THREE APPLICATIONS OF THE SIEGEL MASS FORMULA

JEAN BOURGAIN AND CIPRIAN DEMETER

Abstract. We present three applications of the Siegel mass formula, using the explicit upper bounds for densities derived in [2].

1. Background on the Siegel mass formula

Let $m\ge n+1$ and let $\gamma\in M_{m,m}(\mathbb{Z})$ and $\Lambda\in M_{n,n}(\mathbb{Z})$ be two positive definite matrices with integer entries. Denote by $A(\gamma,\Lambda)$ the number of solutions $\mathcal{L}\in M_{m,n}(\mathbb{Z})$ for

$$\mathcal{L}^*\gamma\mathcal{L}=\Lambda. \tag{1}$$

Then Siegel's mass formula [5] asserts that

$$A(\gamma,\Lambda)\lesssim_{n,m,\gamma}(\det(\Lambda))^{\frac{m-n-1}{2}}\prod_{p\text{ prime}}\nu_p(\gamma,\Lambda). \tag{2}$$

In our forthcoming applications $m=n+1$ and γ will always be the identity matrix I_{n+1}. In this case, the factor $(\det(\Lambda))^{\frac{m-n-1}{2}}$ is 1.

In evaluating the densities $\nu_p(I_{n+1},\Lambda)$ we distinguish two separate cases: $p\nmid\det(\Lambda)$ and $p|\det(\Lambda)$. We recall the following estimate (Proposition 5.6.2. (ii) in [6]), see also Proposition 4.2 in [2].

Proposition 1.1. *We have*

$$\prod_{p\nmid\det(\Lambda)}\nu_p(I_{n+1},\Lambda)\lesssim 1, \tag{3}$$

with some universal implicit constant.

Let us next consider the primes p which divide $\det(\Lambda)$. Recall that the number of such primes is

$$O(\frac{\log\det(\Lambda)}{\log\log\det(\Lambda)}). \tag{4}$$

We will denote by $o_p(T)$ the largest α such that $p^\alpha\,|\,T$. We denote by $d(T)$ the number of divisors on T, and by gcd the greatest common divisor. If T has factorization

$$T=\prod p_i^{\alpha_i}$$

then

$$d(T)=\prod(1+\alpha_i).$$

The authors are partially supported by the Collaborative Research NSF grant DMS-1800305.
AMS subject classification: Primary 11L03.

Recall that we have the bound

$$d(T) \lesssim_\epsilon T^\epsilon.$$

For an $n \times n$ matrix Λ and for $A, B \subset \{1, \dots, n\}$ with $|A| = |B|$ we define

$$\mu_{A,B} = \det((\Lambda_{i,j})_{i \in A, j \in B}).$$

We recall the following result from [2].

Proposition 1.2. *Let $\Lambda \in M_{n,n}(\mathbb{Z})$ be a positive definite matrix and let $p|\det(\Lambda)$. Then*

$$\nu_p(I_{n+1}, \Lambda) \lesssim \sum_{\substack{0 \le l_i : 1 \le i \le n \\ l_1 + l_2 + \dots + l_n \le o_p(\det(\Lambda))}} p^{\beta_2(l_1, \dots, l_n) + \dots + \beta_n(l_1, \dots, l_n)},$$

where $\beta_i = \beta_i(l_1, \dots, l_n)$ satisfies

$$\beta_i = \min\{(i-1)l_i, (i-2)l_i + \min_{|A|=1} o_p(\mu_{\{1\},A}) - l_1, (i-3)l_i + \min_{|A|=2} o_p(\mu_{\{1,2\},A}) - l_1 - l_2, \dots,$$

$$\dots, \min_{|A|=i-1} o_p(\mu_{\{1,2,\dots,i-1\},A}) - l_1 - l_2 - \dots - l_{i-1}\}$$

Let us list two consequences that will be used in the next sections.

Corollary 1.3 $(n = 2)$**.** *Let $\Lambda \in M_{2,2}(\mathbb{Z})$ be a positive definite symmetric matrix. Then*

$$A(I_3, \Lambda) \lesssim_\epsilon (\det(\Lambda))^\epsilon \gcd(\Lambda_{1,1}, \Lambda_{1,2}, \Lambda_{2,2}).$$

Proof Let $p \mid \det(\Lambda)$. Proposition 1.2 and its symmetric version implies that

$$\nu_p(I_3, \Lambda) \lesssim [o_p(\det(\Lambda))]^2 p^{\min\{o_p(\Lambda_{1,1}), o_p(\Lambda_{1,2})\}}$$

and

$$\nu_p(I_3, \Lambda) \lesssim [o_p(\det(\Lambda))]^2 p^{\min\{o_p(\Lambda_{2,1}), o_p(\Lambda_{2,2})\}}.$$

Combining them leads to

$$\nu_p(I_3, \Lambda) \le C[o_p(\det(\Lambda))]^2 p^{\min\{o_p(\Lambda_{1,1}), o_p(\Lambda_{1,2}), o_p(\Lambda_{2,2})\}},$$

with C independent of p. Thus

$$\prod_{p|\det(\Lambda)} \nu_p(I_3, \Lambda) \lesssim C^{O(\frac{\log\det(\Lambda)}{\log\log\det(\Lambda)})} d(\det(\Lambda))^2 \gcd(\Lambda_{1,1}, \Lambda_{1,2}, \Lambda_{2,2})$$

$$\lesssim_\epsilon (\det(\Lambda))^\epsilon \gcd(\Lambda_{1,1}, \Lambda_{1,2}, \Lambda_{2,2}).$$

The result now follows by combining this inequality with (2) and (3).

∎

Corollary 1.4 $(n = 3)$**.** *Let $\Lambda \in M_{3,3}(\mathbb{Z})$ be a positive definite matrix. Then*

$$A(I_4, \Lambda) \lesssim_\epsilon (\det(\Lambda))^\epsilon \gcd(\Lambda_{A,B} : \ A, B \subset \{1, 2, 3\}, \ |A| = |B| = 2).$$

Proof Use the bound

$$\beta_2(l_1, l_2, l_3) \le l_2$$

and

$$\beta_3(l_1, l_2, l_3) \le \min_{|A|=2} o_p(\mu_{\{1,2\},A}) - l_1 - l_2$$

(and its symmetric versions). The rest is the same as in Corollary 1.3.

■

In the next sections we present three applications of these corollaries.

2. Uneven Parsell-Vinogradov sums

Our first application concerns a sharp estimate for the quadratic Parsell–Vinogradov sums, in the general case when N and M are unrelated. The special case $N \sim M$ was proved in [3], as a consequence of the $l^8(L^8)$ decoupling for the surface

$$(t, s, ts, t^2, s^2).$$

In the same paper, the point is made that the $l^2(L^8)$ decoupling for this surface is false. As a result, we do not know of any way to recover the following theorem using decoupling technology.

Theorem 2.1. *For each $N, M \ge 1$*

$$\|\sum_{n=1}^{N}\sum_{m=1}^{M} e(nx_1 + mx_2 + nmx_3 + n^2x_4 + m^2x_5)\|_{L^8([0,1]^5)} \lesssim (NM)^{\frac12+\epsilon}$$

Proof We need to show that the number of integral solutions $n_1, \dots, n_8 \in [1, N]$, $m_1, \dots, m_8 \in [1, M]$ of the system

$$\begin{cases} n_1 + \dots + n_4 = n_5 + \dots + n_8 \\ m_1 + \dots + m_4 = m_5 + \dots + m_8 \\ n_1^2 + \dots + n_4^2 = n_5^2 + \dots + n_8^2 \\ m_1^2 + \dots + m_4^2 = m_5^2 + \dots + m_8^2 \\ n_1m_1 + \dots + n_4m_4 = n_5m_5 + \dots + n_8m_8 \end{cases}$$

is $O((NM)^{4+\epsilon})$. For positive integers $A \lesssim N$, $B \lesssim M$, $C \lesssim N^2$, $D \lesssim M^2$, $E \lesssim NM$, we note that the number of integral solutions of the system

$$\begin{cases} n_1 + \dots + n_4 = A \\ m_1 + \dots + m_4 = B \\ n_1^2 + \dots + n_4^2 = C \\ m_1^2 + \dots + m_4^2 = D \\ n_1m_1 + \dots + n_4m_4 = E \end{cases}$$

is smaller than the number $N_{A,B,C,D,E}$ of solutions to the following system

$$\begin{cases} n_1+\ldots+n_4=4A\\ m_1+\ldots+m_4=4B\\ n_1^2+\ldots+n_4^2=16C\\ m_1^2+\ldots+m_4^2=16D\\ n_1m_1+\ldots+n_4m_4=16E\end{cases}.$$

We can rephrase our goal as follows

$$\sum_{A,B,C,D,E} N_{A,B,C,D,E}^2 \lesssim_\epsilon (NM)^{4+\epsilon}. \tag{5}$$

We also note that $N_{A,B,C,D,E}$ is equal to the number N_{C_1,D_1,E_1} of solutions for the system

$$\begin{cases} n_1+\ldots+n_4=0\\ m_1+\ldots+m_4=0\\ n_1^2+\ldots+n_4^2=C_1\\ m_1^2+\ldots+m_4^2=D_1\\ n_1m_1+\ldots+n_4m_4=E_1\end{cases} \tag{6}$$

where

$$\begin{cases} C_1=16C-4A^2\\ D_1=16D-4B^2\\ E_1=16E-4AB\end{cases}.$$

So

$$\sum_{A,B,C,D,E} N_{A,B,C,D,E}^2 \lesssim$$

$$\sum_{C_1,D_1,E_1} N_{C_1,D_1,E_1}^2 |\{(A,B,C,D,E):\ C_1=16C-4A^2,\ D_1=16D-4B^2,\ E_1=16E-4AB\}|.$$

Note that the second summation runs over $C_1\lesssim N^2$, $D_1\lesssim M^2$, $E_1\lesssim NM$ and that

$$|\{(A,B,C,D,E):\ C_1=16C-4A^2,\ D_1=16D-4B^2,\ E_1=16E-4AB\}|\lesssim NM.$$

It follows that

$$\sum_{A,B,C,D,E} N_{A,B,C,D,E}^2 \lesssim NM \sum_{C_1,D_1,E_1} N_{C_1,D_1,E_1}^2.$$

The system (6) can be rewritten as follows

$$\begin{cases} n_1^2+n_2^2+n_3^2+(n_1+n_2+n_3)^2=C_1\\ m_1^2+m_2^2+m_3^2+(m_1+m_2+m_3)^2=D_1\\ n_1m_1+n_2m_2+n_3m_3+(n_1+n_2+n_3)(m_1+m_2+m_3)=E_1\end{cases}.$$

This has at most as many solutions as the system

$$\begin{cases} n_1^2+n_2^2+n_3^2=C_1 \\ m_1^2+m_2^2+m_3^2=D_1 \\ n_1m_1+n_2m_2+n_3m_3=E_1 \end{cases}. \tag{7}$$

This can be seen by changing variables

$$\begin{cases} (n_1+n_2,n_2+n_3,n_3+n_1)\mapsto(n_1,n_2,n_3) \\ (m_1+m_2,m_2+m_3,m_3+m_1)\mapsto(m_1,m_2,m_3) \end{cases}.$$

On the other hand, (7) is equivalent with

$$\begin{bmatrix} n_1 & n_2 & n_3 \\ m_1 & m_2 & m_3 \end{bmatrix} I_3 \begin{bmatrix} n_1 & m_1 \\ n_2 & m_2 \\ n_3 & m_3 \end{bmatrix} = \begin{bmatrix} C_1 & E_1 \\ E_1 & D_1 \end{bmatrix}.$$

Let us analyze the number $\tilde{N}_{C_1,D_1,E_1}$ of solutions of this system. We start with the singular case, when $C_1D_1=E_1^2$. In this case the number can be estimated directly. Using only the first two equations and the bound on the number of lattice points on spheres we find that

$$\tilde{N}_{C_1,D_1,(C_1D_1)^{1/2}} \lesssim_\epsilon (C_1D_1)^{\frac{1}{2}+\epsilon}.$$

This proves that the contribution from the singular case is acceptable

$$NM\sum_{C_1\lesssim N^2}\sum_{D_1\lesssim M^2}\tilde{N}^2_{C_1,D_1,(C_1D_1)^{1/2}} \lesssim_\epsilon (NM)^{4+\epsilon}. \tag{8}$$

Let us next assume that $C_1D_1\neq E_1^2$. Corollary 1.3 shows that

$$\tilde{N}_{C_1,D_1,E_1} \lesssim_\epsilon (NM)^\epsilon \gcd(C_1,D_1,E_1).$$

Fix $\lambda\lesssim N^2$. The number of triples (C_1,D_1,E_1) with $C_1\lesssim N^2$, $D_1\lesssim M^2$, $E_1\lesssim NM$, such that $\lambda=\gcd(C_1,D_1,E_1)$ is trivially dominated by

$$\frac{N^2}{\lambda}\frac{M^2}{\lambda}\frac{NM}{\lambda}=\frac{N^3M^3}{\lambda^3}.$$

Using these, the contribution from the nonsingular case can be dominated by

$$\begin{aligned} NM\sum_{\lambda\lesssim N^2}\sum_{\substack{C_1,D_1,E_1 \\ \gcd(C_1,D_1,E_1)=\lambda}}\tilde{N}^2_{C_1,D_1,E_1} &\lesssim (NM)^{1+\epsilon}\sum_{\lambda\lesssim N^2}\sum_{\substack{C_1,D_1,E_1 \\ \gcd(C_1,D_1,E_1)=\lambda}}\lambda^2 \\ &\lesssim (NM)^{4+\epsilon}\sum_{\lambda\lesssim N^2}\frac{1}{\lambda} \\ &\lesssim_\epsilon (NM)^{4+\epsilon}. \end{aligned}$$

This together with (8) completes the proof of (5).

∎

3. Non-congruent tetrahedra in the truncated lattice $[0,q]^3\cap\mathbb{Z}^3$

Our goal here is to answer the following question asked in [4].

Question 3.1. *Let $T_3([0,q]^3\cap\mathbb{Z}^3)$ denote the collection of all equivalence classes of congruent tetrahedra with vertices in $[0,q]^3\cap\mathbb{Z}^3$. Is there a $\delta>0$ and some $C>0$, both independent of q such that*
$$\#T_3([0,q]^3\cap\mathbb{Z}^3)\le Cq^{9-\delta}$$
for each $q>1$?

A positive answer to this question would have implications on producing lower bounds for the Falconer distance-type problem for tetrahedra. We refer to [4] for details on this interesting problem.

Here we give a negative answer to this question. We hope that our approach to answering this question will inspire further constructions which might eventually improve the lower bound for the Falconer-type problem.

Theorem 3.2. *We have for each $\epsilon>0$ and each $q>1$*
$$\#T_3([0,q]^3\cap\mathbb{Z}^3)\gtrsim_\epsilon q^{9-\epsilon}.$$

Note the following trivial upper bound, which shows the essential tightness of our result
$$\#T_3([0,q]^3\cap\mathbb{Z}^3)\le Cq^9.$$
Indeed, by translation invariance it suffices to fix one vertex at the origin. The upper bound follows since there are $(q+1)^3$ possibilities for each of the remaining three vertices.

Proof [of Theorem 3.2]

As mentioned before, we fix one vertex to be the origin $\mathbf{0}=(0,0,0)$. A class of congruent tetrahedra in $T_3([0,q]^3\cap\mathbb{Z}^3)$ can be identified with a matrix $\Lambda\in M_{3,3}(\mathbb{Z})$. Namely, the congruence class of the tetrahedron with vertices $\mathbf{0},\mathbf{x},\mathbf{y},\mathbf{z}\in[0,q]^3\cap\mathbb{Z}^3$ is represented by the matrix
$$\Lambda=\begin{bmatrix}\langle\mathbf{x},\mathbf{x}\rangle & \langle\mathbf{x},\mathbf{y}\rangle & \langle\mathbf{x},\mathbf{z}\rangle\\ \langle\mathbf{y},\mathbf{x}\rangle & \langle\mathbf{y},\mathbf{y}\rangle & \langle\mathbf{y},\mathbf{z}\rangle\\ \langle\mathbf{z},\mathbf{x}\rangle & \langle\mathbf{z},\mathbf{y}\rangle & \langle\mathbf{z},\mathbf{z}\rangle\end{bmatrix}.$$
A tetrahedron is called non-degenerate if $\mathbf{x},\mathbf{y},\mathbf{z}$ are linearly independent. We will implicitly assume the congruence classes correspond to non-degenerate tetrahedra.

We seek for an upper bound on the number N_Λ of integral solutions $\mathcal{L}=(\mathbf{x},\mathbf{y},\mathbf{z})\in(\mathbb{Z}^3)^3$ to the equation
$$\mathcal{L}^*\mathcal{L}=\Lambda.$$
This will represent the number of congruent tetrahedra with side lengths specified by Λ.

In the numerology from the Section 1, this corresponds to $n=m=3$. To make the theorems in that section applicable we reduce the counting problem to the $m=3,n=2$ case as follows. One can certainly bound N_Λ by $q^\epsilon N_\Lambda'$, where N_Λ' is the number of integral solutions $\mathcal{L}'=(\mathbf{x},\mathbf{y})\in(\mathbb{Z}^3)^2$ satisfying
$$(\mathcal{L}')^*\mathcal{L}'=\Lambda'$$
and Λ' is the 2×2 minor of Λ obtained from the first two rows and columns of Λ. Indeed, if $\mathbf{x},\mathbf{y}$ are fixed, the matrix Λ forces $\mathbf{z}$ to lie on the intersection of the sphere of radius

$\Lambda_{3,3}^{1/2}$ centered at the origin with, say, a sphere centered at $\mathbf{x}$ whose radius is determined only by the entries of Λ. These radii are $O(q)$, so the resulting circle can only have $O(q^\epsilon)$ points.

Note also that we only care about those Λ' for which there exist $\mathbf{x}, \mathbf{y} \in [0,q]^3 \cap \mathbb{Z}^3$ linearly independent, such that

$$\Lambda' = \begin{bmatrix} \langle \mathbf{x}, \mathbf{x}\rangle & \langle \mathbf{x}, \mathbf{y}\rangle \\ \langle \mathbf{y}, \mathbf{x}\rangle & \langle \mathbf{y}, \mathbf{y}\rangle \end{bmatrix}.$$

This in particular forces Λ' to be positive definite.

Apply now Corollary 1.3. This will bound N'_Λ by

$$q^\epsilon \gcd(\Lambda_{i,j} : i,j \neq 3) \leq q^\epsilon \gcd(\Lambda_{1,1}, \Lambda_{2,2}).$$

Thus

$$N_\Lambda \lesssim_\epsilon q^\epsilon \gcd(\Lambda_{1,1}, \Lambda_{2,2}), \tag{9}$$

for each Λ corresponding to a non-degenerate tetrahedron.

Denote by M_r the number of lattice points on the sphere or radius $r^{1/2}$ centered at the origin. In our case $r \leq q^2$ so we know that $M_r \lesssim_\epsilon q^{1+\epsilon}$. We need to work with spheres that contain many points. Let

$$A := \{r \leq q^2 : M_r \geq q/2\}.$$

Since for each $\epsilon > 0$ we have $M_r \leq C_\epsilon q^{1+\epsilon}$, a double counting argument shows that $q^3 \leq C_\epsilon \# A q^{1+\epsilon} + \frac{1}{2}q^2 q$. Thus $\# A \gtrsim_\epsilon q^{2-\epsilon}$.

Note that for each $r_i \in A$ there are $\sim M_{r_1} M_{r_2} M_{r_3}$ non-degenerate tetrahedrons with vertices $\mathbf{x}, \mathbf{y}, \mathbf{z}$ on the spheres centered at the origin and with radii $r_1^{1/2}, r_2^{1/2}, r_3^{1/2}$ respectively. The congruence class of such a tetrahedron contains

$$\lesssim_\epsilon q^\epsilon \gcd(r_1, r_2)$$

elements, according to (9).

We conclude that there are at least

$$\frac{M_{r_1} M_{r_2} M_{r_3}}{q^\epsilon \gcd(r_1, r_2)}$$

congruence classes generated by such non-degenerate tetrahedra. As distinct radii necessarily give rise to distinct congruence classes, we obtain the lower bound

$$\# T_3([0,q]^3 \cap \mathbb{Z}^3) \gtrsim_\epsilon \sum_{r_i \in A} \frac{M_{r_1} M_{r_2} M_{r_3}}{q^\epsilon \gcd(r_1, r_2)} \gtrsim_\epsilon q^{3-\epsilon} \sum_{r_1, r_2, r_3 \in A} \frac{1}{\gcd(r_1, r_2)}.$$

It is immediate that for each integer d there can be at most $\frac{q^6}{d^2}$ tuples $(r_1, r_2, r_3) \in [0, q^2]^3$, hence also in A^3, with $\gcd(r_1, r_2) = d$. Using this observation and the bound $\#(A^3) \geq C_\epsilon q^{6-\epsilon}$, it follows that for each $\epsilon > 0$ at least $\frac{1}{2}\#(A^3)$ among the triples $(r_1, r_2, r_3) \in A^3$ will have $\gcd(r_1, r_2) \leq \frac{10 q^\epsilon}{C_\epsilon}$.

This implies that

$$\sum_{r_1, r_2, r_3 \in A} \frac{1}{\gcd(r_1, r_2)} \gtrsim_\epsilon q^{6-\epsilon},$$

which finishes the proof of the theorem. ∎

4. Distribution of lattice points on caps

Let $n \ge 2$ and $\lambda \ge 1$ be two integers. Define the lattice points of the sphere

$$\mathcal{F}_{n,\lambda} = \{\xi = (\xi_1, \dots, \xi_n) \in \mathbb{Z}^n : |\xi_1|^2 + \dots |\xi_n|^2 = \lambda\}.$$

It was proved in [1] that

$$|\{(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^3 \times \mathbb{Z}^3 : \ |\mathbf{x}|^2 = |\mathbf{y}|^2 = \lambda, \ |\mathbf{x} - \mathbf{y}| < \lambda^{1/4}\}| \lesssim_\epsilon \lambda^{\frac{1}{2}+\epsilon}.$$

This is a statement on the average distribution of the lattice points on $\mathcal{F}_{3,\lambda}$ in caps of size $\lambda^{1/4}$. Roughly speaking it states that most such caps contain at most $O(\lambda^\epsilon)$ lattice points. It seems reasonable to conjecture that for $n \ge 3$

$$|\{(\mathbf{x}^1, \dots, \mathbf{x}^{n-1}) \in (\mathbb{Z}^n)^{n-1} : \ |\mathbf{x}^i|^2 = \lambda, \ |\mathbf{x}^i - \mathbf{x}^j| < \lambda^{\frac{1}{2(n-1)}} \text{ for } i \ne j\}| \lesssim_\epsilon \lambda^{\frac{n-2}{2}+\epsilon}. \tag{10}$$

We next prove this conjecture for $n = 4$.

Note that if $|\mathbf{x}|^2 = |\mathbf{y}|^2 = \lambda$ then $\mathbf{x} \cdot \mathbf{y} = \lambda - \frac{1}{2}|\mathbf{x} - \mathbf{y}|^2$. Denote by X the $(n-1) \times n$ matrix with entries $x_{ij} = x_j^i$, the latter being the j^{th} entry of $\mathbf{x}^i$. We can thus bound the left hand side from (10) by

$$\sum_\Lambda |\{X \in \mathbb{Z}^{(n-1)\times n} : \ XX^T = \Lambda\}|, \tag{11}$$

with the sum extending over all symmetric $(n-1) \times (n-1)$ matrices with integer entries of the form

$$\begin{cases} \Lambda_{i,i} = \lambda \ \text{ for } 1 \le i \le n-1 \\ |\lambda - \Lambda_{i,j}| \le \rho^2 \ \text{ for } 1 \le i \ne j \le n. \end{cases} \tag{12}$$

We use $\rho = \lambda^{\frac{1}{2(n-1)}}$.

Replacing $(\mathbf{x}^1, \dots, \mathbf{x}^{n-1})$ by $(\mathbf{x}^1, \mathbf{y}^2, \dots, \mathbf{y}^{n-1})$ with $\mathbf{y}^i = \mathbf{x}^i - \mathbf{x}^1$ for $2 \le i \le n-1$, an alternative expression for (11) is

$$\sum_{\Lambda'} |\{X' \in \mathbb{Z}^{(n-1)\times n} : \ X'(X')^T = \Lambda'\}|, \tag{13}$$

with the sum over symmetric $(n-1) \times (n-1)$ matrices Λ' with integer entries of the form

$$\begin{cases} \Lambda'_{1,1} = \lambda \\ |\Lambda'_{i,j}| \le \rho^2 \ \text{ for } i, j \ne 1 \\ \Lambda'_{i,1} = \Lambda'_{1,i} = -\frac{1}{2}\Lambda'_{i,i} \ \text{ for } 2 \le i \le n-1. \end{cases} \tag{14}$$

We will now estimate (13) when $n = 4$, using the bounds on local densities from Section 1. We assume $\mathbf{x}^1 \wedge \mathbf{x}^2 \wedge \mathbf{x}^3 \ne 0$ and leave the other more immediate case to the reader. Note that a typical Λ' in our summation has the form

$$\Lambda' = \begin{bmatrix} \lambda & -a & -b \\ -a & 2a & c \\ -b & c & 2b \end{bmatrix},$$

with $\det(\Lambda') \ne 0$.

Using Corollary 1.4 we bound (13) by

$$\lesssim_\epsilon \lambda^\epsilon \sum_{|a|,|b|,|c|\le\rho^2} \gcd(\Lambda'_{A,B}:\ A,B\subset\{1,2,3\},\ |A|=|B|=2)$$

$$\lesssim_\epsilon \lambda^\epsilon \sum_{|a|,|b|,|c|\le\rho^2} \gcd(a(2\lambda-a),b(2\lambda-b),4ab-c^2)$$

$$\lesssim_\epsilon \lambda^\epsilon \sum_{d\in\mathcal{D}} d|\{(a,b,c):\ |a|,|b|,|c|\le\rho^2,\ d|a(2\lambda-a),\ d|b(2\lambda-b),\ d|4ab-c^2\}|,$$

where $|\mathcal{D}|\lesssim_\epsilon \rho^{2+\epsilon}$ and $\mathcal{D}$ has all elements $O(\rho^4)$.

Write $d=d_1d_2$ where $\prod_{p|d_1}p$ divides λ and $(d_2,\lambda)=(d_1,d_2)=1$. Let also d_1^* be the smallest number such that $d_1^*|d_1$ and $d_1|(d_1^*)^2$. The Chinese Remainder Theorem shows that $d|a(2\lambda-a)$ determines a modulo $d_1^*d_2$ within at most 2 values. The same holds for b. Once a,b are fixed, c is similarly determined modulo d^* where d^* is the smallest number such that $d^*|d$ and $d|(d^*)^2$. We can refine the estimate for (13) as

$$\lambda^\epsilon \sum_{d\in\mathcal{D}} d \sum_{\substack{d=d_1d_2\\ \prod_{p|d_1}p|\lambda}} \sum_{\substack{\Delta|d\\ d|\Delta^2}} \sum_{\substack{d_1',d_1''|d_1\\ d_1|(d_1')^2,(d_1'')^2}} (\frac{\rho^2}{d_1'd_2}+1)(\frac{\rho^2}{d_1''d_2}+1)(\frac{\rho^2}{\Delta}+1)$$

$$\lesssim_\epsilon \rho^{2+\epsilon}\sum_{d\in\mathcal{D}} d^{1/2} \sum_{\substack{d=d_1d_2\\ \prod_{p|d_1}p|\lambda}} (\frac{\rho^4}{d_1d_2^2}+\frac{\rho^2}{d_1^{1/2}d_2}+1)$$

$$\lesssim_\epsilon \rho^{6+\epsilon}\lesssim_\epsilon \lambda^{1+\epsilon}.$$

This proves the conjectured bound (10) for $n=4$.

References

[1] Bourgain, J., Rudnick, Z. and Sarnak, P. *Spatial statistics for lattice points on the sphere I: Individual results*, Bull. Iranian Math. Soc. 43 (2017), no. 4, 361-386

[2] Bourgain, J. and Demeter, C. *New bounds for the discrete Fourier restriction to the sphere in 4D and 5D*, Int. Math. Res. Not. IMRN 2015, no. 11, 3150-3184.

[3] Bourgain, J. and Demeter, C. *Mean value estimates for Weyl sums in two dimensions*, J. Lond. Math. Soc. (2) 94 (2016), no. 3, 814-838

[4] A. Greenleaf, A. Iosevich, B. Liu and E. Palsson, *A group-theoretic viewpoint on Erdös-Falconer problems and the Mattila integral*, Rev. Mat. Iberoam. 31 (2015), no. 3, 799-810.

[5] Siegel, L. C. *Lectures on the analytical theory of quadratic forms: second term 1934-35*, The Institute for Advanced Study and Princeton University, revised edition 1949, reprinted January 1955.

[6] Kitaoka, Y. *Arithmetic of quadratic forms. Cambridge Tracts in Mathematics*, 106. Cambridge University Press, Cambridge, 1993

School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540
E-mail address: `bourgain@math.ias.edu`

Department of Mathematics, Indiana University, 831 East 3rd St., Bloomington IN 47405
E-mail address: `demeterc@indiana.edu`