On the Representation of Quadratic Forms by Quadratic Forms

RAINER DIETMANN & MICHAEL HARVEY

1. Introduction

The study of representing an integral quadratic form by another integral quadratic form has a long history in number theory. In this paper we use matrix notation for quadratic forms, so let $A = (A_{ij})$ and $B = (B_{ij})$ be symmetric positive definite integer matrices of dimensions *n* and *m*, respectively. We are interested in finding $n \times m$ integer matrices *X* such that

$$X^{\mathrm{T}}\!AX = B,\tag{1}$$

thereby generalizing the classical problem of representing a positive integer as a sum of squares. Although the local-global principle is known to hold for *rational* solutions X of the Diophantine problem (1), existence of solutions over \mathbb{R} (which is here automatic by positive definiteness) and all local rings \mathbb{Z}_p is not enough to ensure the existence of an *integer* solution X. It is therefore natural to look for additional conditions for ensuring that the local-global principle holds also over \mathbb{Z} . The usual approach is to fix m, n, and A and then try to represent "large enough" Bfor dimension m as large as possible in terms of n. In this context, Hsia, Kitaoka, and Kneser [9] have shown the local-global principle to hold whenever $n \ge 2m+3$ and min $B \ge c_1$ for some constant c_1 depending only on A and n, where (as usual) min B denotes the first successive minimum of B; that is,

$$\min B = \min_{\mathbf{x} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}} \mathbf{x}^{\mathrm{T}} B \mathbf{x}.$$

Ellenberg and Venkatesh [7] used ergodic theory to show that the condition on n can be greatly improved to $n \ge m + 5$ under the additional assumption that the discriminant of B is square-free. This latter condition has been refined by Schulze-Pillot [15].

The methods just described do not yield any quantitative information about integer solutions to (1). Let N(A, B) denote the number of integer matrices X satisfying (1), and note that this quantity is finite because A is positive definite. Siegel [17] gave an exact formula for a weighted version of N(A, B). Let \mathfrak{A} be a set of representatives of all equivalence classes of forms in the genus of A. For

Received January 2, 2013. Revision received May 23, 2013.

Work of both authors was supported by Grant no. EP/I018824/1, "Forms in Many Variables".

such a representative $A' \in \mathfrak{A}$, let o(A') denote the number of automorphs of A' and let $W(\mathfrak{A}) = \sum_{A' \in \mathfrak{A}} 1/o(A')$. Then Siegel showed that

$$\frac{\sum_{A' \in \mathfrak{A}} N(A', B) / o(A')}{W(\mathfrak{A})} = \begin{cases} \alpha_{\infty}(A, B) \prod_{p} \alpha_{p}(A, B) & \text{if } m < n - 1, \\ \frac{1}{2} \alpha_{\infty}(A, B) \prod_{p} \alpha_{p}(A, B) & \text{if } m = n - 1, \end{cases}$$

where (i) these factors depend only on the genera of A and B, (ii) the term

$$\alpha_{\infty}(A,B) = (\det A)^{-m/2} (\det B)^{(n-m-1)/2} \pi^{m(2n-m+1)/4} \prod_{n-m < j \le n} \frac{1}{\Gamma(j/2)}$$
(2)

corresponds to the density of real solutions to (1), and (iii) for any prime p we have

$$\alpha_p(A, B) = (p^{-t})^{mn - m(m+1)/2} \# \{ X \mod p^t : X^{\mathsf{T}} A X \equiv B \pmod{p^t} \}$$
(3)

for all sufficiently large integers t. In particular, if the genus of A contains only one equivalence class then this gives an exact formula for N(A, B); however, if the genus of A contains more than one class then we obtain only an upper bound on N(A, B). Our focus in this paper is on deriving not an exact but rather an *asymptotic* formula for N(A, B), yet one that is valid for all forms A. In this context, by "asymptotic" we mean asymptotic in terms of the successive minima of B. Without changing N(A, B) and by replacing B with an equivalent form if necessary, we may assume that B is Minkowski-reduced. In particular,

 $0 < \min B = B_{11} \le B_{22} \le \cdots \le B_{mm}, |B_{ij}| \le B_{ii} \ (1 \le i < j \le m).$

For $1 \le i \le m$, define γ_i to be the positive real number satisfying

$$B_{11} = B_{ii}^{\gamma_i}, (4)$$

and define

$$\gamma := \sum_{i=1}^{m} \frac{1}{\gamma_i}.$$
(5)

Note that $\gamma_i \leq 1 \ (1 \leq i \leq m)$.

THEOREM 1.1. Suppose that $n > (2\gamma + m(m-1))(\frac{m(m+1)}{2} + 1)$. Then there exists $a \delta > 0$ such that

$$N(A, B) = \alpha_{\infty}(A, B) \prod_{p} \alpha_{p}(A, B) + O((\det B)^{(n-m-1)/2-\delta}),$$
(6)

where $\alpha_{\infty}(A, B), \alpha_p(A, B)$ are defined as before and the implied O-constant does not depend on B.

For $n \ge 2m + 3$ it was shown by Kitaoka [11, Props. 5 and 9] that

$$1 \ll \prod_{p} \alpha_{p}(A, B) \ll 1 \tag{7}$$

whenever equation (1) is soluble over each \mathbb{Z}_p , where the implicit constants are independent of *B*. Recalling (2), we find that the main term in (6) is of greater order of magnitude than the error term and gives a true asymptotic formula—provided

that det *B* is large enough in terms of *m*, *n*, and *A*. Since γ is bounded for fixed *m* and *n*, the latter condition is equivalent to $B_{11} \ge c_2$ for some constant c_2 depending only on *m*, *n*, and *A*.

Let us now briefly connect our result to others in the literature. If m = 1 then, as mentioned previously, equation (1) reduces to the classical problem of representing a positive integer by a positive definite quadratic form. One attains such an asymptotic formula for N(A, B) as long as $n \ge 3$ (see [6; 8]). For general m > 1, Raghavan [14] used the theory of Siegel modular forms to establish an asymptotic formula whenever $n \ge 2m + 3$ under the assumption

$$B_{11} = \min B \ge c_3 (\det B)^{1/m}$$
(8)

for some fixed constant c_3 . We note that there exists some constant c_4 , depending only on *m*, such that $B_{11} \le c_4 (\det B)^{1/m}$. Hence Raghavan's result requires the successive minima of *B* to be of similar order, which essentially translates into the condition $\gamma = 1$ in our setting. Our result does not require this condition, but it may require a much larger number *n* of variables when B_{11} is much smaller than det *B*. For m = 2 and $n \ge 7$, Kitaoka [11] showed that the condition $B_{11} \ge c_5$ for some constant c_5 (depending only on *n* and *A*) suffices, thus avoiding any further assumptions and in this way paralleling what is known for m = 1. No such result is known yet for m > 2; see Schulze-Pillot [16] for more background information on this topic.

Whereas most previous approaches to this problem have used modular forms, our strategy is to treat equation (1) as a system of R := m(m + 1)/2 quadratic equations and then to apply the circle method; see [5] and [2] for circle method approaches to related higher-degree problems. The main difficulty is adapting the method to work in a box with uneven side lengths, and this is exactly where the dependence on γ comes in. We obtain a version of Weyl's inequality in Section 2 upon following the method of Birch [1] as well as an argument of Parsell [13, Lemma 4.1]. We then use that inequality to estimate the minor arcs in Section 3 before handling the major arcs in Section 4. Once this has been accomplished, we need to establish the main term in Theorem 1.1 by examining the singular series and the singular integral in Sections 5 and 6, respectively.

NOTATION. As usual, ε will denote a small positive number that may change in value from one statement to the next. All implied constants may depend on A, m, n, and ε . We apply the usual notation that $e(z) = e^{2\pi i z}$ and $e_q(z) = e^{2\pi i z/q}$. We use ||x|| to denote the distance of the nearest integer to a real number x. We also set $|\mathbf{x}| = \max_{1 \le i \le n} |x_i|$ for the maximum norm for any vector $\mathbf{x} \in \mathbb{R}^n$, and we write (a, b) for the greatest common divisor of two integers a and b. Summations over vectors \mathbf{x} are usually to be understood as summation over $\mathbf{x} \in \mathbb{Z}^n$, and multidimensional integrations are usually to be understood as occurring in R-dimensional space. We sometimes use conditions of the form $q \ll L$ for a certain quantity L—in particular, in summations and integrals. These conditions are to be understood in the following way: There exists a suitable constant C, depending at most on A, m, n, and ε , such that the condition $q \ll L$ can be replaced by $q \leq CL$.

2. Weyl-Type Inequalities

By letting $X = (\mathbf{x}_1 \cdots \mathbf{x}_m)$, with column vectors $\mathbf{x}_i = (x_{i1}, \dots, x_{in}) \in \mathbb{Z}^n$ for each $i \in \{1, \dots, m\}$, we may write (1) as the following system of R := m(m + 1)/2 equations:

$$\mathbf{x}_i^{\mathrm{T}} A \mathbf{x}_j = B_{ij} \quad (1 \le i \le j \le m)$$

Since A is positive definite, these equations clearly imply that

$$|\mathbf{x}_i| \ll B_{ii}^{1/2} \quad (1 \le i \le m)$$

for an implicit constant depending only on A; and since B is positive definite, there exists a real solution of these equations within that range. So for sufficiently large C depending only on A, define

$$P_i := C^{1/\gamma_i} B_{ii}^{1/2} \tag{9}$$

for each $i \in \{1, ..., m\}$ and note that, by (4), we have

$$0 < P_1 \le \dots \le P_m, \quad P_1 = P_i^{\gamma_i} \quad (1 \le i \le m).$$
⁽¹⁰⁾

For convenience, we shall also define

$$\Pi := \prod_{i=1}^m P_i.$$

Observe that

$$\Pi = P_i^{\gamma \gamma_i} \quad (1 \le i \le m) \tag{11}$$

by (5) and (10).

For real $\boldsymbol{\alpha} = (\alpha_{ij})_{1 \le i \le j \le m}$ and $\mathbf{b} = (B_{ij})_{1 \le i \le j \le m}$, we define the exponential sum

$$S(\boldsymbol{\alpha}, \mathbf{b}) := \sum_{|\mathbf{x}_1| \le P_1} \cdots \sum_{|\mathbf{x}_m| \le P_m} e\left(\sum_{1 \le i \le j \le m} \alpha_{ij}(\mathbf{x}_i^{\mathrm{T}} A \mathbf{x}_j - B_{ij})\right)$$

and let $S(\boldsymbol{\alpha}) := S(\boldsymbol{\alpha}, \boldsymbol{0})$. By our choice of *C* and P_i , we then have

$$N(A, B) = \int_{[0,1)^R} S(\boldsymbol{\alpha}, \mathbf{b}) \, d\boldsymbol{\alpha}.$$
 (12)

Our aim is to show that, if *n* is large enough, then $S(\alpha)$ is "small" unless each α_{ij} is well approximated by a rational number with small denominator. The next lemma achieves this for the diagonal coefficients α_{ii} .

LEMMA 2.1. Let $0 < \theta < 1$. Suppose that $S(\alpha) \gg \Pi^{n-k}$ for some positive real number k. For each $i \in \{1, ..., m\}$, if

$$n > \frac{2k\gamma_i\gamma}{\theta} \tag{13}$$

then there exists an integer $q_{ii} \ge 1$ satisfying

 $q_{ii} \ll P_i^{\theta}$ and $||q_{ii}\alpha_{ii}|| \le P_i^{-2+\theta}$.

Proof. Fix $i \in \{1, \ldots, m\}$. Then

$$|S(\boldsymbol{\alpha})| \leq \sum_{|\mathbf{x}_1| \leq P_1} \cdots \sum_{|\mathbf{x}_{i-1}| \leq P_{i-1}} \sum_{|\mathbf{x}_{i+1}| \leq P_{i+1}} \cdots \sum_{|\mathbf{x}_m| \leq P_m} |T_i(\boldsymbol{\alpha})|,$$
(14)

where

$$T_{i}(\boldsymbol{\alpha}) = T_{i}(\boldsymbol{\alpha}; \mathbf{x}_{1}, \dots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \dots, \mathbf{x}_{m}) := \sum_{|\mathbf{x}_{i}| \le P_{i}} e\left(\sum_{j=1}^{m} \alpha_{ij} \mathbf{x}_{i}^{\mathrm{T}} A \mathbf{x}_{j}\right)$$
(15)

and, for ease of notation, we let $\alpha_{ij} = \alpha_{ji}$ if i > j. By squaring and differencing, it is clear that if we put $\mathbf{z} = \tilde{\mathbf{x}}_i - \mathbf{x}_i$ then

$$|T_{i}(\boldsymbol{\alpha})|^{2} = \sum_{|\mathbf{x}_{i}| \leq P_{i}} \sum_{\substack{|\tilde{\mathbf{x}}_{i}| \leq P_{i} \\ j \neq i}} e\left(\sum_{\substack{j=1\\j \neq i}}^{m} \alpha_{ij} (\tilde{\mathbf{x}}_{i}^{\mathrm{T}} - \mathbf{x}_{i}^{\mathrm{T}}) A \mathbf{x}_{j} + \alpha_{ii} (\tilde{\mathbf{x}}_{i}^{\mathrm{T}} A \tilde{\mathbf{x}}_{i} - \mathbf{x}_{i}^{\mathrm{T}} A \mathbf{x}_{i})\right)$$
$$= \sum_{|\mathbf{z}| \leq 2P_{i}} \sum_{\substack{|\mathbf{x}_{i}| \leq P_{i}:\\|\mathbf{z} + \mathbf{x}_{i}| \leq P_{i}}} e\left(\sum_{\substack{j=1\\j \neq i}}^{m} \alpha_{ij} \mathbf{z}^{\mathrm{T}} A \mathbf{x}_{j} + \alpha_{ii} (\mathbf{z}^{\mathrm{T}} A \mathbf{z} + 2\mathbf{x}_{i}^{\mathrm{T}} A \mathbf{z})\right).$$
(16)

In particular,

$$\begin{aligned} |T_i(\boldsymbol{\alpha})|^2 &\leq \sum_{|\mathbf{z}| \leq 2P_i} \left| \sum_{\substack{|\mathbf{x}| \leq P_i: \\ |\mathbf{z} + \mathbf{x}| \leq P_i}} e(2\alpha_{ii}\mathbf{x}^{\mathrm{T}}A\mathbf{z}) \right| \\ &\ll \sum_{|\mathbf{z}| \leq 2P_i} \prod_{u=1}^n \min\{P_i, \|2\alpha_{ii}(A_{u1}z_1 + \dots + A_{un}z_n)\|^{-1}\} \end{aligned}$$

uniformly in $\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_m$. Let

 $N(\alpha_{ii}, P_i) := #\{\mathbf{z} \in \mathbb{Z}^n : |\mathbf{z}| \le P_i \text{ and }$

$$\|2\alpha_{ii}(A_{u1}z_1 + \dots + A_{un}z_n)\| \le P_i^{-1} \ (1 \le u \le n)\}.$$

Then, by standard techniques (see e.g. the proof of [4, Lemma 13.2]), for any $\varepsilon > 0$ we have

$$|T_i(\boldsymbol{\alpha})|^2 \ll N(\alpha_{ii}, P_i) P_i^{n+\varepsilon}.$$

For any real number θ with $0 < \theta < 1$, define

$$M(\alpha_{ii}, P_i^{\theta}) := \#\{\mathbf{z} \in \mathbb{Z}^n : |\mathbf{z}| \le P_i^{\theta} \text{ and} \\ \|2\alpha_{ii}(A_{u1}z_1 + \dots + A_{un}z_n)\| \le P_i^{-2+\theta} \ (1 \le u \le n)\}.$$

Then, by a standard argument using [4, Lemma 12.6], we have

$$M(\alpha_{ii}, P_i^{\theta}) \gg P_i^{n\theta-n} N(\alpha_{ii}, P_i)$$

as in the proof of [4, Lemma 13.3]. Therefore,

$$|T_i(\boldsymbol{\alpha})|^2 \ll P_i^{2n-n\theta+\varepsilon} M(\alpha_{ii}, P_i^{\theta})$$

and hence, by (14), we conclude that

$$S(\boldsymbol{\alpha}) \ll \Pi^n P_i^{-n\theta/2+\varepsilon} M(\alpha_{ii}, P_i^{\theta})^{1/2}.$$

Suppose that $S(\alpha) \gg \Pi^{n-k}$ for some positive real number *k*. Then

$$\Pi^{n-k} \ll S(\boldsymbol{\alpha}) \ll \Pi^n P_i^{-n\theta/2+\varepsilon} M(\alpha_{ii}, P_i^{\theta})^{1/2}$$

and thus, using (11), we obtain

$$M(\alpha_{ii}, P_i^{\theta}) \gg \Pi^{-2k} P_i^{n\theta - \varepsilon}$$
$$= P_i^{-2k\gamma_i \gamma + n\theta - \varepsilon}.$$

Our assumption (13) implies that this exponent is strictly positive for small enough ε , so it follows that $M(\alpha_{ii}, P_i^{\theta}) \ge 2$. Hence there exists some $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{z} \neq \mathbf{0}$ and

$$|\mathbf{z}| \leq P_i^{\theta}, \quad ||2\alpha_{ii}(A_{u1}z_1 + \dots + A_{un}z_n)|| \leq P_i^{-2+\theta} \quad (1 \leq u \leq n).$$

Now, since z is nonzero and our matrix A is nonsingular, we have

$$A_{u1}z_1 + \dots + A_{un}z_n \neq 0$$

for some $u \in \{1, ..., n\}$. For this u, define $q_i = 2|A_{u1}z_1 + \cdots + A_{un}z_n| \neq 0$. Then $1 \leq q_i \ll P_i^{\theta}$ and $||q_i \alpha_{ii}|| \leq P_i^{-2+\theta}$.

We deal with the remaining α_{ij} $(i \neq j)$ in the following lemma, whose proof is along the lines of that for [13, Lemma 4.1].

LEMMA 2.2. Let δ be a real number satisfying $0 < \delta \leq 1/\gamma$, and suppose that $S(\alpha) \gg \prod^{n-k}$ for some positive real number k. For fixed i, j satisfying $1 \leq i < j \leq m$, suppose

$$n > 2k\gamma_i\gamma. \tag{17}$$

Then there exists an integer $q_{ij} \ge 1$ such that

$$q_{ij} \ll \Pi^{2k/n+\delta}$$
 and $||q_{ij}\alpha_{ij}|| \leq \Pi^{2k/n+\delta} (P_i P_j)^{-1}$

Proof. Fix $i, j \in \{1, ..., m\}$ such that $1 \le i < j \le m$. By an application of the Cauchy–Schwarz inequality, we have

$$|S(\boldsymbol{\alpha})|^2 \le (\Pi P_i^{-1})^n \sum_{\substack{|\mathbf{x}_t| \le P_t \\ (1 \le t \le m, t \ne i, j)}} \sum_{\substack{|\mathbf{x}_j| \le P_j}} |T_i(\boldsymbol{\alpha})|^2,$$
(18)

where $T_i(\alpha)$ is as defined in (15). Now (16) gives

$$\sum_{|\mathbf{x}_{j}| \leq P_{j}} |T_{i}(\boldsymbol{\alpha})|^{2} \leq \sum_{|\mathbf{y}| \leq P_{i}} \sum_{\substack{|\mathbf{h}| \leq 2P_{i}: \\ |\mathbf{y}+\mathbf{h}| \leq P_{i}}} \left| \sum_{\substack{|\mathbf{x}_{j}| \leq P_{j} \\ |\mathbf{y}+\mathbf{h}| \leq P_{i}}} min\{P_{j}, \|\alpha_{ij}(A_{u1}h_{1} + \dots + A_{un}h_{n})\|^{-1} \right\}$$
$$\ll (P_{i})^{n} \sum_{|\mathbf{h}| \leq 2P_{i}} \prod_{u=1}^{n} min\{P_{j}, \|\alpha_{ij}(A_{u1}h_{1} + \dots + A_{un}h_{n})\|^{-1} \}.$$
(19)

Let

$$z_u = A_{u1}h_1 + \dots + A_{un}h_n$$

for each $u \in \{1, \ldots, n\}$, and set

$$\lambda := 2nP_i \max_{1 \le r, \, s \le n} |A_{rs}|.$$

Note that

 $P_i \ll \lambda \ll P_i$.

Then, since A is a nonsingular matrix, we have

$$\sum_{\|\mathbf{h}\| \le 2P_i} \prod_{u=1}^n \min\{P_j, \|\alpha_{ij}(A_{u1}h_1 + \dots + A_{un}h_n)\|^{-1}\}$$

$$\ll \sum_{\|\mathbf{z}\| \le \lambda} \prod_{u=1}^n \min\{P_j, \|\alpha_{ij}z_u\|^{-1}\}$$

$$= \left(\sum_{\|z\| \le \lambda} \min\{P_j, \|\alpha_{ij}z\|^{-1}\}\right)^n.$$

Combining (18) and (19) yields

$$|S(\boldsymbol{\alpha})|^{2} \ll \Pi^{2n} (P_{i}P_{j})^{-n} \left(P_{j} + \sum_{1 \le z \le \lambda} \min\{P_{j}, \|\alpha_{ij}z\|^{-1}\}\right)^{n}$$
$$\ll \Pi^{2n} \left(P_{i}^{-n} + \left(\frac{1}{q} + \frac{1}{P_{j}} + \frac{q}{P_{i}P_{j}}\right)^{n} (\log 2P_{i}q)^{n}\right)$$

upon applying [18, Lemma 2.2], provided that $|\alpha_{ij} - a/q| \le q^{-2}$ for coprime integers a, q with $q \ge 1$.

Let δ be a positive real number with $0 < \delta \le 1/\gamma$. Then we can use (5), (10), and (11) to show that

$$P_i P_j \Pi^{-2k/n-\delta} = P_j^{1+\gamma_j/\gamma_i - 2k\gamma_j\gamma/n - \delta\gamma_j\gamma} > 1$$

by virtue of the inequality $\gamma_i \ge \gamma_j$ and (17). By Dirichlet's theorem, there exist coprime integers q_{ij} and *a* satisfying

$$1 \le q_{ij} \le P_i P_j \Pi^{-2k/n-\delta}$$
 and $|q_{ij}\alpha_{ij} - a| \le (P_i P_j)^{-1} \Pi^{2k/n+\delta}$.

Therefore,

$$S(\boldsymbol{\alpha}) \ll \Pi^{n+\varepsilon} \left(P_i^{-n/2} + \left(\frac{1}{q_{ij}} + \frac{1}{P_j} + \frac{q_{ij}}{P_i P_j} \right)^{n/2} \right).$$

Now

$$\Pi^{n+\varepsilon} P_j^{-n/2} \ll \Pi^{n-k}$$

provided that $P_j \gg \Pi^{2k/n+\varepsilon}$. For sufficiently small ε , this follows from (17) because

$$\Pi^{2k/n+\varepsilon} = P_j^{2k\gamma_j\gamma/n+\varepsilon}$$

by (11). Analogously, we get

$$\Pi^{n+\varepsilon} P_i^{-n/2} \ll \Pi^{n-k}.$$

Since $q_{ij} \leq P_i P_j \Pi^{-2k/n-\delta}$, it follows that

$$\Pi^{n+\varepsilon} \left(\frac{q_{ij}}{P_i P_j}\right)^{n/2} \ll \Pi^{n-k}$$

provided $\varepsilon > 0$ is small enough compared with δ . Therefore,

$$S(\boldsymbol{\alpha}) \ll \frac{\Pi^{n+\varepsilon}}{q_{ij}^{n/2}} + \Pi^{n-k}.$$

If $q_{ij} \gg \Pi^{2k/n+\delta}$ then $S(\boldsymbol{\alpha}) \ll \Pi^{n-k}$ for sufficiently small $\varepsilon > 0$, which contradicts the hypothesis of the lemma. Hence $q_{ij} \ll \Pi^{2k/n+\delta}$.

Combining Lemmas 2.1 and 2.2 gives the following Weyl-type inequality for our exponential sum $S(\alpha)$.

LEMMA 2.3. Let $0 < \theta < 1$ and k > 0. Assume that

$$n > \frac{2k\gamma}{\theta}.$$
 (20)

Then either (i) we have

 $S(\boldsymbol{\alpha}) \ll \Pi^{n-k}$

or (ii) there exist integers q and a_{ij} $(1 \le i \le j \le m)$ that are coprime (i.e., $(q, \mathbf{a}) = (q, a_{11}, a_{12}, \dots, a_{mm}) = 1)$ such that

$$1 \le q \ll \Pi^{\theta(1+m(m-1)/2\gamma)},$$

$$|q\alpha_{ij} - a_{ij}| \ll \Pi^{\theta(1+m(m-1)/2\gamma)} (P_i P_j)^{-1} \quad (1 \le i \le j \le m).$$
(21)

Proof. Suppose that (i) does not hold. Since (20) implies (13) and (17) for all $i, j \in \{1, ..., m\}$, we may apply Lemmas 2.1 and 2.2 to show that there exist integers q_{ij} and b_{ij} $(1 \le i \le j \le m)$ satisfying

$$(q_{ij}, b_{ij}) = 1,$$

$$q_{ii} \ll P_i^{\theta}, \qquad |q_{ii}\alpha_{ii} - b_{ii}| \le P_i^{\theta - 2},$$

$$q_{ij} \ll \Pi^{2k/n+\delta}, \quad |q_{ij}\alpha_{ij} - b_{ij}| \le \Pi^{2k/n+\delta} (P_i P_j)^{-1} \ (1 \le i < j \le m)$$

whenever $0 < \delta \le 1/\gamma$. The condition (20) implies that

$$\frac{2k}{n} + \delta < \frac{\theta}{\gamma}$$

provided we choose δ to be a sufficiently small positive real number.

Define q to be the least common multiple of the q_{ij} $(1 \le i \le j \le m)$, and set $a_{ij} := qb_{ij}/q_{ij}$. Then q and the a_{ij} are coprime: Let p be a prime dividing q, and let p^r be the maximum power of p dividing at least one of the q_{ij} . By definition

of q, we have $r \ge 1$. It follows that, if $p^r \parallel q_{ij}$, then p does not divide q/q_{ij} . Since $(q_{ij}, b_{ij}) = 1$, neither does p divide b_{ij} , whence p does not divide a_{ij} . Moreover,

$$q \leq \prod_{r=1}^{m} q_{rr} \prod_{1 \leq s < t \leq m} q_{st} \ll \Pi^{\theta(1+m(m-1)/2\gamma)},$$

$$\frac{q}{q_{ii}} \ll (\Pi P_i^{-1})^{\theta} \Pi^{\theta m(m-1)/2\gamma} \quad (1 \leq i \leq m),$$

$$\frac{q}{q_{ij}} \ll \Pi^{\theta} \Pi^{(\theta/\gamma)(m(m-1)/2-1)} \quad (1 \leq i < j \leq m)$$

Therefore,

$$\begin{aligned} |q\alpha_{ii} - a_{ii}| &= \frac{q}{q_{ii}} |q_{ii}\alpha_{ii} - b_{ii}| \ll \frac{q}{q_{ii}} P_i^{\theta - 2} \\ &\ll \Pi^{\theta(1 + m(m-1)/2\gamma)} P_i^{-2} \quad (1 \le i \le m), \\ |q\alpha_{ij} - a_{ij}| &= \frac{q}{q_{ij}} |q_{ij}\alpha_{ij} - b_{ij}| \ll \frac{q}{q_{ij}} \Pi^{\theta/\gamma} (P_i P_j)^{-1} \\ &\ll \Pi^{\theta(1 + m(m-1)/2\gamma)} (P_i P_j)^{-1} \quad (1 \le i < j \le m); \end{aligned}$$

hence the bound (21) holds for all $i, j \in \{1, ..., m\}$ such that $i \leq j$.

3. Minor Arcs

We are now in a position to set up the scene for an application of the circle method: splitting the α into two subsets, where either $S(\alpha)$ is small or each α_{ij} is well approximated.

For coprime integers q, $\mathbf{a} := a_{ij}$ $(1 \le i \le j \le m)$, and $\Delta > 0$, define the major arc

$$\mathfrak{M}_{\mathbf{a},q}(\Delta) := \{ \boldsymbol{\alpha} \in [0,1)^R : |q\alpha_{ij} - a_{ij}| \ll \Pi^{\Delta} (P_i P_j)^{-1} \ (1 \le i \le j \le m) \}.$$
(22)

Next, define the major arcs $\mathfrak{M}(\Delta)$ as the union of the $\mathfrak{M}_{\mathbf{a},q}(\Delta)$ over all coprime integers q, \mathbf{a} such that $1 \leq q \ll \Pi^{\Delta}$ and $1 \leq a_{ij} < q$ $(1 \leq i \leq j \leq m)$. We denote the minor arcs by $\mathfrak{m}(\Delta) := [0, 1)^R \setminus \mathfrak{M}(\Delta)$.

We may split the integral in (12) to see that

$$N(A, B) = \int_{\mathfrak{M}(\Delta)} S(\boldsymbol{\alpha}, \mathbf{b}) \, d\boldsymbol{\alpha} + \int_{\mathfrak{m}(\Delta)} S(\boldsymbol{\alpha}, \mathbf{b}) \, d\boldsymbol{\alpha}.$$
 (23)

We shall use the following corollary of Lemma 2.3 to show that the latter integral does not contribute to the main term of the asymptotic formula for N(A, B).

LEMMA 3.1. Let $\varepsilon > 0$ and $0 < \Delta < \frac{2\gamma + m(m-1)}{2\gamma}$ be real numbers. Then either: (i) the bound $S(\alpha) \ll \Pi^{n-n\Delta/(2\gamma+m(m-1))+\varepsilon}$ holds; or (ii) $\alpha \in \mathfrak{M}(\Delta)$.

Proof. The claim follows from taking $k = n\theta/2\gamma - \varepsilon$ in Lemma 2.3 for $\theta = \frac{2\gamma\Delta}{2\gamma+m(m-1)}$ and then noting that (20) is therefore satisfied.

LEMMA 3.2. Suppose that $n > (2\gamma + m(m-1))(R+1)$. Then, for any $0 < \Delta < \frac{m+1}{R+1}$, we have

$$\int_{\mathfrak{m}(\Delta)} S(\boldsymbol{\alpha}, \mathbf{b}) \, d\boldsymbol{\alpha} \ll \Pi^{n-m-1-\delta}$$

for some $\delta > 0$.

Proof. We follow the method of Davenport and Birch (see e.g. [1, Sec. 4]). Let $\delta > 0$ be a real number satisfying

$$\frac{n}{2\gamma + m(m-1)} - (R+1) > \frac{2\delta}{\Delta},\tag{24}$$

whose existence is guaranteed by the condition on *n*. We shall define a sequence $\Delta_0, \Delta_1, \dots, \Delta_T$ such that

$$0 < \Delta = \Delta_0 < \Delta_1 < \dots < \Delta_T = \frac{m+1}{R+1}$$
$$\Delta_{t+1} - \Delta_t < \frac{\delta}{R+1}$$
(25)

for each $0 \le t \le T - 1$. Note that

$$\mathfrak{m}(\Delta) = \mathfrak{m}(\Delta_T) \cup (\mathfrak{M}(\Delta_T) \setminus \mathfrak{M}(\Delta_{T-1})) \cup \cdots \cup (\mathfrak{M}(\Delta_1) \setminus \mathfrak{M}(\Delta_0)).$$
(26)

By Lemma 3.1, for any $\varepsilon > 0$ we have

$$\int_{\mathfrak{m}(\Delta_T)} |S(\boldsymbol{\alpha}, \mathbf{b})| \, d\boldsymbol{\alpha} = \int_{\mathfrak{m}(\Delta_T)} |S(\boldsymbol{\alpha})| \, d\boldsymbol{\alpha}$$
$$\ll \Pi^{n-n\Delta_T/(2\gamma+m(m-1))+\varepsilon}$$
$$< \Pi^{n-\Delta_T(R+1+2\delta/\Delta)+\varepsilon}$$
$$< \Pi^{n-m-1-2\delta+\varepsilon}$$

by (24) and the inequality $\Delta < \Delta_T$. Therefore,

$$\int_{\mathfrak{m}(\Delta_T)} |S(\boldsymbol{\alpha})| \, d\boldsymbol{\alpha} \ll \Pi^{n-m-1-\delta}$$

provided ε is small enough.

For $0 \le t \le T - 1$, we have $\mathfrak{M}(\Delta_{t+1}) \setminus \mathfrak{M}(\Delta_t) \subset \mathfrak{M}(\Delta_{t+1})$ and hence the measure of $\mathfrak{M}(\Delta_{t+1}) \setminus \mathfrak{M}(\Delta_t)$ is bounded by

$$\sum_{q \ll \Pi^{\Delta_{t+1}}} \sum_{\mathbf{a} \pmod{q}} \prod_{1 \le i \le j \le m} (q^{-1} \Pi^{\Delta_{t+1}} (P_i P_j)^{-1}) \\ \ll \sum_{q \ll \Pi^{\Delta_{t+1}}} \sum_{\mathbf{a} \pmod{q}} q^{-R} \Pi^{R \Delta_{t+1}} \Pi^{-(m+1)} \\ \ll \Pi^{\Delta_{t+1}(R+1)-m-1}.$$

We may therefore use Lemma 3.1 and (25) to show that, for sufficiently small $\varepsilon > 0$,

878

and

$$\int_{\mathfrak{M}(\Delta_{t+1})\backslash\mathfrak{M}(\Delta_{t})} |S(\boldsymbol{\alpha}, \mathbf{b})| d\boldsymbol{\alpha} = \int_{\mathfrak{M}(\Delta_{t+1})\backslash\mathfrak{M}(\Delta_{t})} |S(\boldsymbol{\alpha})| d\boldsymbol{\alpha}$$
$$\ll \Pi^{n-n\Delta_{t}/\Gamma+\Delta_{t+1}(R+1)-m-1+\varepsilon}$$
$$< \Pi^{n-m-1-\Delta_{t}(n/\Gamma-(R+1))+\delta+\varepsilon}$$

where for ease of notation we have put $\Gamma = 2\gamma + m(m-1)$. Now $\Delta \leq \Delta_t$ and (24) yield

$$\int_{\mathfrak{M}(\Delta_{t+1})\backslash\mathfrak{M}(\Delta_{t})} |S(\boldsymbol{\alpha})| \, d\boldsymbol{\alpha} \ll \Pi^{n-m-1-\delta}.$$

Given (26), this completes the proof after noting that $T \ll 1$.

4. Major Arcs

In dealing with the major arcs, we shall find it more convenient to enlarge the sets $\mathfrak{M}_{\mathbf{a},q}(\Delta)$ slightly. So let $\mathfrak{M}'_{\mathbf{a},q}(\Delta)$ denote the set in (22) but instead with the inequality

$$|q\alpha_{ij} - a_{ij}| \ll q \Pi^{\Delta} (P_i P_j)^{-1} \quad (1 \le i \le j \le m),$$

and let $\mathfrak{M}'(\Delta)$ denote the corresponding union.

It follows from (23) and Lemma 3.2 that, provided

$$n > (2\gamma + m(m-1))(R+1) \quad \text{and} \quad 0 < \Delta < \frac{m+1}{R+1},$$

we have

$$N(A, B) = \int_{\mathfrak{M}'(\Delta)} S(\boldsymbol{\alpha}, \mathbf{b}) \, d\boldsymbol{\alpha} + O(\Pi^{n-m-1-\delta}) \tag{27}$$

for some $\delta > 0$.

LEMMA 4.1. Suppose that $0 < \Delta < 2/3\gamma$. Then, for sufficiently large P_1 , the major arcs $\mathfrak{M}'_{\mathbf{a},q}(\Delta)$ are disjoint. Similarly, if $0 < \Delta < 1/\gamma$ then, for sufficiently large P_1 , the $\mathfrak{M}_{\mathbf{a},q}(\Delta)$ are disjoint.

Proof. Suppose there exists an α lying in the intersection of two different sets of the form $\mathfrak{M}'_{\mathbf{a},q}(\Delta)$. Then, for some i, j with $1 \le i \le j \le m$, there exist integers a_{ij}, a'_{ij}, q, q' with $a_{ij}q' \ne a'_{ij}q$ that satisfy

$$q, q' \ll \Pi^{\Delta},$$

 $|q lpha_{ij} - a_{ij}| \ll q \Pi^{\Delta} (P_i P_j)^{-1},$
 $|q' lpha_{ij} - a'_{ij}| \ll q' \Pi^{\Delta} (P_i P_j)^{-1}.$

We can therefore use (10), (11), and $\gamma_1 = 1$ to show that

$$\begin{split} 1 &\leq |a_{ij}q' - a'_{ij}q| = |q'(a_{ij} - q\alpha_{ij}) + q(q'\alpha_{ij} - a'_{ij})| \\ &\leq q'|q\alpha_{ij} - a_{ij}| + q|q'\alpha_{ij} - a'_{ij}| \\ &\ll \Pi^{3\Delta}(P_iP_j)^{-1} \\ &= P_1^{3\gamma\Delta - 1/\gamma_i - 1/\gamma_j}. \end{split}$$

This expression contradicts our assumption on Δ when one considers that $1/\gamma_i + 1/\gamma_j \ge 2$. The proof of the second statement is completely analogous. \Box

Whenever $\boldsymbol{\alpha} \in \mathfrak{M}'_{\mathbf{a},q}(\Delta)$, for each $1 \leq i \leq j \leq m$ we may write

$$\alpha_{ij} = \frac{a_{ij}}{q} + \beta_{ij}, \quad |\beta_{ij}| \ll \Pi^{\Delta} (P_i P_j)^{-1}, \tag{28}$$

for suitable integers a_{ij} and $1 \le q \ll \Pi^{\Delta}$. Define

$$S_{\mathbf{a},q}(\mathbf{b}) := \sum_{\mathbf{z}_1 \bmod q} \cdots \sum_{\mathbf{z}_m \bmod q} e_q \bigg(\sum_{1 \le i \le j \le m} a_{ij} (\mathbf{z}_i^{\mathsf{T}} A \mathbf{z}_j - B_{ij}) \bigg),$$

and let $S_{\mathbf{a},q} := S_{\mathbf{a},q}(\mathbf{0})$. Also, define

$$I(\mathbf{P},\boldsymbol{\beta}) := \int_{[-1,1]^{mn}} e\left(\sum_{1 \le i \le j \le m} P_i P_j \beta_{ij} \mathbf{v}_i^{\mathrm{T}} A \mathbf{v}_j\right) d\mathbf{v}_1 \cdots d\mathbf{v}_m$$

and let

$$I(\boldsymbol{\beta}) := I((1,\ldots,1),\boldsymbol{\beta}).$$

LEMMA 4.2. Suppose that (28) holds for $\boldsymbol{\alpha} \in \mathfrak{M}'_{\mathbf{a},q}(\Delta)$. Then

$$S(\boldsymbol{\alpha}, \mathbf{b}) = q^{-mn} \Pi^n S_{\mathbf{a}, q}(\mathbf{b}) I(\mathbf{P}, \boldsymbol{\beta}) e\left(-\sum_{1 \le i \le j \le m} \beta_{ij} B_{ij}\right) + O(\Pi^{n+2\Delta} P_1^{-1}).$$

Proof. By (28) we have

 $S(\boldsymbol{\alpha}, \mathbf{b})$

$$=\sum_{|\mathbf{x}_1|\leq P_1}\cdots\sum_{|\mathbf{x}_m|\leq P_m}e_q\bigg(\sum_{1\leq i\leq j\leq m}a_{ij}(\mathbf{x}_i^{\mathrm{T}}A\mathbf{x}_j-B_{ij})\bigg)e\bigg(\sum_{1\leq i\leq j\leq m}\beta_{ij}(\mathbf{x}_i^{\mathrm{T}}A\mathbf{x}_j-B_{ij})\bigg).$$

Letting $\mathbf{x}_i = \mathbf{z}_i + q \mathbf{y}_i \ (1 \le i \le m)$, we obtain

$$S(\boldsymbol{\alpha}, \mathbf{b}) = \sum_{\mathbf{z}_1, \dots, \mathbf{z}_m \pmod{q}} e_q \left(\sum_{1 \le i \le j \le m} a_{ij} (\mathbf{z}_i^{\mathrm{T}} A \mathbf{z}_j - B_{ij}) \right) \\ \times \sum_{\mathbf{y}_1, \dots, \mathbf{y}_m} e \left(\sum_{1 \le i \le j \le m} \beta_{ij} ((\mathbf{z}_i + q \mathbf{y}_i)^{\mathrm{T}} A(\mathbf{z}_j + q \mathbf{y}_j) - B_{ij}) \right),$$

where the sum over $\mathbf{y}_1, \ldots, \mathbf{y}_m \in \mathbb{Z}^n$ is such that $|\mathbf{z}_i + q\mathbf{y}_i| \le P_i$ for $1 \le i \le m$.

It follows from Iwaniec and Kowalski [10, Lemma 4.1] and a simple induction argument that the sum

$$\sum_{\mathbf{y}_1,\ldots,\mathbf{y}_m} e\left(\sum_{1\leq i\leq j\leq m} \beta_{ij} (\mathbf{z}_i + q\mathbf{y}_i)^{\mathrm{T}} A(\mathbf{z}_j + q\mathbf{y}_j)\right)$$

may be replaced by the integral

$$\int_{\substack{\mathbf{y}_1,\ldots,\mathbf{y}_m\in\mathbb{R}^n:\\|\mathbf{z}_i+q\mathbf{y}_i|\leq P_i}} \beta_{ij}(\mathbf{z}_i+q\mathbf{y}_i)^{\mathrm{T}}A(\mathbf{z}_j+q\mathbf{y}_j) d\mathbf{y}_1\cdots d\mathbf{y}_m$$
(29)

with error

$$\ll \max_{\substack{1 \le s \le m \\ 1 \le t \le n}} \left| \frac{\partial}{\partial y_{st}} e \left(\sum_{1 \le i \le j \le m} \beta_{ij} (\mathbf{z}_i + q \mathbf{y}_i)^{\mathrm{T}} A(\mathbf{z}_j + q \mathbf{y}_j) \right) \right| \frac{\Pi^n}{q^{mn}} + \frac{\Pi^n}{q^{mn-1} P_1}.$$

For any $1 \le s \le m$ and $1 \le t \le n$, after substituting $\mathbf{u}_i = \mathbf{z}_i + q\mathbf{y}_i$ we find that

$$\frac{\partial}{\partial \mathbf{y}_s} \sum_{1 \le i \le j \le m} \beta_{ij} (\mathbf{z}_i + q\mathbf{y}_i)^{\mathrm{T}} A(\mathbf{z}_j + q\mathbf{y}_j)$$

= $q \frac{\partial}{\partial \mathbf{u}_s} \sum_{1 \le i \le j \le m} \beta_{ij} \mathbf{u}_i^{\mathrm{T}} A \mathbf{u}_j$
= $q \left(2\beta_{ss} A \mathbf{u}_s + \sum_{1 \le i < s} \beta_{is} A \mathbf{u}_i + \sum_{s < j \le m} \beta_{sj} A \mathbf{u}_j \right),$

whence (28) and $|\mathbf{u}_i| \le P_i$ $(1 \le i \le m)$ yield

$$\frac{\partial}{\partial y_{st}} e \left(\sum_{1 \le i \le j \le m} \beta_{ij} (\mathbf{z}_i + q\mathbf{y}_i)^{\mathrm{T}} A(\mathbf{z}_j + q\mathbf{y}_j) \right) \\ \ll q \left(\sum_{1 \le i \le s} |\beta_{is}| P_i + \sum_{s < j \le m} |\beta_{sj}| P_j \right) \\ \ll q \Pi^{\Delta} P_s^{-1};$$

therefore, the difference between the sum and the integral is equal to

$$O\left(\frac{\Pi^{n+\Delta}}{q^{mn-1}P_1}\right).$$

Making the change of variables $\mathbf{v}_i = P_i^{-1}(\mathbf{z}_i + q\mathbf{y}_i)$ $(1 \le i \le m)$ in (29), we see that

$$\int_{\substack{\mathbf{y}_1,\ldots,\mathbf{y}_m\in\mathbb{R}^n:\\|\mathbf{z}_i+q\mathbf{y}_i|\leq P_i}} \int_{\substack{1\leq i\leq j\leq m}} \beta_{ij}(\mathbf{z}_i+q\mathbf{y}_i)^{\mathrm{T}}A(\mathbf{z}_j+q\mathbf{y}_j) d\mathbf{y}_1\cdots d\mathbf{y}_m = q^{-mn}\Pi^n I(\mathbf{P},\boldsymbol{\beta}).$$

The lemma now follows easily after using the trivial bound $|S_{\mathbf{a},q}(\mathbf{b})| \le q^{mn}$ and noting that $q \ll \Pi^{\Delta}$.

For $Q \ge 1$, we now define

$$\mathfrak{S}(Q; \mathbf{b}) := \sum_{q \ll Q} q^{-mn} \sum_{\substack{\mathbf{a} \bmod q \\ (\mathbf{a}, q) = 1}} S_{\mathbf{a}, q}(\mathbf{b})$$
(30)

and

$$\Im(Q; \mathbf{c}) := \int_{|\boldsymbol{\eta}| \ll Q} I(\boldsymbol{\eta}) e\left(-\sum_{1 \le i \le j \le m} \eta_{ij} c_{ij}\right) d\boldsymbol{\eta}$$
(31)

for $\mathbf{c} = (c_{ij})_{1 \le i \le j \le m} \in \mathbb{R}^R$.

LEMMA 4.3. Let $0 < \Delta < 1/\gamma (2R + 3)$. Then there exists a $\delta > 0$ such that $N(A, B) = \Pi^{n-m-1} \mathfrak{S}(\Pi^{\Delta}; \mathbf{b}) \mathfrak{I}(\Pi^{\Delta}; \mathbf{c}) + O(\Pi^{n-m-1-\delta}),$

where $c_{ij} = (P_i P_j)^{-1} B_{ij}$ for $1 \le i \le j \le m$.

Proof. By our assumption on Δ together with (27) and Lemma 4.1, for some $\delta > 0$ we have

$$N(A, B) = \int_{\mathfrak{M}'(\Delta)} S(\boldsymbol{\alpha}, \mathbf{b}) d\boldsymbol{\alpha} + O(\Pi^{n-m-1-\delta})$$

= $\sum_{q \ll \Pi^{\Delta}} \sum_{\substack{\mathbf{a} \mod q \\ (\mathbf{a}, q) = 1}} \int_{\mathfrak{M}'_{\mathbf{a}, q}(\Delta)} S(\boldsymbol{\alpha}, \mathbf{b}) d\boldsymbol{\alpha} + O(\Pi^{n-m-1-\delta}).$

We shall use Lemma 4.2 to approximate $S(\boldsymbol{\alpha}, \mathbf{b})$ on $\mathfrak{M}'_{\mathbf{a},q}(\Delta)$. The error term, when integrated over $\mathfrak{M}'(\Delta)$, is bounded by a value

$$\ll \sum_{q \ll \Pi^{\Delta}} \sum_{\substack{\mathbf{a} \bmod q \\ (\mathbf{a},q)=1}} \int_{|\beta_{ij}| \ll \Pi^{\Delta}(P_i P_j)^{-1}} \Pi^{n+2\Delta} P_1^{-1} d\boldsymbol{\beta}$$
$$\ll \sum_{q \ll \Pi^{\Delta}} \sum_{\substack{\mathbf{a} \bmod q \\ (\mathbf{a},q)=1}} \Pi^{n+2\Delta+R\Delta-(m+1)} P_1^{-1}$$
$$\ll \Pi^{n-m-1+\Delta(2R+3)} P_1^{-1}$$
$$\ll \Pi^{n-m-1-\delta'}$$

for some $\delta' > 0$; this claim follows from (11), the equality $\gamma_1 = 1$, and our assumption on Δ . This bound $O(\Pi^{n-m-1-\delta'})$ contributes to the error term in the lemma. The main term gives

$$N(A,B) = \Pi^{n} \mathfrak{S}(\Pi^{\Delta}; \mathbf{b}) \int_{\boldsymbol{\beta}} I(\mathbf{P}, \boldsymbol{\beta}) e\left(-\sum_{1 \leq i \leq j \leq m} \beta_{ij} B_{ij}\right) d\boldsymbol{\beta},$$

where the integral is over $|\beta_{ij}| \ll \Pi^{\Delta}(P_i P_j)^{-1}$ $(1 \le i \le j \le m)$. Now substituting $\eta_{ij} = P_i P_j \beta_{ij}$ completes the proof of the lemma.

Let

$$\mathfrak{S}(\mathbf{b}) := \mathfrak{S}(\infty; \mathbf{b})$$

be the singular series and let

$$\mathfrak{I}(\mathbf{c}) := \mathfrak{I}(\infty; \mathbf{c})$$

be the singular integral, with **c** as in Lemma 4.3.

LEMMA 4.4. Assume that $n > (2\gamma + m(m-1))(R+1)$. Then $\mathfrak{S}(\mathbf{b})$ is absolutely convergent. Moreover, for some $\delta > 0$, we have

$$|\mathfrak{S}(\mathbf{b}) - \mathfrak{S}(\Pi^{\Delta}; \mathbf{b})| \ll \Pi^{-2\delta + \varepsilon}$$

uniformly in **b**.

Proof. Let $(q, \mathbf{a}) = 1$. We may use Lemma 3.1 (with $P_1 = \cdots = P_m = q, \gamma = m$, and $\alpha_{ij} = a_{ij}/q$ for $1 \le i \le j \le m$) to see that either

$$|S_{\mathbf{a},q}(\mathbf{b})| \ll q^{mn-n\Delta/(m+1)+\varepsilon}$$
(32)

or $(a_{ij}/q)_{1 \le i \le j \le m} \in \mathfrak{M}(\Delta)$ for any $0 < \Delta < (m+1)/2$. According to the latter, there exist coprime integers q' and $(a'_{ij})_{1 \le i \le j \le m}$ that satisfy

$$q' \ll q^{m\Delta}, \quad |q'a_{ij} - qa'_{ij}| \ll q^{m\Delta - 1} \ (1 \le i \le j \le m).$$

Since $(q, \mathbf{a}) = 1$, these conditions are clearly impossible to satisfy if $\Delta < 1/m$ and so (32) must hold. Setting $\Delta = 1/m - \varepsilon$ for any $\varepsilon > 0$ gives

$$|S_{\mathbf{a},q}(\mathbf{b})| \ll q^{mn-n/2R+\varepsilon}.$$
(33)

Therefore,

$$\sum_{q=1}^{\infty} q^{-mn} \sum_{\substack{\mathbf{a} \bmod q \\ (\mathbf{a},q)=1}} |S_{\mathbf{a},q}(\mathbf{b})| \ll \sum_{q=1}^{\infty} q^{R-n/2R+\varepsilon} \ll \sum_{q=1}^{\infty} q^{-1-1/2R+\varepsilon} \ll 1;$$

this follows because $n \ge (2\gamma + m(m-1))(R+1) + 1 \ge 2R(R+1) + 1$, which shows that $\mathfrak{S}(\mathbf{b})$ is absolutely convergent.

For the second part of the lemma, let $\delta > 0$ be as in (24). Then we use (33) to obtain

$$\begin{split} |\mathfrak{S}(\mathbf{b}) - \mathfrak{S}(\Pi^{\Delta}; \mathbf{b})| \ll \sum_{q \gg \Pi^{\Delta}} q^{R-n/2R+\varepsilon} \\ \ll \sum_{q \gg \Pi^{\Delta}} q^{R-n/\Gamma+\varepsilon} \\ \ll \sum_{q \gg \Pi^{\Delta}} q^{-2\delta/\Delta - 1+\varepsilon} \\ \ll \Pi^{-2\delta+\varepsilon}, \end{split}$$

where again $\Gamma = 2\gamma + m(m-1)$.

LEMMA 4.5. We have

$$I(\boldsymbol{\eta}) \ll \min\{1, \max|\eta_{ij}|^{-n/2R+\varepsilon}\}.$$

Proof. The first bound is trivial, so we may assume that $\max |\eta_{ii}| > 1$.

Let $P \ge 1$ be a parameter, and define

$$S'(\boldsymbol{\alpha}) := \sum_{|\mathbf{x}_1|,\ldots,|\mathbf{x}_m| \leq P} e\bigg(\sum_{1 \leq i \leq j \leq m} \alpha_{ij} \mathbf{x}_i^{\mathrm{T}} A \mathbf{x}_j\bigg).$$

By following the proof of Lemma 4.2 with q = 1 and $\mathbf{a} = \mathbf{0}$, we get

$$S'(\boldsymbol{\alpha}) = P^{mn} \int_{[-1,1]^{mn}} e\left(P^2 \sum_{1 \le i \le j \le m} \alpha_{ij} \mathbf{v}_i^{\mathrm{T}} A \mathbf{v}_j\right) d\mathbf{v}_1 \cdots d\mathbf{v}_m$$
$$+ O\left(\sum_{1 \le i \le j \le m} |\alpha_{ij}| P^{mn+1} + P^{mn-1}\right).$$

 \square

It is a simple corollary to Lemma 3.1 (see e.g. the corollary to [1, Lemma 4.3]) that, for $\max |\alpha_{ij}| < P^{-1}$, we have

$$S'(\boldsymbol{\alpha}) \ll P^{mn+\varepsilon} (P^2 \max|\alpha_{ij}|)^{-n/2R}.$$
(34)

For if $\max |\alpha_{ij}| \leq P^{-2}$ then the bound is trivial; otherwise, write $\max |\alpha_{ij}| = P^{-2+m\Delta}$ for a suitable $\Delta > 0$. Since $\max |\alpha_{ij}| < P^{-1}$ and since $\gamma = m$ in our situation, it follows that $\Delta < 1/\gamma$. Thus, by Lemma 4.1, the major arcs are disjoint and so α is at the boundary of $\mathfrak{M}(\Delta)$; hence, for any $\varepsilon > 0$, we have $\alpha \notin \mathfrak{M}(\Delta - \varepsilon)$. By Lemma 3.1, then,

$$S'(\boldsymbol{\alpha}) \ll P^{mn(1-(\Delta-\varepsilon)/2R+\varepsilon)} \ll P^{mn+\varepsilon} (P^2 \max\{|\alpha_{ij}|\})^{-n(\Delta-\varepsilon)/2\Delta R}$$

which confirms the bound (34). Therefore, whenever $\max |\alpha_{ij}| < P^{-1}$, we have

$$P^{mn} \int_{[-1,1]^{mn}} e\left(P^2 \sum_{1 \le i \le j \le m} \alpha_{ij} \mathbf{v}_i^{\mathrm{T}} A \mathbf{v}_j\right) d\mathbf{v}_1 \cdots d\mathbf{v}_m$$
$$\ll \left(P^2 \sum_{1 \le i \le j \le m} |\alpha_{ij}| + 1\right) P^{mn-1} + P^{mn+\varepsilon} (P^2 \max |\alpha_{ij}|)^{-n/2R}.$$

Substituting $\eta_{ij} = P^2 \alpha_{ij}$ and noting that the left-hand side of the preceding inequality is just $P^{mn}I(\eta)$, we obtain

$$I(\boldsymbol{\eta}) \ll (\max|\eta_{ij}|+1)P^{-1} + P^{\varepsilon}(\max|\eta_{ij}|)^{-n/2R}$$

For given η , we may set $P = \max |\eta_{ij}|^{1+n/2R} > 1$; in this way, α_{ij} is defined as $\alpha_{ij} = \eta_{ij}P^{-2}$, which implies that $\max |\alpha_{ij}| < P^{-1}$. Hence the bound just given yields

$$I(\boldsymbol{\eta}) \ll \max|\eta_{ij}|^{-n/2R+\varepsilon}.$$

LEMMA 4.6. Assume that $n > (2\gamma + m(m-1))(R+1)$. Then $\Im(\mathbf{c})$ converges absolutely and, for any $Q \ge 1$,

$$|\mathfrak{I}(\mathbf{c}) - \mathfrak{I}(Q, \mathbf{c})| \ll Q^{-1+\varepsilon}$$

uniformly in **c**.

Proof. Let $N := \max |\eta_{ij}|$. Then, for any $1 \ll Q_1 < Q_2$ and for suitable positive constants c_6 and c_7 ,

$$\begin{aligned} |\Im(Q_2,\mathbf{c}) - \Im(Q_1,\mathbf{c})| &= \int_{c_6 Q_1 \le N \le c_7 Q_2} I(\boldsymbol{\eta}) e\left(-\sum_{1 \le i \le j \le m} \eta_{ij} c_{ij}\right) d\boldsymbol{\eta} \\ &\ll \int_{c_6 Q_1 \le N \le c_7 Q_2} \min\{1, N^{-R-1-1/2R+\varepsilon}\} d\boldsymbol{\eta} \end{aligned}$$

by Lemma 4.5 and the inequality

$$n \ge (2\gamma + m(m-1))(R+1) + 1 \ge 2R(R+1) + 1.$$

Therefore, applying Fubini's theorem, and noting that $Q_1 \gg 1$, we obtain

$$|\mathfrak{I}(Q_2,\mathbf{c})-\mathfrak{I}(Q_1,\mathbf{c})|\ll \int_{c_6Q_1}^{c_7Q_2} N^{-2-1/2R+\varepsilon} \, dN \ll Q_1^{-1-1/2R+\varepsilon}.$$

Both parts of the lemma now follow.

Next we make use of our assumption that B is Minkowski reduced. As is well known, this assumption implies that

$$\det B \ll \prod_{i=1}^m B_{ii} \ll \det B,$$

where the implied *O*-constant depends only on the dimension *m* of *B*. Combining Lemmas 4.3, 4.4, and 4.6 and noting that $\mathfrak{S}(\mathbf{b}) \ll 1$ and $\mathfrak{I}(\mathbf{c}) \ll 1$ (see Sections 5 and 6 as well as (7) and (2)), we thus obtain the following result.

LEMMA 4.7. Assume that $n > (2\gamma + m(m-1))(R+1)$. Then there exists a $\delta > 0$ such that

$$N(A, B) = \Pi^{n-m-1} \mathfrak{S}(\mathbf{b}) \mathfrak{I}(\mathbf{c}) + O((\det B)^{(n-m-1)/2-\delta}),$$

where $c_{ij} = (P_i P_j)^{-1} B_{ij}$ for $1 \le i \le j \le m$.

5. Singular Series

The singular series $\mathfrak{S}(\mathbf{b})$ corresponds to *p*-adic solutions to the system of equations, and we shall show that it factors as a product over all primes of $\alpha_p(A, B)$.

LEMMA 5.1. Suppose that $n > (2\gamma + m(m-1))(R+1)$. Then $\mathfrak{S}(\mathbf{b}) = \prod_{p} \alpha_{p}(A, B).$

Proof. Since $\mathfrak{S}(\mathbf{b})$ is absolutely convergent by Lemma 4.4, a standard argument (see e.g. [1, Sec. 7]) then gives

$$\mathfrak{S}(\mathbf{b}) = \prod_{p} \sum_{r=0}^{\infty} \sum_{\substack{\mathbf{a} \bmod p^{r} \\ (\mathbf{a}, p) = 1}} p^{-rmn} S_{\mathbf{a}, p^{r}}(\mathbf{b})$$
$$= \prod_{p} \mathfrak{S}_{p}(\mathbf{b}),$$

say. Now, for each prime p, we have

$$\begin{split} \mathfrak{S}_{p}(\mathbf{b}) &= \lim_{N \to \infty} \sum_{r=0}^{N} \sum_{\substack{\mathbf{a} \bmod p^{r} \\ (\mathbf{a}, p) = 1}} p^{-rmn} S_{\mathbf{a}, p^{r}}(\mathbf{b}) \\ &= \lim_{N \to \infty} (p^{-N})^{mn-R} \\ &\times \#\{\mathbf{x}_{1}, \dots, \mathbf{x}_{m} \pmod{p^{N}} : \mathbf{x}_{i}^{\mathrm{T}} A \mathbf{x}_{j} \equiv B_{ij} \pmod{p^{N}} \ (1 \leq i \leq j \leq m)\} \\ &= \lim_{N \to \infty} (p^{-N})^{mn-R} \#\{X \pmod{p^{N}} : X^{\mathrm{T}} A X \equiv B \pmod{p^{N}}\}. \end{split}$$

By [12, Lemma 5.6.1], there exists an integer $t \ge 0$ such that

$$(p^{-N})^{mn-R} \# \{X \pmod{p^N} : X^{\mathrm{T}}AX \equiv B \pmod{p^N} \}$$

remains constant for all $N \ge t$. This is the $\alpha_p(A, B)$ defined in (3), so we have $\mathfrak{S}_p(\mathbf{b}) = \alpha_p(A, B)$.

6. Singular Integral

The proof of Theorem 1.1 will be complete once we show that $\Pi^{n-m-1}\mathfrak{I}(\mathbf{c}) = \alpha_{\infty}(A, B)$ as defined in equation (2).

Let $U \subset \mathbb{R}^{m(m+1)/2}$ be a real neighborhood of *B*, and let $V \subset \mathbb{R}^{mn}$ be the set of real $n \times m$ matrices *X* such that $X^{T}AX$ lies inside *U*. Then it is known [3, Chap. B.3] that $\alpha_{\infty}(A, B)$ is equal to the limit of $\operatorname{vol}(V)/\operatorname{vol}(U)$ as the neighborhood *U* shrinks to *B*. Therefore, taking the neighborhood

$$\prod_{1 \le i \le j \le m} [B_{ij} - \varepsilon P_i P_j, B_{ij} + \varepsilon P_i P_j]$$

for $\varepsilon > 0$, we may deduce that

$$\alpha_{\infty}(A,B) = \lim_{\varepsilon \to 0} \frac{1}{\Pi^{m+1}(2\varepsilon)^R} \int_{\substack{|\mathbf{x}_i^{\mathsf{T}}A\mathbf{x}_j - B_{ij}| \le (P_i P_j)\varepsilon \\ 1 \le i \le j \le m}} d\mathbf{x}_1 \cdots d\mathbf{x}_m.$$
(35)

For $\mathbf{c} = (c_{ij})_{1 \le i \le j \le m}$ with $c_{ij} = (P_i P_j)^{-1} B_{ij}$, let $V(\mathbf{c})$ denote the real variety defined by

$$\mathbf{x}_i^{\mathrm{T}} A \mathbf{x}_j - c_{ij} = 0 \quad (1 \le i \le j \le m).$$

LEMMA 6.1. The variety $V(\mathbf{c})$ is nonempty and nonsingular.

Proof. By our choice of the P_i in (9), there exist real vectors $\mathbf{y}_1, \ldots, \mathbf{y}_m$ such that

$$\mathbf{y}_i^{\mathrm{T}} A \mathbf{y}_j = B_{ij} \quad (1 \le i \le j \le m).$$

Therefore, taking $\mathbf{x}_i = P_i^{-1} \mathbf{y}_i$ for each $i \in \{1, ..., m\}$ gives a real point on $V(\mathbf{c})$.

Now consider the Jacobian matrix of this variety. This is an $R \times mn$ matrix, and suppose there exist real vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m$ where this Jacobian has rank strictly less than R. The rows of the Jacobian would then be linearly dependent, in which case—after considering the n columns corresponding to some suitable vector \mathbf{x}_i we can deduce the existence of real numbers $\lambda_1, \ldots, \lambda_m$, not all zero, such that

$$A\left(2\lambda_i\mathbf{x}_i+\sum_{\substack{j=1\\j\neq i}}^m\lambda_j\mathbf{x}_j\right)=\mathbf{0}.$$

Because A is nonsingular, we must have

$$2\lambda_i \mathbf{x}_i + \sum_{\substack{j=1\\j\neq i}}^m \lambda_j \mathbf{x}_j = \mathbf{0}.$$

Hence the matrix X whose columns are the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m$ does not have full rank. It follows that X^TAX does not have full rank for any vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m$ where the Jacobian does not have full rank. Recall that the matrix B has full rank; the matrix $C = (c_{ij})_{1 \le i, j \le m}$ can be written as C = DBD, where D denotes the diagonal matrix having entries $P_1^{-1}, \ldots, P_m^{-1}$ on the diagonal. Therefore, C also has full rank, from which it follows that there cannot be a solution to $X^TAX = C$ where X does not have full rank. As a result, the variety $V(\mathbf{c})$ is nonsingular.

Combining Lemma 4.7, Lemma 5.1, equation (35), and the following lemma serves to conclude the proof of Theorem 1.1.

LEMMA 6.2. We have

$$\Pi^{n-m-1}\mathfrak{I}(\mathbf{c}) = \lim_{\varepsilon \to 0} \frac{1}{\Pi^{m+1}(2\varepsilon)^R} \int_{\substack{|\mathbf{x}_i^T A \mathbf{x}_j - B_{ij}| \le (P_i P_j)\varepsilon \\ 1 \le i \le j \le m}} d\mathbf{x}_1 \cdots d\mathbf{x}_m.$$

Proof. We shall denote the variety $V(\mathbf{c})$ by

$$G_{i,j}(\mathbf{x}) = 0 \quad (1 \le i \le j \le m)$$

for $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{R}^{mn}$. By Lemma 6.1, this variety is nonempty and nonsingular. Hence the variety has positive (mn - R)-dimensional measure, and the Jacobian matrix

$$\left(\frac{\partial G_{i,j}(\mathbf{x})}{\partial x_{st}}\right)_{\substack{1 \le i \le j \le m \\ 1 \le s \le m, 1 \le t \le n}}$$

has rank *R* at all real points. Since *A* is positive definite, for any $\varepsilon > 0$ it follows that the set *V*(**c**, ε) of real **x** satisfying

$$|G_{i,j}(\mathbf{x})| \le \varepsilon \quad (1 \le i \le j \le m)$$

is closed, bounded, and therefore compact. Moreover, by continuity, for small enough ε the Jacobian is still nonsingular at any point of this set because this is true for $V(\mathbf{c})$. We can thus divide $V(\mathbf{c}, \varepsilon)$ into a finite number of measurable partitions; on each partition (say, ξ), there exists some *R*-tuple $x_{s_1t_1}, \ldots, x_{s_Rt_R}$ with $1 \le s_1, \ldots, s_R \le m$ and $1 \le t_1, \ldots, t_R \le n$ such that, for

$$\delta := \det \left(\frac{\partial G_{i,j}(\mathbf{x})}{\partial x_{s_k t_k}} \right)_{\substack{1 \le i \le j \le m \\ 1 \le k \le R}},$$

we have $|\delta| \gg 1$ for all points in ξ . In particular, for all $1 \le k \le R$ for at least one pair *i*, *j* we have

$$\left|\frac{\partial G_{i,j}(\mathbf{y}, \mathbf{z})}{\partial x_{s_k t_k}}\right| \gg 1 \tag{36}$$

throughout ξ , with an implied constant that is independent of ε . Since the number of possibilities for choosing the s_k and the t_k is both finite and independent of ε , we can assume that the number of partitions is also independent of ε .

We shall write a typical vector $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \xi$ as (\mathbf{y}, \mathbf{z}) , where

$$\mathbf{y} = (x_{s_1t_1}, \dots, x_{s_Rt_R})$$

and **z** denotes the remaining variables. Suppose that $(\mathbf{y}^{(1)}, \mathbf{z})$ is a point in ξ that lies on the variety $V(\mathbf{c})$. Then

$$|G_{i,j}(\mathbf{y},\mathbf{z}) - G_{i,j}(\mathbf{y}^{(1)},\mathbf{z})| \leq \varepsilon \quad (1 \leq i \leq j \leq m).$$

By (36) and the mean value theorem, it then follows that $|x_{s_k t_k} - x_{s_k t_k}^{(1)}| \ll \varepsilon$ for each $1 \le k \le R$.

Now, by Taylor's theorem, we may write

$$G_{i,j}(\mathbf{y}, \mathbf{z}) - G_{i,j}(\mathbf{y}^{(1)}, \mathbf{z}) = \sum_{k=1}^{R} (x_{s_k t_k} - x_{s_k t_k}^{(1)}) \frac{\partial G_{i,j}(\mathbf{y}^{(1)}, \mathbf{z})}{\partial x_{s_k t_k}} + O(\varepsilon^2) \quad (1 \le i \le j \le m)$$

given that the second partial derivatives of the $G_{i,j}$ are all constant. Therefore, upon inverting these *R* linear equations, we see that the conditions $|G_{i,j}(\mathbf{x})| \le \varepsilon$ $(1 \le i \le j \le m)$ imply that **y** lies in a region of volume $(2\varepsilon)^R \delta^{-1} + O(\varepsilon^{R+1})$.

As a result,

$$\frac{1}{(2\varepsilon)^R}\int_{\xi} d\mathbf{x}_1\cdots d\mathbf{x}_m = \int_{V(\mathbf{c})\cap\xi} \frac{d\mathbf{z}}{\delta} + O(\varepsilon).$$

After we sum over all partitions ξ and take the limit as $\varepsilon \to 0$, the right-hand side of this expression is equal to $\Im(\mathbf{c})$ by the argument in [1, Sec. 6]. The left-hand side becomes

$$\lim_{\varepsilon \to 0} \frac{1}{(2\varepsilon)^R} \int_{\substack{|G_{i,j}(\mathbf{x})| \le \varepsilon \\ 1 \le i \le j \le m}} d\mathbf{x}_1 \cdots d\mathbf{x}_m$$

= $\Pi^{-n} \lim_{\varepsilon \to 0} \frac{1}{(2\varepsilon)^R} \int_{\substack{|\mathbf{x}_i^T A \mathbf{x}_j - B_{ij}| \le (P_i P_j)\varepsilon \\ 1 \le i \le j \le m}} d\mathbf{x}_1 \cdots d\mathbf{x}_m$

after a change of variables. This completes the proof of the lemma and hence of Theorem 1.1. $\hfill \Box$

References

- B. J. Birch, Forms in many variables, Proc. Roy. Soc. London Ser. A 265 (1961/62), 245–263.
- J. Brandes, Forms representing forms and linear spaces on hypersurfaces, Proc. London Math. Soc. (3) (to appear).
- [3] J. W. S. Cassels, *Rational quadratic forms*, London Math. Soc. Monogr., 13, Academic Press, London, 1978.
- [4] H. Davenport, Analytic methods for Diophantine equations and Diophantine inequalities, 2nd ed., Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 2005.
- [5] R. Dietmann, *Linear spaces on rational hypersurfaces of odd degree*, Bull. London Math. Soc. 42 (2010), 891–895.
- [6] W. Duke and R. Schulze-Pillot, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. 99 (1990), 49–57.

- [7] J. S. Ellenberg and A. Venkatesh, Local-global principles for representations of quadratic forms, Invent. Math. 171 (2008), 257–279.
- [8] 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.
- [9] J. S. Hsia, Y. Kitaoka, and M. Kneser, *Representations of positive definite quadratic forms*, J. Reine Angew. Math. 301 (1978), 132–141.
- [10] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ., 53, Amer. Math. Soc., Providence, RI, 2004.
- [11] Y. Kitaoka, *Modular forms of degree n and representation by quadratic forms. II*, Nagoya Math. J. 87 (1982), 127–146.
- [12] —, Arithmetic of quadratic forms, Cambridge Tracts in Math., 106, Cambridge Univ. Press, Cambridge, 1993.
- [13] S. T. Parsell, *The density of rational lines on cubic hypersurfaces*, Trans. Amer. Math. Soc. 352 (2000), 5045–5062.
- [14] S. Raghavan, Modular forms of degree n and representation by quadratic forms, Ann. of Math. (2) 70 (1959), 446–477.
- [15] R. Schulze-Pillot, Local conditions for global representations of quadratic forms, Acta Arith. 138 (2009), 289–299.
- [16] ——, Representation of quadratic forms by integral quadratic forms, Quadratic and higher degree forms (K. Alladi, M. Bhargava, D. Savitt, P. H. Tiep, eds.), Dev. Math., 31, Springer-Verlag, New York, 2013.
- [17] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. of Math.
 (2) 36 (1935), 527–606.
- [18] R. C. Vaughan, *The Hardy–Littlewood method*, 2nd ed., Cambridge Tracts in Math., 125, Cambridge Univ. Press, Cambridge, 1997.

R. Dietmann Department of Mathematics Royal Holloway University of London TW20 0EX Egham United Kingdom

Rainer.Dietmann@rhul.ac.uk

M. Harvey Department of Mathematics Royal Holloway University of London TW20 0EX Egham United Kingdom

Michael.Harvey@rhul.ac.uk