arXiv:1309.6767v1 [math.NT] 26 Sep 2013

Simultaneous Integer Values of Pairs of Quadratic Forms

D. R. Heath-Brown*
L. B. Pierce†

Abstract

We prove that a pair of integral quadratic forms in 5 or more variables will simultaneously represent "almost all" pairs of integers that satisfy the necessary local conditions, provided that the forms satisfy a suitable nonsingularity condition. In particular such forms simultaneously attain prime values if the obvious local conditions hold. The proof uses the circle method, and in particular pioneers a two-dimensional version of a Kloosterman refinement.

Contents

*Mathematical Institute, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, *rhb@maths.ox.ac.uk*

†Hausdorff Center for Mathematics, 60 Endenicher Allee, 53115 Bonn, *pierce@math.uni-bonn.de*

2010 Mathematics Subject Classification: 11P55, 11D85

1 Introduction

Given two quadratic forms $Q_1, Q_2 \in \mathbb{Z}[x_1, \ldots, x_k]$, we would like to understand which pairs of integers n_1, n_2 are represented simultaneously by Q_1 and Q_2. The situation for a single form is fairly well understood, but less is known for pairs of forms. Naturally there may be local obstructions to representability. However one might expect that if the variety V defined by the simultaneous equations

$$\begin{cases} Q_1(\mathbf{x}) &= 0 \\ Q_2(\mathbf{x}) &= 0 \end{cases} \tag{1.1}$$

is nonsingular, and if k is large enough, then every pair n_1, n_2 satisfying the necessary local conditions should be representable, or at least that all but finitely many such pairs are representable.

The method of Birch [1] can be adapted to obtain an asymptotic for the number of representations of a pair of integers n_1, n_2 by quadratic forms Q_1, Q_2 for $k \geq 13 + s$ variables, where s denotes the dimension of the set

$$\{\mathbf{x} \in \overline{\mathbb{Q}}^k : \text{rank} \begin{pmatrix} \nabla Q_1(\mathbf{x}) \\ \nabla Q_2(\mathbf{x}) \end{pmatrix} < 2\};$$

in particular, if the variety (1.1) is nonsingular then $s = 1$. In a recent preprint, Munshi [11] employs a new 'nested δ-method' version of the circle method to reduce the number of variables to $k \geq 11$ if (1.1) is nonsingular.

In order to handle as small a value for k as possible, this paper asks only that "almost all" suitable pairs are representable. By this we mean that the number of suitable pairs for which $|n_1|, |n_2| \leq N$ but n_1, n_2 are not simultaneously representable, should be $o(N^2)$ as N tends to infinity.

As a by-product of our investigation we will be able to say something about pairs of quadratic forms which simultaneously take prime values infinitely often. Certainly such pairs of forms exist: for example, Q_1 and Q_2 defined by

$$\begin{aligned} Q_1(x_1, x_2, x_3) &= x_1^2 + 4x_2^2 \\ Q_2(x_1, x_2, x_3) &= 4x_1^2 + x_3^2, \end{aligned}$$

simultaneously attain prime values infinitely often. Indeed one can use the result of Fouvry and Iwaniec [5] to show that for "almost all" odd integers x_1 there is a prime of the form $x_1^2 + 4x_2^2$, and equally that for almost all such x_1 there is a prime of the form $4x_1^2 + x_3^2$. The claim then follows easily.

The geometric condition we must impose on the pair of quadratic forms is as follows:

Condition 1 *The projective variety defined over* $\overline{\mathbb{Q}}$ *by*

$$V : Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0 \tag{1.2}$$

is nonsingular, by which we mean for every $\mathbf{x} \in \overline{\mathbb{Q}}^k$, *if* $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ *with* $\mathbf{x} \neq 0$ *then*

$$\mathrm{rk} \begin{pmatrix} \nabla Q_1(\mathbf{x}) \\ \nabla Q_2(\mathbf{x}) \end{pmatrix} = 2. \tag{1.3}$$

We will count solutions using a smooth non-negative weight $w : \mathbb{R}^k \to \mathbb{R}$ of compact support. We then define the normalized weight function

$$w_B(\mathbf{x}) = w(B^{-1}\mathbf{x}) \tag{1.4}$$

and the weighted representation function

$$R_B(n_1, n_2) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^k \\ \underline{Q}(\mathbf{x}) = \underline{n}}} w_B(\mathbf{x}), \tag{1.5}$$

where we use an underscore to denote variables in 2-dimensional spaces, so that $\underline{Q}(\mathbf{x}) = (Q_1(\mathbf{x}), Q_2(\mathbf{x}))$, for example.

By an "integral quadratic form" we will always mean a form with integral matrix, so that the off-diagonal terms of the form have even coefficients. Our principal result is then the following, in which we set

$$F(x, y) = \det(xQ_1 + yQ_2).$$

Theorem 1.1 *Suppose we have two integral quadratic forms Q_1, Q_2 satisfying Condition 1, in $k \geq 5$ variables. Then if $N = B^2$ we have*

$$\sum_{\substack{\max\{|n_1|,|n_2|\} \leq N \\ F(n_2,-n_1) \neq 0}} |R_B(\underline{n}) - \mathcal{J}_w(B^{-2}\underline{n})\mathfrak{S}(\underline{n})B^{k-4}|^2 \ll_{Q_1,Q_2,w} B^{2k-4-1/16}, \quad (1.6)$$

where $\mathcal{J}_w(\underline{\mu})$ and $\mathfrak{S}(\underline{n})$ are the singular integral and singular series, given respectively by (3.9) and (6.1).

Of course this is of little use without some information about $\mathcal{J}_w(\underline{\mu})$ and $\mathfrak{S}(\underline{n})$. This will be provided in our second result.

Theorem 1.2 *Let Q_1 and Q_2 be as in Theorem 1.1 and suppose that $k \geq 5$ and $F(n_2, -n_1) \neq 0$. Then $\mathfrak{S}(\underline{n}) \ll_{\varepsilon,Q_1,Q_2} \max(|n_1|, |n_2|)^{\varepsilon}$ for any $\varepsilon > 0$. Moreover if the system of equations $Q_1(\mathbf{x}) = n_1$, $Q_2(\mathbf{x}) = n_2$ is solvable in every p-adic ring $\mathbb{Z}_p$, then $\mathfrak{S}(\underline{n})$ is real and positive. Indeed there is then a constant p_0 depending only on Q_1 and Q_2 such that*

$$\mathfrak{S}(\underline{n}) \gg_{\varepsilon,Q_1,Q_2} \max(|n_1|, |n_2|)^{-\varepsilon} \prod_{p \leq p_0} |F(n_2, -n_1)|_p^{k-2},$$

for any fixed $\varepsilon > 0$, where $|\cdot|_p$ denotes the standard p-adic valuation.

Similarly, under the same conditions on $\underline{Q}$, for any smooth weight w of compact support we have $\mathcal{J}_w(\underline{\mu}) \ll_{Q_1,Q_2,w} 1$. Moreover there is a constant C, depending on Q_1 and Q_2, with the following property. Suppose that $w(\mathbf{x}) > 0$ for $|\mathbf{x}| \leq C$. Then we have

$$\mathcal{J}_w(\underline{\mu}) \gg_{Q_1,Q_2,w} |F(\mu_2, -\mu_1)|^{k-2}$$

for any $\underline{\mu}$ in the region $1/2 \leq \max(|\mu_1|, |\mu_2|) \leq 1$ for which the system of equations $Q_1(\mathbf{x}) = \mu_1$, $Q_2(\mathbf{x}) = \mu_2$ has a solution $\mathbf{x} \in \mathbb{R}^k$.

As a corollary we have the following result.

Theorem 1.3 *Suppose we have two integral quadratic forms Q_1, Q_2 satisfying Condition 1, in $k \geq 5$ variables. Let $\mathcal{E}(N)$ denote the number of integer pairs (n_1, n_2) with $|n_1|, |n_2| \leq N$ for which the system $Q_1(\mathbf{x}) = n_1$, $Q_2(\mathbf{x}) = n_2$ has a real solution and solutions in each $\mathbb{Z}_p$, but for which there is no solution $\mathbf{x} \in \mathbb{Z}^k$. Then*

$$\mathcal{E}(N) \ll_{Q_1,Q_2,\varpi} N^{2-\varpi},$$

with $\varpi = 1/(8k^3)$.

We have made no effort to get the best possible exponent ϖ here, but note that our value is dependent only on k.

In particular, we may derive from Theorem 1.3 the following result on simultaneous prime values:

Theorem 1.4 *Suppose two integral quadratic forms $Q_1(\mathbf{x}), Q_2(\mathbf{x})$ satisfy Condition 1 with $k \geq 5$. Suppose further that there is an $\mathbf{x}_0 \in \mathbb{R}^k$ such that $Q_1(\mathbf{x}_0), Q_2(\mathbf{x}_0) > 0$, and that for every prime q there is an $\mathbf{x}_q \in \mathbb{Z}^k$ for which $q \nmid Q_1(\mathbf{x}_q)Q_2(\mathbf{x}_q)$. Then there are infinitely many pairs of primes simultaneously representable by $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$.*

We will prove in Section 2.1 that for diagonal quadratic forms, say $Q_1 = \sum a_i x_i^2$ and $Q_2 = \sum b_i x_i^2$, Condition 1 is equivalent to the condition that the ratios a_i/b_i are all distinct, for $i = 1, \ldots, k$. As a result, it is simple to find examples of pairs of forms that satisfy the requirements of Theorem 1.4. For instance, one may take

$$\begin{aligned} Q_1(\mathbf{x}) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 \\ Q_2(\mathbf{x}) &= x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 + 5x_5^2, \end{aligned}$$

for which the choices $\mathbf{x}_0 = (1, 0, \ldots, 0)$, $\mathbf{x}_q = (1, 0, \ldots, 0)$ clearly suffice.

If Condition 1 is dropped from the hypotheses of Theorem 1.4, then the result of the theorem can fail to hold. For example, the pencil generated by $Q_1(\mathbf{x}) = x_1^2$, $Q_2(\mathbf{x}) = x_1^2 + \cdots + x_k^2$ is singular as soon as $k \geq 3$, and certainly Q_1 will never attain prime values. In fact, it is reasonable to conjecture that this is representative of the only type of exception to arise. Motivated by Schinzel's Hypothesis, one may conjecture that the result of Theorem 1.4 should continue to hold if the assumption of Condition 1 is replaced by the assumption that neither $Q_1(\mathbf{x})$ nor $Q_2(\mathbf{x})$ factors over $\mathbb{Z}$; this is discussed further in Section 10.

We should remark at this point that one can handle "target sets" other than the primes in much the same way. Provided that the target set has a counting function that grows faster than $N^{1-\varpi/2}$, all that is necessary is that one should be able to deal satisfactorily with the local conditions that arise. In particular we can handle the case in which the target set consists of the integers that are sums of two squares. This leads to an analytic proof of the following example of the Hasse Principle (which is a special case of a far more general result due to Colliot-Thélène, Sansuc and Swinnerton-Dyer [4, Theorem A, case (i)(a)]).

Corollary 1.4.1 *Let $q_1(\mathbf{x}, \mathbf{y}) = Q_1(\mathbf{x}) - y_1^2 - y_2^2$, $q_2(\mathbf{x}, \mathbf{y}) = Q_2(\mathbf{x}) - y_3^2 - y_4^2$, where $Q_1, Q_2 \in \mathbb{Z}[x_1, \ldots, x_k]$ are integral quadratic forms satisfying Condition 1. Then the Hasse Principle holds for the intersection $q_1(\mathbf{x}, \mathbf{y}) = q_2(\mathbf{x}, \mathbf{y}) = 0$ as soon as $k + 4 \geq 9$.*

We leave the details of the proof to the reader. Here $k+4$ is the total number of variables in the system $q_1(\mathbf{x}, \mathbf{y}) = q_2(\mathbf{x}, \mathbf{y}) = 0$. This result may be compared to the recent work of Browning and Munshi [3] on the Hasse Principle for the intersection $q_1(\mathbf{x}, \mathbf{y}) = q_2(\mathbf{x}, \mathbf{y}) = 0$. Browning and Munshi assume that the forms q_1 and q_2 take the shape $q_1(\mathbf{x}, \mathbf{y}) = Q_1(\mathbf{x}) - y_1^2 - y_2^2$, $q_2(\mathbf{x}, \mathbf{y}) = Q_2(\mathbf{x})$ in $k + 2 \geq 9$ variables, where the intersection $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ is assumed to be nonsingular.

We observe that the range $k \geq 5$ in Theorem 1.3 is best possible in the sense that the theorem statement would be false with $k = 4$. To justify this we first note that for any integer $L \geq 2$ the forms

$$Q_1(\mathbf{x}) = x_1^2 + x_3^2 + x_4^2, \quad Q_2(\mathbf{x}) = x_2^2 + x_3^2 + Lx_4^2 \tag{1.7}$$

satisfy Condition 1. It can be shown (by a method similar to the derivation of Theorem 1.4 in Section 10) that there is a value p_0 depending only on Q_1, Q_2 such that the equations

$$Q_1(\mathbf{x}) = n_1, \quad Q_2(\mathbf{x}) = n_2 \tag{1.8}$$

will have a nonsingular solution in $\mathbb{F}_p$, and hence a solution in $\mathbb{Z}_p$, for any $p \geq p_0$ not dividing both L and n_2. Moreover, there exists a modulus M and residue classes a_1, a_2 dependent only on Q_1, Q_2 and the primes $p < p_0$ such that the system (1.8) has a solution over $\mathbb{Z}_p$ for $p < p_0$ as long as

$$n_1 \equiv a_1, n_2 \equiv a_2 \pmod{M}.$$

For the pair (1.7), computation shows that $p_0 = 11, a_1 = a_2 = 1$, and $M = 840$ suffice, so that taking L as a large prime, one may conclude that the system has solutions over every $\mathbb{Z}_p$ provided that $n_1 \equiv n_2 \equiv 1 \pmod{840}$ and $L \nmid n_2$. Moreover there will be a real solution (with $x_3 = x_4 = 0$) whenever n_1 and n_2 are positive. Thus there are $\gg N^2$ pairs of positive integers $n_1, n_2 \leq N$ for which the local conditions are everywhere satisfied, with an implied constant independent of L. However for a global solution one clearly has $|x_1|, |x_2|, |x_3| \leq N^{1/2}$ and $|x_4| \leq N^{1/2}L^{-1/2}$ so that there are $O(N^2L^{-1/2})$ possible 4-tuples $(x_1, \ldots, x_4)$. Thus if L is chosen sufficiently large there will be $\gg N^2$ pairs n_1, n_2 for which there are local solutions but no global solution.

Thus far we have interpreted the results of Theorems 1.1 and 1.2 as providing "almost-every" results. In particular, these theorems verify that for a pair of integral quadratic forms satisfying Condition 1 in $k \geq 5$ variables, for "almost every" pair (n_1, n_2) the counting function $R_B(\underline{n})$ is asymptotically equal to $\mathcal{J}_w(B^{-2}\underline{n})\mathfrak{S}(\underline{n})B^{k-4}$. Precisely, if $N = B^2$ and for each $0 < \theta < 1/32$ we let $\mathcal{E}_\theta(N)$ denote the number of $|n_1|, |n_2| \leq N$ for which either $F(n_2, -n_1) = 0$ or the difference

$$R_B(\underline{n}) - \mathcal{J}_w(B^{-2}\underline{n})\mathfrak{S}(\underline{n})B^{k-4}$$

fails to be $O(B^{k-4-\theta})$, then Theorem 1.1 shows that $\mathcal{E}_\theta(N) \ll N^{2-(\frac{1}{32}-\theta)}$.

Our results also imply universal results for certain forms in $k \geq 10$ variables. Suppose that Q_1, Q_2 are integral forms in $k_1 + k_2$ variables that split, so that we may write

$$\begin{aligned} Q_1(\mathbf{x}, \mathbf{y}) &= q_1(\mathbf{x}) + q_2(\mathbf{y}) \\ Q_2(\mathbf{x}, \mathbf{y}) &= q_3(\mathbf{x}) + q_4(\mathbf{y}), \end{aligned} \tag{1.9}$$

where $\mathbf{x} \in \mathbb{Z}^{k_1}, \mathbf{y} \in \mathbb{Z}^{k_2}$, q_1, q_3 are integral quadratic forms in k_1 variables and q_2, q_4 are integral quadratic forms in k_2 variables. Note that if the pair Q_1, Q_2 satisfies Condition 1 then each of the pairs q_1, q_3 and q_2, q_4 also satisfies Condition 1 (but the reverse implication need not hold); this is visible by applying Condition 2 (see section 2.1) to the factorization

$$\det(xQ_1 + yQ_2) = \det(xq_1 + yq_3)\det(xq_2 + yq_4).$$

Our results (in particular Propositions 7.1 and 8.1) imply immediately the following, by a classical application of the circle method:

Theorem 1.5 *Suppose that $k_1, k_2 \geq 5$ and that we have two integral quadratic forms $Q_1, Q_2 \in \mathbb{Z}[X_1, \ldots, X_{k_1+k_2}]$ satisfying Condition 1. Assume further that Q_1 and Q_2 are split as in (1.9). Then for any (n_1, n_2) such that $F(n_2, -n_1) \neq 0$,*

$$R_B(n_1, n_2) = \mathfrak{S}(\underline{n})\mathcal{J}_w(B^{-2}\underline{n})B^{k_1+k_2-4} + O(B^{k_1+k_2-4-1/32}),$$

where as usual $R_B(n_1, n_2)$ is defined by (1.5) and the singular series $\mathfrak{S}(\underline{n})$ and singular integral $\mathcal{J}_w(\underline{n})$ are given respectively by (6.1) and (3.9), and satisfy the properties of Theorem 1.2.

Theorem 1.5 does not apply to the case $(n_1, n_2) = (0, 0)$, but we are able to modify our argument to establish the following results.

Theorem 1.6 *Let $k_1, k_2 \geq 5$ and suppose that we have two integral quadratic forms $Q_1, Q_2 \in \mathbb{Z}[X_1, \ldots, X_{k_1+k_2}]$ satisfying Condition 1. Assume further that Q_1 and Q_2 are split as in (1.9). Then*

$$R_B(0, 0) = \mathfrak{S}(\underline{0})\mathcal{J}_w(\underline{0})B^{k_1+k_2-4} + O(B^{k_1+k_2-4-1/32}),$$

where the singular series $\mathfrak{S}(\underline{0})$ and singular integral $\mathcal{J}_w(\underline{0})$ are given respectively by (6.1) and (3.9), and satisfy the properties of Theorem 1.7 below.

Theorem 1.7 *Let Q_1 and Q_2 be as in Theorem 1.6. If the system of equations $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ has a nonzero solution in every p-adic ring $\mathbb{Z}_p$, then $\mathfrak{S}(\underline{0})$ is real and positive. Suppose further that the weight $w(\mathbf{x})$ is supported on a neighbourhood of the origin. Then if the system of equations $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ has a nonzero solution $\mathbf{x} \in \mathbb{R}^k$, we have $\mathcal{J}_w(\underline{0}) > 0$.*

1.1 Method of proof

Our approach uses the two-dimensional circle method. The novel idea that allows us to reduce to $k \geq 5$ is a two-dimensional Kloosterman refinement applied to the contribution of the minor arcs.

The proofs of our results are long and involved. In order to aid the reader, we begin by sketching the method of proof schematically, as follows. With the notations introduced above we set

$$S(\alpha_1, \alpha_2) = \sum_{\mathbf{x} \in \mathbb{Z}^k} e(\alpha_1 Q_1(\mathbf{x}) + \alpha_2 Q_2(\mathbf{x}))w_B(\mathbf{x}), \tag{1.10}$$

for any $(\alpha_1, \alpha_2) \in \mathbb{R}^2$, so that

$$R_B(n_1, n_2) = \int_0^1 \int_0^1 S(\alpha_1, \alpha_2)e(-\alpha_1 n_1 - \alpha_2 n_2)d\alpha_1 d\alpha_2.$$

With a suitable definition of the major arcs $\mathfrak{M}$ and minor arcs $\mathfrak{m}$ in two dimensions, we may break R_B into the two pieces

$$R_B(n_1, n_2) = \iint_{\mathfrak{M}} + \iint_{\mathfrak{m}}$$

so that

$$\begin{aligned} &\sum_{\underline{n} \in \mathbb{Z}^2} \left| R_B(n_1, n_2) - \iint_{\mathfrak{M}} S(\alpha_1, \alpha_2) e(-\alpha_1 n_1 - \alpha_2 n_2) d\alpha_1 d\alpha_2 \right|^2 \\ &\qquad = \sum_{\underline{n} \in \mathbb{Z}^2} \left| \iint_{\mathfrak{m}} S(\alpha_1, \alpha_2) e(-\alpha_1 n_1 - \alpha_2 n_2) d\alpha_1 d\alpha_2 \right|^2 . \end{aligned} \tag{1.11}$$

Temporarily set $f(\alpha_1, \alpha_2) = S(\alpha_1, \alpha_2)\chi_{\mathfrak{m}}(\alpha_1, \alpha_2)$. Then the right hand side of (1.11) is

$$\begin{aligned} \sum_{\underline{n} \in \mathbb{Z}^2} &\left| \iint_{[0,1]^2} f(\alpha_1, \alpha_2) e(-\alpha_1 n_1 - \alpha_2 n_2) d\alpha_1 d\alpha_2 \right|^2 \\ &= \iint_{[0,1]^2} |f(\alpha_1, \alpha_2)|^2 d\alpha_1 d\alpha_2 \\ &= \iint_{\mathfrak{m}} |S(\alpha_1, \alpha_2)|^2 d\alpha_1 d\alpha_2, \end{aligned} \tag{1.12}$$

where in the first equality we have applied Parseval's identity.

We will show that if $\max\{|n_1|, |n_2|\} \le N = O(B^2)$ and $F(n_2, -n_1) \ne 0$, the contribution of the major arcs may be approximated as

$$\iint_{\mathfrak{M}} S(\alpha_1, \alpha_2) e(-\alpha_1 n_1 - \alpha_2 n_2) d\alpha_1 d\alpha_2 = M(n_1, n_2) + E(n_1, n_2), \tag{1.13}$$

where $M(n_1, n_2)$ is the expected main term, including the singular series and the singular integral, and $E(n_1, n_2)$ is an acceptable error term. Thus it will follow that

$$\begin{aligned} \sum_{\substack{\max\{|n_1|,|n_2|\} \le N \\ F(n_2,-n_1) \ne 0}} &|R_B(n_1, n_2) - M(n_1, n_2)|^2 \\ &\ll \iint_{\mathfrak{m}} |S(\alpha_1, \alpha_2)|^2 d\alpha_1 d\alpha_2 + E(N), \end{aligned} \tag{1.14}$$

where

$$E(N) = \sum_{\underline{n} \in \mathbb{Z}^2} |E(n_1, n_2)|^2.$$

When $\max(|n_1|, |n_2|)$ is of order B^2 the expected size of $M(n_1, n_2)$ is B^{k-4}, since roughly speaking, this is the probability that as $\mathbf{x}$ ranges over B^k possible choices, both of the values $Q_1(\mathbf{x})-n_1$ and $Q_2(\mathbf{x})-n_2$ (each of size up to $O(B^2)$), is zero. Imagine for the moment that $M(n_1,n_2) \gg B^{k-4}$; this implicitly assumes that the singular series and singular integral have suitable lower bounds. (In fact, proving such lower bounds is a significant source of complication.) Suppose furthermore that the right hand side of (1.14) is bounded by B^β for some $\beta > 0$. Under these two significant assumptions, (1.14) would imply that

$$\#\{(n_1,n_2) \in \mathbb{Z}^2 : \max(|n_1|,|n_2|) \ll B^2 : R_B(n_1,n_2) = 0\} \cdot (B^{k-4})^2 \ll B^\beta,$$

whence

$$\#\{(n_1,n_2) \in \mathbb{Z}^2 : \max(|n_1|,|n_2|) \leq N \ : R_B(n_1,n_2) = 0\} \leq B^{\beta-(2k-8)} \quad (1.15)$$

for $N = O(B^2)$. If β is such that the right hand side of (1.15) is $o(N^2)$, then we may conclude that almost all pairs of integers n_1, n_2 of size N are represented simultaneously by Q_1, Q_2.

Thus we seek to bound (1.14) by B^β with $\beta < 2k-4$. The mean square argument above has appeared before in settings in which the circle method is used to show that almost all integers (in some suitable sense) are represented by a particular form. It dates from the work of Hardy and Littlewood [6] who showed, for example, that almost all positive integers are the sum of 5 non-negative cubes.

Our main goals now are therefore a representation of the contribution of the major arcs in the form (1.13), and a bound for the right hand side of (1.14) of the form $o(B^{2k-4})$. In particular, this will require an estimate for the integral over the minor arcs of the shape

$$\iint_{\mathfrak{m}} |S(\alpha_1,\alpha_2)|^2 d\alpha_1 d\alpha_2 = o(B^{2k-4}). \quad (1.16)$$

It is here that the main innovation of our work lies. Note that the application of Parseval's identity in (1.12) has achieved several things: first, it has raised the weighted exponential sum $S(\alpha_1,\alpha_2)$ to a higher power and homogenized the problem, thus passing the problem of counting simultaneous solutions of $Q_1(\mathbf{x}) = n_1$, $Q_2(\mathbf{x}) = n_2$ to the problem of counting simultaneous solutions of

$$Q_1(\mathbf{x}_1) - Q_1(\mathbf{x}_2) = 0, \quad Q_2(\mathbf{x}_1) - Q_2(\mathbf{x}_2) = 0,$$

where $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}^k$. Moreover, it has passed the power of $S(\alpha_1,\alpha_2)$ inside the relevant integral, thus increasing the possibility for advantageous averaging. In order to achieve this, we must treat the double integral over α_1, α_2, and the possible interactions between α_1 and α_2, nontrivially. We accomplish this by developing a two-dimensional Kloosterman refinement.

Historically, the Kloosterman refinement applies to a generating function of a single variable, say

$$F(\alpha) = \sum_n r(n) e(\alpha n),$$

in which case one may be interested in computing the representation number

$$r(0) = \int_0^1 F(\alpha) d\alpha.$$

To do so, one would traditionally apply the circle method to estimate portions of the integral with $\alpha \approx a/q$ for certain rational numbers a/q. Kloosterman's innovation [10] was to exploit cancellation between the contributions corresponding to pairs of distinct rationals $a_1/q, a_2/q$ with a common denominator q.

As suggested in [7], it would be desirable to apply a Kloosterman refinement to two-dimensional problems, in which case one would consider

$$\iint_{[0,1]^2} \sum_{m,n} r(m,n) e(\alpha_1 m + \alpha_2 n) d\alpha_1 d\alpha_2,$$

and hope to extract cancellation between portions of the integral corresponding to neighbourhoods of distinct pairs of rationals $(a_1/q, a_2/q)$ and $(b_1/q, b_2/q)$. To do so, one would need to approximate α_1, α_2 simultaneously by rationals with the same denominator, in such a way that the intervals in the refinement all share the same length. This can be accomplished by a 2-dimensional application of Dirichlet's principle, which guarantees for any $S \geq 1$ the existence of $1 \leq a_1, a_2 \leq q \leq S$, with $(a_1, a_2, q) = 1$ such that

$$|\alpha_1 - a_1/q| \leq \frac{1}{q\sqrt{S}}, \qquad |\alpha_2 - a_2/q| \leq \frac{1}{q\sqrt{S}}. \tag{1.17}$$

In the corresponding case in one dimension, Dirichlet's approximation principle places α in an interval of length $(qS)^{-1}$, and one can show that α can lie in at most two such intervals, if $q \leq S$. In two dimensions, the intervals are longer, and a given pair (α_1, α_2) may lie in many such intervals simultaneously. This makes a true 2-dimensional Kloosterman refinement difficult to carry out.

The key feature in our application is that we apply the 2-dimensional Kloosterman refinement only to the minor arcs contribution, for which we need simply an upper bound rather than an asymptotic. Thus we include all approximations (1.17) (accepting the possible overlap and resulting loss in sharpness) and then carry out a procedure to extract cancellation between the contributions of distinct pairs of rationals. We note that while in a 1-dimensional application of the Kloosterman refinement one typically encounters exponential sums involving both a and its inverse $\overline{a}$ modulo q, in our particular 2-dimensional application, such inverses do not appear. This is because in the usual 1-dimensional version one has to take detailed account of the end points of the Farey arcs, while in our 2-dimensional situation it suffices to use the simple explicit squares (1.17).

It is worth remarking that if one simply wanted to prove a result such as Theorem 1.3 for any $k > k_0$ sufficiently large one could avoid the Kloosterman refinement. In particular, one could use the simpler methods of Birch [1] for the treatment of the minor arcs for k sufficiently large. But in order to push the number of variables down to 5, we must use the more technical argument presented in this paper.

1.2 Notation

We denote by $v_p(n)$ the p-adic order of n, and by $|n|_p = p^{-v_p(n)}$ the p-adic valuation. We will use an underscore to denote variables in 2-dimensional spaces, such as $\underline{\alpha} \in \mathbb{R}^2$, $\underline{a} \in \mathbb{Z}^2$. Similarly we will use boldface to denote variables in k-dimensional spaces, such as $\mathbf{x} \in \mathbb{Z}^k$, and in $2k$-dimensional spaces, such as $\mathbf{l} = (\mathbf{l}_1, \mathbf{l}_2) \in \mathbb{Z}^k \times \mathbb{Z}^k$. We will use $Q(\mathbf{x})$ to denote a quadratic form with off-diagonal elements divisible by 2, as well as Q to denote the matrix associated with the quadratic form, so that $Q(\mathbf{x}) = \mathbf{x}^t Q \mathbf{x}$; which meaning is intended will be clear from context. We will write $|\mathbf{x}|$ for the Euclidean length of the vector $\mathbf{x}$, and $|\mathbf{x}|_p$ for the p-adic height. We will use $\underline{Q}$ to denote a pair of quadratic forms (Q_1, Q_2) and $\underline{a} \cdot \underline{Q}$ to denote the linear combination of forms $a_1 Q_1 + a_2 Q_2$. For a quadratic form Q we will let $||Q|| = \sup_{|\mathbf{x}|=1} |Q(\mathbf{x})|$. Throughout the paper all constants, explicit or implied, will be allowed to depend on the forms Q_1 and Q_2, as well as on the choice of the weight function w.

We say a weight function is smooth if it is C^∞. Denote by $\partial_{\mathbf{x}}^{\alpha}$ the derivative with respect to $\mathbf{x} \in \mathbb{R}^k$ of order α, where α is any multi-index $\alpha = (\alpha_1, \ldots, \alpha_k)$ of magnitude $|\alpha| = \alpha_1 + \cdots + \alpha_k$. We write

$$\frac{\partial^\alpha}{\partial \mathbf{x}^\alpha} \quad \text{for} \quad \frac{\partial^{|\alpha|}}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_k} x_k}.$$

We use the notation $\iint_{\{\phi_1,\phi_2\}}$ to denote integration over the region

$$([-2\phi_1, -\phi_1] \cup [\phi_1, 2\phi_1]) \times ([-2\phi_2, -\phi_2] \cup [\phi_2, 2\phi_2]).$$

2 Geometric conditions

2.1 Conditions related to Condition 1

Recall Condition 1, which stated that the variety V defined by $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ is nonsingular over $\overline{\mathbb{Q}}$. In general, if we have any algebraically closed field K of characteristic zero or of odd characteristic, we can consider the analogous statement for Q_1, Q_2 over K. We shall refer to this as Condition 1 with respect to K. Note that for any algebraically closed field K of characteristic zero, the field of definition of the forms Q_1, Q_2 will be taken to be $\mathbb{Q}$.

We now fix such a field K and define three more conditions. For convenience, we will refer to the relevant Jacobian matrix as

$$J(\mathbf{x}) = \begin{pmatrix} \nabla Q_1(\mathbf{x}) \\ \nabla Q_2(\mathbf{x}) \end{pmatrix},$$

so that Condition 1 may be stated as $\mathrm{rk}(J(\mathbf{x})) = 2$ for $\mathbf{x} \in V$ over K. We also define the matrix

$$\Delta(\mathbf{x}) = \Delta(\mathbf{x}; Q_1, Q_2) = (\Delta_{ij}(\mathbf{x}))_{i,j \le k} \tag{2.1}$$

where for each pair i, j we write

$$\Delta_{ij}(\mathbf{x}) = \begin{vmatrix} \frac{\partial Q_1}{\partial x_i} & \frac{\partial Q_1}{\partial x_j} \\ \frac{\partial Q_2}{\partial x_i} & \frac{\partial Q_2}{\partial x_j} \end{vmatrix}$$

for the i, j-th minor of the Jacobian matrix $J(\mathbf{x})$. Then $\mathrm{rk}(J(\mathbf{x})) = 2$ precisely when $\Delta(\mathbf{x}) \neq 0$.

We begin by proving that Condition 1 is equivalent to two other conditions. Recall that we defined the determinant form

$$F(x, y) = \det(xQ_1 + yQ_2).$$

This function will play a key role in the analysis throughout the paper; note that F is a binary form in x and y of degree k, and that its discriminant is a rational integer.

Condition 2 *The determinant form $F(x, y) = \det(xQ_1 + yQ_2)$ is not identically zero and has distinct linear factors over K; that is to say the discriminant of $F(x, y)$ is nonzero in K.*

We say that Q_1 and Q_2 can by simultaneously diagonalized over K if there exists a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ for K^k in which we may write

$$Q_1(\sum x_i \mathbf{e}_i) = \sum_{i=1}^{k} a_i x_i^2, \quad Q_2(\sum x_i \mathbf{e}_i) = \sum_{i=1}^{k} b_i x_i^2,$$

with coefficients $a_i, b_i \in K$.

Condition 3 *The forms Q_1 and Q_2 can be simultaneously diagonalized over K, so that $Q_1 = diag(a_i)$, $Q_2 = diag(b_i)$ with $a_i, b_i \in K$. Moreover, the ratios a_i/b_i are well-defined as elements of $K \cup \{\infty\}$ (that is to say a_i and b_i are not both zero), and are distinct, for $i = 1, \ldots, k$.*

Finally there is a fourth condition which is a consequence of the three we have discussed, but not in general equivalent to them.

Condition 4 *For every coefficient pair $(\nu_1, \nu_2) \in K^2 - \{0, 0\}$, the rank of the matrix associated to the quadratic form $\nu_1 Q_1 + \nu_2 Q_2$ satisfies*

$$\mathrm{rk}(\nu_1 Q_1 + \nu_2 Q_2) \geq k - 1.$$

Note that one cannot expect to have $\mathrm{rk}(\nu_1 Q_1 + \nu_2 Q_2) = k$ for every pair (ν_1, ν_2). For example, considering two diagonal quadratic forms, it is clear that one may always choose a linear combination that lowers the rank of the combination by one. Thus we cannot expect more than Condition 4 to hold, in general.

The main result of this section shows the relationships between these conditions; this equivalence has been observed before, such as in Proposition 2.1 of [12]; here we will argue in more elementary terms.

Proposition 2.1 *Fix any algebraically closed field K of characteristic zero or of odd characteristic. Conditions 1, 2 and 3 with respect to K are equivalent, and they each imply Condition 4 with respect to K. Furthermore, Conditions 1, 2, and 3 with respect to $\overline{\mathbb{Q}}$ are equivalent to Conditions 1, 2, and 3 with respect to any algebraically closed field K of characteristic zero.*

The last observation is visible when noting the equivalence of Condition 2 with respect to $\overline{\mathbb{Q}}$ and with respect to any K of characteristic zero, since the notion of disc $(F) \neq 0$ is equivalent in $\mathbb{Q}$ or in the prime field of K. In contrast, even if Condition 1 holds with respect to $\overline{\mathbb{Q}}$, Condition 1 may or may not hold with respect to $\overline{\mathbb{F}_p}$ for each fixed odd prime; we will distinguish between these possibilities in the next section when we define good and bad primes.

We first prove that Condition 1 implies Condition 4, by showing the contrapositive. Suppose that there exist $\nu_1, \nu_2 \in K$ for which $\text{rk}(\nu_1 Q_1 + \nu_2 Q_2) \leq k-2$. Given such a pair, set $Q_1' = \nu_1 Q_1 + \nu_2 Q_2$, and then choose Q_2' to be any other form such that the pair $\{Q_1', Q_2'\}$ generates the same pencil as the original pair $\{Q_1, Q_2\}$. Then by assumption,

$$\text{rk}(Q_1') \leq k-2. \tag{2.2}$$

Via change of basis over K, we can diagonalize $Q_1'(\mathbf{x}) = a_1 x_1^2 + \cdots + a_{k-2} x_{k-2}^2$, where we note that we may omit the last two variables x_{k-1}, x_k, due to the rank assumption. After this change of basis, we also have some representation for Q_2', call it $Q_2'(x_1, \ldots, x_k)$. For any $\mathbf{x}_0$ with $x_1 = \cdots = x_{k-2} = 0$, we obtain $Q_1'(\mathbf{x}_0) = 0$ and $\nabla Q_1'(\mathbf{x}_0) = 0$, so that

$$\text{rk} \begin{pmatrix} \nabla Q_1'(\mathbf{x}_0) \\ \nabla Q_2'(\mathbf{x}_0) \end{pmatrix} < 2. \tag{2.3}$$

So to show that Condition 1 fails, it is sufficient to find such an $\mathbf{x}_0$ lying on the variety $Q_1'(\mathbf{x}) = Q_2'(\mathbf{x}) = 0$. It is automatic that $Q_1'(\mathbf{x}_0) = 0$. Moreover, when $x_1 = \cdots = x_{k-2} = 0$ we see that $Q_2'(\mathbf{x}_0)$ is a quadratic form in the two variables x_{k-1}, x_k, so that it will have a non-trivial zero in K. We therefore obtain $\mathbf{x}_0 \neq \mathbf{0} \in K^k$ such that $Q_1'(\mathbf{x}_0) = Q_2'(\mathbf{x}_0) = 0$ and (2.3) holds, contradicting Condition 1. We therefore conclude that Condition 1 implies Condition 4.

We next show that Condition 1 also implies Condition 2. We begin by observing that a change of basis via some invertible matrix M converts the matrices Q_1, Q_2 into $M^t Q_1 M, M^t Q_2 M$, and therefore multiplies $F(x,y)$ by the non-zero constant $(\det M)^2$. Moreover, replacing Q_1, Q_2 by another pair of forms generating the same pencil has the effect of making an invertible linear substitution in the variables x, y occurring in $F(x,y)$. The properties described in Conditions 1 and 2 are clearly unchanged by these two types of transformations. Now, to prove our assertion we will again argue by contradiction. If Condition 2 fails we can make a linear change between Q_1 and Q_2 so that $y^2 | F(x,y)$. Thus $\det(Q_1) = 0$, since this is the coefficient of x^k in $F(x,y)$. However, since we now know that Condition 1 implies Condition 4, we see that $\text{rk}(Q_1) \geq k-1$ whence in fact $\text{rk}(Q_1) = k-1$. After a change of basis we may then write $Q_1(\mathbf{x})$ as

$Q_1'(x_1, \ldots, x_{k-1})$, and $Q_2(\mathbf{x})$ as

$$Q_2'(x_1, \ldots, x_{k-1}) + (c_1x_1 + \ldots + c_{k-1}x_{k-1})x_k + c_kx_k^2,$$

say. One then sees that the coefficient of $x^{k-1}y$ in $\det(xQ_1 + yQ_2)$ must be $\det(Q_1')c_k$. This coefficient must in fact vanish in view of the condition $y^2|F(x, y)$. However $\det(Q_1') \neq 0$ since $\mathrm{rk}(Q_1) = k - 1$, and we therefore deduce that $c_k = 0$. The point $\mathbf{x}_0 = (0, \ldots, 0, 1)$ will therefore satisfy $Q_1'(\mathbf{x}_0) = Q_2(\mathbf{x}_0) = 0$ and also $\nabla Q_1'(\mathbf{x}_0) = \mathbf{0}$. We therefore have a singular point on the variety V, contradicting Condition 1. This suffices to establish our assertion that Condition 1 implies Condition 2.

We next assume that Condition 2 holds and deduce Condition 3. Since the field K is infinite Condition 2 implies that at least one linear combination of Q_1 and Q_2 is nonsingular, and by a linear change between the two forms we may assume that $\det(Q_2) \neq 0$. Such a linear change does not affect the validity or otherwise of Condition 3. For each of the k distinct roots λ_i of the equation $\det(Q_1 - \lambda Q_2) = 0$, there exists an $\mathbf{x}_i \neq 0$, $\mathbf{x}_i \in K^k$, such that

$$Q_1\mathbf{x}_i = \lambda_i Q_2\mathbf{x}_i. \tag{2.4}$$

Note that as the $\mathbf{x}_i$ are eigenvectors for $Q_2^{-1}Q_1$, corresponding to distinct eigenvalues, they are linearly independent, and hence form a basis of K^k. Taking the dot product of equation (2.4) with any basis vector $\mathbf{x}_j$ we obtain

$$\mathbf{x}_j^tQ_1\mathbf{x}_i = \lambda_i\mathbf{x}_j^tQ_2\mathbf{x}_i. \tag{2.5}$$

But the transpose of a real number is itself, and Q_1, Q_2 are symmetric matrices, so

$$\mathbf{x}_j^tQ_1\mathbf{x}_i = (\mathbf{x}_j^tQ_1\mathbf{x}_i)^t = \mathbf{x}_i^tQ_1\mathbf{x}_j = \lambda_j\mathbf{x}_i^tQ_2\mathbf{x}_j = (\lambda_j\mathbf{x}_i^tQ_2\mathbf{x}_j)^t = \lambda_j\mathbf{x}_j^tQ_2\mathbf{x}_i.$$

Thus for any i, j,

$$\lambda_i(\mathbf{x}_j^tQ_2\mathbf{x}_i) = \lambda_j(\mathbf{x}_j^tQ_2\mathbf{x}_i),$$

and so by the assumption that the λ_i are distinct we have

$$\mathbf{x}_j^tQ_2\mathbf{x}_i = 0,$$

for any pair $i \neq j$. Hence by (2.5),

$$\mathbf{x}_j^tQ_1\mathbf{x}_i = 0.$$

This means that the basis $\mathbf{x}_1, \ldots, \mathbf{x}_k$ diagonalizes both matrices simultaneously, as desired. In the notation of Condition 3 we will have $a_i = \mathbf{x}_i^tQ_1\mathbf{x}_i$ and $b_i = \mathbf{x}_i^tQ_2\mathbf{x}_i$ so that $a_i/b_i = \lambda_i$. We therefore see that these ratios are distinct as required. This completes the proof that Condition 2 implies Condition 3.

Finally, we show that Condition 3 implies Condition 1. We may assume that $Q_1 = \mathrm{diag}\,(a_i)$, $Q_2 = \mathrm{diag}\,(b_i)$ have been diagonalized. Let $\mathbf{t} \neq \mathbf{0}$ be any point such that $Q_1(\mathbf{t}) = Q_2(\mathbf{t}) = 0$. Suppose that $\mathrm{rk}(J(\mathbf{t})) < 2$, so that there exists $\lambda \in K \cup \{\infty\}$ such that

$$\nabla Q_1(\mathbf{t}) = \lambda \nabla Q_2(\mathbf{t}). \tag{2.6}$$

We therefore see that $a_i t_i = \lambda b_i t_i$ for all $i = 1, \ldots, k$. Since $\mathbf{t} \neq \mathbf{0}$, there exists at least one index i for which $t_i \neq 0$ and hence we may deduce $\lambda = a_i/b_i$. If there are at least two indices $i \neq j$ with $t_i \neq 0$, $t_j \neq 0$, then $\lambda = a_i/b_i$ and $\lambda = a_j/b_j$, which contradicts the condition that the ratios are distinct. Thus there can only be one nonzero coordinate of $\mathbf{t}$, which we may assume is t_1. Then $Q_1(\mathbf{t}) = a_1 t_1^2$ and $Q_2(\mathbf{t}) = b_1 t_1^2$. But we also assumed that $Q_1(\mathbf{t}) = Q_2(\mathbf{t}) = 0$, and since a_1 and b_1 cannot both vanish in Condition 3, we obtain a contradiction. Hence Condition 3 implies Condition 1. This completes the proof of Proposition 2.1.

2.2 Definition of the good and bad primes

Recall from Proposition 2.1 that under the assumption of Condition 1, the determinant form F has distinct linear factors over $\overline{\mathbb{Q}}$. In particular, if we set

$$D_F := \mathrm{Disc}(F),$$

then D_F is a non-zero rational integer. Furthermore, if we write K for the splitting field for F over $\mathbb{Q}$, then we can factor F as

$$F(x, y) = c^{-1} \prod_{i=1}^{k} (\lambda_i x - \mu_i y)$$

with $c \in \mathbb{N}$ and $\lambda_i, \mu_i \in \mathcal{O}_K$.

Definition 1 *We shall say that a prime p is "bad" if*

$$p \mid 2cD_F \prod_{\sigma} \prod_{1 \leq i < j \leq k} (\lambda_i \mu_j - \lambda_j \mu_i)^{\sigma}, \tag{2.7}$$

where σ runs over the Galois automorphisms of $K/\mathbb{Q}$. Otherwise we shall say that p is "good."

It is an immediate consequence of this definition that the set of bad primes is finite, and is determined by the original forms Q_1 and Q_2. Moreover, if p is good, then the system $Q_1 = Q_2 = 0$ is nonsingular over $\overline{\mathbb{F}_p}$, in the sense that Condition 1 holds relative to $\overline{\mathbb{F}_p}$. For indeed, if this system is singular over $\overline{\mathbb{F}_p}$ (with p odd), then Condition 1 and hence Condition 2 fails relative to $\overline{\mathbb{F}_p}$, so that $D_F = 0$ in $\overline{\mathbb{F}_p}$, whence p satisfies (2.7) and hence is bad.

Similarly, we will later call upon the following local version of Condition 4:

Lemma 2.1 *If $\mathrm{rk}(a_1 Q_1 + a_2 Q_2) \leq k - 2$ over $\mathbb{F}_p$ for some $a_1, a_2 \in \mathbb{Z}$ with $(a_1, a_2, p) = 1$, then p is bad.*

To establish this we note that if p is odd, the existence of such a_1, a_2 would mean that Condition 4 fails for $K = \overline{\mathbb{F}_p}$. By Proposition 2.1, Condition 2 also fails for $K = \overline{\mathbb{F}_p}$, and hence $D_F = 0$ in $K = \overline{\mathbb{F}_p}$. The lemma then follows.

2.3 Definition of Type I and Type II primes

In our consideration of the singular series associated to a given pair (n_1, n_2), we will require an affine smoothness condition. Given any pair $(n_1, n_2) \in \mathbb{Z}^2$, and any prime p, set

$$V_p(n_1, n_2) = \{\mathbf{x} \in \overline{\mathbb{F}_p}^k : Q_1(\mathbf{x}) = n_1, Q_2(\mathbf{x}) = n_2 \text{ in } \overline{\mathbb{F}_p}\}. \tag{2.8}$$

Definition 2 *We will say that a prime p is of "Type I" with respect to a fixed pair of values (n_1, n_2) if p is good and $V_p(n_1, n_2)$ is nonsingular over $\overline{\mathbb{F}_p}$, in the sense that $\Delta(\mathbf{x}) \neq 0$ in $\overline{\mathbb{F}_p}$, for all $\mathbf{x} \in V_p(n_1, n_2)$. We will say that a prime p is of "Type II" with respect to (n_1, n_2) if p is good but p is not of Type I.*

It is worth remarking that while the distinction between good and bad primes is completely independent of any values (n_1, n_2), the distinction between Type I and Type II primes is always with respect to a fixed pair (n_1, n_2). Note that the condition that p is a Type I prime is a local version of the requirement that the Jacobian matrix $J(\mathbf{x})$ be full rank. On the other hand, if p is a Type II prime, there exists $\mathbf{x}_0 \in V_p(n_1, n_2)$ for which there is a pair α, β with $(\alpha, \beta) \neq (0, 0)$ in $\mathbb{F}_p$ that satisfies

$$\alpha \nabla Q_1(\mathbf{x}_0) + \beta \nabla Q_2(\mathbf{x}_0) \equiv 0 \ (\text{mod } p). \tag{2.9}$$

Such an $\mathbf{x}_0$ must be nonzero, since p is good.

In order to prove the convergence of the singular series it will be crucial that for any pair (n_1, n_2) we consider, the number of Type II primes with respect to (n_1, n_2) is finite.

Lemma 2.2 *Given n_1, n_2 (not both zero) such that $n_2 Q_1(\mathbf{x}) - n_1 Q_2(\mathbf{x})$ is globally nonsingular, finitely many primes are of Type II with respect to n_1, n_2. Indeed, any Type II prime must satisfy $p | F(n_2, -n_1)$.*

Suppose p is a Type II prime with respect to n_1, n_2 so that there exists a non-zero point $\mathbf{x}_0 \in V_p(n_1, n_2)$ for which (2.9) holds. Then taking the dot product of $\mathbf{x}_0$ with (2.9) yields

$$2\alpha Q_1(\mathbf{x}_0) + 2\beta Q_2(\mathbf{x}_0) \equiv 0 \ (\text{mod } p). \tag{2.10}$$

But by assumption $\mathbf{x}_0$ lies on the variety $Q_1(\mathbf{x}_0) - n_1 \equiv Q_2(\mathbf{x}_0) - n_2 \equiv 0$, so that (2.10) implies

$$2\alpha n_1 + 2\beta n_2 \equiv 0 \ (\text{mod } p).$$

Recall that 2 is a bad prime, whereas Type II primes are good primes, so $p \neq 2$. In the case that $p | \gcd(n_1, n_2)$, we have $p | F(n_2, -n_1)$ and we are finished. Otherwise, we may assume that $p \nmid n_1$, say, and solve for $\alpha \equiv -\beta n_2 \bar{n}_1$. Hence in (2.9),

$$-\beta n_2 \bar{n}_1 \nabla Q_1(\mathbf{x}_0) + \beta \nabla Q_2(\mathbf{x}_0) \equiv 0 \ (\text{mod } p).$$

If $p | \beta$ then $\alpha \equiv -\beta n_2 \bar{n}_1 \equiv 0$ (mod p), contradicting the fact that $(\alpha, \beta) \neq (0, 0)$. Hence $p \nmid \beta$ and we conclude that

$$n_2 \nabla Q_1(\mathbf{x}_0) \equiv n_1 \nabla Q_2(\mathbf{x}_0) \ (\text{mod } p). \tag{2.11}$$

Regarding Q_1, Q_2 as matrices, (2.11) is equivalent to the statement

$$(n_2Q_1 - n_1Q_2)\mathbf{x}_0 \equiv 0 \ (\mathrm{mod}\ p). \tag{2.12}$$

However by assumption $\mathbf{x}_0 \not\equiv 0 \ (\mathrm{mod}\ p)$, whence (2.12) implies that p divides $\det(n_2Q_1 - n_1Q_2)$. Given a pair of values n_1, n_2, there are finitely many such primes p, unless the determinant vanishes as an element of $\mathbb{Z}$. However this is precisely the condition we have ruled out by assuming that $n_2Q_1(\mathbf{x}) - n_1Q_2(\mathbf{x})$ is globally nonsingular so that $\det(n_2Q_1 - n_1Q_2) \neq 0$. This proves the lemma.

We remark that when $n_2Q_1 - n_1Q_2$ is globally singular there may be infinitely many primes of Type II. For example, suppose that Q_1 is itself singular, so that $\nabla Q_1(\mathbf{x}_0) = 0$ for some non-zero integer vector $\mathbf{x}_0$. Taking $n_1 = 0$ and $n_2 = Q_2(\mathbf{x}_0)$ we then see that $n_2Q_1(\mathbf{x}) - n_1Q_2(\mathbf{x})$ is globally singular and $\mathbf{x}_0$ is a singular point of $V_p(n_1, n_2)$ for every prime p. Thus in our consideration of the major arcs, we restrict to those pairs (n_1, n_2) for which $\det(n_2Q_1 - n_1Q_2) \neq 0$, which is the condition $F(n_2, -n_1) \neq 0$ in Theorem 1.1.

In connection with Theorem 1.7 we note that if $(n_1, n_2) = (0, 0)$ there are no Type I primes, since $\mathbf{x} = \mathbf{0}$ is always a singular point on $V_p(0, 0)$.

2.4 Bounds for eigenvalues

Given any pair $(\nu_1, \nu_2) \in \mathbb{R}^2$, Condition 4 allows that $\underline{\nu} \cdot \underline{Q}$ may be of rank $k-1$ and hence $F(\nu_1, \nu_2)$ may vanish. Nevertheless, as we prove in the following lemma, under Condition 4, at most one of the eigenvalues of $\underline{\nu} \cdot \underline{Q}$ may be small.

Lemma 2.3 *Let $\nu^* = \max(|\nu_1|, |\nu_2|)$, and let $\rho_1, \ldots, \rho_k$ denote the eigenvalues associated to $\underline{\nu} \cdot \underline{Q}$, ordered so that $|\rho_1| \leq \cdots \leq |\rho_k|$. Then, under Condition 4, we have*

$$|\rho_2| \gg \nu^* \quad \textit{and} \quad |\rho_k| \ll \nu^*.$$

We may assume that $|\nu_2| \leq 1 = |\nu_1|$ (by normalizing and possibly interchanging the roles of ν_1, ν_2, Q_1, Q_2). We therefore study a linear combination of the type $Q_1 + \lambda Q_2$ with $|\lambda| \leq 1$. Then

$$|\rho_k| \leq ||Q_1 + \lambda Q_2|| \ll_{Q_1,Q_2} 1,$$

so that it remains to prove that

$$|\rho_2| \gg_{Q_1,Q_2} 1.$$

We will argue by contradiction. It will be convenient to write $\rho_i(Q)$ to denote the i-th smallest eigenvalue of a real quadratic form Q. We will then assume for a contradiction that for any positive integer n there is a $\lambda_n \in [-1, 1]$ for which $|\rho_2(Q_1 + \lambda_n Q_2)| \leq 1/n$. We can diagonalize $Q_1 + \lambda_n Q_2$ using an orthogonal matrix M_n, say, so that $M_n^T(Q_1 + \lambda_n Q_2)M_n = \mathrm{diag}(\rho_1^{(n)}, \ldots, \rho_k^{(n)})$, say, with

$$|\rho_1^{(n)}| \leq \ldots \leq |\rho_k^{(n)}|.$$

By construction, both $\rho_1^{(n)}$ and $\rho_2^{(n)}$ tend to zero as n goes to infinity. The set of orthogonal matrices of order k is compact, as is the interval $[-1,1]$. Hence by choosing a suitable subsequence we can suppose that $\lambda_n \to \lambda$ and that $M_n \to M$, say. We then see that $M^T(Q_1+\lambda Q_2)M = \mathrm{diag}(\rho_1,\ldots,\rho_k)$, say, with $\rho_1 = \rho_2 = 0$. This contradicts Condition 4 and hence proves the lemma.

3 Bounds for oscillatory integrals

In considering both the major and minor arcs, we will require estimates for oscillatory integrals of the form

$$I(\mathcal{Q};\boldsymbol{\lambda}) = \int_{\mathbb{R}^n} e(\mathcal{Q}(\mathbf{u}) - \boldsymbol{\lambda}\cdot\mathbf{u})w(\mathbf{u})d\mathbf{u}, \tag{3.1}$$

where for the moment $\boldsymbol{\lambda} \in \mathbb{R}^n$, $\mathcal{Q}$ is any real quadratic form in n variables and w is any smooth weight on $\mathbb{R}^n$ supported in $[-1,1]^n$.

Lemma 3.1 *Let $\rho_1,\ldots,\rho_n$ be the eigenvalues associated to the quadratic form $\mathcal{Q}$. If $|\boldsymbol{\lambda}| \geq 4||\mathcal{Q}||$, then*

$$I(\mathcal{Q};\boldsymbol{\lambda}) \ll_{M,w} |\boldsymbol{\lambda}|^{-M}, \tag{3.2}$$

for any $M \geq 1$. Moreover

$$|I(\mathcal{Q};\boldsymbol{\lambda})| \ll_w \prod_{i=1}^n \min(1, \frac{1}{|\rho_i|^{1/2}}). \tag{3.3}$$

We will estimate $I(\mathcal{Q};\boldsymbol{\lambda})$ by the method of stationary phase. Note first that if $|\boldsymbol{\lambda}| \geq 4||\mathcal{Q}||$, then

$$|\nabla_u\{\mathcal{Q}(\mathbf{u}) - \boldsymbol{\lambda}\cdot\mathbf{u}\}| = |\nabla_u\mathcal{Q}(\mathbf{u}) - \boldsymbol{\lambda}| \geq |\boldsymbol{\lambda}|/2$$

on $\mathrm{supp}(w)$, since $|\nabla_u\mathcal{Q}(\mathbf{u})| \leq 2||\mathcal{Q}|| \leq |\boldsymbol{\lambda}|/2$. On the other hand, for any multi-index α with $|\alpha| = 2$ we have,

$$|\partial_u^\alpha\{\mathcal{Q}(u) - \boldsymbol{\lambda}\cdot u\}| = |\partial_u^\alpha\mathcal{Q}(u)| \leq 2C||\mathcal{Q}|| \leq \frac{C}{2}|\boldsymbol{\lambda}|,$$

for some constant C depending on n. Moreover, when $|\alpha| \geq 3$ the left-hand side vanishes. Thus an application of the first derivative test for an infinitely differentiable function in high dimensions, as presented in Lemma 10 of [7], shows that $I(\mathcal{Q};\boldsymbol{\lambda}) \ll |\boldsymbol{\lambda}|^{-M}$, for any $M \geq 1$, which proves (3.2).

To prove our second estimate we will apply the second derivative test. Let R be an orthogonal transformation such that $R^t\mathcal{Q}R = D$, where $D = \mathrm{diag}\{\rho_1,\ldots,\rho_n\}$. Under this change of variables,

$$I(\mathcal{Q};\boldsymbol{\lambda}) = \int_{\mathbb{R}^n} e(\sum_{i=1}^n \rho_i u_i^2 - (R^t\boldsymbol{\lambda})\cdot\mathbf{u})w(R\mathbf{u})d\mathbf{u}.$$

Next, we apply the following lemma, in order to remove the presence of the weight w.

Lemma 3.2 *Let f, w be smooth functions of $\mathbb{R}^n$ and suppose that w is supported on $[-1,1]^n$. Then*

$$|\int_{\mathbb{R}^n} f(\mathbf{x})w(\mathbf{x})d\mathbf{x}| \leq \left\{\int_{\mathbb{R}^n} |\hat{w}(\mathbf{y})|d\mathbf{y}\right\} \sup_{\mathbf{y}\in\mathbb{R}^n} \left|\int_{[-1,1]^n} f(\mathbf{x})e(\mathbf{x}\cdot\mathbf{y})d\mathbf{x}\right|,$$

where $\hat{w}$ is the Fourier transform of w.

To prove the lemma we express $w(\mathbf{x})$ in terms of its Fourier transform as

$$w(\mathbf{x}) = \int_{\mathbb{R}^n} \hat{w}(\mathbf{y})e(\mathbf{x}\cdot\mathbf{y})d\mathbf{y},$$

where $\hat{w}$ is smooth and of rapid decay. Using an interchange in the orders of integration we then find that

$$\begin{aligned}\int_{\mathbb{R}^n} f(\mathbf{x})\chi_{[-1,1]^n}(\mathbf{x})w(\mathbf{x})d\mathbf{x} &= \int_{\mathbb{R}^n} f(\mathbf{x})\chi_{[-1,1]^n}(\mathbf{x})\int_{\mathbb{R}^n} \hat{w}(\mathbf{y})e(\mathbf{x}\cdot\mathbf{y})d\mathbf{y}d\mathbf{x} \\ &= \int_{\mathbb{R}^n} \hat{w}(\mathbf{y})\int_{\mathbb{R}^n} f(\mathbf{x})\chi_{[-1,1]^n}(\mathbf{x})e(\mathbf{x}\cdot\mathbf{y})d\mathbf{x}d\mathbf{y},\end{aligned}$$

and the lemma follows.

Continuing our treatment of Lemma 3.1, we now see that we can bound $I(\mathcal{Q};\boldsymbol{\lambda})$ using an n-fold product of one-dimensional integrals:

$$|I(\mathcal{Q};\boldsymbol{\lambda})| \ll_w \prod_{i=1}^n \sup_{y\in\mathbb{R}} \left|\int_{-1}^1 e(\rho_i u^2 + yu)du\right|.$$

Applying the second derivative test, each one-dimensional integral is bounded by $|\rho_i|^{-1/2}$. Alternatively we may use the trivial bound for the integral, and clearly (3.3) follows.

We will apply Lemma 3.1 to the situation in which $\mathcal{Q}$ takes the shape $\underline{\nu}\cdot\underline{F} = \nu_1 F_1 + \nu_2 F_2$ for two fixed quadratic forms F_1, F_2. In this case we write

$$I(\underline{\nu}\cdot\underline{F};\boldsymbol{\lambda}) = \int_{\mathbb{R}^n} e(\underline{\nu}\cdot\underline{F}(\mathbf{u}) - \boldsymbol{\lambda}\cdot\mathbf{u})w(\mathbf{u})d\mathbf{u}.$$

We now employ Lemma 3.1 to estimate the average of $|I(\underline{\nu}\cdot\underline{F};\boldsymbol{\lambda})|$ over dyadic ranges of ν_1, ν_2, using the notation $\iint_{\{\phi_1,\phi_2\}}$ to denote integration over the region

$$([-2\phi_1, -\phi_1]\cup[\phi_1, 2\phi_1])\times([-2\phi_2, -\phi_2]\cup[\phi_2, 2\phi_2])$$

when $\phi_1, \phi_2 > 0$.

Lemma 3.3 *Let $\phi^* = \max(\phi_1, \phi_2)$. Take $F_1 = Q_1$, $F_2 = Q_2$ to be the original quadratic forms acting on $\mathbb{Z}^k$. Then*

$$\iint_{\{\phi_1,\phi_2\}} |I(\underline{\nu}\cdot\underline{F};\boldsymbol{\lambda})|d\underline{\nu} \ll \min((\phi^*)^2, (\phi^*)^{2-k/2}).$$

This will be applied to prove the convergence of the singular integral on the major arcs. When we consider the oscillatory integral on the minor arcs we will need a version related to a different choice of quadratic forms acting on $\mathbb{Z}^{2k}$:

Lemma 3.4 *Let* $\phi^* = \max(\phi_1, \phi_2)$. *Take*

$$F_1(\mathbf{x}_1, \mathbf{x}_2) = Q_1(\mathbf{x}_1) - Q_1(\mathbf{x}_2), \quad F_2(\mathbf{x}_1, \mathbf{x}_2) = Q_2(\mathbf{x}_1) - Q_2(\mathbf{x}_2),$$

for $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{Z}^k$. *Then*

$$\iint_{\{\phi_1,\phi_2\}} |I(\underline{\nu} \cdot \underline{F}; \boldsymbol{\lambda})| d\underline{\nu} \ll \begin{cases} (\phi^*)^2, & \phi^* \leq 1, \\ (\phi^*)^{2-k}(1 + \log \phi^*), & \phi^* \geq 1. \end{cases}$$

3.1 Proof of Lemmas 3.3 and 3.4

For each fixed $\underline{\nu} = (\nu_1, \nu_2)$, let $\nu^* = \max(|\nu_1|, |\nu_2|)$ and let $\rho_1, \ldots, \rho_k$ be the eigenvalues associated to the quadratic form $\underline{\nu} \cdot \underline{Q}$, ordered so that $|\rho_1| \leq \cdots \leq |\rho_k|$. Recall from Lemma 2.3 that for each fixed $\underline{\nu}$, at most one eigenvalue of $\underline{\nu} \cdot \underline{Q}$ may be of smaller order than ν^*, and that for $i = 2, \ldots, k$ we have $|\rho_i| \approx \nu^*$, where the implied constant depends on the initial forms Q_1, Q_2. Applying this in (3.3), it follows that

$$|I(\underline{\nu} \cdot \underline{F}; \boldsymbol{\lambda})| \ll \min(1, (\frac{1}{\nu^*})^{\frac{k-1}{2}}) \min(1, \frac{1}{|\rho_1|^{1/2}}). \tag{3.4}$$

Recalling the definition $F(\nu_1, \nu_2) = \det(\nu_1 Q_1 + \nu_2 Q_2)$, it follows that

$$\rho_1 \cdots \rho_k = F(\nu_1, \nu_2).$$

Since in the range of the integral we have $|\underline{\nu}| \ll \phi^*$, it follows in particular that $\rho_i \ll \phi^*$ for $i = 2, \ldots, k$, and hence

$$|\rho_1| \gg \frac{|F(\nu_1, \nu_2)|}{(\phi^*)^{k-1}}.$$

We therefore deduce that

$$\begin{aligned} &\iint_{\{\phi_1,\phi_2\}} |I(\underline{\nu} \cdot \underline{F}; \boldsymbol{\lambda})| d\underline{\nu} \\ &\ll \min(1, (\frac{1}{\phi^*})^{\frac{k-1}{2}}) \iint_{\{\phi_1,\phi_2\}} \min(1, \left(\frac{(\phi^*)^{k-1}}{|F(\nu_1, \nu_2)|}\right)^{1/2}) d\underline{\nu}. \end{aligned} \tag{3.5}$$

According to Condition 3 we can factor $F(\nu_1, \nu_2)$ over $\mathbb{C}$ as

$$F(\nu_1, \nu_2) = \prod_{i=1}^{k} (a_i \nu_1 - b_i \nu_2), \tag{3.6}$$

with distinct ratios a_i/b_i in $\mathbb{C} \cup \{\infty\}$. We will fix an admissible choice for the coefficients a_i, b_i once and for all. Write $\psi_i = a_i \nu_1 - b_i \nu_2$ and order the indices so that

$$|\psi_1| \leq |\psi_2| \leq \cdots. \tag{3.7}$$

Since
$$\nu_1 = \frac{b_2\psi_1 - b_1\psi_2}{a_1b_2 - a_2b_1}$$
and similarly for ν_2, we conclude that $\nu^* \ll |\psi_2|$, so that $|\psi_2| \gg \phi^*$ and hence
$$|F(\nu_1,\nu_2)| \gg (\phi^*)^{k-1}|\psi_1|. \tag{3.8}$$
Certainly $|\psi_1| \geq \min_i |a_i\nu_1 - b_i\nu_2|$. Thus,
$$\left(\frac{(\phi^*)^{k-1}}{|F(\nu_1,\nu_2)|}\right)^{1/2} \leq \frac{1}{\min_i |a_i\nu_1 - b_i\nu_2|^{1/2}} \leq \sum_{1\leq i\leq k} \frac{1}{|a_i\nu_1 - b_i\nu_2|^{1/2}}.$$
Integrating over the appropriate region gives us an upper bound for the integral in (3.5):
$$\begin{aligned}&\iint_{\{\phi_1,\phi_2\}} \min(1, \left(\frac{(\phi^*)^{k-1}}{|F(\nu_1,\nu_2)|}\right)^{1/2})d\underline{\nu} \\ &\qquad\ll \sum_{1\leq i\leq k} \iint_{\{\phi_1,\phi_2\}} \min(1, \frac{1}{|a_i\nu_1 - b_i\nu_2|^{1/2}})d\underline{\nu}.\end{aligned}$$
For each fixed index i, we may exchange the roles of Q_1 and Q_2 if necessary so that $a_i \neq 0$, and set $c_i = b_i/a_i$. Then the contribution of the integral corresponding to the index i is majorized by
$$\iint_{\{\phi_1,\phi_2\}} \min(1, \frac{1}{|\nu_1 - c_i\nu_2|^{1/2}})d\underline{\nu},$$
which after the change of variables $v_1 = \nu_1 - c_i\nu_2$, $v_2 = \nu_2$, is the sum of four integrals of the type
$$\begin{aligned}\int_{\phi_2}^{2\phi_2}\int_{\phi_1 - c_iv_2}^{2\phi_1 - c_iv_2} \min(1, \frac{1}{|v_1|^{1/2}})dv_1dv_2 &\leq 2\phi^* \int_0^{(2+|c_i|)\phi^*} \min(1, \frac{1}{v^{1/2}})dv \\ &\ll \phi^* \min(\phi^*, (\phi^*)^{1/2}).\end{aligned}$$
Incorporating this upper bound in (3.5) completes the proof of Lemma 3.3.

Lemma 3.4 is proved in the same manner as Lemma 3.3, with one important difference. Again let $\rho_1, \rho_2, \ldots, \rho_k$ be the eigenvalues of $\underline{\nu}\cdot\underline{Q}$ acting on $\mathbb{Z}^k$, where $\underline{Q} = (Q_1, Q_2)$. Then the particular choice of $\underline{F}$ in Lemma 3.4 means that the eigenvalues of $\underline{\nu}\cdot\underline{F}$ occur in pairs, as $\pm\rho_1, \pm\rho_2, \ldots, \pm\rho_k$. In particular, *two* of the eigenvalues can now be small. However, this is easy to handle, as we simply replace (3.4) with
$$|I(\underline{\nu}\cdot\underline{F}, \boldsymbol{\lambda})| \ll \min(1, (\frac{1}{\nu^*})^{k-1}) \min(1, \frac{1}{|\rho_1|}),$$
and the argument proceeds along the same lines as in the previous case.

3.2 The singular integral

We end this section by considering the singular integral, defined by

$$\mathcal{J}_w(\underline{\mu}) = \iint_{\mathbb{R}^2} \int_{\mathbb{R}^k} e(\underline{\theta} \cdot (\underline{Q}(\mathbf{x}) - \underline{\mu})) w(\mathbf{x}) d\mathbf{x} d\theta_1 d\theta_2. \tag{3.9}$$

We also define the truncated singular integral as

$$\mathcal{J}_w(\underline{\mu}; R) = \int_{-R}^{R} \int_{-R}^{R} \int_{\mathbb{R}^k} e(\underline{\theta} \cdot (\underline{Q}(\mathbf{x}) - \underline{\mu})) w(\mathbf{x}) d\mathbf{x} d\theta_1 d\theta_2, \tag{3.10}$$

so that $\mathcal{J}_w(\underline{\mu}) = \lim_{R\to\infty} \mathcal{J}_w(\underline{\mu}; R)$, if the limit exists. We now prove the following proposition.

Proposition 3.1 *For $k \geq 5$, the singular integral $\mathcal{J}_w(\underline{\mu})$ is absolutely convergent in the sense that*

$$\iint_{\mathbb{R}^2} \left| \int_{\mathbb{R}^k} e(\underline{\theta} \cdot (\underline{Q}(\mathbf{x}) - \underline{\mu})) w(\mathbf{x}) d\mathbf{x} \right| d\theta_1 d\theta_2 < \infty.$$

Moreover it is bounded uniformly in $\underline{\mu}$. The rate of convergence may be quantified for $R \geq 2$ as

$$|\mathcal{J}_w(\underline{\mu}) - \mathcal{J}_w(\underline{\mu}; R)| \ll R^{\frac{4-k}{2}} \log R.$$

We first verify that $\mathcal{J}_w(\underline{\mu})$ converges. Letting $\theta^* = \max(|\theta_1|, |\theta_2|)$, we may write

$$|\mathcal{J}_w(\underline{\mu}) - \mathcal{J}_w(\underline{\mu}; R)| \ll \iint_{\theta^* > R} |I(\underline{\theta})| d\underline{\theta},$$

where

$$I(\underline{\theta}) = \int_{\mathbb{R}^k} e(\underline{\theta} \cdot \underline{Q}(\mathbf{x})) w(\mathbf{x}) d\mathbf{x}. \tag{3.11}$$

Lemma 3.3 implies that

$$\iint_{\{\phi_1, \phi_2\}} |I(\underline{\theta})| d\underline{\theta} \ll (\phi^*)^{\frac{4-k}{2}}, \tag{3.12}$$

for any dyadic range $\{\phi_1, \phi_2\}$ with $\phi^* = \max(\phi_1, \phi_2) \geq 1$. Since $I(\underline{\theta}) \ll 1$ we also have

$$\iint_{\{\phi_1, \phi_2\}} |I(\underline{\theta})| d\underline{\theta} \ll \phi_1 \phi_2.$$

We now sum over dyadic ranges for ϕ_1 and ϕ_2, using this latter bound when $\min(\phi_1, \phi_2) \leq (\phi^*)^{-k}$, and (3.12) otherwise. This shows that

$$\begin{aligned} \iint_{\theta^* > R} |I(\underline{\theta})| d\underline{\theta} &\ll \sum_{2^n > R} \left\{ \sum_{\substack{m \in \mathbb{Z} \\ m \leq -kn}} 2^m . 2^n + \sum_{\substack{m \in \mathbb{Z} \\ -kn < m \leq n}} (2^n)^{(4-k)/2} \right\} \\ &\ll \sum_{2^n > R} \left\{ 2^{n(1-k)} + n (2^n)^{(4-k)/2} \right\} \\ &\ll R^{\frac{4-k}{2}} (1 + \log R). \end{aligned} \tag{3.13}$$

Thus $\mathcal{J}_w(\underline{\mu}; R)$ converges absolutely for $k \geq 5$. A similar argument shows that $\mathcal{J}_w(\underline{\mu})$ is uniformly bounded with respect to $\underline{\mu}$.

Our second major result on the singular integral gives an interpretation in terms of the density of real solutions of $\underline{Q}(\mathbf{x}) = \underline{\mu}$.

Proposition 3.2 *Let $k \geq 5$. Then*

$$\varepsilon^{-2} \int_{\max |Q_i(\mathbf{x}) - \mu_i| \leq \varepsilon} w(\mathbf{x}) \left(1 - \frac{|Q_1(\mathbf{x}) - \mu_1|}{\varepsilon}\right) \left(1 - \frac{|Q_2(\mathbf{x}) - \mu_2|}{\varepsilon}\right) d\mathbf{x}$$

tends to $\mathcal{J}_w(\underline{\mu})$ as $\varepsilon \to 0$.

We remark for later reference that Propositions 3.1 and 3.2 hold even when $\underline{\mu} = \underline{0}$.

For the proof we define

$$K_\varepsilon(\underline{\theta}) = \left(\frac{\sin \pi\varepsilon\theta_1}{\pi\varepsilon\theta_1}\right)^2 \left(\frac{\sin \pi\varepsilon\theta_2}{\pi\varepsilon\theta_2}\right)^2.$$

Then $K_\varepsilon(\underline{\theta}) = 1 + O(\varepsilon^{3/2})$ if $\max(|\theta_1|, |\theta_2|) < \varepsilon^{-1/4}$ and $K_\varepsilon(\underline{\theta}) \ll 1$ in general. It follows that

$$\begin{aligned} &\iint_{\max(|\theta_1|,|\theta_2|)<\varepsilon^{-1/4}} |K_\varepsilon(\underline{\theta}) - 1|.|I(\underline{\theta})| d\underline{\theta} \\ &\qquad \ll \varepsilon^{3/2} \iint_{\max(|\theta_1|,|\theta_2|)<\varepsilon^{-1/4}} |I(\underline{\theta})| d\underline{\theta} \\ &\qquad \ll \varepsilon, \end{aligned}$$

since $I(\underline{\theta}) \ll 1$. Similarly we have

$$\begin{aligned} \iint_{\max(|\theta_1|,|\theta_2|)\geq\varepsilon^{-1/4}} |K_\varepsilon(\underline{\theta}) - 1|.|I(\underline{\theta})| d\underline{\theta} &\ll \iint_{\max(|\theta_1|,|\theta_2|)\geq\varepsilon^{-1/4}} |I(\underline{\theta})| d\underline{\theta} \\ &\ll \varepsilon^{\frac{k-4}{8}} (1 + \log(\varepsilon^{-1/4})), \end{aligned}$$

by (3.13). We therefore deduce that

$$\iint_{\mathbb{R}^2} |K_\varepsilon(\underline{\theta}) - 1|.|I(\underline{\theta})| d\theta \to 0$$

as $\varepsilon \to 0$, provided that $k \geq 5$. It then follows that

$$\lim_{\varepsilon \to 0} \iint_{\mathbb{R}^2} K_\varepsilon(\underline{\theta}) I(\underline{\theta}) e(-\underline{\theta} \cdot \underline{\mu}) d\underline{\theta} = \mathcal{J}_w(\underline{\mu})$$

when $k \geq 5$.

However

$$\iint_{\mathbb{R}^2} K_\varepsilon(\underline{\theta}) I(\underline{\theta}) e(-\underline{\theta} \cdot \underline{\mu}) d\underline{\theta} = \int_{\mathbb{R}^k} w(\mathbf{x}) L(\underline{Q}(\mathbf{x}) - \underline{\mu}) d\mathbf{x},$$

with

$$L(\underline{\lambda}) = \iint_{\mathbb{R}^2} K_\varepsilon(\underline{\theta}) e(\underline{\theta} \cdot \underline{\lambda}) d\underline{\theta}.$$

We can evaluate this last integral as a product of two one-dimensional integrals of the form

$$\int_{-\infty}^{\infty} \left(\frac{\sin \pi \varepsilon t}{\pi \varepsilon t} \right)^2 e(t\lambda) dt = \begin{cases} \varepsilon^{-1}(1 - \varepsilon^{-1}|\lambda|), & |\lambda| \le \varepsilon, \\ 0, & |\lambda| > \varepsilon, \end{cases}$$

and the proposition follows.

4 Exponential sums: the major arcs

Let

$$S_q(\underline{a}) = \sum_{\mathbf{x} \ (\mathrm{mod}\ q)} e_q(\underline{a} \cdot \underline{Q}(\mathbf{x})),$$

$$S_q(\underline{a}; \underline{n}) = S_q(\underline{a}) e_q(-\underline{a} \cdot \underline{n}),$$

and

$$T(\underline{n}; q) = \sum_{\substack{1 \le a_1, a_2 \le q \\ (a_1, a_2, q) = 1}} S_q(\underline{a}; \underline{n}). \tag{4.1}$$

We will require estimates for $T(\underline{n}; q)$ in order to show that the singular series converges, as well as to give a precise rate of convergence and a lower bound for the singular series. The work on $T(\underline{n}; q)$ follows standard arguments and is less technical than the methods we will use for exponential sums encountered in the minor arcs, although it still requires us to make a distinction between Type I and Type II primes with respect to each fixed value (n_1, n_2), as defined in Section 2.3. Note that $T(\underline{n}; q)$ is a multiplicative function with respect to q: namely if $q = q_1 q_2$ with $(q_1, q_2) = 1$, then

$$T(\underline{n}; q) = T(\underline{n}; q_1) T(\underline{n}; q_2).$$

Thus it is sufficient to consider the case where $q = p^e$.

We first note that the following simple relation holds, for all primes p:

Lemma 4.1 *For any prime p and any $e \ge 1$ we have*

$$T(\underline{n}; p^e) = p^{2e} N(\underline{n}; p^e) - p^{k+2(e-1)} N(\underline{n}; p^{e-1}), \tag{4.2}$$

where

$$N(\underline{n}; q) = \# V_q(n_1, n_2) = \#\{\mathbf{x} \ (mod\ q) : Q_1(\mathbf{x}) \equiv n_1, Q_2(\mathbf{x}) \equiv n_2 \ (mod\ q)\}.$$

We can simply write

$$T(\underline{n}; p^e) = \sum_{1 \le a_1, a_2 \le p^e} S_{p^e}(\underline{a}; \underline{n}) - \sum_{1 \le a_1, a_2 \le p^{e-1}} S_{p^e}(p\underline{a}; \underline{n}) \tag{4.3}$$

and observe that in the second term,

$$S_{p^e}(p\underline{a};\underline{n}) = \sum_{\mathbf{x} \pmod{p^e}} e_{p^{e-1}}(\underline{a}\cdot\underline{Q}(\mathbf{x}) - \underline{a}\cdot\underline{n}) = p^k S_{p^{e-1}}(\underline{a};\underline{n}). \tag{4.4}$$

Next we note that

$$\begin{aligned}\sum_{1\le a_1,a_2\le p^e} S_{p^e}(\underline{a};\underline{n}) &= \sum_{\mathbf{x} \pmod{p^e}} \sum_{1\le a_1,a_2\le p^e} e_{p^e}(\underline{a}\cdot(\underline{Q}(\mathbf{x})-\underline{n})) \\ &= p^{2e}N(\underline{n};p^e). \end{aligned} \tag{4.5}$$

Inserting (4.4) in (4.3) and applying the representation (4.5) to both resulting terms proves the lemma.

Moreover, we note that the sum $\sum_e p^{-ek}T(\underline{n};p^e)$ telescopes:

Lemma 4.2 *For any prime p,*

$$1+\sum_{e=1}^{E} p^{-ek}T(\underline{n};p^e) = p^{-E(k-2)}N(\underline{n};p^E).$$

For in fact,

$$\begin{aligned}\sum_{e=1}^{E} p^{-ek}T(\underline{n};p^e) &= \sum_{e=1}^{E} p^{-e(k-2)}N(\underline{n};p^e) - \sum_{e=1}^{E} p^{-(k-2)(e-1)}N(\underline{n};p^{e-1}) \\ &= p^{-E(k-2)}N(\underline{n};p^E) + \sum_{e=1}^{E-1} p^{-e(k-2)}N(\underline{n};p^e) \\ &\qquad - \sum_{e=1}^{E-1} p^{-e(k-2)}N(\underline{n};p^e) - N(\underline{n};1) \\ &= p^{-E(k-2)}N(\underline{n};p^E) - 1.\end{aligned}$$

Thus the key to understanding $T(\underline{n};p^e)$ is bounding $N(\underline{n};p^e)$. We would expect that $N(\underline{n};q)$ is of order q^{k-2}, up to a smaller error term, since there are q^k choices of $\mathbf{x}$ modulo q, and the probability that a certain value (n_1,n_2) is taken by $(Q_1(\mathbf{x}),Q_2(\mathbf{x}))$ is q^{-2}. In the case of Type I primes, $V_p(n_1,n_2)$ is smooth and we can apply Deligne's estimates to get a good error term for $N(\underline{n};p)$. We can then control $N(\underline{n};p^e)$ by lifting solutions modulo p to solutions modulo p^e. In the case of Type II primes, we obtain a slightly worse error term for prime moduli, and we avoid $N(\underline{n};p^e)$ for prime power moduli.

Proposition 4.1 *For all good primes (and hence primes of Type I or Type II) we have*

$$N(\underline{n};p) = p^{k-2} + O(p^{\frac{k-1}{2}}). \tag{4.6}$$

For Type I primes p, we have

$$N(\underline{n};p) = p^{k-2} + O(p^{\frac{k-2}{2}}) \tag{4.7}$$

and

$$N(\underline{n}; p^e) = p^{e(k-2)} + O(p^{e(k-2)} p^{-\frac{(k-2)}{2}}). \tag{4.8}$$

The implied constants may depend on Q_1 and Q_2 but are independent of p, e, n_1 and n_2.

For $T(\underline{n}; q)$ we obtain the following bounds:

Proposition 4.2 *For all good primes (and hence primes of Type I or Type II) we have*

$$T(\underline{n}; p) = O(p^{\frac{k+3}{2}}) \tag{4.9}$$

and

$$T(\underline{n}; p^e) \ll p^{e(\frac{k+4}{2})}. \tag{4.10}$$

For bad primes p, there exists a constant c_p such that for all $e \geq 1$, we have

$$|T(\underline{n}; p^e)| \leq c_p p^{e(\frac{k+4}{2})}. \tag{4.11}$$

For Type I primes p we have

$$T(\underline{n}; p) = O(p^{\frac{k+2}{2}}) \tag{4.12}$$

and

$$T(\underline{n}; p^e) = 0 \quad (e \geq 2). \tag{4.13}$$

The implied constants may depend on Q_1 and Q_2, but are independent of p, e, n_1 and n_2.

Since the finite set of bad primes is determined by the original choice of Q_1 and Q_2, and since our $\ll$ constants are allowed to depend on this choice, we may replace (4.11) by the bound $T(\underline{n}; p^e) \ll p^{e(\frac{k+4}{2})}$.

4.1 Upper bounds for N

We first prove Proposition 4.1; we will prove Proposition 4.2 in Section 4.2 . We projectivize the counting problem, writing

$$N(\underline{n}; p) = (p-1)^{-1}(N^{(1)}(\underline{n}; p) - N^{(2)}(\underline{n}; p)) \tag{4.14}$$

with

$$N^{(1)}(\underline{n}; p) = \#\{(x_0, \mathbf{x}) \in \mathbb{F}_p^{k+1} : \underline{Q}(\mathbf{x}) \equiv \underline{n} x_0^2 \pmod{p}\}$$

and

$$N^{(2)}(\underline{n}; p) = \#\{\mathbf{x} \in \mathbb{F}_p^k : \underline{Q}(\mathbf{x}) \equiv \underline{0} \pmod{p}\},$$

say. The last term is independent of $\underline{n}$, and p is a good prime (whether it is Type I or Type II), so that the variety defined by $\underline{Q}(\mathbf{x}) = \underline{0}$ is smooth over $\mathbb{F}_p$. Thus we may apply Deligne's bound to obtain

$$N^{(2)}(\underline{n}; p) = \#\{\mathbf{x} \in \mathbb{F}_p^k : \underline{Q}(\mathbf{x}) \equiv \underline{0} \pmod{p}\} = p^{k-2} + O(p^{\frac{k-1}{2}}). \tag{4.15}$$

In order to bound the first term on the right hand side of (4.14), which may involve a singular variety in the case where p is of Type II, we recall the following theorem of Hooley [8].

Proposition 4.3 *If V is a projective complete intersection of dimension n defined over the finite field $\mathbb{F}_p$, with singular locus of dimension s, then the number of $\mathbb{F}_p$-rational points is $(p^{n+1}-1)/(p-1)+O(p^{(n+s+1)/2})$.*

We apply this to the variety

$$Z=\{(x_0,\mathbf{x})\in\mathbb{F}_p^{k+1}:\underline{Q}(\mathbf{x})-\underline{n}x_0^2=0\}$$

which has projective dimension $k-2$ and singular locus of projective dimension s, say, giving

$$N^{(1)}(\underline{n};p)=p^{k-1}+O(p^{\frac{k+1+s}{2}}).$$

We first verify that if p is a Type I prime, then Z is nonsingular over $\mathbb{F}_p$. Otherwise, there is a nontrivial pair $(\mathbf{x},x_0)$ for which

$$\mathrm{rk}\begin{pmatrix}2x_0n_1 & \nabla Q_1(\mathbf{x})\\ 2x_0n_2 & \nabla Q_2(\mathbf{x})\end{pmatrix}<2,$$

so that certainly $\nabla Q_1(\mathbf{x})$ and $\nabla Q_2(\mathbf{x})$ are proportional over $\mathbb{F}_p$. If $x_0\neq 0$, this would imply that $\nabla Q_1(\overline{x_0}\mathbf{x})$ and $\nabla Q_2(\overline{x_0}\mathbf{x})$ are proportional, while also $\underline{Q}(\overline{x_0}\mathbf{x})=\underline{n}$ in $\mathbb{F}_p$. This would contradict the fact that p is Type I. If $x_0=0$, then $\nabla Q_1(\mathbf{x})$ would be proportional to $\nabla Q_2(\mathbf{x})$ while also $\underline{Q}(\mathbf{x})=\underline{0}$, which contradicts the fact that p is good (and hence satisfies Condition 1 over $\overline{\mathbb{F}_p}$).

Thus if p is a Type I prime then Z is nonsingular over $\mathbb{F}_p$, so that $s=-1$ and

$$N^{(1)}(\underline{n};p)=p^{k-1}+O(p^{\frac{k}{2}}).$$

Combining this with (4.15) in (4.14) proves (4.7).

If p is a Type II prime the variety Z may be singular and we must estimate the dimension of the singular locus. Let H be the hyperplane $\{(x_0,\mathbf{x}):x_0=0\}$. Then $Z\cap H$ is nonsingular, since by Condition 1 the variety $V=\{\mathbf{x}:\underline{Q}(\mathbf{x})=\underline{0}\}$ is smooth. Thus the projective dimension of the singular locus of $Z\cap H$ is -1, whence the singular locus of Z itself can have dimension at most 0. Thus for Type II primes we have $s\le 0$ and hence

$$N^{(1)}(\underline{n};p)=p^{k-1}+O(p^{\frac{k+1}{2}}).$$

Now combining this with (4.15) in (4.14) proves (4.6).

For prime power moduli with p of Type I, we have the recursion

$$N(\underline{n};p^e)=N(\underline{n};p^{e-1})p^{k-2}. \tag{4.16}$$

The proof of this follows a standard route, lifting solutions from $\mathbb{F}_p$ via Hensel's Lemma. This is always possible since $V_p(n_1,n_2)$ is smooth. We leave the details to the reader. Given (4.16) the second result (4.8) of Proposition 4.1 follows immediately from (4.7).

4.2 Upper bounds for T

We now prove Proposition 4.2. The result (4.12) for Type I primes follows directly from the bound (4.7) for $N(\underline{n};p)$, via the relation (4.2). Similarly, for Type II primes, the bound (4.9) for $T(\underline{n};p)$ follows directly from (4.6). To prove (4.13) for Type I primes we again use (4.2), coupled now with (4.16).

For Type II primes, it is not effective to bound $T(\underline{n};p^e)$ via $N(\underline{n};p^e)$ when $e \geq 2$, since we cannot lift solutions. Instead, we recall that $T(\underline{n};p^e)$ is a sum of twists of

$$S_{p^e}(\underline{a}) = \sum_{\mathbf{x} \pmod{p^e}} e_{p^e}(\underline{a} \cdot \underline{Q}(\mathbf{x})),$$

and we bound $S_{p^e}(\underline{a})$ directly, ignoring the role of $\underline{n}$. This is also how we will obtain the bound (4.11) for bad primes; this makes inherent sense, since the property of being bad is independent of $\underline{n}$.

Thus let p be any prime, good or bad. Writing $q = p^e$ for convenience, and setting $\mathbf{x} = \mathbf{y} + \mathbf{z}$, we find that

$$\begin{aligned} |S_q(\underline{a})|^2 &= \sum_{\mathbf{x},\mathbf{y} \pmod{q}} e_q(\underline{a} \cdot \underline{Q}(\mathbf{x}) - \underline{a} \cdot \underline{Q}(\mathbf{y})) \\ &= \sum_{\mathbf{y},\mathbf{z} \pmod{q}} e_q(\underline{a} \cdot \underline{Q}(\mathbf{z}) + 2\mathbf{z}^t(\underline{a} \cdot \underline{Q})\mathbf{y}) \\ &= q^k \sum_{\substack{\mathbf{z} \pmod{q} \\ q \mid 2\mathbf{z}^t(\underline{a} \cdot \underline{Q})}} e_q(\underline{a} \cdot \underline{Q}(\mathbf{z})), \end{aligned}$$

so that

$$|S_q(\underline{a})|^2 \leq q^k Z(\underline{a};q), \tag{4.17}$$

where $Z(\underline{a};q)$ is defined by

$$Z(\underline{a};q) := \#\{\underline{z} \pmod{q} : \ q \mid 2\underline{z}^T(\underline{a} \cdot \underline{Q})\}. \tag{4.18}$$

The analysis of $Z(\underline{a};q)$ lies more naturally within the realm of the dichotomy of good and bad primes, which are the focus of Section 5; thus for the moment, we merely state the following claim:

Lemma 4.3 *For all good primes (and hence for all primes either of Type I or of Type II), we have*

$$Z(\underline{a};p^e) \leq \gcd(F(a_1,a_2),p^e). \tag{4.19}$$

For each bad prime p, there exists a constant C_p such that for all $e \geq 1$, we have

$$Z(\underline{a};p^e) \leq C_p \gcd(F(a_1,a_2),p^e). \tag{4.20}$$

We will prove this result in Section 5.3; see (5.12). For now, we will assume the bounds (4.19) and (4.20) and apply them to (4.17). In order to simplify notation, we temporarily adopt the convention that $C_p^* = 1$ if p is a good prime, and $C_p^* = \sqrt{C_p}$ if p is a bad prime.

We estimate $|T(\underline{n};p^e)|$ as

$$|T(\underline{n};p^e)| \le C_p^* p^{ek/2} \sum_{\substack{\underline{a} \pmod{p^e} \\ (\underline{a},p)=1}} \gcd(F(a_1,a_2),p^e)^{1/2}.$$

The sum on the right is

$$\begin{aligned} &\sum_{f=0}^{e} p^{f/2} \#\{\underline{a} \pmod{p^e} : (\underline{a},p)=1,\ \gcd(F(a_1,a_2),p^e)=p^f\} \\ \le\ & \sum_{f=0}^{e} p^{f/2} \#\{\underline{a} \pmod{p^e} : (\underline{a},p)=1,\ p^f \mid F(a_1,a_2)\} \\ \le\ & p^{2e} + \sum_{f=1}^{e} p^{f/2} p^{2(e-f)} \#\{\underline{a} \pmod{p^f} : (\underline{a},p)=1,\ p^f | F(a_1,a_2)\} \end{aligned} \tag{4.21}$$

For a given value of f, the number of allowable $\underline{a}$ with $p \nmid a_2$ is

$$\phi(p^f)\#\{u \pmod{p^f} : p^f \mid F(u,1)\}. \tag{4.22}$$

According to Huxley [9] the polynomial congruence $F(u,1) \equiv 0 \pmod{p^f}$ has at most $k|D_F|^{1/2}$ roots, where D_F is the discriminant of $F(x_1,x_2)$. (It is important to note here that Huxley's result requires $D_F \neq 0$, which is certainly true in our case). When $p \mid a_2$ we have the same estimate, by reversing the roles of a_1 and a_2. We therefore conclude that

$$\sum_{\substack{\underline{a} \pmod{p^e} \\ (\underline{a},p)=1}} \gcd(F(a_1,a_2),p^e)^{1/2} \ll p^{2e} + \sum_{f=1}^{e} p^{2e-3f/2}\phi(p^f) \ll p^{2e}.$$

This implies that

$$T(\underline{n};p^e) \ll p^{e\left(\frac{k+4}{2}\right)}$$

in the case of good primes, and

$$T(\underline{n};p^e) \ll C_p^* p^{e\left(\frac{k+4}{2}\right)}$$

in the case of bad primes. This suffices for the proof of Proposition 4.2.

4.3 The congruence problem: lower bounds for N

In order to prove that the singular series is nonvanishing—and in particular to give an effective lower bound for it—we will require a lower bound for $N(\underline{n};p^e)$ with an explicit dependence on p, for any prime p (whether good, bad, Type I or Type II). This effectively means we must show that the local congruence problem $Q_1(\mathbf{x}) \equiv n_1$, $Q_2(\mathbf{x}) \equiv n_1$ modulo p^e has sufficiently many solutions. Define for each p the local density

$$\sigma_p(\underline{n}) = \sum_{e=0}^{\infty} p^{-ek} T(\underline{n}; p^e) = \sum_{e=0}^{\infty} p^{-ek} \sum_{\substack{1 \le a_1, a_2 \le p^e \\ (a_1, a_2, p^e)=1}} S_{p^e}(\underline{a}; \underline{n}).$$

We will give a lower bound for $\sigma_p(\underline{n})$ for appropriate $\underline{n}$.

Proposition 4.4 *For each prime p there is a constant $\varpi_p > 0$ such that if the system $\underline{Q}(\mathbf{x}) = \underline{n}$ has a solution $\mathbf{x}_0$ over $\mathbb{Z}_p$, then*

$$\sigma_p(\underline{n}) \ge p^{-(k-2)} \max_{i,j} |\Delta_{ij}(\mathbf{x}_0)|_p^{2(k-2)} \ge \varpi_p |F(n_2, -n_1)|_p^{k-2}.$$

When $k \ge 5$, Lemma 4.2 coupled with (4.10) and (4.11) shows that for all primes we have

$$\sigma_p(\underline{n}) = \lim_{e \to \infty} \frac{N(\underline{n}; p^e)}{p^{e(k-2)}}. \tag{4.23}$$

We will need to understand how the size of $|F(n_2, -n_1)|_p$ controls the p-adic valuation of $\Delta(\mathbf{x})$. The necessary information is given by our next result.

Lemma 4.4 *For each prime p there is a constant $c_p > 0$ as follows. Let $\mathbf{x}_0 \in \mathbb{Z}_p^k$ and suppose that $\underline{Q}(\mathbf{x}_0) = \underline{n}$. Then*

$$|F(n_2, -n_1)|_p \le c_p \max_{i,j} |\Delta_{ij}(\mathbf{x}_0)|_p^2.$$

For the proof we use Condition 3 to diagonalize Q_1, Q_2 simultaneously over $\overline{\mathbb{Q}_p}$, writing $Q_1 = M^T A M$ and $Q_2 = M^T B M$ with a nonsingular matrix M and diagonal matrices $A = \mathrm{diag}(a_i)$ and $B = \mathrm{diag}(b_i)$. Then since $\underline{Q}(\mathbf{x}_0) = \underline{n}$,

$$F(n_2, -n_1) = \det\left(Q_2(\mathbf{x}_0) Q_1 - Q_1(\mathbf{x}_0) Q_2\right) = \det(M)^2 \det\left(B(\mathbf{y}) A - A(\mathbf{y}) B\right),$$

where $\mathbf{y} = M\mathbf{x}_0$. If we set $\Delta_{ij} = a_i b_j - a_j b_i$ then the matrix $\Delta(\mathbf{y}; A, B)$, as defined in (2.1), has entries $\Delta_{ij}(\mathbf{y}) = 4\Delta_{ij} y_i y_j$; note that for $i \ne j$, Δ_{ij} is nonzero by Condition 3. Moreover

$$\det\left(B(\mathbf{y}) A - A(\mathbf{y}) B\right) = \prod_{i=1}^{k} \left(\sum_{\substack{1 \le j \le k \\ j \ne i}} \Delta_{ij} y_j^2 \right),$$

which is a form of degree $2k$ in $\mathbf{y}$. On expanding out the product we see that every resulting term contains a factor $y_i^2 y_j^2$ for some pair $i \ne j$, and this factor is a constant multiple of $\Delta_{ij}(\mathbf{y})^2$. It is therefore possible to choose certain forms G_{ij}, depending on A and B, for which there is an identity in $\mathbf{y}$ of the shape

$$\det\left(B(\mathbf{y}) A - A(\mathbf{y}) B\right) = \sum_{i,j} \Delta_{ij}(\mathbf{y})^2 G_{ij}(\mathbf{y}).$$

Since by assumption $|\mathbf{x}_0|_p \leq 1$, we have $|\mathbf{y}|_p \ll_p 1$, and hence $|G_{ij}(\mathbf{y})|_p \ll_p 1$. We then deduce that

$$|F(n_2, -n_1)|_p \ll_p \max_{i,j} |\Delta_{ij}(\mathbf{y})^2|_p.$$

To complete the proof of the lemma it remains to observe that

$$\frac{\partial A(\mathbf{y})}{\partial y_i} = \sum_j (M^{-1})_{ji} \frac{\partial Q_1(\mathbf{x})}{\partial x_j}$$

and similarly for B and Q_2. This may be verified by a tedious piece of linear algebra. It follows that the determinants $\Delta_{ij}(\mathbf{y})$ are linear combinations of the entries $\Delta_{ij}(\mathbf{x}_0)$ in $\Delta(\mathbf{x}_0; Q_1, Q_2)$, so that

$$\max_{i,j} |\Delta_{ij}(\mathbf{y})^2|_p \ll_p \max_{i,j} |\Delta_{ij}(\mathbf{x}_0)^2|_p.$$

This establishes the lemma.

We can now complete the proof of Proposition 4.4. After permuting the indices as necessary, Lemma 4.4 allows us to assume that that

$$|\Delta_{12}(\mathbf{x}_0)|_p^2 = \max_{i,j} |\Delta_{ij}(\mathbf{x}_0)|_p^2 \geq c_p^{-1} |F(n_2, -n_1)|_p. \tag{4.24}$$

Since Proposition 4.4 is trivial unless $\Delta_{12}(\mathbf{x}_0)$ is non-zero we may set

$$|\Delta_{12}(\mathbf{x}_0)|_p = p^{-v}, \tag{4.25}$$

say. Suppose now that $e \geq 2v+1$ and take any integers $y_3, \ldots, y_k \pmod{p^e}$ all divisible by p^{2v+1}. There are $p^{(k-2)(e-2v-1)}$ such $(k-2)$-tuples. We then claim that the congruences

$$\underline{Q}(\mathbf{x}_0 + (w_1, w_2, y_3, y_4, \ldots, y_k)) \equiv \underline{n} \pmod{p^e}$$

will have an integer solution (w_1, w_2). Thus $N(\underline{n}; p^e) \geq p^{(k-2)(e-2v-1)}$, whence (4.23) yields

$$\sigma_p(\underline{n}) \geq p^{-(k-2)(2v+1)} = p^{-(k-2)} |\Delta_{12}(\mathbf{x}_0)|_p^{2(k-2)} \geq (c_p p)^{-(k-2)} |F(n_2, -n_1)|_p^{k-2}$$

in view of (4.24) and (4.25). This will suffice for Proposition 4.4, with $\varpi_p = (c_p p)^{-(k-2)}$.

To prove the claim we set

$$\mathbf{y} = \mathbf{x}_0 + (0, 0, y_3, y_4, \ldots, y_k).$$

Then $\mathbf{y} \equiv \mathbf{x}_0 \pmod{p^{2v+1}}$, whence $\underline{Q}(\mathbf{y}) \equiv \underline{n} \pmod{p^{2v+1}}$ and

$$\Delta_{12}(\mathbf{y}) \equiv \Delta_{12}(\mathbf{x}_0) \pmod{p^{2v+1}}.$$

In particular we will have $|\Delta_{12}(\mathbf{y})|_p = p^{-v}$, in view of (4.25). We therefore require an integer solution (w_1, w_2) to the simultaneous congruences

$$q_1(w_1, w_2) \equiv q_2(w_1, w_2) \equiv 0 \ (\mathrm{mod}\ p^e),$$

where

$$q_i(w_1, w_2) = Q_i(\mathbf{x}_0 + (w_1, w_2, y_3, y_4, \ldots, y_k)) - Q_i(\mathbf{x}_0), \quad (i = 1, 2).$$

The existence of suitable w_1, w_2 now follows from a standard application of Hensel's Lemma, since $p^{2v+1}|q_1(0,0), q_2(0,0)$ and

$$\det \begin{pmatrix} \frac{\partial q_1(0,0)}{\partial w_1} & \frac{\partial q_1(0,0)}{\partial w_2} \\ \frac{\partial q_2(0,0)}{\partial w_1} & \frac{\partial q_2(0,0)}{\partial w_2} \end{pmatrix} \not\equiv 0 \ (\mathrm{mod}\ p^{v+1}).$$

This completes the proof of Proposition 4.4.

Theorem 1.7 relates to the case $(n_1, n_2) = (0, 0)$ for which we replace Proposition 4.4 with the following result.

Proposition 4.5 *For each prime p such that the system $\underline{Q}(\mathbf{x}) = \underline{0}$ has a nonzero local solution in $\mathbb{Z}_p$ we have $\sigma_p(\underline{0}) > 0$.*

This will follow immediately from the following analogue of Lemma 4.4.

Lemma 4.5 *For each prime p such that the system $\underline{Q}(\mathbf{x}) = \underline{0}$ has a nonzero local solution $\mathbf{x}_0$ over $\mathbb{Z}_p$ we have*

$$\max_{i,j} |\Delta_{i,j}(\mathbf{x}_0)|_p > 0.$$

For the proof we merely observe that if $\Delta_{i,j}(\mathbf{x}_0) = 0$ for every pair i, j then $\mathrm{rk}(J(\underline{\mathbf{x}_0})) < 2$, which contradicts Condition 1 over $\overline{\mathbb{Q}_p}$, and hence equivalently over $\overline{\mathbb{Q}}$.

5 Exponential sums: minor arcs

In this section we consider exponential sums of the form

$$S(\mathbf{l}; q) = \sum_{\substack{a_1, a_2 \\ (a_1, a_2, q) = 1}} \sum_{\substack{\mathbf{r}_1 \ (\mathrm{mod}\ q) \\ \mathbf{r}_2 \ (\mathrm{mod}\ q)}} e_q(\underline{a} \cdot \underline{Q}(\mathbf{r}_1) - \underline{a} \cdot \underline{Q}(\mathbf{r}_2)) e_q(\mathbf{r}_1 \cdot \mathbf{l}_1 + \mathbf{r}_2 \cdot \mathbf{l}_2)$$

where $\mathbf{l} = (\mathbf{l}_1, \mathbf{l}_2) \in \mathbb{Z}^k \times \mathbb{Z}^k$. Such sums arise naturally in the analysis of the minor arcs, for which the original generating function is squared.

We first observe that $S(\mathbf{l}; q)$ satisfies a standard multiplicative property: if $q = q_1 q_2$ with $(q_1, q_2) = 1$, then one may easily check that

$$S(\mathbf{l}; q) = S(\mathbf{l}; q_1) S(\mathbf{l}; q_2). \tag{5.1}$$

We may thus reduce our consideration to the case in which $q = p^e$ for some prime p and $e \geq 1$.

The sum $S(\mathbf{l}; q)$ is in $2k+2$ variables, so a square-root cancellation bound would take the form $S(\mathbf{l}; q) \ll q^{k+1}$. This is out of reach; for general primes p, the best we can prove is that $S(\mathbf{l}; p^e) \ll_{p,e} p^{e(k+2)}$. However, for most primes we can do a bit better, and this is the heart of the work in showing that the minor arcs make a small enough contribution.

5.1 Preliminaries

Recall the determinant form

$$F(x, y) := \det(xQ_1 + yQ_2)$$

which we factored over its splitting field K as

$$F(x, y) = c^{-1} \prod_{i=1}^{k} (\lambda_i x - \mu_i y) \tag{5.2}$$

with $c \in \mathbb{N}$ and $\lambda_i, \mu_i \in \mathcal{O}_K$. According to Condition 4, for each index i the matrix $(\mu_i, \lambda_i).\underline{Q}$ will have rank exactly $k-1$. In particular the null space of $(\mu_i, \lambda_i).\underline{Q}$ is one-dimensional, and we may choose a generator $\underline{\mathrm{e}}_i \in \mathcal{O}_K^k$ for it. We then define

$$G(\underline{\mathrm{x}}) := \prod_{i=1}^{k} \prod_{\sigma} \left(\underline{\mathrm{x}}^T \underline{\mathrm{e}}_i^{\sigma} \right), \tag{5.3}$$

where σ runs over $\mathrm{Gal}(K/\mathbb{Q})$. This will be a non-zero form in k variables of a certain fixed degree, with coefficients in $\mathbb{Z}$.

A further collection of forms will also appear in our analysis. To define these we consider the $(k+1) \times (k+1)$ matrix

$$M(\underline{\alpha}; \underline{\mathrm{x}}, \underline{\mathrm{y}}) := \left(\begin{array}{c|c} \underline{\alpha} \cdot \underline{Q} & \underline{\mathrm{y}} \\ \hline \underline{\mathrm{x}}^T & 0 \end{array} \right), \tag{5.4}$$

where $\underline{\mathrm{x}}$ and $\underline{\mathrm{y}}$ are vectors of length k, and write $H_{rs}(\underline{\alpha}; \underline{\mathrm{x}}, \underline{\mathrm{y}})$ for its (r, s)-minor, this being a determinant of size $k \times k$. We then define

$$H_{rsi}(\underline{\mathrm{x}}, \underline{\mathrm{y}}) := \prod_{\sigma} H_{rs}\big((\mu_i^{\sigma}, \lambda_i^{\sigma}); \underline{\mathrm{x}}, \underline{\mathrm{y}}\big) \tag{5.5}$$

for $r, s \leq k+1$ and $i \leq k$, where as usual σ runs over $\mathrm{Gal}(K/\mathbb{Q})$. Finally we set

$$H(\underline{\mathrm{x}}, \underline{\mathrm{y}}) := \prod_{i=1}^{k} \left\{ \sum_{r,s \leq k+1} H_{rsi}(\underline{\mathrm{x}}, \underline{\mathrm{y}})^2 \right\}.$$

Note that the coefficients of H_{rsi} and H are rational integers.

5.2 Results

Recall the definition of "bad" primes as given in (2.7). The bound we obtain for the exponential sum $S(\mathbf{l};p^e)$ will depend on whether p is good or bad.

Lemma 5.1 *For each bad prime p, there exists a constant c_p such that*

$$|S(\mathbf{l};p^e)| \le c_p(e+1)p^{e(k+2)}.$$

If there were square-root cancellation we would have a bound $O(p^{e(k+1)})$, so our bound is worse by a factor of p^e. Moreover we have an implied constant which depends on p. However this is acceptable since there are only finitely many bad primes p.

For good primes, we will prove:

Lemma 5.2 *For good primes p we have*

$$S(\mathbf{l};p^e) \ll (e+1)p^{e(k+2)}$$

in all cases. Moreover if we set $\mathbf{l}_3 := \mathbf{l}_1 + \mathbf{l}_2$ and $\mathbf{l}_4 := \mathbf{l}_1 - \mathbf{l}_2$ we will have

$$S(\mathbf{l};p^e) \ll (e+1)p^{ek}\left(p^{2e-1} + \#\{\underline{b} \,(mod\, p^e) : \, p \mid \det M(\underline{b};\mathbf{l}_3,\mathbf{l}_4)\}\right) \qquad (5.6)$$

unless p divides each of

$$G(\mathbf{l}_3), \;\; G(\mathbf{l}_4) \;\; \text{and} \;\; H(\mathbf{l}_3,\mathbf{l}_4).$$

This is a truly unpleasant result, and its proof and later application are the most awkward parts of our entire argument.

5.3 A first bound

In this section we shall prove the following estimate.

Lemma 5.3 *For good primes p we have*

$$|S(\mathbf{l};p^e)| \ll (e+1)p^{e(k+2)},$$

while for bad primes we have

$$|S(\mathbf{l};p^e)| \ll_p (e+1)p^{e(k+2)}$$

uniformly in e.

Evidently Lemma 5.3 implies Lemma 5.1 and the first part of Lemma 5.2.

For the proof we write $q = p^e$ for convenience, and recall that

$$S(\mathbf{l};q) = \sum_{\substack{\underline{a} \,(\mathrm{mod}\, q) \\ (\underline{a},q)=1}} \sum_{\substack{\underline{x} \,(\mathrm{mod}\, q) \\ \underline{y} \,(\mathrm{mod}\, q)}} e_q(\underline{a}\cdot\underline{Q}(\underline{x}) - \underline{a}\cdot\underline{Q}(\underline{y}) + \mathbf{l}_1^T\underline{x} + \mathbf{l}_2^T\underline{y}). \qquad (5.7)$$

Making the change of variables $\underline{x} = \underline{z} + \underline{y}$ we now obtain

$$\begin{aligned} S(\mathbf{l}; q) &= \sum_{\substack{\underline{a} \ (\mathrm{mod}\ q) \\ (\underline{a}, q)=1}} \sum_{\underline{y}, \underline{z} \ (\mathrm{mod}\ q)} e_q(\underline{a} \cdot \underline{Q}(\underline{z}) + 2\underline{z}^T(\underline{a} \cdot \underline{Q})\underline{y} + \mathbf{l}_1^T \underline{z} + \mathbf{l}_3^T \underline{y}) \\ &= q^k \sum_{\substack{\underline{a} \ (\mathrm{mod}\ q) \\ (\underline{a}, q)=1}} \sum_{\substack{\underline{z} \ (\mathrm{mod}\ q) \\ q \mid 2\underline{z}^T(\underline{a} \cdot \underline{Q}) + \mathbf{l}_3^T}} e_q(\underline{a} \cdot \underline{Q}(\underline{z}) + \mathbf{l}_1^T \underline{z}). \end{aligned}$$

Hence

$$|S(\mathbf{l}; q)| \leq q^k \sum_{\substack{\underline{a} \ (\mathrm{mod}\ q) \\ (\underline{a}, q)=1}} \#\mathcal{S}(\mathbf{l}_3, \underline{a}; q),$$

where

$$\mathcal{S}(\mathbf{l}_3, \underline{a}; q) = \{\underline{z} \ (\mathrm{mod}\ q) : \ q \mid 2\underline{z}^T(\underline{a} \cdot \underline{Q}) + \mathbf{l}_3^T\}. \tag{5.8}$$

Note that if a set $\mathcal{S}(\mathbf{l}_3, \underline{a}; q)$ is non-empty then it must be a coset of $\mathcal{S}(\underline{0}, \underline{a}; q)$ in $(\mathbb{Z}/q\mathbb{Z})^k$. For indeed, if $\mathcal{S}(\mathbf{l}_3, \underline{a}; q)$ is non-empty then there exists a solution $\mathbf{z}_1$ of $2\mathbf{z}_1^T(\underline{a} \cdot \underline{Q}) + \mathbf{l}_3^T \equiv \mathbf{0} \ (\mathrm{mod}\ q)$, so that every solution $\mathbf{z}$ lying in $\mathcal{S}(\mathbf{l}_3, \underline{a}; q)$ can be written as $\mathbf{z} = \mathbf{z}_1 + \mathbf{z}_0$, where $\mathbf{z}_0 \in \mathcal{S}(\mathbf{0}, \underline{a}; q)$.

As a consequence,

$$|S(\mathbf{l}; q)| \leq q^k \sum_{\substack{\underline{a} \ (\mathrm{mod}\ q) \\ (\underline{a}, q)=1}} Z(\underline{a}; q)$$

where as in (4.18) we have defined

$$Z(\underline{a}; q) := \#\{\underline{z} \ (\mathrm{mod}\ q) : \ q \mid 2\underline{z}^T(\underline{a} \cdot \underline{Q})\}. \tag{5.9}$$

Our task is now to analyse $Z(\underline{a}; q)$. We will first prove Lemma 4.3, which gives an upper bound for $Z(\underline{a}; q)$, and then use it to prove the following result, from which Lemma 5.3 is now an immediate consequence.

Lemma 5.4 *For good primes p we have*

$$\sum_{\substack{\underline{a} \ (mod\ p^e) \\ (\underline{a}, p)=1}} Z(\underline{a}; p^e) \ll (e+1)p^{2e}$$

while for bad primes we have

$$\sum_{\substack{\underline{a} \ (mod\ p^e) \\ (\underline{a}, p)=1}} Z(\underline{a}; p^e) \ll_p (e+1)p^{2e}.$$

We proceed to prove Lemma 4.3. We begin by putting the matrix $\underline{a} \cdot \underline{Q}$ into Smith normal form as

$$S(\underline{a} \cdot \underline{Q})T = \mathrm{diag}\,(d_i), \tag{5.10}$$

say, using unimodular integer matrices S, T. We may assume here that the integer diagonal entries d_i are ordered so that their p-adic valuations satisfy

$$|d_1|_p \leq |d_2|_p \leq \ldots \leq |d_k|_p \leq 1. \tag{5.11}$$

If $p \mid d_i$ for some $i \geq 2$, then $S(\underline{a} \cdot \underline{Q})T$ has rank at most $k-2$ over $\mathbb{F}_p$. Since S, T have determinants ± 1 over $\mathbb{Z}$, they also have determinants ± 1 over $\mathbb{F}_p$, and are hence invertible over $\mathbb{F}_p$. Thus if $p \mid d_i$ for some $i \geq 2$, it would then follow that $\underline{a} \cdot \underline{Q}$ also has rank at most $k-2$ over $\mathbb{F}_p$. Thus, by the local version of Condition 4 given in Lemma 2.1, we can only have $p | d_i$ with $i \geq 2$ in the case in which p is bad.

We now see that

$$Z(\underline{a}; p^e) = \#\{\underline{\mathrm{w}} \pmod{p^e} : p^e \mid 2\underline{\mathrm{w}}^T \mathrm{diag}\,(d_i)\}.$$

For each i, the congruence $2w_i d_i \equiv 0 \pmod{p^e}$ has exactly $(2d_i, p^e)$ solutions modulo p^e, so that

$$Z(\underline{a}; p^e) = \prod_{i=1}^{k} (2d_i, p^e).$$

We now call on the following result, which we shall prove in a moment.

Lemma 5.5 *For each bad p there is a constant c_p such that*

$$\nu_p(2d_2) \leq c_p$$

for every pair $\underline{a}$ with $(a_1, a_2, p) = 1$.

We have already observed that $(d_i, p) = 1$ for $i \geq 2$ and good primes p, and we now conclude that

$$Z(\underline{a}; p^e) \leq \begin{cases} (d_1, p^e), & p \text{ good}, \\ p^{(k-1)c_p}(2d_1, p^e), & p \text{ bad}. \end{cases}$$

In order to relate d_1 to the vector $\underline{a}$ we note from (5.10) that

$$(d_1, p^e) \mid \det\left(S(\underline{a} \cdot \underline{Q})T\right),$$

and since S and T are unimodular we see that

$$(d_1, p^e) \mid \left(\det(\underline{a} \cdot \underline{Q}), p^e\right) = (F(a_1, a_2), p^e).$$

It then follows that

$$Z(\underline{a}; p^e) \leq \begin{cases} (F(a_1, a_2), p^e), & p \text{ good}, \\ 2p^{(k-1)c_p}(F(a_1, a_2), p^e), & p \text{ bad}. \end{cases} \tag{5.12}$$

This establishes Lemma 4.3, subject to the proof of Lemma 5.5.

To handle Lemma 5.4 we now sum over $\underline{a} \pmod{p^e}$ with $(\underline{a}, p^e) = 1$, via a similar procedure as in (4.21), with the only modification that a factor $(e+1)$ appears. This yields:

$$\begin{aligned}
&\sum_{\substack{\underline{a} \pmod{p^e} \\ (\underline{a},p)=1}} (F(a_1, a_2), p^e) \\
&\qquad \ll \sum_{f=0}^{e} p^f \#\{\underline{a} \pmod{p^e} : (\underline{a}, p) = 1, (F(a_1, a_2), p^e) = p^f\} \\
&\qquad \ll (e+1)p^{2e},
\end{aligned}$$

and Lemma 5.4 follows.

We conclude the present subsection by establishing Lemma 5.5. We remark that the lemma may be seen as a p-adic analogue of Lemma 2.3, and our proof will follow similar lines. We argue by contradiction, using a compactness argument over the p-adics $\mathbb{Z}_p$. Our assumption, contrary to the conclusion of Lemma 5.5, is that there exists a sequence of unimodular matrices S_i, T_i, and of pairs $\underline{a}^{(i)}$, all of whose entries are in $\mathbb{Z}_p$, and such that the values $|d_2^{(i)}|_p$ of the corresponding Smith normal forms tend to zero. By compactness of $\mathbb{Z}_p$, there will be a subsequence of triples $(S_i, T_i, \underline{a}^{(i)})$ converging to $S^{(*)}, T^{(*)}, \underline{a}^{(*)}$, say. It follows that $S^{(*)}$ and $T^{(*)}$ are unimodular matrices, and also that at least one of $a_1^{(*)}$ and $a_2^{(*)}$ is a p-adic unit. We then see from (5.10) that

$$S^{(*)}(\underline{a}^{(*)} \cdot \underline{Q})T^{(*)} = \mathrm{diag}\,(d_i^{(*)})$$

with $d_2^{(*)} = 0$. However (5.11) shows that if $|d_2^{(i)}|_p$ tends to zero then so also must $|d_1^{(i)}|_p$. We deduce that $d_1^{(*)} = d_2^{(*)} = 0$, whence $\mathrm{diag}\,(d_i^{(*)})$ has rank at most $k-2$. Since the matrices $S^{(*)}$ and $T^{(*)}$ are invertible over $\mathbb{Z}_p$ we see that $\underline{a}^{(*)} \cdot \underline{Q}$ also has rank at most $k-2$ over $\mathbb{Z}_p$. This finally contradicts Condition 4 with respect to $\overline{\mathbb{Q}_p}$ since the pair $\underline{a}^{(*)}$ cannot vanish in $\mathbb{Z}_p$. (Recall that Condition 4 over $\overline{\mathbb{Q}_p}$ is implied by Condition 1 over $\overline{\mathbb{Q}_p}$, which in turn is equivalent to Condition 1 over $\overline{\mathbb{Q}}$.) This completes the proof of Lemma 5.5.

5.4 Good primes

We now turn to the good primes p, for which it remains to prove the second part of Lemma 5.2. We begin with a slight variant of the previous analysis in which we make a symmetric change of variables, writing $\underline{\mathrm{x}} = \underline{\mathrm{u}} + \underline{\mathrm{v}}$ and $\underline{\mathrm{y}} = \underline{\mathrm{u}} - \underline{\mathrm{v}}$. Since $p = 2$ is a bad prime, by convention, this is permissible. We now find for $q = p^e$ that

$$\begin{aligned}
S(\mathbf{l}; q) &= \sum_{\substack{\underline{a} \pmod q \\ (\underline{a},q)=1}} \sum_{\underline{\mathrm{u}},\underline{\mathrm{v}} \pmod q} e_q(4\underline{\mathrm{u}}^T(\underline{a} \cdot \underline{Q})\underline{\mathrm{v}} + \mathbf{l}_3^T\underline{\mathrm{u}} + \mathbf{l}_4^T\underline{\mathrm{v}}) \\
&= q^k \sum_{\substack{\underline{a} \pmod q \\ (\underline{a},q)=1}} \sum_{\substack{\underline{\mathrm{u}} \pmod q \\ q | 4\underline{\mathrm{u}}^T(\underline{a} \cdot \underline{Q}) + \mathbf{l}_4^T}} e_q(\mathbf{l}_3^T\underline{\mathrm{u}}).
\end{aligned}$$

Since p is odd, the factor 4 can be absorbed into $\underline{a}$. We may simplify the exponential sum further by using homogeneity, averaging over an auxiliary variable r as follows. We have

$$\begin{aligned}\phi(q)S(\mathbf{l};q) &= q^k \sum_{(r,q)=1} \sum_{\substack{\underline{a} \pmod q\\ (\underline{a},q)=1}} \sum_{\substack{\underline{\mathrm{u}} \pmod q\\ q \mid r^{-1}\underline{\mathrm{u}}^T(r\underline{a}\cdot\underline{Q})+\mathbf{l}_4^T}} e_q(\mathbf{l}_3^T\underline{\mathrm{u}})\\ &= q^k \sum_{(r,q)=1} \sum_{\substack{\underline{b} \pmod q\\ (\underline{b},q)=1}} \sum_{\substack{\underline{\mathrm{w}} \pmod q\\ q \mid \underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q})+\mathbf{l}_4^T}} e_q(r\mathbf{l}_3^T\underline{\mathrm{w}})\end{aligned}$$

on replacing $r\underline{a}$ by $\underline{b}$ and $r^{-1}\underline{\mathrm{u}}$ by $\underline{\mathrm{w}}$. We can now perform the summation over r, on recalling that $q = p^e$. This produces

$$\phi(p^e)S(\mathbf{l};p^e) = p^{ek}\left(-p^{e-1}N_1(p^e) + p^eN_2(p^e)\right), \tag{5.13}$$

where

$$N_1(p^e) := \#\{\underline{b}, \underline{\mathrm{w}} \pmod{p^e} : (\underline{b},p)=1,\ p^e \mid \underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) + \mathbf{l}_4^T,\ p^{e-1} \mid \mathbf{l}_3^T\underline{\mathrm{w}}\},$$

and

$$N_2(p^e) := \#\{\underline{b}, \underline{\mathrm{w}} \pmod{p^e} : (\underline{b},p)=1,\ p^e \mid \underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) + \mathbf{l}_4^T,\ p^{e} \mid \mathbf{l}_3^T\underline{\mathrm{w}}\}.$$

We may easily dispose of $N_1(p^e)$ by ignoring the condition $p^{e-1} \mid \mathbf{l}_3^T\underline{\mathrm{w}}$. The set

$$\{\underline{b}, \underline{\mathrm{w}} \pmod{p^e} : (\underline{b},p)=1,\ p^e \mid \underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) + \mathbf{l}_4^T\}$$

is either empty, or is a coset (in $\mathbb{Z}/p^e\mathbb{Z}$) of

$$\{\underline{b}, \underline{\mathrm{w}} \pmod{p^e} : (\underline{b},p)=1,\ p^e \mid \underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q})\}, \tag{5.14}$$

by the same reasoning applied to (5.8). Certainly the set (5.14) is contained in

$$\{\underline{b}, \underline{\mathrm{w}} \pmod{p^e} : (\underline{b},p)=1,\ p^e \mid 2\underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q})\},$$

so that in the notation of (5.9),

$$N_1(p^e) \le \sum_{\substack{\underline{b} \pmod{p^e}\\ (\underline{b},p)=1}} Z(\underline{b};p^e).$$

Then Lemma 5.4 yields

$$N_1(p^e) \ll (e+1)p^{2e}$$

for good primes p. It follows that the corresponding contribution to $S(\mathbf{l};p^e)$, after dividing (5.13) through by $\phi(p^e)$, is therefore $O((e+1)p^{e(k+2)-1})$, which is satisfactory for (5.6).

We turn now to $N_2(p^e)$, which will be somewhat harder. We decompose $N_2(p^e)$ into two parts $N_3(p^e) + N_4(p^e)$, the first of which corresponds to pairs $\underline{b}$

for which $\underline{b}\cdot\underline{Q}$ is invertible modulo p and the second to those for which it is not. For $N_3(p^e)$ the condition $p^e \mid \underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) + \mathbf{l}_4^T$ determines $\underline{\mathrm{w}}$ (mod p^e) uniquely. Moreover, for a fixed $\underline{b}$ (mod p^e), the system of linear equations

$$\underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) + \mathbf{l}_4^T = \underline{0}^T, \ \mathbf{l}_3^T\underline{\mathrm{w}} = 0 \tag{5.15}$$

will have a solution over $\mathbb{F}_p$ if and only if the matrix $M(\underline{b};\mathbf{l}_3,\mathbf{l}_4)$ given by (5.4) has rank k over $\mathbb{F}_p$. It follows that

$$N_3(p^e) \le \#\{\underline{b} \ (\mathrm{mod}\ p^e) : \ p \mid \det M(\underline{b};\mathbf{l}_3,\mathbf{l}_4)\},$$

which leads to a satisfactory contribution in (5.6).

We handle $N_4(p^e)$ by splitting it as $N_5(p^e)+N_6(p^e)$, the first of which counts those solutions for which the matrix

$$M_0(\underline{b};\mathbf{l}_3) := \left(\begin{array}{c}\underline{b}\cdot\underline{Q}\\ \hline \mathbf{l}_3^T\end{array}\right)$$

has rank k over $\mathbb{F}_p$, and the second of which counts solutions for which the rank is $k-1$. Here we recall that the rank of $M_0(\underline{b};\mathbf{l}_3)$ cannot be lower than $k-1$ over $\mathbb{F}_p$, since p is a good prime.

In the case of $N_5(p^e)$, we have

$$\underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) \equiv \underline{0}^T, \ \mathbf{l}_3^T\underline{\mathrm{w}} \equiv 0 \ (\mathrm{mod}\ p)$$

only when $p \mid \underline{\mathrm{w}}$. Then the only solution modulo p^e will be $\underline{\mathrm{w}} \equiv \underline{0}$ (mod p^e), so that (again by the coset argument) the congruences

$$\underline{\mathrm{w}}^T(\underline{b}\cdot\underline{Q}) + \mathbf{l}_4^T \equiv \underline{0}^T, \ \mathbf{l}_3^T\underline{\mathrm{w}} \equiv 0 \ (\mathrm{mod}\ p^e)$$

have at most one solution $\mathbf{w}$ (mod p^e). Moreover, as in our treatment of $N_3(p^e)$, in order for (5.15) to have a solution over $\mathbb{F}_p$ the matrix $M(\underline{b};\mathbf{l}_3,\mathbf{l}_4)$ must have rank k over $\mathbb{F}_p$ and hence

$$N_5(p^e) \le \#\{\underline{b} \ (\mathrm{mod}\ p^e) : \ p \mid \det M(\underline{b};\mathbf{l}_3,\mathbf{l}_4)\},$$

which is again satisfactory.

To handle $N_6(p^e)$ we must first understand better the condition that $\underline{b}\cdot\underline{Q}$ is singular modulo p. We recall the notation defined in §5.1 and we take P to be a prime ideal of $\mathcal{O}_K$ lying over p. Since p is a good prime neither p nor P can divide the constant c in (5.2). Moreover, since p is good, none of the determinants $\lambda_i\mu_j - \lambda_j\mu_i$ can be divisible by P and so in particular, for each i, the ideal P can divide at most one of λ_i or μ_i. For $N_6(p^e)$ we have $p \mid \det(\underline{b}\cdot\underline{Q})$ and hence $P \mid \det(\underline{b}\cdot\underline{Q})$. It follows that

$$P \mid \prod_{i=1}^{k}(\lambda_i b_1 - \mu_i b_2),$$

so that $P \mid \lambda_i b_1 - \mu_i b_2$ for some index i. Since $(b_1, b_2, p) = 1$ and P cannot divide both λ_i and μ_i, we deduce that $\underline{b} \equiv \alpha(\mu_i, \lambda_i) \pmod{P}$ for some $\alpha \in \mathcal{O}_K$ not divisible by P. As in our treatment of $N_3(p^e)$ we obtain a codition for (5.15) to be solvable modulo p. Here we require the matrices $M_0(\underline{b}; \mathbf{l}_3)$ and $M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)$ to have the same rank over $\mathbb{F}_p$. Since the first of these has rank $k-1$ for $N_6(p^e)$ we see that all the $k \times k$ minors of $M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)$ must vanish modulo p. It follows that $p \mid H_{rs}(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)$ for each $r, s \leq k+1$, and hence that $P \mid H_{rs}(\alpha(\mu_i, \lambda_i); \mathbf{l}_3, \mathbf{l}_4)$. However the polynomial $H_{rs}(\underline{x}; \underline{y}, \underline{z})$ is homogeneous in $\underline{x}$, and we may therefore conclude that there is an index i for which each of $H_{rs}((\mu_i, \lambda_i); \mathbf{l}_3, \mathbf{l}_4)$, for $r, s \leq k+1$, is divisible by P. We then deduce that $H_{rsi}(\mathbf{l}_3, \mathbf{l}_4)$ is divisible by P for each $r, s \leq k+1$, since all the other factors in (5.5) are algebraic integers. This then implies firstly that P divides $H(\mathbf{l}_3, \mathbf{l}_4)$ and then that $p \mid H(\mathbf{l}_3, \mathbf{l}_4)$, because the coefficients of H are rational integers. It follows that $N_6(p^e)$ vanishes unless $p \mid H(\mathbf{l}_3, \mathbf{l}_4)$.

Finally, recall the requirement for $N_6(p^e)$: if $\underline{b}$ and $\underline{w}$ are counted by $N_6(p^e)$, then $M_0(\underline{b}; \mathbf{l}_3)$ has rank $k-1$ over $\mathbb{F}_p$. Thus $\mathbf{l}_3 = (\underline{b} \cdot \underline{Q})\underline{x}$ for some $\underline{x} \in \mathbb{F}_p^k$ and then, with some abuse of notation,

$$(\underline{b} \cdot \underline{Q})\underline{x} \equiv \mathbf{l}_3 \pmod{P}.$$

By the argument above one then has

$$\big(\alpha(\mu_i, \lambda_i) \cdot \underline{Q}\big)\, \underline{x} \equiv \mathbf{l}_3 \pmod{P}$$

for some some index i and $\alpha \in \mathcal{O}_K$ such that $P \nmid \alpha$. Pre-multiplying by the null-vector $\underline{e}_i$ described in §5.1 we deduce that $P \mid \underline{e}_i^T \mathbf{l}_3$. It then follows that $G(\mathbf{l}_3)$ is divisible by P, since all the other factors in (5.3) are algebraic integers. Just as in the case of $H(\mathbf{l}_3, \mathbf{l}_4)$ we now deduce that $N_6(p^e)$ vanishes unless $p \mid G(\mathbf{l}_3)$. In exactly the same way, if p divides $\underline{w}^T(\underline{b} \cdot \underline{Q}) + \mathbf{l}_4^T$ we may conclude that $p \mid G(\mathbf{l}_4)$. Thus $N_6(p^e)$ vanishes unless p divides each of $H(\mathbf{l}_3, \mathbf{l}_4)$, $G(\mathbf{l}_3)$ and $G(\mathbf{l}_4)$. This now suffices for Lemma 5.2.

5.5 Averages of $S(\mathbf{l}; q)$

We will now use Lemmas 5.1 and 5.2 to establish the following estimate.

Lemma 5.6 *Let $\varepsilon > 0$ be given and suppose that $k \geq 4$. Then for any $Q, L \in \mathbb{N}$ we have*

$$\sum_{q \leq Q} \sum_{|\mathbf{l}| \leq L} |S(\mathbf{l}; q)| \ll_\varepsilon Q^{k+2+\varepsilon} L^{2k+\varepsilon} + Q^{k+3+\varepsilon} L^{2k-3+\varepsilon}.$$

We shall write Σ for the double sum to be estimated, and we begin by considering those terms for which $G(\mathbf{l}_3)$, $G(\mathbf{l}_4)$ and $H(\mathbf{l}_3, \mathbf{l}_4)$ all vanish. We write Σ_1 for the corresponding contribution to Σ. In this case Lemmas 5.1 and 5.2 show that there is a constant C such that $|S(\mathbf{l}; p^e)| \leq C(e+1)p^{e(k+2)}$ for all prime powers p^e. One merely takes C to be the maximum of the implied constant from Lemma 5.2 and the various constants c_p in Lemma 5.1 for the finite number of bad primes. In view of the multiplicative property (5.1) we then see that

$$|S(\mathbf{l};q)| \le C^{\omega(q)} d(q) q^{k+2} \ll_\varepsilon q^{k+2+\varepsilon},$$

where $\omega(q)$ is the number of distinct prime factors of q, and $d(q)$ is the divisor function. In particular, we record for later reference that in the case $\mathbf{l} = \mathbf{0}$,

$$|S(\mathbf{0};q)| \ll_\varepsilon q^{k+2+\varepsilon}. \tag{5.16}$$

Continuing our estimation, it follows that

$$\Sigma_1 \ll_\varepsilon Q^{k+3+\varepsilon} \#\{\mathbf{l} : \, |\mathbf{l}| \le L, \, G(\mathbf{l}_3) = G(\mathbf{l}_4) = H(\mathbf{l}_3, \mathbf{l}_4) = 0\}.$$

Examining the definition of $H(\underline{\mathrm{x}}, \underline{\mathrm{y}})$ we see that there must be some index $i \le k$ such that

$$\Sigma_1 \ll_\varepsilon Q^{k+3+\varepsilon} \#\{\mathbf{l} : \, |\mathbf{l}| \le L, \, G(\mathbf{l}_3) = G(\mathbf{l}_4) = H_{rsi}(\mathbf{l}_3, \mathbf{l}_4) = 0, \, (r, s \le k+1)\}.$$

Moreover, if $H_{rsi}(\mathbf{l}_3, \mathbf{l}_4) = 0$ then $H_{rs}\big((\mu_i^\sigma, \lambda_i^\sigma); \mathbf{l}_3, \mathbf{l}_4\big) = 0$, for one of the automorphisms σ, and hence $H_{rs}\big((\mu_i, \lambda_i); \mathbf{l}_3, \mathbf{l}_4\big) = 0$. It follows that

$$\begin{aligned} \Sigma_1 \quad \ll_\varepsilon \quad Q^{k+3+\varepsilon} \#\{\mathbf{l} : \, |\mathbf{l}| \le L, \, G(\mathbf{l}_3) = G(\mathbf{l}_4) = H_{rs}\big((\mu_i, \lambda_i); \mathbf{l}_3, \mathbf{l}_4\big) = 0 \\ (r, s \le k+1)\}. \end{aligned}$$

According to Theorem 1 of Browning and Heath-Brown [2], the number of admissible vectors $\mathbf{l}$ is $O(L^{m+1})$, where m is the dimension of the projective variety defined over the field K by

$$\{[\mathbf{x}, \mathbf{y}] \in \mathbb{P}^{2k-1} : G(\underline{\mathrm{x}}) = G(\underline{\mathrm{y}}) = H_{rs}\big((\mu_i, \lambda_i); \underline{\mathrm{x}}, \underline{\mathrm{y}}\big) = 0 \quad (r, s \le k+1)\}. \tag{5.17}$$

We will then have

$$\Sigma_1 \ll_\varepsilon Q^{k+3+\varepsilon} L^{m+1}. \tag{5.18}$$

It remains to provide an upper bound for the dimension m. Both of the varieties $G(\underline{\mathrm{x}}) = 0$ and $G(\underline{\mathrm{y}}) = 0$ are unions of hyperplanes, $L_j(\underline{\mathrm{x}}) = 0$ or $L_j(\underline{\mathrm{y}}) = 0$ say, while the variety

$$H_{rs}\big((\mu_i, \lambda_i); \underline{\mathrm{x}}, \underline{\mathrm{y}}\big) = 0 \quad (r, s \le k+1)$$

describes the vanishing of all the $k \times k$ minors of a matrix

$$B := \left(\begin{array}{c|c} A & \underline{\mathrm{y}} \\ \hline \underline{\mathrm{x}}^T & 0 \end{array} \right).$$

Here $A = (\mu_i, \lambda_i) \cdot \underline{Q}$ is a $k \times k$ symmetric matrix, which is known to have rank $k-1$ by construction. To examine this further we diagonalize A over

$\overline{\mathbb{Q}}$ as $R^T DR$, say, where R is nonsingular, and $D = \mathrm{diag}(0, d_2, \ldots, d_k)$ with $d_2 \ldots d_k \neq 0$. If B has rank at most $k-1$ the matrix

$$\left(\begin{array}{c|c} R^{-T} & \underline{0} \\ \hline \underline{0}^T & 1 \end{array}\right) \left(\begin{array}{c|c} A & \underline{y} \\ \hline \underline{x}^T & 0 \end{array}\right) \left(\begin{array}{c|c} R & \underline{0} \\ \hline \underline{0}^T & 1 \end{array}\right) = \left(\begin{array}{c|c} D & R^{-T}\underline{y} \\ \hline \underline{x}^T R & 0 \end{array}\right)$$

will also have rank at most $k-1$. However if we write $\underline{x}^T R = \underline{u}$ and $R^{-T}\underline{y} = \underline{v}$ then the $(1,1)$-minor of the above matrix is

$$-u_2 v_2 \widehat{d_2} - \ldots - u_k v_k \widehat{d_k}, \tag{5.19}$$

where

$$\widehat{d_j} = \prod_{\substack{2 \leq h \leq k \\ h \neq j}} d_h \neq 0.$$

In terms of the coordinates $\underline{u}$ and $\underline{v}$ the intersection $G(\underline{x}) = G(\underline{y}) = 0$ is a union of linear spaces of codimension 2, of the type $L(\underline{u}) = L'(\underline{v}) = 0$. However it is clear that the expression (5.19) cannot vanish on such a linear space, providing that $k \geq 4$. (One may verify that (5.19) is a quadratic form in $(\mathbf{u}, \mathbf{v})$ of rank $2k-2$, and in general a quadratic form that vanishes on a codimension r linear space has rank $\leq 2r$.) It therefore follows that the variety (5.17) has codimension at least 3 in $\mathbb{P}^{2k-1}$, whence $m \leq 2k-4$. The bound (5.18) then yields

$$\Sigma_1 \ll_\varepsilon Q^{k+3+\varepsilon} L^{2k-3}$$

which is satisfactory for Lemma 5.6.

We turn now to the case in which $F(\mathbf{l}) \neq 0$, where we have set

$$F(\mathbf{l}) := G(\mathbf{l}_3)^2 + G(\mathbf{l}_4)^2 + H(\mathbf{l}_3, \mathbf{l}_4)^2$$

for convenience. Here we will write Σ_2 for the sum to be estimated. We begin by claiming that Lemmas 5.1 and 5.2 may be combined to say that there is a constant C for which

$$|S(\mathbf{l}; p^e)| \leq C(e+1) p^{e(k+2)} \{p^{-1}(p, F(\mathbf{l})) + p^{-2} f(\mathbf{l}; p)\} \tag{5.20}$$

for all primes p, where we define

$$f(\mathbf{l}; q) := \#\{\underline{b} \pmod{q} : \, q \mid \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)\}$$

for any square-free q. Since $(p, F(\mathbf{l})) \geq 1$, the claim is plainly true for the bad primes, on taking $C \geq p\, c_p$ for all such primes. The claim is also straightforward in the case in which p is a good prime dividing each of $G(\mathbf{l}_3)$, $G(\mathbf{l}_4)$ and $H(\mathbf{l}_3, \mathbf{l}_4)$, since then $(p, F(\mathbf{l})) = p$. In the remaining case all that is needed is to observe that

$$\#\{\underline{b} \pmod{p^e} : \, p \mid \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)\} = p^{2e-2} f(\mathbf{l}; p).$$

This establishes our claim.

We will find it convenient to introduce the notation

$$\kappa(q) := \prod_{p|q} p.$$

Since the function $f(\mathbf{l};q)$ is multiplicative on square-free integers q we can now extend the estimate (5.20) to general moduli q by multiplicativity, to give

$$|S(\mathbf{l};q)| \leq C^{\omega(q)} d(q) q^{k+2} \sum_{\substack{q_1 q_2 = q \\ (q_1,q_2)=1}} \frac{(\kappa(q_1), F(\mathbf{l}))}{\kappa(q_1)} \frac{f(\mathbf{l};\kappa(q_2))}{\kappa(q_2)^2}.$$

We then deduce that

$$\Sigma_2 \ll Q^{k+2+\varepsilon} \sum_{\substack{|\mathbf{l}|\leq L \\ F(\mathbf{l})\neq 0}} \Sigma_3(\mathbf{l})\Sigma_4(\mathbf{l}),$$

with

$$\Sigma_3(\mathbf{l}) := \sum_{q\leq Q} \frac{(\kappa(q), F(\mathbf{l}))}{\kappa(q)}$$

and

$$\Sigma_4(\mathbf{l}) := \sum_{q\leq Q} \frac{f(\mathbf{l};\kappa(q))}{\kappa(q)^2}.$$

We estimate $\Sigma_3(\mathbf{l})$ using Rankin's trick. We have

$$\begin{aligned} \Sigma_3(\mathbf{l}) &\leq Q^{\varepsilon} \sum_{q=1}^{\infty} \frac{(\kappa(q), F(\mathbf{l}))}{q^{\varepsilon}\kappa(q)} \\ &= Q^{\varepsilon} \prod_p \left\{ \sum_{e=0}^{\infty} \frac{(\kappa(p^e), F(\mathbf{l}))}{p^{e\varepsilon}\kappa(p^e)} \right\} \\ &= Q^{\varepsilon} \prod_{p|F(\mathbf{l})} \left\{1 + p^{-\varepsilon} + p^{-2\varepsilon} + \cdots \right\} \prod_{p\nmid F(\mathbf{l})} \left\{1 + p^{-1-\varepsilon} + p^{-1-2\varepsilon} + \cdots \right\}. \end{aligned}$$

Hence if

$$c = c(\varepsilon) := 1 + 2^{-\varepsilon} + 4^{-\varepsilon} + \cdots \tag{5.21}$$

we will have

$$\Sigma_3(\mathbf{l}) \leq Q^{\varepsilon} c^{\omega(F(\mathbf{l}))} \prod_p \{1 + cp^{-1-\varepsilon}\} \leq Q^{\varepsilon} c^{\omega(F(\mathbf{l}))} \zeta(1+\varepsilon)^c \ll_{\varepsilon} (QL)^{\varepsilon}.$$

To handle $\Sigma_4(\mathbf{l})$ we observe that for $q \leq Q$,

$$\left[\frac{Q}{\kappa(q)}\right]^2 f(\mathbf{l};\kappa(q)) \leq \#\{b_1, b_2 \leq Q : \kappa(q) \mid \det M(\underline{b};\mathbf{l}_3,\mathbf{l}_4)\}.$$

Since $[\theta] \geq \theta/2$ for any real $\theta \geq 1$ we deduce that

$$\Sigma_4(\mathbf{l}) \ll Q^{-2} \sum_{b_1, b_2 \leq Q} \#\{q \leq Q : \kappa(q) \mid \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)\}.$$

Let $\Sigma_5(\mathbf{l})$ be the contribution to $\Sigma_4(\mathbf{l})$ from terms in which $\Delta := \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)$ is non-zero; and write $\Sigma_6(\mathbf{l})$ for the contribution in which $\det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4) = 0$. For $\Sigma_5(\mathbf{l})$ we use Rankin's trick again, which shows that

$$\begin{aligned}
\#\{q \leq Q : \kappa(q) \mid \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)\} &\leq Q^{\varepsilon} \sum_{\substack{q=1 \\ \kappa(q)\mid\Delta}}^{\infty} q^{-\varepsilon} \\
&= Q^{\varepsilon} \prod_{p\mid\Delta} \left\{1 + p^{-\varepsilon} + p^{-2\varepsilon} + \cdots\right\} \\
&\leq Q^{\varepsilon} c^{\omega(|\Delta|)}
\end{aligned}$$

with c as in (5.21). Since Δ is bounded by a suitable power of QL we deduce that

$$\#\{q \leq Q : \kappa(q) \mid \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)\} \ll_{\varepsilon} Q^{2\varepsilon} L^{\varepsilon}$$

so that

$$\Sigma_5(\mathbf{l}) \ll_{\varepsilon} Q^{2\varepsilon} L^{\varepsilon}.$$

It remains to deal with $\Sigma_6(\mathbf{l})$, for which we clearly have

$$\Sigma_6(\mathbf{l}) \ll Q^{-1} \#\{b_1, b_2 \leq Q : \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4) = 0\}.$$

Combining our various estimates we now see that

$$\begin{aligned}
\Sigma \ll_{\varepsilon} \; & Q^{k+3+\varepsilon} L^{2k-3} + Q^{k+2+4\varepsilon} L^{2k+2\varepsilon} \\
& + Q^{k+1+2\varepsilon} L^{\varepsilon} \sum_{|\mathbf{l}| \leq L} \#\{b_1, b_2 \leq Q : \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4) = 0\}. \quad (5.22)
\end{aligned}$$

For each fixed $\mathbf{l}$ the expression $\det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4)$ is a binary form in b_1, b_2 of degree $k-1$. It follows that there are at most $O(Q)$ pairs $b_1, b_2 \leq Q$ for which $\det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4) = 0$, unless the form vanishes identically. We therefore have

$$\sum_{|\mathbf{l}| \leq L} \#\{b_1, b_2 \leq Q : \det M(\underline{b}; \mathbf{l}_3, \mathbf{l}_4) = 0\} \ll QL^{2k} + Q^2 n(L), \quad (5.23)$$

where

$$n(L) := \#\{\mathbf{l} : |\mathbf{l}| \leq L, \det M(\underline{x}; \mathbf{l}_3, \mathbf{l}_4) \equiv 0\},$$

so that $n(L)$ counts vectors $\mathbf{l}$ for which $\det M(\underline{x}; \mathbf{l}_3, \mathbf{l}_4)$ vanishes with respect to $\underline{x}$.

To analyse $n(L)$ we consider the choice $\underline{x} = (\mu_i, \lambda_i)$, using the notation from §5.1. This produces a matrix $(\mu_i, \lambda_i) \cdot \underline{Q}$ of rank exactly $k-1$. Suppose that

$$M := \left(\begin{array}{c|c} (\mu_i, \lambda_i) \cdot \underline{Q} & \mathbf{l}_4 \\ \hline \mathbf{l}_3^T & 0 \end{array} \right)$$

is singular. If $\mathbf{l}_4$ is not in the column space for $(\mu_i,\lambda_i)\cdot \underline{Q}$ then

$$M_0 := \left(\ (\mu_i,\lambda_i)\cdot \underline{Q} \ \Big| \ \mathbf{l}_4 \ \right)$$

will have rank k, and hence has linearly independent rows. Since M is singular it would follow that $(\mathbf{l}_3^T \mid 0)$ is in the row space for M_0, whence in particular $\mathbf{l}_3^T$ would be in the row space for $(\mu_i,\lambda_i)\cdot \underline{Q}$. We therefore conclude that either $\mathbf{l}_3$ or $\mathbf{l}_4$ must lie in the column space of $(\mu_i,\lambda_i)\cdot \underline{Q}$. In §5.1 we chose a null vector $\underline{\mathrm{e}}_i$ for $(\mu_i,\lambda_i)\cdot \underline{Q}$, and we now see that either $\underline{\mathrm{e}}_i^T\mathbf{l}_3 = 0$ or $\underline{\mathrm{e}}_i^T\mathbf{l}_4 = 0$. This conclusion is valid for any index $i \le k$ so that for each vector $\mathbf{l}$ counted by $n(L)$ there will be a subset $S \subseteq \{1,\ldots,k\}$ for which

$$\underline{\mathrm{e}}_i^T\mathbf{l}_3 = 0 \quad (i \in S) \quad \text{and} \quad \underline{\mathrm{e}}_i^T\mathbf{l}_4 = 0 \quad (i \notin S).$$

These conditions restrict $\mathbf{l}$ to a k-dimensional subspace of $\mathbb{Z}^{2k}$. Any such subspace can contain at most $O(L^k)$ integral points with $|\mathbf{l}| \le L$, whence $n(L) \ll L^k$. It then follows from (5.22) and (5.23) that

$$\Sigma \ll_\varepsilon Q^{k+3+\varepsilon}L^{2k-3} + Q^{k+2+4\varepsilon}L^{2k+2\varepsilon} + Q^{k+1+2\varepsilon}L^{\varepsilon}(QL^{2k}+Q^2L^k),$$

which suffices for Lemma 5.6, on redefining ε.

6 Exponential sums: The singular series

We will now use our results about exponential sums to establish some key results about the singular series, given by

$$\mathfrak{S}(\underline{n}) = \sum_{q=1}^{\infty} \frac{1}{q^k} \sum_{\substack{1\le a_1,a_1\le q\\ (a_1,a_2,q)=1}} S_q(\underline{a};\underline{n}) = \sum_{q=1}^{\infty}\frac{1}{q^k}T(\underline{n};q), \tag{6.1}$$

with

$$S_q(\underline{a};\underline{n}) = S_q(\underline{a})e_q(-\underline{a}\cdot\underline{n}).$$

We will prove the following propositions.

Proposition 6.1 *The singular series $\mathfrak{S}(\underline{n})$ is absolutely convergent for every $\underline{n}$ for which $F(n_2,-n_1) \ne 0$, providing that $k \ge 5$. Indeed*

$$\sum_{q\ge R}\frac{1}{q^k}|T(\underline{n};q)| \ll |\underline{n}|^{\varepsilon}R^{-1/3}, \tag{6.2}$$

for such $\underline{n}$, where the implied constant depends only on Q_1, Q_2 and ε.

Proposition 6.2 *There is a constant p_0 depending only on Q_1 and Q_2 with the following property. Let $k \ge 5$ and $F(n_2,-n_1)\ne 0$. Suppose further that the system $\underline{Q}(\mathbf{x}) = \underline{n}$ is locally solvable in $\mathbb{Z}_p$ for every prime p. Then for any $\varepsilon > 0$ we will have*

$$\mathfrak{S}(\underline{n}) \gg |\underline{n}|^{-\varepsilon}\prod_{p\le p_0}|F(n_2,-n_1)|_p^{k-2}.$$

Of course (6.2) yields not only the statement about absolute convergence, by taking $R = 1$, but also the estimate

$$\mathfrak{S}(\underline{n}) \ll |\underline{n}|^{\varepsilon}$$

for $F(n_2, -n_1) \neq 0$.

We begin by establishing (6.2). For any $R \geq 1$ we have

$$\sum_{q \geq R} q^{-k} |T(\underline{n}; q)| \leq R^{-1/3} \sum_{q=1}^{\infty} q^{1/3-k} |T(\underline{n}; q)|.$$

Let

$$\psi_p := \sum_{e=0}^{\infty} p^{-e(k-1/3)} |T(\underline{n}; p^e)|,$$

so that

$$\sum_{q \geq R} q^{-k} |T(\underline{n}; q)| \leq R^{-1/3} \prod_p \psi_p$$

by multiplicativity. By Proposition 4.2 we have

$$\psi_p = 1 + O(p^{4/3-k/2}) = 1 + O(p^{-7/6})$$

for Type I primes, and

$$\begin{aligned} \psi_p &= 1 + O(p^{11/6-k/2}) + O(\sum_{e=2}^{\infty} p^{(7/3-k/2)e}) \\ &= 1 + O(p^{11/6-k/2}) + O(p^{14/3-k}) \\ &= O(1) \end{aligned} \tag{6.3}$$

for Type II primes. Finally, for bad primes, we will have

$$\psi_p = 1 + O_p(\sum_{e=1}^{\infty} p^{(7/3-k/2)e}) \ll_p 1.$$

The product of ψ_p for Type I primes is thus $O(1)$, and similarly for bad primes, since the collection of bad primes finite and is determined purely by Q_1 and Q_2. Finally, for the Type II primes, if $|\psi_p| \leq C$ say for such primes p, then the corresponding product is at most

$$C^{\omega(F(n_2,-n_1))} \ll |\underline{n}|^{\varepsilon}.$$

The bound (6.2) then follows.

Turning to Proposition 6.2, we begin by observing that

$$\mathfrak{S}(\underline{n}) = \prod_p \sigma_p \tag{6.4}$$

with

$$\sigma_p = 1 + \sum_{e=1}^{\infty} p^{-ek} T(\underline{n}; p^e).$$

By another application of Proposition 4.2 we have

$$\sigma_p = 1 + p^{-k} T(\underline{n}; p) = 1 + O(p^{1-k/2}) = 1 + O(p^{-3/2}) \tag{6.5}$$

for Type I primes and

$$\begin{aligned}
\sigma_p &= 1 + p^{-k} T(\underline{n}; p) + \sum_{e=2}^{\infty} p^{-ek} T(\underline{n}; p^e) \\
&= 1 + O(p^{(3-k)/2}) + O(\sum_{e=2}^{\infty} p^{(2-k/2)e}) \\
&= 1 + O(p^{(3-k)/2}) + O(p^{4-k}) \\
&= 1 + O(p^{-1}) \qquad (6.6)
\end{aligned}$$

for Type II primes. Suppose that $\sigma_p \geq 1 - Ap^{-3/2}$ for some explicit constant $A \geq 1$, for Type I primes. Then $\sigma_p \geq (1 - p^{-3/2})^{2A}$ for Type I primes $p \geq 2A$, since we have $1 - At \geq (1-t)^{2A}$ for any positive real $t \leq (2A)^{-1}$. Similarly, if $\sigma_p \geq 1 - Ap^{-1}$ for Type II primes we will have $\sigma_p \geq (1 - p^{-1})^{2A}$ for $p \geq 2A$. The contribution of such primes to the product (6.4) is therefore

$$\geq \prod_p (1 - p^{-3/2})^{2A} \prod_{p \mid F(n_2, -n_1)} 2^{-2A} \gg d(|F(n_2, -n_1)|)^{-2A} \gg |\underline{n}|^{-\varepsilon},$$

where $d(*)$ is the usual divisor function.

It remains to consider bad primes, along with the remaining primes $p \leq 2A$. Let p_0 be the largest of all these primes, so that p_0 depends only on the original forms Q_1 and Q_2. Then according to Proposition 4.4 we have

$$\sigma_p(\underline{n}) \geq \varpi_p |F(n_2, -n_1)|_p^{k-2}$$

for $p \leq p_0$. The required lower bound then follows since $\varpi_p \gg 1$ for $p \leq p_0$.

In the special case $(n_1, n_2) = (0, 0)$ similar results continue to hold.

Proposition 6.3 *The singular series $\mathfrak{S}(\underline{0})$ is absolutely convergent providing that $k \geq 6$. Indeed we then have*

$$\sum_{q \geq R} \frac{1}{q^k} |T(\underline{0}; q)| \ll R^{-1/3}, \tag{6.7}$$

where the implied constant depends only on Q_1 and Q_2.

Proposition 6.4 *Let $k \geq 6$ and suppose further that for each prime p the system $\underline{Q}(\mathbf{x}) = \underline{0}$ has a nonzero solution $\mathbf{x}_p \in \mathbb{Z}_p^k$. Then $\mathfrak{S}(\underline{0}) > 0$.*

Proposition 6.4 is an immediate consequence of Propositions 4.5 and 6.3.

To prove Proposition 6.3 we note that there are no Type I primes, and that

$$\psi_p = 1 + O(p^{11/6-k/2}) + O(p^{14/3-k})$$

for Type II primes, as in (6.3). Thus $\psi_p = 1 + O(p^{-7/6})$ for $k \geq 6$ and all good primes p. Moreover $\psi_p = O_p(1)$ for bad primes p as before. One may then establish (6.7) by exactly the same argument used for (6.2). Finally we note that the absolute convergence of $\mathfrak{S}(\underline{0})$ is a direct consequence of (6.7).

7 Application of the circle method

We now begin our detailed application of the circle method.

7.1 Division into major and minor arcs

Let $Q = B^{\Delta}$ for some fixed $\Delta > 0$ to be chosen later. We define the box

$$I(a_1, a_2; q) = \left[\frac{a_1}{q} - \frac{Q}{B^2}, \frac{a_1}{q} + \frac{Q}{B^2}\right] \times \left[\frac{a_2}{q} - \frac{Q}{B^2}, \frac{a_2}{q} + \frac{Q}{B^2}\right]$$

for any integers $1 \leq a_1, a_2 \leq q \leq Q$. Such boxes are disjoint provided that

$$Q = B^{\Delta}, \qquad \Delta < 2/3,$$

since if $(a_1, a_2; q) \neq (a_1', a_2'; q')$, then for $j = 1$ or 2 we have

$$\left|\frac{a_j}{q} - \frac{a_j'}{q'}\right| \geq \frac{1}{qq'} \geq \frac{1}{Q^2} > 2\frac{Q}{B^2},$$

for large enough B. We now define the major arcs to be

$$\mathfrak{M}(\Delta) = \bigcup_{1 \leq q \leq Q} \bigcup_{\substack{1 \leq a_1, a_2 \leq q \\ (a_1, a_2, q) = 1}} I(a_1, a_2; q)$$

and we take the minor arcs to be the complement of the major arcs in $[0,1]^2$:

$$\mathfrak{m}(\Delta) = [0,1]^2 \setminus \mathfrak{M}(\Delta).$$

7.2 The major arcs: the singular integral and singular series

Recall the definition

$$S(\alpha_1, \alpha_2) = \sum_{\mathbf{x} \in \mathbb{Z}^k} e(\alpha_1 Q_1(\mathbf{x}) + \alpha_2 Q_2(\mathbf{x})) w_B(x),$$

and the representation function

$$R_B(n_1,n_2)=\iint_{[0,1]^2} S(\alpha_1,\alpha_2)e(-\underline{\alpha}\cdot\underline{n})d\alpha_1 d\alpha_2.$$

The contribution of the major arcs to $R_B(n_1,n_2)$ may now be represented as

$$\iint_{\mathfrak{M}(\Delta)} S(\alpha_1,\alpha_2)e(-\underline{\alpha}\cdot\underline{n})d\alpha_1 d\alpha_2 = \sum_{1\le q\le Q}\sum_{\substack{1\le a_1,a_1\le q\\(a_1,a_2,q)=1}}\iint_{I(a_1,a_2;q)} S(\alpha_1,\alpha_2)e(-\underline{\alpha}\cdot\underline{n})d\alpha_1 d\alpha_2.$$

Our goal is to approximate this by a main term of size B^{k-4}, times a singular integral and a singular series.

Proposition 7.1 *Suppose either that $k\ge 5$ and $|\underline{n}|\ll B^2$ with $F(n_2,-n_1)\ne 0$, or that $k\ge 6$ and $(n_1,n_2)=(0,0)$. Then for any fixed positive $\Delta\le 1/8$ we have*

$$\iint_{\mathfrak{M}(\Delta)} S(\underline{\alpha})e(-\underline{\alpha}\cdot\underline{n})d\alpha_1 d\alpha_2=\mathfrak{S}(\underline{n})\mathcal{J}_w(B^{-2}\underline{n})B^{k-4}+E(\underline{n}),$$

with

$$E(\underline{n})\ll B^{k-4-\Delta/4}, \tag{7.1}$$

where $\mathfrak{S}(\underline{n})$ and $\mathcal{J}_w(\underline{\mu})$ are given by (6.1) and (3.9) respectively.

We will first prove by a standard argument that:

Lemma 7.1 *If $\underline{\alpha}$ belongs to one of the major arcs $I(a_1,a_2;q)$, and $\underline{\theta}=\underline{\alpha}-\underline{a}/q$, then*

$$S(\alpha_1,\alpha_2)=q^{-k}B^kS_q(a_1,a_2)I(B^2\underline{\theta})+O(B^{k-1+2\Delta}), \tag{7.2}$$

with $I(\underline{\phi})$ given by (3.11).

Write $\theta_j=\alpha_j-a_j/q$ for $j=1,2$. Then

$$\begin{aligned} S(\alpha_1,\alpha_2) &= \sum_{\mathbf{x}\in\mathbb{Z}^k} e(\underline{\alpha}\cdot\underline{Q}(\mathbf{x}))w_B(\mathbf{x})\\ &= \sum_{\mathbf{y}\ (\mathrm{mod}\ q)}\sum_{\mathbf{z}\in\mathbb{Z}^k} e(\underline{\alpha}\cdot\underline{Q}(q\mathbf{z}+\mathbf{y}))w_B(q\mathbf{z}+\mathbf{y})\\ &= \sum_{\mathbf{y}\ (\mathrm{mod}\ q)} e_q(\underline{a}\cdot\underline{Q}(\mathbf{y}))\sum_{\mathbf{z}\in\mathbb{Z}^k} f(\mathbf{z}), \end{aligned} \tag{7.3}$$

where

$$f(\mathbf{z})=e(\underline{\theta}\cdot\underline{Q}(q\mathbf{z}+\mathbf{y}))w_B(q\mathbf{z}+\mathbf{y}).$$

Note that $f(\mathbf{z})$ is supported in a k-dimensional cube K centred at the origin, with side-length of order $B/q+1 \ll B/q$. We will now replace the summation over $\mathbf{z}$ by integration over a continuous variable, incurring a small error in the process. Note first that for any $\mathbf{w} \in [0,1]^k$ we have

$$|f(\mathbf{z}+\mathbf{w}) - f(\mathbf{z})| \leq k \max_{\mathbf{u}\in[0,1]^k} |\nabla f(\mathbf{z}+\mathbf{u})|$$

by the mean-value theorem. Thus

$$\begin{aligned} |\int_{\mathbb{R}^k} f(\mathbf{z})d\mathbf{z} - \sum_{\mathbf{z}\in\mathbb{Z}^k} f(\mathbf{z})| &\ll (B/q)^k \max_{\mathbf{z}\in K} |\nabla f(\mathbf{z})| \\ &\ll (B/q)^k \max_{\mathbf{z}\in K} (q/B + q|\underline{\theta}|.|q\mathbf{z}+\mathbf{y}|) \\ &\ll q^{1-k}B^{k-1} + |\underline{\theta}|q^{1-k}B^{k+1}. \end{aligned}$$

Consequently,

$$\sum_{\mathbf{z}\in\mathbb{Z}^k} f(\mathbf{z}) = \int_{\mathbb{R}^k} e(\underline{\theta}\cdot \underline{Q}(q\mathbf{z}+\mathbf{y}))w_B(q\mathbf{z}+\mathbf{y})d\mathbf{z} + O(|\underline{\theta}|q^{1-k}B^{k+1} + q^{1-k}B^{k-1}),$$

which upon setting $B\mathbf{x} = \mathbf{z}q + \mathbf{y}$ becomes

$$\sum_{\mathbf{z}\in\mathbb{Z}^k} f(\mathbf{z}) = \frac{B^k}{q^k}\int_{\mathbb{R}^k} e(B^2\underline{\theta}\cdot \underline{Q}(\mathbf{x}))w(\mathbf{x})d\mathbf{x} + O(|\underline{\theta}|q^{1-k}B^{k+1} + q^{1-k}B^{k-1}).$$

Applying this to the innermost sum in (7.3), we then see that

$$S(\alpha_1,\alpha_2) = q^{-k}B^kS_q(a_1,a_2)I(B^2\underline{\theta}) + O(B^{k-1}q(|\underline{\theta}|B^2+1)). \qquad (7.4)$$

This proves the lemma, upon noting that $|\underline{\theta}| \leq B^{-2+\Delta}$ and $q \leq B^{\Delta}$ in the major arcs, so that the error term is no more than $O(B^{k-1+2\Delta})$.

Our goal is now to integrate $S(\alpha_1,\alpha_2)$ over the full collection of major arcs. Note that the measure of the total collection of major arcs is

$$\ll B^{\Delta}\cdot B^{2\Delta}\cdot (B^{-2+\Delta})^2 \ll B^{-4+5\Delta}.$$

Thus Lemma 7.1 immediately implies:

Lemma 7.2 *We have*

$$\begin{aligned} \iint_{\mathfrak{M}(\Delta)} S(\alpha_1,\alpha_2)e(-\underline{\alpha}\cdot\underline{n})d\alpha_1 d\alpha_2 &= B^{k-4}\mathcal{J}_w(B^{-2}\underline{n};B^{\Delta})\sum_{q\leq B^{\Delta}} q^{-k}T(\underline{n};q) \\ &\quad +O(B^{k-5+7\Delta}) \end{aligned}$$

with $\mathcal{J}_w(\underline{n};R)$ *given by (3.10).*

Finally, we apply the results of Propositions 3.1 and 6.1 to the truncated singular integral and singular series in order to pass to the limit on the right hand side. We obtain:

$$\iint_{\mathfrak{M}(\Delta)} S(\alpha_1,\alpha_2)e(-\underline{\alpha}\cdot\underline{n})d\alpha_1 d\alpha_2 = \mathfrak{S}(\underline{n})\mathcal{J}_w(B^{-2}\underline{n})B^{k-4} + O(B^{k-4-\Delta/3+\varepsilon}) + O(B^{k-5+7\Delta}),$$

for $F(n_2,-n_1)\neq 0$, as long as $k\geq 5$. Similarly, if $k\geq 6$ and $(n_1,n_2)=(0,0)$ we may apply Propositions 3.1 and 6.3. Proposition 7.1 then follows, upon restricting $\Delta\leq 1/8$ and replacing $B^{-\Delta/3+\varepsilon}$ by $B^{-\Delta/4}$.

8 Proof of Theorem 1.1

8.1 The mean square argument

We are now ready to make precise the mean square argument sketched in §1.1. Proposition 7.1 establishes (1.13) with

$$M(n_1,n_2)=\mathfrak{S}(\underline{n})\mathcal{J}_w(B^{-2}\underline{n})B^{k-4}$$

and $E(n_1,n_2)=O(B^{k-4-\Delta/4})$, whence (1.14) yields

$$\sum_{\substack{\max(|n_1|,|n_2|)\leq N\\ F(n_2,-n_1)\neq 0}} |R_B(n_1,n_2)-\mathfrak{S}(\underline{n})\mathcal{J}_w(B^{-2}\underline{n})B^{k-4}|^2 \ll \iint_{\mathfrak{m}(\Delta)} |S(\alpha_1,\alpha_2)|^2 d\alpha_1 d\alpha_2 + B^{2k-4-\Delta/2},$$

provided that $N\ll B^2$.

The crucial result is the following upper bound for the minor arcs integral.

Proposition 8.1 *For any $k\geq 5$, any $\varepsilon>0$, and any $\Delta\in(0,1/6)$, we have*

$$\iint_{\mathfrak{m}(\Delta)} |S(\alpha_1,\alpha_2)|^2 d\alpha_1 d\alpha_2 \ll B^{2k-4-2\Delta+\varepsilon}. \tag{8.1}$$

The choice $\Delta=1/8$ then establishes Theorem 1.1.

The proof of Proposition 8.1 is the most delicate part of the paper. We begin by employing a 2-dimensional Dirichlet approximation with a parameter $S\geq 1$. Thus for every pair α_1,α_2 in $[0,1]$ there exist $1\leq q\leq S$ and $1\leq a_1,a_2\leq q$ with $(a_1,a_2,q)=1$ such that

$$\left|\alpha_1-\frac{a_1}{q}\right|\leq\frac{1}{q\sqrt{S}},\quad\text{and}\quad\left|\alpha_2-\frac{a_2}{q}\right|\leq\frac{1}{q\sqrt{S}}.$$

Given α_1,α_2 and approximations $\alpha_1=a_1/q+\theta_1,\alpha_2=a_2/q+\theta_2$ of the above type, then if $\alpha_1,\alpha_2\in\mathfrak{m}(\Delta)$ at least one of the inequalities

$$q\leq B^{\Delta},\qquad |\theta_1|\leq B^{-2+\Delta},\qquad |\theta_2|\leq B^{-2+\Delta}, \tag{8.2}$$

must fail to hold. For our application we shall choose

$$S = B^{4/3},$$

which is essentially optimal.

We bound the integral (8.1) from above, using a collection of dyadic sums

$$\Sigma(R,\phi_1,\phi_2) = \sum_{R\le q<2R} \sum_{\substack{1\le a_1,a_2\le q\\ (a_1,a_2,q)=1}} \iint_{\{\phi_1,\phi_2\}} |S(a_1/q+\theta_1, a_2/q+\theta_2)|^2 d\underline{\theta}. \quad (8.3)$$

The reader should recall that $\iint_{\{\phi_1,\phi_2\}}$ denotes an integral over the range

$$([-2\phi_1,-\phi_1]\cup[\phi_1,2\phi_1])\times([-2\phi_2,-\phi_2]\cup[\phi_2,2\phi_2]).$$

We will prove:

Proposition 8.2 *For any $k\ge 5$, any $\varepsilon>0$, and any $\Delta\in(0,1/6)$, we have*

$$\Sigma(R,\phi_1,\phi_2) \ll B^{2k-4-2\Delta+\varepsilon} \quad (8.4)$$

for $R\ll B^{4/3}$ and $\phi_1,\phi_2\ll R^{-1}B^{-2/3}$, unless all three conditions

$$R\le \frac{1}{2}B^{\Delta}, \qquad \phi_1\le\frac{1}{2}B^{-2+\Delta}, \qquad \phi_2\le\frac{1}{2}B^{-2+\Delta}, \quad (8.5)$$

hold.

Before proving Proposition 8.2 we show how it implies Proposition 8.1. When $q\ge B^{\Delta}$ we handle the squares

$$\{(\alpha_1,\alpha_2)=(a_1/q+\theta_1,a_2/q+\theta_2):\max(|\theta_1|,|\theta_2|)\le B^{-k}\}$$

by a trivial estimate, producing an overall contribution $\ll S^3B^{-2k}.B^{2k}$ to (8.1), since we trivially have $S(\alpha_1,\alpha_2)\ll B^k$. When $q\le B^{\Delta}$ we know that

$$\max(|\theta_1|,|\theta_2|)\ge B^{-2+\Delta}$$

since at least one of the conditions (8.2) is known to fail. The remaining cases may then be covered by $O((\log B)^3)$ dyadic intervals for q, θ_1 and θ_2.

Proposition 8.2 now yields

$$\iint_{\mathfrak{m}(\Delta)} |S(\alpha_1,\alpha_2)|^2 d\alpha_1 d\alpha_2 \ll S^3 + (\log B)^3 \sup \Sigma(R,\phi_1,\phi_2),$$

where the supremum is taken over all dyadic parameters with $0<R<S$ and $B^{-k}\le\phi_1,\phi_2\le(R\sqrt{S})^{-1}$ such that not all three conditions (8.5) hold. This clearly suffices for Proposition 8.1, with the choice $S=B^{4/3}$.

8.2 Proof of Proposition 8.2

Recalling the definition (1.10) of $S(\alpha_1, \alpha_2)$, we may expand the integrand in (8.3) and write $\mathbf{x}_j = \mathbf{l}_j q + \mathbf{r}_j$, where $\mathbf{l}_j \in \mathbb{Z}^k$ and $\mathbf{r}_j \in (\mathbb{Z}/q\mathbb{Z})^k$ for $j = 1, 2$. This produces

$$|S(a_1/q + \theta_1, a_2/q + \theta_2)|^2 = \sum_{\substack{\mathbf{r}_1 \pmod q \\ \mathbf{r}_2 \pmod q}} e_q(\underline{a} \cdot \underline{Q}(\mathbf{r}_1) - \underline{a} \cdot \underline{Q}(\mathbf{r}_2))\Sigma(\underline{\theta}, \mathbf{r}_1, \mathbf{r}_2, q),$$

where we have temporarily set

$$\Sigma(\underline{\theta}, \mathbf{r}_1, \mathbf{r}_2, q) = \sum_{\mathbf{l}_1, \mathbf{l}_2 \in \mathbb{Z}^k} e(\underline{\theta} \cdot \underline{Q}(\mathbf{l}_1 q + \mathbf{r}_1) - \underline{\theta} \cdot \underline{Q}(\mathbf{l}_2 q + \mathbf{r}_2)) w_B(\mathbf{l}_1 q + \mathbf{r}_1) w_B(\mathbf{l}_2 q + \mathbf{r}_2).$$

Applying Poisson summation to the sum over $\mathbf{l}_1, \mathbf{l}_2$, we may rewrite this as

$$\Sigma(\underline{\theta}, \mathbf{r}_1, \mathbf{r}_2, q) = (\frac{B}{q})^{2k} \sum_{\mathbf{l} \in \mathbb{Z}^{2k}} e_q(\mathbf{r} \cdot \mathbf{l}) J(B^2 \underline{\theta}, B\mathbf{l}/q),$$

where for any $\boldsymbol{\lambda} \in \mathbb{R}^{2k}$ we have defined

$$J(\underline{\nu}, \boldsymbol{\lambda}) = \iint_{\mathbb{R}^{2k}} e(\underline{\nu} \cdot \underline{Q}(\mathbf{u}_1) - \underline{\nu} \cdot \underline{Q}(\mathbf{u}_2)) w(\mathbf{u}_1) w(\mathbf{u}_2) e(-\mathbf{u} \cdot \boldsymbol{\lambda}) d\mathbf{u}.$$

It follows that

$$|S(a_1/q + \theta_1, a_2/q + \theta_2)|^2 = (\frac{B}{q})^{2k} \sum_{\mathbf{l} \in \mathbb{Z}^{2k}} S(\mathbf{l}; q) J(B^2 \underline{\theta}, B\mathbf{l}/q)$$

with

$$S(\mathbf{l}; q) = \sum_{\substack{1 \le a_1, a_2 \le q \\ (a_1, a_2, q) = 1}} \sum_{\substack{\mathbf{r}_1 \pmod q \\ \mathbf{r}_2 \pmod q}} e_q(\underline{a} \cdot \underline{Q}(\mathbf{r}_1) - \underline{a} \cdot \underline{Q}(\mathbf{r}_2)) e_q(\mathbf{r} \cdot \mathbf{l}).$$

We then conclude that

$$\Sigma(R, \phi_1, \phi_2) = B^{2k} \sum_{R \le q < 2R} \frac{1}{q^{2k}} \sum_{\mathbf{l} \in \mathbb{Z}^{2k}} S(\mathbf{l}; q) \mathcal{I}_{\{\phi_1, \phi_2\}}(\mathbf{l}; q), \tag{8.6}$$

where

$$\mathcal{I}_{\{\phi_1, \phi_2\}}(\mathbf{l}; q) = \iint_{\{\phi_1, \phi_2\}} J(B^2 \underline{\theta}, B\mathbf{l}/q) d\underline{\theta} = B^{-4} \iint_{B^2\{\phi_1, \phi_2\}} J(\underline{\nu}, B\mathbf{l}/q) d\underline{\nu}.$$

We now observe that $J(\underline{\nu}, \boldsymbol{\lambda})$ is essentially the integral $I(\underline{\nu} \cdot \underline{F}; \boldsymbol{\lambda})$ occurring in Lemma 3.4. Indeed Lemma 3.1 shows that

$$J(\underline{\nu}, \boldsymbol{\lambda}) \ll_M |\boldsymbol{\lambda}|^{-M}$$

for any fixed $M > 0$, when $|\boldsymbol{\lambda}| \gg |\underline{\nu}|$. We may therefore deduce the following bound, via Lemma 3.4.

Lemma 8.1 *Let $\phi^* = \max(\phi_1, \phi_2)$. Then*

$$\iint_{B^2\{\phi_1,\phi_2\}} J(\underline{\nu}, B\mathbf{l}/q)d\underline{\nu} \ll (B^2\phi^*)^2 \min(1, (B^2\phi^*)^{-k}) \log B. \tag{8.7}$$

Moreover, for any $M > 0$ we have

$$\iint_{B^2\{\phi_1,\phi_2\}} J(\underline{\nu}, B\mathbf{l}/q)d\underline{\nu} \ll_M (B^2\phi^*)^2 (B|\mathbf{l}|/R)^{-M}, \tag{8.8}$$

if $|\mathbf{l}| \gg RB\phi^*$.

We trivially have $S(\mathbf{l}; q) \ll q^{2k+2}$, so on writing

$$L = RB^{-1+\varepsilon}(1 + B^2\phi^*)$$

with a small $\varepsilon > 0$, and assuming that $M > 2k + 1$, we see that

$$\begin{aligned} B^{2k} \sum_{R \le q < 2R} \frac{1}{q^{2k}} \sum_{|\mathbf{l}| \ge L} &|S(\mathbf{l}; q)\mathcal{I}_{\{\phi_1,\phi_2\}}(\mathbf{l}; q)| \\ &\ll_{\varepsilon,M} \quad B^{2k-4}R^3(B^2\phi^*)^2(R/B)^M \sum_{|\mathbf{l}| \ge L} |\mathbf{l}|^{-M} \\ &\ll_{\varepsilon,M} \quad B^{2k}R^3(R/B)^M L^{2k+1-M} \\ &\ll_{\varepsilon,M} \quad B^{2k}R^3(R/B)^M (RB^{-1+\varepsilon})^{2k+1-M} \\ &\ll_{\varepsilon,M} \quad B^{2k}R^3(RB^{-1+\varepsilon})^{2k+1}B^{-\varepsilon M}. \end{aligned}$$

Thus, taking M as a suitably large multiple of ε^{-1}, we see that terms with $|\mathbf{l}| \ge L$ contribute $O(1)$ to $\Sigma(R, \phi_1, \phi_2)$. This is satisfactory for Proposition 8.2.

We dispose next of the term $\mathbf{l} = \mathbf{0}$. As noted in (5.16),

$$S(\mathbf{0}; q) \ll q^{k+2+\varepsilon}$$

for any $\varepsilon > 0$. Then, applying (8.7) with $\mathbf{l} = \mathbf{0}$ we conclude that the contribution to $\Sigma(R, \phi_1, \phi_2)$ is

$$\begin{aligned} &\ll \quad B^{2k-4}(B^2\phi^*)^2 \min(1, (B^2\phi^*)^{-k})(\log B) \sum_{R \le q < 2R} q^{-2k}q^{k+2+\varepsilon} \\ &\ll \quad B^{2k-4} \min((B^2\phi^*)^2, (B^2\phi^*)^{2-k})(\log B)R^{-k+3+\varepsilon}. \end{aligned}$$

When $R \le \frac{1}{2}B^\Delta$ we have $\phi^* \ge \frac{1}{2}B^{-2+\Delta}$ and the above is

$$\ll B^{2k-4}(B^2\phi^*)^{2-k}(\log B)R^{-k+3+\varepsilon} \ll B^{2k-4}B^{\Delta(2-k)}(\log B).$$

This too is satisfactory for Proposition 8.2. Similarly when $R \ge \frac{1}{2}B^\Delta$ we see that our bound becomes

$$\ll B^{2k-4}(\log B)R^{-k+3+\varepsilon} \ll B^{2k-4}(\log B)B^{\Delta(-k+3+\varepsilon)}$$

which again is satisfactory.

It remains to handle the range $1 \leq |\mathbf{l}| \leq L$. Using the bound (8.7) we see that the contribution to $\Sigma(R, \phi_1, \phi_2)$ will be

$$\ll B^{2k-4} \min((B^2\phi^*)^2, (B^2\phi^*)^{2-k})(\log B) \sum_{R \leq q < 2R} q^{-2k} \sum_{1 \leq |\mathbf{l}| \leq L} |S(\mathbf{l}; q)|. \quad (8.9)$$

We may now apply Lemma 5.6, which shows the above to be

$$\ll B^{2k-4} \min((B^2\phi^*)^2, (B^2\phi^*)^{2-k})(\log B) R^{-2k} \\ \times (R^{k+2+\varepsilon} L^{2k+\varepsilon} + R^{k+3+\varepsilon} L^{2k-3+\varepsilon}). \quad (8.10)$$

When $B^2\phi^* \geq 1$ we have $L \ll RB^{1+\varepsilon}\phi^*$ and this becomes

$$\begin{aligned} &\ll B^{2k-4+3k\varepsilon}(B^2\phi^*)^{2-k} R^{-2k}(R^{k+2}(RB\phi^*)^{2k} + R^{k+3}(RB\phi^*)^{2k-3}) \\ &= B^{2k-4+3k\varepsilon}(R^{k+2}B^4{\phi^*}^{k+2} + R^k B {\phi^*}^{k-1}). \end{aligned} \quad (8.11)$$

Here we use the crude bound $RL \ll B^2$ to show that $(RL)^\varepsilon \ll B^{2\varepsilon}$. On using first the assumption that $\phi^* \ll R^{-1}B^{-2/3}$, and then that $R \ll B^{4/3}$, we see that (8.11) is

$$\ll B^{2k-4+3k\varepsilon}(B^{-(2k-8)/3} + RB^{-(2k-5)/3}) \ll B^{2k-4+3k\varepsilon}.B^{-(2k-9)/3}. \quad (8.12)$$

Since $k \geq 5$ this is satisfactory for Proposition 8.2, after re-defining ε.

Finally, if $B^2\phi^* \leq 1$, then $L \ll RB^{-1+\varepsilon}$, so that (8.10) becomes

$$\ll B^{2k-4}(\log B)R^{-2k}(R^{k+2+\varepsilon}(RB^{-1+\varepsilon})^{2k+\varepsilon} + R^{k+3+\varepsilon}(RB^{-1+\varepsilon})^{2k-3+\varepsilon}).$$

We may simplify this if ε is small enough to get

$$\ll B^{2k-4+3k\varepsilon}(R^{k+2}B^{-2k} + R^k B^{3-2k}) \ll B^{2k-4+3k\varepsilon}.B^{-(2k-9)/3}, \quad (8.13)$$

since $R \ll B^{4/3}$. For $k \geq 5$ this is also satisfactory for Proposition 8.2, after re-defining ε.

We remark here that it is now visible that the most significant terms (8.12) and (8.13) contributing to the minor arcs involve a saving $O(B^{-(2k-9)/3})$, so that the result is non-trivial for $k > 9/2$. Thus to handle $k = 4$ one would have to do more than shave off a small power of B.

9 Proof of Theorems 1.2 and 1.7

We first prove Theorem 1.2. The statements about $\mathfrak{S}(\underline{n})$ follow from Propositions 6.1 and 6.2, while the uniform boundedness of $\mathcal{J}_w(\underline{\mu})$ is part of Proposition 3.1. Thus it remains to consider lower bounds for the singular integral $\mathcal{J}_w(\underline{\mu})$.

We begin by establishing the following result.

Lemma 9.1 *Let $A_1 > A_2 > 0$ be given. Then there exists $\Lambda > 0$, dependent only on A_1, A_2 and $\underline{Q}$, such that if $A_2 \leq |\underline{\nu}| \leq A_1$ and if $\underline{Q}(\mathbf{x}) = \underline{\nu}$ has a solution $\mathbf{x} \in \mathbb{R}^k$, then in fact there exists a real solution of $\underline{Q}(\mathbf{x}) = \underline{\nu}$ satisfying $|\mathbf{x}| \leq \Lambda$.*

We may clearly reduce to the case $|\underline{\nu}| = 1$ by rescaling. To find a suitable value for Λ we consider two cases. First suppose that $\underline{Q}(\mathbf{x}) \neq \underline{0}$ for all $\mathbf{x}$ with $|\mathbf{x}| = 1$. Then by continuity and compactness, we deduce that $\inf_{|\mathbf{x}|=1} |\underline{Q}(\mathbf{x})| > 0$. Thus for any $\mathbf{x}$ such that $\underline{Q}(\mathbf{x}) = \underline{\nu}$ we have

$$1 = |\underline{\nu}| = |Q(\mathbf{x})| \geq |\mathbf{x}|^2 \inf_{|\mathbf{x}|=1} |\underline{Q}(\mathbf{x})|.$$

It follows that if we define

$$\Lambda = \left(\inf_{|\mathbf{x}|=1} |\underline{Q}(\mathbf{x})| \right)^{-1/2}$$

then $|\mathbf{x}| \leq \Lambda$.

In the alternative case there exists $\underline{a}$ with $|\underline{a}| = 1$ such that $\underline{Q}(\underline{a}) = \underline{0}$. Then by Condition 1 we have $\mathrm{rk}(J(\underline{a})) = 2$. We shall suppose that

$$\begin{vmatrix} \frac{\partial Q_1(\underline{a})}{\partial x_1} & \frac{\partial Q_1(\underline{a})}{\partial x_2} \\ \frac{\partial Q_2(\underline{a})}{\partial x_1} & \frac{\partial Q_2(\underline{a})}{\partial x_2} \end{vmatrix} \neq 0,$$

as we may, without any loss of generality. We can therefore apply the Implicit Function Theorem to the mapping $F : \mathbb{R}^4 \to \mathbb{R}^2$ given by

$$F(t_1, t_2, \mu_1, \mu_2) = \underline{Q}(t_1 + a_1, t_2 + a_2, a_3, \ldots, a_n) - \underline{\mu}.$$

Since $F(\underline{0}, \underline{0}) = \underline{0}$ we deduce that there is a $\delta > 0$ and a continuous function

$$G : \{\underline{\mu} : |\underline{\mu}| \leq \delta\} \to \mathbb{R}^2$$

such that $G(\underline{0}) = \underline{0}$ and $F(G(\underline{\mu}), \underline{\mu}) = \underline{0}$. Since G is continuous it is bounded for $|\underline{\mu}| \leq \delta$, by κ, say. Thus if $|\underline{\mu}| \leq \delta$ there will be a solution

$$\mathbf{x} = (t_1 + a_1, t_2 + a_2, a_3, \ldots, a_n)$$

of $\underline{Q}(\mathbf{x}) = \underline{\mu}$ satisfying $|\mathbf{x}| \leq 1 + \kappa$. Hence, given $|\underline{\nu}| = 1$, we take $\delta > 0$ as found above and set $\underline{\mu} = \delta\underline{\nu}$ so that there exists $\mathbf{x}$ with $|\mathbf{x}| \leq 1 + \kappa$ such that $\underline{Q}(\mathbf{x}) = \underline{\mu} = \delta\underline{\nu}$. Then by setting $\mathbf{y} = \delta^{-1/2}\mathbf{x}$ we provide a solution to $\underline{Q}(\mathbf{y}) = \underline{\nu}$ with $|\mathbf{y}| \leq \delta^{-1/2}(1 + \kappa)$. This establishes the lemma in the second case, with $\Lambda = \delta^{-1/2}(1 + \kappa)$.

Our next result is a real analogue of Lemma 4.4.

Lemma 9.2 *Let $A_1 > A_2 > 0$ be given. Let $\mathbf{x} \in \mathbb{R}^k$ with $A_2 \leq |\mathbf{x}| \leq A_1$, and suppose that $\underline{Q}(\mathbf{x}) = \underline{\nu}$. Then*

$$F(\nu_2, -\nu_1) \ll \max_{i,j} |\Delta_{ij}(\mathbf{x})|^2.$$

Again we may reduce to the case $|\underline{\nu}| = 1$ by rescaling. Since the proof of the lemma is completely analogous to that of Lemma 4.4 we leave the details to the reader.

To complete the proof of Theorem 1.2 we require one further lemma.

Lemma 9.3 *Let $A_1 > A_2 > 0$ be given. Then there is a constant $\kappa_0 = \kappa_0(A_1, A_2, Q_1, Q_2)$ with $0 < \kappa_0 \leq 1$ such that for any $\kappa \leq \kappa_0$ the following holds. Let $\underline{a} \in \mathbb{R}^k$ with $A_2 \leq |\underline{a}| \leq A_1$. Write*

$$M = \max_{i,j} |\Delta_{ij}(\underline{a})|$$

and assume that $M > 0$. Re-order the indices i so that $|\Delta_{12}(\underline{a})| = M$. Then for any $x_3, \ldots, x_k$ with

$$\max_{3 \leq i \leq k} |x_i| \leq (\kappa M)^2 \tag{9.1}$$

there exist x_1 and x_2 in the square S given by

$$S = \{(x_1, x_2) \in \mathbb{R}^2 : \max(|x_1|, |x_2|) \leq \kappa M\} \tag{9.2}$$

such that

$$\underline{Q}(\underline{a} + \mathbf{x}) = \underline{Q}(\underline{a}).$$

It will suffice to show that the conclusion of the lemma holds whenever $\kappa > 0$ is sufficiently small in terms of A_1, A_2, Q_1 and Q_2. For the proof it will be convenient to write

$$\mathcal{M}(\mathbf{x}) = \begin{pmatrix} \frac{\partial Q_1(\underline{x})}{\partial x_1} & \frac{\partial Q_1(\underline{x})}{\partial x_2} \\ \frac{\partial Q_2(\underline{x})}{\partial x_1} & \frac{\partial Q_2(\underline{x})}{\partial x_2} \end{pmatrix}.$$

Then $||\mathcal{M}(\mathbf{x})|| \ll 1$ if $|\mathbf{x}| \ll 1$, and

$$|\det(\mathcal{M}(\underline{x}))| \geq M/2 \tag{9.3}$$

if $|\mathbf{x} - \underline{a}| \ll M$ with a small enough implied constant. It follows that

$$||\mathcal{M}(\mathbf{x})^{-1}|| \ll M^{-1} \tag{9.4}$$

when $|\mathbf{x} - \underline{a}| \ll M$.

We now write each $\mathbf{x} \in \mathbb{R}^k$ in the shape $(\underline{u}, \underline{v})$ where $\underline{u}$ corresponds to the first two variables x_1, x_2 and $\underline{v}$ to the remaining variables $x_3, \ldots, x_k$. It will also be convenient to write $\underline{a} = (\underline{b}, \underline{c})$ accordingly. For each vector $\underline{v} \in \mathbb{R}^{k-2}$ we now consider the function $F_{\underline{v}} : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$F_{\underline{v}}(\underline{u}) = \underline{u} - \mathcal{M}(\underline{b}, \underline{v})^{-1}\{\underline{Q}(\underline{b} + \underline{u}, \underline{v}) - \underline{Q}(\underline{b}, \underline{c})\}.$$

It follows from the definition that

$$F_{\underline{v}}(\underline{u}) = -\mathcal{M}(\underline{b}, \underline{v})^{-1}\{\underline{Q}(\underline{b}, \underline{v}) + \underline{Q}(\underline{u}, \underline{0}) - \underline{Q}(\underline{b}, \underline{c})\}, \tag{9.5}$$

whence (9.4) yields

$$F_{\underline{v}}(\underline{u}) \ll M^{-1}(|\underline{u}|^2 + |\underline{v} - \underline{c}|)$$

if $|\underline{v} - \underline{c}| \ll M$ with a sufficiently small implied constant. Hence choosing $\kappa \in (0, 1)$ sufficiently small, if $\underline{u} = (x_1, x_2)$ lies in S and if $\underline{v} - \underline{c} = (x_3, \ldots, x_k)$ satisfies (9.1), then $F_{\underline{v}}$ maps the square (9.2) to itself.

Moreover if we have two vectors $\underline{u}^{(1)}, \underline{u}^{(2)}$ in S, then

$$F_{\underline{v}}(\underline{u}^{(1)}) - F_{\underline{v}}(\underline{u}^{(2)}) = \mathcal{M}(\underline{b}, \underline{v})^{-1}\{\underline{Q}(\underline{u}^{(2)}, \underline{0}) - \underline{Q}(\underline{u}^{(1)}, \underline{0})\},$$

and

$$Q_i(\underline{u}^{(2)}, \underline{0}) - Q_i(\underline{u}^{(1)}, \underline{0}) \ll |\underline{u}^{(1)} - \underline{u}^{(2)}| \max(|\underline{u}^{(1)}|, |\underline{u}^{(2)}|) \ll \kappa M |\underline{u}^{(1)} - \underline{u}^{(2)}|.$$

It follows that (9.4) yields

$$|F_{\underline{v}}(\underline{u}^{(1)}) - F_{\underline{v}}(\underline{u}^{(2)})| \ll \kappa |\underline{u}^{(1)} - \underline{u}^{(2)}|$$

if $|\underline{v} - \underline{c}| \ll M$. We therefore conclude that if κ is small enough then the function $F_{\underline{v}}$ is a contraction mapping on S whenever (9.1) holds. It follows that $F_{\underline{v}}$ has a fixed point $\underline{u} \in S$, which means that

$$\underline{Q}(\underline{b} + \underline{u}, \underline{v}) = \underline{Q}(\underline{b}, \underline{c})$$

by construction of $F_{\underline{v}}$. The lemma now follows.

We are finally in a position to complete the proof of Theorem 1.2. Suppose that $1/2 \leq \max(|\mu_1|, |\mu_2|) \leq 1$, whence $1/\sqrt{2} \leq |\underline{\mu}| \leq \sqrt{2}$. Suppose further that $Q_1(\mathbf{x}) = \mu_1$, $Q_2(\mathbf{x}) = \mu_2$ has a solution $\mathbf{x} = \underline{a} \in \mathbb{R}^k$. According to Lemma 9.1 we may assume that $|\underline{a}| \leq \Lambda$ for some Λ depending only on Q_1 and Q_2. Moreover, since $\max(|Q_1(\underline{a})|, |Q_2(\underline{a})|) \geq 1/2$ we deduce that $|\underline{a}| \gg 1$. We shall take $C = 2 + \Lambda$ in Theorem 1.2, with Λ as above. Then if $w(\mathbf{x}) > 0$ for all $\mathbf{x}$ with $\max|x_i| \leq C$ we may use compactness to show that there is a constant $c_0 > 0$ such that $w(\mathbf{x}) \geq c_0$ for all such $\mathbf{x}$.

We now write $M = \max|\Delta_{ij}(\mathbf{a})|$ as in Lemma 9.3, whence Lemma 9.2 shows that $|F(\mu_2, -\mu_1)| \leq c_0 M^2$ for some c_0 depending only on Q_1 and Q_2. Now take $\kappa_0 = \kappa_0(\sqrt{2}, 1/\sqrt{2}, Q_1, Q_2)$ as in Lemma 9.3. Then if $0 < \kappa \leq \kappa_0$ and

$$|(x_3, \ldots, x_k)| \leq \kappa^2 c_0^{-1} |F(\mu_2, -\mu_1)| \tag{9.6}$$

we will have $|(x_3, \ldots, x_k)| \leq (\kappa M)^2$, whence Lemma 9.3 will produce values of x_1, x_2 with $\max(|x_1|, |x_2|) \leq \kappa M$ such that $\underline{Q}(\underline{a} + \mathbf{x}) = \underline{\mu}$. By taking κ sufficiently small we may ensure that $|\mathbf{x}| \leq 1$.

We now use the same notation $\underline{a} = (\underline{b}, \underline{c})$ as before, and set $\underline{u}_0 = (x_1, x_2)$ and $\underline{v} = (x_3, \ldots, x_k)$, so that for any $\underline{v}$ satisfying (9.6) there is a corresponding $\underline{u}_0$ such that $\underline{Q}(\underline{u}_0, \underline{v}) = \underline{\mu}$. We proceed to consider values of $\underline{Q}$ near to $\underline{\mu}$. If $c_1 > 0$ is small enough, then for any $\underline{v} = (x_3, \ldots, x_k)$ satisfying (9.6), and any $\varepsilon \in (0, 1)$, there is a square

$$\{\mathbf{u} = (u_1, u_2) : |u_1 - x_1| \leq c_1\varepsilon, \quad |u_2 - x_2| \leq c_1\varepsilon\}$$

on which $|\underline{Q}(\underline{b} + \underline{u}, \underline{c} + \underline{v}) - \underline{\mu}| \leq \varepsilon/2$. Moreover, if c_1 is small enough then we will have $|(\mathbf{b} + \mathbf{u}, \mathbf{c} + \mathbf{v})| \leq \Lambda + 2$ for all such $(\mathbf{u}, \mathbf{v})$. We therefore see that

$$\int_{\substack{|\mathbf{x}| \leq \Lambda + 2 \\ \max|Q_i(\mathbf{x}) - \mu_i| \leq \varepsilon}} \left(1 - \frac{|Q_1(\mathbf{x}) - \mu_1|}{\varepsilon}\right)\left(1 - \frac{|Q_2(\mathbf{x}) - \mu_2|}{\varepsilon}\right) d\mathbf{x}$$
$$\gg \quad \varepsilon^2 |F(\mu_2, -\mu_1)|^{k-2},$$

whence

$$\int_{\max|Q_i(\mathbf{x})-\mu_i|\le\varepsilon} w(\mathbf{x})\left(1-\frac{|Q_1(\mathbf{x})-\mu_1|}{\varepsilon}\right)\left(1-\frac{|Q_2(\mathbf{x})-\mu_2|}{\varepsilon}\right)d\mathbf{x}$$
$$\gg \quad \varepsilon^2|F(\mu_2,-\mu_1)|^{k-2}.$$

The claimed lower bound for $\mathcal{J}_w(\underline{\mu})$ then follows from Proposition 3.2.

We turn now to the proof of Theorem 1.7, which follows similar lines. The positivity of the singular series follows immediately from Propositions 6.3 and 6.4, so that it remains to show that $\mathcal{J}_w(\underline{0}) > 0$. We first do this under the assumption that $w(\mathbf{x})$ is supported on the hypercube $\max|x_i| \le 3$. We are supposing also that $\underline{Q}(\underline{a}) = \underline{0}$ for some non-zero real vector $\underline{a}$, and by homogeneity we may take $|\underline{a}| = 1$. Such a solution has $\mathrm{rk}(J(\underline{a})) = 2$ by Condition 1, whence $\max_{i,j}|\Delta_{i,j}(\underline{a})| > 0$. We may therefore complete the proof that $\mathcal{J}_w(\underline{0}) > 0$ using Lemma 9.3, just as we did for Theorem 1.2, but with each occurence of the numbers Λ and $F(\mu_2,-\mu_1)$ replaced by the value 1. Finally we note that we can rescale the weight $w(\mathbf{x})$ and the parameter B without affecting the conclusion that $\mathcal{J}_w(\underline{0}) > 0$. Since our theorem assumes that the support of $w(\mathbf{x})$ includes a small hypercube around the origin this allows us to suppose that in fact the support includes the set $\max|x_i| \le 3$. This observation completes the proof.

10 Proof of Theorems 1.3 and 1.4

It is easy to see, using a dyadic subdivision, that in proving Theorem 1.3 it will suffice to handle pairs of integers n_1, n_2 with $N/2 \le \max(|n_1|,|n_2|) \le N$. We choose a weight w such that $w(\mathbf{x}) > 0$ for $|\mathbf{x}| \le C$, with C as in Theorem 1.2, and we take $B = N^{1/2}$. We classify pairs $\underline{n}$ contributing to $\mathcal{E}(N)$ into three cases, which may overlap. Case I will consist of pairs for which $\mathcal{J}_w(B^{-2}\underline{n}) \ge B^{-(k-2)/(16k^2)}$ and $\mathfrak{S}(\underline{n}) \ge B^{-(k-2)/(32k)}$. Case II will be that in which $\mathcal{J}_w(B^{-2}\underline{n}) \le B^{-(k-2)/(16k^2)}$ or $F(n_2,-n_1) = 0$, while Case III will have $\mathfrak{S}(\underline{n}) \le B^{-(k-2)/(32k)}$ and $F(n_2,-n_1) \ne 0$.

The number of pairs $\underline{n}$ for which $F(n_2,-n_1) = 0$ is clearly $O(N)$. For the remaining pairs, if there is no integer solution $\mathbf{x}$ with $\underline{Q}(\mathbf{x}) = \underline{n}$ then $R_B(\underline{n}) = 0$. For pairs $\underline{n}$ in Case I the corresponding summand in (1.6) is then

$$\gg (B^{-(k-2)/(16k^2)}.B^{-(k-2)/(32k)}.B^{k-4})^2.$$

It follows from Theorem 1.1 that there are

$$\ll B^{4-1/(4k^2)} \ll N^{2-1/(2k^2)}$$

pairs (n_1,n_2) for which this first case holds. This is satisfactory for Theorem 1.3.

We have already treated those $\underline{n}$ for which $F(n_2,-n_1) = 0$, so we turn to Case II with the assumption that $\mathcal{J}_w(B^{-2}\underline{n}) \le B^{-(k-2)/(16k^2)}$ but $F(n_2,-n_1) \ne 0$. Since we are assuming that the system of equations $Q_1(\mathbf{x}) = n_1$, $Q_2(\mathbf{x}) = n_2$

has a real solution $\mathbf{x}$, we may deduce from Theorem 1.2 with $\underline{\mu} = B^{-2}\underline{n}$ that $|F(\mu_2, -\mu_1)| \ll B^{-1/(16k^2)}$, whence $|F(n_2, -n_1)| \ll N^k B^{-1/(16k^2)}$. We factor $F(x_1, x_2)$ over $\mathbb{C}$ as in (3.6), and write $\psi = an_2 + bn_1$ for the smallest factor ψ_i of $F(n_2, -n_1)$. Then, as in the proof of (3.8), we see that $|F(n_2, -n_1)| \gg N^{k-1}|\psi|$, since $\max(|n_1|, |n_2|) \geq N/2$. It follows that $|\psi| \ll NB^{-1/(16k^2)}$ for some factor ψ on the right of (3.6). Assuming that the coefficient a, say, is non-zero we deduce that for each n_1 the value for n_2 is restricted to an interval of length $O(NB^{-1/(16k^2)})$. We then deduce that the number of possible pairs $\underline{n}$ in Case II is $O(N^2 B^{-1/(16k^2)})$, which is satisfactory for Theorem 1.3.

We turn finally to Case III. Since we are assuming that the system of equations $Q_1(\mathbf{x}) = n_1$, $Q_2(\mathbf{x}) = n_2$ is solvable in every p-adic ring $\mathbb{Z}_p$, we may deduce from Theorem 1.2 that if (n_1, n_2) belongs to Case III then

$$\prod_{p \leq p_0} |F(n_2, -n_1)|_p \ll_\varepsilon B^{\varepsilon - 1/(32k)}$$

for any fixed $\varepsilon > 0$. Let $P = \prod_{p \leq p_0} p$. We then see that there is a divisor $q \gg_\varepsilon B^{-\varepsilon + 1/(32k)}$ of $F(n_2, -n_1)$ such that $q | P^\infty$. Since $F(n_2, -n_1)$ is non-zero and $\ll B^{2k}$, we conclude that $q \ll B^{2k}$. Thus the exponent to which any given prime divides q will be $O(\log B)$. It follows that $q | P^E$ for some $E \ll \log B$, so that the number of possibilities for q is $O((\log B)^{p_0})$. Since p_0 depends only on Q_1 and Q_2 we deduce that the number of possibilities for q is $O_\varepsilon(B^\varepsilon)$, following our convention that the implied constant may depend also on the forms Q_1 and Q_2. We therefore conclude that the number of pairs $\underline{n}$ in Case III is controlled by up to B^ε factors q of size $q \gg_\varepsilon B^{-\varepsilon + 1/(32k)}$, where for each such q, the corresponding number of $\underline{n}$ belonging to Case III is

$$\ll_\varepsilon \#\{\underline{n} \in \mathbb{Z}^2 : |n_1|, |n_2| \leq N, \, q | F(n_2, -n_1)\}.$$

We shall estimate this for each q very crudely. For any fixed $n_1 \neq 0$ the polynomial $F(x, n_1)$ in x has discriminant $n_1^{k(k-1)} D_F$, where $D_F \neq 0$ is the discriminant of $F(x_1, x_2)$. According to Huxley [9] the congruence $F(X, n_1) \equiv 0 \pmod{q}$ then has at most $k^{\omega(q)} |D_F|^{1/2} a^{k(k-1)/2}$ roots modulo q, where $a = a(n_1, q)$ is the largest factor of n_1 which divides q^∞. If we now fix $A > 0$ we see that $F(X, n_1) \equiv 0 \pmod{q}$ has $O_\varepsilon(B^\varepsilon A^{k(k-1)/2})$ roots when $a \leq A$, so that the range $|X| \leq N$ produces $O_\varepsilon(B^\varepsilon A^{k(k-1)/2}(N/q + 1))$ solutions. The contribution to Case III from the $\ll B^\varepsilon$ appropriate q and non-zero integers n_1 with $|n_1| \leq N$ such that $a(n_1, q) \leq A$ is therefore

$$\ll_\varepsilon B^{2\varepsilon} A^{k(k-1)/2} (N/q + 1) N \ll_\varepsilon B^{3\varepsilon - 1/(32k)} A^{k(k-1)/2} N^2,$$

since $q \gg_\varepsilon B^{-\varepsilon + 1/(32k)}$. In the remaining case either $n_1 = 0$ or $r | n_1$ for some integer $r | q^\infty$ satisfying $A < r \leq N$. The number of possibilities for r is $O_\varepsilon(B^\varepsilon)$, by the same argument that bounded the number of possibilities for q. Thus there are $O_\varepsilon(1 + B^\varepsilon N/A)$ choices for n_1, with a total contribution $O_\varepsilon((1 + B^\varepsilon N/A)N)$ for Case III. We will choose $A = B^\phi$ with $\phi = (16k(2 + k(k-1)))^{-1}$, in which case we may verify that $B^{3\varepsilon-1/(32k)}A^{k(k-1)/2} \ll B^{-1/(16k^3)}$. This shows that Case III makes a satisfactory contribution of $O_\varepsilon(N^2B^{-1/(16k^3)})$ to Theorem 1.3. This completes the proof of the theorem.

We turn now to the proof of Theorem 1.4. By (6.5) and (6.6) we see that there is a constant p_1 depending on Q_1 and Q_2 alone, such that $\sigma_p > 0$ for all good primes $p \geq p_1$. We may of course choose p_1 sufficiently large that we have $p < p_1$ for all bad primes. Whenever $\sigma_p > 0$ we see from (4.23) that $N(\underline{n}; p^e) > 0$ for all large enough e, from which a compactness argument shows that there is at least one solution of $\underline{Q}(\mathbf{x}) = \underline{n}$ with $\mathbf{x} \in \mathbb{Z}_p^k$. Thus this local condition holds for all $\underline{n} \in \mathbb{Z}^2$ as soon as $p \geq p_1$.

For each of the finitely many primes $p < p_1$ we will show that there is an exponent $e = e(p)$ and a congruence class $\underline{n}^{(p)} \pmod{p^e}$ with $p \nmid n_1^{(p)}n_2^{(p)}$, such that $\underline{Q}(\mathbf{x}) = \underline{n}$ has a solution $\mathbf{x} \in \mathbb{Z}_p^k$ whenever $\underline{n} \equiv \underline{n}^{(p)} \pmod{p^e}$. To do this we consider vectors $\mathbf{y}_p$ of the form $\mathbf{x}_p + p\underline{\mathrm{m}}$ where $\mathbf{x}_p$ is as in the statement of Theorem 1.4 and $\underline{\mathrm{m}}$ runs over $\mathbb{Z}^k$. Since the determinants $\Delta_{ij}(\mathbf{x})$ do not all vanish identically we can find an integer vector $\underline{\mathrm{m}}$ for which some $\Delta_{ij}(\mathbf{y}_p)$ is non-zero. We then set $\underline{n}^{(p)} = \underline{Q}(\mathbf{y}_p)$ so that

$$n_i^{(p)} = Q_i(\mathbf{y}_p) \equiv Q_i(\mathbf{x}_p) \not\equiv 0 \pmod{p}$$

for $i = 1, 2$. Suppose now that $e = 2f + 1$ where $p^f || \Delta_{ij}(\mathbf{y}_p)$ and let $\underline{n} \equiv \underline{n}^{(p)} \pmod{p^e}$. Then $\underline{Q}(\mathbf{x}) \equiv \underline{n} \pmod{p^e}$ has a solution $\mathbf{x} = \mathbf{y}_p$ which can be lifted to $\mathbb{Z}_p$ by Hensel's Lemma since $e \geq 2f + 1$. This establishes our claim.

For the real valuation we can produce a completely analogous argument. There is a neighbourhood of $\mathbf{x}_0$ on which the forms $\underline{Q}$ are both positive, and this neighbourhood will include a point $\mathbf{y}_0$ at which some determinant $\Delta_{ij}(\mathbf{y}_0)$ is non-vanishing. There is then a small $\delta > 0$ such that the system $\underline{Q}(\mathbf{x}) = \underline{\mu}$ has a real solution whenever $|\underline{\mu} - \underline{Q}(\mathbf{y}_0)| \leq \delta$.

We can now use the Chinese Remainder Theorem to produce a modulus $M = \prod_{p<p_1} p^{e(p)}$ and a residue class $\underline{n}^{(M)} \pmod{M}$ such that $n_1^{(M)}$ and $n_2^{(M)}$ are both coprime to M, and with the property that if $\underline{n} \equiv \underline{n}^{(M)} \pmod{M}$ then $\underline{Q}(\mathbf{x}) = \underline{n}$ has a solution in every ring $\mathbb{Z}_p$ for $p < p_1$. Of course there is also a solution for $p \geq p_1$, by our choice of p_1. It follows that if r_1 and r_2 are primes such that $r_i \equiv n_i^{(M)} \pmod{M}$ for $i = 1, 2$ and such that

$$|r_i - KQ_i(\mathbf{y}_0)| \leq \delta K/2, \quad (i = 1, 2)$$

for some dilation factor $K > 0$, then the equations $\underline{Q}(\mathbf{x}) = (r_1, r_2)$ have a solution in $\mathbb{R}$ and in every ring $\mathbb{Z}_p$. The number of such pairs of primes is $\gg K^2(\log K)^{-2}$ by the Prime Number Theorem for arithmetic progressions, but, according to Theorem 1.3 at most $O(K^{2-\varpi})$ pairs can fail to have a representation over $\mathbb{Z}$. Hence there is at least one representable pair of primes (r_1, r_2) for each sufficiently large K. This completes the proof of the theorem.

We conclude with an explanation of the conjecture that the result of Theorem 1.4 should continue to hold if the assumption of Condition 1 is replaced by the assumption that neither $Q_1(\mathbf{x})$ nor $Q_2(\mathbf{x})$ factors over $\mathbb{Z}$. By one of the assumptions of Theorem 1.4, there exists $\mathbf{a} \in \mathbb{Z}^k$ such that $Q_1(\mathbf{a})$ and $Q_2(\mathbf{a})$ are both positive. Set $A := Q_1(\mathbf{a})Q_2(\mathbf{a})$ and $M = \prod_{p|A} p$. By a further hypothesis of Theorem 1.4, for each p there exists $\mathbf{x}_p \in \mathbb{Z}^k$ such that $p \nmid Q_1(\mathbf{x}_p)Q_2(\mathbf{x}_p)$. Apply the Chinese Remainder Theorem to construct a residue class $\mathbf{m}^{(M)} \pmod{M}$ such that $\mathbf{m}^{(M)} \equiv \mathbf{x}_p \pmod{p}$ for each $p|A$. Fix any $\mathbf{b} \in \mathbb{Z}^k$ with $\mathbf{b} \equiv \mathbf{m}^{(M)} \pmod{M}$ and $\mathbf{b} \neq \mathbf{a}$ (of which there are infinitely many choices). Define for this choice of $\mathbf{a}, \mathbf{b}$ a pair of quadratic polynomials in a real variable t given by

$$q_i(t) = Q_i(\mathbf{b} + t(\mathbf{a} - \mathbf{b})),$$

for $i = 1, 2$. Then $q_i(t) \to \infty$ as $t \to \infty$. By construction, if $p \nmid A$, then $p \nmid q_i(t)$ when $t = 1$, and if $p|A$ then $p \nmid q_i(t)$ when $t = 0$. Thus the polynomials $q_1(t), q_2(t)$ have no fixed prime divisor. If q_1, q_2 are irreducible over $\mathbb{Z}$ as polynomials in t, then Schinzel's Hypothesis would imply that $q_1(t)$, $q_2(t)$ simultaneously attain infinitely many prime values, and hence so would Q_1, Q_2. Thus the remaining consideration is to show that if Q_1, Q_2 are irreducible over $\mathbb{Q}$, then there is a choice of $\mathbf{b} \equiv \mathbf{m}^{(M)} \pmod{M}$ such that $q_1(t)$ and $q_2(t)$ are both irreducible.

The polynomial $q_i(t)$ is reducible if and only if its discriminant is a square. However the discriminant will be (up to a factor of 4)

$$Q_i(\mathbf{b}, \mathbf{a})^2 - Q_i(\mathbf{b})Q_i(\mathbf{a}), \tag{10.1}$$

where $Q_i(\mathbf{x}, \mathbf{y}) = \mathbf{x}^t Q_i \mathbf{y}$ is the associated bilinear form. As a function of $\mathbf{b}$, (10.1) is a quadratic form, $R_i(\mathbf{b})$, say. Moreover, if R_i were the square $L_i(\mathbf{x})^2$ of a linear form L_i defined over $\mathbb{Q}$, then we would have

$$Q_i(\mathbf{x}) = Q_i(\mathbf{a})^{-1}\{Q_i(\mathbf{x}, \mathbf{a}) + L_i(\mathbf{x})\}\{Q_i(\mathbf{x}, \mathbf{a}) - L_i(\mathbf{x})\},$$

in contradiction to the assumption that $Q_i(\mathbf{x})$ is irreducible over $\mathbb{Q}$. Thus neither $R_1(\mathbf{x})$ nor $R_2(\mathbf{x})$ can be squares.

It follows that each of the quadratic forms

$$S_1(\mathbf{x}, y) = R_1(\mathbf{x}) - y^2 \quad \text{and} \quad S_2(\mathbf{x}, y) = R_2(\mathbf{x}) - y^2$$

is irreducible over $\mathbb{Q}$. For any $\mathbf{b}$ such that $q_1(t)$ is reducible, there will be a corresponding integer y such that $S_1(\mathbf{b}, y) = 0$. Moreover if $|\mathbf{b}| \le B$, say, then $y \ll B$. Since an irreducible quadratic form S in n variables has $O_{S,\varepsilon}(B^{n-2+\varepsilon})$ integral zeros of size $O(B)$ we deduce, on taking $\varepsilon = 1/2$, that there are $O(B^{k-1/2})$ admissible values of $\mathbf{b}$ with $|\mathbf{b}| \le B$, such that $q_1(t)$ is reducible.

There is a similar estimate for $q_2(t)$. However there are $\gg B^k$ vectors $\mathbf{b} \equiv \mathbf{m}^{(M)} \pmod{M}$ such that $|\mathbf{b}| \le B$, whence if B is large enough there must be some such value for which both $q_1(t)$ and $q_2(t)$ are irreducible. This provides the final step in our argument. We conclude with the observation that the above argument is essentially a proof of a case of the Hilbert irreducibility theorem.

Acknowledgements

Pierce was partially supported during this work by a Marie Curie Fellowship funded by the European Commission and NSF DMS-0902658. Gratitude is extended to Damaris Schindler for comments on the manuscript, and to the Max-Planck-Institut für Bioanorganische Chemie, which graciously provided a very pleasant working environment to the second author during the preparation of an early version of this manuscript.

References

[1] B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. Ser. A **265** (1961/62), 245–263.

[2] T. D. Browning and D. R. Heath-Brown, *Counting rational points on hypersurfaces*, J. Reine Angew. Math. **584** (20045), 83–115.

[3] T. D. Browning and R. Munshi, *Rational points on singular intersections of quadrics*, Compositio Math., in press.

[4] J. L. Colliot-Thélène, J. J. Sansuc, and P. Swinnerton-Dyer, *Intersections of two quadrics and chtelet surfaces. i*, J. Reine Angew. Math. **373** (1987), 37–107.

[5] E. Fouvry and H. Iwaniec, *Gaussian primes*, Acta Arith. **79** (1997), 249–287.

[6] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum" VI: Further researches in Waring's problem*, Math. Zeitschrift **23** (1925), no. 1, 1–37.

[7] 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.

[8] C. Hooley, *On Hypothesis K^* in Waring's problem*, Sieve Methods, Exponential Sums, and their Applications in Number Theory, London Math. Soc. Lecture Notes No. 237, Cambridge University Press, 1997, pp. 175–185.

[9] M. N. Huxley, *A note on polynomial congruences*, Recent progress in analytic number theory, Durham, 1979, vol. 1, Academic Press, London–New York, 1981, pp. 193–196.

[10] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. **49** (1926), 407–464.

[11] R. Munshi, *Pairs of quadrics in 11 variables*, arXiv:1305.1461v1 (2013).

[12] M. Reid, *The complete intersection of two or more quadrics*, PhD Thesis, Trinity College, Cambridge 1972.