J. Inst. Math. Jussieu (2024), **23**(6), 2859–2912
doi:10.1017/S1474748024000161

GENERALISED QUADRATIC FORMS OVER TOTALLY REAL NUMBER FIELDS

TIM BROWNING[1], LILLIAN B. PIERCE[2] AND DAMARIS SCHINDLER[3]

[1] *IST Austria, Am Campus 1, 3400 Klosterneuburg, Austria*
(tdb@ist.ac.at)
[2] *Department of Mathematics, Duke University, Durham NC 27708, USA*
(pierce@math.duke.edu)
[3] *Göttingen University, Bunsenstraße 3–5, 37073 Göttingen, Germany*
(damaris.schindler@mathematik.uni-goettingen.de)

(Received 4 January 2023; revised 29 February 2024; accepted 5 March 2024;
first published online 11 April 2024)

Abstract We introduce a new class of generalised quadratic forms over totally real number fields, which is rich enough to capture the arithmetic of arbitrary systems of quadrics over the rational numbers. We explore this connection through a version of the Hardy–Littlewood circle method over number fields.

Contents

1 Introduction **2860**

2 Generalised quadratic forms and the descended system **2865**

3 Recap from algebraic number theory **2867**

4 Enter the circle method **2871**

5 Homogeneous case: proof of Theorems 1.3 and 1.4 **2886**

6 Inhomogeneous case: proof of Theorem 1.5 **2900**

References **2912**

Key words and phrases: quadratic form; circle method; number field

2020 Mathematics subject classification: Primary 11P55
Secondary 11D09; 14G05

1. Introduction

The study of quadratic forms over number fields is a rich and highly developed area of mathematics. Let K be a number field of degree $d \geqslant 2$ over $\mathbb{Q}$, and let

$$Q(X_1,\dots,X_n) = \sum_{1\leqslant i,j\leqslant n} c_{i,j}X_iX_j$$

be a nonsingular quadratic form, with symmetric coefficients $c_{i,j} \in \mathfrak{o}_K$. For given $N \in \mathfrak{o}_K$, it is very natural to ask about the solubility of

$$Q(x_1,\dots,x_n) = N,$$

with $x_1,\dots,x_n \in \mathfrak{o}_K$. If $n \geqslant 4$, a number field version of the Hardy–Littlewood circle method is capable of establishing the Hasse principle for these equations. When $n \geqslant 5$, this follows from work of Skinner [13], and for $n = 4$ it is carried out by Helfrich in a 2015 PhD thesis [8].

In this paper, we shall introduce the notion of a *generalised quadratic form* over K and ask about the Hasse principle in this new setting. We shall always assume that $K/\mathbb{Q}$ is a Galois extension of degree d that is totally real. (Our methods can handle arbitrary number fields, but doing so causes extra notational complexity and gives no new insight into the arithmetic of generalised quadratic forms.) We may now make the following definition.

Definition 1.1. Let $n \geqslant 2$. A *generalised quadratic form* is given by

$$F(X_1,\dots,X_n) = \sum_{1\leqslant i,j\leqslant n}\sum_{\tau,\tau'\in \mathrm{Gal}(K/\mathbb{Q})} c_{i,j,\tau,\tau'}X_i^{\tau}X_j^{\tau'},$$

for symmetric coefficients $c_{i,j,\tau,\tau'} = c_{j,i,\tau',\tau} \in \mathfrak{o}_K$.

We will be interested in the set of $(x_1,\dots,x_n) \in \mathfrak{o}_K^n$ for which

$$F(x_1,\dots,x_n) = N,$$

for given $N \in \mathfrak{o}_K$, in which case x_i^{τ} should be interpreted as the conjugate of x_i under $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Definition 1.1 encompasses standard integral quadratic forms over $\mathfrak{o}_K$ and forms defined using norms and traces. For example, let $\mathrm{Tr}_{K/\mathbb{Q},H} : K \to K$ be the *partial trace*, defined via $\mathrm{Tr}_{K/\mathbb{Q},H}(u) = \sum_{\tau\in H} u^{\tau}$ for any subset $H \subset \mathrm{Gal}(K/\mathbb{Q})$. Then, a natural generalisation of the question about representing elements of $\mathfrak{o}_K$ as a sum of squares is to ask about the existence of $\mathbf{x} \in \mathfrak{o}_K^n$ such that

$$\mathrm{Tr}_{K/\mathbb{Q},H}(x_1^2) + \cdots + \mathrm{Tr}_{K/\mathbb{Q},H}(x_n^2) = N, \tag{1.1}$$

for given $N \in \mathfrak{o}_K$ and a given subset $H \subset \mathrm{Gal}(K/\mathbb{Q})$.

The coefficients of a generalised quadratic form $F(X_1,\dots,X_n)$ form a $dn \times dn$ matrix $\mathbf{M} = (c_{i,j,\tau,\tau'})_{(i,\tau)\times(j,\tau')}$. In the generic setting, we might expect this matrix to have full rank, but there are many cases of interest where the rank is much smaller. For example, standard quadratic forms produce a coefficient matrix $\mathbf{M}$, which after reordering rows and columns, contains a $n \times n$ block matrix in the upper left corner and has zeros everywhere

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

else. Our methods break down in the completely generic situation, and so our interest in this paper lies at the opposite end of the spectrum, in which the rank of $\mathbf{M}$ is not much bigger than n.

Let $W : (K \otimes_{\mathbb{Q}} \mathbb{R})^n \to \mathbb{R}_{\geqslant 0}$ be a smooth weight function, whose precise construction is deferred until §4. Our main results will comprise of asymptotic formulae for sums of the shape

$$N_W(F,N;P) = \sum_{\substack{\mathbf{x}\in \mathfrak{o}_K^n \\ F(\mathbf{x})=N}} W(\mathbf{x}/P),$$

as $P \to \infty$ for given $N \in \mathfrak{o}_K$ and suitable generalised quadratic forms F. When $N = 0$, we shall simply write $N_W(F;P) = N_W(F,0;P)$.

1.1. Homogeneous setting

Of particular interest is the case $N = 0$, which we now assume. For standard quadratic forms $Q \in \mathfrak{o}_K[X_1,\dots,X_n]$, studying nontrivial zeros of Q over $\mathfrak{o}_K$ is equivalent to studying K-rational points on the smooth quadric $X \subset \mathbb{P}_K^{n-1}$ cut out by $Q = 0$. This, in turn, can be accessed via the Weil restriction (or restriction of scalars). The Weil restriction $R_{K/\mathbb{Q}}X$ is an algebraic variety whose set of $\mathbb{Q}$-points is canonically in bijection with the K-rational points of X. In the setting where $Q \in \mathfrak{o}_K[X_1,\dots,X_n]$ is a nonsingular quadratic form, the Weil restriction $R_{K/\mathbb{Q}}X$ is a smooth complete intersection of d quadrics in $\mathbb{P}_{\mathbb{Q}}^{dn-1}$, all of which are defined over $\mathbb{Q}$. However, the set of complete intersections that arise in this way is a very limited subset of the family of all smooth codimension d complete intersections of quadrics over $\mathbb{Q}$ in $\mathbb{P}_{\mathbb{Q}}^{dn-1}$. Our first result shows that, after Weil restriction, the space of generalised quadratic forms is rich enough to capture the arithmetic over $\mathbb{Q}$ of arbitrary codimension d complete intersections of quadrics in $\mathbb{P}_{\mathbb{Q}}^{M-1}$, provided that $d \mid M$.

Let $F(X_1,\dots,X_n)$ be a generalised quadratic form, and let $\omega_1,\dots,\omega_d$ be a $\mathbb{Z}$-basis for $\mathfrak{o}_K$. Any element $\mathbf{x} \in \mathfrak{o}_K^n$ can be written $\mathbf{x} = \omega_1\mathbf{u}_1 + \cdots + \omega_d\mathbf{u}_d$ for $(\mathbf{u}_1,\dots,\mathbf{u}_d) \in \mathbb{Z}^{dn}$. Taking the Weil restriction corresponds to writing down a set of quadratic forms $Q_1,\dots,Q_d \in \mathbb{Z}[\mathbf{U}_1,\dots,\mathbf{U}_d]$, in dn variables such that

$$F(X_1,\dots,X_n) = \sum_{1\leqslant i\leqslant d} \omega_i Q_i(\mathbf{U}_1,\dots,\mathbf{U}_d). \tag{1.2}$$

We henceforth call $\{Q_1,\dots,Q_d\}$ the *descended system*. We shall prove the following result in §2.

Theorem 1.2. *Let $K/\mathbb{Q}$ be a Galois extension of degree d. Then there is a bijection between the space of generalised quadratic forms in n variables over K and systems of d rational quadratic forms in dn variables.*

It is interesting to note that this theorem is valid for *any* fixed degree d Galois extension $K/\mathbb{Q}$. It follows from the bijection in Theorem 1.2 that the question of $\mathfrak{o}_K$-solubility for a generalised quadratic form is equivalent to the question of $\mathbb{Z}$-solubility for the descended system. It presents an intriguing challenge to gain insight into smooth codimension d

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

complete intersections of quadrics in $\mathbb{P}^{M-1}_{\mathbb{Q}}$ over $\mathbb{Q}$ by working with generalised quadratic forms.

It follows from work of Birch [1] that the usual Hardy–Littlewood asymptotic formula holds for systems of quadrics over $\mathbb{Q}$, provided that $M > B + 2d(d+1)$, where B is the affine dimension of the 'Birch singular locus' of the descended system. (Note that one can take $B \leqslant d-1$ when the descended system is a smooth complete intersection.) Breakthrough work of Rydin Myerson [11] handles smooth codimension d complete intersections of quadrics in $\mathbb{P}^{M-1}_{\mathbb{Q}}$ when $M \geqslant 9d$. The latter result is particularly significant since it allows one to handle arbitrary generalised quadratic forms over K in $n \geqslant 9$ variables, provided that the descended system defines a smooth complete intersection of codimension d.

Our main results will concern a special class of generalised quadratic forms, in which only one nontrivial automorphism appears and in which the conjugated variables separate completely from the unconjugated variables. These examples are chosen to represent a first step on the way to a fuller understanding of generalised quadratic forms, and yet exhibit enough features that make them untreatable by other methods. In the light of Theorem 1.2, a complete understanding of generalised quadratic forms must lie rather deep.

Let $Q \in \mathfrak{o}_K[X_1, \dots, X_n]$ and $R \in \mathfrak{o}_K[X_1, \dots, X_m]$ be quadratic forms in n and m variables, respectively, for $1 \leqslant m \leqslant n$. The generalised quadratic forms we shall treat take the shape

$$F(X_1, \dots, X_n) = Q(X_1, \dots, X_n) + R(X_1^\tau, \dots, X_m^\tau), \tag{1.3}$$

for a fixed nontrivial automorphism $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Let $\rho_1, \dots, \rho_d$ be the d distinct embeddings of K into $\mathbb{R}$, where we recall that K is totally real. For each $1 \leqslant l \leqslant d$, we define l_τ through the relation

$$\rho_{l_\tau} \tau = \rho_l. \tag{1.4}$$

Suppose that $\mathbf{A}$ is the $n \times n$ symmetric matrix defining Q and that $\mathbf{B}$ is the $n \times n$ symmetric matrix given by the condition that its upper left $m \times m$ submatrix defines R, with all other entries equal to 0. For any $1 \leqslant l \leqslant d$, we shall write $\mathbf{A}^{(l)}$ and $\mathbf{B}^{(l)}$ for the l-th embeddings of $\mathbf{A}$ and $\mathbf{B}$, respectively. We make the following key hypotheses about $\mathbf{A}$ and $\mathbf{B}$.

Assumption 1. Assume that the descended system

$$Q_1(\mathbf{U}_1, \dots, \mathbf{U}_d) = \cdots = Q_d(\mathbf{U}_1, \dots, \mathbf{U}_d) = 0$$

has codimension d in $\mathbb{P}^{dn-1}$. Furthermore, assume that $\det \mathbf{A} \neq 0$ and that the upper left $m \times m$ submatrix of $\mathbf{B}$ is nonsingular.

Our first result deals with the special case $m = 1$.

Theorem 1.3. *Let $K/\mathbb{Q}$ be a totally real Galois extension of degree $d \geqslant 2$. Suppose that $m = 1$ and that Assumption 1 holds. Assume that $\det(\mathbf{A}^{(l)} + t\mathbf{B}^{(l_\tau)})$ is a constant polynomial in t, for each $1 \leqslant l \leqslant d$, where l_τ is defined via Equation (1.4). Let $n \geqslant 6$ and*

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

assume that the descended system has nonsingular points everywhere locally. Then there exist constants $c > 0$ *and* $\Delta > 0$ *such that*

$$N_W(F;P) = cP^{(n-2)d} + O(P^{(n-2)d-\Delta}).$$

The implied constants in our work are always allowed to depend on K and F. The generalised quadratic form $2X_1X_2 + a(X_1^\tau)^2 + \tilde{Q}(X_3,\dots,X_n)$ meets the hypotheses of the theorem, for example, where $\tilde{Q} \in \mathfrak{o}_K[X_3,\dots,X_n]$ is a nonsingular quadratic form and $a \in \mathfrak{o}_K$ is nonzero.

We are also able to prove an asymptotic formula for $N_W(F;P)$ for arbitrary $m \geqslant 1$, provided we make additional assumptions about the matrices $\mathbf{A}$ and $\mathbf{B}$.

Assumption 2. For all $1 \leqslant l \leqslant d$, assume that $\operatorname{rank}(\mathbf{A}^{(l)} + t\mathbf{B}^{(l_\tau)}) \geqslant n-1$, for all $t \in \mathbb{R}$, where l_τ is defined via Equation (1.4).

Assumption 3. For all $1 \leqslant l \leqslant d$, assume that $\det(\mathbf{A}^{(l)} + t\mathbf{B}^{(l_\tau)})$ has degree at least $m-1$, viewed as a polynomial in t.

When $m = 1$ and $\det(\mathbf{A}^{(l)} + t\mathbf{B}^{(l_\tau)})$ has degree exactly 0 in Assumption 3, we see that Assumption 2 is implied by Assumption 1 since then $\operatorname{rank}(\mathbf{A}^{(l)} + t\mathbf{B}^{(l_\tau)}) = \operatorname{rank}(\mathbf{A}^{(l)}) = n$. For general $m \geqslant 1$, Assumption 2 is similar to one that is commonly made in the study of pairs of quadratic forms. Indeed, suppose one is given two matrices $A, B \in M_{n\times n}(L)$ over an algebraically closed field L of characteristic not equal to 2, with associated quadratic forms Q_A and Q_B. It follows from Reid's thesis [10, Prop. 2.1] that the rank of any element in the pencil $\lambda A + \mu B$, with $(\lambda,\mu) \neq (0,0)$, is never smaller than $n-1$, provided the intersection $Q_A = Q_B = 0$ is nonsingular as a projective variety and of the expected dimension. In our situation, by contrast, we only look at the pencil $\mathbf{A}^{(l)} + t\mathbf{B}^{(l_\tau)}$ since the matrix $\mathbf{B}^{(l_\tau)}$ has rank m by construction. (We shall relate this situation to the properties of an appropriate singular locus in Lemma 5.1 below.)

We are now ready to reveal our main result in the homogeneous setting.

Theorem 1.4. *Let* $K/\mathbb{Q}$ *be a totally real Galois extension of degree* $d \geqslant 2$. *Suppose that Assumptions 1–3 hold and that* $n > 3m + 4 - 4m/d$. *Assume that the descended system has nonsingular points everywhere locally. Then there exist constants* $c > 0$ *and* $\Delta > 0$ *such that*

$$N_W(F;P) = cP^{(n-2)d} + O(P^{(n-2)d-\Delta}).$$

On taking $m = 1$, we note that this result subsumes Theorem 1.3 when $n \geqslant 7$. If one makes further assumptions on Q, one can do even better. Suppose, for example, that the last $n-m$ variables split off from Q so that

$$Q(X_1,\dots,X_n) = Q_1(X_1,\dots,X_m) + Q_2(X_{m+1},\dots,X_n),$$

for quadratic forms Q_1 and Q_2 over $\mathfrak{o}_K$. Then it seems likely that a classical version of the circle method can be employed. On summing trivially over the first m-variables of the associated exponential sums, one would be left with handling an exponential sum in $n-m$ variables involving Q_2. If Q_2 has rank at least 5, then Skinner's treatment over

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

number fields [13] would yield the necessary saving. This ought to allow $n \geqslant m+5$ in the statement of Theorem 1.4 if $Q(0,\dots,0,\ X_{m+1},\dots,X_n)$ has rank at least 5.

1.2. Inhomogeneous setting

We now assume that $N \in \mathfrak{o}_K$ is nonzero. Then we may write $N = \omega_1 N_1 + \cdots + \omega_d N_d$, where $N_1,\dots,N_d \in \mathbb{Z}$ are not all zero. We shall henceforth call $\{Q_1 - N_1,\dots,Q_d - N_d\}$ the *shifted descended system*, where $Q_1,\dots,Q_d$ are obtained from F via Equation (1.2), continuing to call $\{Q_1,\dots,Q_d\}$ the associated *descended system*.

Our next result demonstrates that sharper results are available if $N \neq 0$ and Q,R are both diagonal. Suppose that

$$F(X_1,\dots,X_n) = a_1X_1^2 + \cdots + a_nX_n^2 + \sum_{i=1}^{m} b_i(X_i^\tau)^2, \tag{1.5}$$

for $1 \leqslant m \leqslant n$ and nonzero $a_1,\dots,a_n,b_1,\dots,b_m \in \mathfrak{o}_K$, and where $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ is a fixed nontrivial automorphism. Taking $m = n$ and $a_i = b_i = 1$ for $1 \leqslant i \leqslant n$, we are led to an instance of the partial trace problem in Equation (1.1) with $H = \{\mathrm{id},\tau\}$. We will prove the following result.

Theorem 1.5. *Let $K/\mathbb{Q}$ be a totally real Galois extension of degree $d \geqslant 2$. Assume that $N \in \mathfrak{o}_K$ is nonzero and that $n \geqslant m+4$. Suppose that the descended system has codimension d and a nonsingular real point and that the shifted descended system has nonsingular points over $\mathbb{Z}_p$ for every prime p. Then there exist constants $c > 0$ and $\Delta > 0$ such that*

$$N_W(F,N;P) = cP^{(n-2)d} + O(P^{(n-2)d-\Delta}).$$

The implied constant in this result is allowed to depend on N, in addition to K and F. In order to illustrate our result, take the quadratic number field $K = \mathbb{Q}(\sqrt{2})$ in Equation (1.5) and assume that $a_1,\dots,a_n,b_1,\dots,b_m \in \mathbb{Z}$ are all nonzero. Then it follows from Theorem 1.5 that our work treats the shifted descended system

$$\sum_{i=1}^{m}(a_i+b_i)u_i^2 + 2\sum_{i=1}^{m}(a_i+b_i)v_i^2 + \sum_{i=m+1}^{n} a_i(u_i^2+2v_i^2) = N_1,$$
$$2\sum_{i=1}^{m}(a_i-b_i)u_iv_i + 2\sum_{i=m+1}^{n} a_iu_iv_i = N_2,$$

when $n \geqslant m+4$ and $N_1,N_2 \in \mathbb{Z}$ are not both zero.

1.3. Some words on the proof

Let $F(X_1,\dots,X_n)$ be a generalised quadratic form defined over $\mathfrak{o}_K$, and let $N \in \mathfrak{o}_K$. Our analysis of $N_W(F,N;P)$ relies on a Fourier-analytic interpretation of the indicator function

$$\delta_K(\alpha) = \begin{cases} 1, & \text{if } \alpha = 0, \\ 0, & \text{if } \alpha \in \mathfrak{o}_K \setminus \{0\}. \end{cases} \tag{1.6}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Browning and Vishe [2, Thm 1.2] have extended to arbitrary number fields the smooth δ-function technology of Duke–Friedlander–Iwaniec [4], as later refined by Heath-Brown [5]. This will underpin the work in this paper, affording us the opportunity to extract nontrivial savings, in the spirit of Kloosterman's method, in the proof of Theorem 1.5. We will be led to an expression for $N_W(F,N;P)$ in Equation (4.6), involving an infinite sum over nonzero integral ideals $\mathfrak{b}$. The next stage is to apply Poisson summation, but an obstacle arises from the fact that it is no longer possible to break into residue classes modulo $\mathfrak{b}$ for generalised quadratic forms F. Instead, we shall break into residue classes modulo a larger ideal ${}^G\mathfrak{b}$, which is the least common multiple of the ideals $\mathfrak{b}^{\tau^{-1}}$, as τ ranges over the automorphisms that actually occur in F. Poisson summation then leads to the analysis of certain *exponential sums* $S_{\mathfrak{b}}(N;\mathbf{m})$ and *oscillatory integrals* $I_{\mathfrak{b}}(N;\mathbf{m})$, which are indexed by $\mathfrak{b} \subset \mathfrak{o}_K$ and suitable vectors $\mathbf{m} \in K^n$. While the treatment of $S_{\mathfrak{b}}(N;\mathbf{m})$ is relatively standard, the main challenge is to understand $I_{\mathfrak{b}}(N;\mathbf{m})$. When F is a standard quadratic form, these integrals factorise into a product of d oscillatory integrals, one for each of the d real embeddings of K. This reduces the problem to looking at oscillatory integrals over $\mathbb{R}^n$. For generic generalised quadratic forms, it seems very difficult to obtain the kind of cancellation one needs for the method to go through for the relevant oscillatory integrals over $\mathbb{R}^{dn}$.

We now summarise the contents of the paper. In §2, we shall prove Theorem 1.2 by spelling out the connection between generalised quadratic forms over K and descended systems over $\mathbb{Q}$. In §3, we collect together some useful facts from algebraic number theory. The rest of the paper will be concerned with estimating the size of the counting function $N_W(F,N;P)$, as $P \to \infty$. In order to facilitate future investigation, we shall present most of the arguments for arbitrary generalised quadratic forms in §4. Next, in §5 we shall specialise to the case (1.3) and $N = 0$, in order to deduce Theorems 1.3 and 1.4. Finally, §6 will deal with Theorem 1.5, which pertains to the diagonal generalised quadratic form (1.5) and $N \neq 0$.

2. Generalised quadratic forms and the descended system

In this section, we shall prove Theorem 1.2, by making explicit the correspondence between generalised quadratic forms F and the descended system of d quadratic forms over $\mathbb{Q}$ in dn variables. Let $K/\mathbb{Q}$ be a degree d Galois number field, which (in this section only) need not be totally real. Assume that we are given a set of coefficients $(c_{i,j,\tau,\tau'})$ of a generalised quadratic form, with $c_{i,j,\tau,\tau'} = c_{j,i,\tau',\tau}$ for all $1 \leqslant i,j \leqslant n$ and $\tau,\tau' \in \mathrm{Gal}(K/\mathbb{Q})$. We can write each coefficient $c_{i,j,\tau,\tau'} \in K$ with respect to the basis $\{\omega_1,\dots,\omega_d\}$ as $c_{i,j,\tau,\tau'} = \sum_{k=1}^d c_{i,j,\tau,\tau'}^{(k)}\omega_k$. We proceed to compute the descended system explicitly by writing $X_i = \sum_{k=1}^d U_{k,i}\omega_k$, for $1 \leqslant i \leqslant n$. Then

$$F(X_1,\dots,X_n) = \sum_{1\leqslant i,j\leqslant n} \sum_{\tau,\tau'\in \mathrm{Gal}(K/\mathbb{Q})} \sum_{1\leqslant l,m,k\leqslant d} c_{i,j,\tau,\tau'}^{(k)}\omega_k U_{l,i}\omega_l^{\tau} U_{m,j}\omega_m^{\tau'}.$$

Let $\{\rho_1,\dots,\rho_d\}$ be a dual basis of $\{\omega_1,\dots,\omega_d\}$ with respect to the trace so that $(\mathrm{Tr}_{K/\mathbb{Q}}(\rho_i\omega_j))_{i,j}$ is the identity matrix and any $\alpha \in K$ can be written in the form

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

$\alpha = \sum_{p=1}^{d} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\rho_p)\omega_p$. Thus, $F(X_1,\dots,X_n)$ is equal to

$$\sum_{p=1}^{d}\omega_p \sum_{1\leqslant i,j\leqslant n}\sum_{1\leqslant l,m\leqslant d} U_{l,i}U_{m,j}\,\mathrm{Tr}_{K/\mathbb{Q}}\left(\rho_p \sum_{1\leqslant k\leqslant d}\sum_{\tau,\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c^{(k)}_{i,j,\tau,\tau'}\omega_k\omega_l^{\tau}\omega_m^{\tau'}\right)$$

and we arrive at our descended system (1.2), with

$$Q_p(\underline{\mathbf{U}}) = \sum_{1\leqslant i,j\leqslant n}\sum_{1\leqslant l,m\leqslant d}\beta_{p,l,i,m,j}U_{l,i}U_{m,j},$$

for rational coefficients

$$\begin{aligned}\beta_{p,l,i,m,j} &= \mathrm{Tr}_{K/\mathbb{Q}}\left(\rho_p \sum_{1\leqslant k\leqslant d}\sum_{\tau,\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c^{(k)}_{i,j,\tau,\tau'}\omega_k\omega_l^{\tau}\omega_m^{\tau'}\right)\\ &= \sum_{1\leqslant k\leqslant d}\sum_{\tau,\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c^{(k)}_{i,j,\tau,\tau'}\,\mathrm{Tr}_{K/\mathbb{Q}}(\rho_p\omega_k\omega_l^{\tau}\omega_m^{\tau'}).\end{aligned}$$

By construction, the coefficients $\beta_{p,l,i,m,j}$ satisfy $\beta_{p,l,i,m,j} = \beta_{p,m,j,l,i}$, for all $1\leqslant p,l,m\leqslant d$ and $1\leqslant i,j\leqslant n$. Moreover, they depend linearly on the given set of coefficients $(c^{(k)}_{i,j,\tau,\tau'})$. Now, the space of all tuples $(c^{(k)}_{i,j,\tau,\tau'})$ of rational numbers satisfying the symmetry relation $c^{(k)}_{i,j,\tau,\tau'} = c^{(k)}_{j,i,\tau',\tau}$ can be parametrised by $\mathbb{Q}^{\frac{1}{2}dn(dn+1)d}$. Similarly, the space of all symmetric rational tuples $(\beta_{p,l,i,m,j})$ is naturally parametrised by $\mathbb{Q}^{\frac{1}{2}dn(dn+1)d}$. We define the map

$$\Phi : \mathbb{Q}^{\frac{1}{2}dn(dn+1)d} \to \mathbb{Q}^{\frac{1}{2}dn(dn+1)d}, \quad (c^{(k)}_{i,j,\tau,\tau'}) \mapsto (\beta_{p,l,i,m,j}).$$

We claim that this map is an injective linear map. This implies that there is a bijection between generalised quadratic forms in n variables and systems of d rational quadratic forms in nd variables, as claimed in Theorem 1.2.

To check the claim, we assume that $\beta_{p,l,i,m,j} = 0$ for all $1\leqslant p,l,m\leqslant d$ and $1\leqslant i,j\leqslant n$. By the nondegeneracy of the trace as a bilinear form, we deduce that

$$\sum_{\tau,\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c_{i,j,\tau,\tau'}\omega_l^{\tau}\omega_m^{\tau'} = 0, \quad 1\leqslant i,j\leqslant n,\ 1\leqslant l,m\leqslant d.$$

Note that the matrix $(\omega_l^{\tau})_{\substack{1\leqslant l\leqslant d\\ \tau\in\mathrm{Gal}(K/\mathbb{Q})}}$ is of maximal rank, and hence we obtain

$$\sum_{\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c_{i,j,\tau,\tau'}\omega_m^{\tau'} = 0, \quad 1\leqslant i,j\leqslant n,\ \tau\in\mathrm{Gal}(K/\mathbb{Q}),\ 1\leqslant m\leqslant d.$$

Applying the same argument again, we finally obtain

$$c_{i,j,\tau,\tau'} = 0, \quad 1\leqslant i,j\leqslant n,\ \tau,\tau'\in\mathrm{Gal}(K/\mathbb{Q}),$$

and hence $c^{(k)}_{i,j,\tau,\tau'} = 0$ for all $1\leqslant k\leqslant d$.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

3. Recap from algebraic number theory

In this section, we collect together some of the facts about algebraic number fields that are important in our work. As usual, $K/\mathbb{Q}$ is a totally real Galois extension of degree d. We shall henceforth write $\mathfrak{o} = \mathfrak{o}_K$ for its ring of integers. In §3.1 and §3.2, we recall some facts about ideals and discuss the construction of primitive characters modulo ideals, respectively. The need to deal with generalised quadratic forms naturally leads to two basic objects that can be associated to a given integral ideal $\mathfrak{b}$ in K, both of which depend on the particular generalised quadratic form we are working with and will be introduced in §3.3.

3.1. Properties of ideals

For any fractional ideal $\mathfrak{a}$ in K, one defines the dual ideal

$$\hat{\mathfrak{a}} = \{\alpha \in K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x) \in \mathbb{Z} \text{ for all } x \in \mathfrak{a}\}.$$

In particular, $\hat{\mathfrak{a}} = \mathfrak{a}^{-1}\mathfrak{d}^{-1}$, where $\mathfrak{d} = \{\alpha \in K : \alpha\hat{\mathfrak{o}} \subseteq \mathfrak{o}\}$ denotes the different ideal of K and is itself an integral ideal. One notes that $\hat{\mathfrak{o}} = \mathfrak{d}^{-1}$. Furthermore, we have $\hat{\mathfrak{a}} \subseteq \hat{\mathfrak{b}}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$. An additional integral ideal featuring in our work is the denominator ideal

$$\mathfrak{a}_\gamma = \{\alpha \in \mathfrak{o} : \alpha\gamma \in \mathfrak{o}\},$$

associated to any $\gamma \in K$. Recall that $\mathrm{N}\mathfrak{a} = |\mathfrak{o}/\mathfrak{a}|$ is the ideal norm of any integral ideal $\mathfrak{a}$. One important property of the ideal norm is that $\mathrm{N}\mathfrak{a}^\tau = \mathrm{N}\mathfrak{a}$ for any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. (This follows from the isomorphism $\mathfrak{o}/\mathfrak{a} \to \mathfrak{o}/\mathfrak{a}^\tau$ given by $\alpha \mapsto \alpha^\tau$.) Furthermore, we have $\mathrm{N}\mathfrak{a} \in \mathfrak{a}$ for any integral ideal $\mathfrak{a}$.

We will write $(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}+\mathfrak{b}$ for the greatest common divisor of two integral ideals $\mathfrak{a},\mathfrak{b} \subset \mathfrak{o}$. When these ideals are coprime, meaning that $\mathfrak{a}+\mathfrak{b} = \mathfrak{o}$, we shall adopt the abuse of notation $(\mathfrak{a},\mathfrak{b}) = 1$. We close this section by recording the following basic result.

Lemma 3.1. *Let $\varepsilon > 0$, and let $\mathfrak{b},\mathfrak{c}$ be integral ideals. Then*

(i) *there exists $\alpha \in \mathfrak{b}$ such that $\mathrm{ord}_\mathfrak{p}(\alpha) = \mathrm{ord}_\mathfrak{p}(\mathfrak{b})$ for every prime ideal $\mathfrak{p} \mid \mathfrak{c}$;*

(ii) *there exists $\alpha \in \mathfrak{b}$ and an unramified prime ideal $\mathfrak{p}$ coprime to $\mathfrak{b}^\tau$ for all $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, with $\mathrm{N}\mathfrak{p} \ll (\mathrm{N}\mathfrak{b})^\varepsilon$, such that $(\alpha) = \mathfrak{b}\mathfrak{p}$.*

Proof. Part (i) is [2, Lemma 2.2(i)] and part (ii) follows from an obvious modification to the proof of [2, Lemma 2.2(ii)]. □

We shall also require a version of the Chinese remainder theorem, as in [12, Lemma 3].

Lemma 3.2. *Suppose that $\mathfrak{a},\mathfrak{a}_1,\mathfrak{a}_2$ are integral ideals such that $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$, with $\mathfrak{a}_1$ and $\mathfrak{a}_2$ coprime. Let $\alpha_1,\alpha_2 \in \mathfrak{o}$ satisfy $\mathrm{ord}_\mathfrak{p}(\alpha_1) = \mathrm{ord}_\mathfrak{p}(\mathfrak{a}_1)$ and $\mathrm{ord}_\mathfrak{p}(\alpha_2) = \mathrm{ord}_\mathfrak{p}(\mathfrak{a}_2)$, for all $\mathfrak{p} \mid \mathfrak{a}$. Then*

$$\mathfrak{o}/\mathfrak{a} = \{\alpha_1\mu + \alpha_2\beta : \beta \in \mathfrak{o}/\mathfrak{a}_1,\ \mu \in \mathfrak{o}/\mathfrak{a}_2\}.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

3.2. Construction of primitive characters

Let $\psi(\cdot) = \exp(2\pi i \operatorname{Tr}_{K/\mathbb{Q}}(\cdot))$ be a character on K. The following result gives a way to construct primitive characters $\mathfrak{o}/\mathfrak{b} \to \mathbb{C}$.

Lemma 3.3. *Let $\sigma_0(\cdot) = \psi(\gamma\cdot) : K \to \mathbb{C}$, for any $\gamma \in K$, and let $\mathfrak{b} \subsetneq \mathfrak{o}$ be an integral ideal. Then σ_0 is a nontrivial primitive additive character modulo $\mathfrak{b}$ if and only if $\mathfrak{a}_\gamma = \mathfrak{b}\mathfrak{e}$ for some $\mathfrak{e} \mid \mathfrak{d}$ such that $(\mathfrak{d}/\mathfrak{e}, \mathfrak{b}) = 1$.*

Proof. We begin by showing that σ_0 is an additive character modulo $\mathfrak{b}$ if and only if $\mathfrak{b}\mathfrak{d} \subset \mathfrak{a}_\gamma$. But σ_0 is an additive character modulo $\mathfrak{b}$ if and only if $\sigma_0(x+z) = \sigma_0(x)$ for all $x \in \mathfrak{o}$ and $z \in \mathfrak{b}$. But this happens if and only if $\gamma z \in \hat{\mathfrak{o}}$ for all $z \in \mathfrak{b}$, which is if and only if $\mathfrak{b}\mathfrak{d} \subset \mathfrak{a}_\gamma$. This establishes the claim.

Now, suppose that $\mathfrak{b}\mathfrak{d} \subset \mathfrak{a}_\gamma$, which means that $\mathfrak{a}_\gamma \mid \mathfrak{b}\mathfrak{d}$. Thus, there is an integral ideal $\mathfrak{h}$ such that $\mathfrak{b}\mathfrak{d} = \mathfrak{a}_\gamma\mathfrak{h}$. We wish to show that σ_0 is primitive if and only if $\mathfrak{h} \mid \mathfrak{d}$ with $(\mathfrak{h}, \mathfrak{b}) = 1$. To do so, we note that σ_0 is primitive if and only if $\mathfrak{a}_\gamma \nmid \mathfrak{b}_1\mathfrak{d}$ for all $\mathfrak{b}_1 \mid \mathfrak{b}$ with $\mathfrak{b}_1 \neq \mathfrak{b}$. Indeed, if $\mathfrak{a}_\gamma \mid \mathfrak{b}_1\mathfrak{d}$ for some proper divisor $\mathfrak{b}_1 \mid \mathfrak{b}$, then $\gamma z \in \hat{\mathfrak{o}}$ for every $z \in \mathfrak{b}_1$, which would mean that σ_0 is a character modulo $\mathfrak{b}_1$. Suppose that σ_0 is primitive, and suppose that there is a prime ideal $\mathfrak{p} \mid \mathfrak{h}$ such that $\mathfrak{p} \mid \mathfrak{b}$. Writing $\mathfrak{h}' = \mathfrak{h}\mathfrak{p}^{-1}$ and $\mathfrak{b}' = \mathfrak{b}\mathfrak{p}^{-1}$, it follows that $\mathfrak{b}'\mathfrak{d} = \mathfrak{a}_\gamma\mathfrak{h}'$, whence $\mathfrak{a}_\gamma \mid \mathfrak{b}'\mathfrak{d}$, which is a contradiction. Thus, $\mathfrak{h}$ is coprime to $\mathfrak{b}$ and we must have $\mathfrak{h} \mid \mathfrak{d}$. Suppose now that $\mathfrak{b}\mathfrak{d} = \mathfrak{a}_\gamma\mathfrak{h}$ for some $\mathfrak{h} \mid \mathfrak{d}$ such that $(\mathfrak{h}, \mathfrak{b}) = 1$. We wish to deduce that σ_0 is primitive, for which we suppose for a contradiction that there exists a proper divisor $\mathfrak{b}_1 \mid \mathfrak{b}$ such that $\mathfrak{a}_\gamma \mid \mathfrak{b}_1\mathfrak{d}$. Writing $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ and recalling that $\mathfrak{b}\mathfrak{d} = \mathfrak{a}_\gamma\mathfrak{h}$, we deduce that $\mathfrak{h} = (\mathfrak{a}_\gamma^{-1}\mathfrak{b}_1\mathfrak{d})\mathfrak{b}_2$, whence $\mathfrak{b}_2 \mid \mathfrak{h}$, which is impossible since $(\mathfrak{h}, \mathfrak{b}) = 1$.

Finally we note that σ_0 is a trivial character if and only if $\gamma \in \hat{\mathfrak{o}}$, which is equivalent to $\mathfrak{a}_\gamma \supseteq \mathfrak{d}$. This is clearly impossible for any primitive character σ_0 modulo a proper ideal $\mathfrak{b} \subsetneq \mathfrak{o}$ since $(\mathfrak{d}/\mathfrak{e}, \mathfrak{b}) = 1$ if $\mathfrak{a}_\gamma = \mathfrak{b}\mathfrak{e}$. □

We proceed to define a particularly convenient additive character modulo $\mathfrak{b}$. Associated to any nonzero integral ideal $\mathfrak{b}$ is the subset $\mathfrak{F}(\mathfrak{b}) \subset K$ given by

$$\mathfrak{F}(\mathfrak{b}) = \left\{ \frac{g}{\alpha} \in K : \begin{array}{l} \exists \text{ prime ideal } \mathfrak{p}_1 \text{ with } \mathrm{N}\mathfrak{p}_1 \ll \mathrm{N}\mathfrak{b} \text{ s.t.} \\ \quad \text{(i).} \quad (\alpha) = \mathfrak{b}\mathfrak{d}\mathfrak{p}_1 \\ \quad \text{(ii).} \quad g \in \mathfrak{p}_1 \cap \mathbb{Z} \text{ with } ((g),\ \mathfrak{b}^\tau\mathfrak{d}) = 1 \ \forall\ \tau \in \mathrm{Gal}(K/\mathbb{Q}) \\ \quad \text{(iii).} \quad \exists\ \mathfrak{e} \mid \mathfrak{d} \text{ s.t. } (\mathfrak{d}/\mathfrak{e}, \mathfrak{b}) = 1 \text{ and } \mathfrak{a}_{g/\alpha} = \mathfrak{b}\mathfrak{e} \end{array} \right\}.$$

Note that condition (i) implies that $\alpha \in \mathfrak{b}\mathfrak{d}$ and condition (ii) implies that $\mathfrak{p}_1 \nmid \mathfrak{b}^\tau\mathfrak{d}$ for any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. We may now record a variant of [2, Lemma 2.3], which shows that $\mathfrak{F}(\mathfrak{b}) \neq \emptyset$ for any choice of $\mathfrak{b}$.

Lemma 3.4. *Let $\mathfrak{b} \subsetneq \mathfrak{o}$ be a nonzero ideal. Then there exists $\gamma \in \mathfrak{F}(\mathfrak{b})$ such that $\psi(\gamma\cdot)$ defines a nontrivial primitive additive character modulo $\mathfrak{b}$.*

Proof. We consider the integral ideal $\mathfrak{c} = \mathfrak{b}\mathfrak{d}$. Observe that $\mathfrak{d}^\tau = \mathfrak{d}$ for all $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ since $\mathfrak{d} = \hat{\mathfrak{o}}^{-1}$ and the trace is invariant under the action of the Galois group. Taking $\varepsilon = 1$ in Lemma 3.1(ii), we can find $\alpha \in \mathfrak{c}$ and a prime ideal $\mathfrak{p}_1$ coprime to $\mathfrak{c}^\tau = \mathfrak{b}^\tau\mathfrak{d}$, for every $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, with $\mathrm{N}\mathfrak{p}_1 \ll \mathrm{N}\mathfrak{b}$ and such that $(\alpha) = \mathfrak{c}\mathfrak{p}_1$. It follows from Lemma 3.1(i) that there exists $\nu \in \mathfrak{p}_1$ such that $((\nu), \mathfrak{c}^\tau) = 1$ for any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. But this implies

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

that $g = N_{K/\mathbb{Q}}(\nu)$ is coprime to $\mathfrak{c}^\tau$, for any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, with $g \in \mathfrak{p}_1$. We will show that $\mathfrak{c} = \mathfrak{a}_\gamma$ with $\gamma = g/\alpha$, after which an application of Lemma 3.3 with $\mathfrak{e} = \mathfrak{d}$ will complete the proof. To check the claim we note that

$$\beta \in \mathfrak{a}_\gamma \Leftrightarrow \gamma\beta \in \mathfrak{o} \Leftrightarrow (g\beta) \subset (\alpha) \Leftrightarrow (\alpha) = \mathfrak{b}\mathfrak{d}\mathfrak{p}_1 \mid (g\beta) \Leftrightarrow \beta \in \mathfrak{b}\mathfrak{d}$$

since $\mathfrak{p}_1 \mid (g)$ and $\mathfrak{b}\mathfrak{d}$ is coprime with (g). □

3.3. The G-invariant ideal and an important $\mathbb{Z}$-module

Let F be a generalised quadratic form, as in Definition 1.1. Let $G = G_F \subset \mathrm{Gal}(K/\mathbb{Q})$ be the subset of automorphisms $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ that actually appear in F. Note that $G = \{\mathrm{id}\}$ if and only if F is a standard quadratic form. For any integral ideal $\mathfrak{b}$, we define the *G-invariant ideal* to be

$$^G\mathfrak{b} = \bigcap_{\tau \in G} \mathfrak{b}^{\tau^{-1}}. \tag{3.1}$$

This is the least common multiple of the ideals $\mathfrak{b}^{\tau^{-1}}$ for $\tau \in G$.

Next, associated to our generalised quadratic form F is a *generalised bilinear form*

$$B(X_1,\dots,X_n;Y_1,\dots,Y_n) = \sum_{1 \leqslant i,j \leqslant n} \sum_{\tau,\tau' \in \mathrm{Gal}(K/\mathbb{Q})} c_{i,j,\tau,\tau'} X_i^\tau Y_j^{\tau'}. \tag{3.2}$$

This defines a map $K^n \times K^n \to K$, with

$$B(\mathbf{x};\mathbf{u}+\mathbf{v}) = B(\mathbf{x};\mathbf{u}) + B(\mathbf{x};\mathbf{v}) \quad \text{and} \quad B(\mathbf{u}+\mathbf{v};\mathbf{y}) = B(\mathbf{u};\mathbf{y}) + B(\mathbf{v};\mathbf{y}),$$

for any vectors $\mathbf{x},\mathbf{y},\mathbf{u},\mathbf{v} \in K^n$. (However, this fails to be a bilinear form on K^n since $B(\lambda\mathbf{x};\mathbf{y})$, $B(\mathbf{x};\lambda\mathbf{y})$ and $\lambda B(\mathbf{x};\mathbf{y})$ needn't be equal for $\lambda \in K$.)

For any ideal $\mathfrak{b} \subset \mathfrak{o}$, let

$$\mathscr{H}_\mathfrak{b} = \{\mathbf{h} \in \mathfrak{o}^n : F(\mathbf{a}+\mathbf{h}) \equiv F(\mathbf{a}) \bmod \mathfrak{b} \text{ for all } \mathbf{a} \in \mathfrak{o}^n\}.$$

This is an additive group, and it is clear that $^G\mathfrak{b}^n \subset \mathscr{H}_\mathfrak{b} \subset \mathfrak{o}^n$, where $^G\mathfrak{b}$ is the G-invariant ideal defined in Equation (3.1). By testing the hypothesis with $\mathbf{a} \equiv \mathbf{0} \bmod {}^G\mathfrak{b}$, we have $F(\mathbf{h}) \equiv 0 \bmod \mathfrak{b}$ for any $\mathbf{h} \in \mathscr{H}_\mathfrak{b}$. Hence,

$$\mathscr{H}_\mathfrak{b} = \{\mathbf{h} \in \mathfrak{o}^n : 2B(\mathbf{a};\mathbf{h}) \in \mathfrak{b} \text{ for all } \mathbf{a} \in \mathfrak{o}^n\}. \tag{3.3}$$

We claim that $\mathscr{H}_\mathfrak{b}$ has the structure of a finitely generated $\mathbb{Z}$-module. To see this, let $\mathbf{e}_i$ be the ith unit vector, for $1 \leqslant i \leqslant n$. Observe that $(\mathrm{N}\mathfrak{b})\omega_j\mathbf{e}_i \in \mathscr{H}_\mathfrak{b}$ for all $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant d$. Hence, the image of $\mathscr{H}_\mathfrak{b}$ under the isomorphism $\mathfrak{o}^n \cong \mathbb{Z}^{nd}$ is a lattice of full rank and, thus, finitely generated as a $\mathbb{Z}$-module.

The set $\mathscr{H}_\mathfrak{b}$ will emerge naturally in our analysis of certain key exponential sums, and it will be important to have an estimate for its index in $\mathfrak{o}^n$. In the special case (1.3), it will be easier to calculate $\mathscr{H}_\mathfrak{b}$ directly, but for now we content ourselves with proving a general bound. In the following lemma, we consider the coefficient matrix $(c_{i,j,\tau,\tau'})_{(i,\tau)\times(j,\tau')}$ of a generalised quadratic form as a $nd \times nd$ matrix.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Lemma 3.5. *There is a constant $C_1 > 0$, depending only on F, such that for all $\mathfrak{b}$ we have*

$$|\mathfrak{o}^n/\mathscr{H}_{\mathfrak{b}}| \leqslant C_1(\mathrm{N}\,\mathfrak{b})^{\mathrm{rank}(c_{i,j,\tau,\tau'})}.$$

Moreover, there is an integral ideal $\mathfrak{d}_1$ such that one can take $C_1 = 1$ for all ideals $\mathfrak{b}$ with $(\mathfrak{b},\mathfrak{d}_1) = 1$.

Proof. Let $\Delta = \mathrm{rank}(c_{i,j,\tau,\tau'})_{(i,\tau)\times(j,\tau')}$. Let $\mathscr{S} \subset \{1,\dots,n\} \times \mathrm{Gal}(K/\mathbb{Q})$ be a subset of indices such that the vectors $(c_{i,j,\tau,\tau'})_{(j,\tau')}$, $(i,\tau) \in \mathscr{S}$, are linearly independent and $|\mathscr{S}|$ is maximal. Then, for any $(k,\sigma) \in \{1,\dots,n\} \times \mathrm{Gal}(K/\mathbb{Q})$ there are numbers $a_{i,\tau}^{(k,\sigma)}$ (for $(i,\tau) \in \mathscr{S}$) such that

$$c_{k,j,\sigma,\tau'} = \sum_{(i,\tau)\in\mathscr{S}} a_{i,\tau}^{(k,\sigma)} c_{i,j,\tau,\tau'},$$

for all $1 \leqslant j \leqslant n$ and $\tau' \in \mathrm{Gal}(K/\mathbb{Q})$. Let $\alpha \in \mathfrak{o}$ such that $\alpha a_{i,\tau}^{(k,\sigma)} \in \mathfrak{o}$ for all $(i,\tau) \in \mathscr{S}$ and $(k,\sigma) \in \{1,\dots,n\} \times \mathrm{Gal}(K/\mathbb{Q})$. Now, set

$$\mathscr{H}'_{\mathfrak{b}} = \left\{ \mathbf{h} \in \mathfrak{o}^n : \sum_{1\leqslant j\leqslant n} \sum_{\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c_{i,j,\tau,\tau'} h_j^{\tau'} \in (\alpha)\mathfrak{b}, \forall (i,\tau) \in \mathscr{S} \right\}.$$

Observe that $\mathscr{H}'_{\mathfrak{b}} \subset \mathscr{H}_{\mathfrak{b}}$. Moreover, if $\mathfrak{b}$ and (α) are coprime, then the ideal (α) may be omitted in the definition of $\mathscr{H}'_{\mathfrak{b}}$.

Finally, we observe that there is an injection

$$\psi : \mathfrak{o}^n/\mathscr{H}'_{\mathfrak{b}} \to (\mathfrak{o}/\alpha\mathfrak{b})^{\Delta}, \quad [\mathbf{h}] \mapsto \left(\sum_{1\leqslant j\leqslant n} \sum_{\tau'\in\mathrm{Gal}(K/\mathbb{Q})} c_{i,j,\tau,\tau'} h_j^{\tau'} \right)_{(i,\tau)\in\mathscr{S}}.$$

Hence, $|\mathfrak{o}^n/\mathscr{H}'_{\mathfrak{b}}| \leqslant (\mathrm{N}(\alpha\mathfrak{b}))^{\Delta}$, which suffices since $\mathscr{H}'_{\mathfrak{b}} \subset \mathscr{H}_{\mathfrak{b}}$. □

We now wish to provide an alternative upper bound involving $\mathscr{H}_{\mathfrak{b}}$ under a suitable assumption on the generalised quadratic form.

Definition 3.6. We say that $F(X_1,\dots,X_n)$ is *admissible* if there exist vectors

$$\mathbf{v}_1,\dots,\mathbf{v}_n \in K^n$$

such that $B(\mathbf{v}_i;\mathbf{h}) = 0$ for all $1 \leqslant i \leqslant n$ if and only if $\mathbf{h} = \mathbf{0}$.

In this language, a standard quadratic form is admissible if and only if it is nonsingular. We may now prove the following result.

Lemma 3.7. *Assume that F is admissible. Then there exists a constant $C_2 > 0$, depending only on F, such that*

$$|\mathscr{H}_{\mathfrak{b}}/{}^G\mathfrak{b}^n| \leqslant C_2 \frac{(\mathrm{N}^G\mathfrak{b})^n}{(\mathrm{N}\,\mathfrak{b})^n}.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Moreover, there exists an integral ideal $\mathfrak{d}_2$ *such that one can take* $C_2 = 1$ *for all ideals* $\mathfrak{b}$ *with* $(\mathfrak{b}, \mathfrak{d}_2) = 1$.

We can use this result to get information about the index of $\mathscr{H}_\mathfrak{b}$ in $\mathfrak{o}^n$ via the identity

$$|\mathfrak{o}^n/\mathscr{H}_\mathfrak{b}||\mathscr{H}_\mathfrak{b}/{}^G\mathfrak{b}^n| = |\mathfrak{o}^n/{}^G\mathfrak{b}^n| = (\mathrm{N}^G\mathfrak{b})^n. \tag{3.4}$$

Lemma 3.7 is of the expected magnitude, which we can see by considering the case of the standard diagonal quadratic form $F(\boldsymbol{X}) = \sum_{i=1}^n c_i X_i^2$, for example, with nonzero $c_1, \dots, c_n \in \mathfrak{o}$. In this case, $G = \{\mathrm{id}\}$ and ${}^G\mathfrak{b} = \mathfrak{b}$. It therefore follows that $|\mathscr{H}_\mathfrak{b}/{}^G\mathfrak{b}^n| \ll 1$ since $\mathscr{H}_\mathfrak{b} = (2c_1)^{-1}\mathfrak{b} \times \cdots \times (2c_n)^{-1}\mathfrak{b}$.

Proof of Lemma 3.7. Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be a set of vectors as in Definition 3.6. By scaling these vectors with a rational integer, we may assume that $\mathbf{v}_i \in \mathfrak{o}^n$ for all $1 \leqslant i \leqslant n$. We define the auxiliary set

$$\widetilde{\mathscr{H}_\mathfrak{b}} = \{\mathbf{h} \in \mathfrak{o}^n : 2B(\mathbf{v}_i;\ \mathbf{h}) \in \mathfrak{b},\ \forall 1 \leqslant i \leqslant n\},$$

and observe that $\mathscr{H}_\mathfrak{b} \subset \widetilde{\mathscr{H}_\mathfrak{b}}$. Next, consider the map

$$\varphi : \mathfrak{o}^n \to \mathfrak{o}^n, \quad \mathbf{h} \mapsto (2B(\mathbf{v}_i; \mathbf{h}))_{1 \leqslant i \leqslant n},$$

which is injective by the definition of admissibility in Definition 3.6. Let Γ be the image of $\mathfrak{o}^n$ under the map φ. Then φ induces an isomorphism

$$\mathfrak{o}^n/\widetilde{\mathscr{H}_\mathfrak{b}} \cong \Gamma/(\mathfrak{b}^n \cap \Gamma).$$

Note that Γ only depends on $B(\boldsymbol{X}; \boldsymbol{Y})$ and vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ and hence can be taken to be independent of the ideal $\mathfrak{b}$. As in Equation (3.4), we therefore obtain

$$|\mathscr{H}_\mathfrak{b}/{}^G\mathfrak{b}^n| \leqslant |\widetilde{\mathscr{H}_\mathfrak{b}}/{}^G\mathfrak{b}^n| = \frac{|\mathfrak{o}^n/{}^G\mathfrak{b}^n|}{|\mathfrak{o}^n/\widetilde{\mathscr{H}_\mathfrak{b}}|} = \frac{(\mathrm{N}^G\mathfrak{b})^n}{|\Gamma/(\mathfrak{b}^n \cap \Gamma)|} \leqslant C_\Gamma \frac{(\mathrm{N}^G\mathfrak{b})^n}{(\mathrm{N}\,\mathfrak{b})^n},$$

where C_Γ is a constant only depending on Γ. Moreover, there is an ideal $\mathfrak{d}_2$ such that $|\Gamma/(\mathfrak{b}^n \cap \Gamma)| = (\mathrm{N}\,\mathfrak{b})^n$ whenever $(\mathfrak{d}_2, \mathfrak{b}) = 1$. This completes the proof of the lemma. □

4. Enter the circle method

Our primary tool in this paper is a number field version of the Hardy–Littlewood circle method to interpret the function δ_K in Equation (1.6). Let K be a totally real Galois extension of $\mathbb{Q}$ of degree d. Let $Q \geqslant 1$, and let $\alpha \in \mathfrak{o}$. Then we shall use the version worked out by Browning and Vishe [2, Thm. 1.2]. This states that there exists a positive constant $c_Q = 1 + O_A(Q^{-A})$, for any $A > 0$ and an infinitely differentiable function $h : (0, \infty) \times \mathbb{R} \to \mathbb{R}$ such that

$$\delta_K(\alpha) = \frac{c_Q}{Q^{2d}} \sum_{(0) \neq \mathfrak{b} \subseteq \mathfrak{o}} \sideset{}{^*}\sum_{\sigma \,(\mathrm{mod}\,\mathfrak{b})} \sigma(\alpha) h\left(\frac{\mathrm{N}\,\mathfrak{b}}{Q^d}, \frac{|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|}{Q^{2d}}\right), \tag{4.1}$$

where $\mathrm{N}\,\mathfrak{b} = |\mathfrak{o}/\mathfrak{b}|$ denotes the norm of the ideal $\mathfrak{b}$ and the notation $\sum^*_{\sigma\,(\mathrm{mod}\,\mathfrak{b})}$ means that the sum is taken over primitive additive characters modulo $\mathfrak{b}$. Furthermore, we have $h(x,y) \ll x^{-1}$ and $h(x,y) \neq 0$ only if $x \leqslant \max\{1, 2|y|\}$.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We fix some notation before proceeding further. Let D_K be the discriminant of K, and note that $D_K > 0$ since K is totally real. Let $\rho_1, \dots, \rho_d : K \hookrightarrow \mathbb{R}$ be the distinct real embeddings of K, and let $V = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^d$. There is a canonical embedding $K \hookrightarrow V$ given by $\alpha \mapsto (\rho_1(\alpha), \dots, \rho_d(\alpha))$. We identify K with its image in V. If $v = (v_1, \dots, v_d) \in V$, then we extend the norm and trace on K to get functions $\mathrm{Nm}(v) : V \to \mathbb{R}$ and $\mathrm{Tr}(v) : V \to \mathbb{R}$, with

$$\mathrm{Nm}(v) = \prod_{l=1}^{d} v_l, \quad \mathrm{Tr}(v) = \sum_{l=1}^{d} v_l.$$

We extend the absolute value on $\mathbb{R}$ to give a norm on V via $|v| = \max_{1 \leqslant l \leqslant d} |v_l|$, which we extend to V^n in the obvious way.

Let $N \in \mathfrak{o}$ and let $F(X_1, \dots, X_n)$ be a generalised quadratic form defined over $\mathfrak{o}$. Our central concern is with the asymptotic behaviour of the sum

$$N_W(F, N; P) = \sum_{\substack{\mathbf{x} \in \mathfrak{o}^n \\ F(\mathbf{x}) = N}} W(\mathbf{x}/P),$$

as $P \to \infty$, for $W \in \mathscr{W}_n^+(V)$, where $\mathscr{W}_n^+(V)$ is the class of smooth weight functions described in [2, §2.2]. Our goal in this section is to lay some groundwork that will be useful for Theorems 1.3–1.5 but which applies to arbitrary generalised quadratic forms.

First, in §4.1 we shall discuss the link between the descended system associated to F and the 'embedded system' that arises from looking at all of the different real embeddings of F. In §4.2, we shall construct the weight function W that features in our counting function $N_W(F, N; P)$. In §4.3, we shall combine Equation (4.1) with Poisson summation in order to arrive at a preliminary expression for $N_W(F, N; P)$ in Lemma 4.1. In §4.4, we make some preliminary investigations into exponential sums and similarly for exponential integrals in §4.5. In §4.6, we shall discuss the main term that comes from the trivial character after Poisson summation is applied. Finally, in §4.7 we shall make some initial observations concerning the contribution from the nontrivial characters.

4.1. The embedded system

Let $F(X_1, \dots, X_n)$ be a generalised quadratic form, and let $\{\omega_1, \dots, \omega_d\}$ be a $\mathbb{Z}$-basis for $\mathfrak{o}$. We have seen in Equation (1.2) how there is a descended system $\{Q_1, \dots, Q_d\}$ of quadratic forms, that is associated to F via

$$F(X_1, \dots, X_n) = \sum_{1 \leqslant i \leqslant d} \omega_i Q_i(\mathbf{U}_1, \dots, \mathbf{U}_d),$$

with variables $\mathbf{U}_l = (U_{l1}, \dots, U_{ln})$ for $1 \leqslant l \leqslant d$.

We will need to be able to relate the descended system to the *embedded system*, which amounts to how $F(\mathbf{x})$ embeds in V for given $\mathbf{x} \in K^n$. We extend $F : K^n \to K$ to get a map $V^n \to V$, through the identification of K with V. Associated to $\mathbf{x}$ is the vector $(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)})$, with $\mathbf{x}^{(l)} \in \mathbb{R}^n$ for $1 \leqslant l \leqslant d$. Let $l \in \{1, \dots, d\}$. To any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ may be associated a unique integer $l_\tau \in \{1, \dots, d\}$ such that Equation (1.4) holds. Then we

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

define

$$F^{(l)}(\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)}) = \sum_{1\leqslant i,j\leqslant n}\sum_{\tau,\tau'\in \mathrm{Gal}(K/\mathbb{Q})} c^{(l)}_{i,j,\tau,\tau'} x_i^{(l_{\tau^{-1}})} x_j^{(l_{\tau'^{-1}})}, \tag{4.2}$$

where $c'^{(l)}_{i,j,\tau,\tau} = \rho_l(c_{i,j,\tau,\tau'}) \in \mathbb{R}$. With this notation, we have

$$\rho_l(F(\mathbf{x})) = F^{(l)}(\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)}).$$

Thus, $\rho_l(F(\mathbf{x}))$ is a real quadratic form in the dn variables $\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)}$. We call $\{F^{(1)},\dots,F^{(d)}\}$ the *embedded system*. In particular, it is clear that $N_{K/\mathbb{Q}}(F(\mathbf{x})) = \mathrm{Nm}(F(\mathbf{x}))$ and

$$\mathrm{Tr}(vF(\mathbf{x})) = \sum_{1\leqslant l\leqslant d} v_l \rho_l\left(F(\mathbf{x})\right), \tag{4.3}$$

for any $v = (v_1,\dots,v_d) \in V$ and $\mathbf{x} \in V^n$, identities that we shall often make use of in our analysis of the exponential integrals in §4.5.

Note that if F is a standard quadratic form, then $\rho_l(F(\mathbf{x})) = F^{(l)}(\mathbf{x}^{(l)})$ for $1 \leqslant l \leqslant d$. One positive effect of this is that the relevant oscillatory integrals factorise into a product of d integrals, one for each embedding. The situation is much more complicated for generalised quadratic forms since there is usually no such factorisation.

Let $\mathbf{A} = (\omega_j^{(i)})_{1\leqslant i,j\leqslant d}$, where $\omega_j^{(i)} = \rho_i(\omega_j)$. Then $(\det \mathbf{A})^2 = D_K$. Moreover, on recalling that $\mathbf{x} = \omega_1\mathbf{u}_1 + \cdots + \omega_d\mathbf{u}_d$, we have

$$\begin{pmatrix} \mathbf{x}^{(1)} \\ \vdots \\ \mathbf{x}^{(d)} \end{pmatrix} = \mathbf{W} \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_d \end{pmatrix}, \tag{4.4}$$

where $\mathbf{W}$ is the $dn \times dn$ block matrix

$$\mathbf{W} = \begin{pmatrix} \omega_1^{(1)}\mathbf{I}_n & \omega_2^{(1)}\mathbf{I}_n & \dots & \omega_d^{(1)}\mathbf{I}_n \\ \omega_1^{(2)}\mathbf{I}_n & \omega_2^{(2)}\mathbf{I}_n & \dots & \omega_d^{(2)}\mathbf{I}_n \\ \dots & \dots & \dots & \dots \\ \omega_1^{(d)}\mathbf{I}_n & \omega_2^{(d)}\mathbf{I}_n & \dots & \omega_d^{(d)}\mathbf{I}_n \end{pmatrix}. \tag{4.5}$$

Switching appropriate rows and columns takes $\mathbf{W}$ to $\mathrm{Diag}(\mathbf{A},\dots,\mathbf{A})$, whence $\det \mathbf{W} = (\det \mathbf{A})^n = D_K^{n/2}$. In particular, it follows that

$$F^{(l)}(\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)}) = \sum_{1\leqslant i\leqslant d} \omega_i^{(l)} Q_i(\mathbf{u}_1\dots,\mathbf{u}_d),$$

for any $1 \leqslant l \leqslant d$, under the transformation (4.4).

4.2. Construction of the weight W

We assume that the descended system is of codimension d and has a nonsingular real point. This means that there exists $\underline{\boldsymbol{\xi}} = (\boldsymbol{\xi}_1,\dots,\boldsymbol{\xi}_d) \in \mathbb{R}^{dn}$ such that $J_{Q_1,\dots,Q_d}(\underline{\boldsymbol{\xi}})$ has rank

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

d, where

$$J_{Q_1,\dots,Q_d} = \left(\frac{\partial}{\partial X_j^{(k)}} Q_l \right)_{\substack{1 \leqslant l \leqslant d \\ 1 \leqslant k \leqslant d, 1 \leqslant j \leqslant n}}$$

is the associated $d \times dn$ Jacobian matrix. Define the smooth weight function

$$w(x) = \begin{cases} e^{-1/(1-x^2)} & \text{if } |x| < 1, \\ 0 & \text{if } |x| \geqslant 1, \end{cases}$$

and let $\delta > 0$ be a small parameter. In this paper, we shall work with the weight function $W : V^n \to \mathbb{R}_{\geqslant 0}$, which is given by

$$W(\mathbf{x}) = w(\delta^{-1} |\mathbf{W}^{-1}\mathbf{x} - \underline{\boldsymbol{\xi}}|),$$

where $\mathbf{x}$ is identified with $(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)})$, and where $\mathbf{W}$ is the matrix in Equation (4.5). It is clear that W is infinitely differentiable and that it is supported on the region $|\mathbf{W}^{-1}\mathbf{x} - \underline{\boldsymbol{\xi}}| \leqslant \delta$. Ultimately, we will want to work with a value of δ that is sufficiently small but which still satisfies $1 \ll \delta \leqslant 1$ for an absolute implied constant.

4.3. Poisson summation

It follows from Equation (4.1) that

$$\begin{aligned} &N_W(F, N; P) \\ &\quad = \frac{c_Q}{Q^{2d}} \sum_{\mathfrak{b}} \sideset{}{^*}\sum_{\sigma \,(\mathrm{mod}\, \mathfrak{b})} \sum_{\mathbf{x} \in \mathfrak{o}^n} \sigma(F(\mathbf{x}) - N) W(\mathbf{x}/P) h\left(\frac{\mathrm{N}\mathfrak{b}}{Q^d}, \frac{|N_{K/\mathbb{Q}}(F(\mathbf{x}) - N)|}{Q^{2d}} \right), \end{aligned} \tag{4.6}$$

for any $Q \geqslant 1$. Here, the constant c_Q satisfies $c_Q = 1 + O_A(Q^{-A})$, for any $A > 0$. Furthermore, we have $h(x,y) \ll x^{-1}$ for all y and $h(x,y) \neq 0$ only if $x \leqslant \max\{1, 2|y|\}$.

In our work, we will take $Q = P$ and we henceforth follow the convention that the implied constant in any estimate involving W is allowed to depend implicitly on the parameters that enter into its definition of $\mathscr{W}_n(V)$ in [2, §2.2]. Likewise, the integer N and the number field K are considered fixed once and for all so that all implied constants are allowed to depend implicitly on N and K. In view of the fact that $h(x,y) \neq 0$ only if $x \leqslant \max(1, 2|y|)$, it is clear that the sum over $\mathfrak{b}$ is restricted to $\mathrm{N}\mathfrak{b} \ll Q^d = P^d$.

If F were a standard quadratic form over $\mathfrak{o}$, we would proceed by breaking the sum over $\mathbf{x}$ into residue classes modulo $\mathfrak{b}$ before executing an application of Poisson summation. This would ultimately lead to an expression of the form [2, Thm. 5.1]. For generalised quadratic forms F, this route is not directly accessible, since for given $\mathbf{a}, \mathbf{h} \in \mathfrak{o}^n$ and any primitive character σ modulo $\mathfrak{b}$, one may have $\sigma(F(\mathbf{a}+\mathbf{h})) \neq \sigma(F(\mathbf{a}))$ even when $\mathbf{h} \in \mathfrak{b}^n$. In this way, we see that a special role will be played by the set $\mathscr{H}_{\mathfrak{b}}$ that was introduced in §3.3.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Lemma 4.1. *We have*

$$N_W(F,N;P)=\frac{c_P P^{(n-2)d}}{D_K^{n/2}}\sum_{\mathrm{N}\,\mathfrak{b}\ll P^d}\sum_{\mathbf{m}\in\widehat{{}^G\mathfrak{b}}^n}(\mathrm{N}\,{}^G\mathfrak{b})^{-n}S_{\mathfrak{b}}(N;\mathbf{m})I_{\mathfrak{b}}(N/P^2;P\mathbf{m}),$$

where the sum over $\mathfrak{b}$ *is over nonzero integral ideals and*

$$S_{\mathfrak{b}}(N;\mathbf{m})=\sum_{\sigma\,(\mathrm{mod}\,\mathfrak{b})}^{*}\sum_{\mathbf{a}\,(\mathrm{mod}\,{}^G\mathfrak{b})}\sigma(F(\mathbf{a})-N)\psi(\mathbf{m}.\mathbf{a}),$$

$$I_{\mathfrak{b}}(t;\mathbf{k})=\int_{V^n}W(\mathbf{x})h\left(\frac{\mathrm{N}\,\mathfrak{b}}{P^d},|\mathrm{Nm}(F(\mathbf{x})-t)|\right)\psi(-\mathbf{k}.\mathbf{x})\,\mathrm{d}\mathbf{x}.$$

Proof. Our approach is based on breaking the $\mathbf{x}$-sum in Equation (4.6) into residue classes modulo ${}^G\mathfrak{b}$. Since $Q=P$ and ${}^G\mathfrak{b}^n\subset\mathscr{H}_{\mathfrak{b}}$, it follows that this sum equals

$$\sum_{\mathbf{a}\in(\mathfrak{o}/{}^G\mathfrak{b})^n}\sigma(F(\mathbf{a})-N)\sum_{\mathbf{x}\in{}^G\mathfrak{b}^n}W((\mathbf{x}+\mathbf{a})/P)\,h\left(\frac{\mathrm{N}\,\mathfrak{b}}{P^d},\frac{|N_{K/\mathbb{Q}}(F(\mathbf{x}+\mathbf{a})-N)|}{P^{2d}}\right),$$

for any primitive character σ modulo $\mathfrak{b}$. We apply the multidimensional Poisson summation formula (cf. [2, §5]). Recalling that K is totally real, we find that the inner $\mathbf{x}$-sum is equal to

$$\frac{1}{D_K^{n/2}(\mathrm{N}\,{}^G\mathfrak{b})^n}\sum_{\mathbf{m}\in\widehat{{}^G\mathfrak{b}}^n}\psi(\mathbf{m}.\mathbf{a})\int_{V^n}W(\mathbf{x}/P)h\left(\frac{\mathrm{N}\,\mathfrak{b}}{P^d},\frac{|\mathrm{Nm}(F(\mathbf{x})-N)|}{P^{2d}}\right)\psi(-\mathbf{m}.\mathbf{x})\mathrm{d}\mathbf{x},$$

where we recall that $\widehat{{}^G\mathfrak{b}}={}^G\mathfrak{b}^{-1}\mathfrak{d}^{-1}$ is the dual of ${}^G\mathfrak{b}$. Putting everything together in Equation (4.6), we have therefore established that

$$N_W(F,N;P)=\frac{c_P}{D_K^{n/2}P^{2d}}\sum_{\mathrm{N}\,\mathfrak{b}\ll P^d}\sum_{\mathbf{m}\in\widehat{{}^G\mathfrak{b}}^n}(\mathrm{N}\,{}^G\mathfrak{b})^{-n}S_{\mathfrak{b}}(N;\mathbf{m})\tilde{I}_{\mathfrak{b}}(\mathbf{m}),$$

with $S_{\mathfrak{b}}(N;\mathbf{m})$ as in the statement of the lemma and

$$\tilde{I}_{\mathfrak{b}}(\mathbf{m})=\int_{V^n}W(\mathbf{x}/P)h\left(\frac{\mathrm{N}\,\mathfrak{b}}{P^d},\frac{|\mathrm{Nm}(F(\mathbf{x})-N)|}{P^{2d}}\right)\psi(-\mathbf{m}.\mathbf{x})\,\mathrm{d}\mathbf{x}.$$

A simple change of variables yields $\tilde{I}_{\mathfrak{b}}(\mathbf{m})=P^{dn}I_{\mathfrak{b}}(N/P^2;P\mathbf{m})$, as required. □

4.4. The exponential sum

We proceed by discussing $S_{\mathfrak{b}}(N;\mathbf{m})$ in Lemma 4.1, for $\mathbf{m}\in\widehat{{}^G\mathfrak{b}}^n$. Let $\gamma=g/\alpha\in\mathfrak{F}(\mathfrak{b})$ be as in Lemma 3.4. Then we have

$$\sum_{\sigma\,(\mathrm{mod}\,\mathfrak{b})}^{*}\sigma(x)=\sum_{a\in(\mathfrak{o}/\mathfrak{b})^*}\psi(\gamma ax),$$

for any $x\in\mathfrak{o}$. It follows that

$$S_{\mathfrak{b}}(N;\mathbf{m})=\sum_{a\in(\mathfrak{o}/\mathfrak{b})^*}\psi(-\gamma aN)\sum_{\mathbf{x}\,(\mathrm{mod}\,{}^G\mathfrak{b})}\psi(\gamma aF(\mathbf{x})+\mathbf{m}.\mathbf{x}).\tag{4.7}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Our work hinges upon the following upper bound for this sum.

Lemma 4.2. *We have*

$$|S_{\mathfrak{b}}(N;\mathbf{m})| \leqslant |(\mathfrak{o}/\mathfrak{b})^*||\mathscr{H}_{\mathfrak{b}}/{}^G\mathfrak{b}^n|^{1/2}|\mathfrak{o}/{}^G\mathfrak{b}|^{n/2},$$

where $\mathscr{H}_{\mathfrak{b}}$ is given by Equation (3.3).

Proof. For fixed $a \in (\mathfrak{o}/\mathfrak{b})^*$, we have

$$\begin{aligned}\Bigg|\sum_{\mathbf{x}\,(\mathrm{mod}\,{}^G\mathfrak{b})} \psi(\gamma a F(\mathbf{x}) + \mathbf{m}.\mathbf{x})\Bigg|^2 &= \sum_{\mathbf{h}\,(\mathrm{mod}\,{}^G\mathfrak{b})} \sum_{\mathbf{u}\,(\mathrm{mod}\,{}^G\mathfrak{b})} \psi(\gamma a(F(\mathbf{u}+\mathbf{h}) - F(\mathbf{u})) + \mathbf{m}.\mathbf{h}) \\ &\leqslant \sum_{\mathbf{h}\,(\mathrm{mod}\,{}^G\mathfrak{b})} \Bigg|\sum_{\mathbf{u}\,(\mathrm{mod}\,{}^G\mathfrak{b})} \psi(2\gamma a B(\mathbf{u};\mathbf{h}))\Bigg|\end{aligned}$$

in the notation of Equation (3.2). We observe that the function $\mathbf{u} \mapsto \psi(2\gamma a B(\mathbf{u};\mathbf{h}))$ is a character modulo ${}^G\mathfrak{b}^n$, and it is the trivial character precisely when

$$2\gamma a B(\mathbf{u};\mathbf{h}) \in \mathfrak{d}^{-1}, \qquad \forall \mathbf{u} \in (\mathfrak{o}/{}^G\mathfrak{b})^n.$$

We rewrite γ in the form $\gamma = g/\alpha$ with $(\alpha) = \mathfrak{b}\mathfrak{d}\mathfrak{p}_1$ for some prime ideal $\mathfrak{p}_1$ and $g \in \mathfrak{p}_1 \cap \mathbb{Z}$ with the property that $((g),\mathfrak{d}^G\mathfrak{b}) = 1$. Thus, the above condition is equivalent to the condition

$$2gaB(\mathbf{u};\mathbf{h}) \in (\alpha)\mathfrak{d}^{-1} = \mathfrak{b}\mathfrak{p}_1, \qquad \forall \mathbf{u} \in (\mathfrak{o}/{}^G\mathfrak{b})^n.$$

Since $a \in (\mathfrak{o}/\mathfrak{b})^*$, $g \in \mathfrak{p}_1$ and $((g),\mathfrak{d}^G\mathfrak{b}) = 1$, this is equivalent to saying that

$$2B(\mathbf{u};\mathbf{h}) \in \mathfrak{b}, \qquad \forall \mathbf{u} \in (\mathfrak{o}/{}^G\mathfrak{b})^n.$$

Finally, since this condition on $\mathbf{u}$ is invariant modulo ${}^G\mathfrak{b}^n$, this is equivalent to the condition $2B(\mathbf{u};\mathbf{h}) \in \mathfrak{b}$, for all $\mathbf{u} \in \mathfrak{o}^n$, which is equivalent to specifying that $\mathbf{h} \in \mathscr{H}_{\mathfrak{b}}$, by Equation (3.3). The statement of the lemma now follows. □

Corollary 4.3. *Assume that F is admissible in the sense of Definition 3.6. Let $\mathfrak{b}$ be an integral ideal, and let $\mathbf{m} \in K^n$. Then $S_{\mathfrak{b}}(N;\mathbf{m}) \ll (\mathrm{N}\,\mathfrak{b})^{1-n/2}(\mathrm{N}^G\mathfrak{b})^n$.*

Proof. This follows from combining Lemmas 3.7 and 4.2. □

It is straightforward to show that $S_{\mathfrak{b}}(N;\mathbf{m})$ vanishes unless $\mathbf{m}$ satisfies additional constraints, as demonstrated in the following result.

Lemma 4.4. *We have $S_{\mathfrak{b}}(N;\mathbf{m}) = 0$ unless $\mathbf{m}.\mathbf{h} \in \mathfrak{d}^{-1}$ for all $\mathbf{h} \in \mathscr{H}_{\mathfrak{b}}$.*

Proof. Returning to the definition of $S_{\mathfrak{b}}(N;\mathbf{m})$ in Lemma 4.1 and noting that ${}^G\mathfrak{b}^n \subset \mathscr{H}_{\mathfrak{b}} \subset \mathfrak{o}^n$, we may write

$$S_{\mathfrak{b}}(N;\mathbf{m}) = \sideset{}{^*}\sum_{\sigma\,(\mathrm{mod}\,\mathfrak{b})} \sum_{\mathbf{a}\in\mathfrak{o}^n/\mathscr{H}_{\mathfrak{b}}} \sigma(-N) \sum_{\mathbf{h}\in\mathscr{H}_{\mathfrak{b}}/{}^G\mathfrak{b}^n} \sigma(F(\mathbf{a}))\psi(\mathbf{m}.\mathbf{a})\psi(\mathbf{m}.\mathbf{h}).$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

However, orthogonality of characters gives

$$\sum_{\mathbf{h}\in\mathscr{H}_{\mathfrak{b}}/{}^{G}\mathfrak{b}^{n}}\psi(\mathbf{m}.\mathbf{h})=\begin{cases}|\mathscr{H}_{\mathfrak{b}}/{}^{G}\mathfrak{b}^{n}| & \text{if } \mathbf{m}.\mathbf{h}\in\mathfrak{d}^{-1}\ \forall\mathbf{h}\in\mathscr{H}_{\mathfrak{b}}/{}^{G}\mathfrak{b}^{n},\\ 0 & \text{otherwise.}\end{cases}$$

Since we automatically have $\mathbf{m}.\mathbf{h}\in\mathfrak{d}^{-1}$ for any $\mathbf{m}\in\widehat{{}^{G}\mathfrak{b}}^{n}$ and $\mathbf{h}\in{}^{G}\mathfrak{b}^{n}$, the statement of the lemma follows. □

We shall also need to establish a multiplicativity property for the exponential sums. This is achieved in the following result.

Lemma 4.5. *Let $\mathfrak{b}$ be a nonzero integral ideal, and suppose that $\mathfrak{b}=\mathfrak{b}_1\mathfrak{b}_2$ for integral ideals $\mathfrak{b}_1,\mathfrak{b}_2$ such that $\gcd(\mathrm{N}\,\mathfrak{b}_1,\mathrm{N}\,\mathfrak{b}_2)=1$. Then, for any $N\in\mathfrak{o}$ and any $\mathbf{m}\in\widehat{{}^{G}\mathfrak{b}}^{n}$, we have*

$$S_{\mathfrak{b}}(N;\mathbf{m})=S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^{2}N;(\mathrm{N}\,\mathfrak{b}_2)\mathbf{m})S_{\mathfrak{b}_2}(\overline{\mathrm{N}\,\mathfrak{b}_1}^{2}N;(\mathrm{N}\,\mathfrak{b}_1)\mathbf{m}).$$

Proof. According to Lemma 3.4, there exists $\gamma=g/\alpha\in\mathfrak{F}(\mathfrak{b})$ such that $\psi(\gamma\cdot)$ is a primitive character modulo $\mathfrak{b}$. Then, Equation (4.7) implies that

$$S_{\mathfrak{b}}(N;\mathbf{m})=\sum_{a\in(\mathfrak{o}/\mathfrak{b})^{*}}\psi(-\gamma aN)\sum_{\mathbf{x}\,(\mathrm{mod}\,{}^{G}\mathfrak{b})}\psi\left(\gamma aF(\mathbf{x})+\mathbf{m}.\mathbf{x}\right).$$

Let us write $\mathrm{N}\,\mathfrak{b}_i=b_i$ for $i=1,2$. The assumption $\gcd(b_1,b_2)=1$ implies that $({}^{G}\mathfrak{b}_1,{}^{G}\mathfrak{b}_2)=1$. Moreover, we have $b_1\in\mathfrak{b}_1$, $b_2\in\mathfrak{b}_2$ and

$$((b_1),\mathfrak{b}_2)=((b_2),\mathfrak{b}_1)=1. \tag{4.8}$$

According to Lemma 3.1(i), we find elements $\lambda,\mu\in\mathfrak{o}$ such that $\mathrm{ord}_{\mathfrak{p}}(\lambda)=\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}_1)$ and $\mathrm{ord}_{\mathfrak{p}}(\mu)=\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}_2)$ for all $\mathfrak{p}\mid{}^{G}\mathfrak{b}_1{}^{G}\mathfrak{b}_2$. It follows from the Chinese remainder theorem, in the form Lemma 3.2, that we can write $a=\mu b+\lambda c$ for $b\,(\mathrm{mod}\,\mathfrak{b}_1)$ and $c\,(\mathrm{mod}\,\mathfrak{b}_2)$. Likewise, we claim that we can write $\mathbf{x}=b_2\mathbf{b}+b_1\mathbf{c}$, for $\mathbf{b}\,(\mathrm{mod}\,{}^{G}\mathfrak{b}_1)$ and $\mathbf{c}\,(\mathrm{mod}\,{}^{G}\mathfrak{b}_2)$. To prove the claim it suffices to show that there is an isomorphism $\mathfrak{o}/{}^{G}\mathfrak{b}_1\times\mathfrak{o}/{}^{G}\mathfrak{b}_2\to\mathfrak{o}/{}^{G}\mathfrak{b}$, given by $(u,v)\mapsto b_2u+b_1v$. This map is clearly well defined since $b_1\in{}^{G}\mathfrak{b}_1$ and $b_2\in{}^{G}\mathfrak{b}_2$. Moreover, injectivity follows from the coprimality conditions $((b_2),{}^{G}\mathfrak{b}_1)=((b_1),{}^{G}\mathfrak{b}_2)=1$, which are a direct consequence of Equation (4.8). The claim follows, since the cardinalities are the same, by the Chinese remainder theorem.

In summary, on observing that $b_1\in{}^{G}\mathfrak{b}_1$ and $b_2\in{}^{G}\mathfrak{b}_2$, it follows that

$$\begin{aligned}S_{\mathfrak{b}}(N;\mathbf{m})=&\sum_{\substack{b\in(\mathfrak{o}/\mathfrak{b}_1)^{*}\\ c\in(\mathfrak{o}/\mathfrak{b}_2)^{*}}}\psi(-\gamma(\mu b+\lambda c)N)\\ &\times\sum_{\substack{\mathbf{b}\,(\mathrm{mod}\,{}^{G}\mathfrak{b}_1)\\ \mathbf{c}\,(\mathrm{mod}\,{}^{G}\mathfrak{b}_2)}}\psi\left(\gamma(\mu b+\lambda c)F(b_2\mathbf{b}+b_1\mathbf{c})+\mathbf{m}.(b_2\mathbf{b}+b_1\mathbf{c})\right)\\ =&\sum_{b\in(\mathfrak{o}/\mathfrak{b}_1)^{*}}\psi(-\gamma\mu bN)\sum_{\mathbf{b}\,(\mathrm{mod}\,{}^{G}\mathfrak{b}_1)}\psi\left(\gamma\mu b_2^{2}bF(\mathbf{b})+b_2\mathbf{m}.\mathbf{b}\right)\\ &\times\sum_{c\in(\mathfrak{o}/\mathfrak{b}_2)^{*}}\psi(-\gamma\lambda cN)\sum_{\mathbf{c}\,(\mathrm{mod}\,{}^{G}\mathfrak{b}_2)}\psi\left(\gamma\lambda b_1^{2}cF(\mathbf{c})+b_1\mathbf{m}.\mathbf{c}\right).\end{aligned}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We claim that $\psi(\gamma\mu b_2^2\cdot)$ defines a primitive character modulo $\mathfrak{b}_1$. For this, we note that

$$\beta \in \mathfrak{a}_{\gamma\mu b_2^2} \Leftrightarrow \gamma\mu b_2^2\beta \in \mathfrak{o} \Leftrightarrow (g\mu b_2^2\beta) \subset (\alpha) \Leftrightarrow \mathfrak{b}_1\mathfrak{d} \mid (\mu b_2^2\mathfrak{b}_2^{-1})(g\mathfrak{p}_1^{-1})(\beta)$$

since $b_2 \in \mathfrak{b}_2$ and $g \in \mathfrak{p}_1$. Now, (g) is coprime to $\mathfrak{b}_1\mathfrak{d}$ and (μb_2) is coprime to $\mathfrak{b}_1$. Thus, it follows that

$$\beta \in \mathfrak{a}_{\gamma\mu b_2^2} \Leftrightarrow \beta \in \mathfrak{b}_1\mathfrak{e},$$

where $\mathfrak{e} = \mathfrak{d}/(\mathfrak{d}, \mu b_2^2\mathfrak{b}_2^{-1})$. Clearly, $\mathfrak{e} \mid \mathfrak{d}$. We claim that $(\mathfrak{d}/\mathfrak{e}, \mathfrak{b}_1) = 1$. To see this, note that $\mathfrak{d}/\mathfrak{e}$ is equal to the common divisor $(\mathfrak{d}, \mu b_2^2\mathfrak{b}_2^{-1})$. Now, μ is coprime to $\mathfrak{b}_1$ and so is $\mathfrak{b}_2$. Hence, the common divisor of these ideals most be coprime to the ideal $\mathfrak{b}_1$, as claimed. Thus, Lemma 3.3 establishes the claim that $\psi(\gamma\mu b_2^2\cdot)$ is a primitive character modulo $\mathfrak{b}_1$. It follows that

$$\sum_{b \in (\mathfrak{o}/\mathfrak{b}_1)^*} \psi(-\gamma\mu bN) \sum_{\mathbf{b} \,(\mathrm{mod}^G \mathfrak{b}_1)} \psi\left(\gamma\mu b_2^2 bF(\mathbf{b}) + b_2\mathbf{m}.\mathbf{b}\right) = S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2 N; (\mathrm{N}\,\mathfrak{b}_2)\mathbf{m}),$$

where $\overline{\mathrm{N}\,\mathfrak{b}_2}$ is the multiplicative inverse of $\mathrm{N}\,\mathfrak{b}_2$ modulo $\mathfrak{b}_1$. Similarly,

$$\sum_{c \in (\mathfrak{o}/\mathfrak{b}_2)^*} \psi(-\gamma\lambda cN) \sum_{\mathbf{c} \,(\mathrm{mod}^G \mathfrak{b}_2)} \psi\left(\gamma\lambda b_1^2 cF(\mathbf{c}) + b_1\mathbf{m}.\mathbf{c}\right) = S_{\mathfrak{b}_2}(\overline{\mathrm{N}\,\mathfrak{b}_1}^2 N; (\mathrm{N}\,\mathfrak{b}_1)\mathbf{m}),$$

from which the lemma follows. □

Corollary 4.6. *Let $\mathfrak{b}$ be a nonzero integral ideal, and suppose that $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ for integral ideals $\mathfrak{b}_1, \mathfrak{b}_2$ such that $\gcd(\mathrm{N}\,\mathfrak{b}_1, \mathrm{N}\,\mathfrak{b}_2) = 1$. Then $S_{\mathfrak{b}}(N; \mathbf{0}) = S_{\mathfrak{b}_1}(N; \mathbf{0})S_{\mathfrak{b}_2}(N; \mathbf{0})$.*

Proof. On making an obvious change of variables to the a-sum and the $\mathbf{x}$-sum in Equation (4.7), we note that $S_{\mathfrak{b}}(c^2N; \mathbf{0}) = S_{\mathfrak{b}}(N; \mathbf{0})$ for any $c \in \mathbb{Z}$ which is coprime to $\mathfrak{b}$. The statement now follows from an application of Lemma 4.5. □

4.5. The exponential integral

In this section, we discuss the exponential integral $I_{\mathfrak{b}}(t; \mathbf{k})$ that appears in Lemma 4.1 for given $t \in V$ and $\mathbf{k} \in V^n$. It will be convenient to set

$$0 < \rho = \frac{\mathrm{N}\,\mathfrak{b}}{P^d} \ll 1,$$

with which notation we have

$$I_{\mathfrak{b}}(t; \mathbf{k}) = \int_{V^n} W(\mathbf{x}) h\left(\rho, |\mathrm{Nm}(F(\mathbf{x}) - t)|\right) \psi(-\mathbf{k}.\mathbf{x})\, \mathrm{d}\mathbf{x}.$$

We now bring into play the work in [2, §6]. It follows from an application of Fourier inversion, as in [2, Eq. (6.3)], that there exists a function $p_\rho(v) : V \to \mathbb{C}$ such that

$$I_{\mathfrak{b}}(t; \mathbf{k}) = \int_V p_\rho(v)\psi(-vt)K(v, \mathbf{k})\mathrm{d}v, \tag{4.9}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

where

$$K(v,\mathbf{k}) = \int_{V^n} W(\mathbf{x})\psi\left(vF(\mathbf{x}) - \mathbf{k}.\mathbf{x}\right)\mathrm{d}\mathbf{x}. \tag{4.10}$$

In our analysis, it will be useful to have the notion of a height function on V. Accordingly, we define $\mathfrak{H} : V \to \mathbb{R}_{\geqslant 1}$ via

$$\mathfrak{H}(v) = \prod_{l=1}^{d} \max\{1, |v_l|\},$$

for $v = (v_1, \ldots, v_d) \in V$. In the closing stages of our argument, we will need to estimate integrals involving powers of $\mathfrak{H}(v)$ over various regions in V. First, it follows from [2, Lemma 5.3] that

$$\int_V \mathfrak{H}(v)^{\alpha}\mathrm{d}v \ll 1 \quad \text{if } \alpha < -1. \tag{4.11}$$

We can use this to deduce two further bounds that will play important roles.

For any $A \geqslant 1$ and $\varepsilon > 0$, we claim that

$$\int_{\{v\in V:\mathfrak{H}(v)\geqslant A\}} \mathfrak{H}(v)^{\alpha}\mathrm{d}v \ll A^{\alpha+1+\varepsilon} \quad \text{if } \alpha < -1. \tag{4.12}$$

If $\alpha < -1$, then we can clearly assume that $\varepsilon < -\alpha - 1$. But then the conditions of integration imply that $(\mathfrak{H}(v)/A)^{-\alpha-1-\varepsilon} \geqslant 1$, whence

$$\int_{\{v\in V:\mathfrak{H}(v)\geqslant A\}} \mathfrak{H}(v)^{\alpha}\mathrm{d}v \leqslant A^{\alpha+1+\varepsilon} \int_V \mathfrak{H}(v)^{-1-\varepsilon}\mathrm{d}v \ll A^{\alpha+1+\varepsilon}$$

by Equation (4.11).

Next, for any $B \geqslant 1$ and $\varepsilon > 0$, we claim that

$$\int_{\{v\in V:\mathfrak{H}(v)\leqslant B\}} \mathfrak{H}(v)^{\alpha}\mathrm{d}v \ll B^{\alpha+1+\varepsilon} \quad \text{if } \alpha \geqslant -1. \tag{4.13}$$

To see this, we note that $(B/\mathfrak{H}(v))^{\alpha+1+\varepsilon} \geqslant 1$, under the conditions of the integral, if $\alpha \geqslant -1$. But then

$$\int_{\{v\in V:\mathfrak{H}(v)\leqslant B\}} \mathfrak{H}(v)^{\alpha}\mathrm{d}v \leqslant B^{\alpha+1+\varepsilon} \int_V \mathfrak{H}(v)^{-1-\varepsilon}\mathrm{d}v \ll B^{\alpha+1+\varepsilon}$$

by Equation (4.11).

Returning to the function $p_\rho(v)$ in Equation (4.9), the following result summarises its key properties and is extracted from [2, Lemmas 6.3 and 6.4].

Lemma 4.7. *For any $\varepsilon > 0$, we have $p_\rho(v) \ll P^{\varepsilon}$, for any $v \in V$. Moreover, for any $\varepsilon > 0$ and $A \geqslant 1$, we have*

$$p_\rho(v) \ll_A \rho^{-1}\left(\rho^{-1}P^{\varepsilon}\mathfrak{H}(v)^{-1}\right)^A.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Recall here that $\rho > 0$. The next result is a straightforward consequence of the previous result, once combined with Equation (4.9) and the bound

$$|K(v,\mathbf{k})| \leqslant \int_{V^n} W(\mathbf{x})\mathrm{d}\mathbf{x} \ll 1,$$

which follows from the fact that W is compactly supported.

Corollary 4.8. *Let $\varepsilon > 0$. Let $t \in V$ and $\mathbf{k} \in V^n$. Then*

$$I_{\mathfrak{b}}(t;\mathbf{k}) \ll_A P^{\varepsilon} \int_{\mathscr{U}} |K(v,\mathbf{k})|\mathrm{d}v + P^{-A},$$

for any $A \geqslant 1$, where

$$\mathscr{U} = \mathscr{U}_{\varepsilon} = \left\{ v \in V : \mathfrak{H}(v) \leqslant \frac{P^{d+\varepsilon}}{\mathrm{N}\,\mathfrak{b}} \right\}.$$

It is interesting to pause and reflect on the corresponding situation for cubic forms G over a number field K that was considered in [2], recalling that we are assuming K to be totally real in our setting. In [2], crucial use was made of the fact that the integral over $\mathbf{x}$ factors as

$$\prod_{1 \leqslant l \leqslant d} \int_{\mathbb{R}^n} W^{(l)}(\mathbf{x}^{(l)}) e\left(v^{(l)} G^{(l)}(\mathbf{x}^{(l)}) - \mathbf{k}^{(l)}.\mathbf{x}^{(l)} \right) \mathrm{d}\mathbf{x}^{(l)}$$

since $\mathrm{Tr}(vG(\mathbf{x})) = \sum_{l=1}^{d} v^{(l)} G^{(l)}(\mathbf{x}^{(l)})$, where $G^{(l)} = \rho_l(G)$ is a cubic form over $\mathbb{R}$. We have chosen our main example Equation (1.3) in order that a similar property holds. Such a factorisation is not necessarily enjoyed for arbitrary generalised quadratic forms F, however, and it seems very difficult to analyse the integrals $K(v,\mathbf{k})$ in generic situations.

Define

$$\mathscr{Q}(\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)}) = \sum_{1 \leqslant l \leqslant d} v_l F^{(l)}(\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)}), \tag{4.14}$$

for fixed $v \in V$, where $F^{(l)}$ is the quadratic form (4.2). Thus, $\mathscr{Q}$ is a quadratic form over $\mathbb{R}$ in dn variables. Let us write, temporarily, $\underline{\mathbf{x}} = (\mathbf{x}^{(1)},\dots,\mathbf{x}^{(d)})$ and $\underline{\mathbf{k}} = (\mathbf{k}^{(1)},\dots,\mathbf{k}^{(d)})$. Then, in the light of Equation (4.3), we may write

$$K(v,\mathbf{k}) = \int_{\mathbb{R}^{dn}} W(\underline{\mathbf{x}}) e\left(\mathscr{Q}(\underline{\mathbf{x}}) - \underline{\mathbf{k}}.\underline{\mathbf{x}}\right) \mathrm{d}\underline{\mathbf{x}}. \tag{4.15}$$

A general study of these exponential integrals has been carried out by Heath-Brown and Pierce [6, Lemma 3.1]. Assuming that the support of W is contained in $[-1,1]^{dn}$, we may appeal to their work, which we record here for the convenience of the reader.

Lemma 4.9. *Let $\mathscr{Q} \in \mathbb{R}[X_1,\dots,X_m]$ be a quadratic form with coefficients of maximum modulus $\|\mathscr{Q}\|$ and eigenvalues $\rho_1,\dots,\rho_m$. Let $\boldsymbol{\lambda} \in \mathbb{R}^m$, and suppose that $w : \mathbb{R}^m \to \mathbb{R}$ is any smooth weight function supported on $[-1,1]^m$. Then*

$$\int_{\mathbb{R}^m} w(\mathbf{u}) e\left(\mathscr{Q}(\mathbf{u}) - \boldsymbol{\lambda}.\mathbf{u}\right) \mathrm{d}\mathbf{u} \ll_w \prod_{i=1}^{m} \min\left\{1, |\rho_i|^{-1/2}\right\}.$$

Furthermore, if $|\boldsymbol{\lambda}| \geqslant 4\|\mathscr{Q}\|$, then the integral is $O_{w,A}(|\boldsymbol{\lambda}|^{-A})$ for any $A \geqslant 1$.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We will apply this result with $\boldsymbol{\lambda} = \underline{\mathbf{k}}$ and with the real quadratic form in Equation (4.14). Note that $\|\mathscr{Q}\| \ll |v|$. Next, define

$$\mathscr{F}(v) = \det\left(\sum_{1 \leqslant l \leqslant d} v_l \mathbf{M}^{(l)}\right),$$

where $\mathbf{M}^{(l)}$ is the $dn \times dn$ matrix associated to $F^{(l)}$. The function $\mathscr{F}(v)$ is a real form of degree dn in the variables $v_1, \dots, v_d$. The following estimate is a direct consequence of Lemma 4.9.

Corollary 4.10. *Assume* $|\mathbf{k}| \gg |v|$. *Then* $K(v,\mathbf{k}) \ll_A |\mathbf{k}|^{-A}$, *for any* $A \geqslant 1$. *Moreover,* $K(v,\mathbf{k}) \ll \min\{1, |\mathscr{F}(v)|^{-1/2}\}$ *for any* $\mathbf{k} \in V^n$.

Unfortunately, it appears difficult to extract anything useful from the second bound, unless the generalised quadratic form is assumed to have extra structure.

4.6. Contribution from the trivial character

In this section, we study the overall contribution from the vector $\mathbf{m} = \mathbf{0}$ in the expression for $N_W(F,N;P)$ in Lemma 4.1. This contribution is

$$M(P) = \frac{P^{(n-2)d}}{D_K^{n/2}} \sum_{\substack{0 \neq \mathfrak{b} \subset \mathfrak{o} \\ \mathrm{N}\,\mathfrak{b} \ll P^d}} (\mathrm{N}^G \mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}) I_{\mathfrak{b}}(N/P^2;\mathbf{0}) + O_A(P^{-A})$$

in the notation of that result.

It will ease notation if we put $t = N/P^2 \in \mathbb{R}$. Assuming that the descended system has codimension d, we begin by analysing the exponential integral $I_{\mathfrak{b}}(t;\mathbf{0})$, writing

$$I_{\mathfrak{b}}(t;\mathbf{0}) = \int_{V^n} W(\mathbf{x}) h(\rho, |\mathrm{Nm}(F(\mathbf{x}) - t)|)\, \mathrm{d}\mathbf{x} = \int_V f(v) h(\rho, |\mathrm{Nm}(v)|)\, \mathrm{d}\mathbf{v}, \tag{4.16}$$

where $\rho = \mathrm{N}\,\mathfrak{b}/P^d$ and

$$f(v) = \int_{\substack{\mathbf{x} \in V^n \\ F(\mathbf{x}) - t = v}} W(\mathbf{x}) \mathrm{d}\mathbf{x},$$

where, by an abuse of notation, $\mathrm{d}\mathbf{x}$ is the surface measure obtained by eliminating d variables from the equation $F(\mathbf{x}) - t = v$. We shall think of $f(y)$ as a function of $\mathbf{y} = (y_1, \dots, y_d)$ on $\mathbb{R}^d$, in which t is fixed and bounded absolutely. The following result summarises its main properties.

Lemma 4.11. *Assume that the descended system has codimension d. There exist positive constants* $C, C_0, C_1, \dots$ *such that the function* $f : \mathbb{R}^d \to \mathbb{R}$ *is a smooth weight function that is supported on* $[-C,C]^d$ *and satisfies*

$$\left| \frac{\partial^{i_1 + \dots + i_d}}{\partial y_1^{i_1} \cdots \partial y_d^{i_d}} f(\mathbf{y}) \right| \leqslant C_{i_1 + \dots + i_d}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

for any $\mathbf{y} \in [-C,C]^d$ *and any* $i_1,\dots,i_d \geqslant 0$. *The constants* $C, C_0, C_1, \dots$ *depend only on the coefficients of* F *and the parameter* δ *in the definition of* W.

Proof. In the course of the proof, it will be convenient to write $\underline{\mathbf{s}} = (\mathbf{s}_1,\dots,\mathbf{s}_d)$, $\underline{\mathbf{u}} = (\mathbf{u}_1,\dots,\mathbf{u}_d)$, $\underline{\boldsymbol{\xi}} = (\boldsymbol{\xi}_1,\dots,\boldsymbol{\xi}_d)$ and $\mathbf{t} = (t_1,\dots,t_d)$. Recall the definition of the weight function W in §4.2 for a suitable fixed $\underline{\boldsymbol{\xi}} \in \mathbb{R}^{dn}$. Making the change of variables in Equation (4.4), we see that

$$f(\mathbf{y}) = D_K^{-n/2} \int_{\substack{\underline{\mathbf{u}} \in \mathbb{R}^{dn} \\ Q_l(\underline{\mathbf{u}}) - \tau_l = w_l}} w(\delta^{-1}|\underline{\mathbf{u}} - \underline{\boldsymbol{\xi}}|) \mathrm{d}\underline{\mathbf{u}}, \tag{4.17}$$

where $\boldsymbol{\tau} = \mathbf{A}^{-1}\mathbf{t}$ and $\mathbf{w} = \mathbf{A}^{-1}\mathbf{y}$. It will clearly suffice to prove the properties recorded in the lemma for the integral on the right-hand side, $\widetilde{f}(\mathbf{w})$ say, regarded as a function of $\mathbf{w}$. Making the change of variables $\underline{\mathbf{s}} = \underline{\mathbf{u}} - \underline{\boldsymbol{\xi}}$, we have

$$\widetilde{f}(\mathbf{w}) = \int_{\substack{\underline{\mathbf{s}} \in \mathbb{R}^{dn} \\ Q_l(\underline{\mathbf{s}} + \underline{\boldsymbol{\xi}}) - \tau_l = w_l}} w(\delta^{-1}|\underline{\mathbf{s}}|) \mathrm{d}\underline{\mathbf{s}}.$$

It is now clear that $\widetilde{f}(\mathbf{w}) = 0$ unless $\mathbf{w} \in [-C,C]^d$ for suitable $C > 0$.

Next, we recall that $J_{Q_1,\dots,Q_d}(\underline{\boldsymbol{\xi}})$ has rank d. We may assume without loss of generality that

$$\det\left(\frac{\partial}{\partial U_{j1}} Q_i(\underline{\boldsymbol{\xi}})\right)_{1 \leqslant i,j \leqslant d} \neq 0.$$

Let $\varphi : \mathbb{R}^{dn} \to \mathbb{R}^{dn}$ be given by

$$\underline{\mathbf{s}} \mapsto \left(Q_1(\underline{\mathbf{s}} + \underline{\boldsymbol{\xi}}) - \tau^{(1)}, s_{1,2}, \dots, s_{1,n}, \dots, Q_d(\underline{\mathbf{s}} + \underline{\boldsymbol{\xi}}) - \tau^{(d)}, s_{d,2}, \dots, s_{d,n}\right).$$

The implicit function theorem implies that there exist open subsets $W', W \subset \mathbb{R}^{dn}$ with $\underline{\mathbf{0}} \in W'$ and $\varphi(\underline{\mathbf{0}}) \in W$ such that $\varphi : W' \to W$ is a bijection and has differentiable inverse φ^{-1} on W. It is now clear that we wish to choose $\delta > 0$ small enough to ensure that $\underline{\mathbf{s}} \in W'$ whenever $|\underline{\mathbf{s}}| \leqslant \delta$.

We may now conclude that

$$\widetilde{f}(\mathbf{w}) = \int_{\underline{\mathbf{s}}' \in \mathbb{R}^{d(n-1)}} \partial_1 \varphi^{-1} w(\delta^{-1}|(s_{1,1},\dots,s_{d,n})|) \mathrm{d}\underline{\mathbf{s}}',$$

where $\underline{\mathbf{s}}' = (s_{1,2},\dots,s_{1,n},\dots,s_{d,2},\dots,s_{d,n})$, and $s_{1,1}, s_{2,1}, \dots, s_{d,1}$ are implicitly given by $\underline{\mathbf{s}}'$ and $\mathbf{w}$, and

$$\partial_1 \varphi^{-1} = \det\left(\frac{\partial(\varphi^{-1})_{in+1-n}}{\partial w_j}\right)_{1 \leqslant i,j \leqslant d} \Bigg|_{(s_{1,1},\dots,s_{d,n})}$$

is the associated Jacobian. Since φ^{-1} is smooth, this implies that $\widetilde{f}(\mathbf{w})$ is infinitely differentiable and that its partial derivatives satisfy the bound claimed in the lemma. □

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Now, it follows from Corollary 4.8 that for $t = N/P^2 \in \mathbb{R}$, and ε fixed as in the corollary, we have

$$I_{\mathfrak{b}}(t;\mathbf{0}) \ll \frac{P^{d+2\varepsilon}}{\mathrm{N}\,\mathfrak{b}}.$$

Furthermore, in view of Lemma 4.11, it follows from Equation (4.16) and [2, Lemma 4.1] that

$$I_{\mathfrak{b}}(t;\mathbf{0}) = \sqrt{D_K} f(0) + O_A\left(\left(\frac{\mathrm{N}\,\mathfrak{b}}{P^d}\right)^A\right),$$

for any $A \geqslant 0$, where

$$f(0) = \int_{\substack{\underline{\mathbf{x}} \in \mathbb{R}^{dn} \\ F^{(l)}(\underline{\mathbf{x}}) = t_l}} W(\underline{\mathbf{x}}) \mathrm{d}\underline{\mathbf{x}},$$

if $\underline{\mathbf{x}} = (\mathbf{x}_1, \ldots, \mathbf{x}_d)$. According to Equation (4.17), we have $f(0) = D_K^{-n/2}\sigma_\infty(t)$, where

$$\sigma_\infty(t) = \int_{\substack{\underline{\mathbf{u}} \in \mathbb{R}^{dn} \\ Q_l(\underline{\mathbf{u}}) = \tau_l}} w(\delta^{-1}|\underline{\mathbf{u}} - \underline{\boldsymbol{\xi}}|) \mathrm{d}\underline{\mathbf{u}} \tag{4.18}$$

is the usual singular integral for the descended system. In particular, arguing as in Davenport and Lewis [3, §6], a standard argument ensures that $\sigma_\infty(t) > 0$ since $\underline{\boldsymbol{\xi}}$ is a nonsingular real point on the descended system.

We summarise our preliminary treatment of the main term in the following result.

Lemma 4.12. *Let $\varepsilon > 0$. Then, for any $A \geqslant 1$, we have*

$$M(P) = \frac{P^{(n-2)d}}{D_K^{n-1/2}} \sum_{\substack{0 \neq \mathfrak{b} \subset \mathfrak{o} \\ \mathrm{N}\,\mathfrak{b} \ll P^d}} (\mathrm{N}^G \mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}) \left(\sigma_\infty(N/P^2) + O_A\left(\left(\frac{\mathrm{N}\,\mathfrak{b}}{P^d}\right)^A\right)\right) + O_A(P^{-A}),$$

where $\sigma_\infty(N/P^2) > 0$ is given by Equation (4.18).

In order to proceed further, it is clear that one requires a good enough upper bound for $S_{\mathfrak{b}}(N;\mathbf{0})$ in order to show that the error term is satisfactory and the sum over $\mathfrak{b}$ can be extended to infinity. Such a bound is available for admissible F, thanks to Corollary 4.3. Although we omit details, one can use it to prove that

$$M(P) = \frac{\sigma_\infty(N/P^2)}{D_K^{n-1/2}} P^{(n-2)d} \sum_{0 \neq \mathfrak{b} \subset \mathfrak{o}} (\mathrm{N}^G \mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}) + O(P^{dn/2+\varepsilon}),$$

for any admissible F such that $n \geqslant 5$. In the setting of Theorems 1.4 and 1.5, we shall produce better bounds for $S_{\mathfrak{b}}(N;\mathbf{0})$ which allow such a deduction under milder hypotheses.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We close this section with a formal analysis of the singular series

$$\mathfrak{S}(N) = \sum_{(0)\neq\mathfrak{b}\subset\mathfrak{o}} (\mathrm{N}^G\mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}),$$

ignoring issues of convergence. This is summarised in the following result.

Lemma 4.13. *Assume that $\mathfrak{S}(N)$ is absolutely convergent. Then*

$$\mathfrak{S}(N) = \prod_p \lim_{\ell\to\infty} p^{-d\ell(n-1)} \#\left\{\mathbf{x}\in(\mathfrak{o}/p^\ell\mathfrak{o})^n : F(\mathbf{x})\equiv N \,(\mathrm{mod}\, p^\ell)\right\}.$$

We have $\mathfrak{S}(N)>0$ if the shifted descended system has a nonsingular p-adic solution for every prime p.

Proof. We may write

$$\mathfrak{S}(N) = \sum_{k=1}^{\infty} \sum_{\substack{\mathfrak{b}\subset\mathfrak{o}\\ \mathrm{N}\,\mathfrak{b}=k}} (\mathrm{N}^G\mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}) = \sum_{k=1}^{\infty} S(k),$$

say. It follows from Corollary 4.6 that $S(k_1k_2)=S(k_1)S(k_2)$ if k_1,k_2 are coprime integers. Hence,

$$\mathfrak{S}(N) = \prod_p \sum_{j\geqslant 0} S(p^j).$$

Since K is Galois, we may assume that p admits a factorisation $(p)=(\mathfrak{p}_1\cdots\mathfrak{p}_r)^e$, with $\mathrm{N}\mathfrak{p}_1=\cdots=\mathrm{N}\mathfrak{p}_r=p^f$. Let $\ell\geqslant 0$, and let I_ℓ denote the set of integral ideals $\mathfrak{b}=\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r}$, with $0\leqslant k_i\leqslant \ell e$ for $1\leqslant i\leqslant r$. Then the union of I_ℓ over $\ell\geqslant 0$ exactly matches the set of integral ideals whose norm is a power of p. Hence,

$$\mathfrak{S}(N) = \prod_p \lim_{\ell\to\infty} \sum_{\mathfrak{b}\in I_\ell} (\mathrm{N}^G\mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}).$$

It follows from Equation (4.7) that

$$\begin{aligned} S_{\mathfrak{b}}(N;\mathbf{0}) &= \sum_{a\in(\mathfrak{o}/\mathfrak{b})^*} \psi(-\gamma aN) \sum_{\mathbf{x}\,(\mathrm{mod}^G\,\mathfrak{b})} \psi(\gamma aF(\mathbf{x}))\\ &= \frac{(\mathrm{N}^G\mathfrak{b})^n}{p^{\ell dn}} \sum_{a\in(\mathfrak{o}/\mathfrak{b})^*} \psi(-\gamma aN) \sum_{\mathbf{x}\,(\mathrm{mod}\,p^\ell\mathfrak{o})} \psi(\gamma aF(\mathbf{x})), \end{aligned}$$

on extending the inner sum to a sum over elements of $(\mathfrak{o}/p^\ell\mathfrak{o})^n$. Hence, on rearranging, we obtain

$$\sum_{\mathfrak{b}\in I_\ell} (\mathrm{N}^G\mathfrak{b})^{-n} S_{\mathfrak{b}}(N;\mathbf{0}) = \frac{1}{p^{\ell dn}} \sum_{\mathbf{x}\,(\mathrm{mod}\,p^\ell\mathfrak{o})} E(p),$$

where

$$E(p) = \sum_{\mathfrak{b}\in I_\ell} \sum_{a\in(\mathfrak{o}/\mathfrak{b})^*} \psi(\gamma a(F(\mathbf{x})-N)).$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We claim that $\psi(\gamma a\cdot)$ runs over all characters modulo p^ℓ, as a runs over $(\mathfrak{o}/\mathfrak{b})^*$ and $\mathfrak{b}$ runs over I_ℓ. On one hand, since $a \in (\mathfrak{o}/\mathfrak{b})^*$, each character $\psi(\gamma a\cdot)$ is a primitive character modulo $\mathfrak{b}$. Since $\mathfrak{b} = \mathfrak{p}^{k_1}\cdots\mathfrak{p}_r^{k_r}$, for $k_1,\dots,k_r \leqslant \ell e$ and $p^\ell = (\mathfrak{p}_1\cdots\mathfrak{p}_r)^{\ell e}$, we conclude that each such character induces a character modulo p^ℓ. In order to complete the proof of the claim, it remains to show that we get all $p^{\ell d}$ characters modulo p^ℓ this way. But the number of characters is precisely

$$\begin{aligned}\sum_{\mathfrak{b}\in I_\ell} \mathrm{N}\mathfrak{b}\prod_{\mathfrak{p}\mid\mathfrak{b}}\left(1-\frac{1}{\mathrm{N}\mathfrak{p}}\right) &= \sum_{\mathfrak{b}\in I_\ell} p^{f(k_1+\cdots+k_r)}\prod_{\mathfrak{p}\mid\mathfrak{b}}\left(1-\frac{1}{p^f}\right)\\ &= \prod_{1\leqslant i\leqslant r}\left(1+\sum_{1\leqslant k\leqslant \ell e} p^{fk}\left(1-\frac{1}{p^f}\right)\right)\\ &= p^{\ell d},\end{aligned}$$

as required.

We may now conclude from orthogonality of characters that

$$E(p) = \begin{cases} p^{\ell d} & \text{if } F(\mathbf{x}) \equiv N \,(\mathrm{mod}\, p^\ell),\\ 0 & \text{otherwise,}\end{cases}$$

from which the first part of the lemma follows. The second part is standard. Using Equation (1.2), the solubility of $F(\mathbf{x}) - N$ in $\mathfrak{o}/p^\ell\mathfrak{o}$ can be reduced to the solubility of a shifted descended system $Q_i(\mathbf{u}_1,\dots,\mathbf{u}_d) - N_i$ modulo primes powers, for $1 \leqslant i \leqslant d$, where we have written $N = \omega_1 N_1 + \cdots + \omega_d N_d$. Arguing as in work of Birch [1, Lemma 7.1], for example, the existence of nonsingular p-adic zeros of this system is enough to deduce that $\mathfrak{S}(N) > 0$. The details of this will not be repeated here. □

4.7. Contribution from the nontrivial characters

In this section, we make some initial steps in the treatment of the contribution from the nonzero vectors $\mathbf{m}$ in the asymptotic formula for $N_W(F,N;P)$ in Lemma 4.1. This contribution is

$$\ll P^{(n-2)d}E(N;P),$$

where

$$E(N;P) = \sum_{\substack{0\neq\mathfrak{b}\subset\mathfrak{o}\\ \mathrm{N}\mathfrak{b}\ll P^d}}\sum_{\mathbf{0}\neq\mathbf{m}\in\widehat{G_\mathfrak{b}}^n} (\mathrm{N}^G\mathfrak{b})^{-n}|S_\mathfrak{b}(N;\mathbf{m})||I_\mathfrak{b}(N/P^2;P\mathbf{m})|. \tag{4.19}$$

The primary task is to establish conditions under which there is an absolute constant $\Delta > 0$ such that $E(N;P) = O(P^{-\Delta})$.

We now place ourselves in the context of the generalised quadratic forms (1.3) and make some initial steps that will be common to Theorems 1.3–1.5. It will be convenient to consider the overall contribution from $\mathfrak{b}$ such that $\mathrm{N}\mathfrak{b}$ and $\mathrm{N}^G\mathfrak{b}$ are constrained to lie in dyadic intervals. Note that $\mathrm{N}\mathfrak{b} \ll P^d$ and $\mathrm{N}^G\mathfrak{b} \leqslant (\mathrm{N}\mathfrak{b})^2$ since $\#G = 2$. Accordingly, we

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

let X,Y be parameters such that

$$1 \leqslant X \leqslant Y \leqslant X^2, \quad X \ll P^d. \tag{4.20}$$

We then write $E(N;P;X,Y)$ for the overall contribution to $E(N;P)$ from nonzero ideals $\mathfrak{b} \subset \mathfrak{o}$ for which

$$X \leqslant \mathrm{N}\mathfrak{b} < 2X \quad \text{and} \quad Y \leqslant \mathrm{N}^G\mathfrak{b} < 2Y.$$

We denote by $\mathscr{B}(X,Y)$ the set of all such ideals. On summing over dyadic intervals for X,Y satisfying Equation (4.20), it will suffice to establish the existence of $\Delta > 0$ such that

$$E(N;P;X,Y) = O(P^{-\Delta}), \tag{4.21}$$

for any X,Y satisfying Equation (4.20).

It follows from Corollary 4.8 that

$$I_{\mathfrak{b}}(N/P^2;P\mathbf{m}) \ll_A P^{\varepsilon} \int_{\mathscr{U}} |K(u,P\mathbf{m})|\mathrm{d}u + P^{-A},$$

for any $A \geqslant 1$, where $K(u,P\mathbf{m})$ is given by Equation (4.10) and

$$\mathscr{U} = \left\{ u \in V : \mathfrak{H}(u) \leqslant \frac{P^{d+\varepsilon}}{\mathrm{N}\mathfrak{b}} \right\}. \tag{4.22}$$

Hence, Equation (4.19) yields

$$E(N;P;X,Y) \ll_A P^{-A} + P^{\varepsilon} Y^{-n} \sum_{\mathfrak{b} \in \mathscr{B}(X,Y)} \sum_{0 \neq \mathbf{m} \in \widetilde{G}\mathfrak{b}^n} |S_{\mathfrak{b}}(N;\mathbf{m})| \int_{\mathscr{U}} |K(u,P\mathbf{m})|\mathrm{d}u, \tag{4.23}$$

for any $A \geqslant 1$, where $\mathscr{B}(X,Y)$ is the set of nonzero ideals $\mathfrak{b} \subset \mathfrak{o}$ for which $X \leqslant \mathrm{N}\mathfrak{b} < 2X$ and $Y \leqslant \mathrm{N}^G\mathfrak{b} < 2Y$.

5. Homogeneous case: proof of Theorems 1.3 and 1.4

We begin by proving a general result about rank drop in pencils of quadratic forms in situations where one of the matrices has much smaller rank. It parallels the basic fact in Reid's thesis [10, Prop. 2.1] about rank drop in pencils $\nu_1 A + \nu_2 B$, for suitable $n \times n$ matrices A,B, and shows how Assumption 2 can be deduced from an appropriate hypothesis about the shape of the associated singular locus.

Lemma 5.1. *Let L be an algebraically closed field of characteristic not equal to 2, and let $m < n$. Consider two matrices $A,B \in M_{n\times n}(L)$ such that B has only nonzero entries in the upper left $m \times m$ submatrix, which we also assume to be nonsingular. Let $\det(A) \neq 0$. Assume that all singular points of the intersection of the two quadratic forms associated to A and B have the shape $(0,\mathbf{x}'')$ with $\mathbf{x}'' = (x_{m+1},\dots,x_n)$, and that the intersection has codimension 2. Then we have*

$$\mathrm{rank}(A + \lambda B) \geqslant n-1, \quad \forall \lambda \in L.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Proof. Assume that there is some $\lambda \in L$ with

$$\operatorname{rank}(A+\lambda B) \leqslant n-2.$$

Let $V_0 \subset \mathbb{A}^n$ be the affine subspace given by the kernel of $A+\lambda B$. Then $\dim V_0 \geqslant 2$. Let $\mathbb{P}(V_0) = V \subset \mathbb{P}^{n-1}$, and let $Q_B \subset \mathbb{P}^{n-1}$ be the quadric given by the matrix B. Then $\dim V \geqslant 1$ and $\dim Q_B = n-2$ as projective varieties. We deduce that the intersection $V \cap Q_B$ is nonempty. Consider a point $\mathbf{x} = (\mathbf{x}', \mathbf{x}'') \in L^n \setminus \{0\}$ in the affine cone of $V \cap Q_B$, where $\mathbf{x}' \in L^m$ and $\mathbf{x}'' \in L^{n-m}$. Then we deduce that

$$0 = \mathbf{x}^t(A+\lambda B)\mathbf{x} = \mathbf{x}^t A\mathbf{x} + \lambda \mathbf{x}^t B\mathbf{x} = \mathbf{x}^t A\mathbf{x}.$$

We deduce that $\mathbf{x}$ lies on the quadric given by A and as it is in the kernel of $A+\lambda B$, it is a singular point of the intersection $Q_A \cap Q_B$. We claim that $\mathbf{x}' \neq 0$, that is, $\mathbf{x}$ is not of the shape $(0, \mathbf{x}'')$. Assume for a moment that $\mathbf{x} = (0, \mathbf{x}'')$. Note that

$$0 = (A+\lambda B)(0, \mathbf{x}'') = A(0, \mathbf{x}'').$$

This is a contradiction to A being nonsingular. Hence, we found a singular point of the intersection $Q_A \cap Q_B$ which is not of the form $(0, \mathbf{x}'')$. □

The main aim of this section is to carry out the proof of Theorems 1.3 and 1.4, which corresponds to taking $N = 0$ and

$$F(X_1, \dots, X_n) = Q(X_1, \dots, X_n) + R(X_1^\tau, \dots, X_m^\tau),$$

as in Equation (1.3). Suppose that $\mathbf{A}$ is the $n \times n$ symmetric matrix defining Q and that $\mathbf{B}$ is the $n \times n$ symmetric matrix given by the condition that its upper left $m \times m$ submatrix defines R, with all other entries are equal to 0. We may proceed under the assumption that Assumptions 1–3 hold.

We have two tasks remaining. The first is to show that the sum over $\mathfrak{b}$ in Lemma 4.12 can be extended to infinity, with acceptable error, and the second is to prove that Equation (4.21) holds. We'll need some more preparations for estimating the relevant exponential sum in Lemma 4.12 and Equation (4.23). Recalling the definition (3.3) of $\mathscr{H}_{\mathfrak{b}}$, we lower bound its index in $\mathfrak{o}^n$.

Lemma 5.2. *There exist nonzero constants $\kappa_1, \dots, \kappa_n, \tilde{\kappa}_1, \dots, \tilde{\kappa}_m \in K$, depending only on F and K such that*

$$\mathscr{H}_{\mathfrak{b}} \subseteq (\kappa_1 \mathfrak{b} \cap \tilde{\kappa}_1 \mathfrak{b}^{\tau^{-1}}) \times \cdots \times (\kappa_m \mathfrak{b} \cap \tilde{\kappa}_m \mathfrak{b}^{\tau^{-1}}) \times \kappa_{m+1}\mathfrak{b} \times \cdots \times \kappa_n \mathfrak{b}.$$

Moreover, we have $\kappa_1^{-1}, \dots, \kappa_n^{-1}, \tilde{\kappa}_1^{-1}, \dots, \tilde{\kappa}_m^{-1} \in \mathfrak{o}$.

Proof. Assume that $\mathbf{A}$ has symmetric entries $a_{i,j} \in \mathfrak{o}$, for $1 \leqslant i,j \leqslant n$, and that $\mathbf{B}$ has symmetric entries $b_{i,j} \in \mathfrak{o}$ for $1 \leqslant i,j \leqslant m$. Then the associated bilinear form takes the shape

$$B(X_1, \dots, X_n; Y_1, \dots, Y_n) = \sum_{i,j \leqslant n} a_{i,j} X_i Y_j + \sum_{i,j \leqslant m} b_{i,j} X_i^\tau Y_j^\tau.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Now, $\mathbf{h} \in \mathscr{H}_{\mathfrak{b}}$ if and only if $2B(\mathbf{h},\mathbf{k}) \in \mathfrak{b}$ for all $\mathbf{k} \in \mathfrak{o}^n$. Let $\omega_1,\dots,\omega_d$ be an integral basis of $\mathfrak{o}$ with $\omega_1 = 1$. Let $l \in \{1,\dots,d\}$ and $j \in \{1,\dots,n\}$ and consider a vector $\mathbf{k}$ such that the j-th entry is equal to ω_l and all other entries are equal to zero. Then the condition $B(\mathbf{h},\mathbf{k}) \in \mathfrak{b}$ implies that

$$2\omega_l \sum_{i=1}^{n} a_{i,j} h_i + 2\omega_l^{\tau} \sum_{i=1}^{m} b_{i,j} h_i^{\tau} \in \mathfrak{b}, \quad 1 \leqslant l \leqslant d,\ 1 \leqslant j \leqslant n.$$

As the matrix $(\omega_l^{\tau})_{1 \leqslant l \leqslant d, \tau \in \mathrm{Gal}(K/\mathbb{Q})}$ is invertible, this implies that there exists $\beta \in K$ with $\beta^{-1} \in \mathfrak{o}$ such that

$$\sum_{i=1}^{n} a_{i,j} h_i \in \beta\mathfrak{b}, \quad \sum_{i=1}^{m} b_{i,j} h_i^{\tau} \in \beta\mathfrak{b}, \quad 1 \leqslant j \leqslant n.$$

Thus, we find that $\mathbf{A}\mathbf{h} \in (\beta\mathfrak{b})^n$ and $\mathbf{B}(\mathbf{h}')^{\tau} \in (\beta\mathfrak{b})^m$, where $\mathbf{h}' = (h_1,\dots,h_m)$. As both matrices $\mathbf{A}$ and $\mathbf{B}$ are nonsingular, this implies that

$$\mathbf{h} \in \frac{1}{(\det \mathbf{A})}(\beta\mathfrak{b})^n, \quad \mathbf{h}' \in \frac{1}{(\det \mathbf{B})^{\tau^{-1}}}(\beta^{\tau^{-1}}\mathfrak{b}^{\tau^{-1}})^m.$$

Putting these together, the statement of the lemma easily follows. □

Corollary 5.3. *Let $N \in \mathfrak{o}$ and let F be given by Equation (1.3). Suppose that Assumption 1 holds. Then*

$$S_{\mathfrak{b}}(N;\mathbf{m}) \ll (\mathrm{N}\,\mathfrak{b})^{1-(n-m)/2}(\mathrm{N}^G\mathfrak{b})^{n-m/2}.$$

Moreover, $S_{\mathfrak{b}}(N;\mathbf{m}) = 0$ unless $m_i \in \mathfrak{d}^{-1}\mathfrak{b}^{-1}$ for $m < i \leqslant n$.

Proof. It follows from Lemma 5.2 that $|\mathfrak{o}^n/\mathscr{H}_{\mathfrak{b}}| \gg (\mathrm{N}^G\mathfrak{b})^m(\mathrm{N}\,\mathfrak{b})^{n-m}$. Thus, Equation (3.4) implies that

$$|\mathscr{H}_{\mathfrak{b}}/{}^G\mathfrak{b}^n| = \frac{|\mathfrak{o}^n/{}^G\mathfrak{b}^n|}{|\mathfrak{o}^n/\mathscr{H}_{\mathfrak{b}}|} \ll \frac{(\mathrm{N}^G\mathfrak{b})^n}{(\mathrm{N}^G\mathfrak{b})^m(\mathrm{N}\,\mathfrak{b})^{n-m}} = \left(\frac{\mathrm{N}^G\mathfrak{b}}{\mathrm{N}\,\mathfrak{b}}\right)^{n-m}.$$

Inserting this into Lemma 4.2 yields the desired upper bound. We have already observed in Lemma 4.4 that $S_{\mathfrak{b}}(N;\mathbf{m}) = 0$ unless $\mathbf{m}.\mathbf{h} \in \mathfrak{d}^{-1}$ for all $\mathbf{h} \in \mathscr{H}_{\mathfrak{b}}$. Noting that ${}^G\mathfrak{b}^m \times \mathfrak{b}^{n-m} \subset \mathscr{H}_{\mathfrak{b}}$, the second part easily follows. □

Returning to Lemma 4.12, it immediately follows from this that the overall contribution from the tail $\mathrm{N}\,\mathfrak{b} \gg P^d$ is

$$\begin{aligned} &\ll P^{(n-2)d} \sum_{\substack{\mathfrak{b} \subset \mathfrak{o} \\ \mathrm{N}\,\mathfrak{b} \gg P^d}} (\mathrm{N}^G\mathfrak{b})^{-n} |S_{\mathfrak{b}}(N;\mathbf{0})| \\ &\ll P^{(n-2)d} \sum_{\substack{\mathfrak{b} \subset \mathfrak{o} \\ \mathrm{N}\,\mathfrak{b} \gg P^d}} (\mathrm{N}\,\mathfrak{b})^{1-n/2+m/2} (\mathrm{N}^G\mathfrak{b})^{-m/2}. \end{aligned}$$

Since $\mathrm{N}^G\mathfrak{b} \geqslant \mathrm{N}\,\mathfrak{b}$, this is acceptable provided that $n > 4$, which is certainly implied by the hypotheses in Theorems 1.3 and 1.4. Thus, we can focus our remaining efforts on establishing Equation (4.21).

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Our next goal is to analyse the integrals $K(u,P\mathbf{m})$ in Equation (4.23) for the case that F has the shape $F(\mathbf{x}) = Q(\mathbf{x}) + R(x_1^\tau, x_2^\tau, \dots, x_m^\tau)$, for $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ some fixed automorphism. Taking the lth embedding into the real numbers gives

$$F^{(l)}(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d)}) = Q^{(l)}(\mathbf{x}^{(l)}) + R^{(l)}(\rho_l(\mathbf{x}^{(\tau)})), \quad 1 \leqslant l \leqslant d,$$

where we write $\mathbf{x}^{(l)} = \rho_l(\mathbf{x})$. For each $1 \leqslant l \leqslant d$, we define l_τ through the relation (1.4). With this notation, we obtain

$$\begin{aligned}\mathscr{Q}(\underline{\mathbf{x}}) &= \sum_{1 \leqslant l \leqslant d} u_l F^{(l)}(\underline{\mathbf{x}}) \\ &= \sum_{1 \leqslant l \leqslant d} u_l Q^{(l)}(\mathbf{x}^{(l)}) + \sum_{1 \leqslant l \leqslant d} u_l R^{(l)}(\rho_l(\mathbf{x}^{\tau})) \\ &= \sum_{1 \leqslant l \leqslant d} u_l Q^{(l)}(\mathbf{x}^{(l)}) + \sum_{1 \leqslant l \leqslant d} u_{l_\tau} R^{(l_\tau)}(\mathbf{x}^{(l)}).\end{aligned}$$

Hence,

$$K(u,P\mathbf{m}) = \prod_{l=1}^{d} \int_{\mathbb{R}^n} W(\mathbf{x}^{(l)}) e(G^{(l)}(\mathbf{x}^{(l)}) - P\mathbf{m}^{(l)}.\mathbf{x}^{(l)}) \mathrm{d}\mathbf{x}^{(l)},$$

with

$$G^{(l)}(\mathbf{x}^{(l)}) = u_l Q^{(l)}(\mathbf{x}^{(l)}) + u_{l_\tau} R^{(l_\tau)}(\mathbf{x}^{(l)}).$$

Note that $G^{(l)}(\mathbf{x}^{(l)})$ is a quadratic form in $\mathbf{x}^{(l)}$ and hence can be represented by a symmetric matrix, which can be diagonalised using an orthogonal base change. Thus, for every tuple $u = (u_1, \dots, u_d)$, there exists a diagonal matrix $\mathrm{Diag}(\eth_{l,i}(u))_{1 \leqslant i \leqslant n}$ and an orthogonal matrix $M_l(u) \in O(n)$ such that

$$G^{(l)}(\mathbf{x}^{(l)}) = (\mathbf{x}^{(l)})^t M_l(u)^t \,\mathrm{Diag}(\eth_{l,i}(u)) M_l(u) \mathbf{x}^{(l)}.$$

Set

$$K^{(l)}(u,P\mathbf{m}) = \int_{\mathbb{R}^n} W(\mathbf{x}^{(l)}) e(G^{(l)}(\mathbf{x}^{(l)}) - P\mathbf{m}^{(l)}.\mathbf{x}^{(l)}) \mathrm{d}\mathbf{x}^{(l)}, \quad \text{for } 1 \leqslant l \leqslant d.$$

With the change of coordinates $M_l(u)\mathbf{x}^{(l)} = \mathbf{y}^{(l)}$, we get

$$\begin{aligned}&K^{(l)}(u,P\mathbf{m}) \\ &\quad = \pm \int_{\mathbb{R}^n} W(M_l(u)^t \mathbf{y}^{(l)}) e((\mathbf{y}^{(l)})^t \,\mathrm{Diag}(\eth_{l,i}(u)) \mathbf{y}^{(l)} - P\mathbf{m}^{(l)}.(M_l(u))^t \mathbf{y}^{(l)}) \mathrm{d}\mathbf{y}^{(l)} \\ &\quad = \pm \int_{\mathbb{R}^n} W(M_l(u)^t \mathbf{y}^{(l)}) e((\mathbf{y}^{(l)})^t \,\mathrm{Diag}(\eth_{l,i}(u)) \mathbf{y}^{(l)} - PM_l(u)\mathbf{m}^{(l)}.\mathbf{y}^{(l)}) \mathrm{d}\mathbf{y}^{(l)}.\end{aligned}$$

We are now ready to prove the following result.

Lemma 5.4. *For any $\varepsilon > 0$, the integral $K^{(l)}(u,P\mathbf{m})$ is essentially supported on the set of u and $\mathbf{m}$ for which*

$$|(M_l(u)\mathbf{m}^{(l)})_i| \ll P^{-1+\varepsilon} |\eth_{l,i}(u)|, \quad 1 \leqslant i \leqslant n,$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

and

$$|m_i^{(l)}| \ll P^{-1+\varepsilon}|u_l|, \quad m < i \leqslant n.$$

Moreover, we have

$$K^{(l)}(u, P\mathbf{m}) \ll \prod_{i=1}^{n} \min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right).$$

Proof. Recall that $M_l(u) \in O(n)$. In particular, all entries of $M_l(u)$ are bounded independently of u and we obtain

$$\frac{\partial^k}{\partial (y_i^{(l)})^k} W(M_l(u)^t \mathbf{y}^{(l)}) \ll_k 1,$$

uniformly in u for all $k \in \mathbb{N}$. The result now follows from Lemma 4.9. □

Henceforth, we take $N = 0$ and write $E(P; X, Y) = E(0; P; X, Y)$ in Equation (4.23). We shall adhere to common convention and allow the value of $\varepsilon > 0$ to change at each appearance so that $P^{\varepsilon} \log P \ll P^{\varepsilon}$, for example. Moreover, all implied constants are allowed to depend on ε.

Applying Corollary 5.3, we deduce that

$$E(P; X, Y) \ll P^{\varepsilon} X^{1-(n-m)/2} Y^{-m/2} \sum_{\mathfrak{b} \in \mathscr{B}(X,Y)} \sum_{\substack{\mathbf{0} \neq \mathbf{m} \in \widehat{{}^G\mathfrak{b}}^n \\ i > m \Rightarrow m_i \in \mathfrak{d}^{-1}\mathfrak{b}^{-1}}} \int_{\mathscr{U}} |K(u, P\mathbf{m})| \mathrm{d}u.$$

Let $\delta \in {}^G\mathfrak{b}\mathfrak{d}$, and let $\mathfrak{p}_1$ be a prime ideal coprime to ${}^G\mathfrak{b}\mathfrak{d}$, with $\mathrm{N}\mathfrak{p}_1 \ll (\mathrm{N}\mathfrak{b})^{\varepsilon/d}$, such that $(\delta) = {}^G\mathfrak{b}\mathfrak{d}\mathfrak{p}_1$. On multiplying δ by an appropriate unit, there is no loss of generality in assuming that

$$Y^{1/d} \ll |\delta^{(l)}| \ll Y^{1/d+\varepsilon}, \tag{5.1}$$

for $1 \leqslant l \leqslant d$, since $Y \leqslant \mathrm{N}\,{}^G\mathfrak{b} < 2Y$. We are led to make the change of variables

$$c_i = \delta m_i, \tag{5.2}$$

for $1 \leqslant i \leqslant n$, so that $\mathbf{c} = (c_1, \ldots, c_n) \in \mathfrak{o}^n$. Then

$$c_i \in \delta\mathfrak{d}^{-1}\mathfrak{b}^{-1} = \mathfrak{p}_1\mathfrak{b}^{-1\,G}\mathfrak{b} \subset \mathfrak{b}^{-1\,G}\mathfrak{b}, \quad \text{for } m < i \leqslant n. \tag{5.3}$$

We may now write

$$E(P; X, Y) \ll P^{\varepsilon} X^{1-(n-m)/2} Y^{-m/2} \sum_{\mathfrak{b} \in \mathscr{B}(X,Y)} \sum_{\substack{\mathbf{0} \neq \mathbf{c} \in \mathfrak{o}^n \\ (5.3) \text{ holds}}} \int_{\mathscr{U}} |K(u, P\delta^{-1}\mathbf{c})| \mathrm{d}u.$$

Define the function

$$f(u) = \prod_{1 \leqslant l \leqslant d} \prod_{1 \leqslant i \leqslant n} \min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right). \tag{5.4}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Let $\mathscr{R}(\mathbf{m})$ be the set of $u \in \mathscr{U}$ such that

$$|(M_l(u)\mathbf{m}^{(l)})_i| \ll P^{-1+\varepsilon}|\eth_{l,i}(u)|, \quad 1 \leqslant i \leqslant n, 1 \leqslant l \leqslant d,$$

and

$$|m_i^{(l)}| \ll P^{-1+\varepsilon}|u_l|, \quad m < i \leqslant n, 1 \leqslant l \leqslant d.$$

We now have

$$E(P;X,Y) \ll P^{\varepsilon}X^{1-(n-m)/2}Y^{-m/2} \sum_{\mathfrak{b} \in \mathscr{B}(X,Y)} \sum_{\substack{\mathbf{0} \neq \mathbf{c} \in \mathfrak{o}^n \\ (5.3) \text{ holds}}} \int_{\mathscr{R}(\delta^{-1}\mathbf{c})} f(u)\mathrm{d}u.$$

Let

$$L(u) = \sum_{\mathfrak{b} \in \mathscr{B}(X,Y)} \sum_{\mathbf{c} \in \mathscr{C}(u,\mathfrak{b})} 1,$$

where $\mathscr{C}(u,\mathfrak{b})$ is the set of nonzero vectors $\mathbf{c} \in \mathfrak{o}^n$ for which Equation (5.3) holds,

$$|(M_l(u)\mathbf{c}^{(l)})_i| \ll P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|, \quad 1 \leqslant i \leqslant n, 1 \leqslant l \leqslant d,$$

and

$$|c_i^{(l)}| \ll P^{-1+\varepsilon}Y^{1/d}|u_l|, \quad m < i \leqslant n, 1 \leqslant l \leqslant d.$$

Then we have

$$E(P;X,Y) \ll P^{\varepsilon}X^{1-(n-m)/2}Y^{-m/2} \int_{\mathscr{U}} f(u)L(u)\mathrm{d}u.$$

Our next goal is to estimate $L(u)$. For each $1 \leqslant l \leqslant d$, we sort the eigenvalues $\eth_{l,i}(u)$ in a way such that

$$|\eth_{l,1}(u)| \geqslant |\eth_{l,2}(u)| \geqslant \cdots \geqslant |\eth_{l,n}(u)|.$$

Note that we can always achieve this by adjusting the orthogonal matrix $M_l(u)$ with suitable permutations. Moreover, for all $1 \leqslant i \leqslant n$ and $1 \leqslant l \leqslant d$, we have

$$|\eth_{l,i}(u)| \ll |u_l| + |u_{l_\tau}|. \tag{5.5}$$

It will now be useful to make the observation

$$\prod_{l=1}^{d}(1+|u_l|+|u_{l_\tau}|) \ll \prod_{l=1}^{d}((1+|u_l|)(1+|u_{l_\tau}|)) \ll \mathfrak{H}(u)^2. \tag{5.6}$$

We proceed by proving the following result.

Lemma 5.5. *Let $u \in V$ such that $\mathfrak{H}(u) \leqslant P^{d+\varepsilon}/X$. If $L(u) \neq 0$, then*

$$P^{-d+\varepsilon}Y\mathfrak{H}(u)^2 \gg 1. \tag{5.7}$$

Moreover, we have $L(u) \ll P^{\varepsilon}XJ(u)$, where

$$J(u) = \prod_{1 \leqslant l \leqslant d} \prod_{1 \leqslant i \leqslant m} (1 + P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|).$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Proof. Let us write $\mathbf{c} = (\mathbf{c}', \mathbf{c}'')$, where $\mathbf{c}' = (c_1, \dots, c_m)$ and $\mathbf{c}'' = (c_{m+1}, \dots, c_n)$. Keeping in mind Equation (5.3), we first fix a choice of $\mathbf{c}'' \in \left(\mathfrak{b}^{-1G}\mathfrak{b}\right)^{n-m}$ satisfying

$$|c_i^{(l)}| \ll P^{-1+\varepsilon} Y^{1/d} |u_l|,$$

for $m+1 \leqslant i \leqslant n$ and $1 \leqslant l \leqslant d$. Choose $\lambda \in K$ such that $(\lambda) = \mathfrak{b}^{-1G}\mathfrak{b}\mathfrak{p}_2^{-1}$, for a suitable prime ideal $\mathfrak{p}_2$ of norm $O(P^\varepsilon)$. We may assume that λ is well shaped in the sense of Equation (5.1), on multiplying by a suitable unit. Thus, $X^{1/d}Y^{1/d} \ll |\lambda^{(l)}| \ll X^{1/d}Y^{1/d+\varepsilon}$, for $1 \leqslant l \leqslant d$. Making the change of variables $\mathbf{c}'' = \lambda \mathbf{d}''$ and recalling that $\mathrm{N}\,\mathfrak{b} \asymp X$ and $\mathrm{N}^G\mathfrak{b} \asymp Y$, we must have

$$|d_i^{(l)}| \ll P^{-1+\varepsilon} X^{1/d} |u_l|,$$

for $m+1 \leqslant i \leqslant n$ and $1 \leqslant l \leqslant d$.

We begin by showing that Equation (5.7) holds if $L(u) \neq 0$. Thus, there exists $\mathbf{c} \neq \mathbf{0}$ counted by $L(u)$. Suppose first that $\mathbf{c}'' \neq \mathbf{0}$. Then there exists $i \in \{m+1, \dots, n\}$ such that

$$1 \leqslant |N_{K/\mathbb{Q}}(d_i)| \ll P^{-d+\varepsilon} X |\mathrm{Nm}(u)|,$$

whence $1 \ll P^{-d+\varepsilon} X \mathfrak{H}(u) \ll P^{-d+\varepsilon} Y \mathfrak{H}(u)^2$ since $X \leqslant Y$. This is satisfactory for Equation (5.7). Suppose next that $\mathbf{c}' \neq \mathbf{0}$. In particular, we have

$$|(M_l(u)\mathbf{c}^{(l)})_i| \ll P^{-1+\varepsilon} Y^{1/d} |\eth_{l,i}(u)|, \quad 1 \leqslant i \leqslant n, 1 \leqslant l \leqslant d. \tag{5.8}$$

As $M_l(u)$ is an orthogonal matrix, this implies that

$$|c_j^{(l)}| \ll P^{-1+\varepsilon} Y^{1/d} \max_{1 \leqslant i \leqslant n} |\eth_{l,i}(u)|, \quad 1 \leqslant j \leqslant n, 1 \leqslant l \leqslant d,$$

whence Equation (5.6) yields

$$1 \ll P^{-d+\varepsilon} Y \prod_{l=1}^{d} \max_{1 \leqslant i \leqslant n} |\eth_{l,i}(u)| \ll P^{-d+\varepsilon} Y \prod_{l=1}^{d} (|u_l| + |u_{l_\tau}|) \ll P^{-d+\varepsilon} Y \mathfrak{H}(u)^2.$$

This completes the proof of Equation (5.7) under the assumption that $L(u) \neq 0$.

Turning now to the estimation of $L(u)$, it readily follows from a result in Lang [9, Thm. 0 in §V.1] that the overall number of vectors $\mathbf{d}''$ is

$$\ll \left(1 + \prod_{l=1}^{d} P^{-1+\varepsilon} X^{1/d} |u_l|\right)^{n-m} \ll \left(1 + P^{-d+\varepsilon} X \,\mathrm{Nm}(u)\right)^{n-m} \ll P^{\varepsilon}.$$

It remains to count the number of vectors $\mathbf{c}'$ associated to a particular choice of $\mathbf{c}''$. Let $L(u, \mathfrak{b}, \mathbf{c}'')$ be the number of $\mathbf{c}' \in \mathfrak{o}^m$ such that Equation (5.8) holds. Assume that the matrix $M_l(u)$ is given by $M_l(u) = (m_{l\alpha\beta})_{1 \leqslant \alpha, \beta \leqslant n}$. Write

$$M_l(u) = (M_l'(u) M_l''(u)),$$

with $M_l'(u) = (m_{l\alpha\beta})_{\substack{1 \leqslant \alpha \leqslant n \\ 1 \leqslant \beta \leqslant m}}$ and $M_l''(u) = (m_{l\alpha\beta})_{\substack{1 \leqslant \alpha \leqslant n \\ m < \beta \leqslant n}}$. Then we consider the system of inequalities

$$|M_l'(u)\mathbf{c}'^{(l)} + r_{li}| \ll P^{-1+\varepsilon} Y^{1/d} |\eth_{l,i}(u)|, \quad 1 \leqslant i \leqslant n, 1 \leqslant l \leqslant d,$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

where $\mathbf{r}_l = (r_{li})_{1\leqslant i\leqslant n} = M_l''(u)\mathbf{c}''^{(l)}$.

Write

$$c_i = \sum_{l=1}^{d} c_{il}\omega_l, \quad c_{il} \in \mathbb{Z}, 1 \leqslant i \leqslant m.$$

Then, for $1 \leqslant i \leqslant n$, we can write

$$(M_l'(u)\mathbf{c}'^{(l)})_i = \sum_{\beta=1}^{m} m_{li\beta}c_\beta^{(l)} = \sum_{\beta=1}^{m} m_{li\beta}\sum_{k=1}^{d} c_{\beta k}\omega_k^{(l)} = \sum_{\beta=1}^{m}\sum_{k=1}^{d} m_{li\beta}\omega_k^{(l)}c_{\beta k}.$$

Let H be the $dn\times dm$ matrix given by

$$H = (m_{li\beta}\omega_k^{(l)})_{(l,i)\times(k,\beta)},$$

with $1 \leqslant l \leqslant d$, $1 \leqslant i \leqslant n$, $1 \leqslant k \leqslant d$, $1 \leqslant \beta \leqslant m$, and consider the lattice

$$\Lambda = H\mathbb{Z}^{md} \subset \mathbb{R}^{nd}.$$

Then $L(u,\mathfrak{b},\mathbf{c}'')$ counts lattice points in Λ which lie in a box of side length

$$\ll P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|, \quad 1 \leqslant i \leqslant n, 1 \leqslant l \leqslant d.$$

We claim that the successive minima of the lattice Λ are bounded above and below by constants depending only on K and n. Taking this on faith, it will then follow that

$$L(u,\mathfrak{b},\mathbf{c}'') \ll \prod_{1\leqslant l\leqslant d}\prod_{1\leqslant i\leqslant m}(1+P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|),$$

which will settle the lemma, on summing over $O(X)$ choices for $\mathfrak{b} \in \mathscr{B}(X,Y)$.

To check the claim, we order the index tuples (l,i) and (k,β) in the matrix H lexicographically. Write

$$A_{lk} = (m_{li\beta}\omega_k^{(l)})_{1\leqslant i\leqslant n, 1\leqslant\beta\leqslant m} = \omega_k^{(l)}(m_{li\beta})_{(i,\beta)} = \omega_k^{(l)}B_l,$$

with the $n\times m$ matrix $B_l = (m_{li\beta})_{1\leqslant i\leqslant n, 1\leqslant\beta\leqslant m}$. Note that B_l has orthogonal and norm one columns for $1 \leqslant l \leqslant d$. We can then write H as a block matrix

$$H = (A_{lk})_{1\leqslant l,k\leqslant d}.$$

Let $B = B(u)$ be the $nd\times md$ matrix which is a diagonal block matrix, with the matrices $B_1,\dots,B_d$ on the diagonal. Let W be the $md\times md$ block matrix, with blocks $\omega_k^{(l)}E_m$ at each place $1 \leqslant l,k \leqslant d$, where E_m is the m-dimensional identity matrix. Then

$$H = BW.$$

Consider the lattice $\Gamma = W\mathbb{Z}^{md} \subset \mathbb{R}^{md}$, and note that this only depends on the basis $\omega_1,\dots,\omega_d$. Moreover, if $\mathbf{w} \in \Gamma$, then

$$\langle B\mathbf{w}, B\mathbf{w}\rangle = \mathbf{w}^tB^tB\mathbf{w} = \mathbf{w}^tE_{md}\mathbf{w} = \langle\mathbf{w},\mathbf{w}\rangle.$$

Hence, the successive minima of the lattice Λ coincide with those of Γ, which thereby establishes the claim. □

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

It follows from the previous result that

$$E(P;X,Y) \ll P^{\varepsilon} X^{2-(n-m)/2} Y^{-m/2} \times \int_{\mathscr{U}^*} f(u) \prod_{1 \leqslant i \leqslant m} \prod_{1 \leqslant l \leqslant d} (1 + P^{-1+\varepsilon} Y^{1/d} |\eth_{l,i}(u)|) \mathrm{d}u, \tag{5.9}$$

where $f(u)$ is given by Equation (5.4) and $\mathscr{U}^*$ is the set of $u \in \mathscr{U}$ such that Equation (5.7) holds.

Recall that the $\eth_{l,i}(u)$ are the eigenvalues of the matrix associated to the quadratic form

$$u_l Q^{(l)}(\mathbf{x}^{(l)}) + u_{l_\tau} R^{(l_\tau)}(\mathbf{x}^{(l)}).$$

The next result collects together a number of properties concerning the size of the eigenvalues $\eth_{l,i}(u)$.

Lemma 5.6. *Assume that Assumptions 1–3 hold, and suppose that $\tilde{m} \geqslant m-1$ is the degree of the polynomial appearing in Assumption 3. For each $1 \leqslant l \leqslant d$, we order the eigenvalues $\eth_{l,i}(u)$ such that*

$$|\eth_{l,1}(u)| \geqslant |\eth_{l,2}(u)| \geqslant \cdots \geqslant |\eth_{l,n}(u)|.$$

Then there exist constants $C_1, \ldots, C_d > 0$ such that the following holds:

(1) *If $|u_{l_\tau}| \leqslant C_l |u_l|$, then*

$$|\eth_{l,1}(u)| \ll |u_l| \quad \text{and} \quad |\eth_{l,n-1}(u)| \gg |u_l|.$$

Moreover, if $m = 1$ and $\tilde{m} = 0$, then

$$|\eth_{l,1}(u)| \ll |u_l| \quad \text{and} \quad |\eth_{l,n}(u)| \gg |u_l|.$$

(2) *If $|u_{l_\tau}| > C_l |u_l|$, then*

$$|\eth_{l,m+1}(u) \cdots \eth_{l,n}(u)| \gg \frac{|u_l|^{n-\tilde{m}}}{|u_{l_\tau}|^{m-\tilde{m}}}.$$

Proof. To begin with, according to Assumption 3, for each $1 \leqslant l \leqslant d$ there exists a constant C_l such that

$$|\det(Q^{(l)} + t R^{(l_\tau)})| \gg |t|^{\tilde{m}},$$

for $|t| \geqslant C_l$.

We start by examining the case $|u_{l_\tau}| \leqslant C_l |u_l|$. The first bound $|\eth_{l,1}(u)| \ll |u_l|$ follows directly from Equation (5.5). Assume now that $u_l \neq 0$. Note that each of the eigenvalues $\eth_{l,i}(u)$ arises by multiplication with u_l from the eigenvalues of the matrix corresponding to

$$Q^{(l)} + \frac{u_{l_\tau}}{u_l} R^{(l_\tau)}.$$

Write $\tilde{\eth}_{l,i}(u)$ for those eigenvalues in the same ordering. Assume that the lower bound $|\tilde{\eth}_{l,n-1}(u)| \gg 1$ is not satisfied. Thus, there exists a sequence of t_j in the range $|t_j| \leqslant C_l$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

such that $\tilde{\eth}_{l,n-1}(t_j) \to 0$, for $j \to \infty$, where we write $\tilde{\eth}_{l,n-1}(t)$ for the second smallest eigenvalues of $Q^{(l)} + tR^{(l_\tau)}$. As the set of t is compact there is a convergent subsequence, convergent to t' say, with $\operatorname{rank}(Q^{(l)} + t'R^{(l_\tau)}) < n-1$. This contradicts Assumption 2.

Now, we consider the case $m = 1$ and $\tilde{m} = 0$. By Assumptions 1 and 3, we deduce that $\det(Q^{(l)} + tR^{(l_\tau)})$ is a nonzero constant independent of t. In particular, the rank of this matrix is always n and the argument above shows that $|\eth_{l,n}(u)| \gg |u_l|$.

Next, we consider the case $|u_{l_\tau}| > C_l|u_l|$ and $u_l \neq 0$. Again, we write $\tilde{\eth}_{l,i}(u)$ for the eigenvalues of $Q^{(l)} + \frac{u_{l_\tau}}{u_l} R^{(l_\tau)}$. Note that we have

$$|\tilde{\eth}_{l,i}(u)| \ll |\frac{u_{l_\tau}}{u_l}|, \quad 1 \leqslant i \leqslant n.$$

Moreover, we observe that

$$|\tilde{\eth}_{l,1}(u) \cdots \tilde{\eth}_{l,n}(u)| = |\det(Q^{(l)} + \frac{u_{l_\tau}}{u_l} R^{(l_\tau)})| \gg \left|\frac{u_{l_\tau}}{u_l}\right|^{\tilde{m}}.$$

We therefore find that

$$|\tilde{\eth}_{l,m+1}(u) \cdots \tilde{\eth}_{l,n}(u)| \gg \left|\frac{u_l}{u_{l_\tau}}\right|^m \left|\frac{u_{l_\tau}}{u_l}\right|^{\tilde{m}} = \left|\frac{u_l}{u_{l_\tau}}\right|^{m-\tilde{m}}.$$

From this, we obtain the lower bound

$$|\eth_{l,m+1}(u) \cdots \eth_{l,n}(u)| \gg |u_l|^{n-m} \left|\frac{u_l}{u_{l_\tau}}\right|^{m-\tilde{m}} = \frac{|u_l|^{n-\tilde{m}}}{|u_{l_\tau}|^{m-\tilde{m}}},$$

which completes the proof of the lemma. □

We now continue with our analysis of $E(P;X,Y)$ in Equation (5.9). Recall our assumptions on X,Y in Equation (4.20). Let $E_1(P;X,Y)$ denote the overall contribution from the case $Y \geqslant P^d$, and let $E_2(P;X,Y)$ denote the remaining contribution. The following pair of results treats these two quantities in turn.

Lemma 5.7. *Assume $\tilde{m} \geqslant m-1$. Then $E_1(P;X,Y) \ll P^{d(2-n/2+m/2)+\varepsilon} + P^{-dm+\varepsilon}$.*

Proof. On recalling the definition Equation (5.4) of $f(u)$, we deduce from Equation (5.9) that

$$E_1(P;X,Y) \ll P^\varepsilon X^{2-(n-m)/2} Y^{-m/2} P^{-md} Y^m \times \int_{\mathscr{U}^*} \left(\prod_{1 \leqslant l \leqslant d} (1 + |u_l| + |u_{l_\tau}|)^{m/2} \right) \prod_{1 \leqslant l \leqslant d} \prod_{m < i \leqslant n} \min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) \mathrm{d}u$$

since Equation (5.5) implies that

$$\prod_{1 \leqslant i \leqslant m} (1 + |\eth_{l,i}(u)|)^{1/2} \ll (1 + |u_l| + |u_{l_\tau}|)^{m/2}.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Here, we recall that $\mathscr{U}^*$ is the set of $u \in \mathscr{U}$ such that Equation (5.7) holds. Consider for a moment a fixed value of l. If $C_l|u_l| \geqslant |u_{l_\tau}|$, then Lemma 5.6 yields

$$\prod_{m<i\leqslant n} \min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) \ll \min\left(1, |u_l|^{-(n-m-1)/2}\right).$$

If $C_l|u_l| < |u_{l_\tau}|$ and $\tilde{m} \geqslant m-1$, then Lemma 5.6 yields

$$\begin{aligned}\prod_{m<i\leqslant n} \min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) &\ll \min\left(1, \frac{1}{|\eth_{l,m+1}(u)\cdots\eth_{l,n}(u)|^{1/2}}\right)\\ &\ll \min\left(1, \frac{|u_{l_\tau}|^{1/2}}{|u_l|^{(n-m+1)/2}}\right).\end{aligned}$$

In either of these two cases, we therefore have

$$\prod_{m<i\leqslant n} \min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) \ll (1+|u_l|+|u_{l_\tau}|)^{1/2} \min\left(1, |u_l|^{-(n-m)/2}\right),$$

whence

$$\begin{aligned}E_1(P;X,Y) &\ll P^\varepsilon X^{2-(n-m)/2} Y^{-m/2} P^{-md} Y^m\\ &\quad\times \int_{\mathscr{U}} \left(\prod_{1\leqslant l\leqslant d} (1+|u_l|+|u_{l_\tau}|)^{(m+1)/2}\right) \prod_{1\leqslant l\leqslant d} \min\left(1, \frac{1}{|u_l|^{(n-m)/2}}\right) \mathrm{d}u.\end{aligned}$$

It follows from Equation (5.6) that

$$\begin{aligned}E_1(P;X,Y) &\ll P^\varepsilon X^{2-(n-m)/2} Y^{-m/2} P^{-md} Y^m \int_{\mathfrak{H}(u)\leqslant P^{d+\varepsilon}/X} \mathfrak{H}(u)^{m+1-(n-m)/2} \mathrm{d}u\\ &\ll P^\varepsilon X^{2-(n-m)/2} Y^{-m/2} P^{-dm} Y^m (1+(P^d/X)^{2+m-(n-m)/2})\\ &\ll P^\varepsilon X^{-m} Y^{m/2} P^{d(2-n/2+m/2)} + P^\varepsilon X^{2-(n-m)/2} Y^{m/2} P^{-dm}.\end{aligned}$$

The contribution gets maximal for $Y \asymp X^2$, in which case we get the upper bound

$$\begin{aligned}E_1(P;X,Y) &\ll P^\varepsilon X^{-m} X^m P^{d(2-n/2+m/2)} + P^\varepsilon X^{2-n/2+3m/2} P^{-dm}\\ &\ll P^{d(2-n/2+m/2)+\varepsilon} + X^{2-n/2+3m/2} P^{-dm+\varepsilon}.\end{aligned}$$

The first term is satisfactory for the lemma. If $2-n/2+3m/2 \leqslant 0$, then the second term is $O(P^{-dm+\varepsilon})$, which is satisfactory. If $n \leqslant 3+3m$, on the other hand, then we take $X \ll P^d$ and get the satisfactory upper bound $O(P^{d(2-n/2+m/2)+\varepsilon})$. □

Lemma 5.8. *Assume that $n \geqslant m+4$ and $\tilde{m} \geqslant m-1$. Let*

$$\kappa = \begin{cases} 1 & \text{if } m = 1 \text{ and } \tilde{m} = 0,\\ 0 & \text{otherwise.}\end{cases}$$

Then $E_2(P;X,Y)$ is

$$\ll P^{-d(n-m-4+\kappa)/4+\varepsilon} + P^{-1/2+\varepsilon} + P^{-2m+d(3m+4-\kappa-n)/2+\varepsilon} + P^{-2m+d(3m+4-\kappa-n)/4+\varepsilon}.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Proof. For $1 \leqslant i \leqslant m$, we clearly have

$$\min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right)(1+P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|) \ll 1+P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|^{1/2}.$$

Hence, we find that $E_2(P;X,Y)$ is

$$\ll P^{\varepsilon}X^{2-(n-m)/2}Y^{-m/2}$$
$$\times \int_{\mathscr{U}^*}\left(\prod_{1\leqslant l\leqslant d}\prod_{m<i\leqslant n}\min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right)\right)\prod_{1\leqslant l\leqslant d}\prod_{1\leqslant i\leqslant m}(1+P^{-1+\varepsilon}Y^{1/d}|\eth_{l,i}(u)|^{1/2})\mathrm{d}u.$$

If $C_l|u_l| \geqslant |u_{l_\tau}|$, then Lemma 5.6 leads to the bound

$$\prod_{m<i\leqslant n}\min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) \ll \min\left(1, |u_l|^{-(n-m-1+\kappa)/2}\right).$$

For the case $C_l|u_l| < |u_{l_\tau}|$, we still have

$$\prod_{m<i\leqslant n}\min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) \ll \min\left(1, \frac{|u_{l_\tau}|^{1/2}}{|u_l|^{(n-m+1)/2}}\right)$$

since $\tilde{m} \geqslant m-1$. We now deduce that in either case we have

$$\prod_{m<i\leqslant n}\min\left(1, \frac{1}{|\eth_{l,i}(u)|^{1/2}}\right) \ll (1+|u_l|+|u_{l_\tau}|)^{1/2}\min\left(1, |u_l|^{-(n-m+\kappa)/2}\right).$$

It now follows from Equation (5.6) that $E_2(P;X,Y)$ is

$$\begin{aligned}
&\ll P^{\varepsilon}X^{2-(n-m)/2}Y^{-m/2}\\
&\quad\times\int_{\mathscr{U}^*}\mathfrak{H}(u)^{1-(n-m+\kappa)/2}\prod_{1\leqslant l\leqslant d}\prod_{1\leqslant i\leqslant m}(1+P^{-1+\varepsilon}Y^{1/d}(|u_l|+|u_{l_\tau}|)^{1/2})\mathrm{d}u\\
&\ll P^{\varepsilon}X^{2-(n-m)/2}Y^{-m/2}\\
&\quad\times\int_{\mathscr{U}^*}\mathfrak{H}(u)^{-\frac{n-m-2+\kappa}{2}}\prod_{1\leqslant l\leqslant d}(1+P^{-1+\varepsilon}Y^{1/d}(|u_l|+|u_{l_\tau}|)^{1/2})^m\mathrm{d}u.
\end{aligned}$$

Let I_1 denote the contribution to the integral from those u for which there exists at least one u_l with $|u_l| \gg (P/Y^{1/d})^2$, and let I_2 denote the remaining contribution.

On recalling that $\mathscr{U}^*$ is the set of $u \in \mathscr{U}$ such that Equation (5.7) holds, it is clear that

$$I_2 \ll \int_{\substack{P^{d/2-\varepsilon}/Y^{1/2}\ll\mathfrak{H}(u)\ll P^{d+\varepsilon}/X\\ |u_l|\ll P^2Y^{-2/d},\ 1\leqslant l\leqslant d}}\mathfrak{H}(u)^{-\frac{n-m-2+\kappa}{2}}\mathrm{d}u.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Turning to I_1, we see that

$$\begin{aligned}\prod_{1\leqslant l\leqslant d}(1+P^{-1+\varepsilon}Y^{1/d}(|u_l|+|u_{l_\tau}|)^{1/2})^m&\\ \ll P^{\varepsilon}\prod_{\substack{1\leqslant l\leqslant d\\ |u_l|+|u_{l_\tau}|\geqslant (P/Y^{1/d})^2}}&(P^{-1}Y^{1/d}(|u_l|+|u_{l_\tau}|)^{1/2})^m\\ \ll P^{\varepsilon}\mathfrak{H}(u)^m(P^{-1}Y^{1/d})^{m\sharp\{1\leqslant l\leqslant d:|u_l|+|u_{l_\tau}|\geqslant (P/Y^{1/d})^2\}}&\end{aligned}$$

by Equation (5.6). But if there is one u_l with $|u_l|\gg (P/Y^{1/d})^2$, then clearly

$$\sharp\{1\leqslant l\leqslant d:|u_l|+|u_{l_\tau}|\geqslant (P/Y^{1/d})^2\}\geqslant 2.$$

Hence, since $P^{-1}Y^{1/d}\ll 1$, it now follows that

$$I_1\ll P^{\varepsilon}\int_{P^{d/2-\varepsilon}/Y^{1/2}\ll\mathfrak{H}(u)\ll P^{d+\varepsilon}/X}\mathfrak{H}(u)^{-\frac{n-m-2+\kappa}{2}+m}(P^{-1}Y^{1/d})^{2m}\mathrm{d}u.$$

In summary, we have shown that

$$E_2(P;X,Y)\ll P^{\varepsilon}X^{2-(n-m)/2}Y^{-m/2}(I_1+I_2),$$

with I_1,I_2 as above.

Since $n\geqslant m+4$, the exponent of $\mathfrak{H}(u)$ in I_2 is less than or equal to -1. If $\frac{n-m-2+\kappa}{2}>1$, then it follows from Equation (4.12) that

$$I_2\ll P^{\varepsilon}(P^{d/2}/Y^{1/2})^{-\frac{n-m-2+\kappa}{2}+1}.$$

However, if $\frac{n-m-2+\kappa}{2}=1$, then we apply Equation (4.13) to deduce that the same bound holds.

On the other hand, Equations (4.12) and (4.13) also yield

$$\begin{aligned}I_1&\ll P^{-2m+\varepsilon}Y^{2m/d}\left((P^d/X)^{-\frac{n-m-2+\kappa}{2}+m+1}+(P^{d/2}/Y^{1/2})^{-\frac{n-m-2+\kappa}{2}+m+1}\right)\\ &\ll X^{\frac{n-m-2+\kappa}{2}-m-1}Y^{2m/d}P^{-2m-d(\frac{n-m-2+\kappa}{2})+md+d+\varepsilon}\\ &\quad+Y^{2m/d+n/4-3m/4+\kappa/4-1}P^{-2m+d/2(-\frac{n-m-2+\kappa}{2}+m+1)+\varepsilon}.\end{aligned}$$

We conclude that

$$\begin{aligned}E_2(P;X,Y)&\ll X^{\kappa/2-m}Y^{-m/2+2m/d}P^{-2m+3md/2+(4-\kappa)d/2-dn/2+\varepsilon}\\ &\quad+X^{2-(n-m)/2}Y^{2m/d+n/4-5m/4-(4-\kappa)/4}P^{-2m-dn/4+3md/4+(4-\kappa)d/4+\varepsilon}\\ &\quad+X^{2-(n-m)/2}Y^{-3m/4+n/4-(4-\kappa)/4}P^{d/2(-\frac{n-m-2+\kappa}{2}+1)+\varepsilon}.\end{aligned}$$

We now consider these three terms separately, starting with the third and recalling that $n-m\geqslant 4$. If $-3m/4+n/4-(4-\kappa)/4\leqslant 0$, then we get an upper bound

$$\ll P^{d/2(-\frac{n-m-2+\kappa}{2}+1)+\varepsilon}\ll P^{-d(n-m-4+\kappa)/4+\varepsilon}.$$

In the opposite case, we get the upper bound $\ll P^{-dm/2+\varepsilon}\ll P^{-m+\varepsilon}$, on using $Y\leqslant P^d$ and $d\geqslant 2$.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We now turn to the second term. If $2m/d+n/4-5m/4-(4-\kappa)/4 \leqslant 0$, then we get the upper bound

$$\ll P^{-2m-dn/4+3md/4+(4-\kappa)d/4+\varepsilon}.$$

In the opposite case, on using $X \geqslant Y^{1/2}$, we get the upper bound

$$\begin{aligned}&\ll Y^{1-(n-m)/4} Y^{2m/d+n/4-5m/4-(4-\kappa)/4} P^{-2m-dn/4+3md/4+(4-\kappa)d/4+\varepsilon}\\ &\ll Y^{\kappa/4-m+2m/d} P^{-2m-dn/4+3md/4+(4-\kappa)d/4+\varepsilon}.\end{aligned}$$

If $d \geqslant 3$ or $\kappa = 0$, then we reduce to the case above. If $d = 2$ and $\kappa = 1$, on the other hand, we obtain the upper bound

$$\ll P^{d/4} P^{-2m-dn/4+3md/4+(4-\kappa)d/4} \ll P^{-(n+m-4)/2+\varepsilon}$$

since $Y \leqslant P^d$. Clearly, $(n+m-4)/2 \geqslant m$ if $n \geqslant m+4$, whence this case contributes $O(P^{-m+\varepsilon})$, which is satisfactory.

It remains to deal with the first term. Again, we use the lower bound $X \geqslant Y^{1/2}$, allowing us to bound the first term by

$$\begin{aligned}&\ll Y^{\kappa/4-m/2} Y^{-m/2+2m/d} P^{-2m+3md/2+(4-\kappa)d/2-dn/2+\varepsilon}\\ &\ll Y^{\kappa/4-m+2m/d} P^{-2m+3md/2+(4-\kappa)d/2-dn/2+\varepsilon}.\end{aligned}$$

If $d \geqslant 3$ or $\kappa = 0$, then we get $O(P^{-2m+3md/2+(4-\kappa)d/2-dn/2+\varepsilon})$, which is satisfactory. Alternatively, if $d = 2$ and $\kappa = 1$, then we get

$$\ll P^{1/2} P^{-2m+3md/2+(4-\kappa)d/2-dn/2+\varepsilon} \ll P^{-(n-m-7/2)+\varepsilon}.$$

This is $\ll P^{-1/2+\varepsilon}$ since $n \geqslant m+4$, which thereby completes the proof of the lemma. □

It remains to combine Lemmas 5.7 and 5.8. We make the assumption

$$n \geqslant m+5.$$

Under this assumption, the bound in Lemma 5.7 is $O(P^{-d/2+\varepsilon})$. Moreover, the bound in Lemma 5.8 is

$$\ll P^{-d(1+\kappa)/4+\varepsilon} + P^{-1/2+\varepsilon} + P^{-2m+d(3m+4-\kappa-n)/2+\varepsilon} + P^{-2m+d(3m+4-\kappa-n)/4+\varepsilon}.$$

Hence, since $d \geqslant 2$ and $m \geqslant 1$, it finally follows that Equation (4.21) holds for a suitable $\Delta > 0$, provided that $n \geqslant m+5$ and

$$n > 3m+4-\frac{4m}{d}-\kappa,$$

where κ is defined in the statement of Lemma 5.8.

Suppose first that $m = 1$ and place ourselves under the hypotheses of Theorem 1.3. Then Assumptions 1–3 hold with $\tilde{m} = 0$. Hence, $\kappa = 1$ and the condition on n reduces to $n \geqslant 6$, as required for Theorem 1.3. Assume now that $m \geqslant 1$, but $\kappa = 0$. Since $d \geqslant 2$, we have $3m+4-4m/d \geqslant m+4$, from which the statement of Theorem 1.4 follows.

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

6. Inhomogeneous case: proof of Theorem 1.5

In this section, we complete the proof of Theorem 1.5. We note that the quadratic form in Equation (1.5) is a special case of Equation (1.3), with $\mathbf{A} = \mathrm{Diag}(a_1, \dots, a_n)$ and $\mathbf{B} = \mathrm{Diag}(b_1, \dots, b_m, 0, \dots, 0)$. Hence, Corollary 5.3 applies to the situation considered in Theorem 1.5. In particular, assuming that $n > 4$, the argument in the previous section shows that the sum over $\mathfrak{b}$ in Lemma 4.12 can be extended to infinity with acceptable error. Since the assumption $n > 4$ is implied by the hypotheses in Theorem 1.5, this leaves us free to focus our efforts on proving Equation (4.21).

In the present setting, it will be vital to obtain additional cancellation from the sum over primitive characters in $S_{\mathfrak{b}}(N; \mathbf{m})$. We plan to improve on Corollary 5.3 in generic situations, beginning with an examination of a particular exponential sum modulo degree 1 prime ideals. The saving we shall achieve is linked to the fact that $N \neq 0$ and will also involve the special generalised quadratic form

$$G(\mathbf{x}) = a_1 \cdots a_n b_1 \cdots b_m \left(\frac{x_1^2}{a_1} + \cdots + \frac{x_n^2}{a_n} + \frac{(x_1^\tau)^2}{b_1} + \cdots + \frac{(x_m^\tau)^2}{b_m} \right), \tag{6.1}$$

that is the analogue of the *dual form* in our setting. (Note that it has coefficients in $\mathfrak{o}$.) For any unramified prime ideal $\mathfrak{p}$ and any vector $\mathbf{v} \in \widehat{G_{\mathfrak{p}}}^n$, it will be convenient to observe that $\mathrm{ord}_{\mathfrak{p}}(G(\mathbf{v})) \geqslant -2$, since $\mathrm{ord}_{\mathfrak{p}}(v_i) \geqslant -1$ and $\mathrm{ord}_{\mathfrak{p}}(v_i^\tau) \geqslant -1$ for any $v_i \in \widehat{G_{\mathfrak{p}}}$. With this in mind, we proceed by proving the following bound for $S_{\mathfrak{p}}(N; \mathbf{v})$.

Lemma 6.1. *Let $\mathfrak{p}$ be a prime ideal of residue degree 1, and let $\mathbf{v} \in \widehat{G_{\mathfrak{p}}}^n$. Then*

$$S_{\mathfrak{p}}(N; \mathbf{v}) \ll (\mathrm{N}\mathfrak{p})^{\theta_{\mathfrak{p}}(\mathbf{v}) + (3n-m)/2},$$

where

$$\theta_{\mathfrak{p}}(\mathbf{v}) = \begin{cases} 1 & \text{if } \mathfrak{p} \mid N \text{ and } \mathrm{ord}_{\mathfrak{p}}(G(\mathbf{v})) \geqslant -1, \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Proof. Let $\mathfrak{p}$ be a prime ideal of residue degree 1 so that $\mathrm{N}\mathfrak{p} = p$ for a rational prime p. We may assume that p is unramified in K and that

$$\mathfrak{p} \nmid 2a_1 \cdots a_n b_1 \cdots b_m$$

since the desired estimate is trivial otherwise. Since $K/\mathbb{Q}$ is Galois, this means that there is a factorisation $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_d$ into prime ideals, where $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ are the d conjugates of $\mathfrak{p}$ under $\mathrm{Gal}(K/\mathbb{Q})$, satisfying $\mathrm{N}\mathfrak{p}_i = p$ for $1 \leqslant i \leqslant d$.

It will be convenient to write $S_{\mathfrak{p}} = S_{\mathfrak{p}}(N; \mathbf{v})$ and $\tilde{\mathfrak{p}} = \mathfrak{p}^{\tau^{-1}}$ in the proof. Then $\mathfrak{p}$ and $\tilde{\mathfrak{p}}$ are distinct prime ideals, with ${}^G\mathfrak{p} = \mathfrak{p}\tilde{\mathfrak{p}}$ and $\mathrm{N}\mathfrak{p} = \mathrm{N}\tilde{\mathfrak{p}} = p$. Choose $\gamma = g/\alpha \in \mathfrak{F}(\mathfrak{p})$ as in Lemma 3.4 so that $\psi(\gamma \cdot)$ is a primitive character modulo $\mathfrak{p}$. Then we can write

$$\begin{aligned} S_{\mathfrak{p}} &= \sum_{a \in (\mathfrak{o}/\mathfrak{p})^*} \sum_{\mathbf{x} \,(\mathrm{mod}\, {}^G\mathfrak{p})} \psi\left(\gamma a (F(\mathbf{x}) - N) + \mathbf{v}.\mathbf{x}\right) \\ &= \sum_{a \in (\mathfrak{o}/\mathfrak{p})^*} \psi(-\gamma a N) \sum_{\mathbf{x} \,(\mathrm{mod}\, {}^G\mathfrak{p})} \psi\left(\gamma \{a F(\mathbf{x}) + \alpha \mathbf{v}.\mathbf{x}\}\right), \end{aligned}$$

as in Equation (4.7).

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Lemma 3.2 yields

$$S_{\mathfrak{p}} = \sum_{a \in (\mathfrak{o}/\mathfrak{p})^*} \psi(-\gamma a N) \sum_{\mathbf{u} \in (\mathfrak{o}/\mathfrak{p})^n} \sum_{\mathbf{w} \in (\mathfrak{o}/\tilde{\mathfrak{p}})^n} \psi\left(\gamma\{aF(\mu\mathbf{u}+\lambda\mathbf{w})+\alpha(\mu\mathbf{u}+\lambda\mathbf{w}).\mathbf{v}\}\right),$$

for suitable $\lambda, \mu \in \mathfrak{o}$ such that

$$\mathrm{ord}_{\mathfrak{p}}(\mu) = \mathrm{ord}_{\tilde{\mathfrak{p}}}(\lambda) = 0 \quad \text{and} \quad \mathrm{ord}_{\mathfrak{p}}(\lambda) = \mathrm{ord}_{\tilde{\mathfrak{p}}}(\mu) = 1.$$

Clearly,

$$\psi\left(\gamma\alpha(\mu\mathbf{u}+\lambda\mathbf{w}).\mathbf{v}\right) = \psi\left(\gamma\alpha\mu\mathbf{u}.\mathbf{v}\right)\psi\left(\gamma\alpha\lambda\mathbf{w}.\mathbf{v}\right)$$

and

$$\psi\left(\gamma a F(\mu\mathbf{u}+\lambda\mathbf{w})\right) = \psi\left(\gamma a\left\{\mu^2\sum_{i=1}^{n} a_i u_i^2 + (\lambda^\tau)^2 \sum_{i=1}^{m} b_i (w_i^\tau)^2\right\}\right)$$

since the characters $\psi(\gamma\lambda\cdot)$ and $\psi(\gamma\mu^\tau\cdot)$ are both trivial on $\mathfrak{o}$. Putting everything together, it follows that

$$S_{\mathfrak{p}} = \Sigma_0 \sum_{a \in (\mathfrak{o}/\mathfrak{p})^*} \psi(-\gamma a N)\Sigma_1(a)\Sigma_2(a), \tag{6.2}$$

where

$$\begin{aligned}
\Sigma_0 &= \prod_{i=m+1}^{n} \sum_{w \in \mathfrak{o}/\tilde{\mathfrak{p}}} \psi\left(\gamma\alpha\lambda w v_i\right), \\
\Sigma_1(a) &= \sum_{\mathbf{u} \in (\mathfrak{o}/\mathfrak{p})^n} \psi\left(\gamma\left\{a\mu^2\sum_{i=1}^{n} a_i u_i^2 + \alpha\mu\mathbf{u}.\mathbf{v}\right\}\right), \\
\Sigma_2(a) &= \sum_{\mathbf{w} \in (\mathfrak{o}/\tilde{\mathfrak{p}})^m} \psi\left(\gamma\left\{a(\lambda^\tau)^2\sum_{i=1}^{m} b_i (w_i^\tau)^2 + \alpha\lambda\sum_{i=1}^{m} w_i v_i\right\}\right).
\end{aligned}$$

We estimate the first sum trivially via $\Sigma_0 \ll (\mathrm{N}\tilde{\mathfrak{p}})^{n-m} = (\mathrm{N}\mathfrak{p})^{n-m}$.

The second sum factorises as

$$\Sigma_1(a) = \prod_{i=1}^{n} \sum_{u \in \mathfrak{o}/\mathfrak{p}} \psi\left(\gamma\left\{a\mu^2 a_i u^2 + u(\alpha\mu v_i)\right\}\right).$$

Recall from the definition of $\mathfrak{F}(\mathfrak{p})$ that $\alpha \in \mathfrak{p}\mathfrak{d}$. Hence,

$$\alpha\mu v_i \in \mathfrak{p}\mathfrak{d}\cdot\tilde{\mathfrak{p}}\cdot\mathscr{A}^G\mathfrak{p} = \mathfrak{o}$$

since $\mathrm{ord}_{\tilde{\mathfrak{p}}}(\mu) = 1$ and $\mathbf{v} \in \widehat{{}^G\mathfrak{p}}^n$, by assumption. Making the change of variables

$$u \to u - \overline{2a\mu^2 a_i}\alpha\mu v_i,$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

where $\overline{2a\mu^2a_i}$ denotes the multiplicative inverse of $2a\mu^2a_i$ modulo $\mathfrak{p}$, we are led to the expression

$$\sum_{u\in\mathfrak{o}/\mathfrak{p}}\psi\left(\gamma\left\{a\mu^2a_iu^2+u(\alpha\mu v_i)\right\}\right)=\psi\left(-\gamma\overline{4a\mu^2a_i}(\mu\alpha v_i)^2\right)\sum_{u\in\mathfrak{o}/\mathfrak{p}}\psi\left(\gamma a\mu^2a_iu^2\right)$$

since $\overline{4}-\overline{2}\equiv-\overline{4}\pmod{\mathfrak{p}}$. The inner sum is a classical Gauss sum, as found in work of Hecke [7, Satz 155], for example. We obtain

$$\sum_{u\in\mathfrak{o}/\mathfrak{p}}\psi\left(\gamma\left\{a\mu^2a_iu^2+u(\alpha\mu v_i)\right\}\right)=\left(\frac{aa_i}{\mathfrak{p}}\right)\tau_{\mathfrak{p}}\psi\left(-\gamma\overline{4a\mu^2a_i}(\mu\alpha v_i)^2\right),$$

where

$$\tau_{\mathfrak{p}}=\sum_{u\in\mathfrak{o}/\mathfrak{p}}\psi\left(\gamma u^2\right).$$

This completes the proof of the identity

$$\Sigma_1(a)=\left(\frac{a}{\mathfrak{p}}\right)^n\left(\frac{a_1\cdots a_n}{\mathfrak{p}}\right)\tau_{\mathfrak{p}}^n\psi\left(-\gamma\overline{4a\mu^2}\sum_{i=1}^n\overline{a_i}(\mu\alpha v_i)^2\right).$$

It turns out that the remaining sum $\Sigma_2(a)$ can also be interpreted as a product of Gauss sums. First, we observe that we have the factorisation

$$\begin{aligned}\Sigma_2(a)&=\prod_{i=1}^m\sum_{w\in\mathfrak{o}/\tilde{\mathfrak{p}}}\psi\left(\gamma\left\{a(\lambda^\tau)^2b_i(w^\tau)^2+\alpha\lambda wv_i\right\}\right)\\&=\prod_{i=1}^m\sum_{u\in\mathfrak{o}/\mathfrak{p}}\psi\left(\gamma\left\{a(\lambda^\tau)^2b_iu^2+\alpha\lambda u^{\tau^{-1}}v_i\right\}\right),\end{aligned}$$

on making the change of variables $u=w^\tau$. The trace is left invariant under conjugation. On recalling that $g\in\mathbb{Z}$ so that $g^\tau=g$, it therefore follows that

$$\psi\left(\gamma\alpha\lambda u^{\tau^{-1}}v_i\right)=\psi\left(\gamma^\tau\alpha^\tau\lambda^\tau uv_i^\tau\right)=\psi\left(\gamma\alpha\lambda^\tau uv_i^\tau\right)$$

since $(\gamma\alpha)^\tau=g=\gamma\alpha$. Hence,

$$\Sigma_2(a)=\prod_{i=1}^m\sum_{u\in\mathfrak{o}/\mathfrak{p}}\psi\left(\gamma\left\{a(\lambda^\tau)^2b_iu^2+u(\alpha\lambda^\tau v_i^\tau)\right\}\right),$$

where

$$\alpha\lambda^\tau v_i^\tau\in\mathfrak{p}\mathfrak{d}\cdot\mathfrak{p}^\tau\cdot\left(\tilde{}^G\mathfrak{p}\right)^\tau\in\mathfrak{o},$$

for $1\leqslant i\leqslant m$. The inner sum is a Gauss sum that we can evaluate, as previously. This yields

$$\Sigma_2(a)=\left(\frac{a}{\mathfrak{p}}\right)^m\left(\frac{b_1\cdots b_m}{\mathfrak{p}}\right)\tau_{\mathfrak{p}}^m\psi\left(-\gamma\overline{4a(\lambda^\tau)^2}\sum_{i=1}^m\overline{b_i}(\lambda^\tau\alpha v_i^\tau)^2\right).$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We now piece everything together in Equation (6.2). To begin with, it follows from squaring and differencing that

$$|\tau_{\mathfrak{p}}|^2 = \sum_{u \in \mathfrak{o}/\mathfrak{p}} \psi\left(\gamma u^2\right) \sum_{v \in \mathfrak{o}/\mathfrak{p}} \psi\left(2\gamma uv\right).$$

Since $\mathfrak{p} \nmid 2$, we see that the inner sum is $\mathrm{N}\mathfrak{p}$ if $u \in \mathfrak{p}$ and and 0 otherwise. Hence, it follows that $|\tau_{\mathfrak{p}}| = \sqrt{\mathrm{N}\mathfrak{p}}$, from which we deduce that

$$S_{\mathfrak{p}} \ll (\mathrm{N}\mathfrak{p})^{(3n-m)/2} \left| \sum_{a \in (\mathfrak{o}/\mathfrak{p})^*} \left(\frac{a}{\mathfrak{p}}\right)^{m+n} \psi\left(\gamma\left\{-aN - \overline{4a}M\right\}\right) \right|,$$

where

$$M = \overline{\mu^2} \sum_{i=1}^{n} \overline{a_i} (\mu \alpha v_i)^2 + \overline{(\lambda^\tau)^2} \sum_{i=1}^{m} \overline{b_i} (\lambda^\tau \alpha v_i^\tau)^2.$$

Since $\mathfrak{p} \nmid 2a_1 \cdots a_n b_1 \cdots b_m \mu \lambda^\tau$, we may replace $\overline{a}$ by $4aa_1 \cdots a_n b_1 \cdots b_m \mu^2 (\lambda^\tau)^2$ by a in order to obtain

$$S_{\mathfrak{p}}(\mathbf{v}) \ll (\mathrm{N}\mathfrak{p})^{(3n-m)/2} |K_{\mathfrak{p}}|,$$

with

$$K_{\mathfrak{p}} = \sum_{a \in (\mathfrak{o}/\mathfrak{p})^*} \left(\frac{a}{\mathfrak{p}}\right)^{m+n} \psi\left(\gamma\left\{-a\mu^2(\lambda^\tau)^2\alpha^2 G(\mathbf{v}) - \overline{4aa_1 \cdots a_n b_1 \cdots b_m \mu^2 (\lambda^\tau)^2} N\right\}\right),$$

with G is given by Equation (6.1). One notes that $\mu^2(\lambda^\tau)^2\alpha^2 G(\mathbf{v}) \in \mathfrak{o}$ when $\mathbf{v} \in (\widehat{G\mathfrak{p}})^n$. In particular,

$$\mathrm{ord}_{\mathfrak{p}}\left(\mu^2(\lambda^\tau)^2\alpha^2 G(\mathbf{v})\right) = \mathrm{ord}_{\mathfrak{p}}(G(\mathbf{v})) + 2.$$

Thus, $K_{\mathfrak{p}}$ is a Kloosterman sum, if $2 \mid m+n$, and a Salié sum if $2 \nmid m+n$. It follows that

$$K_{\mathfrak{p}} \ll \begin{cases} \mathrm{N}\mathfrak{p} & \text{if } \mathfrak{p} \mid N \text{ and } \mathrm{ord}_{\mathfrak{p}}(G(\mathbf{v})) + 2 > 0, \\ \sqrt{\mathrm{N}\mathfrak{p}} & \text{otherwise.} \end{cases}$$

The statement of the lemma is now clear. □

We are now ready to reveal our final estimate for the exponential sum $S_{\mathfrak{b}}(N; \mathbf{m})$.

Lemma 6.2. *Let $\varepsilon > 0$. Let $\mathfrak{b} \subset \mathfrak{o}$ be a nonzero ideal, and let $\mathbf{m} \in \widehat{{}^{G}\mathfrak{b}}^{n}$. Then*

$$S_{\mathfrak{b}}(N; \mathbf{m}) \ll (\mathrm{N}\mathfrak{b})^{\frac{1}{2} - (n-m)/2 + \varepsilon} (\mathrm{N}\,{}^{G}\mathfrak{b})^{n-m/2} \prod_{\substack{\mathfrak{p} \mid (\mathfrak{b}, N) \\ \mathrm{N}\mathfrak{p} \parallel \mathrm{N}\mathfrak{b} \\ \mathrm{ord}_{\mathfrak{p}}(G(\mathbf{m})) \geqslant -1}} (\mathrm{N}\mathfrak{p})^{\frac{1}{2}} \prod_{\substack{p^k \parallel \mathrm{N}\mathfrak{b} \\ k \geqslant 2}} p^{\frac{k}{2}},$$

where G is given by Equation (6.1).

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Proof. There is a factorisation $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$, where $\mathrm{N}\,\mathfrak{b}_1$ is square-free and $\mathrm{N}\,\mathfrak{b}_2$ is square-full, with $\gcd(\mathrm{N}\,\mathfrak{b}_1, \mathrm{N}\,\mathfrak{b}_2) = 1$. It follows from Lemma 4.5 and Corollary 5.3 that

$$\begin{aligned} S_{\mathfrak{b}}(N;\mathbf{m}) &= S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2 N;(\mathrm{N}\,\mathfrak{b}_2)\mathbf{m}) S_{\mathfrak{b}_2}(\overline{\mathrm{N}\,\mathfrak{b}_1}^2 N;(\mathrm{N}\,\mathfrak{b}_1)\mathbf{m}) \\ &\ll |S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2 N;(\mathrm{N}\,\mathfrak{b}_2)\mathbf{m})| (\mathrm{N}\,\mathfrak{b}_2)^{1-(n-m)/2} (\mathrm{N}^G\mathfrak{b}_2)^{n-m/2}. \end{aligned} \tag{6.3}$$

We now turn to $S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2 N;(\mathrm{N}\,\mathfrak{b}_2)\mathbf{m})$, in which we note that

$$(\mathrm{N}\,\mathfrak{b}_2)m_i \in (\mathrm{N}\,\mathfrak{b}_2)\widehat{{}^G\mathfrak{b}} \in \widehat{{}^G\mathfrak{b}_1}(\mathrm{N}\,\mathfrak{b}_2)^G\mathfrak{b}_2^{-1} \in \widehat{{}^G\mathfrak{b}_1},$$

for $1 \leqslant i \leqslant n$. Since $\mathrm{N}\,\mathfrak{b}_1$ is square-free, we have a factorisation

$$\mathfrak{b}_1 = \mathfrak{q}_1 \cdots \mathfrak{q}_r,$$

for distinct prime ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$ of residue degree 1 such that $\mathrm{N}\,\mathfrak{q}_1, \cdots, \mathrm{N}\,\mathfrak{q}_r$ are distinct rational primes. Let

$$c_i = \prod_{\substack{j=1 \\ j\neq i}}^{r} \mathrm{N}\,\mathfrak{q}_j,$$

for $1 \leqslant i \leqslant r$. It now follows from a further application of Lemma 4.5 that

$$S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2 N;(\mathrm{N}\,\mathfrak{b}_2)\mathbf{m}) = S_{\mathfrak{q}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2\overline{c_1}^2 N;(\mathrm{N}\,\mathfrak{b}_2)c_1\mathbf{m}) \cdots S_{\mathfrak{q}_r}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2\overline{c_r}^2 N;(\mathrm{N}\,\mathfrak{b}_2)c_r\mathbf{m}).$$

In particular, we plainly have $(\mathrm{N}\,\mathfrak{b}_2)c_i\mathbf{m} \in (\widehat{{}^G\mathfrak{q}_i})^n$ for $1 \leqslant i \leqslant r$.

We are now aligned for an application of Lemma 6.1. For each $i \in \{1,\dots,r\}$, this yields

$$S_{\mathfrak{q}_i}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2\overline{c_i}^2 N;(\mathrm{N}\,\mathfrak{b}_2)c_i\mathbf{m}) \ll (\mathrm{N}\,\mathfrak{q}_i)^{\theta_{\mathfrak{q}_i}+(3n-m)/2},$$

where

$$\theta_{\mathfrak{q}_i} = \begin{cases} 1 & \text{if } \mathfrak{q}_i \mid N \text{ and } \mathrm{ord}_{\mathfrak{q}_i}(G(\mathbf{m})) \geqslant -1, \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Note that

$$(\mathrm{N}\,\mathfrak{q}_i)^{\theta_{\mathfrak{q}_i}+(3n-m)/2} = (\mathrm{N}\,\mathfrak{q}_i)^{\theta_{\mathfrak{q}_i}-(n-m)/2} (\mathrm{N}^G\mathfrak{q}_i)^{n-m/2}$$

since $\mathrm{N}^G\mathfrak{q}_i = (\mathrm{N}\,\mathfrak{q}_i)^2$. Thus,

$$S_{\mathfrak{b}_1}(\overline{\mathrm{N}\,\mathfrak{b}_2}^2 N;(\mathrm{N}\,\mathfrak{b}_2)\mathbf{m}) \ll (\mathrm{N}\,\mathfrak{b}_1)^{\frac{1}{2}-(n-m)/2+\varepsilon} (\mathrm{N}^G\mathfrak{b}_1)^{n-m/2} \prod_{\substack{\mathfrak{p}\mid(\mathfrak{b}_1,N) \\ \mathrm{ord}_{\mathfrak{p}}(G(\mathbf{m}))\geqslant -1}} (\mathrm{N}\,\mathfrak{p})^{\frac{1}{2}}.$$

Combining these estimates in Equation (6.3), we conclude that

$$S_{\mathfrak{b}}(N;\mathbf{m}) \ll (\mathrm{N}\,\mathfrak{b})^{\frac{1}{2}-(n-m)/2+\varepsilon} (\mathrm{N}^G\mathfrak{b})^{n-m/2} (\mathrm{N}\,\mathfrak{b}_2)^{\frac{1}{2}} \prod_{\substack{\mathfrak{p}\mid(\mathfrak{b}_1,N) \\ \mathrm{ord}_{\mathfrak{p}}(G(\mathbf{m}))\geqslant -1}} (\mathrm{N}\,\mathfrak{p})^{\frac{1}{2}}$$

since $(\mathrm{N}\,\mathfrak{b}_1)(\mathrm{N}\,\mathfrak{b}_2) = \mathrm{N}\,\mathfrak{b}$ and $(\mathrm{N}^G\mathfrak{b}_1)(\mathrm{N}^G\mathfrak{b}_2) = \mathrm{N}^G\mathfrak{b}$. The statement of the lemma is now clear. □

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Our next task is to analyse the oscillatory integral $K(u,P\mathbf{m})$ when F is given by Equation (1.5), based on Equation (4.15). To the fixed automorphism $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ in Equation (1.5), we can associated a unique integer $l_\tau \in \{1,\dots,d\}$, as in Equation (1.4). We therefore have

$$F^{(l)}(\underline{\mathbf{x}}) = \sum_{i=1}^{n} a_i^{(l)} (x_i^{(l)})^2 + \sum_{i=1}^{m} b_i^{(l)} (x_i^{(l_{\tau^{-1}})})^2,$$

for $1 \leqslant l \leqslant d$. Let $\mathbf{A}_l = \mathrm{Diag}(a_1^{(l)},\dots,a_n^{(l)})$ and $\mathbf{B}_l = \mathrm{Diag}(b_1^{(l)},\dots,b_m^{(l)},0,\dots,0)$. Then it follows that the quadratic form Equation (4.14) has an underlying matrix which is the block diagonal matrix

$$\begin{pmatrix} u_1\mathbf{A}_1 + u_{1_\tau}\mathbf{B}_{1_\tau} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & u_2\mathbf{A}_2 + u_{2_\tau}\mathbf{B}_{2_\tau} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & u_d\mathbf{A}_d + u_{d_\tau}\mathbf{B}_{d_\tau} \end{pmatrix}.$$

If $\mathbf{m}$ is given coordinates $\underline{\mathbf{m}} = (\mathbf{m}^{(1)},\dots,\mathbf{m}^{(d)})$ on V^n, then we have

$$K(u,P\mathbf{m}) = \prod_{l=1}^{d} \int_{\mathbb{R}^n} W(\mathbf{x}^{(l)}) e\left(G^{(l)}(\mathbf{x}^{(l)}) - P\mathbf{m}^{(l)}.\mathbf{x}^{(l)}\right) \mathrm{d}\mathbf{x}^{(l)},$$

where $G^{(l)}$ has underlying matrix $u_l\mathbf{A}_l + u_{l_\tau}\mathbf{B}_l$. Since this matrix is diagonal, on assuming that the weight W is chosen suitably, we may further factorise to obtain

$$K(u,P\mathbf{m}) = \prod_{l=1}^{d} H_1^{(l)} \cdots H_m^{(l)} I_{m+1}^{(l)} \cdots I_n^{(l)},$$

where we write

$$H_i^{(l)} = \int_{\mathbb{R}} W(x) e\left((a_i^{(l)}u_l + b_i^{(l_\tau)}u_{l_\tau})x^2 - Pm_i^{(l)}x\right) \mathrm{d}x$$

for $i \leqslant m$, and

$$I_i^{(l)} = \int_{\mathbb{R}} W(x) e\left(a_i^{(l)}u_l x^2 - Pm_i^{(l)}x\right) \mathrm{d}x$$

for $i > m$.

Lemma 6.3. *Let*

$$L_i(u) = a_i u + \tau^{-1}(b_i u),$$

for $1 \leqslant i \leqslant m$. Then, for any $\varepsilon > 0$, $K(u,P\mathbf{m})$ is essentially supported on the set of u and $\mathbf{m}$ for which

$$|m_i^{(l)}| \ll \begin{cases} P^{-1+\varepsilon}|\rho_l(L_i(u))| & \text{if } i \leqslant m, \\ P^{-1+\varepsilon}|u_l| & \text{if } i > m, \end{cases} \tag{6.4}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

for $1 \leqslant l \leqslant d$. Moreover, we have

$$K(u,P\mathbf{m}) \ll \frac{1}{\sqrt{\mathfrak{H}(L_1(u))\cdots\mathfrak{H}(L_m(u))\mathfrak{H}(u)^{n-m}}}.$$

Proof. Clearly, we get exponential decay in $K(u,P\mathbf{m})$ unless $P|\mathbf{m}| \ll |u|P^{\varepsilon}$, as we now assume. However, on examining each of the factors in $K(u,P\mathbf{m})$ separately, the essential support of $K(u,P\mathbf{m})$ is rendered clear. Next, for each $i \leqslant m$ and $1 \leqslant l \leqslant d$, we have $\rho_l(L_i(u)) = a_i^{(l)}u_l + b_i^{(l_\tau)}u_{l_\tau}$. The second derivative bound for exponential integrals yields

$$H_i^{(l)} \ll \min\left(1,\ |\rho_l(L_i(u))|^{-1/2}\right),$$

for $i \leqslant m$, and

$$I_i^{(l)} \ll \min\left(1,\ |u_l|^{-1/2}\right),$$

for $i > m$. The statement is now clear. □

We now piece everything together in our expression (4.23) for $E(N;P;X,Y)$. We shall continue to adhere to the convention that the value of $\varepsilon > 0$ is allowed to change at each appearance and that all implied constants are allowed to depend on ε.

Recall the definition of $\mathscr{U}$ from Equation (4.22). Combining Equation (4.23) and Lemma 6.3, we obtain

$$E(N;P;X,Y) \ll_A P^{\varepsilon}Y^{-n} \sum_{\mathfrak{b}\in\mathscr{B}(X,Y)} \sum_{0\neq\mathbf{m}\in\widehat{G}_{\mathfrak{b}}{}^n} |S_{\mathfrak{b}}(N;\mathbf{m})| \int_{\mathscr{R}(\mathbf{m})} f(u)\mathrm{d}u + P^{-A},$$

where now

$$f(u) = \frac{1}{\sqrt{\mathfrak{H}(L_1(u))\cdots\mathfrak{H}(L_m(u))\mathfrak{H}(u)^{n-m}}} \tag{6.5}$$

and $\mathscr{R}(\mathbf{m})$ denotes the set of $u \in \mathscr{U}$ such that Equation (6.4) holds.

We now make the exact same change of variables $\mathbf{c} = \delta\mathbf{m}$ that we made previously in Equation (5.2). Then, in particular, we can assume that Equation (5.3) holds. Moreover, on dropping the information about $G(\mathbf{m})$, Lemma 6.2 yields

$$\begin{aligned} S_{\mathfrak{b}}(N;\delta^{-1}\mathbf{c}) &\ll (\mathrm{N}\,\mathfrak{b})^{\frac{1}{2}-(n-m)/2+\varepsilon}(\mathrm{N}^{G}\mathfrak{b})^{n-m/2}\sqrt{g(\mathfrak{b})} \\ &\ll X^{\frac{1}{2}-(n-m)/2+\varepsilon}Y^{n-m/2}\sqrt{g(\mathfrak{b})}, \end{aligned}$$

where

$$g(\mathfrak{b}) = \prod_{\substack{\mathfrak{p}|(\mathfrak{b},N)\\ \mathrm{N}\,\mathfrak{p}\|\,\mathrm{N}\,\mathfrak{b}}} \mathrm{N}\,\mathfrak{p} \prod_{\substack{p^k\|\,\mathrm{N}\,\mathfrak{b}\\ k\geqslant 2}} p^k.$$

In this notation, we conclude that

$$E(N;P;X,Y) \ll_A \frac{X^{\frac{1}{2}-(n-m)/2}P^{\varepsilon}}{Y^{m/2}} \sum_{\mathfrak{b}\in\mathscr{B}(X,Y)} \sum_{\substack{0\neq\mathbf{c}\in\mathfrak{o}^n\\ \text{(5.3) holds}}} \sqrt{g(\mathfrak{b})} \int_{\mathscr{R}(\delta^{-1}\mathbf{c})} f(u)\mathrm{d}u + P^{-A}.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Let

$$L(u) = \sum_{\mathfrak{b} \in \mathscr{B}(X,Y)} \sum_{\mathbf{c} \in \mathscr{C}(u,\mathfrak{b})} \sqrt{g(\mathfrak{b})},$$

where $\mathscr{C}(u,\mathfrak{b})$ is the set of nonzero vectors $\mathbf{c} \in \mathfrak{o}^n$ for which Equation (5.3) holds and

$$|c_i^{(l)}| \ll \begin{cases} P^{-1+\varepsilon} Y^{1/d} |\rho_l(L_i(u))| & \text{if } i \leqslant m, \\ P^{-1+\varepsilon} Y^{1/d} |u_l| & \text{if } i > m, \end{cases}$$

for $1 \leqslant l \leqslant d$. Then we may write

$$E(N;P;X,Y) \ll \frac{X^{\frac{1}{2}-(n-m)/2} P^{\varepsilon}}{Y^{m/2}} \int_{\mathscr{U}} f(u) L(u) \mathrm{d}u, \tag{6.6}$$

rendering our next task to estimate $L(u)$. The following result is an analogue of Lemma 5.5.

Lemma 6.4. *Let $u \in V$ be such that $\mathfrak{H}(u) \leqslant P^{d+\varepsilon}/X$. If $L(u) \neq 0$, then*

$$\frac{P^{d-\varepsilon}}{X} \ll \mathfrak{H}(u) \ll \frac{P^{d+\varepsilon}}{X} \quad \text{or} \quad P^{-d+\varepsilon} Y \max_{1 \leqslant i \leqslant m} \mathfrak{H}(L_i(u)) \gg 1. \tag{6.7}$$

Moreover, we have $L(u) \ll P^{\varepsilon} X J(u)$, where

$$J(u) = \prod_{i=1}^{m} \max\left\{1, P^{-d} Y \mathfrak{H}(L_i(u))\right\}.$$

Proof. Let us write $\mathfrak{b} = \mathfrak{b}_1 \mathfrak{b}_2$, where $\mathrm{N}\mathfrak{b}_1$ is square-free and $\mathrm{N}\mathfrak{b}_2$ is square-full, with $\gcd(\mathrm{N}\mathfrak{b}_1, \mathrm{N}\mathfrak{b}_2) = 1$. Then $g(\mathfrak{b}) = \mathrm{N}\mathfrak{b}_2 \mathrm{N}\mathfrak{h}$, where $\mathfrak{h}$ is the greatest common ideal divisor of $\mathfrak{b}_1$ and N. In summary, we may now write

$$L(u) \leqslant \sum_{\substack{\mathrm{N}\mathfrak{b}_2 \ll X \\ \mathrm{N}\mathfrak{b}_2 \text{ square-full}}} \sqrt{\mathrm{N}\mathfrak{b}_2} \sum_{\substack{\mathrm{N}\mathfrak{b}_1 \ll X/(\mathrm{N}\mathfrak{b}_2) \\ \mathrm{N}^G\mathfrak{b}_1 \ll Y/\mathrm{N}^G\mathfrak{b}_2 \\ \gcd(\mathrm{N}\mathfrak{b}_1, \mathrm{N}\mathfrak{b}_2)=1}} \mu^2(\mathrm{N}\mathfrak{b}_1) \sum_{\mathfrak{h} | (\mathfrak{b}_1, N)} \sqrt{\mathrm{N}\mathfrak{h}} \#\mathscr{C}(u, \mathfrak{b}_1\mathfrak{b}_2). \tag{6.8}$$

In order to proceed, we assume without loss of generality that $u \in V$ satisfies

$$\mathfrak{H}(L_1(u)) \leqslant \cdots \leqslant \mathfrak{H}(L_m(u)).$$

Let us write $\mathbf{c} = (\mathbf{c}', \mathbf{c}'')$, where $\mathbf{c}' = (c_1, \ldots, c_m)$ and $\mathbf{c}'' = (c_{m+1}, \ldots, c_n)$. Keeping in mind Equation (5.3), we first fix a choice of $\mathbf{c}'' \in \left((\mathfrak{b}_1\mathfrak{b}_2)^{-1G} \mathfrak{b}_1{}^G \mathfrak{b}_2\right)^{n-m}$ satisfying

$$|c_i^{(l)}| \ll P^{-1+\varepsilon} Y^{1/d} |u_l|,$$

for $m+1 \leqslant i \leqslant n$ and $1 \leqslant l \leqslant d$. We claim that there exists $\lambda \in K$ such that

$$(\lambda) = (\mathfrak{b}_1\mathfrak{b}_2)^{-1G} \mathfrak{b}_1{}^G \mathfrak{b}_2 \mathfrak{p}_2^{-1},$$

for a suitable prime ideal $\mathfrak{p}_2$ of norm $O(P^{\varepsilon})$. To begin with, it follows from part (ii) of Lemma 3.1 that there exists $\lambda_3 \in \mathfrak{o}$ such that $(\lambda_3) = (\mathfrak{b}_1\mathfrak{b}_2)^{-1G} \mathfrak{b}_1{}^G \mathfrak{b}_2 \mathfrak{p}_3$ for a suitable prime ideal $\mathfrak{p}_3$ of norm $O(P^{\varepsilon})$. A second application of this result reveals that there exists

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

$\lambda_2 \in \mathfrak{o}$ and a prime ideal $\mathfrak{p}_2$ of norm $O(P^{\varepsilon})$ such that $(\lambda_2) = \mathfrak{p}_3\mathfrak{p}_2$. The claim now follows with $\lambda = \lambda_3/\lambda_2$.

On multiplying by units, we can further assume that

$$X^{-1/d}Y^{1/d} \ll |\lambda^{(l)}| \ll X^{-1/d}Y^{1/d+\varepsilon},$$

for $1 \leqslant l \leqslant d$, on recalling that $\mathrm{N}\,\mathfrak{b}_1\,\mathrm{N}\,\mathfrak{b}_2 \asymp X$ and $\mathrm{N}^G\mathfrak{b}_1\,\mathrm{N}^G\mathfrak{b}_2 \asymp Y$. Making the change of variables $\mathbf{c}'' = \lambda\mathbf{d}''$, we deduce that for $m+1 \leqslant i \leqslant n$, we have $d_i \in \mathfrak{o}$ and

$$|d_i^{(l)}| \ll P^{-1+\varepsilon}X^{1/d}|u_l|,$$

for $1 \leqslant l \leqslant d$. In particular, if $\mathbf{c}'' \neq \mathbf{0}$, then there exists $i \in \{m+1,\dots,n\}$ such that

$$1 \leqslant |N_{K/\mathbb{Q}}(d_i)| \ll P^{-d+\varepsilon}X|\mathrm{Nm}(u)|.$$

Recalling that $\mathrm{Nm}(u) \leqslant \mathfrak{H}(u) \ll P^{d+\varepsilon}/X$, we deduce that

$$\mathbf{c}'' \neq \mathbf{0} \Longrightarrow \frac{P^{d-\varepsilon}}{X} \ll \mathfrak{H}(u) \ll \frac{P^{d+\varepsilon}}{X}. \tag{6.9}$$

Moreover, arguing as in Lemma 5.5, it readily follows from a result in Lang [9, Thm. 0 in §V.1] that the overall number of vectors $\mathbf{d}''$ is $O(P^{\varepsilon})$. We must next address the number of $\mathbf{c}' \in \mathfrak{o}^m$, with $(\mathbf{c}',\mathbf{c}'') \neq \mathbf{0}$, which satisfy

$$|c_i^{(l)}| \ll P^{-1+\varepsilon}Y^{1/d}|\rho_l(L_i(u))|,$$

for $1 \leqslant i \leqslant m$ and $1 \leqslant l \leqslant d$. It is clear that

$$\mathbf{c}' \neq \mathbf{0} \Longrightarrow 1 \ll P^{-d+\varepsilon}Y\mathfrak{H}(L_m(u)). \tag{6.10}$$

Together, Equations (6.9) and (6.10) yield the first part of the lemma.

Appealing once more to Lang [9, Thm. 0 in §V.1], we deduce that the number of $\mathbf{c}'$ is

$$\ll \prod_{i=1}^{m}\left(1+\prod_{l=1}^{d}P^{-1+\varepsilon}Y^{1/d}|\rho_l(L_i(u))|\right) \ll J(u)$$

in the notation of the lemma. Returning to Equation (6.8), we deduce that

$$\begin{aligned} L(u) &\ll P^{\varepsilon}J(u) \sum_{\substack{\mathrm{N}\,\mathfrak{b}_2 \ll X \\ \mathrm{N}\,\mathfrak{b}_2 \text{ square-full}}} \sqrt{\mathrm{N}\,\mathfrak{b}_2}\sum_{\mathfrak{h}\mid N}\sqrt{\mathrm{N}\,\mathfrak{h}} \sum_{\substack{\mathrm{N}\,\mathfrak{b}_1 \ll X/(\mathrm{N}\,\mathfrak{b}_2) \\ \mathfrak{h}\mid\mathfrak{b}_1}} 1 \\ &\ll P^{\varepsilon}J(u) \sum_{\substack{\mathrm{N}\,\mathfrak{b}_2 \ll X \\ \mathrm{N}\,\mathfrak{b}_2 \text{ square-full}}} \sqrt{\mathrm{N}\,\mathfrak{b}_2}\sum_{\mathfrak{h}\mid N}\sqrt{\mathrm{N}\,\mathfrak{h}} \cdot \frac{X}{(\mathrm{N}\,\mathfrak{b}_2)(\mathrm{N}\,\mathfrak{h})} \\ &\ll P^{\varepsilon}XJ(u) \sum_{\substack{\mathrm{N}\,\mathfrak{b}_2 \ll X \\ \mathrm{N}\,\mathfrak{b}_2 \text{ square-full}}} \frac{1}{\sqrt{\mathrm{N}\,\mathfrak{b}_2}} \end{aligned}$$

since there are $O(1)$ ideal divisors $\mathfrak{h} \mid N$ when $N \in \mathfrak{o}$ is nonzero. Finally, the lemma follows on noting that there are $O(\sqrt{X})$ integral ideals such that $\mathrm{N}\,\mathfrak{b}_2$ is a square-full integer of modulus at most X. □

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

We may now apply Lemma 6.4 in Equation (6.6). Let R denote the set of $u \in \mathscr{U}$ such that Equation (6.7) holds. On recalling the definition (6.5) of $f(u)$, we deduce that

$$E(N;P;X,Y) \ll_A P^{-A} + \frac{X^{\frac{3}{2}-(n-m)/2}P^{\varepsilon}}{Y^{m/2}} I(X,Y), \tag{6.11}$$

where

$$I(X,Y) = \int_R \frac{\prod_{i=1}^m \max\left\{1, P^{-d}Y\mathfrak{H}(L_i(u))\right\}}{\sqrt{\mathfrak{H}(L_1(u))\cdots\mathfrak{H}(L_m(u))\mathfrak{H}(u)^{n-m}}}\mathrm{d}u.$$

The following result deals with this integral.

Lemma 6.5. *We have*

$$\begin{aligned} I(X,Y) \ll\ & P^{\varepsilon}(P^{-d}Y)^m \left(\left(\frac{P^d}{X}\right)^{3m/2-n/2+1} + 1\right) \\ & + c_Y P^{\varepsilon}\left(\frac{P^{d(m/2-n/2+1)}Y^{m-1}}{X^{3m/2-n/2}} + \frac{Y}{P^d}\right) + P^{\varepsilon}\left(\frac{P^d}{X}\right)^{1-(n-m)/2}, \end{aligned}$$

where

$$c_Y = \begin{cases} 1 & \text{if } Y \leqslant P^d, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. In the proof of this result, we shall make frequent use of the observation that

$$\mathfrak{H}(L_i(u)) = \prod_{l=1}^{d} \max\{1, |a_i^{(l)}u_l + b_i^{(l_\tau)}u_{l_\tau}|\} \ll \mathfrak{H}(u)^2,$$

for any $i \in \{1,\dots,n\}$, which follows from Equation (5.6).

We may assume without loss of generality that the range of integration is restricted to satisfy

$$\mathfrak{H}(L_1(u)) \leqslant \cdots \leqslant \mathfrak{H}(L_m(u)). \tag{6.12}$$

We further break the range of integration into $m+1$ regions. For $0 \leqslant t \leqslant m$, let R_t denote the set of $u \in V$ with $\mathfrak{H}(u) \leqslant P^{d+\varepsilon}/X$, such that Equations (6.7) and (6.12) hold, with

$$\mathfrak{H}(L_t(u)) \ll P^{d-\varepsilon}/Y, \quad \mathfrak{H}(L_{t+1}(u)) \gg P^{d-\varepsilon}/Y.$$

(Note that the left inequality is vacuous when $t = 0$ and similarly for the right-hand inequality when $t = m$.) In particular, it is clear that $R_m = \emptyset$ when the second inequality in Equation (6.7) holds. Moreover, when $t \in \{1,\dots,m-1\}$, we observe that

$$R_t \neq \emptyset \Longrightarrow Y \ll P^{d-\varepsilon}$$

since $\mathfrak{H}(L_t(u)) \geqslant 1$. We have

$$I(X,Y) \ll \sum_{t=0}^{m} P^{\varepsilon} \int_{R_t} \frac{\left((P^{-d}Y)^{m-t}\mathfrak{H}(L_{t+1}(u))\cdots\mathfrak{H}(L_m(u))\right)}{\sqrt{\mathfrak{H}(L_1(u))\cdots\mathfrak{H}(L_m(u))\mathfrak{H}(u)^{n-m}}}\mathrm{d}u.$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

Thus,

$$I(X,Y) \ll \sum_{t=0}^{m} I^{(t)}(X,Y),$$

where

$$I^{(t)}(X,Y) = (P^{-d}Y)^{m-t}P^{\varepsilon}\int_{R_t} \frac{(\mathfrak{H}(L_{t+1}(u))\cdots\mathfrak{H}(L_m(u)))^{\frac{1}{2}}}{\mathfrak{H}(u)^{(n-m)/2}}\mathrm{d}u,$$

on taking $\mathfrak{H}(L_1(u))\cdots\mathfrak{H}(L_t(u)) \geqslant 1$.

We first deal with $I^{(0)}(X,Y)$. Recalling that $\mathfrak{H}(L_i(u)) \ll \mathfrak{H}(u)^2$ for $1 \leqslant i \leqslant m$, it follows that

$$\frac{(\mathfrak{H}(L_1(u))\cdots\mathfrak{H}(L_m(u)))^{\frac{1}{2}}}{\mathfrak{H}(u)^{(n-m)/2}} \ll \mathfrak{H}(u)^{3m/2-n/2}.$$

If $3m/2-n/2 \geqslant -1$, then Equation (4.13) yields

$$\int_{R_0} \mathfrak{H}(u)^{3m/2-n/2}\mathrm{d}u \ll P^{\varepsilon}\left(\frac{P^d}{X}\right)^{3m/2-n/2+1}.$$

Alternatively, if $3m/2-n/2 < -1$, then the left-hand side is $O(1)$ by Equation (4.11). Thus,

$$I^{(0)}(X,Y) \ll P^{\varepsilon}(P^{-d}Y)^m\left(\left(\frac{P^d}{X}\right)^{3m/2-n/2+1}+1\right),$$

which is satisfactory.

Terms with $1 \leqslant t \leqslant m-1$ only contribute when $Y \leqslant P^d$. Arguing as above, it follows from Equations (4.11) and (4.13) that

$$\begin{aligned}\sum_{t=1}^{m-1} I^{(t)}(X,Y) &\ll \sum_{t=1}^{m-1}(P^{-d}Y)^{m-t}\int_{R_t}\mathfrak{H}(u)^{3m/2-t-n/2}\mathrm{d}u\\ &\ll P^{\varepsilon}\sum_{t=1}^{m-1}(P^{-d}Y)^{m-t}\left(\left(\frac{P^d}{X}\right)^{3m/2-t-n/2+1}+1\right)\\ &\ll P^{\varepsilon}\sum_{t=1}^{m-1}\left((P^{-d}Y)^m\left(\frac{P^d}{X}\right)^{3m/2-n/2+1}\left(\frac{X}{Y}\right)^t+(P^{-d}Y)^{m-t}\right)\\ &\ll P^{\varepsilon}\left\{\frac{P^{d(m/2-n/2+1)}Y^{m-1}}{X^{3m/2-n/2}}+\frac{Y}{P^d}\right\}\end{aligned}$$

since $X \leqslant Y$. This is satisfactory for the lemma.

It remains to estimate $I^{(m)}(X,Y)$. In this case, we may assume that u satisfies the first inequality in Equation (6.7) since $R_m = \emptyset$ otherwise. Hence, Equation (4.12) yields

$$I^{(m)}(X,Y) = \int_{\{u\in V: P^{d-\varepsilon}/X \ll \mathfrak{H}(u) \ll P^{d+\varepsilon}/X\}} \frac{1}{\mathfrak{H}(u)^{(n-m)/2}}\mathrm{d}u \ll P^{\varepsilon}\left(\frac{P^d}{X}\right)^{1-(n-m)/2},$$

which is satisfactory and so completes the proof of the lemma. □

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

It is now time to return to our goal of proving that Equation (4.21) holds for a suitable $\Delta > 0$ for any $X, Y \geqslant 1$ satisfying Equation (4.20). We wish to do so under the assumption that $n - m \geqslant 4$. Applying Lemma 6.5 in Equation (6.11), the overall contribution to $E(N; P; X, Y)$ from the final term is seen to be

$$\begin{aligned}
&\ll \frac{X^{\frac{3}{2}-(n-m)/2} P^{\varepsilon}}{Y^{m/2}} \cdot \left(\frac{P^d}{X}\right)^{1-(n-m)/2} \\
&\ll \frac{X^{1/2}}{Y^{m/2}} P^{-d(n-m-2)/2+\varepsilon} \\
&\ll P^{-d(n-m-2)/2+\varepsilon},
\end{aligned}$$

on taking $X \leqslant Y$ and $m \geqslant 1$. This is $O(P^{-d+\varepsilon})$, if $n - m \geqslant 4$, which is satisfactory for Equation (4.21). Next, the second term in Lemma 6.5 makes the overall contribution

$$\begin{aligned}
&\ll \frac{X^{\frac{3}{2}-(n-m)/2} P^{\varepsilon}}{Y^{m/2}} \cdot c_Y \left(\frac{P^{d(m/2-n/2+1)} Y^{m-1}}{X^{3m/2-n/2}} + \frac{Y}{P^d}\right) \\
&\ll c_Y P^{\varepsilon} \left(\frac{Y^{m/2-1}}{X^{m-3/2} P^{d(n-m-2)/2}} + \frac{X^{3/2-(n-m)/2}}{Y^{m/2-1} P^d}\right).
\end{aligned}$$

If $m \geqslant 2$, we take $Y \leqslant X^2$ in the first term, and $X, Y \geqslant 1$ in the second term. Assuming that $n - m \geqslant 4$, this yields

$$\ll P^{-d(n-m-2)/2+\varepsilon} + P^{-d+\varepsilon} \ll P^{-d+\varepsilon},$$

which is satisfactory for Equation (4.21). If $m = 1$, on the other hand, then we get the contribution

$$\ll c_Y P^{\varepsilon} \left(\frac{X^{1/2}}{Y^{1/2} P^{d(n-3)/2}} + \frac{Y^{1/2}}{X^{(n-4)/2} P^d}\right) \ll P^{-d/2+\varepsilon},$$

by Equation (4.20) and the assumption $n \geqslant m + 4 = 5$, together with the fact that $Y \leqslant P^d$ when $c_Y \neq 0$.

Turning to the contribution to Equation (6.11) from the first term in Lemma 6.5, we see that this is

$$\begin{aligned}
&\ll \frac{X^{\frac{3}{2}-(n-m)/2} P^{\varepsilon}}{Y^{m/2}} \cdot (P^{-d} Y)^m \left(\left(\frac{P^d}{X}\right)^{3m/2-n/2+1} + 1\right) \\
&= \frac{Y^{m/2} P^{d(m-n+2)/2+\varepsilon}}{X^{m-1/2}} + \frac{X^{\frac{3}{2}-(n-m)/2} Y^{m/2} P^{\varepsilon}}{P^{dm}} \\
&\leqslant X^{1/2} P^{d(m-n+2)/2+\varepsilon} + X^{\frac{3}{2}-n/2+3m/2} P^{-dm+\varepsilon}.
\end{aligned}$$

Taking $X \ll P^d$, the first term is $O(P^{-d(n-m-3)/2+\varepsilon})$, which is $O(P^{-d/2+\varepsilon})$, if $n - m \geqslant 4$. The second term is plainly $P^{-dm+\varepsilon}$ if $\frac{3}{2} - n/2 + 3m/2 \leqslant 0$, and it is

$$\ll P^{d(\frac{3}{2}-n/2+m/2)+\varepsilon} = P^{-d(n-m-3)/2+\varepsilon}$$

https://doi.org/10.1017/S1474748024000161 Published online by Cambridge University Press

otherwise, on taking $X \ll P^d$. This is $O(P^{-d/2+\varepsilon})$ if $n-m \geqslant 4$. All of our estimates are satisfactory for Equation (4.21), which therefore concludes the proof of Theorem 1.5.

Acknowledgements. The authors are grateful to Jayce Getz for asking questions that set this project in motion and to the anonymous referee for useful comments. T.B. was supported by a FWF grant (DOI 10.55776/P32428) and by a grant from the Institute for Advanced Study School of Mathematics. L.B.P. was partially supported by NSF DMS-2200470 and DMS-1652173, and thanks the Hausdorff Centre for Mathematics for hosting research visits.

Competing interest. None.

References

[1] B. J. Birch, 'Forms in many variables', *Proc. Roy. Soc. Ser. A* **265** (1961/62), 245–263.
[2] T. D. Browning and P. Vishe, 'Cubic hypersurfaces and a version of the circle method for number fields', *Duke Math. J.* **163** (2014), 1825–1883.
[3] H. Davenport and D. J. Lewis, 'Non-homogeneous cubic equations', *J. Lond. Math. Soc.* **39** (1964), 657–671.
[4] W. Duke, J. B. Friedlander and H. Iwaniec, 'Bounds for automorphic L-functions', *Invent. Math.* **112** (1993), 1–8.
[5] D. R. Heath-Brown, 'A new form of the circle method, and its application to quadratic forms', *J. Reine Angew. Math.* **481** (1996), 149–206.
[6] D. R. Heath-Brown and L. B. Pierce, 'Simultaneous integer values of pairs of quadratic forms', *J. Reine Angew. Math.* **727** (2017), 85–143.
[7] E. Hecke, *Lectures on the Theory of Algebraic Numbers* (Springer-Verlag, 1981).
[8] L.C. Helfrich, 'Quadratische Diophantische Gleichungen über algebraischen Zahlkörpern', PhD thesis, Göttingen University, 2015.
[9] S. Lang, *Algebraic Number Theory* (Springer-Verlag, 1986).
[10] M. Reid, 'The complete intersection of two or more quadrics', PhD thesis, Trinity College, Cambridge, 1972.
[11] S. L. Rydin Myerson, 'Quadratic forms and systems of forms in many variables', *Invent. Math.* **213** (2018), 205–235.
[12] C. M. Skinner, 'Rational points on nonsingular cubic hypersurfaces', *Duke Math. J.* **75** (1994), 409–466.
[13] C. M. Skinner, 'Forms over number fields and weak approximation', *Compositio Math.* **106** (1997), 11–29.