for all i, and get

$$I_{\underline{x}} \cap I_{\underline{y}} = I_{\underline{z}}. \tag{2-2}$$

Even more generally, for any set T of partitions we let

$$I_T = \sum_{\underline{y}\in T} I_{\underline{y}} \tag{2-3}$$

and have

$$I_{\underline{x}} \cap I_T = \sum_{\underline{y}\in T} I_{\max(\underline{x},\underline{y})}. \tag{2-4}$$

For $p \in \{0, 1, \dots, n\}$ and $\underline{x}$ a partition, we write

$$\mathrm{Succ}(\underline{x}, p) = \{\underline{y} : \underline{x} \subset \underline{y}, \text{ and } y_i > x_i \text{ for some } i > p\}. \tag{2-5}$$

By the discussion above, $I_{\underline{y}} \subset I_{\underline{x}}$ for all $\underline{y} \in \mathrm{Succ}(\underline{x}, p)$. We define

$$J_{\underline{x},p} = I_{\underline{x}}/I_{\mathrm{Succ}(\underline{x},p)} \tag{2-6}$$

It follows from (2-1) that

$$J_{\underline{x},p} = \bigoplus_{\substack{\underline{x}\subset\underline{y} \\ y_i = x_i \text{ for all } i>p}} S_{\underline{y}}F \otimes S_{\underline{y}}G. \tag{2-7}$$

If $p = n$ then $J_{\underline{x},p} = I_{\underline{x}}$, while if $p = 0$ then $J_{\underline{x},0} = S_{\underline{x}}F \otimes S_{\underline{x}}G$, which as an S-module is annihilated by the maximal ideal of S. We have:

Lemma 2.1. *Fix an index $p \in \{0, 1, \dots, n-1\}$, and consider a partition $\underline{x}$ with $x_1 = \cdots = x_{p+1}$. Let*

$$Z = \{\underline{z} : z_1 = \cdots = z_{p+1} = x_1\}. \tag{2-8}$$

We have

$$I_{\mathrm{Succ}(\underline{x},p)} = \left(\sum_{\underline{z}\in Z,\ \underline{x}\subsetneq\underline{z}} I_{\underline{z}} \right) + I_{\max(\underline{x},(x_1+1)^{p+1})}. \tag{2-9}$$

Proof. "$\supset$": Consider $\underline{z} \in Z$, $\underline{x} \subsetneq \underline{z}$. We have $z_i > x_i$ for some i, and since $x_i = z_i$ for $i \le p+1$, we conclude that $z_i > x_i$ for some $i > p+1$; thus, $\underline{z} \in \mathrm{Succ}(\underline{x}, p)$. Writing $\underline{y} = \max(\underline{x}, (x_1+1)^{p+1})$, we have that $y_{p+1} > x_{p+1}$ and $\underline{y} \supset \underline{x}$, so $\underline{y} \in \mathrm{Succ}(\underline{x}, p)$, proving that the right side of (2-9) is contained in the left.

"$\subset$": Consider a partition $\underline{y} \in \mathrm{Succ}(\underline{x}, p)$. If $y_{p+1} > x_{p+1} = x_1$ then $\underline{y}$ contains $\max(\underline{x}, (x_1+1)^{p+1})$, so $I_{\underline{y}}$ is contained in the right side of (2-9). Otherwise $y_{p+1} = x_{p+1}$, so by possibly shrinking some of the first p rows of $\underline{y}$ (which would enlarge $I_{\underline{y}}$), we may assume that $\underline{y} \in Z$. Clearly $\underline{y} \supsetneq \underline{x}$, since $y_i > x_i$ for some $i > p+1$, so it follows again that $I_{\underline{y}}$ is contained in the right side of (2-9). □

The following result will be used in Section 4:

Lemma 2.2. *Fix an index $p \in \{0, 1, \dots, n-1\}$, and consider a partition $\underline{x}$ with $x_1 = \cdots = x_{p+1}$. For a nonnegative integer $d \ge 0$, let $\underline{y}$ be the partition defined by $y_i = x_i + d + 1$ for $i = 1, \dots, p+1$ and $y_i = x_i$ for $i > p+1$ ($\underline{y} = \max(\underline{x}, (x_1+d+1)^{p+1})$). The quotient $I_{\underline{x}}/I_{\underline{y}}$ admits a filtration with successive quotients $J_{\underline{z},p}$, where $\underline{z}$ runs over all partitions with*

$$\begin{cases} x_1 \le z_1 = \cdots = z_{p+1} \le x_1 + d, \\ z_i \ge x_i \quad \text{for } i > p+1. \end{cases}$$

Proof. By induction, it suffices to prove the result when $d = 0$. We consider Z as in (2-8) and define

$$\mathcal{I}(Z) = \{I_T : T \subset Z\}.$$

For $I \in \mathcal{I}(Z)$, we write

$$Z(I) = \{\underline{z} \in Z : I_{\underline{z}} \subset I\}.$$

Note that if $\underline{z}^0 \in Z(I)$ then

$$\text{if } \underline{z} \in Z \text{ and } \underline{z}^0 \subset \underline{z} \text{ then } \underline{z} \in Z(I). \tag{2-10}$$

We let $I_0 = I_{((x_1+1)^{p+1})}$ and prove by induction on $|Z(I)|$ that for $I \in \mathcal{I}(Z)$, the quotient $(I + I_0)/I_0$ has a filtration with successive quotients $J_{\underline{z},p}$, where $\underline{z}$ varies

over the set of elements of $Z(I)$. Once we do this, we can take $I = I_{\underline{x}}$ and observe that $I_{\underline{x}} \cap I_0 = I_{\underline{y}}$ (by (2-2)), which yields

$$(I + I_0)/I_0 \simeq I/(I \cap I_0) = I_{\underline{x}}/I_{\underline{y}},$$

concluding the proof of the lemma.

For the induction, assume first that $|Z(I)| = 1$, so that $I = I_{\underline{z}}$ with $z_1 = \cdots = z_n = x_1$. We have $(I_{\underline{z}} + I_0)/I_0 = J_{\underline{z},p}$ so the base case for the induction follows.

Suppose now that $|Z(I)| > 1$ and consider a *maximal* element $\underline{z}^0$ in $Z(I)$, i.e., a partition $\underline{z}^0$ with the property that $I_{\underline{z}^0} \not\subset I_{\underline{z}}$ for any $\underline{z} \in Z(I) \setminus \{\underline{z}^0\}$. Define

$$I' = I_{Z(I)\setminus\{\underline{z}^0\}},$$

and note that $|Z(I')| = |Z(I)| - 1$, $I = I' + I_{\underline{z}^0}$, and

$$(I + I_0)/(I' + I_0) \simeq J_{\underline{z}^0,p}, \tag{2-11}$$

which is proved as follows. The equality $I = I' + I_{\underline{z}^0}$ implies that the natural map

$$I_{\underline{z}^0} \to (I + I_0)/(I' + I_0)$$

is surjective. Its kernel is

$$\begin{aligned} I_{\underline{z}^0} \cap (I' + I_0) &\overset{(2\text{-}4)}{=} \left(\sum_{\underline{z} \in Z(I)\setminus\{\underline{z}^0\}} I_{\max(\underline{z}^0,\underline{z})} \right) + I_{\max(\underline{z}^0,(x_1+1)^{p+1})} \\ &\overset{(2\text{-}10)}{=} \left(\sum_{\underline{z} \in Z,\, \underline{z}^0 \subsetneq \underline{z}} I_{\underline{z}} \right) + I_{\max(\underline{z}^0,(x_1+1)^{p+1})} \overset{(2\text{-}9)}{=} I_{\mathrm{Succ}(\underline{z}^0,p)}, \end{aligned}$$

from which (2-11) follows. Since by induction $(I' + I_0)/I_0$ has a filtration with successive quotients $J_{\underline{z},p}$ for $\underline{z} \in Z(I')$, we get the corresponding statement for $(I + I_0)/I_0$, finishing the induction step. □

2C. ***Partial flag varieties and Bott's theorem*** [Weyman 2003, Chapter 4]. Consider a $\mathbb{K}$-vector space V with $\dim(V) = d$ and positive integers $q \le n \le d$. We denote by $\mathrm{Flag}([q,n]; V)$ the variety of partial flags

$$V_\bullet : \quad V \twoheadrightarrow V_n \twoheadrightarrow V_{n-1} \twoheadrightarrow \cdots \twoheadrightarrow V_q \twoheadrightarrow 0,$$

where V_p is a p-dimensional quotient of V for each $p = q, q+1, \ldots, n$. For p in $[q,n]$ we write $\mathcal{Q}_p(V)$ for the tautological rank-p quotient bundle on $\mathrm{Flag}([q,n]; V)$ whose fiber over a point $V_\bullet \in \mathrm{Flag}([q,n]; V)$ is V_p. For each p there is a natural surjection of vector bundles

$$V \otimes \mathcal{O}_{\mathrm{Flag}([q,n];V)} \twoheadrightarrow \mathcal{Q}_p(V). \tag{2-12}$$

Note that for $q=n$, $\mathrm{Flag}([q,n];V)=\mathbb{G}(n,V)$ is the Grassmannian of n-dimensional quotients of V.

We consider the natural projection maps

$$\pi^{(q)}:\mathrm{Flag}([q,n];V)\to\mathrm{Flag}([q+1,n];V), \tag{2-13}$$

defined by forgetting V_q from the flag $V_\bullet$. For $q\leq n-1$, this map identifies $\mathrm{Flag}([q,n];V)$ with the projective bundle $\mathbb{P}_{\mathrm{Flag}([q+1,n];V)}(\mathcal{Q}_{p+1}(V))$, which comes with a tautological surjection

$$\mathcal{Q}_{p+1}(V)\twoheadrightarrow\mathcal{Q}_p(V).$$

For $q=n$ we make the convention $\mathrm{Flag}([q+1,n];V)=\mathrm{Spec}(\mathbb{K})$, so $\pi^{(n)}$ is just the structure map of $\mathbb{G}(n,V)$. With the usual notation $R^\bullet\pi^{(q)}_*$ for the derived push-forward, we obtain using [Weyman 2003, Corollary 4.1.9] the following:

Theorem 2.3. (a) *Suppose that $q\leq n-1$, and consider a dominant weight $\mu\in\mathbb{Z}^q$. For $q<p\leq n$,*

$$R^j\pi^{(q)}_*(S_\mu\mathcal{Q}_p(V))=\begin{cases}S_\mu\mathcal{Q}_p(V) & \text{if } j=0,\\ 0 & \text{otherwise.}\end{cases}$$

If $\mu_{q-t}+t=-1$ for some $t=0,\dots,q-1$, then

$$R^j\pi^{(q)}_*(S_\mu\mathcal{Q}_q(V))=0\quad\text{for all } j.$$

Otherwise (with the convention $\mu_0=\infty$, $\mu_{q+1}=-\infty$), consider the unique index $0\leq t\leq q$ such that

$$\mu_{q-t+1}+t+1\leq 0\leq\mu_{q-t}+t.$$

Letting

$$\tilde{\mu}=(\mu_1,\dots,\mu_{q-t},-t,\mu_{q-t+1}+1,\dots,\mu_q+1),$$

we have

$$R^j\pi^{(q)}_*(S_\mu\mathcal{Q}_q(V))=\begin{cases}S_{\tilde{\mu}}\mathcal{Q}_{q+1}(V) & \text{if } j=t,\\ 0 & \text{otherwise.}\end{cases}$$

(b) *Consider a dominant weight $\mu\in\mathbb{Z}^n$. If $n-d\leq\mu_{n-s}+s\leq-1$ for some $s=0,\dots,n-1$, then*

$$R^j\pi^{(n)}_*(S_\mu\mathcal{Q}_n(V))=0\quad\text{for all } j.$$

Otherwise (with the convention $\mu_0=\infty$, $\mu_{n+1}=-\infty$), consider the unique index $0\leq s\leq n$ such that

$$\mu_{n-s}\geq -s\quad\text{and}\quad\mu_{n-s+1}\leq -s-d+n.$$

Letting

$$\tilde{\mu} = \big(\mu_1, \dots, \mu_{n-s}, \underbrace{-s, \dots, -s}_{d-n}, \mu_{n-s+1} + (d-n), \dots, \mu_n + (d-n)\big) \in \mathbb{Z}^d,$$

(*compare to* (1-2)), *we have*

$$R^j \pi_*^{(n)}(S_\mu \mathcal{Q}_n(V)) = \begin{cases} S_{\tilde{\mu}} V & \text{if } j = s \cdot (d-n), \\ 0 & \text{otherwise.} \end{cases}$$

2D. ***Computing* Ext *modules via duality.*** In this section we recall [Raicu et al. 2014, Theorem 3.1] as a tool to compute $\mathrm{Ext}_S^\bullet(M, S)$ when M comes as the push-forward of certain vector bundles with vanishing higher cohomology. More precisely, we have:

Theorem 2.4. *Let X be a projective variety, and let W be a finite-dimensional $\mathbb{K}$-vector space. Suppose*

$$W \otimes \mathcal{O}_X \twoheadrightarrow \eta$$

is a surjective map, where η is locally free, and let $k = \dim(W) - \mathrm{rank}(\eta)$. Consider a locally free sheaf $\mathcal{V}$ on X, and define

$$\mathcal{M}(\mathcal{V}) = \mathcal{V} \otimes \mathrm{Sym}(\eta), \quad \mathcal{M}^*(\mathcal{V}) = \mathcal{V} \otimes \det(W) \otimes \det(\eta^*) \otimes \mathrm{Sym}(\eta^*).$$

Giving $\mathcal{V}$ internal degree v, and η and W degree 1, we think of $\mathcal{M}(\mathcal{V})$ and $\mathcal{M}^*(\mathcal{V})$ as graded sheaves, with

$$\mathcal{M}(\mathcal{V})_{i+v} = \mathcal{V} \otimes \mathrm{Sym}^i(\eta), \quad \mathcal{M}^*(\mathcal{V})_{i+v} = \mathcal{V} \otimes \det(W) \otimes \det(\eta^*) \otimes \mathrm{Sym}^{-i+k}(\eta^*).$$

Suppose that $H^j(X, \mathcal{M}(\mathcal{V})) = 0$ for $j > 0$, and let

$$M(\mathcal{V}) = H^0(X, \mathcal{M}(\mathcal{V})).$$

We have for each $j \geq 0$ a graded isomorphism

$$\mathrm{Ext}_S^j(M(\mathcal{V}), S) = H^{k-j}(X, \mathcal{M}^*(\mathcal{V}))^*, \tag{2-14}$$

where $(-)^*$ stands for the graded dual.

3. Ext modules for the subquotients $J_{\underline{x},p}$

The goal of this section is to compute explicitly the character of $\mathrm{Ext}_S^\bullet(J_{\underline{x},p}, S)$ for all p and all partitions $\underline{x}$ with $x_1 = \cdots = x_p$, where $J_{\underline{x},p}$ is defined as in (2-6). We will achieve this by realizing $J_{\underline{x},p}$ as the global sections of a vector bundle with vanishing higher cohomology on a certain product of flag varieties, and then using duality (Theorem 2.4) and Bott's theorem (Theorem 2.3).

Consider as before vector spaces F, G, with $\dim(F) = m$, $\dim(G) = n$, $m \geq n$. For $q = 1, \ldots, n$, we consider the projective varieties

$$X^{(q)} = \mathrm{Flag}([q, n]; F) \times \mathrm{Flag}([q, n]; G), \quad X = X^{(\infty)} = \mathrm{Spec}\, \mathbb{K},$$

and the locally free sheaves (see Section 2C)

$$\eta^{(p)} = \mathcal{Q}_p(F) \otimes \mathcal{Q}_p(G), \ p = 1, \ldots, n, \quad \eta = \eta^{(\infty)} = F \otimes G.$$

Note that $\eta^{(p)}$ can be thought of as a sheaf on $X^{(q)}$ whenever $p \geq q$. We consider for $q \leq n-1$ (resp. $q = n$) the natural maps $\pi^{(q)} : X^{(q)} \to X^{(q+1)}$ (resp. $\pi^{(n)} : X^{(n)} \to X$) induced from (2-13). We define

$$S^{(q)} = \mathrm{Sym}\, \eta^{(q)}$$

as relative versions of the polynomial ring $S = S^{(\infty)} = \mathrm{Sym}(F \otimes G)$. We will always work implicitly with quasicoherent sheaves on the affine bundles

$$Y^{(q)} = \mathbb{A}_{X^{(q)}}(\eta^{(q)}) = \underline{\mathrm{Spec}}_{X^{(q)}}(S^{(q)}),$$

which we identify with $S^{(q)}$-modules on $X^{(q)}$ as in [Hartshorne 1977, Exercise II.5.17]. The Cauchy formula (1-1) becomes in the relative setting

$$S^{(q)} = \bigoplus_{\underline{x} = (x_1 \geq \cdots \geq x_q \geq 0)} S_{\underline{x}} \mathcal{Q}_q(F) \otimes S_{\underline{x}} \mathcal{Q}_q(G), \tag{3-1}$$

and we can define the ideals $I^{(q)}_{\underline{x}} \subset S^{(q)}$ and subquotients $J^{(q)}_{\underline{x},p}$ for $0 \leq p \leq q$ analogously to (2-1) and (2-6). For $1 \leq p \leq q$, we write $I^{(q)}_p$ for $I^{(q)}_{(1^p)}$, the ideal of $p \times p$ minors in $S^{(q)}$. We define the line bundle

$$\det^{(q)} = \det(\mathcal{Q}_q(F)) \otimes \det(\mathcal{Q}_q(G)), \tag{3-2}$$

and note that the ideal $I^{(q)}_q$ is generated by $\det^{(q)}$. It follows easily from (3-1) and Theorem 2.3 that

$$R^j \pi^{(q)}_* (S^{(q)}) = \begin{cases} S^{(q+1)}/I^{(q+1)}_{q+1} & \text{if } j = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{3-3a}$$

and, for $p > q$,

$$R^j \pi^{(q)}_* (S^{(p)}) = \begin{cases} S^{(p)} & \text{if } j = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3-3b}$$

Lemma 3.1. (a) *For a partition $\underline{x} = (x_1 \geq \cdots \geq x_q)$, there exist natural identifications*

$$\det^{(q)} \otimes I^{(q)}_{\underline{x}} = I^{(q)}_{\underline{x}+(1^q)}, \tag{3-4}$$

and

$$\det^{(q)} \otimes J^{(q)}_{\underline{x},p} = J^{(q)}_{\underline{x}+(1^q),p} \quad \textit{for } 0 \leq p \leq q. \tag{3-5}$$

(b) *For a partition* $\underline{x} = (x_1 \geq \cdots \geq x_q)$, *we have*

$$R^j \pi_*^{(q)} I_{\underline{x}}^{(q)} = \begin{cases} (I_{\underline{x}}^{(q+1)} + I_{q+1}^{(q+1)})/I_{q+1}^{(q+1)} & \text{if } j = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3-6}$$

(c) *For a partition* $\underline{x} = (x_1 \geq \cdots \geq x_q)$ *and* $0 \leq p \leq q$, *we have*

$$R^j \pi_*^{(q)} J_{\underline{x},p}^{(q)} = \begin{cases} J_{\underline{x},p}^{(q+1)} & \text{if } j = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3-7}$$

Proof. (a) The multiplication map $\det^{(q)} \otimes S^{(q)} \to S^{(q)}$ is injective: if we think of $S^{(q)}$ as locally the ring of polynomial functions on $q \times q$ matrices, then $\det^{(q)}$ is the determinant of the generic $q \times q$ matrix. It follows that $\det^{(q)} \otimes I_{\underline{x}}^{(q)} = \det^{(q)} \cdot I_{\underline{x}}^{(q)}$ is in fact an ideal in $S^{(q)}$. Equation (3-4) then follows from the fact that multiplying by the determinant corresponds to adding a column of maximal size to the Young diagram (a special case of Pieri's rule). In fact, the same argument shows that for any set of partitions Z

$$\det^{(q)} \otimes \left(\sum_{\underline{z} \in Z} I_{\underline{z}}^{(q)} \right) = \sum_{\underline{z} \in Z} I_{\underline{z}+(1^q)}^{(q)}.$$

Given the definition of $J_{\underline{x},p}^{(q)}$ as the analogue of (2-6), (3-5) follows by taking $Z = \mathrm{Succ}^{(q)}(\underline{x}, p)$ (the analogue of (2-5)) in the formula above, and using (3-4) and the exactness of tensoring with $\det^{(q)}$.

Part (b) follows from (3-3), while (c) follows from the fact that if $\underline{x} = (x_1, \ldots, x_q)$ and $0 \leq p \leq q$, then

$$\mathrm{Succ}^{(q+1)}(\underline{x}, p) = \mathrm{Succ}^{(q)}(\underline{x}, p) \cup \{\underline{z} : \underline{z} \supset \underline{x},\ z_{p+1} \geq 1\}. \qquad \square$$

For each partition $\underline{x} = (x_1 = \cdots = x_p \geq x_{p+1} \geq \cdots \geq x_n \geq x_{n+1} = 0)$, we define the locally free sheaf $\mathcal{M}_{\underline{x},p}$ on $X^{(p)}$ by

$$\mathcal{M}_{\underline{x},p} = \left(\bigotimes_{q=p}^{n} (\det^{(q)})^{\otimes (x_q - x_{q+1})} \right) \otimes S^{(p)}. \tag{3-8}$$

Lemma 3.2. *With the notation above, we have*

$$H^j(X^{(p)}, \mathcal{M}_{\underline{x},p}) = \begin{cases} J_{\underline{x},p} & \text{if } j = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Note that $S^{(p)} = J_{\underline{0},p}^{(p)}$, so using (3-4) we get

$$\mathcal{M}_{\underline{x},p} = \left(\bigotimes_{q=p+1}^{n} (\det^{(q)})^{\otimes (x_q - x_{q+1})} \right) \otimes J_{((x_p - x_{p+1})^p),p}^{(p)}.$$

It follows that

$$R\pi_*^{(p)}\mathcal{M}_{\underline{x},p} = \pi_*^{(p)}\mathcal{M}_{\underline{x},p} \overset{(3\text{-}7)}{=} \left(\bigotimes_{q=p+1}^{n} (\det^{(q)})^{\otimes(x_q - x_{q+1})}\right) \otimes J^{(p+1)}_{((x_p - x_{p+1})^p),p}$$
$$\overset{(3\text{-}4)}{=} \left(\bigotimes_{q=p+2}^{n} (\det^{(q)})^{\otimes(x_q - x_{q+1})}\right) \otimes J^{(p+1)}_{((x_p - x_{p+2})^p, x_{p+1}-x_{p+2}),p}.$$

Applying $R\pi_*^{(p+1)}, R\pi_*^{(p+2)}, \ldots, R\pi_*^{(n)}$ iteratively, and using (3-7) and (3-4) as above, we obtain

$$R\pi_*\mathcal{M}_{\underline{x},p} = \pi_*\mathcal{M}_{\underline{x},p} = J_{(x_p^p, x_{p+1},\ldots,x_n),p} \overset{(x_1=\cdots=x_p)}{=} J_{\underline{x},p},$$

where $\pi = \pi^{(n)} \circ \cdots \circ \pi^{(p)}$ is the structure map $X^{(p)} \to \operatorname{Spec} \mathbb{K}$, concluding the proof of the lemma. □

We are now ready to prove the main result of this section:

Theorem 3.3. *The character of the doubly graded module* $\operatorname{Ext}_S^\bullet(J_{\underline{x},p}, S)$ *is given by*

$$\chi_{\operatorname{Ext}_S^\bullet(J_{\underline{x},p},S)}(z,w) = \sum_{\substack{0\le s\le t_1\le\cdots\le t_{n-p}\le p \\ \lambda\in W(\underline{x},p;\underline{t},s)}} [S_{\lambda(s)}F \otimes S_\lambda G]\cdot z^{|\lambda|}\cdot w^{m\cdot n - p^2 - s\cdot(m-n) - 2\cdot(\sum_{j=1}^{n-p} t_j)}, \quad (3\text{-}9)$$

where $W(\underline{x}, p; \underline{t}, s)$ *is the set of dominant weights* $\lambda \in \mathbb{Z}^n$ *with the properties*

$$\begin{cases} \lambda_n \ge p - x_p - m, & (3\text{-}10a)\\ \lambda_{t_j+j} = t_j - x_{n+1-j} - m \quad \textit{for } j = 1,\ldots,n-p, & (3\text{-}10b)\\ \lambda_s \ge s - n \quad \textit{and} \quad \lambda_{s+1} \le s - m. & (3\text{-}10c) \end{cases}$$

Remark 3.4. If we take $p = n$ and $x_1 = \cdots = x_n = d$ in the above theorem, we recover [Raicu et al. 2014, Theorem 4.3]. The character of $J_{\underline{x},n} = I_{\underline{x}} = I_n^d$ is

$$\chi_{\operatorname{Ext}_S^\bullet(J_{\underline{x},n},S)}(z,w) = \sum_{\substack{0\le s\le n \\ \lambda_n\ge n-d-m \\ \lambda_s\ge s-n \\ \lambda_{s+1}\le s-m}} [S_{\lambda(s)}F \otimes S_\lambda G]\cdot z^{|\lambda|}\cdot w^{(n-s)\cdot(m-n)}.$$

When $p = 0$, since $J_{\underline{x},0} = S_{\underline{x}}F \otimes S_{\underline{x}}G$ is just a vector space the only nonvanishing Ext module is

$$\operatorname{Ext}_S^{mn}(J_{\underline{x},0}, S) = \big(S_{\underline{x}}F \otimes S_{\underline{x}}G \otimes \det(F\otimes G)\big)^*.$$

Proof of Theorem 3.3. We apply Theorem 2.4 with

$$X = X^{(p)}, \quad \eta = \eta^{(p)}, \quad W = F \otimes G, \quad \mathcal{V} = \bigotimes_{q=p}^{n} (\det^{(q)})^{\otimes (x_q - x_{q+1})},$$

so that $\mathcal{M}(\mathcal{V}) = \mathcal{M}_{\underline{x},p}$ (see (3-8)). Lemma 3.2 ensures that the hypotheses of the duality theorem hold, and $M(\mathcal{V}) = J_{\underline{x},p}$. We have $\operatorname{rank}(\eta^{(p)}) = p^2$, $\dim(W) = m \cdot n$, so $k = m \cdot n - p^2$. We give $\mathcal{V}$ internal degree $v = |\underline{x}|$, and get

$$\begin{aligned}\operatorname{Ext}_S^j(J_{\underline{x},p}, S)_{r-|\underline{x}|} &= H^{m\cdot n - p^2 - j}\Bigg(X^{(p)}, \bigotimes_{q=p}^{n} (\det^{(q)})^{\otimes (x_q - x_{q+1})} \otimes \det(F \otimes G) \\ &\qquad \otimes \det(\eta^*) \otimes \operatorname{Sym}^{r+m\cdot n - p^2}(\eta^*)\Bigg)^*. \quad (3\text{-}11)\end{aligned}$$

Formula (3-9) now follows from a direct application of Theorem 2.3, which we sketch below.

Using Cauchy's formula and that $\det(\eta^*) = \det(\mathcal{Q}_p(F))^{-p} \otimes \det(\mathcal{Q}_p(G))^{-p}$, we get

$$\det(\eta^*) \otimes \operatorname{Sym}^{r+m\cdot n - p^2}(\eta^*) = \bigoplus_{\substack{\mu \in \mathbb{Z}^p_{\mathrm{dom}} \\ |\mu| = r + m\cdot n \\ \mu_1 \le -p}} S_\mu \mathcal{Q}_p(F) \otimes S_\mu \mathcal{Q}_p(G).$$

For each μ in the formula above, we have to first compute

$$R\pi_*\Bigg(\bigotimes_{q=p}^{n} (\det^{(q)})^{\otimes (x_q - x_{q+1})} \otimes S_\mu \mathcal{Q}_p(F) \otimes S_\mu \mathcal{Q}_p(G)\Bigg), \quad (3\text{-}12)$$

where $\pi = \pi^{(n)} \circ \cdots \circ \pi^{(p)} : X^{(p)} \to \operatorname{Spec} \mathbb{K}$ is the structure map, then tensor with $\det(F \otimes G)$ and dualize, in order to get the corresponding contribution to (3-11). If (3-12) is nonzero, then there exist uniquely determined dominant weights $\mu^{(q)}, \delta^{(q)} \in \mathbb{Z}^q$ for $q = p, \ldots, n$, and nonnegative integers t_{n-q}, $q = p, \ldots, n-1$, and s, such that $\mu^{(p)} = \mu$, and if for $q = p, \ldots, n$ we write

$$\mathcal{M}^{(q)} = S_{\mu^{(q)}} \mathcal{Q}_q(F) \otimes S_{\mu^{(q)}} \mathcal{Q}_q(G), \quad \mathcal{N}^{(q)} = S_{\delta^{(q)}} \mathcal{Q}_q(F) \otimes S_{\delta^{(q)}} \mathcal{Q}_q(G),$$

then

$$\mathcal{N}^{(q)} = \mathcal{M}^{(q)} \otimes (\det^{(q)})^{\otimes (x_q - x_{q+1})} \quad \text{for } q = p, \ldots, n, \quad (3\text{-}13)$$

$2 \cdot t_{n-q}$ is the unique integer j for which $R^j \pi_*^{(q)}(\mathcal{N}^{(q)}) \neq 0$, and

$$R^{2\cdot t_{n-q}} \pi_*^{(q)}(\mathcal{N}^{(q)}) = \mathcal{M}^{(q+1)} \quad \text{for } q = p, \ldots, n-1, \quad (3\text{-}14)$$

and finally, $s \cdot (m-n)$ is the unique integer j for which $R^j \pi_*^{(n)}(\mathcal{N}^{(n)}) \neq 0$.

The dominant weight $\delta^{(q)}$ is easy to determine; namely, we get from (3-13) that

$$\delta^{(q)} = \mu^{(q)} + ((x_q - x_{q+1})^q). \tag{3-15}$$

Assuming we know $\delta^{(q)}$, (3-14) determines t_{n-q} and $\mu^{(q)}$ according to (a) of Theorem 2.3: t_{n-q} is the unique integer t with the property

$$\delta^{(q)}_{q-t+1} + t + 1 \leq 0 \leq \delta^{(q)}_{q-t} + t, \tag{3-16}$$

and

$$\mu^{(q+1)} = \big(\delta^{(q)}_1, \ldots, \delta^{(q)}_{q-t_{n-q}}, -t_{n-q}, \delta^{(q)}_{q-t_{n-q}+1} + 1, \ldots, \delta^{(q)}_q + 1\big). \tag{3-17}$$

It follows from (3-17) and (3-15) that

$$\delta^{(q+1)}_{q+1-t_{n-q}} = -t_{n-q} + x_{q+1} - x_{q+2} \geq -t_{n-q},$$

so $t = t_{n-q}$ satisfies the right-hand inequality in (3-16) with q replaced by $(q+1)$, which forces $t_{n-(q+1)} \leq t_{n-q}$. It follows easily that

$$\delta^{(i)}_{q+1-t_{n-q}} = -t_{n-q} + x_{q+1} - x_{i+1} \quad \text{for } i = q+1, \ldots, n. \tag{3-18}$$

We have seen so far how to calculate $\mu^{(q)}, \delta^{(q)}$ for $q = p, \ldots, n$, and t_{n-q} for $q = p, \ldots, n-1$, so we're left with determining s. By Theorem 2.3(b), s is uniquely determined by the inequalities

$$\delta^{(n)}_{n-s} \geq -s \quad \text{and} \quad \delta^{(n)}_{n-s+1} \leq -s - m + n, \tag{3-19}$$

and moreover

$$R^{s\cdot(m-n)}\pi^{(n)}_*(\mathcal{N}^{(n)}) = S_{\tilde{\delta}}F \otimes S_\delta G, \tag{3-20}$$

where $\delta = \delta^{(n)}$ and

$$\tilde{\delta} = \big(\delta_1, \ldots, \delta_{n-s}, (-s)^{m-n}, \delta_{n-s+1} + (m-n), \ldots, \delta_n + (m-n)\big).$$

Since $\delta^{(n)}_{n-t_1} = -t_1 + x_n \geq -t_1$, it follows as before that $s \leq t_1$. Tensoring (3-20) with $\det(F \otimes G) = \det(F)^{\otimes n} \otimes \det(G)^{\otimes m}$ and dualizing, we obtain by putting everything together that there exist integers $0 \leq s \leq t_1 \leq \cdots \leq t_{n-p} \leq p$ such that

$$R^{s\cdot(m-n)+2\cdot\sum_{j=1}^{n-p} t_j}\pi_*\Big(\bigotimes_{q=p}^{n}(\det{}^{(q)})^{\otimes(x_q - x_{q+1})} \otimes \det(F\otimes G) \otimes S_\mu \mathcal{Q}_p(F) \otimes S_\mu \mathcal{Q}_p(G)\Big)^* = S_{\lambda(s)}F \otimes S_\lambda G,$$

where $\lambda(s)$ is defined as in (1-2) and

$$\lambda_i = -m - \delta_{n-i+1} \quad \text{for all } i = 1, \ldots, n. \tag{3-21}$$

We next check that $\lambda \in W(\underline{x}, p; \underline{t}, s)$. Since $\mu_1 \leq -p$, it follows from (3-15) and (3-17) that $\delta_1 \leq -p + x_p$, so $\lambda_n = -\delta_1 - m \geq p - x_p - m$; i.e., (3-10a) holds. Letting $i = n$ in (3-18) we get $\delta_{q+1-t_{n-q}} = -t_{n-q} + x_{q+1}$, so $\lambda_{n-q+t_{n-q}} = t_{n-q} - x_{q+1} - m$; i.e., (3-10b) holds. Finally, (3-10c) follows from (3-19).

We conclude from the discussion above that (3-9) holds, after possibly replacing $W(\underline{x}, p; \underline{t}, s)$ by a smaller set. To see that all weights $\lambda \in W(\underline{x}, p; \underline{t}, s)$ in fact appear, one has to reverse the steps above in order to show that each λ can be reached from a certain weight μ. We give the formula for μ, and leave the details to the interested reader. We first define $\delta \in \mathbb{Z}^n_{\text{dom}}$ by reversing (3-21): $\delta_i = -m - \lambda_{n+1-i}$. Letting $t_{n-p+1} = p$ and $t_0 = 0$, for each $i = 0, \ldots, n-p$ and $j = 1, \ldots, t_{i+1} - t_i$ we let

$$\mu_{p-t_{i+1}+j} = \delta_{n-i-t_{i+1}+j} + x_{n-i} + (n - p - i). \qquad \square$$

Corollary 3.5. *Fix an index $p \in \{0, 1, \ldots, n\}$. Suppose that M is an S-module with a compatible $\mathrm{GL}(F) \times \mathrm{GL}(G)$ action, admitting a finite filtration with successive quotients isomorphic to $J_{\underline{x}^j, p}$ for $j = 1, \ldots, r$, where each $\underline{x}^j$ is a partition satisfying $x^j_1 = x^j_2 = \cdots = x^j_p$. We have a decomposition as $\mathrm{GL}(F) \times \mathrm{GL}(G)$-representations*

$$\mathrm{Ext}^i_S(M, S) = \bigoplus_{j=1}^{r} \mathrm{Ext}^i_S(J_{\underline{x}^j, p}, S) \tag{3-22}$$

for each $i = 0, 1, \ldots, m \cdot n$. Equivalently, if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{3-23}$$

is a $\mathrm{GL}(F) \times \mathrm{GL}(G)$-equivariant short exact sequence of S-modules admitting filtrations as above, then for each $i = 0, 1, \ldots, m \cdot n$, the induced sequence

$$0 \longrightarrow \mathrm{Ext}^i_S(C, S) \longrightarrow \mathrm{Ext}^i_S(B, S) \longrightarrow \mathrm{Ext}^i_S(A, S) \longrightarrow 0 \tag{3-24}$$

is exact.

Proof. Suppose that the conclusion of the corollary fails, and consider modules A, B, C sitting in an exact sequence (3-23) such that (3-22) holds for A and C but fails for B. In particular, not all sequences (3-24) are exact, so there exist an index i and a nontrivial connecting homomorphism

$$\mathrm{Ext}^i_S(A, S) \xrightarrow{\delta} \mathrm{Ext}^{i+1}_S(C, S).$$

It follows that some irreducible representation of $\mathrm{GL}(F) \times \mathrm{GL}(G)$ appears in both $\mathrm{Ext}^i_S(A, S)$ and $\mathrm{Ext}^{i+1}_S(C, S)$. This is clearly impossible when $m = n$, because from (3-22) and (3-9) it follows that the cohomological degrees j for which $\mathrm{Ext}^j_S(A, S)$

and $\mathrm{Ext}^j_S(C, S)$ are nonzero satisfy

$$j \equiv m \cdot n - p^2 \pmod 2.$$

When $m > n$, a similar argument applies: if $[S_{\lambda(s)}F \otimes S_\lambda G] = [S_{\mu(t)}F \otimes S_\mu G]$ (with λ, μ, $\lambda(s)$ and $\mu(t)$ dominant), then it follows from (1-2) that $\lambda = \mu$ and $s = t$; moreover, we get from (3-22) and (3-9) that the cohomological degrees j for which $S_{\lambda(s)}F \otimes S_\lambda G$ appears in $\mathrm{Ext}^j_S(A, S)$ and $\mathrm{Ext}^j_S(C, S)$ satisfy

$$j \equiv m \cdot n - p^2 - s \cdot (m - n) \pmod 2. \qquad \square$$

4. Ext modules for $S/I_{\underline{x}}$

In this section we will use the explicit calculation of $\mathrm{Ext}^\bullet_S(J_{\underline{x},p}, S)$ from the previous section in order to deduce a formula for the characters of $\mathrm{Ext}^\bullet_S(S/I_{\underline{x}}, S)$ for all ideals $I_{\underline{x}}$. We begin with an important consequence of the results in the preceding section:

Corollary 4.1. *Fix an index $p \in \{0, 1, \ldots, n-1\}$ and positive integers $b > c > 0$. If we let $\underline{x} = (c^{p+1})$, $\underline{y} = (b^{p+1})$, then the natural quotient map $S/I_{\underline{y}} \twoheadrightarrow S/I_{\underline{x}}$ induces injective maps*

$$\mathrm{Ext}^i_S(S/I_{\underline{x}}, S) \hookrightarrow \mathrm{Ext}^i_S(S/I_{\underline{y}}, S)$$

for all $i = 0, 1, \ldots, m \cdot n$. More generally, if $\underline{z}$ is any partition with $z_1 = \cdots = z_{p+1}$ and $\underline{x} = \underline{z} + (c^{p+1})$, $\underline{y} = \underline{z} + (b^{p+1})$, then the quotient map $I_{\underline{z}}/I_{\underline{y}} \twoheadrightarrow I_{\underline{z}}/I_{\underline{x}}$ induces injective maps

$$\mathrm{Ext}^i_S(I_{\underline{z}}/I_{\underline{x}}, S) \hookrightarrow \mathrm{Ext}^i_S(I_{\underline{z}}/I_{\underline{y}}, S)$$

for all $i = 0, 1, \ldots, m \cdot n$.

Proof. Note that the former statement follows from the latter by taking $\underline{z} = \underline{0}$ and noting that $S = I_{\underline{0}}$. By Lemma 2.2, the modules $A = I_{\underline{x}}/I_{\underline{y}}$, $B = I_{\underline{z}}/I_{\underline{y}}$, and $C = I_{\underline{z}}/I_{\underline{x}}$ have finite filtrations with quotients isomorphic to $J_{\underline{t},p}$ for various partitions $\underline{t}$ satisfying $t_1 = \cdots = t_p$. Apply Corollary 3.5 to yield the desired conclusion. $\square$

Theorem 4.2. *Let $d \geq 0$ and consider partitions $\underline{x}$, $\underline{y}$, where $\underline{x}$ consists of the first d columns of $\underline{y}$; i.e., $x_i = \min(y_i, d)$ for all $i = 1, \ldots, n$. The natural quotient map $S/I_{\underline{y}} \twoheadrightarrow S/I_{\underline{x}}$ induces injective maps*

$$\mathrm{Ext}^i_S(S/I_{\underline{x}}, S) \hookrightarrow \mathrm{Ext}^i_S(S/I_{\underline{y}}, S) \tag{4-1}$$

for all $i = 0, 1, \ldots, m \cdot n$.

Proof. Arguing inductively, it suffices to prove the result when all the columns of $\underline{y}$ outside $\underline{x}$ have the same size (say $p+1$, for $p \in \{0, 1, \ldots, n-1\}$); i.e., $\underline{y} = \underline{x} + (a^{p+1})$ for some positive integer a. Note that this forces $x_1 = x_2 = \cdots = x_{p+1} = d$. We prove by descending induction on p that the induced map (4-1) is injective. When $p = n-1$, we have $\underline{x} = (d^n)$ and $\underline{y} = ((d+a)^n)$, so the conclusion follows from Corollary 4.1 (or from the results in [Raicu et al. 2014]).

Suppose now that $p < n-1$ and $\underline{y} = \underline{x} + (a^{p+1})$, $x_1 = \cdots = x_{p+1} = d$. Let $\underline{z}$ be the partition consisting of the columns of $\underline{x}$ of size strictly larger than $p+1$; i.e., $z_i = \min(x_i, x_{p+2})$ for all $i = 1, \ldots, n$. Consider the partitions $\tilde{\underline{x}}$ (resp. $\tilde{\underline{y}}$), defined by letting $\tilde{x}_i = x_i$ (resp. $\tilde{y}_i = y_i$) for $i \neq p+2$, and $\tilde{x}_{p+2} = x_{p+1}$ (resp. $\tilde{y}_{p+2} = y_{p+1}$). Alternatively, $\tilde{\underline{x}} = \underline{z} + ((d - x_{p+2})^{p+2})$, $\tilde{\underline{y}} = \underline{z} + ((d + a - x_{p+2})^{p+2})$. By induction, for all $i = 0, 1, \ldots, m \cdot n$, we obtain inclusions

$$\operatorname{Ext}^i_S(S/I_{\underline{z}}, S) \hookrightarrow \operatorname{Ext}^i_S(S/I_{\tilde{\underline{x}}}, S) \quad \text{and} \quad \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) \hookrightarrow \operatorname{Ext}^i_S(S/I_{\tilde{\underline{y}}}, S). \tag{4-2}$$

The natural commutative diagrams

$$\begin{array}{ccc} S/I_{\tilde{\underline{x}}} & \longrightarrow & S/I_{\underline{z}} \\ \downarrow & & \| \\ S/I_{\underline{x}} & \longrightarrow & S/I_{\underline{z}} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} S/I_{\tilde{\underline{y}}} & \longrightarrow & S/I_{\underline{z}} \\ \downarrow & & \| \\ S/I_{\underline{y}} & \longrightarrow & S/I_{\underline{z}} \end{array}$$

induce commutative diagrams

$$\begin{array}{ccc} \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\tilde{\underline{x}}}, S) \\ \| & & \uparrow \\ \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\underline{x}}, S) \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\tilde{\underline{y}}}, S) \\ \| & & \uparrow \\ \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\underline{y}}, S) \end{array}$$

Since the top maps are injective by (4-2), the bottom ones must be injective as well. For all $i = 0, 1, \ldots, m \cdot n$, we get commutative diagrams

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\underline{x}}, S) & \longrightarrow & \operatorname{Ext}^i_S(I_{\underline{x}}/I_{\underline{z}}, S) \\ & & \| & & \downarrow \alpha_i & & \downarrow \beta_i \\ 0 & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\underline{z}}, S) & \longrightarrow & \operatorname{Ext}^i_S(S/I_{\underline{y}}, S) & \longrightarrow & \operatorname{Ext}^i_S(I_{\underline{y}}/I_{\underline{z}}, S) \end{array}$$

where the rows are exact. The maps β_i are injective by Corollary 4.1, forcing the maps α_i to be injective as well. We conclude that the inclusion (4-1) holds, finishing the proof of the theorem. □

Theorem 4.3. *The character of the doubly graded module* $\mathrm{Ext}_S^\bullet(S/I_{\underline{x}}, S)$ *is given by*

$$\chi_{\mathrm{Ext}_S^\bullet(S/I_{\underline{x}},S)}(z,w) = \sum_{\substack{1\le p\le n\\ 0\le s\le t_1\le\cdots\le t_{n-p}\le p-1\\ \lambda\in W'(\underline{x},p;\underline{t},s)}} [S_{\lambda(s)}F\otimes S_\lambda G]\cdot z^{|\lambda|}\cdot w^{m\cdot n+1-p^2-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-p}t_j)}, \quad (4\text{-}3)$$

where $W'(\underline{x}, p; \underline{t}, s)$ *is the set of dominant weights* $\lambda\in\mathbb{Z}^n$ *satisfying*

$$\begin{cases} \lambda_n \ge p - x_p - m, & (4\text{-}4a)\\ \lambda_{t_j+j} \le t_j - x_{n+1-j} - m \quad \textit{for } j = 1,\dots,n-p, & (4\text{-}4b)\\ \lambda_s \ge s-n \quad \textit{and} \quad \lambda_{s+1}\le s-m. & (4\text{-}4c)\end{cases}$$

Remark 4.4. The condition $t_{n-p}\le p-1$ in (4-3), combined with the inequalities

$$t_{n-p} - x_{p+1} - m \ge \lambda_{t_{n-p}+n-p} \ge \lambda_n \ge p - x_p - m$$

obtained from (4-4b) by letting $j = n-p$, shows that the only values of p for which there may be a nontrivial contribution to (4-3) are the ones for which $x_p > x_{p+1}$ or $p = n$. It follows that for $x_1 = \cdots = x_n$, the only interesting value of p is $p = n$, in which case $I_{\underline{x}} = J_{\underline{x},n}$ and (4-3) follows from (3-9) and the standard long exact sequence relating $\mathrm{Ext}_S^\bullet(S/I_{\underline{x}}, S)$ to $\mathrm{Ext}_S^\bullet(I_{\underline{x}}, S)$.

Proof of Theorem 4.3. We induct on the number of columns of $\underline{x}$. When $\underline{x} = \underline{0}$, $S/I_{\underline{x}} = 0$, so $\mathrm{Ext}_S^\bullet(S/I_{\underline{x}}, S) = 0$. It follows that (4-3) is verified in this case, since $W'(\underline{0}, p; \underline{t}, s)$ is empty whenever $0\le s\le p-1$: to see this, note that

$$s - m \overset{(4\text{-}4c)}{\ge} \lambda_{s+1} \ge \lambda_n \overset{(4\text{-}4a)}{\ge} p - m$$

implies $s\ge p$, which is incompatible with the condition $s\le p-1$.

Suppose now that $\underline{y}$ is obtained from $\underline{x}$ by appending a column of size $(q+1)$ for some $q = 0,\dots,n-1$. This implies that $x_1 = \cdots = x_{q+1}$ and $y_i = x_i + 1$ for $1\le i\le q+1$. It follows from Theorem 4.2 that

$$\chi_{\mathrm{Ext}_S^\bullet(S/I_{\underline{y}},S)}(z,w) = \chi_{\mathrm{Ext}_S^\bullet(S/I_{\underline{x}},S)}(z,w) + \chi_{\mathrm{Ext}_S^\bullet(I_{\underline{x}}/I_{\underline{y}},S)}(z,w), \quad (4\text{-}5)$$

and from Lemma 2.2 and Corollary 3.5 that

$$\chi_{\mathrm{Ext}_S^\bullet(I_{\underline{x}}/I_{\underline{y}},S)}(z,w) = \sum_{\substack{\underline{z}=(z_1\ge\cdots\ge z_n\ge 0)\\ z_1=\cdots=z_{q+1}=x_1\\ z_i\ge x_i,\ i>q+1}} \chi_{\mathrm{Ext}_S^\bullet(J_{\underline{z},q},S)}(z,w). \quad (4\text{-}6)$$

By Remark 4.4, since $x_1 = \cdots = x_{q+1}$ and $y_1 = \cdots = y_{q+1}$, the only relevant terms in (4-3) (for both $\underline{x}$ and $\underline{y}$) are those for which $p \geq q+1$. For such p, $x_{n+1-j} = y_{n+1-j}$ whenever $1 \leq j \leq n-p$, so condition (4-4b) is the same for $\underline{x}$ as it is for $\underline{y}$. Equation (4-4c) is clearly the same for both $\underline{x}$ and $\underline{y}$, and the same is true for (4-4a) when $p \geq q+2$. We conclude that $W'(\underline{x}, p; \underline{t}, s) = W'(\underline{y}, p; \underline{t}, s)$ for $p \neq q+1$, from which it follows using (4-5) and the induction hypothesis that in order to prove (4-3) for $\underline{y}$, it suffices to show that

$$\begin{aligned}
&\chi_{\mathrm{Ext}^\bullet_S(I_{\underline{x}}/I_{\underline{y}},S)}(z,w) \\
&\quad= \sum_{\substack{p=q+1 \\ 0\leq s\leq t_1\leq\cdots\leq t_{n-p}\leq p-1 \\ \lambda\in W'(\underline{y},p;\underline{t},s)\setminus W'(\underline{x},p;\underline{t},s)}} [S_{\lambda(s)}F\otimes S_\lambda G]\cdot z^{|\lambda|}\cdot w^{m\cdot n+1-p^2-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-p}t_j)} \\
&\quad= \sum_{\substack{0\leq s\leq t_1\leq\cdots\leq t_{n-q-1}\leq q \\ \lambda\in W'(\underline{y},q+1;\underline{t},s)\setminus W'(\underline{x},q+1;\underline{t},s)}} [S_{\lambda(s)}F\otimes S_\lambda G]\cdot z^{|\lambda|} \\
&\qquad\qquad\qquad\qquad \cdot w^{m\cdot n-q^2-2\cdot q-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-q-1}t_j)}. \qquad (4\text{-}7)
\end{aligned}$$

Note that since (4-4b) and (4-4c) are the same for $\underline{x}$ and $\underline{y}$ when $p = q+1$, it follows that

$$\begin{aligned}
&\lambda \in W'(\underline{y}, q+1; \underline{t}, s) \setminus W'(\underline{x}, q+1; \underline{t}, s) \\
&\qquad\qquad \Longleftrightarrow \begin{cases} \lambda_n = q+1-y_{q+1}-m = q-x_1-m, \\ \lambda_{t_j+j} \leq t_j - x_{n+1-j} - m \quad \text{for } j = 1,\ldots,n-q-1, \\ \lambda_s \geq s-n \quad \text{and} \quad \lambda_{s+1} \leq s-m. \end{cases} \qquad (4\text{-}8)
\end{aligned}$$

Consider now a partition $\underline{z}$ appearing in (4-6). We claim that $W(\underline{z}, q; \underline{t}, s)$ is empty unless $t_{n-q} = q$. Furthermore, if $\lambda \in W(\underline{z}, q; \underline{t}, s)$, then $\lambda_n = q - x_1 - m$. To see this, note that

$$\lambda_n \leq \lambda_{t_{n-q}+n-q} \overset{\text{(3-10b)}}{=} t_{n-q} - z_{q+1} - m = t_{n-q} - z_q - m \leq q - z_q - m \overset{\text{(3-10a)}}{\leq} \lambda_n,$$

which forces equalities throughout, and in particular

$$t_{n-q} = q \quad \text{and} \quad \lambda_n = t_{n-q} - z_{q+1} - m = q - x_1 - m.$$

We get from (3-9) that

$$\begin{aligned}
&\chi_{\mathrm{Ext}^\bullet_S(J_{\underline{z},q},S)}(z,w) \\
&= \sum_{\substack{0\leq s\leq t_1\leq\cdots\leq t_{n-q-1}\leq t_{n-q}=q \\ \lambda\in W(\underline{x},q;\underline{t},s)}} [S_{\lambda(s)}F\otimes S_\lambda G]\cdot z^{|\lambda|}\cdot w^{m\cdot n-q^2-2q-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-q-1}t_j)}. \qquad (4\text{-}9)
\end{aligned}$$

Combining (4-6), (4-7) and (4-9), it remains to show that

$$W'(\underline{y}, q+1; \underline{t}, s) \setminus W'(\underline{x}, q+1; \underline{t}, s) = \bigcup_{\substack{\underline{z}=(z_1 \geq \cdots \geq z_n \geq 0) \\ z_1 = \cdots = z_{q+1} = x_1 \\ z_i \geq x_i,\ i > q+1}} W(\underline{x}, q; \underline{t}, s).$$

This follows immediately from (4-8) and the fact that the condition

$$\lambda_{t_j+j} \leq t_j - x_{n+1-j} - m \quad \text{for } j = 1, \ldots, n-q-1$$

in (4-8) is equivalent to the existence of a partition $\underline{z}$ satisfying $z_1 = \cdots = z_{q+1} = x_1$ and $z_{n+1-j} \geq x_{n+1-j}$ for $j = 1, \ldots, n-q-1$ (or equivalently $z_i \geq x_i$ for $i > q+1$), such that

$$\lambda_{t_j+j} = t_j - z_{n+1-j} - m \quad \text{for } j = 1, \ldots, n-q-1. \qquad \square$$

5. Regularity of the ideals $I_{\underline{x}}$

The explicit description of the character of $\mathrm{Ext}^\bullet_S(I_{\underline{x}}, S)$ obtained in Theorem 4.3 allows us to obtain the following result on the regularity of every ideal $I_{\underline{x}}$, whose proof will be the focus of the current section.

Theorem 5.1. *For a partition $\underline{x}$ with at most n parts, letting $x_{n+1} = -1$ we have the following formula for the regularity of the ideal $I_{\underline{x}}$:*

$$\mathrm{reg}(I_{\underline{x}}) = \max_{\substack{p=1,\ldots,n \\ x_p > x_{p+1}}} (n \cdot x_p + (p-2) \cdot (n-p)). \tag{5-1}$$

In particular, the only ideals $I_{\underline{x}}$ which have a linear resolution are those for which $x_1 = \cdots = x_n$ (i.e., powers $I_n^{x_1}$ of the ideal I_n of maximal minors) or $x_1 - 1 = x_2 = \cdots = x_n$ (i.e., $I_n^{x_1-1} \cdot I_1$).

By [Eisenbud 1995, Proposition 20.16], one can compute the regularity of a finitely generated S-module M by the formula

$$\mathrm{reg}(M) = \max\{-r - j : \mathrm{Ext}^j_S(M, S)_r \neq 0\}. \tag{5-2}$$

Since $\mathrm{reg}(I_{\underline{x}}) = \mathrm{reg}(S/I_{\underline{x}}) + 1$, we get by combining (5-2) and (4-3) that

$$\mathrm{reg}(I_{\underline{x}}) = \max_{\substack{1 \leq p \leq n \\ 0 \leq s \leq t_1 \leq \cdots \leq t_{n-p} \leq p-1 \\ \lambda \in W'(\underline{x}, p; \underline{t}, s)}} \left(-|\lambda| - mn + p^2 + s \cdot (m-n) + 2 \cdot \left(\sum_{j=1}^{n-p} t_j \right) \right). \tag{5-3}$$

It is then important to decide when $W'(\underline{x}, p; \underline{t}, s)$ is nonempty, which we do in the following lemma:

Lemma 5.2. *Fix $p \in \{1, \dots, n\}$ and $0 \le s \le t_1 \le \cdots \le t_{n-p} \le p-1$. The set $W'(\underline{x}, p; \underline{t}, s)$ is nonempty if and only if*

$$\begin{cases} x_p - x_{n+1-j} \ge p - t_j & \text{for } j = 1, \dots, (n-p), \\ s \ge p - x_p. \end{cases} \tag{5-4}$$

Moreover, the weight $\lambda \in W'(\underline{x}, p; \underline{t}, s)$ of minimal size (i.e., for which the quantity $-|\lambda|$ is maximal) is given by

$$\begin{cases} \lambda_1 = \cdots = \lambda_s = (s-n), \\ \lambda_{s+1} = \cdots = \lambda_n = (p - x_p - m). \end{cases} \tag{5-5}$$

Proof. If $W'(\underline{x}, p; \underline{t}, s)$ is nonempty, then for any $\lambda \in W'(\underline{x}, p; \underline{t}, s)$ we have

$$t_j - x_{n+1-j} - m \overset{\text{(4-4b)}}{\ge} \lambda_{t_j+j} \ge \lambda_n \overset{\text{(4-4a)}}{\ge} p - x_p - m$$

for $j = 1, \dots, (n-p)$ and

$$s - m \overset{\text{(4-4c)}}{\ge} \lambda_{s+1} \ge \lambda_n \overset{\text{(4-4a)}}{\ge} p - x_p - m,$$

so (5-4) holds.

Conversely, assume that (5-4) holds, and define λ via (5-5). It is immediate to check that λ satisfies (4-4a)–(4-4c), so $\lambda \in W'(\underline{x}, p; \underline{t}, s)$ and the set is nonempty. The fact that this λ has minimal size follows from the fact that any other $\lambda \in W'(\underline{x}, p; \underline{t}, s)$ is dominant and thus satisfies $\lambda_1 \ge \cdots \ge \lambda_s \ge (s-n)$ and $\lambda_{s+1} \ge \cdots \ge \lambda_n \ge (p - x_p - m)$, so

$$|\lambda| \ge s \cdot (s-n) + (n-s) \cdot (p - x_p - m) = (n-s) \cdot (p - x_p - s - m). \qquad \square$$

Lemma 5.2 allows us to rewrite (5-3) in the form

$$\begin{aligned} \operatorname{reg}(I_{\underline{x}}) &= \max_{\substack{1 \le p \le n \\ 0 \le s \le t_1 \le \cdots \le t_{n-p} \le p-1 \\ x_p - x_{n+1-j} \ge p - t_j \\ s \ge p - x_p}} \Big(-(n-s) \cdot (p - x_p - s - m) - mn \\ &\qquad + p^2 + s \cdot (m-n) + 2 \cdot \Big(\sum_{j=1}^{n-p} t_j \Big) \Big) \\ &= \max_{\substack{1 \le p \le n \\ 0 \le s \le t_1 \le \cdots \le t_{n-p} \le p-1 \\ x_p - x_{n+1-j} \ge p - t_j \\ s \ge p - x_p}} \Big(s \cdot (p - x_p - s) + n \cdot (x_p - p) + p^2 + 2 \cdot \Big(\sum_{j=1}^{n-p} t_j \Big) \Big) \\ &= \max_{\substack{1 \le p \le n \\ 0 \le s \le p-1 \\ x_p - x_{p+1} \ge 1 \\ s \ge p - x_p}} \big(s \cdot (p - x_p - s) + n \cdot x_p + (p-2) \cdot (n-p) \big). \end{aligned} \tag{5-6}$$

Since $s \geq p - x_p$, we have $s \cdot (p - x_p - s) \leq 0$, with equality if $s = 0$ or $s = p - x_p$. For $1 \leq p \leq n-1$, the condition $x_p - x_{p+1} \geq 1$ forces $x_p \geq 1$, so $p - x_p \leq p - 1$. It follows that we can take $s = \max(0, p - x_p)$ in order to maximize the expression above. Likewise, if $p = n$ and $x_n \geq 1$, we take $s = \max(0, n - x_n)$. It follows that when $x_n \geq 1$, (5-6) reduces to (5-1). However, if $x_n = 0$ then for $p = n$ the conditions $s \leq p - 1$ and $s \geq p - x_p$ are incompatible, so (5-6) reduces to

$$\operatorname{reg}(I_{\underline{x}}) = \max_{\substack{p=1,\dots,n-1 \\ x_p > x_{p+1}}} (n \cdot x_p + (p-2) \cdot (n-p)).$$

To see that this is the same as (5-1) it suffices to observe that $\operatorname{reg}(I_{\underline{x}}) \geq n x_n = 0$ (which is the term corresponding to $p = n$).

To finish the proof of the theorem, we need to verify the last assertion. Note that $I_{\underline{x}}$ is generated in degree $x_1 + \cdots + x_n$, so it has a linear resolution if and only if

$$\operatorname{reg}(I_{\underline{x}}) = x_1 + \cdots + x_n. \tag{5-7}$$

When $x_1 = \cdots = x_n$, (5-1) reduces to the term with $p = n$, whose value is $n x_n = x_1 + \cdots + x_n$. For $x_1 - 1 = x_2 = \cdots = x_n$, the only surviving terms in (5-1) are those with $p = 1$ and $p = n$, so we get

$$\operatorname{reg}(I_{\underline{x}}) = \max(n \cdot (x_1 - 1) + 1, n x_n) = n \cdot (x_1 - 1) + 1 = x_1 + \cdots + x_n.$$

Conversely, assume that (5-7) holds, and that the x_i aren't all equal. Take p minimal with the property that $x_p > x_{p+1}$, so that $p < n$, $x_1 = \cdots = x_p$ and $x_i \leq x_p - 1$ for $i > p$. We have

$$\begin{aligned} \operatorname{reg}(I_{\underline{x}}) &\geq n \cdot (x_p - p) + p^2 + 2 \cdot (p-1) \cdot (n-p) \\ &= p x_p + (n-p) \cdot (x_p - 1) + (n-p) \cdot (p-1) \geq x_1 + \cdots + x_n, \end{aligned}$$

with equality when $x_i = x_p - 1$ for $i > p$ and $(n-p) \cdot (p-1) = 0$. This forces $p = 1$ and $x_1 - 1 = x_2 = \cdots = x_n$, concluding the proof of the theorem.

6. Local cohomology with support in determinantal ideals

In this section, we prove our main theorem on local cohomology with support in determinantal ideals. Recall that $S = \operatorname{Sym}(\mathbb{C}^m \otimes \mathbb{C}^n)$ denotes the polynomial ring of functions on the space of $m \times n$ matrices, $I_p \subset S$ is the ideal of $p \times p$ minors of the generic $m \times n$ matrix, and $H_p(z, w)$ is the character of the doubly graded module $H^\bullet_{I_p}(S)$. Recall also the definition (1-3) of $h_s(z)$ and the notation (1-4) for Gauss polynomials.

Theorem 6.1. *For each $p = 1, \dots, n$, we have*

$$H_p(z, w) = \sum_{s=0}^{p-1} h_s(z) \cdot w^{(n-p+1)^2+(n-s)\cdot(m-n)} \cdot \binom{n-s-1}{p-s-1}(w^2).$$

To prove the theorem, note that since the system of ideals $\{I_{(d^p)} : d \geq 0\}$ is cofinal with the one consisting of powers of the ideal of $p \times p$ minors, we obtain from [Eisenbud 2005, Exercise A1D.1] that for each $i = 0, 1, \dots, m \cdot n$ we have

$$H^i_{I_p}(S) = \varinjlim_{d} \operatorname{Ext}^i_S(S/I_{(d^p)}, S),$$

where the successive maps in the directed system are induced from the natural quotient maps

$$S/I_{((d+1)^p)} \twoheadrightarrow S/I_{(d^p)}.$$

By Theorem 4.2 all these maps are injective, so the description of the character of $H^i_{I_p}(S)$ can be deduced from Theorem 4.3. Note that the partitions $\underline{x}$ to which we apply Theorem 4.3 have the property that $x_1 = \cdots = x_p = d$ and $x_i = 0$ for $i > p$. Since we are interested in the limit as $d \to \infty$, we might as well assume that $x_1 = \cdots = x_p = \infty$, in which case (4-4a) becomes vacuous. In what follows, λ will always be assumed to be a dominant weight.

If $s \leq t_j$ then $s + 1 \leq t_j + j$ for every $j = 1, \dots, n - p$, so we get

$$\lambda_{t_j+j} \overset{(\lambda\in\mathbb{Z}^n_{\mathrm{dom}})}{\leq} \lambda_{s+1} \overset{\text{(4-4c)}}{\leq} s - m \overset{(s\leq t_j)}{\leq} t_j - m;$$

i.e., (4-4c) implies (4-4b) (note that $x_{n+1-j} = 0$ for $j \leq n - p$). We conclude that

$$\begin{aligned} H_p(z, w) \;&=\; \sum_{\substack{0\leq s\leq t_1\leq\cdots\leq t_{n-p}\leq p-1\\ \lambda_s\geq s-n\\ \lambda_{s+1}\leq s-m}} [S_{\lambda(s)}F \otimes S_\lambda G]\cdot z^{|\lambda|} \cdot w^{m\cdot n+1-p^2-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-p} t_j)} \\ &\overset{\text{(1-3)}}{=} \sum_{0\leq s\leq t_1\leq\cdots\leq t_{n-p}\leq p-1} h_s(z) \cdot w^{m\cdot n+1-p^2-s\cdot(m-n)-2\cdot(\sum_{j=1}^{n-p} t_j)}, \end{aligned}$$

which yields, upon setting $t'_j := p - 1 - t_j$,

$$\begin{aligned} H_p(z, w) \;&=\; \sum_{s=0}^{p-1} h_s(z) \cdot w^{(n-p+1)^2+(n-s)\cdot(m-n)} \cdot \sum_{p-1-s\geq t'_1\geq\cdots\geq t'_{n-p}\geq 0} w^{2\cdot(\sum_{j=1}^{n-p} t'_j)} \\ &\overset{\text{(1-4)}}{=} \sum_{s=0}^{p-1} h_s(z) \cdot w^{(n-p+1)^2+(n-s)\cdot(m-n)} \cdot \binom{n-s-1}{p-s-1}(w^2). \end{aligned}$$

Acknowledgments

This work was initiated while we were visiting the Mathematical Sciences Research Institute, whose hospitality we are grateful for. Special thanks go to Emily Witt, who participated in the initial stages of this project. We would also like to thank David Eisenbud, Steven Sam, Anurag Singh and Uli Walther for helpful conversations, as well as the anonymous referee for suggesting improvements to the presentation. Experiments with the computer algebra software Macaulay2 [Grayson and Stillman 2013] have provided numerous valuable insights. Raicu acknowledges the support of NSF grant 1303042. Weyman acknowledges the support of the Alexander von Humboldt Foundation and of NSF grant 0901185.

References

[Akin and Weyman 2007] K. Akin and J. Weyman, "Primary ideals associated to the linear strands of Lascoux's resolution and syzygies of the corresponding irreducible representations of the Lie superalgebra $\mathbf{gl}(m|n)$", *J. Algebra* **310**:2 (2007), 461–490. MR 2009c:17007 Zbl 1171.17002

[Akin et al. 1981] K. Akin, D. A. Buchsbaum, and J. Weyman, "Resolutions of determinantal ideals: the submaximal minors", *Adv. Math.* **39**:1 (1981), 1–30. MR 82h:13011 Zbl 0474.14035

[Bruns and Schwänzl 1990] W. Bruns and R. Schwänzl, "The number of equations defining a determinantal variety", *Bull. London Math. Soc.* **22**:5 (1990), 439–445. MR 91k:14035 Zbl 0725.14039

[Bruns and Vetter 1988] W. Bruns and U. Vetter, *Determinantal rings*, Lecture Notes in Math. **1327**, Springer, Berlin, 1988. MR 89i:13001 Zbl 0673.13006

[de Concini et al. 1980] C. de Concini, D. Eisenbud, and C. Procesi, "Young diagrams and determinantal varieties", *Invent. Math.* **56**:2 (1980), 129–165. MR 81m:14034 Zbl 0435.14015

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Eisenbud 2005] D. Eisenbud, *The geometry of syzygies: a second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics **229**, Springer, New York, 2005. MR 2005h:13021 Zbl 1066.14001

[Fulton and Harris 1991] W. Fulton and J. Harris, *Representation theory: a first course*, Graduate Texts in Mathematics **129**, Springer, New York, 1991. MR 93a:20069 Zbl 0744.22001

[Grayson and Stillman 2013] D. R. Grayson and M. E. Stillman, "Macaulay 2: a software system for research in algebraic geometry", 2013, Available at http://www.math.uiuc.edu/Macaulay2.

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977. MR 57 #3116 Zbl 0367.14001

[Hochster and Eagon 1971] M. Hochster and J. A. Eagon, "Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci", *Amer. J. Math.* **93** (1971), 1020–1058. MR 46 #1787 Zbl 0244.13012

[Lyubeznik et al. 2013] G. Lyubeznik, A. Singh, and U. Walther, "Local cohomology modules supported at determinantal ideals", preprint, 2013. arXiv 1308.4182

[Peskine and Szpiro 1973] C. Peskine and L. Szpiro, "Dimension projective finie et cohomologie locale: applications à la démonstration de conjectures de M. Auslander, H. Bass et A. Grothendieck", *Inst. Hautes Études Sci. Publ. Math.* **42** (1973), 47–119. MR 51 #10330 Zbl 0268.13008

[Raicu et al. 2014] C. Raicu, J. Weyman, and E. E. Witt, "Local cohomology with support in ideals of maximal minors and sub-maximal Pfaffians", *Adv. Math.* **250** (2014), 596–610. MR 3122178 Zbl 06284419

[Weyman 2003] J. Weyman, *Cohomology of vector bundles and syzygies*, Cambridge Tracts in Mathematics **149**, Cambridge University Press, 2003. MR 2004d:13020 Zbl 1075.13007

[Witt 2012] E. E. Witt, "Local cohomology with support in ideals of maximal minors", *Adv. Math.* **231**:3-4 (2012), 1998–2012. MR 2964631 Zbl 1253.13019

Communicated by David Eisenbud
Received 2013-09-27 Revised 2014-02-25 Accepted 2014-03-26

craicu@nd.edu *Department of Mathematics, University of Notre Dame, 255 Hurley Hall, Notre Dame, IN 46556, United States*

Simion Stoilow Institute of Mathematics of the Romanian Academy, 21 Calea Grivitei Street, 010702 Bucharest, Romania

jerzy.weyman@uconn.edu *Department of Mathematics, University of Connecticut, Storrs, CT 06269, United States*

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1259

Affine congruences and rational points on a certain cubic surface

Pierre Le Boudec

We establish estimates for the number of solutions of certain affine congruences. These estimates are then used to prove Manin's conjecture for a cubic surface split over $\mathbb{Q}$ whose singularity type is D_4. This improves on a result of Browning and answers a problem posed by Tschinkel.

1. Introduction

The aim of this paper is to study the asymptotic behavior of the number of rational points of bounded height on the cubic surface $V \subset \mathbb{P}^3$ defined over $\mathbb{Q}$ by

$$x_0(x_1 + x_2 + x_3)^2 - x_1x_2x_3 = 0.$$

Manin's conjecture [Franke et al. 1989], and the refinements concerning the value of the constant due to Peyre [1995] and to Batyrev and Tschinkel [1998b], describe precisely what should be the solution of this problem.

The variety V has a unique singularity at the point $(1 : 0 : 0 : 0)$, of type D_4. In addition, it contains precisely six lines, which are defined by $x_0 = x_i = 0$ and $x_1 + x_2 + x_3 = x_i = 0$ for $i \in \{1, 2, 3\}$. Rational points accumulate on these six lines, hiding the interesting behavior of the number of rational points lying outside the lines. We thus let U be the open subset formed by removing the six lines

MSC2010: primary 11D45; secondary 14G05.
Keywords: affine congruences, rational points, Manin's conjecture, cubic surfaces, universal torsors.

from V. We also let $H : \mathbb{P}^3(\mathbb{Q}) \to \mathbb{R}_{>0}$ be the exponential height, defined for a vector $(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ satisfying $\gcd(x_0, x_1, x_2, x_3) = 1$ by

$$H(x_0 : x_1 : x_2 : x_3) = \max\{|x_0|, |x_1|, |x_2|, |x_3|\}.$$

The quantity in which we are interested is then defined by

$$N_{U,H}(B) = \#\big\{x \in U(\mathbb{Q}) \;\big|\; H(x) \leq B\big\}.$$

In this specific context, Manin's conjecture states that

$$N_{U,H}(B) = c_{V,H} B (\log B)^6 (1 + o(1)),$$

where $c_{V,H}$ is a constant which is expected to agree with Peyre's prediction. In a more general setting, the exponent of the logarithm is expected to be equal to the rank of the Picard group of the minimal desingularization of V minus one. In comparison, the number $N_{\mathbb{P}^1,H}(B)$ of rational points of bounded height lying on a line satisfies $N_{\mathbb{P}^1,H}(B) = c_{\mathbb{P}^1,H} B^2 (1 + o(1))$, where $c_{\mathbb{P}^1,H} > 0$.

Manin's conjecture for singular cubic surfaces has received an increasing amount of attention over the last years (see, for instance, [de la Bretèche and Swinnerton-Dyer 2007; de la Bretèche et al. 2007; Le Boudec 2012a]). The interested reader is invited to refer to [Le Boudec 2012a, Section 1] for a comprehensive overview of what is currently known concerning singular cubic surfaces defined over $\mathbb{Q}$.

Any cubic surface in $\mathbb{P}^3$ defined over $\mathbb{C}$ which has only isolated singularities and which is not a cone over an elliptic curve can only have ADE singularities (see [Coray and Tsfasman 1988, Proposition 0.2]). In Table 1 below, we recall the classification over $\overline{\mathbb{Q}}$ of cubic surfaces with ADE singularities, and we give the number of lines contained by the surfaces. Moreover, we indicate if Manin's conjecture is known for at least one example of the surface of the specified singularity type by giving the corresponding reference. Note that the difficulty of proving Manin's conjecture increases as we go higher in Table 1.

At the American Institute of Mathematics workshop *Rational and integral points on higher-dimensional varieties* in 2002, Tschinkel posed the problem of studying the quantity $N_{U,H}(B)$. Motivated by [Heath-Brown 2003], which deals with Cayley's cubic surface, Browning [2006] gave a first answer to this question by proving that

$$N_{U,H}(B) \asymp B(\log B)^6,$$

where $\asymp$ means that the ratio of these two quantities is between two positive constants. To do so, he made use of the universal torsor calculated in [Hassett and Tschinkel 2004], which is an open subset of the affine hypersurface embedded in $\mathbb{A}^{10} \simeq \mathrm{Spec}(\mathbb{Q}[\eta_1, \ldots, \eta_{10}])$ and defined by

$$\eta_2 \eta_5^2 \eta_8 + \eta_3 \eta_6^2 \eta_9 + \eta_4 \eta_7^2 \eta_{10} - \eta_1 \eta_2 \eta_3 \eta_4 \eta_5 \eta_6 \eta_7 = 0.$$

Singularity type	Number of lines	Result
A_1	21	
$2A_1$	16	
A_2	15	
$3A_1$	12	
$A_2 + A_1$	11	
A_3	10	
$4A_1$	9	
$2A_1 + A_2$	8	
$A_3 + A_1$	7	
$2A_2$	7	
A_4	6	
D_4	6	[this paper]
$2A_1 + A_3$	5	
$2A_2 + A_1$	5	[Le Boudec 2012a]
$A_4 + A_1$	4	
A_5	3	
D_5	3	[Browning and Derenthal 2009]
$3A_2$	3	[Batyrev and Tschinkel 1998a]
$A_5 + A_1$	2	[Baier and Derenthal 2012]
E_6	1	[de la Bretèche et al. 2007]

Table 1. Cubic surfaces with ADE singularities.

In this paper, we also make use of this auxiliary variety to establish Manin's conjecture for V.

Universal torsors were originally introduced by Colliot-Thélène and Sansuc in order to study the Hasse principle and weak approximation for rational varieties (see [Colliot-Thélène and Sansuc 1976; 1980; 1987]). These descent methods have turned out to be a very pertinent tool for counting problems. The parametrizations of rational points provided by universal torsors have been used in the context of Manin's conjecture for the first time by Peyre [1998] and Salberger [1998].

It is a well-established heuristic that counting rational points on cubic surfaces becomes harder as the number N of (-2)-curves on the minimal desingularizations decreases (which means as we go higher in Table 1). As a consequence, our result can be seen as a new record, since V is the first example of cubic surface with $N = 4$ for which Manin's conjecture is proved. By way of comparison, we record

here that N is also equal to 4 for Cayley's cubic. Previously, Manin's conjecture was known for only two nontoric cubic surfaces with $N = 6$ (see [de la Bretèche et al. 2007; Baier and Derenthal 2012]) and two cubic surfaces with $N = 5$ (see [Browning and Derenthal 2009; Le Boudec 2012a]).

Since the parametrizations of the rational points resorting to universal torsors become extremely complicated as N decreases, it seems to the author that establishing Manin's conjecture for a cubic surface with $1 \leq N \leq 3$, and even for another cubic surface with $N = 4$, is an extremely difficult problem. In particular, all such surfaces have universal torsors which are not hypersurfaces. Actually, it is not even clear if sharp upper bounds for $N_{U,H}(B)$ can be obtained for surfaces with $1 \leq N \leq 3$. As a reminder, the best result known for nonsingular cubic surfaces (that is, with $N = 0$) is the upper bound

$$N_{U,H}(B) \ll B^{4/3+\varepsilon}$$

for any fixed $\varepsilon > 0$, which holds if the surface contains three coplanar lines defined over $\mathbb{Q}$ (see [Heath-Brown 1997]).

To prove Manin's conjecture for V, we start by establishing estimates for the number of $(u, v) \in \mathbb{Z}^2$ lying in a prescribed region and satisfying the congruence

$$a_1 u + a_2 v \equiv b \pmod{q} \tag{1-1}$$

and the condition $\gcd(uv, q) = 1$, where $a_1, a_2 \in \mathbb{Z}_{\neq 0}$, $q \in \mathbb{Z}_{\geq 1}$ are such that $a_1 a_2$ is coprime to q and $b \in \mathbb{Z}$ is divisible by each prime number dividing q. Then, the first step of the proof consists in summing over three variables, viewing the torsor equation as an affine congruence to which these estimates are applied.

At this stage of the proof, a very interesting phenomenon stands out. The error term showing up in these estimates gives birth to a new congruence where the coefficients a_1 and a_2 appear. However, it is not possible to give a good bound for this quantity for any fixed a_1 and a_2 coprime to q. As a consequence, this quantity has to be estimated on average over certain variables dividing a_1 and a_2. More precisely, this error term is nontrivially summed over two other variables whose squares respectively divide a_1 and a_2, using a result due to Heath-Brown and coming from the geometry of numbers.

The step which makes this new congruence appear is definitely the key step of our proof (see Lemma 2). Our method is believed to be quite new and will certainly be useful in dealing with other diophantine problems. For instance, the methods of Lemmas 2 and 9 are used in forthcoming work of la Bretèche and Browning [2014], in which they study in a quantitative way the failure of the Hasse principle for a certain family of Châtelet surfaces.

It is worth pointing out that it is very likely that our work can be adapted to yield a proof of Manin's conjecture for another cubic surface with a single singularity

of type D_4 but lying in the other isomorphism class over $\overline{\mathbb{Q}}$ (there are exactly two isomorphism classes of cubic surfaces with D_4 singularity type over $\overline{\mathbb{Q}}$). This cubic surface is defined over $\mathbb{Q}$ by

$$x_0(x_1+x_2+x_3)^2+x_1(x_1+x_2)=0,$$

and the universal torsor corresponding to this problem is an open subset of the affine hypersurface embedded in $\mathbb{A}^{10}\simeq \mathrm{Spec}(\mathbb{Q}[\eta_1,\dots,\eta_{10}])$ and defined by

$$\eta_2\eta_5^2\eta_8+\eta_3\eta_6^2\eta_9+\eta_4\eta_7^2\eta_{10}=0.$$

The study of the congruence (1-1) in the particular case $b=0$ is expected to solve the problem of proving Manin's conjecture for this surface in a similar fashion.

Our main result is the following:

Theorem 1. *As B tends to $+\infty$, we have the estimate*

$$N_{U,H}(B)=c_{V,H}B(\log B)^6\left(1+O\left(\frac{1}{(\log\log B)^{1/6}}\right)\right),$$

where $c_{V,H}$ agrees with Peyre's prediction.

It has been checked that V is not an equivariant compactification of $\mathbb{G}_m^2$ or $\mathbb{G}_a^2$ (see [Derenthal 2014, Proposition 13] and [Derenthal and Loughran 2010]). Furthermore, let

$$G_d=\mathbb{G}_a\rtimes_d\mathbb{G}_m,$$

where $d\in\mathbb{Z}$ and the action of $g\in\mathbb{G}_m$ on $x\in\mathbb{G}_a$ is given by $g\cdot x=g^dx$. It can be checked that if V were an equivariant compactification of G_d, then the number of negative curves on its minimal desingularization would be less than or equal to 8, which is not the case since this number is equal to 10. As a result, Theorem 1 does not follow from the general results concerning equivariant compactifications of algebraic groups [Batyrev and Tschinkel 1998a; Chambert-Loir and Tschinkel 2002; Tanimoto and Tschinkel 2012].

The next section is dedicated to the proofs of several preliminary results. The two following sections are devoted to the descriptions of the universal torsor and Peyre's constant respectively. Finally, in the remaining section we prove Theorem 1.

Throughout the proof, ε is an arbitrarily small positive number. As a convention, the implicit constants involved in the notation O and $\ll$ are always allowed to depend on ε.

2. Preliminaries

2.1. ***Affine congruences.*** Let $a_1,a_2\in\mathbb{Z}_{\neq 0}$ be two integers, and set $\boldsymbol{a}=(a_1,a_2)$. Let also $q\in\mathbb{Z}_{\geq 1}$ and $b\in\mathbb{Z}$. We assume that a_1a_2 is coprime to q. Moreover, if we let $\mathrm{rad}(n)$ denote the radical of an integer $n\geq 1$; that is,

$$\mathrm{rad}(n) = \prod_{p \mid n} p,$$

then we also assume that

$$\mathrm{rad}(q) \mid b. \tag{2-1}$$

Let $\mathcal{I}$ and $\mathcal{J}$ be two bounded intervals. We introduce the quantities

$$N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) = \#\big\{(u, v) \in \mathcal{I} \times \mathcal{J} \cap \mathbb{Z}^2 \;\big|\; a_1 u + a_2 v \equiv b \pmod{q}, \gcd(uv, q) = 1\big\}, \tag{2-2}$$

and

$$N^*(\mathcal{I}, \mathcal{J}; q) = \frac{1}{\varphi(q)} \#\big\{(u, v) \in \mathcal{I} \times \mathcal{J} \cap \mathbb{Z}^2 \;\big|\; \gcd(uv, q) = 1\big\}. \tag{2-3}$$

It is immediate to check that one of the two conditions among $\gcd(u, q) = 1$ and $\gcd(v, q) = 1$ can be omitted in the definition of $N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b)$. Indeed, if we omit the condition $\gcd(u, q) = 1$, then the conditions $\gcd(a_2, q) = 1$ and $\gcd(v, q) = 1$ together imply that we have $\gcd(a_1 u - b, q) = 1$. This last condition is seen to be equivalent to $\gcd(u, q) = 1$, thanks to the conditions (2-1) and $\gcd(a_1, q) = 1$.

Note that $N^*(\mathcal{I}, \mathcal{J}; q)$ is the average of $N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b)$ over a_1 or a_2 coprime to q. In Lemma 2, we show how we can approximate $N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b)$ by $N^*(\mathcal{I}, \mathcal{J}; q)$. We start by studying some exponential sums which will naturally appear in the proof of Lemma 2. For $q \in \mathbb{Z}_{\geq 1}$, we let e_q be the function defined by $e_q(x) = e^{2i\pi x/q}$, and we set for $r, s \in \mathbb{Z}$

$$S_q(r, s, \boldsymbol{a}, b) = \sum_{\substack{\alpha, \beta = 1 \\ \gcd(\alpha\beta, q) = 1 \\ a_1\alpha + a_2\beta \equiv b \pmod{q}}}^{q} e_q(r\alpha + s\beta).$$

Furthermore, we need to introduce the classical Ramanujan sum. For $q \in \mathbb{Z}_{\geq 1}$ and $n \in \mathbb{Z}$, we set

$$c_q(n) = \sum_{\substack{\alpha = 1 \\ \gcd(\alpha, q) = 1}}^{q} e_q(n\alpha)$$

and we recall that

$$c_q(n) = \sum_{d \mid \gcd(q, n)} \mu\left(\frac{q}{d}\right) d. \tag{2-4}$$

Lemma 1. *For any $r, s \in \mathbb{Z}$, we have*

$$S_q(r, s, \boldsymbol{a}, b) = e_q(r a_1^{-1} b) c_q(a_1 s - a_2 r)$$

and, symmetrically,

$$S_q(r, s, \boldsymbol{a}, b) = e_q(s a_2^{-1} b) c_q(a_2 r - a_1 s),$$

where a_1^{-1} and a_2^{-1} denote respectively the inverses of a_1 and a_2 modulo q.

As a result, we have $S_q(q, s, \boldsymbol{a}, b) = c_q(s)$ and $S_q(r, q, \boldsymbol{a}, b) = c_q(r)$, and thus these two quantities are independent of $\boldsymbol{a}$ and b.

Proof. The symmetry given by the map $(r, s, a_1, a_2) \mapsto (s, r, a_2, a_1)$ implies that we only need to prove one of the two equalities. Let us prove the second one. Just as we can omit the condition $\gcd(v, q) = 1$ in the definition of $N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b)$, we can also omit the condition $\gcd(\beta, q) = 1$ in the definition of $S_q(r, s, \boldsymbol{a}, b)$. Therefore, we get

$$\begin{aligned} S_q(r, s, \boldsymbol{a}, b) &= \sum_{\substack{\alpha=1 \\ \gcd(\alpha,q)=1}}^{q} e_q(r\alpha) \sum_{\substack{\beta=1 \\ a_1\alpha+a_2\beta\equiv b \,(\mathrm{mod}\ q)}}^{q} e_q(s\beta) \\ &= \sum_{\substack{\alpha=1 \\ \gcd(\alpha,q)=1}}^{q} e_q(r\alpha) e_q(s(a_2^{-1}b - a_2^{-1}a_1\alpha)) \\ &= e_q(sa_2^{-1}b) \sum_{\substack{\alpha=1 \\ \gcd(\alpha,q)=1}}^{q} e_q((r - a_2^{-1}a_1 s)\alpha) \\ &= e_q(sa_2^{-1}b) c_q(r - a_2^{-1}a_1 s) = e_q(sa_2^{-1}b) c_q(a_2 r - a_1 s), \end{aligned}$$

as wished. □

From now on, for $\lambda > 0$ we define the arithmetic function $\sigma_{-\lambda}$ by

$$\sigma_{-\lambda}(n) = \sum_{k \mid n} k^{-\lambda}.$$

Lemma 2. *Let $a_1, a_2 \in \mathbb{Z}_{\neq 0}$, $q \in \mathbb{Z}_{\geq 1}$ and $b \in \mathbb{Z}$, satisfying the assumptions $\gcd(a_1 a_2, q) = 1$ and $\mathrm{rad}(q) \mid b$. We have the estimate*

$$N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) - N^*(\mathcal{I}, \mathcal{J}; q) \ll E(q, \boldsymbol{a}),$$

where $E(q, \boldsymbol{a}) = E_0(q, \boldsymbol{a}) + E_1(q)$ with

$$E_0(q, \boldsymbol{a}) = \sum_{d \mid q} \left|\mu\left(\frac{q}{d}\right)\right| d \sum_{\substack{0<|r|,|s|\leq q/2 \\ a_1 s - a_2 r \equiv 0 \,(\mathrm{mod}\ d)}} |r|^{-1}|s|^{-1}$$

and

$$E_1(q) = \left(\frac{q}{\varphi(q)}\right)^3 (\log q)^2.$$

Proof. We detect the congruence using sums of exponentials; we get

$$\begin{aligned} N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) &= \sum_{\substack{\alpha,\beta=1 \\ \gcd(\alpha\beta,q)=1 \\ a_1\alpha+a_2\beta\equiv b \,(\mathrm{mod}\ q)}}^{q} \#\big\{(u,v) \in \mathcal{I}\times\mathcal{J} \cap \mathbb{Z}^2 \;\big|\; q \,|\, \alpha-u, \beta-v\big\} \\ &= \sum_{\substack{\alpha,\beta=1 \\ \gcd(\alpha\beta,q)=1 \\ a_1\alpha+a_2\beta\equiv b \,(\mathrm{mod}\ q)}}^{q} \frac{1}{q^2}\Big(\sum_{u\in\mathcal{I}}\sum_{r=1}^{q} e_q(r\alpha - ru)\Big)\Big(\sum_{v\in\mathcal{J}}\sum_{s=1}^{q} e_q(s\beta - sv)\Big) \\ &= \frac{1}{q^2}\sum_{r,s=1}^{q} S_q(r,s,\boldsymbol{a},b)F_q(r,s), \end{aligned}$$

where

$$F_q(r,s) = \Big(\sum_{u\in\mathcal{I}} e_q(-ru)\Big)\Big(\sum_{v\in\mathcal{J}} e_q(-sv)\Big).$$

Using Lemma 1, we get

$$N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) = \frac{1}{q^2}\sum_{r,s=1}^{q} e_q(ra_1^{-1}b)c_q(a_1s - a_2r)F_q(r,s).$$

Let $\|x\|$ denote the distance from x to the set of integers. If $r, s \neq q$, then $F_q(r,s)$ is the product of two geometric sums, and we therefore have

$$F_q(r,s) \ll \Big\|\frac{r}{q}\Big\|^{-1}\Big\|\frac{s}{q}\Big\|^{-1}.$$

Let $N(\mathcal{I}, \mathcal{J}; q)$ be the sum of the terms corresponding to $r = q$ or $s = q$. As stated in Lemma 1, $N(\mathcal{I}, \mathcal{J}; q)$ is independent of a_1, a_2 and b. Using (2-4), we get

$$\begin{aligned} N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) - N(\mathcal{I}, \mathcal{J}; q) &= \frac{1}{q^2}\sum_{r,s=1}^{q-1} e_q(ra_1^{-1}b)c_q(a_1s - a_2r)F_q(r,s) \\ &\ll \frac{1}{q^2}\sum_{d\,|\,q}\Big|\mu\Big(\frac{q}{d}\Big)\Big| d \sum_{\substack{r,s=1 \\ a_1s-a_2r\equiv 0 \,(\mathrm{mod}\ d)}}^{q-1} \Big\|\frac{r}{q}\Big\|^{-1}\Big\|\frac{s}{q}\Big\|^{-1} \\ &\ll \frac{1}{q^2}\sum_{d\,|\,q}\Big|\mu\Big(\frac{q}{d}\Big)\Big| d \sum_{\substack{0<|r|,|s|\le q/2 \\ a_1s-a_2r\equiv 0 \,(\mathrm{mod}\ d)}} \frac{q}{|r|}\frac{q}{|s|}. \end{aligned}$$

Recall that the right-hand side is equal to $E_0(q, \boldsymbol{a})$. We have thus obtained

$$N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) - N(\mathcal{I}, \mathcal{J}; q) \ll E_0(q, \boldsymbol{a}). \tag{2-5}$$

Since $N(\mathcal{I}, \mathcal{J}; q)$ is independent of a_2 and since $N^*(\mathcal{I}, \mathcal{J}; q)$ is the average of $N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b)$ over a_2 coprime to q, averaging this estimate over a_2 coprime to q shows that

$$N^*(\mathcal{I}, \mathcal{J}; q) - N(\mathcal{I}, \mathcal{J}; q) \ll E_1'(q),$$

where

$$\begin{aligned} E_1'(q) &= \frac{1}{\varphi(q)} \sum_{d \mid q} d \sum_{0<|r|,|s|\le q/2} |r|^{-1}|s|^{-1} \sum_{\substack{a_2=1 \\ \gcd(a_2,q)=1 \\ a_1 s - a_2 r \equiv 0 \,(\mathrm{mod}\, d)}}^{q} 1 \\ &\ll \frac{1}{\varphi(q)} \sum_{d \mid q} d \sum_{0<|r|,|s|\le q/2} \gcd(r, s, d)|r|^{-1}|s|^{-1} \\ &\ll \frac{1}{\varphi(q)} \sum_{d \mid q} d \sum_{d' \mid d} d' \sum_{\substack{0<|r|,|s|\le q/2 \\ d' \mid r,\, d' \mid s}} |r|^{-1}|s|^{-1} \\ &\ll \frac{1}{\varphi(q)} (\log q)^2 \sum_{d \mid q} d\sigma_{-1}(d). \end{aligned}$$

Furthermore, we can check that the right-hand side is bounded by $E_1(q)$. Thus

$$N^*(\mathcal{I}, \mathcal{J}; q) - N(\mathcal{I}, \mathcal{J}; q) \ll E_1(q), \tag{2-6}$$

and therefore, combining the estimates (2-5) and (2-6), we obtain

$$N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) - N^*(\mathcal{I}, \mathcal{J}; q) \ll E(q, \boldsymbol{a}),$$

which completes the proof. □

Note that an immediate consequence of Lemma 2 is the bound

$$N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) \ll \frac{1}{\varphi(q)} \#(\mathcal{I} \times \mathcal{J} \cap \mathbb{Z}^2) + E(q, \boldsymbol{a}). \tag{2-7}$$

We now introduce a certain domain $\mathcal{S} \subset \mathbb{R}^2$ where the couple (u, v) is restricted to lie. Let $X, T, A_1, A_2 \ge 1$. We let $\mathcal{S} = \mathcal{S}(X, T, A_1, A_2)$ be the set of $(x, y) \in \mathbb{R}^2$ such that

$$A_1|x| A_2|y| |A_1 x + A_2 y - T| \le T^2 X, \tag{2-8}$$

$$|A_1 x + A_2 y - T| \le X, \tag{2-9}$$

$$A_1|x| \le X, \tag{2-10}$$

$$A_2|y| \le X. \tag{2-11}$$

Note that the last three conditions imply that we also have

$$T \le 3X.$$

Finally, we set

$$D(\mathcal{S}; q, \boldsymbol{a}, b) = \#\big\{(u, v) \in \mathcal{S} \cap \mathbb{Z}^2_{\neq 0} \;\big|\; a_1 u + a_2 v \equiv b \pmod q, \gcd(uv, q) = 1\big\}$$

and

$$D^*(\mathcal{S}; q) = \frac{1}{\varphi(q)} \#\big\{(u, v) \in \mathcal{S} \cap \mathbb{Z}^2_{\neq 0} \;\big|\; \gcd(uv, q) = 1\big\}.$$

We now aim to prove the following lemma.

Lemma 3. *Let $L \geq 1$. We have the estimate*

$$D(\mathcal{S}; q, \boldsymbol{a}, b) - D^*(\mathcal{S}; q) \ll \frac{1}{L} \frac{X^3}{T A_1 A_2 \varphi(q)} + L^4 \log(2X)^2 E(q, \boldsymbol{a}).$$

Proving this requires a technical result similar to [Le Boudec 2012b, Lemma 4].

Lemma 4. *Let $0 < \nu \leq 1$ and $M_0 \in \mathbb{R}_{>0}$. Let $Y \in \mathbb{R}_{>0}$ and $Y' \in \mathbb{R}$ be such that $0 < Y - Y' \ll \nu M_0^2$. Let also $A \in \mathbb{R}$ and set $M = \max(|A|, Y^{1/2})$. Let $\mathcal{R} \subset \mathbb{R}$ be the set of real numbers y satisfying*

$$Y' < |y^2 + 2Ay| \leq Y.$$

If $M_0 \gg M$ then we have the bound

$$\#(\mathcal{R} \cap \mathbb{Z}) \ll \nu^{1/2} \frac{M_0^2}{M} + 1.$$

Proof. Without using the assumption $M_0 \gg M$, the proof of [Le Boudec 2012b, Lemma 4] shows that we have

$$\#(\mathcal{R} \cap \mathbb{Z}) \ll \nu \frac{M_0^2}{M} + \nu^{1/2} M_0 + 1.$$

Therefore, under the assumption $M_0 \gg M$, we clearly have the claimed upper bound. □

Proof of Lemma 3. If $\mathcal{S} \cap \mathbb{Z}^2_{\neq 0} = \varnothing$ then the result is obvious. We therefore assume from now on that $\mathcal{S} \cap \mathbb{Z}^2_{\neq 0} \neq \varnothing$. We let $0 < \delta,\ \delta' \leq 1$ be two parameters to be selected in due course, and we set $\zeta = 1 + \delta$ and $\zeta' = 1 + \delta'$. In addition, we let U and V be variables running over the sets $\{\pm\zeta^n \mid n \in \mathbb{Z}_{\geq -1}\}$ and $\{\pm\zeta'^n \mid n \in \mathbb{Z}_{\geq -1}\}$, respectively. We define $\mathcal{I} =]U, \zeta U]$ if $U > 0$ and $\mathcal{I} = [\zeta U, U[$ if $U < 0$, and define the interval $\mathcal{J}$ the same way using the variable V and the parameter ζ'. We have

$$D(\mathcal{S}; q, \boldsymbol{a}, b) - \sum_{\mathcal{I} \times \mathcal{J} \cap \mathbb{Z}^2 \subset \mathcal{S}} N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) \ll \sum_{\substack{\mathcal{I} \times \mathcal{J} \cap \mathbb{Z}^2 \not\subseteq \mathcal{S} \\ \mathcal{I} \times \mathcal{J} \cap \mathbb{Z}^2 \not\subseteq \mathbb{R}^2 \setminus \mathcal{S}}} N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b).$$

We define the quantity

$$D(\mathcal{S}; q) = \sum_{\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2\subset\mathcal{S}} N^*(\mathcal{I}, \mathcal{J}; q).$$

We note here that since $N^*(\mathcal{I}, \mathcal{J}; q)$ is independent of a_1, a_2 and b, $D(\mathcal{S}; q)$ is also independent of a_1, a_2 and b. Moreover, we have

$$\sum_{\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2\subset\mathcal{S}} N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) - D(\mathcal{S}; q) \ll \frac{\log(2X)^2}{\delta\delta'} E(q, \boldsymbol{a}),$$

where we have used Lemma 2 and noted that the number of rectangles $\mathcal{I}\times\mathcal{J}$ such that $\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2 \subset \mathcal{S}$ is at most

$$4\left(1+\frac{\log X}{\log\zeta}\right)\left(1+\frac{\log X}{\log\zeta'}\right) \ll \frac{\log(2X)^2}{\delta\delta'},$$

since $\delta, \delta' \le 1$. We have proved that

$$D(\mathcal{S}; q, \boldsymbol{a}, b) - D(\mathcal{S}; q) \ll \sum_{\substack{\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2\not\subset\mathcal{S}\\ \mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2\not\subset\mathbb{R}^2\setminus\mathcal{S}}} N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b) + \frac{\log(2X)^2}{\delta\delta'} E(q, \boldsymbol{a}).$$

Using the bound (2-7) for $N(\mathcal{I}, \mathcal{J}; q, \boldsymbol{a}, b)$, we conclude that

$$D(\mathcal{S}; q, \boldsymbol{a}, b) - D(\mathcal{S}; q) \ll \frac{1}{\varphi(q)} \sum_{\substack{\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2\not\subset\mathcal{S}\\ \mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2\not\subset\mathbb{R}^2\setminus\mathcal{S}}} \#(\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2) + \frac{\log(2X)^2}{\delta\delta'} E(q, \boldsymbol{a}),$$

since the number of rectangles $\mathcal{I}\times\mathcal{J}$ satisfying $\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2 \not\subset \mathcal{S}$ and $\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2 \not\subset \mathbb{R}^2\setminus\mathcal{S}$ is also $\ll \log(2X)^2\delta^{-1}\delta'^{-1}$. The sum of the right-hand side is over all the rectangles $\mathcal{I}\times\mathcal{J}$ for which $(\zeta^{s_1}U, \zeta'^{s_2}V) \in \mathcal{S}\cap\mathbb{Z}^2$ and $(\zeta^{t_1}U, \zeta'^{t_2}V) \in \mathbb{Z}^2\setminus\mathcal{S}$ for some $(s_1, s_2) \in]0, 1]^2$ and $(t_1, t_2) \in]0, 1]^2$. This means that one of the inequalities defining $\mathcal{S}$ is not satisfied by $(\zeta^{t_1}U, \zeta'^{t_2}V)$, and we need to estimate the contribution coming from each of the conditions (2-8)–(2-11). Note that we always have the conditions

$$A_1|U| \le X, \tag{2-12}$$

$$A_2|V| \le X. \tag{2-13}$$

In what follows, we could sometimes write strict inequalities instead of nonstrict ones, but this would not change anything in our reasoning. Let us first deal with condition (2-8). For the rectangles $\mathcal{I}\times\mathcal{J}$ described above, for some $(s_1, s_2) \in]0, 1]^2$ and $(t_1, t_2) \in]0, 1]^2$ we have

$$\zeta^{s_1}\zeta'^{s_2}A_1|U|A_2|V|\left|\zeta^{s_1}A_1U+\zeta'^{s_2}A_2V-T\right|\le T^2X, \tag{2-14}$$

$$\zeta^{t_1}\zeta'^{t_2}A_1|U|A_2|V|\left|\zeta^{t_1}A_1U+\zeta'^{t_2}A_2V-T\right|> T^2X. \tag{2-15}$$

These two conditions imply respectively

$$|A_1U+A_2V-T|\le\frac{T^2X}{A_1|U|A_2|V|}+\delta A_1|U|+\delta' A_2|V|,$$

and

$$|A_1U+A_2V-T|>\zeta^{-1}\zeta'^{-1}\frac{T^2X}{A_1|U|A_2|V|}-\delta A_1|U|-\delta' A_2|V|.$$

Setting $\Delta=\delta+\delta'$, we thus get

$$\zeta^{-1}\zeta'^{-1}\frac{T^2X}{A_1|U|A_2|V|}-\Delta X<|A_1U+A_2V-T|\le\frac{T^2X}{A_1|U|A_2|V|}+\Delta X. \tag{2-16}$$

Going back to the variables u and v, it is immediate to check that

$$\big||A_1u+A_2v-T|-|A_1U+A_2V-T|\big|\le\delta A_1|U|+\delta' A_2|V|\le\Delta X.$$

Therefore, the inequality (2-16) gives

$$\zeta^{-1}\zeta'^{-1}\frac{T^2X}{A_1|u|A_2|v|}-2\Delta X<|A_1u+A_2v-T|\le\zeta\zeta'\frac{T^2X}{A_1|u|A_2|v|}+2\Delta X.$$

Finally, we obtain the condition

$$\zeta^{-1}\zeta'^{-1}\frac{T^2X}{A_1^2A_2|v|}-4\Delta\frac{X^2}{A_1^2}<|u|\left|u+\frac{A_2}{A_1}v-\frac{T}{A_1}\right|\le\zeta\zeta'\frac{T^2X}{A_1^2A_2|v|}+4\Delta\frac{X^2}{A_1^2}. \tag{2-17}$$

Since $T\le 3X$, we can apply Lemma 4 with

$$M_0=\frac{X^{3/2}}{A_1A_2^{1/2}|v|^{1/2}}$$

and $\nu=\Delta$. We see that the error we want to estimate is bounded by

$$\begin{aligned}\sum_{\substack{(2\text{-}12),(2\text{-}13)\\(2\text{-}16)}}\#(\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2)&\ll\#\big\{(u,v)\in\mathbb{Z}^2_{\neq 0}\;\big|\;(2\text{-}17),\ |u|\ll X/A_1,\ |v|\ll X/A_2\big\}\\&\ll\sum_{|v|\ll X/A_2}\left(\Delta^{1/2}\frac{X^{5/2}}{TA_1A_2^{1/2}|v|^{1/2}}+1\right)\ll\Delta^{1/2}\frac{X^3}{TA_1A_2}+\frac{X}{A_2}.\end{aligned}$$

Using the symmetry between the variables u and v, we see that we also have

$$\sum_{\substack{(2\text{-}12),(2\text{-}13)\\(2\text{-}16)}}\#(\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2)\ll\Delta^{1/2}\frac{X^3}{TA_1A_2}+\frac{X}{A_1},$$

and thus

$$\sum_{\substack{\text{(2-12),(2-13)}\\ \text{(2-16)}}} \#(\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2) \ll \Delta^{1/2}\frac{X^3}{TA_1A_2}+\frac{X}{A_1^{1/2}A_2^{1/2}}.$$

We now reason in a similar way to treat the cases of the other conditions. Let us estimate the contribution coming from condition (2-9). We see that the condition which plays the role of (2-16) in the previous case is here

$$X-\Delta X<|A_1U+A_2V-T|\le X+\Delta X. \tag{2-18}$$

Furthermore, going back to the variables u and v, we obtain

$$X-2\Delta X<|A_1u+A_2v-T|\le X+2\Delta X. \tag{2-19}$$

We therefore find that the error in this case is bounded by

$$\begin{aligned}\sum_{\substack{\text{(2-12),(2-13)}\\ \text{(2-18)}}} \#(\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2) &\ll \#\big\{(u,v)\in\mathbb{Z}^2_{\neq 0}\ \big|\ \text{(2-19)},\ |u|\ll X/A_1,\ |v|\ll X/A_2\big\}\\ &\ll \sum_{|v|\ll X/A_2}\left(\Delta\frac{X}{A_1}+1\right)\ll \Delta\frac{X^2}{A_1A_2}+\frac{X}{A_2}.\end{aligned}$$

Once again using the symmetry between the variables u and v, we obtain

$$\sum_{\substack{\text{(2-12),(2-13)}\\ \text{(2-18)}}} \#(\mathcal{I}\times\mathcal{J}\cap\mathbb{Z}^2) \ll \Delta\frac{X^2}{A_1A_2}+\frac{X}{A_1^{1/2}A_2^{1/2}}.$$

Finally, if $X/A_1<2$ then it is clear that we do not have to consider the case of condition (2-10), and if $X/A_1\ge 2$ then we are going to choose δ such that X/A_1 is an integer power of ζ and, as a result, we do not have to consider the case of this condition, here either. The same reasoning holds for the choice of the parameter δ' depending on the size of the quantity X/A_2. As a consequence, we have obtained

$$D(\mathcal{S};q,\boldsymbol{a},b)-D(\mathcal{S};q)\ll\Delta^{1/2}\frac{X^3}{TA_1A_2\varphi(q)}+\frac{\log(2X)^2}{\delta\delta'}E(q,\boldsymbol{a})+\frac{X}{A_1^{1/2}A_2^{1/2}\varphi(q)}.$$

Note that if $q=1$ then the result of Lemma 3 is clear since $D(\mathcal{S};1,\boldsymbol{a},b)=D^*(\mathcal{S};1)$ and if $q>1$ then the third term of the right-hand side is dominated by one of the other two. We can always choose δ and δ' such that ζ and ζ' are integer powers of X/A_1 and X/A_2 respectively if these quantities are greater than or equal to 2; and we can require that, given $L\ge 1$,

$$\delta,\delta'\asymp\frac{1}{L^2}.$$

These choices of δ and δ' give

$$D(\mathcal{S}; q, \boldsymbol{a}, b) - D(\mathcal{S}; q) \ll \frac{1}{L} \frac{X^3}{TA_1A_2\varphi(q)} + L^4 \log(2X)^2 E(q, \boldsymbol{a}).$$

Since $D(\mathcal{S}; q)$ does not depend on a_2 and $D^*(\mathcal{S}; q)$ is the average of $D(\mathcal{S}; q, \boldsymbol{a}, b)$ over a_2 coprime to q, averaging the last estimate over a_2 coprime to q yields

$$D^*(\mathcal{S}; q) - D(\mathcal{S}; q) \ll \frac{1}{L} \frac{X^3}{TA_1A_2\varphi(q)} + L^4 \log(2X)^2 E_1(q).$$

Putting these two estimates together completes the proof. □

Our next aim is to approximate the cardinality which appears in $D^*(\mathcal{S}; q)$ by its corresponding two-dimensional volume. For this, we define the real-valued function

$$h : (x, y, t) \mapsto \max\big\{|xy|\,|x + y - t|, t^2|x|, t^2|y|, t^2|x + y - t|\big\}. \tag{2-20}$$

It is immediate to check that

$$\mathcal{S} = \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; h\left(\frac{A_1x}{X^{1/3}T^{2/3}}, \frac{A_2y}{X^{1/3}T^{2/3}}, \frac{T^{1/3}}{X^{1/3}}\right) \le 1\right\}. \tag{2-21}$$

We also introduce the real-valued functions

$$g_1 : (y, t) \mapsto \int_{h(x,y,t)\le 1} \mathrm{d}x, \quad g_2 : t \mapsto \int g_1(y, t)\,\mathrm{d}y.$$

Lemma 5. *For $(y, t) \in \mathbb{R} \times \mathbb{R}_{>0}$, we have the bounds*

$$g_1(y, t) \ll t^{-2} \quad \textit{and} \quad g_2(t) \ll 1.$$

Proof. The bound for g_1 is clear since $t^2|x| \le 1$. To prove the bound for g_2, we use the elementary result [Derenthal 2009, Lemma 5.1]. We obtain

$$\int_{|xy|\,|x+y-t|\le 1} \mathrm{d}x \ll \min\left\{\frac{1}{|y|^{1/2}}, \frac{1}{|y|\,|y - t|}\right\}.$$

Therefore, we have

$$g_2(t) \ll \int_{|y|\le 1} \frac{\mathrm{d}y}{|y|^{1/2}} + \int_{|y|,|y-t|\ge 1} \frac{\mathrm{d}y}{|y|\,|y - t|} + \int_{|y|\ge 1,|y-t|\le 1} \frac{\mathrm{d}y}{|y|^{3/4}|y - t|^{1/2}}.$$

The three terms of the right-hand side are easily seen to be bounded by an absolute constant, which completes the proof. □

We now prove that the following result holds:

Lemma 6. *We have the estimate*

$$D^*(\mathcal{S};q)-\frac{\varphi(q)}{q^2}\frac{X^{2/3}T^{4/3}}{A_1A_2}g_2\Big(\frac{T^{1/3}}{X^{1/3}}\Big)\ll\frac{X^2}{A_1A_2q}\Big(\frac{A_1^{1/2}}{X^{1/2}}+\frac{A_2^{1/2}}{X^{1/2}}\Big)E_2(q),$$

where

$$E_2(q)=\frac{q}{\varphi(q)}\sigma_{-1/2}(q)\sigma_{-1}(q).$$

Proof. We start by removing the two coprimality conditions $\gcd(u,q)=1$ and $\gcd(v,q)=1$ using Möbius inversions. We get

$$D^*(\mathcal{S};q)=\frac{1}{\varphi(q)}\sum_{\ell_1\mid q}\mu(\ell_1)\sum_{\ell_2\mid q}\mu(\ell_2)C(\ell_1,\ell_2,\mathcal{S}),\tag{2-22}$$

where

$$C(\ell_1,\ell_2,\mathcal{S})=\#\big\{(u',v')\in\mathbb{Z}_{\neq0}^2\;\big|\;(\ell_1u',\ell_2v')\in\mathcal{S}\big\}.$$

To count the number of u' to be considered, we use the estimate

$$\#\{n\in\mathbb{Z}_{\neq0}\cap[t_1,t_2]\}=t_2-t_1+O(\max(|t_1|,|t_2|)^{1/2}),\tag{2-23}$$

which is valid for any $t_1,t_2\in\mathbb{R}$ such that $t_1\le t_2$. We obtain

$$\begin{aligned}C(\ell_1,\ell_2,\mathcal{S})&=\sum_{\substack{v'\in\mathbb{Z}_{\neq0}\\ A_2\ell_2|v'|\le X}}\Big(\frac{X^{1/3}T^{2/3}}{A_1\ell_1}g_1\Big(\frac{A_2\ell_2v'}{X^{1/3}T^{2/3}},\frac{T^{1/3}}{X^{1/3}}\Big)+O\Big(\frac{X^{1/2}}{A_1^{1/2}\ell_1^{1/2}}\Big)\Big)\\&=\frac{X^{1/3}T^{2/3}}{A_1\ell_1}\sum_{\substack{v'\in\mathbb{Z}_{\neq0}\\ A_2\ell_2|v'|\le X}}g_1\Big(\frac{A_2\ell_2v'}{X^{1/3}T^{2/3}},\frac{T^{1/3}}{X^{1/3}}\Big)+O\Big(\frac{X^{3/2}}{A_1^{1/2}\ell_1^{1/2}A_2\ell_2}\Big).\end{aligned}$$

The first bound of Lemma 5 implies that

$$\sup_{|y|\le X^{2/3}/T^{2/3}}g_1\Big(y,\frac{T^{1/3}}{X^{1/3}}\Big)\ll\frac{X^{2/3}}{T^{2/3}}.$$

Since g_1 is easily seen to have a piecewise continuous derivative, this bound, an application of partial summation and a further use of the estimate (2-23) yield

$$\sum_{\substack{v'\in\mathbb{Z}_{\neq0}\\ A_2\ell_2|v'|\le X}}g_1\Big(\frac{A_2\ell_2v'}{X^{1/3}T^{2/3}},\frac{T^{1/3}}{X^{1/3}}\Big)=\frac{X^{1/3}T^{2/3}}{A_2\ell_2}g_2\Big(\frac{T^{1/3}}{X^{1/3}}\Big)+O\Big(\frac{X^{7/6}}{T^{2/3}A_2^{1/2}\ell_2^{1/2}}\Big).$$

We have finally proved that

$$C(\ell_1,\ell_2,\mathcal{S})=\frac{1}{\ell_1\ell_2}\frac{X^{2/3}T^{4/3}}{A_1A_2}g_2\Big(\frac{T^{1/3}}{X^{1/3}}\Big)+O\Big(\frac{X^{3/2}}{A_1\ell_1A_2^{1/2}\ell_2^{1/2}}+\frac{X^{3/2}}{A_1^{1/2}\ell_1^{1/2}A_2\ell_2}\Big).$$

Putting together this estimate and the equality (2-22) completes the proof. □

One of the immediate consequences of Lemmas 3 and 6 is the following result, which corresponds exactly to the setting of the proof of Theorem 1:

Lemma 7. *Let $L \geq 1$ and $\mathscr{L} \geq 1$. If*

$$\frac{X}{\mathscr{L}} \leq T,$$

then we have the estimate

$$D(\mathcal{S}; q, \boldsymbol{a}, b) - \frac{\varphi(q)}{q^2} \frac{X^{2/3} T^{4/3}}{A_1 A_2} g_2\left(\frac{T^{1/3}}{X^{1/3}}\right) \ll E,$$

where $E = E(X, T, A_1, A_2, L, \mathscr{L}, q, \boldsymbol{a})$ is given by

$$E = L^4 \log(2X)^2 E(q, \boldsymbol{a}) + \frac{X^{2/3} T^{4/3}}{A_1 A_2 q} \mathscr{L}^{4/3} \left(\frac{\mathscr{L}}{L} + \frac{A_1^{1/2}}{X^{1/2}} + \frac{A_2^{1/2}}{X^{1/2}}\right) E_2(q).$$

2.2. ***The error term.*** We now turn to the investigation of the error term $E(q, \boldsymbol{a}')$ in the particular case where $\boldsymbol{a}' = (b_1 c_1^2, b_2 c_2^2)$ for $b_1, b_2, c_1, c_2 \in \mathbb{Z}_{\geq 1}$. Recall that we have $\gcd(b_1 b_2 c_1 c_2, q) = 1$. We aim to give an upper bound for the sums of $E(q, \boldsymbol{a}')$ over c_1 and c_2 in some dyadic ranges. For this, we make use of the following result, which comes from the geometry of numbers and is due to Heath-Brown (see [1984, Lemma 3]). Note that this result had already been used by Browning [2006] to prove that $N_{U,H}(B)$ has the expected order of magnitude.

Lemma 8. *Let $(v_1, v_2, v_3) \in \mathbb{Z}^3$ be a primitive vector, and let $W_1, W_2, W_3 \geq 1$. The number of primitive vectors $(w_1, w_2, w_3) \in \mathbb{Z}^3$ satisfying the conditions $|w_i| \leq W_i$ for $i = 1, 2, 3$ and the equation*

$$v_1 w_1 + v_2 w_2 + v_3 w_3 = 0$$

is at most

$$12\pi \frac{W_1 W_2 W_3}{\max\{|v_i| W_i\}} + 4,$$

where the maximum is taken over $i = 1, 2, 3$.

From now on, we let τ be the usual divisor function. Recall the definitions of $E(q, \boldsymbol{a}')$ and $E_1(q)$ given in Lemma 2. We now prove the following lemma:

Lemma 9. *Let $C_1, C_2 \geq \frac{1}{2}$. We have the bound*

$$\sum_{\substack{C_i < c_i \leq 2C_i \\ \gcd(c_1, c_2) = 1}}^{*} E(q, \boldsymbol{a}') \ll (C_1 C_2 \tau(q) + q) 2^{\omega(q)} E_1(q),$$

where the notation $\sum^*$ means that the summation is restricted to integers which are coprime to q and where i implicitly runs over the set $\{1, 2\}$.

Proof. We have

$$\sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1}}^{*} E(q,\boldsymbol{a}') \ll \sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1}}^{*} E_0(q,\boldsymbol{a}') + C_1C_2E_1(q).$$

The first term of the right-hand side is at most

$$\sum_{d\mid q} d \sum_{0<|r|,|s|\le q/2} |r|^{-1}|s|^{-1} \sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ b_1c_1^2s-b_2c_2^2r\equiv 0 \,(\mathrm{mod}\ d)}}^{*} 1.$$

Let us set $g=\gcd(r,s,d)$ and $s'=s/g$, $r'=r/g$ and $d'=d/g$. We have

$$\begin{aligned}\sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ b_1c_1^2s-b_2c_2^2r\equiv 0 \,(\mathrm{mod}\ d)}}^{*} 1 &= \sum_{\substack{1\le\rho\le d\\ \gcd(\rho,d)=1\\ b_1s\rho^2-b_2r\equiv 0 \,(\mathrm{mod}\ d)}} \sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ \rho c_2\equiv c_1 \,(\mathrm{mod}\ d)}}^{*} 1\\ &= \sum_{\substack{1\le\rho\le d\\ \gcd(\rho,d)=1\\ b_1s'\rho^2-b_2r'\equiv 0 \,(\mathrm{mod}\ d')}} \sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ \rho c_2\equiv c_1 \,(\mathrm{mod}\ d)}}^{*} 1\\ &= \sum_{\substack{1\le\rho\le d\\ \gcd(\rho,d)=1\\ \rho^2-(b_1s')^{-1}b_2r'\equiv 0 \,(\mathrm{mod}\ d')}} \sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ \rho c_2\equiv c_1 \,(\mathrm{mod}\ d)}}^{*} 1,\end{aligned}$$

since $\gcd(b_1b_2,d')=1$ and $\gcd(r',s',d')=1$, and where $(b_1s')^{-1}$ denotes the inverse of b_1s' modulo d'. Using Lemma 8, we get

$$\sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ \rho c_2\equiv c_1 \,(\mathrm{mod}\ d)}}^{*} 1 \ll \frac{C_1C_2}{d}+1.$$

As a consequence, we have proved that

$$\sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1\\ b_1c_1^2s-b_2c_2^2r\equiv 0 \,(\mathrm{mod}\ d)}}^{*} 1 \ll \gcd(r,s,d)2^{\omega(d)}\left(\frac{C_1C_2}{d}+1\right).$$

Finally, we easily get

$$\sum_{d\mid q} d \sum_{0<|r|,|s|\le q/2} |r|^{-1}|s|^{-1}\frac{\gcd(r,s,d)2^{\omega(d)}}{d} \ll \sum_{d\mid q} 2^{\omega(d)} \sum_{e\mid d} e \sum_{\substack{0<|r|,|s|\le q/2\\ e\mid r,\, e\mid s}} |r|^{-1}|s|^{-1}$$
$$\ll 2^{\omega(q)}\tau(q)\sigma_{-1}(q)(\log q)^2$$
$$\ll 2^{\omega(q)}\tau(q)E_1(q),$$

and, as in the proof of Lemma 2, we obtain

$$\sum_{d\mid q} d \sum_{0<|r|,|s|\le q/2} |r|^{-1}|s|^{-1}\gcd(r,s,d)2^{\omega(d)} \ll q2^{\omega(q)}E_1(q).$$

As a result, we have proved that

$$\sideset{}{^*}\sum_{\substack{C_i<c_i\le 2C_i\\ \gcd(c_1,c_2)=1}} E_0(q,\boldsymbol{a}') \ll (C_1C_2\tau(q)+q)2^{\omega(q)}E_1(q),$$

which completes the proof. □

2.3. ***Arithmetic functions.*** We now introduce several arithmetic functions which will appear along the proof of Theorem 1. We set

$$\varphi^*(n) = \prod_{p\mid n}\Big(1-\frac{1}{p}\Big), \tag{2-24}$$

$$\varphi^\curlyvee(n) = \prod_{p\mid n}\Big(1-\frac{1}{p}\Big)^{-2}\Big(1+\frac{2}{p}\Big)^{-1}, \tag{2-25}$$

and also, for $a, b \in \mathbb{Z}_{\ge 1}$,

$$\psi_a(n) = \prod_{\substack{p\mid n\\ p\nmid a}}\Big(1-\frac{1}{p}\Big)^2\Big(1-\frac{1}{p-1}\Big), \tag{2-26}$$

and

$$\psi_{a,b}(n) = \begin{cases}\psi_a(n) & \text{if } \gcd(n,b)=1,\\ 0 & \text{otherwise.}\end{cases}$$

Following the straightforward reasoning of the proofs of [Le Boudec 2012b, Lemmas 5, 6], we easily obtain the following result:

Lemma 10. *Let $0<\gamma\le 1$ be fixed. Let $0\le t_1<t_2$, and set $I=[t_1,t_2]$. Let $g:\mathbb{R}_{>0}\to\mathbb{R}$ be a function with a piecewise continuous derivative on I whose sign changes at most $R_g(I)$ times on I. We have*

$$\sum_{n\in I\cap\mathbb{Z}_{>0}} \psi_{a,b}(n)g(n) = \Upsilon\Psi(a,b)\int_I g(t)\,\mathrm{d}t + O_\gamma\big(\sigma_{-\gamma/2}(ab)t_2^\gamma M_I(g)\big),$$

where

$$\Upsilon = \prod_p \varphi^{\curlyvee}(p)^{-1}, \quad \Psi(a,b) = \varphi^*(b)\varphi^{\curlyvee}(ab), \tag{2-27}$$

and

$$M_I(g) = (1 + R_g(I)) \sup_{t \in I \cap \mathbb{R}_{>0}} |g(t)|.$$

3. The universal torsor

In this section we define a bijection between the set of rational points of bounded height on U and a certain set of integral points on the hypersurface defined in the introduction. The universal torsor corresponding to our present problem was first determined by Hassett and Tschinkel [2004] and then used by Browning [2006] to prove the lower and upper bounds of the expected order of magnitude for $N_{U,H}(B)$. We employ the notation used in [Derenthal 2014]. Let $\mathcal{T}(B)$ be the set of $(\eta_1, \dots, \eta_{10}) \in \mathbb{Z}^7_{>0} \times \mathbb{Z}^3_{\neq 0}$ satisfying the equation

$$\eta_2\eta_5^2\eta_8 + \eta_3\eta_6^2\eta_9 + \eta_4\eta_7^2\eta_{10} - \eta_1\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7 = 0, \tag{3-1}$$

the coprimality conditions

$$\gcd(\eta_{10}, \eta_1\eta_2\eta_3\eta_4\eta_5\eta_6) = 1, \tag{3-2}$$
$$\gcd(\eta_9, \eta_1\eta_2\eta_3\eta_4\eta_5\eta_7) = 1, \tag{3-3}$$
$$\gcd(\eta_8, \eta_1\eta_2\eta_3\eta_4\eta_6\eta_7) = 1, \tag{3-4}$$
$$\gcd(\eta_1, \eta_5\eta_6\eta_7) = 1, \tag{3-5}$$
$$\gcd(\eta_2\eta_5, \eta_3\eta_4\eta_6\eta_7) = 1, \tag{3-6}$$
$$\gcd(\eta_3\eta_6, \eta_4\eta_7) = 1, \tag{3-7}$$

and the height conditions

$$|\eta_8\eta_9\eta_{10}| \le B, \tag{3-8}$$
$$\eta_1^2\eta_2^2\eta_3\eta_4\eta_5^2|\eta_8| \le B, \tag{3-9}$$
$$\eta_1^2\eta_2\eta_3^2\eta_4\eta_6^2|\eta_9| \le B, \tag{3-10}$$
$$\eta_1^2\eta_2\eta_3\eta_4^2\eta_7^2|\eta_{10}| \le B. \tag{3-11}$$

Lemma 11. $N_{U,H}(B) = \#\mathcal{T}(B)$.

Proof. It is sufficient to show that the counting problem defined by the set $\mathcal{T}(B)$ is equivalent to the one described in [Browning 2006, Section 4], which we call $\mathcal{T}'(B)$ and which is defined exactly as $\mathcal{T}(B)$ except that the condition (3-5) is replaced by the condition $|\mu(\eta_2\eta_3\eta_4)| = 1$.

For $i = 2, 3, 4$, there is only one way to write $\eta_i = \eta_i' \eta_i''^2$ in such a way that η_i' is squarefree. Setting $\eta_{i+3}' = \eta_{i+3}\eta_i''$ and $\eta_1' = \eta_1 \eta_2'' \eta_3'' \eta_4''$, we claim that the translation between the two counting problems is achieved via the map

$$S : (\eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, \eta_7) \mapsto (\eta_1', \eta_2', \eta_3', \eta_4', \eta_5', \eta_6', \eta_7').$$

Indeed, (3-1) and the height conditions (3-8)–(3-11) are invariant under S. Also, the coprimality conditions (3-2), (3-3), (3-4), (3-6) and (3-7) are preserved under S, and the condition (3-5) is replaced by the condition $|\mu(\eta_2'\eta_3'\eta_4')| = 1$, which completes the proof. □

4. Calculation of Peyre's constant

Peyre [1995] gives an interpretation for the constant $c_{V,H}$ appearing in the main term of $N_{U,H}(B)$ in Theorem 1. In our specific case, we have

$$c_{V,H} = \alpha(\widetilde{V})\beta(\widetilde{V})\omega_H(\widetilde{V}),$$

where $\widetilde{V}$ denotes the minimal desingularization of V. The definitions of these three quantities are omitted (the reader should refer to [Peyre 1995] or to Section 4 of [Le Boudec 2012a] for some more details in an identical setting). Using the work of Derenthal, Joyce and Teitler [Derenthal et al. 2008, Theorem 1.3], it is easy to compute the constant $\alpha(\widetilde{V})$. We find

$$\alpha(\widetilde{V}) = \frac{1}{120} \cdot \frac{1}{\#W(\mathrm{D}_4)} = \frac{1}{23040},$$

where $W(\mathrm{D}_4)$ stands for the Weyl group associated to the Dynkin diagram of the singularity D_4. Here, we have used $\#W(\mathrm{D}_n) = 2^{n-1}n!$ for any $n \geq 4$. In addition, $\beta(\widetilde{V}) = 1$ since V is split over $\mathbb{Q}$. Finally, $\omega_H(\widetilde{V})$ is given by

$$\omega_H(\widetilde{V}) = \omega_\infty \prod_p \Big(1 - \frac{1}{p}\Big)^7 \omega_p,$$

where ω_∞ and ω_p are the archimedean and p-adic densities respectively. Loughran [2010, Lemma 2.3] has shown that we have

$$\omega_p = 1 + \frac{7}{p} + \frac{1}{p^2}.$$

Let us calculate ω_∞. Let $\boldsymbol{x} = (x_0, x_1, x_2, x_3)$ and $f(\boldsymbol{x}) = x_0(x_1+x_2+x_3)^2 - x_1x_2x_3$. We parametrize the points of V with x_1, x_2 and x_3. We have

$$\frac{\partial f}{\partial x_0}(\boldsymbol{x}) = (x_1 + x_2 + x_3)^2,$$

and since $\boldsymbol{x} = -\boldsymbol{x} \in \mathbb{P}^3$, we obtain

$$\omega_\infty = \frac{1}{2} \iiint_{|x_1x_2x_3|/(x_1+x_2+x_3)^2, |x_1|, |x_2|, |x_3| \le 1} \frac{\mathrm{d}x_1\,\mathrm{d}x_2\,\mathrm{d}x_3}{(x_1+x_2+x_3)^2}.$$

Recall the definition (2-20) of the function h. The change of variables defined by $x_1 = t^2x$, $x_2 = t^2y$ and $x_3 = -t^2(x+y-t)$ yields

$$\omega_\infty = \frac{3}{2} \iiint_{h(x,y,t)\le 1} \mathrm{d}x\,\mathrm{d}y\,\mathrm{d}t = 3 \iiint_{t>0, h(x,y,t)\le 1} \mathrm{d}x\,\mathrm{d}y\,\mathrm{d}t. \tag{4-1}$$

5. Proof of the main theorem

5.1. ***Restriction of the domain.*** Note that in the torsor equation (3-1) the first three terms are at most $B/\eta_1^2\eta_2\eta_3\eta_4$ (by the height conditions (3-9)–(3-11)), and thus we have

$$\eta_1^3\eta_2^2\eta_3^2\eta_4^2\eta_5\eta_6\eta_7 \le 3B.$$

From now on, for $n \in \mathbb{Z}_{\ge 1}$ we denote by $\mathrm{sq}(n)$ the unique positive integer such that $\mathrm{sq}(n)^2 \mid n$ and $n/\mathrm{sq}(n)^2$ is squarefree. Note that for two coprime integers $m, n \in \mathbb{Z}_{\ge 1}$, we have $\mathrm{sq}(mn) = \mathrm{sq}(m)\,\mathrm{sq}(n)$.

We now need to show that we can assume along the proof that

$$\eta_1\,\mathrm{sq}(\eta_2\eta_3\eta_4) \ge B^{15/\log\log B}, \tag{5-1}$$

and, in addition, that

$$\eta_1^3\eta_2^2\eta_3^2\eta_4^2\eta_5\eta_6\eta_7 \ge \frac{B}{\log\log B}. \tag{5-2}$$

The proof of Lemma 11 shows that we can make use of the estimates in [Browning 2006, Section 6] to prove that the contributions to $N_{U,H}(B)$ coming from those $(\eta_1, \dots, \eta_{10}) \in \mathcal{T}(B)$ which do not satisfy one of the two inequalities (5-1) and (5-2) are actually negligible.

We start by proving a lemma:

Lemma 12. *Let $\mathcal{M}(B)$ be the overall contribution to $N_{U,H}(B)$ coming from those $(\eta_1, \dots, \eta_{10}) \in \mathcal{T}(B)$ such that $\eta_1\,\mathrm{sq}(\eta_2\eta_3\eta_4) \le B^{15/\log\log B}$. We have*

$$\mathcal{M}(B) \ll \frac{B(\log B)^6}{\log\log B}.$$

Proof. Recall the notation introduced in the proof of Lemma 11. We note that the condition $\eta_1\,\mathrm{sq}(\eta_2\eta_3\eta_4) \le B^{15/\log\log B}$ is equivalent to $\eta_1' \le B^{15/\log\log B}$.

For $i = 1, \dots, 10$ we let Y_i be variables running over the set $\{2^n \mid n \ge -1\}$. By counting the number of $(\eta_1', \dots, \eta_{10}') \in \mathcal{T}'(B)$ which satisfy $Y_i < |\eta_i'| \le 2Y_i$ for $i = 1, \dots, 10$, we claim that [Browning 2006, Sections 6.1, 6.2] gives

$$\mathcal{M}(B) \ll B(\log B)^5 + \sum_{Y_i} X_0^{1/2} X_1^{1/6} X_2^{1/6} X_3^{1/6} + \sum_{Y_i} \max_{\{i,j,k\}=\{2,3,4\}} \left\{ \frac{Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 Y_8 Y_9 Y_{10}}{Y_{k+6} \max\{Y_i Y_{i+3}^2 Y_{i+6}, Y_j Y_{j+3}^2 Y_{j+6}, Z_k\}} \right\}, \quad (5\text{-}3)$$

where the two sums are over the Y_i, $i = 1, \dots, 10$, subject to the inequalities

$$Y_8 Y_9 Y_{10} \le B, \quad (5\text{-}4)$$

$$Y_1^2 Y_2^2 Y_3 Y_4 Y_5^2 Y_8 \le B, \quad (5\text{-}5)$$

$$Y_1^2 Y_2 Y_3^2 Y_4 Y_6^2 Y_9 \le B, \quad (5\text{-}6)$$

$$Y_1^2 Y_2 Y_3 Y_4^2 Y_7^2 Y_{10} \le B, \quad (5\text{-}7)$$

and also

$$Y_1 \le B^{15/\log\log B}, \quad (5\text{-}8)$$

and where X_0, X_1, X_2, X_3 denote the left-hand sides of the inequalities (5-4), (5-5), (5-6) and (5-7) respectively, and finally, for $k \in \{2, 3, 4\}$, Z_k is defined by

$$Z_k = \begin{cases} Y_k Y_{k+3}^2 Y_{k+6} & \text{if } Y_k Y_{k+3}^2 Y_{k+6} \ge Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7, \\ 1 & \text{otherwise.} \end{cases}$$

Let us explain briefly how the upper bound (5-3) can be deduced from Browning's work without making use of the condition (5-8). It is useful to note that our variables Y_i, $i = 1, \dots, 10$, and X_j, $j = 0, \dots, 3$, correspond respectively to Browning's variables S_0, U_1, U_2, U_3, S_1, S_2, S_3, Y_1, Y_2, Y_3 and X_4, X_1, X_2, X_3. First, the second term of the right-hand side of [ibid., (6.26)] is equal to

$$\frac{(X_0 X_1 X_2 X_3)^{1/4}}{Y_1^{1/2}} \left(1 + \frac{\log B}{(Y_8 Y_9 Y_{10})^{1/16}} \max_{k\in\{2,3,4\}} Y_{k+6}^{1/16} \right)$$

in our notation, and is easily seen to have overall contribution $B(\log B)^5$. As a result, the right side of [ibid., (6.29)] can actually be replaced by (in our notation)

$$B(\log B)^5 + \sum_{Y_i} X_0^{1/2} X_1^{1/6} X_2^{1/6} X_3^{1/6}. \quad (5\text{-}9)$$

Taking into account [ibid., (6.31)], we see that the right-hand side of the upper bound in [ibid., Proposition 4] can also be replaced by (5-9). Then, we note that the first term of the right-hand side of the upper bound in [ibid., Lemma 13] has overall contribution $B(\log B)^4$. This implies that the right-hand side of the upper bound in [ibid., Proposition 5] can be replaced by, in our notation,

$$B(\log B)^4 + \sum_{Y_i} \max_{\{i,j,k\}=\{2,3,4\}} \left\{ \frac{Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 Y_8 Y_9 Y_{10}}{Y_{k+6} \max\{Y_i Y_{i+3}^2 Y_{i+6}, Y_j Y_{j+3}^2 Y_{j+6}, Z_k\}} \right\}.$$

This concludes the proof of the upper bound (5-3).

Let us denote by $\mathcal{N}_1(B)$ and $\mathcal{N}_2(B)$ the respective contributions of the two sums in (5-3). In the following estimations, the notation $\sum_{\widehat{Y}_j}$ indicates that the summation is over all the Y_i with $i \neq j$. We start by investigating the quantity $\mathcal{N}_1(B)$ by summing over Y_5, Y_6 and Y_7 using, respectively, the conditions (5-5), (5-6) and (5-7). We get

$$\begin{aligned}\mathcal{N}_1(B) &= \sum_{Y_i} Y_1 Y_2^{2/3} Y_3^{2/3} Y_4^{2/3} Y_5^{1/3} Y_6^{1/3} Y_7^{1/3} Y_8^{2/3} Y_9^{2/3} Y_{10}^{2/3} \\ &\ll B^{1/2} \sum_{\widehat{Y}_5,\widehat{Y}_6,\widehat{Y}_7} Y_8^{1/2} Y_9^{1/2} Y_{10}^{1/2} \ll B \sum_{\widehat{Y}_5,\widehat{Y}_6,\widehat{Y}_7,\widehat{Y}_8} 1 \ll \frac{B(\log B)^6}{\log\log B},\end{aligned}$$

where we have used the condition (5-4) to sum over Y_8 and the condition (5-8) to sum over Y_1. We now deal with the quantity $\mathcal{N}_2(B)$. We only treat the case where $(i, j, k) = (2, 3, 4)$, since the others are all identical. Note that if $Z_4 = Y_4 Y_7^2 Y_{10}$ then $\mathcal{N}_2(B) \leq \mathcal{N}_1(B)$. Thus, we only need to deal with the case where $Z_4 = 1$. In addition, we proceed without loss of generality under the assumption that $Y_2 Y_5^2 Y_8 \leq Y_3 Y_6^2 Y_9$. We first use this condition to sum over Y_5, and then we sum over Y_7 and Y_8 using the conditions (5-7) and (5-4) respectively. We get

$$\begin{aligned}\mathcal{N}_2(B) &\ll \sum_{Y_i} Y_1 Y_2 Y_4 Y_5 Y_6^{-1} Y_7 Y_8 \ll \sum_{\widehat{Y}_5} Y_1 Y_2^{1/2} Y_3^{1/2} Y_4 Y_7 Y_8^{1/2} Y_9^{1/2} \\ &\ll B^{1/2} \sum_{\widehat{Y}_5,\widehat{Y}_7} Y_8^{1/2} Y_9^{1/2} Y_{10}^{-1/2} \ll B \sum_{\widehat{Y}_5,\widehat{Y}_7,\widehat{Y}_8} Y_{10}^{-1} \ll \frac{B(\log B)^6}{\log\log B},\end{aligned}$$

which completes the proof of Lemma 12. □

The following lemma proves that the contribution to $N_{U,H}(B)$ coming from those $(\eta_1, \ldots, \eta_{10}) \in \mathcal{T}(B)$ which are subject to the stronger condition

$$\eta_1^3 \eta_2^2 \eta_3^2 \eta_4^2 \eta_5 \eta_6 \eta_7 \leq \frac{B}{\log\log B},$$

is negligible.

Lemma 13. *Let $\mathcal{M}'(B)$ be the overall contribution to $N_{U,H}(B)$ coming from those $(\eta_1, \ldots, \eta_{10}) \in \mathcal{T}(B)$ such that*

$$\eta_1^3 \eta_2^2 \eta_3^2 \eta_4^2 \eta_5 \eta_6 \eta_7 \leq \frac{B}{\log\log B}.$$

We have

$$\mathcal{M}'(B) \ll \frac{B(\log B)^6}{(\log\log B)^{1/6}}.$$

Proof. We proceed as in the proof of Lemma 12, with the same notation. We have

$$\mathcal{M}'(B) \ll B(\log B)^5 + \sum_{Y_i} X_0^{1/2} X_1^{1/6} X_2^{1/6} X_3^{1/6} + \sum_{Y_i} \max_{\{i,j,k\}=\{2,3,4\}} \left\{ \frac{Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 Y_8 Y_9 Y_{10}}{Y_{k+6} \max\{Y_i Y_{i+3}^2 Y_{i+6}, Y_j Y_{j+3}^2 Y_{j+6}, Z_k\}} \right\}, \quad (5\text{-}10)$$

where the two sums are over the dyadic variables Y_i, $i = 1, \dots, 10$, subject to the inequalities (5-4)–(5-7) and

$$Y_1^3 Y_2^2 Y_3^2 Y_4^2 Y_5 Y_6 Y_7 \le \frac{B}{\log\log B}. \quad (5\text{-}11)$$

Let us denote by $\mathcal{N}_1'(B)$ and $\mathcal{N}_2'(B)$ the respective contributions of the two sums in (5-10). Combining conditions (5-4) and (5-5), we get

$$Y_1^{1/4} Y_2^{1/4} Y_3^{1/8} Y_4^{1/8} Y_5^{1/4} Y_8 Y_9^{7/8} Y_{10}^{7/8} \le B. \quad (5\text{-}12)$$

We start by bounding the contribution of the quantity $\mathcal{N}_1'(B)$ by summing successively over Y_8, Y_9 and Y_{10} using the conditions (5-12), (5-6) and (5-7) respectively. We deduce that

$$\begin{aligned}
\mathcal{N}_1'(B) &= \sum_{Y_i} Y_1 Y_2^{2/3} Y_3^{2/3} Y_4^{2/3} Y_5^{1/3} Y_6^{1/3} Y_7^{1/3} Y_8^{2/3} Y_9^{2/3} Y_{10}^{2/3} \\
&\ll B^{2/3} \sum_{\widehat{Y}_8} Y_1^{5/6} Y_2^{1/2} Y_3^{7/12} Y_4^{7/12} Y_5^{1/6} Y_6^{1/3} Y_7^{1/3} Y_9^{1/12} Y_{10}^{1/12} \\
&\ll B^{5/6} \sum_{\widehat{Y}_8, \widehat{Y}_9, \widehat{Y}_{10}} Y_1^{1/2} Y_2^{1/3} Y_3^{1/3} Y_4^{1/3} Y_5^{1/6} Y_6^{1/6} Y_7^{1/6} \\
&\ll \frac{B}{(\log\log B)^{1/6}} \sum_{\widehat{Y}_7, \widehat{Y}_8, \widehat{Y}_9, \widehat{Y}_{10}} 1 \ll \frac{B(\log B)^6}{(\log\log B)^{1/6}},
\end{aligned}$$

where we have summed over Y_7 using the condition (5-11). We now turn to the case of the quantity $\mathcal{N}_2'(B)$. As in the proof of Lemma 12, we only treat the case where $(i, j, k) = (2, 3, 4)$ and we work under the assumptions that $Z_4 = 1$ and thus

$$Y_4 Y_7^2 Y_{10} \le Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 \quad (5\text{-}13)$$

and $Y_2 Y_5^2 Y_8 \le Y_3 Y_6^2 Y_9$. Combining conditions (5-11) and (5-13), we get

$$Y_1^2 Y_2 Y_3 Y_4^2 Y_7^2 Y_{10} \le \frac{B}{\log\log B}. \quad (5\text{-}14)$$

We first use the condition $Y_2Y_5^2Y_8 \le Y_3Y_6^2Y_9$ to sum over Y_5, and then we sum over Y_8 and Y_7 using the conditions (5-4) and (5-14) respectively. We deduce

$$\begin{aligned}\mathcal{N}_2'(B) &\ll \sum_{Y_i} Y_1Y_2Y_4Y_5Y_6^{-1}Y_7Y_8 \ll \sum_{\widehat{Y}_5} Y_1Y_2^{1/2}Y_3^{1/2}Y_4Y_7Y_8^{1/2}Y_9^{1/2}\\ &\ll B^{1/2}\sum_{\widehat{Y}_5,\widehat{Y}_8} Y_1Y_2^{1/2}Y_3^{1/2}Y_4Y_7Y_{10}^{-1/2}\\ &\ll \frac{B}{(\log\log B)^{1/2}}\sum_{\widehat{Y}_5,\widehat{Y}_7,\widehat{Y}_8} Y_{10}^{-1} \ll \frac{B(\log B)^6}{(\log\log B)^{1/2}},\end{aligned}$$

which completes the proof of Lemma 13. □

5.2. ***Setting up.*** First, we recall that we have the following condition (given at the beginning of Section 5.1):

$$\eta_1^3\eta_2^2\eta_3^2\eta_4^2\eta_5\eta_6\eta_7 \le 3B. \tag{5-15}$$

It is easy to check that the symmetry between the three quantities $\eta_2\eta_5^2$, $\eta_3\eta_6^2$ and $\eta_4\eta_7^2$ is demonstrated by the action of $\mathfrak{S}_3$ on $\{(\eta_2,\eta_5,\eta_8),(\eta_3,\eta_6,\eta_9),(\eta_4,\eta_7,\eta_{10})\}$. Throughout the proof, we will assume that

$$\eta_4\eta_7^2 \le \eta_2\eta_5^2,\ \eta_3\eta_6^2.$$

The following lemma proves that we just need to multiply our future main term by a factor of 3 to take this new assumption into account.

Lemma 14. *Let $N_0(B)$ be the total number of $(\eta_1,\dots,\eta_{10}) \in \mathcal{T}(B)$ such that $\eta_2\eta_5^2 = \eta_4\eta_7^2$ or $\eta_3\eta_6^2 = \eta_4\eta_7^2$. We have the upper bound*

$$N_0(B) \ll B(\log B)^3.$$

Proof. By symmetry, we only need to treat the case of the condition $\eta_3\eta_6^2 = \eta_4\eta_7^2$. This equality and the condition $\gcd(\eta_3\eta_6, \eta_4\eta_7) = 1$ imply that $\eta_3 = \eta_4 = \eta_6 = \eta_7 = 1$. In this situation, the torsor equation is simply

$$\eta_2\eta_5^2\eta_8 + \eta_9 + \eta_{10} - \eta_1\eta_2\eta_5 = 0.$$

Thus, $N_0(B)$ is bounded by the number of $(\eta_1,\eta_2,\eta_5,\eta_8,\eta_9) \in \mathbb{Z}_{>0}^3 \times \mathbb{Z}_{\neq 0}^2$ satisfying

$$|\eta_8\eta_9|\,|\eta_2\eta_5^2\eta_8 + \eta_9 - \eta_1\eta_2\eta_5| \le B \quad \text{and} \quad \eta_1^2\eta_2^2\eta_5^2|\eta_8| \le B.$$

Using [Le Boudec 2012a, Lemma 1] to count the number of η_9 satisfying the first of these two inequalities, we obtain

$$N_0(B) \ll \sum_{\substack{\eta_1,\eta_2,\eta_5,\eta_8\\ \eta_1^2\eta_2^2\eta_5^2|\eta_8|\le B}} \left(\frac{B^{1/2}}{|\eta_8|^{1/2}} + 1\right) \ll B(\log B)^3,$$

as wished. □

Let $N(B)$ be the overall contribution of those $(\eta_1, \dots, \eta_{10}) \in \mathcal{T}(B)$ subject to the conditions

$$\eta_4\eta_7^2 \le \eta_2\eta_5^2,\ \eta_3\eta_6^2, \tag{5-16}$$

$$B^{15/\log\log B} \le \eta_1 \operatorname{sq}(\eta_2\eta_3\eta_4), \tag{5-17}$$

$$\frac{B}{\log\log B} \le \eta_1^3\eta_2^2\eta_3^2\eta_4^2\eta_5\eta_6\eta_7. \tag{5-18}$$

Lemmas 11–14 give us the following result:

Lemma 15. $$N_{U,H}(B) = 3N(B) + O\left(\frac{B(\log B)^6}{(\log\log B)^{1/6}}\right).$$

The end of the proof is devoted to the estimation of $N(B)$.

5.3. ***Application of Lemma 7.*** The idea of the proof is to view the equation (3-1) as a congruence modulo $\eta_4\eta_7^2$. For this, we replace η_{10} by its value given by the equation (3-1) in the height conditions (3-8) and (3-11). These conditions become

$$|\eta_8\eta_9|\,|\eta_2\eta_5^2\eta_8 + \eta_3\eta_6^2\eta_9 - \eta_1\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7| \le B\eta_4\eta_7^2,$$
$$\eta_1^2\eta_2\eta_3\eta_4\,|\eta_2\eta_5^2\eta_8 + \eta_3\eta_6^2\eta_9 - \eta_1\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7| \le B,$$

and we still denote them respectively by (3-8) and (3-11). From now on, we use the notation $\boldsymbol{\eta} = (\eta_2, \eta_3, \eta_4, \eta_5, \eta_6, \eta_7)$, and we set

$$\boldsymbol{\eta}^{(r_2,r_3,r_4,r_5,r_6,r_7)} = \eta_2^{r_2}\eta_3^{r_3}\eta_4^{r_4}\eta_5^{r_5}\eta_6^{r_6}\eta_7^{r_7}$$

for $(r_2, r_3, r_4, r_5, r_6, r_7) \in \mathbb{Q}^6$. We set

$$Y = \frac{B}{\eta_2\eta_3\eta_4}, \quad Z_1 = \frac{B^{1/3}}{\boldsymbol{\eta}^{(2/3,2/3,2/3,1/3,1/3,1/3)}}, \tag{5-19}$$

and, for brevity, $q_8 = \eta_2\eta_5^2$, $q_9 = \eta_3\eta_6^2$, $q_{10} = \eta_4\eta_7^2$. It is immediate to check that $\boldsymbol{\eta}$ is restricted to lie in the region $\mathcal{V}$ defined by

$$\mathcal{V} = \big\{\boldsymbol{\eta} \in \mathbb{Z}_{>0}^6 \mid Y(\log\log B)^{2/3} \ge q_8 Z_1^2,\ Y(\log\log B)^{2/3} \ge q_9 Z_1^2,$$
$$Z_1 \ge 3^{-1/3}, q_8 \ge q_{10}, q_9 \ge q_{10}\big\}. \tag{5-20}$$

We fix $\eta_1 \in \mathbb{Z}_{>0}$ and $\boldsymbol{\eta} \in \mathcal{V}$, subject to the conditions (5-15), (5-17) and (5-18) and to the coprimality conditions (3-5)–(3-7). Let $N(\eta_1, \boldsymbol{\eta}, B)$ be the number of $(\eta_8, \eta_9, \eta_{10}) \in \mathbb{Z}_{\ne 0}^3$ satisfying the equation (3-1), the height conditions (3-8)–(3-11), and finally the coprimality conditions (3-2)–(3-4). The goal of this section is to prove the following lemma:

Lemma 16. *We have the estimate*

$$N(\eta_1, \boldsymbol{\eta}, B) = \frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}} g_2\left(\frac{\eta_1}{Z_1}\right)\theta_1(\eta_1, \boldsymbol{\eta})\theta_2(\boldsymbol{\eta}) + R(\eta_1, \boldsymbol{\eta}, B),$$

where $\theta_1(\eta_1, \boldsymbol{\eta})$ *and* $\theta_2(\boldsymbol{\eta})$ *are arithmetic functions defined in* (5-28) *and* (5-29) *respectively and*

$$\sum_{\eta_1, \boldsymbol{\eta}} R(\eta_1, \boldsymbol{\eta}, B) \ll B(\log B)^5 (\log\log B)^{7/3}.$$

First, we see that since $\gcd(\eta_2\eta_5, \eta_3\eta_6\eta_9) = 1$ and $\gcd(\eta_3\eta_6, \eta_2\eta_5\eta_8) = 1$, the equation (3-1) proves that the coprimality condition (3-2) can be replaced by $\gcd(\eta_{10}, \eta_1\eta_4) = 1$. Let us remove the coprimality conditions $\gcd(\eta_8, \eta_6) = 1$ and $\gcd(\eta_9, \eta_5) = 1$ using Möbius inversions; we obtain

$$N(\eta_1, \boldsymbol{\eta}, B) = \sum_{\substack{k_8 \mid \eta_6 \\ \gcd(k_8, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \mu(k_8) \sum_{\substack{k_9 \mid \eta_5 \\ \gcd(k_9, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \mu(k_9) S_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B),$$

where $S_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B)$ is the cardinality of

$$\{(\eta_8', \eta_9', \eta_{10}) \in \mathbb{Z}^3_{\neq 0} \mid \eta_2\eta_5^2 k_8\eta_8' + \eta_3\eta_6^2 k_9\eta_9' + \eta_4\eta_7^2\eta_{10} = b,\ \gcd(\eta_{10}, \eta_1\eta_4) = 1,$$
$$\text{(3-8), (3-9), (3-10), (3-11)}, \gcd(\eta_8'\eta_9', \eta_1\eta_2\eta_3\eta_4\eta_7) = 1\},$$

and where we use the notation $\eta_8 = k_8\eta_8'$, $\eta_9 = k_9\eta_9'$ and $b = \eta_1\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7$.

From now on, we set

$$\mathscr{L} = B^{1/\log\log B}.$$

To take care of the error terms showing up in the application of Lemma 7, we need to show that the summations over k_8 and k_9 can be restricted to $k_8, k_9 \le \mathscr{L}^3$. To do so, let $N'(\eta_1, \boldsymbol{\eta}, B)$ be the contribution of $N(\eta_1, \boldsymbol{\eta}, B)$ under the assumption $k_8 > \mathscr{L}^3$; that is,

$$N'(\eta_1, \boldsymbol{\eta}, B) = \sum_{\substack{k_8 \mid \eta_6,\ k_8 > \mathscr{L}^3 \\ \gcd(k_8, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \sum_{\substack{k_9 \mid \eta_5 \\ \gcd(k_9, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} S_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B).$$

Let us write $\eta_6 = k_8\eta_6'$ and $\eta_5 = k_9\eta_5'$. We notice that the equation in the definition of $S_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B)$ implies that $k_8k_9 \mid \eta_{10}$, and thus we also write $\eta_{10} = k_8k_9\xi_{10}$. With this notation, we get

$$N'(\eta_1, \boldsymbol{\eta}, B) = \sum_{\substack{\mathscr{L}^3 < k_8 \le B^{1/2} \\ \gcd(k_8, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \sum_{\substack{k_9 \le B^{1/2} \\ \gcd(k_9, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} S'_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B),$$

where $S'_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B)$ is the cardinality of

$$\big\{(\eta_8', \eta_9', \xi_{10}) \in \mathbb{Z}^3_{\neq 0} \mid \eta_2\eta_5'^2 k_9\eta_8' + \eta_3\eta_6'^2 k_8\eta_9' + \eta_4\eta_7^2\xi_{10} = b',\ \gcd(\xi_{10}, \eta_1\eta_4) = 1,\\ \text{(3-8), (3-9), (3-10), (3-11)},\ \gcd(\eta_8'\eta_9', \eta_1\eta_2\eta_3\eta_4\eta_7) = 1\big\},$$

where we have set $b' = \eta_1\eta_2\eta_3\eta_4\eta_5'\eta_6'\eta_7$. Let us split the summations over k_8 and k_9 into dyadic ranges. Let us assume that $K_8, K_9 \geq \frac{1}{2}$ and that $K_8 < k_8 \leq 2K_8$ and $K_9 < k_9 \leq 2K_9$. Let us set $\xi_8 = k_9\eta_8'$ and $\xi_9 = k_8\eta_9'$. The height conditions (3-8), (3-9), (3-10) and (3-11) imply respectively

$$|\xi_8\xi_9\xi_{10}| \leq \frac{B}{K_8K_9}, \tag{5-21}$$

$$\eta_1^2\eta_2^2\eta_3\eta_4\eta_5'^2|\xi_8| \leq \frac{B}{K_8K_9}, \tag{5-22}$$

$$\eta_1^2\eta_2\eta_3^2\eta_4\eta_6'^2|\xi_9| \leq \frac{B}{K_8K_9}, \tag{5-23}$$

$$\eta_1^2\eta_2\eta_3\eta_4^2\eta_7^2|\xi_{10}| \leq \frac{B}{K_8K_9}. \tag{5-24}$$

We thus have, for $K_8 < k_8 \leq 2K_8$ and $K_9 < k_9 \leq 2K_9$,

$$S'_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B)\\ \ll \#\big\{(\xi_8, \xi_9, \xi_{10}) \in \mathbb{Z}^3_{\neq 0} \mid k_8 \mid \xi_9,\ k_9 \mid \xi_8,\ \eta_2\eta_5'^2\xi_8 + \eta_3\eta_6'^2\xi_9 + \eta_4\eta_7^2\xi_{10} = b',\\ \text{(5-21), (5-22), (5-23), (5-24)},\ \gcd(\xi_{10}, \eta_1\eta_4) = 1,\ \gcd(\xi_8\xi_9, \eta_1\eta_2\eta_3\eta_4\eta_7) = 1\big\}.$$

Therefore, using the standard bound for the divisor function,

$$\tau(n) \ll n^{1/\log\log(3n)},$$

for $n \geq 1$, we get

$$\sum_{\substack{K_8 < k_8 \leq 2K_8\\ K_9 < k_9 \leq 2K_9}} S'_{k_8,k_9}(\eta_1, \boldsymbol{\eta}, B) \ll \mathscr{L}^2 S_{K_8,K_9},$$

where $S_{K_8,K_9} = S_{K_8,K_9}(\eta_1, \eta_2, \eta_3, \eta_4, \eta_5', \eta_6', \eta_7, B)$ is the cardinality of

$$\big\{(\xi_8, \xi_9, \xi_{10}) \in \mathbb{Z}^3_{\neq 0} \mid \eta_2\eta_5'^2\xi_8 + \eta_3\eta_6'^2\xi_9 + \eta_4\eta_7^2\xi_{10} = b',\ \text{(5-21), (5-22), (5-23), (5-24)},\\ \gcd(\xi_{10}, \eta_1\eta_4) = 1,\ \gcd(\xi_8\xi_9, \eta_1\eta_2\eta_3\eta_4\eta_7) = 1\big\}.$$

Setting $\xi_{6,8} = \gcd(\eta_6', \xi_8)$ and $\xi_{5,9} = \gcd(\eta_5', \xi_9)$, we see that $\xi_{6,8}\xi_{5,9} \mid \xi_{10}$, and we thus obtain

$$\sum_{\eta_1,\eta_2,\eta_3,\eta_4,\eta_5',\eta_6',\eta_7} S_{K_8,K_9} \ll \sum_{\xi_{6,8},\xi_{5,9} \leq B} N_{U,H}\left(\frac{B}{K_8K_9\xi_{6,8}\xi_{5,9}}\right).$$

Therefore, we can apply [Browning 2006]. We get

$$\sum_{\eta_1,\boldsymbol{\eta}} N'(\eta_1,\boldsymbol{\eta},B) \ll \mathscr{L}^2 \sum_{\substack{\mathscr{L}^3<K_8<B^{1/2}\\ K_9<B^{1/2}}} \sum_{\xi_{6,8},\xi_{5,9}\le B} \frac{B(\log B)^6}{K_8K_9\xi_{6,8}\xi_{5,9}} \ll B\mathscr{L}^{-1/2},$$

which is satisfactory. Therefore, we can restrict from now on the summations over k_8 and k_9 as we wished.

We note that if we allow $\eta_{10}=0$ in the definition of the cardinality $S_{k_8,k_9}(\eta_1,\boldsymbol{\eta},B)$ then the coprimality condition $\gcd(\eta_{10},\eta_1\eta_4)=1$ implies $\eta_1=\eta_4=1$. Moreover, the equation $\eta_2\eta_5^2k_8\eta_8'+\eta_3\eta_6^2k_9\eta_9'=\eta_2\eta_3\eta_5\eta_6\eta_7$ also implies $\eta_2=\eta_3=1$. These restrictions are in contradiction with the condition (5-17), so from now on, we allow η_{10} to vanish in the definition of $S_{k_8,k_9}(\eta_1,\boldsymbol{\eta},B)$. Let us now remove the coprimality condition $\gcd(\eta_{10},\eta_1\eta_4)=1$ using a Möbius inversion. We get that the main term of $N(\eta_1,\boldsymbol{\eta},B)$ is equal to

$$\sum_{\substack{k_8\mid\eta_6,\ k_8\le\mathscr{L}^3\\ \gcd(k_8,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \mu(k_8) \sum_{\substack{k_9\mid\eta_5,\ k_9\le\mathscr{L}^3\\ \gcd(k_9,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \mu(k_9) \sum_{k_{10}\mid\eta_1\eta_4} \mu(k_{10}) S_{k_8,k_9,k_{10}}(\eta_1,\boldsymbol{\eta},B),$$

where $S_{k_8,k_9,k_{10}}(\eta_1,\boldsymbol{\eta},B)$ denotes the cardinality of

$$\big\{(\eta_8',\eta_9',\eta_{10}')\in\mathbb{Z}^2_{\neq0}\times\mathbb{Z} \;\big|\; \eta_2\eta_5^2k_8\eta_8'+\eta_3\eta_6^2k_9\eta_9'+\eta_4\eta_7^2k_{10}\eta_{10}'=b,\\ \text{(3-8), (3-9), (3-10), (3-11)}, \gcd(\eta_8'\eta_9',\eta_1\eta_2\eta_3\eta_4\eta_7)=1\big\}.$$

Since $\gcd(\eta_1\eta_4,k_8k_9\eta_5\eta_6\eta_8'\eta_9')=1$, we have $\gcd(k_{10},k_8k_9\eta_5\eta_6\eta_8'\eta_9')=1$. Also, the two conditions $\gcd(\eta_2\eta_5k_8\eta_8',\eta_3)=1$ and $\gcd(\eta_3\eta_6k_9\eta_9',\eta_2)=1$ imply that we also have $\gcd(k_{10},\eta_2\eta_3)=1$. We now remove the coprimality conditions $\gcd(\eta_8'\eta_9',\eta_1\eta_2\eta_3)=1$ using Möbius inversions. Setting $\eta_8'=\ell_8\eta_8''$ and $\eta_9'=\ell_9\eta_9''$, we obtain that the main term of $N(\eta_1,\boldsymbol{\eta},B)$ is equal to

$$\sum_{\substack{k_8\mid\eta_6,\ k_8\le\mathscr{L}^3\\ \gcd(k_8,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \mu(k_8) \sum_{\substack{k_9\mid\eta_5,\ k_9\le\mathscr{L}^3\\ \gcd(k_9,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \mu(k_9)\\ \times \sum_{\substack{k_{10}\mid\eta_1\eta_4\\ \gcd(k_{10},k_8k_9\eta_2\eta_3\eta_5\eta_6)=1}} \mu(k_{10}) \sum_{\substack{\ell_8,\ell_9\mid\eta_1\eta_2\eta_3\\ \gcd(\ell_8\ell_9,k_{10}\eta_4\eta_7)=1}} \mu(\ell_8)\mu(\ell_9) S(\eta_1,\boldsymbol{\eta},B),$$

where $S(\eta_1,\boldsymbol{\eta},B)$ denotes the cardinality of

$$\big\{(\eta_8'',\eta_9'')\in\mathbb{Z}^2_{\neq0} \;\big|\; \eta_2\eta_5^2k_8\ell_8\eta_8''+\eta_3\eta_6^2k_9\ell_9\eta_9''\equiv b \pmod{k_{10}\eta_4\eta_7^2},\\ \text{(3-8), (3-9), (3-10), (3-11)}, \gcd(\eta_8''\eta_9'',k_{10}\eta_4\eta_7)=1\big\}.$$

Note that we have replaced the equation $\eta_2\eta_5^2k_8\ell_8\eta_8''+\eta_3\eta_6^2k_9\ell_9\eta_9''+\eta_4\eta_7^2k_{10}\eta_{10}'=b$ by a congruence.

Setting

$$X=\frac{B}{\eta_1^2\boldsymbol{\eta}^{(1,1,1,0,0,0)}},\quad T=\eta_1\boldsymbol{\eta}^{(1,1,1,1,1,1)},$$

and $A_1=k_8\ell_8\eta_2\eta_5^2$, $A_2=k_9\ell_9\eta_3\eta_6^2$ and recalling the equality (2-21), it is immediate to check that $(\eta_8'',\eta_9'')\in\mathbb{Z}^2_{\neq 0}$ is subject to the height conditions (3-8)–(3-11) if and only if $(\eta_8'',\eta_9'')\in\mathcal{S}\cap\mathbb{Z}^2_{\neq 0}$. Setting $\mathcal{L}=\log\log B$, we see that the condition (5-18) can be rewritten $X/\mathcal{L}\le T$. We can therefore apply Lemma 7 with $L=\log B$, $q=k_{10}\eta_4\eta_7^2$ and $\boldsymbol{a}=(k_8\ell_8\eta_2\eta_5^2,k_9\ell_9\eta_3\eta_6^2)$. Recall the definitions (2-24) of φ^* and (5-19) of Z_1 and also the definitions of $E(q,\boldsymbol{a})$ and $E_2(q)$, given in Lemmas 2 and 6 respectively . We obtain

$$S(\eta_1,\boldsymbol{\eta},B)-\frac{\varphi^*(k_{10}\eta_4\eta_7)}{k_8\ell_8k_9\ell_9k_{10}}\frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}}g_2\Big(\frac{\eta_1}{Z_1}\Big)\ll\mathscr{E}+\mathscr{E}',$$

where

$$\mathscr{E}=(\log B)^6E(q,\boldsymbol{a})$$

and

$$\mathscr{E}'=\frac{B^{2/3}}{k_8\ell_8k_9\ell_9k_{10}\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}}\mathcal{L}^{4/3}\times\Big(\frac{\mathcal{L}}{\log B}+\frac{k_8^{1/2}\ell_8^{1/2}\eta_1\eta_2\eta_3^{1/2}\eta_4^{1/2}\eta_5}{B^{1/2}}+\frac{k_9^{1/2}\ell_9^{1/2}\eta_1\eta_2^{1/2}\eta_3\eta_4^{1/2}\eta_6}{B^{1/2}}\Big)E_2(q).$$

Let us estimate the contribution of these error terms. Let us start by bounding the overall contribution of $\mathscr{E}$. For this, we write $\eta_5=k_9\eta_5'$ and $\eta_6=k_8\eta_6'$, and we let Y_5, Y_6 and Y_7 be variables running over the set $\{2^n\mid n\ge -1\}$. We define $\mathcal{N}=\mathcal{N}(Y_5,Y_6,Y_7)$ as the sum over η_5', η_6', $\eta_7\in\mathbb{Z}_{\ge 1}$ satisfying $Y_5<k_9\eta_5'\le 2Y_5$, $Y_6<k_8\eta_6'\le 2Y_6$ and $Y_7<\eta_7\le 2Y_7$ and the coprimality conditions $\gcd(\eta_5'\eta_6',\eta_4\eta_7)=1$ and $\gcd(\eta_5',\eta_6')=1$, of the quantity

$$\sum_{\substack{k_8,k_9\le\mathcal{L}^3\\ \gcd(k_8k_9,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}}\ \sum_{\substack{k_{10}\mid\eta_1\eta_4\\ \gcd(k_{10},k_8k_9\eta_2\eta_3\eta_5'\eta_6')=1}}\ \sum_{\substack{\ell_8,\ell_9\mid\eta_1\eta_2\eta_3\\ \gcd(\ell_8\ell_9,k_{10}\eta_4\eta_7)=1}}(\log B)^6E(q,\boldsymbol{a}'),$$

where $\boldsymbol{a}'=(k_9\ell_8\eta_2\eta_5'^2,k_8\ell_9\eta_3\eta_6'^2)$. We now aim to bound the contribution of the error term $\mathscr{E}$ by first estimating the quantity $\mathcal{N}$ and then by summing $\mathcal{N}$ over η_1, η_2, η_3 and η_4 and over all the possible values for Y_5, Y_6 and Y_7. Note that the variables

Y_5, Y_6 and Y_7 satisfy the inequalities

$$\eta_1^3\eta_2^2\eta_3^2\eta_4^2 Y_5Y_6Y_7 \le 3B, \tag{5-25}$$

$$\eta_4 Y_7^2 \le 4\eta_2 Y_5^2, \tag{5-26}$$

$$\eta_4 Y_7^2 \le 4\eta_3 Y_6^2. \tag{5-27}$$

Applying Lemma 9 to sum over η_5' and η_6' and recalling that $q = k_{10}\eta_4\eta_7^2$, we see that

$$\begin{aligned}\mathcal{N} &\ll (\log B)^6 \sum_{Y_7<\eta_7\le 2Y_7} \sum_{k_8,k_9\le \mathscr{L}^3} \sum_{k_{10}\mid \eta_1\eta_4} \sum_{\ell_8,\ell_9\mid \eta_1\eta_2\eta_3} \left(\frac{Y_5Y_6}{k_8k_9} + k_{10}\eta_4\eta_7^2\right)\tau(q)^2 E_1(q)\\ &\ll \mathscr{L}^7 \sum_{Y_7<\eta_7\le 2Y_7} \tau(\eta_1\eta_4)\tau(\eta_1\eta_2\eta_3)^2\tau(\eta_1\eta_4^2\eta_7^2)^2(Y_5Y_6 + \eta_1\eta_4^2\eta_7^2)\\ &\ll \mathscr{L}^{12}(Y_5Y_6Y_7 + \eta_1\eta_4^2Y_7^3).\end{aligned}$$

Using the two conditions (5-26) and (5-27), we finally obtain

$$\mathcal{N} \ll \mathscr{L}^{12}\eta_1\eta_2^{1/2}\eta_3^{1/2}\eta_4 Y_5Y_6Y_7.$$

We now aim to sum this quantity over all the possible values for Y_5, Y_6 and Y_7. Let us start by summing over Y_7 using the condition (5-25) and then over η_1 using the condition (5-17); we obtain

$$\begin{aligned}\sum_{Y_i}\mathcal{N} &\ll \mathscr{L}^{12} \sum_{\eta_1,\eta_2,\eta_3,\eta_4,Y_5,Y_6,Y_7} \eta_1\eta_2^{1/2}\eta_3^{1/2}\eta_4 Y_5Y_6Y_7\\ &\ll B\mathscr{L}^{13} \sum_{\eta_1,\eta_2,\eta_3,\eta_4} \frac{1}{\eta_1^2\eta_2^{3/2}\eta_3^{3/2}\eta_4} \ll B\mathscr{L}^{-2} \sum_{\eta_2,\eta_3,\eta_4} \frac{\mathrm{sq}(\eta_2\eta_3\eta_4)}{\eta_2^{3/2}\eta_3^{3/2}\eta_4}\\ &\ll B\mathscr{L}^{-1},\end{aligned}$$

which is satisfactory. In addition, the overall contributions of the three terms of the error term $\mathscr{E}'$ are easily seen to be bounded by $B(\log B)^5(\log\log B)^{7/3}$, which is also satisfactory.

Therefore, the main term of $N(\eta_1, \boldsymbol{\eta}, B)$ is equal to

$$\sum_{\substack{k_8\mid\eta_6,\ k_8\le\mathscr{L}^3\\ \gcd(k_8,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \frac{\mu(k_8)}{k_8} \sum_{\substack{k_9\mid\eta_5,\ k_9\le\mathscr{L}^3\\ \gcd(k_9,\eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \frac{\mu(k_9)}{k_9} \sum_{\substack{k_{10}\mid\eta_1\eta_4\\ \gcd(k_{10},k_8k_9\eta_2\eta_3\eta_5\eta_6)=1}} \frac{\mu(k_{10})}{k_{10}}$$
$$\times \sum_{\substack{\ell_8,\ell_9\mid\eta_1\eta_2\eta_3\\ \gcd(\ell_8\ell_9,k_{10}\eta_4\eta_7)=1}} \frac{\mu(\ell_8)}{\ell_8}\frac{\mu(\ell_9)}{\ell_9}\varphi^*(k_{10}\eta_4\eta_7)\frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}} g_2\left(\frac{\eta_1}{Z_1}\right).$$

Using the bound of Lemma 5 for g_2, we see that this quantity is

$$\ll \sum_{\substack{k_8 \mid \eta_6,\, k_9 \mid \eta_5 \\ k_8, k_9 \leq \mathscr{L}^3}} \frac{1}{k_8}\frac{1}{k_9}\sigma_{-1}(\eta_1\eta_4)\sigma_{-1}(\eta_1\eta_2\eta_3)^2 \frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}}.$$

As a result, we see that if we remove the conditions $k_8, k_9 \leq \mathscr{L}^3$ from the sums over k_8 and k_9, we create an error term whose overall contribution is, for instance, seen to be bounded by $B\mathscr{L}^{-1}$. Thus, we have proved that we can write

$$N(\eta_1, \boldsymbol{\eta}, B) = M(\eta_1, \boldsymbol{\eta}, B) + R(\eta_1, \boldsymbol{\eta}, B),$$

where

$$\sum_{\eta_1, \boldsymbol{\eta}} R(\eta_1, \boldsymbol{\eta}, B) \ll B(\log B)^5(\log\log B)^{7/3},$$

and

$$M(\eta_1, \boldsymbol{\eta}, B) = \frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}}\, g_2\Big(\frac{\eta_1}{Z_1}\Big)\theta(\eta_1, \boldsymbol{\eta}),$$

where

$$\begin{aligned}\theta(\eta_1, \boldsymbol{\eta}) = {} & \sum_{\substack{k_8 \mid \eta_6 \\ \gcd(k_8, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \frac{\mu(k_8)}{k_8} \sum_{\substack{k_9 \mid \eta_5 \\ \gcd(k_9, \eta_1\eta_2\eta_3\eta_4\eta_7)=1}} \frac{\mu(k_9)}{k_9} \\ & \times \sum_{\substack{k_{10} \mid \eta_1\eta_4 \\ \gcd(k_{10}, k_8k_9\eta_2\eta_3\eta_5\eta_6)=1}} \frac{\mu(k_{10})}{k_{10}} \sum_{\substack{\ell_8, \ell_9 \mid \eta_1\eta_2\eta_3 \\ \gcd(\ell_8\ell_9, k_{10}\eta_4\eta_7)=1}} \frac{\mu(\ell_8)}{\ell_8}\frac{\mu(\ell_9)}{\ell_9}\varphi^*(k_{10}\eta_4\eta_7) \\ = {} & \frac{\varphi^*(\eta_3\eta_6)}{\varphi^*(\eta_3)}\frac{\varphi^*(\eta_2\eta_5)}{\varphi^*(\eta_2)}\varphi^*(\eta_1\eta_2\eta_3\eta_4\eta_7)^2 \sum_{\substack{k_{10} \mid \eta_1\eta_4 \\ \gcd(k_{10}, \eta_2\eta_3\eta_5\eta_6)=1}} \frac{\mu(k_{10})}{k_{10}\varphi^*(\eta_4\eta_7k_{10})}.\end{aligned}$$

It is easy to check that for $a, b, c \geq 1$, we have

$$\sum_{\substack{k \mid a \\ \gcd(k,c)=1}} \frac{\mu(k)}{k\varphi^*(kb)} = \frac{\varphi^*(\gcd(a,b))}{\varphi^*(b)\varphi^*(\gcd(a,b,c))} \prod_{\substack{p \mid a \\ p \nmid bc}} \Big(1 - \frac{1}{p-1}\Big).$$

Using this equality and the remaining coprimality conditions (3-5), (3-6) and (3-7) and recalling the definition (2-26) of ψ, we see that we can write

$$\theta(\eta_1, \boldsymbol{\eta}) = \theta_1(\eta_1, \boldsymbol{\eta})\theta_2(\boldsymbol{\eta}),$$

where

$$\theta_1(\eta_1, \boldsymbol{\eta}) = \psi_{\eta_2\eta_3\eta_4}(\eta_1), \tag{5-28}$$

and

$$\theta_2(\boldsymbol{\eta}) = \varphi^*(\eta_2\eta_3\eta_4)\varphi^*(\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7). \tag{5-29}$$

5.4. ***Summation over η_1.*** We now need to sum the main term of $N(\eta_1, \boldsymbol{\eta}, B)$ over $\eta_1 \in \mathbb{Z}_{>0}$, where η_1 is subject to the conditions (5-17) and (5-18) (the condition (5-15) is implied by the definition of g_2) and to the coprimality condition (3-5). We start by proving that we can remove the restrictions that η_1 satisfies the conditions (5-17) and (5-18). Indeed, let us first assume that we have the condition

$$\eta_1 \operatorname{sq}(\eta_2\eta_3\eta_4) < B^{15/\log\log B}. \tag{5-30}$$

The bound of Lemma 5 for g_2 implies that the main term $M(\eta_1, \boldsymbol{\eta}, B)$ of $N(\eta_1, \boldsymbol{\eta}, B)$ satisfies

$$M(\eta_1, \boldsymbol{\eta}, B) \ll \frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}}.$$

Let us now sum this quantity over η_7 using the condition (5-15) and then over η_1 using the condition (5-30); we obtain

$$\begin{aligned}\sum_{\eta_1,\boldsymbol{\eta}} M(\eta_1, \boldsymbol{\eta}, B) &\ll \sum_{\eta_1,\eta_2,\eta_3,\eta_4,\eta_5,\eta_6} \frac{B}{\eta_1\boldsymbol{\eta}^{(1,1,1,1,1,0)}} \\ &\ll \sum_{\eta_2,\eta_3,\eta_4,\eta_5,\eta_6} \frac{B(\log B)}{\boldsymbol{\eta}^{(1,1,1,1,1,0)}\log\log B} \ll \frac{B(\log B)^6}{\log\log B}.\end{aligned}$$

This error term is satisfactory. Let us now assume that we have the condition

$$\eta_1^3\eta_2^2\eta_3^2\eta_4^2\eta_5\eta_6\eta_7 < \frac{B}{\log\log B}.$$

Let us sum over η_1 using this condition; we get

$$\sum_{\eta_1,\boldsymbol{\eta}} M(\eta_1, \boldsymbol{\eta}, B) \ll \sum_{\boldsymbol{\eta}} \frac{B}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}(\log\log B)^{1/3}} \ll \frac{B(\log B)^6}{(\log\log B)^{1/3}}.$$

This error term is also satisfactory. We can thus remove the restrictions that η_1 satisfies the conditions (5-17) and (5-18), and we proceed to sum over η_1. Recall the definition (5-20) of $\mathscr{V}$. For fixed $\boldsymbol{\eta} \in \mathscr{V}$ satisfying the coprimality conditions (3-6) and (3-7), let $N(\boldsymbol{\eta}, B)$ be the sum of the main term of $N(\eta_1, \boldsymbol{\eta}, B)$ over η_1, where η_1 is subject to the coprimality condition (3-5). Recall the definition (2-27) of Υ. We now prove the following lemma.

Lemma 17. *We have the estimate*

$$N(\boldsymbol{\eta}, B) = \Upsilon\frac{\omega_\infty}{3}\frac{B}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}}\Theta(\boldsymbol{\eta}) + R(\boldsymbol{\eta}, B),$$

where $\Theta(\boldsymbol{\eta})$ is a certain arithmetic function defined in (5-31) *and where*

$$\sum_{\boldsymbol{\eta}} R(\boldsymbol{\eta}, B) \ll B(\log B)^5.$$

Proof. Let us use Lemma 10 to sum over η_1. For any fixed $0 < \gamma \leq 1$, we obtain

$$N(\boldsymbol{\eta}, B) = \Upsilon \frac{B}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}} \Theta(\boldsymbol{\eta}) \int_{t>0} g_2(t)\,\mathrm{d}t + O\bigg(\frac{B^{2/3}}{\boldsymbol{\eta}^{(1/3,1/3,1/3,2/3,2/3,2/3)}} Z_1^{\gamma} \sigma_{-\gamma/2}(\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7) \sup_{t>0} g_2(t) \bigg),$$

where

$$\Theta(\boldsymbol{\eta}) = \varphi^*(\eta_2\eta_3\eta_4)\varphi^*(\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7)\varphi^*(\eta_5\eta_6\eta_7)\varphi^{\Upsilon}(\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7). \quad (5\text{-}31)$$

Let us set $\gamma = 1/2$. Using the bound of Lemma 5 for g_2, we deduce that the overall contribution of this error term is

$$\sum_{\boldsymbol{\eta}} \frac{B^{5/6}}{\boldsymbol{\eta}^{(2/3,2/3,2/3,5/6,5/6,5/6)}} \sigma_{-1/4}(\eta_2\eta_3\eta_4\eta_5\eta_6\eta_7) \ll B(\log B)^5,$$

where we have summed over $\boldsymbol{\eta}$ using the condition $Z_1 \geq 3^{-1/3}$. Recalling the definition of g_2 and the equality (4-1), we see that

$$\int_{t>0} g_2(t)\,\mathrm{d}t = \frac{\omega_\infty}{3},$$

which completes the proof. □

5.5. ***Conclusion.*** It remains to sum the main term of $N(\boldsymbol{\eta}, B)$ over the $\boldsymbol{\eta} \in \mathcal{V}$ satisfying the coprimality conditions (3-6) and (3-7). It is easy to see that replacing $\mathcal{V}$ by the region

$$\mathcal{V}' = \big\{ \boldsymbol{\eta} \in \mathbb{Z}_{>0}^6 \;\big|\; Y \geq q_8 Z_1^2,\ Y \geq q_9 Z_1^2,\ Z_1 \geq 1,\ q_8 \geq q_{10},\ q_9 \geq q_{10} \big\}$$

produces an error term whose overall contribution is $\ll B(\log B)^5 \log\log\log B$. Let us redefine the arithmetic function Θ as being equal to zero if the remaining coprimality conditions (3-6) and (3-7) are not satisfied. Recalling Lemma 15, we see that we have proved the following lemma:

Lemma 18. *We have the estimate*

$$N_{U,H}(B) = \Upsilon\omega_\infty B \sum_{\boldsymbol{\eta}\in\mathcal{V}'} \frac{\Theta(\boldsymbol{\eta})}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}} + O\bigg(\frac{B(\log B)^6}{(\log\log B)^{1/6}} \bigg).$$

The end of the paper is dedicated to the completion of the proof of Theorem 1. Let us introduce the generalized Möbius function $\boldsymbol{\mu}$ defined for $(n_1, \ldots, n_6) \in \mathbb{Z}_{>0}^6$ by $\boldsymbol{\mu}(n_1, \ldots, n_6) = \mu(n_1)\cdots\mu(n_6)$. We set $\boldsymbol{k} = (k_2, k_3, k_4, k_5, k_6, k_7)$ and we define for $s \in \mathbb{C}$, such that $\Re(s) > 1$,

$$F(s)=\sum_{\boldsymbol{\eta}\in\mathbb{Z}^6_{>0}}\frac{|(\Theta*\boldsymbol{\mu})(\boldsymbol{\eta})|}{\eta_2^s\eta_3^s\eta_4^s\eta_5^s\eta_6^s\eta_7^s}=\prod_p\Bigg(\sum_{\boldsymbol{k}\in\mathbb{Z}^6_{\geq 0}}\frac{|(\Theta*\boldsymbol{\mu})(p^{k_2},p^{k_3},p^{k_4},p^{k_5},p^{k_6},p^{k_7})|}{p^{k_2s}p^{k_3s}p^{k_4s}p^{k_5s}p^{k_6s}p^{k_7s}}\Bigg).$$

It is easy to check that if $\boldsymbol{k}\notin\{0,1\}^6$ then $(\Theta*\boldsymbol{\mu})(p^{k_2},p^{k_3},p^{k_4},p^{k_5},p^{k_6},p^{k_7})=0$ and if exactly one of the k_i is equal to 1, then $(\Theta*\boldsymbol{\mu})(p^{k_2},p^{k_3},p^{k_4},p^{k_5},p^{k_6},p^{k_7})\ll 1/p$, so the local factors F_p of F satisfy

$$F_p(s)=1+O\bigg(\frac{1}{p^{\min(\Re(s)+1,2\Re(s))}}\bigg).$$

This proves that the function F converges in the half-plane $\Re(s)>1/2$, which implies that Θ satisfies the assumption of [Le Boudec 2012b, Lemma 8]. The application of this lemma provides

$$\sum_{\boldsymbol{\eta}\in\mathcal{V}'}\frac{\Theta(\boldsymbol{\eta})}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}}=\alpha\Bigg(\sum_{\boldsymbol{\eta}\in\mathbb{Z}^6_{>0}}\frac{(\Theta*\boldsymbol{\mu})(\boldsymbol{\eta})}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}}\Bigg)(\log B)^6+O((\log B)^5),\tag{5-32}$$

where α is the volume of the polytope defined in $\mathbb{R}^6$ by $t_2,t_3,t_4,t_5,t_6,t_7\geq 0$ and

$$\begin{aligned}2t_2-t_3-t_4+4t_5-2t_6-2t_7&\leq 1,\\ -t_2+2t_3-t_4-2t_5+4t_6-2t_7&\leq 1,\\ 2t_2+2t_3+2t_4+t_5+t_6+t_7&\leq 1,\\ -t_2+t_4-2t_5+2t_7&\leq 0,\\ -t_3+t_4-2t_6+2t_7&\leq 0.\end{aligned}$$

It is easy to compute α using Franz's additional Maple package `Convex` [2009]. We find $\alpha=1/23040$; that is,

$$\alpha=\alpha(\widetilde{V}).\tag{5-33}$$

Furthermore, we have

$$\begin{aligned}\sum_{\boldsymbol{\eta}\in\mathbb{Z}^6_{>0}}\frac{(\Theta*\boldsymbol{\mu})(\boldsymbol{\eta})}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}}&=\prod_p\Bigg(\sum_{\boldsymbol{k}\in\mathbb{Z}^6_{\geq 0}}\frac{(\Theta*\boldsymbol{\mu})(p^{k_2},p^{k_3},p^{k_4},p^{k_5},p^{k_6},p^{k_7})}{p^{k_2}p^{k_3}p^{k_4}p^{k_5}p^{k_6}p^{k_7}}\Bigg)\\ &=\prod_p\bigg(1-\frac{1}{p}\bigg)^6\Bigg(\sum_{\boldsymbol{k}\in\mathbb{Z}^6_{\geq 0}}\frac{\Theta(p^{k_2},p^{k_3},p^{k_4},p^{k_5},p^{k_6},p^{k_7})}{p^{k_2}p^{k_3}p^{k_4}p^{k_5}p^{k_6}p^{k_7}}\Bigg).\end{aligned}$$

The calculation of these local factors is straightforward, and we find

$$\sum_{\boldsymbol{k}\in\mathbb{Z}^6_{\geq 0}}\frac{\Theta(p^{k_2},p^{k_3},p^{k_4},p^{k_5},p^{k_6},p^{k_7})}{p^{k_2}p^{k_3}p^{k_4}p^{k_5}p^{k_6}p^{k_7}}=\varphi^{\curlyvee}(p)\bigg(1-\frac{1}{p}\bigg)\bigg(1+\frac{7}{p}+\frac{1}{p^2}\bigg).$$

We finally obtain

$$\sum_{\boldsymbol{\eta}\in\mathbb{Z}^6_{>0}} \frac{(\Theta * \boldsymbol{\mu})(\boldsymbol{\eta})}{\boldsymbol{\eta}^{(1,1,1,1,1,1)}} = \Upsilon^{-1} \prod_p \left(1 - \frac{1}{p}\right)^7 \omega_p. \tag{5-34}$$

Putting together the equalities (5-32)–(5-34) and Lemma 18 completes the proof of Theorem 1.

Acknowledgments

It is a great pleasure for the author to thank his supervisor Professor de la Bretèche for his advice during the preparation of this work. The author is also grateful to Professor Browning for his careful reading of an earlier version of the manuscript.

This work has benefited from the financial support of the ANR PEPR (Points Entiers Points Rationnels).

References

[Baier and Derenthal 2012] S. Baier and U. Derenthal, "Quadratic congruences on average and rational points on cubic surfaces", preprint, 2012. arXiv 1205.0373v2

[Batyrev and Tschinkel 1998a] V. V. Batyrev and Y. Tschinkel, "Manin's conjecture for toric varieties", *J. Algebraic Geom.* **7**:1 (1998), 15–53. MR 2000c:11107 Zbl 0946.14009

[Batyrev and Tschinkel 1998b] V. V. Batyrev and Y. Tschinkel, "Tamagawa numbers of polarized algebraic varieties", pp. 299–340 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), edited by E. Peyre, Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000d:11090 Zbl 0926.11045

[de la Bretèche and Browning 2014] R. de la Bretèche and T. D. Browning, "Density of Châtelet surfaces failing the Hasse principle", *Proc. Lond. Math. Soc.* (3) **108**:4 (2014), 1030–1078. MR 3198755 Zbl 1291.14041

[de la Bretèche and Swinnerton-Dyer 2007] R. de la Bretèche and P. Swinnerton-Dyer, "Fonction zêta des hauteurs associée à une certaine surface cubique", *Bull. Soc. Math. France* **135**:1 (2007), 65–92. MR 2009f:14041 Zbl 1207.11068

[de la Bretèche et al. 2007] R. de la Bretèche, T. D. Browning, and U. Derenthal, "On Manin's conjecture for a certain singular cubic surface", *Ann. Sci. École Norm. Sup.* (4) **40**:1 (2007), 1–50. MR 2008e:11038 Zbl 1125.14008

[Browning 2006] T. D. Browning, "The density of rational points on a certain singular cubic surface", *J. Number Theory* **119**:2 (2006), 242–283. MR 2007d:14046 Zbl 1119.11034

[Browning and Derenthal 2009] T. D. Browning and U. Derenthal, "Manin's conjecture for a cubic surface with D_5 singularity", *Int. Math. Res. Not.* **2009**:14 (2009), 2620–2647. MR 2011a:14041 Zbl 1173.14017

[Chambert-Loir and Tschinkel 2002] A. Chambert-Loir and Y. Tschinkel, "On the distribution of points of bounded height on equivariant compactifications of vector groups", *Invent. Math.* **148**:2 (2002), 421–452. MR 2003d:11094 Zbl 1067.11036

[Colliot-Thélène and Sansuc 1976] J.-L. Colliot-Thélène and J.-J. Sansuc, "Torseurs sous des groupes de type multiplicatif; applications à l'étude des points rationnels de certaines variétés algébriques", *C. R. Acad. Sci. Paris Sér. A-B* **282**:18 (1976), A1113–A1116. MR 54 #2657 Zbl 0337.14014

[Colliot-Thélène and Sansuc 1980] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles", pp. 223–237 in *Journées de Géometrie Algébrique d'Angers* (Angers, 1979), edited by A. Beauville, Sijthoff & Noordhoff, Alphen aan den Rijn, Germantown, MD, 1980. MR 82d:14016 Zbl 0451.14018

[Colliot-Thélène and Sansuc 1987] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles, II", *Duke Math. J.* **54**:2 (1987), 375–492. MR 89f:11082 Zbl 0659.14028

[Coray and Tsfasman 1988] D. F. Coray and M. A. Tsfasman, "Arithmetic on singular Del Pezzo surfaces", *Proc. London Math. Soc.* (3) **57**:1 (1988), 25–87. MR 89f:11083 Zbl 0653.14018

[Derenthal 2009] U. Derenthal, "Counting integral points on universal torsors", *Int. Math. Res. Not.* **2009**:14 (2009), 2648–2699. MR 2010f:14019 Zbl 1173.14014

[Derenthal 2014] U. Derenthal, "Singular del Pezzo surfaces whose universal torsors are hypersurfaces", *Proc. Lond. Math. Soc.* (3) **108**:3 (2014), 638–681. MR 3180592 Zbl 1292.14027

[Derenthal and Loughran 2010] U. Derenthal and D. Loughran, "Singular del Pezzo surfaces that are equivariant compactifications", *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov.* (*POMI*) **377**:10 (2010), 26–43. MR 2012b:14068 Zbl 06246152

[Derenthal et al. 2008] U. Derenthal, M. Joyce, and Z. Teitler, "The nef cone volume of generalized del Pezzo surfaces", *Algebra Number Theory* **2**:2 (2008), 157–182. MR 2009b:14069 Zbl 1158.14032

[Franke et al. 1989] J. Franke, Y. I. Manin, and Y. Tschinkel, "Rational points of bounded height on Fano varieties", *Invent. Math.* **95**:2 (1989), 421–435. MR 89m:11060 Zbl 0674.14012

[Franz 2009] M. Franz, *Convex - a Maple package for convex geometry, version 1.1*, 2009, Available at http://www.math.uwo.ca/~mfranz/convex/.

[Hassett and Tschinkel 2004] B. Hassett and Y. Tschinkel, "Universal torsors and Cox rings", pp. 149–173 in *Arithmetic of higher-dimensional algebraic varieties* (Palo Alto, CA, 2002), edited by B. Poonen and Y. Tschinkel, Progr. Math. **226**, Birkhäuser, Boston, 2004. MR 2005a:14049 Zbl 1077.14046

[Heath-Brown 1984] D. R. Heath-Brown, "Diophantine approximation with square-free numbers", *Math. Z.* **187**:3 (1984), 335–344. MR 85j:11072 Zbl 0539.10026

[Heath-Brown 1997] D. R. Heath-Brown, "The density of rational points on cubic surfaces", *Acta Arith.* **79**:1 (1997), 17–30. MR 98h:11083 Zbl 0863.11021

[Heath-Brown 2003] D. R. Heath-Brown, "The density of rational points on Cayley's cubic surface", pp. 33 in *Proceedings of the Session in Analytic Number Theory and Diophantine Equations* (Bonn, 2002), edited by D. R. Heath-Brown and B. Z. Moroz, Bonner Math. Schriften **360**, Univ. Bonn, Bonn, 2003. Zbl 1060.11038

[Le Boudec 2012a] P. Le Boudec, "Manin's conjecture for a cubic surface with $2\mathrm{A}_2 + \mathrm{A}_1$ singularity type", *Math. Proc. Cambridge Philos. Soc.* **153**:3 (2012), 419–455. MR 2990624 Zbl 1253.14022

[Le Boudec 2012b] P. Le Boudec, "Manin's conjecture for two quartic del Pezzo surfaces with $3\mathbf{A}_1$ and $\mathbf{A}_1 + \mathbf{A}_2$ singularity types", *Acta Arith.* **151**:2 (2012), 109–163. MR 2012j:11135 Zbl 1248.11045

[Loughran 2010] D. Loughran, "Manin's conjecture for a singular sextic del Pezzo surface", *J. Théor. Nombres Bordeaux* **22**:3 (2010), 675–701. MR 2012a:14048 Zbl 1258.14029

[Peyre 1995] E. Peyre, "Hauteurs et mesures de Tamagawa sur les variétés de Fano", *Duke Math. J.* **79**:1 (1995), 101–218. MR 96h:11062 Zbl 0901.14025

[Peyre 1998] E. Peyre, "Terme principal de la fonction zêta des hauteurs et torseurs universels", pp. 259–298 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), edited by E. Peyre, Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000f:11081 Zbl 0966.14016

[Salberger 1998] P. Salberger, "Tamagawa measures on universal torsors and points of bounded height on Fano varieties", pp. 91–258 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), edited by E. Peyre, Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000d:11091 Zbl 0959.14007

[Tanimoto and Tschinkel 2012] S. Tanimoto and Y. Tschinkel, "Height zeta functions of equivariant compactifications of semi-direct products of algebraic groups", pp. 119–157 in *Zeta functions in algebra and geometry*, edited by A. Campillo et al., Contemp. Math. **566**, Amer. Math. Soc., Providence, RI, 2012. MR 2858922 Zbl 06092111

Communicated by Roger Heath-Brown
Received 2013-10-30 Revised 2014-03-05 Accepted 2014-04-26

pierre.leboudec@epfl.ch *École Polytechnique Fédérale de Lausanne, SB MATHGEOM TAN, Bâtiment MA, Station 8, CH-1015 Lausanne, Switzerland*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 8 No. 5 2014

1937-0652(2014)8:5;1-6