REPRESENTATIONS OF BINARY FORMS BY QUATERNARY QUADRATIC FORMS

WOOYEON KIM, ANDREAS WIESER, PENGYU YANG

Abstract. We prove a local-global principle for representations of binary by quaternary quadratic forms. One of the main ingredients is a recent measure rigidity result of Einsiedler and Lindenstrauss for diagonalizable actions on quotients of products of SL_2's. Based on this, it suffices to show that limits of the uniform measures on the associated rank one adelic toral packets have more entropy than one half of the maximal entropy. The latter is proved using the Siegel mass formula and the determinant method as developed by Bombieri and Pila as well as Heath-Brown.

1. Introduction

Consider two integral quadratic forms $q : \mathbb{Z}^m \to \mathbb{Z}$ and $Q : \mathbb{Z}^n \to \mathbb{Z}$ for $m < n$. We write $\mathrm{disc}(Q)$ for the discriminant of Q i.e. the determinant of any matrix representation of Q; $\mathrm{disc}(q)$ is defined analogously. A *representation* of q by Q is a linear map $\iota : \mathbb{Z}^m \to \mathbb{Z}^n$ with $Q \circ \iota = q$. Furthermore, the representation ι is *primitive* if $\iota(\mathbb{Z}^m) = (\iota(\mathbb{Z}^m) \otimes \mathbb{Q}) \cap \mathbb{Z}^n$. Lastly, we will say that q is (primitively) represented by Q if a (primitive) representation of q by Q exists.

Clearly, a (primitive) representation can only exist if a local (primitive) representation $\iota_p : \mathbb{Z}_p^m \to \mathbb{Z}_p^n$ exists for every prime p. In short, we will say that q is locally (primitively) represented by Q if this local condition holds.

The *local-global principle* asks whether q is (primitively) represented when it is locally (primitively) represented. This is in analogy to the classical Hasse-Minkowksi theorem which asserts that there is an isometry $(\mathbb{Q}^m, q) \to (\mathbb{Q}^n, Q)$ whenever there is an isometry over $\mathbb{Q}_p$ for every prime p and over $\mathbb{R}$. The Hasse-Minkowski theorem implies that q is (primitively) represented by an element of the *genus* of Q if it is locally (primitively) represented by Q. (Here, the genus of Q is the set of integral quadratic forms locally equivalent to Q.) The representation by an element of the genus of Q may be upgraded to an element of the *spin genus* of Q whenever $n - m \geq 3$. For indefinite forms the spin genus is trivial by work of Eichler [8], and hence so is the above local-global principle when $n - m \geq 3$. We will from now on assume that Q is positive definite.

1.1. Representations of integers.

The local-global principle is particularly classical when $m = 1$ in which case we are looking for (primitive) representations of numbers. For $n \geq 4$, Kloosterman [25] and Tartakovskii [39] proved in the 1920's

Date: November 26, 2025.

P.Y. is supported by National Key R&D Program of China 2022YFA1007500. W.K. is supported by Korea Institute for Advanced Study, grant no. HP101301. A.W. acknowledges the support of the Swiss National Science Foundation, grant no. 217944. This material is based upon work supported by a grant from the Institute for Advanced Study School of Mathematics.

using the circle method that any sufficiently large number D is primitively represented by Q if it is locally primitively represented. For $n = 3$ the analogous claim is false, since local representation does not guarantee representation by the spin genus. For instance, one can show elementarily that the quadratic form $x^2+xy+y^2+9z^2$ does not primitively represent any number of the form $4m^2$ where $m > 0$ and $m \equiv 1 \bmod 3$ (but it does so locally) — see [40, p. 115]. It is a general phenomenon that outside of finitely many square classes local representation implies representation by the spin genus.

Based on estimates for Fourier coefficients of half-integral weight forms by Duke [6] and Iwaniec [23], Duke and Schulze-Pillot [7] proved the following local-global principle:

Theorem 1.1 ([7])**.** *Suppose $n = 3$. If $D > 0$ is sufficiently large and primitively represented by the spin genus of Q, then D is primitively represented by Q.*

A similar result has been established by Cogdell, Piatetski-Shapiro, and Sarnak [5] over number fields. We also note that a weaker version of the above theorem can be obtained from the method of Linnik [26] (see also [16, 41]); the ideas in the current article build on this method.

Lastly, we remark that none of the above methods for $n = 3$ provide effective thresholds D_0 so that Theorem 1.1 holds for $D \geq D_0$ (due to potential Landau-Siegel zeroes). This makes Theorem 1.1 difficult to use in explicit instances, see for example [30]. In contrast, effective thresholds do exist when $n \geq 4$, see e.g. [20, 34].

1.2. **Representations of quadratic forms.** Suppose now that $m > 1$ i.e. q has at least two variables. In the 70's, Hsia, Kitaoka, and Kneser [22] proved a local-global principle when $n \geq 2m + 3$ under the additional condition that

$$\min(q) := \min_{x \in \mathbb{Z}^m \setminus \{0\}} q(x)$$

is sufficiently large. In a dramatic breakthrough 30 years later, Ellenberg and Venkatesh [18] improved the codimension assumption to $n - m \geq 5$ and under a splitting condition to $n-m \geq 3$. Their work uses measure classification results from unipotent dynamics in an essential way — specifically a p-adic variant of work of Mozes and Shah [29] based on measure classification results of Ratner [31, 32] and Margulis, Tomanov [27] (see also Gorodnik, Oh [19]). Recent work of Einsiedler, Lindenstrauss, Mohammadi, and the second named author [17] established effective equidistribution rates for semisimple adelic periods. This work yields the following local-global principle when $n - m \geq 3$: when q is locally primitively represented by Q and $\min(q) \geq C \operatorname{disc}(Q)^A$ for effective constants $A, C > 0$ depending only on n, then q is primitively represented by Q.

When $n - m = 2$, the above results from unipotent dynamics become inapplicable. Nevertheless, the following is conjectured, also in analogy to the work of Duke and Schulze-Pillot [7] (Theorem 1.1 above).

Conjecture 1.2. *Suppose $n - m = 2$. If q is primitively represented by the spin genus of Q and $\min(q)$ is large enough (depending on Q), then q is primitively represented by Q.*

The current article makes progress on this conjecture in dimensions $m = 2$ and $n = 4$ i.e. when q is a binary integral quadratic form and Q is a quaternary integral

quadratic form (assumed to be positive-definite, as above). In this case, we establish the following:

Theorem 1.3. *Let p_1, p_2 be two distinct odd primes. Then there exists $C = C(p_1, p_2, Q) > 1$ with the following property.*

Let q be a primitive binary integral quadratic form such that $-\operatorname{disc}(q)\operatorname{disc}(Q)$ is a non-zero square modulo p_1, p_2. If q is primitively represented by the spin genus of Q and $\min(q) \geq C$ then q is primitively represented by Q.

We note that the two auxiliary primes p_1, p_2 are an artifact of our method. Indeed, they make the problem accessible by known classification results for measures invariant and ergodic under higher-rank diagonalizable actions. Specifically, we use recent work of Einsiedler and Lindenstrauss [9] for irreducible quotients of a product of SL_2's. The additional assumption that q be primitive can be weakened and should not be seen as central to our approach.

Our methods also yield lower bounds on the number of primitive representations $r(q, Q)$ of q by Q. Denote by $r(q, \operatorname{spin}(Q))$ the usual weighted average of the primitive representation numbers over the spin genus. We establish the following stronger version of the above theorem:

Theorem 1.4. *There exists $\delta > 0$ with the following property. Let p_1, p_2 be two distinct primes and let q, Q be as in Theorem 1.3. Then*

$$r(q, Q) \geq r(q, \operatorname{spin}(Q))\big(\delta + \varepsilon(q)\big)$$

where $\varepsilon(q)$ is a function depending on Q, p_1, p_2 and on q with $\varepsilon(q) \to 0$ as $\min(q)$ goes to infinity.

As already alluded to, the technology available to attack Conjecture 1.2 is generally much weaker than in the works mentioned earlier for the local-global principle when $n - m \geq 3$. For instance, the effective equidistribution statements proven in [17] allow for a precise asymptotic statement for representation numbers $r(q, Q)$ with an effective estimate on $\varepsilon(q)$ in terms of $\min(q)$. Statements of this kind are very far out of reach in the current setting where we do not establish equidistribution results.

We also remark that the local-global principle (in the form of Conjecture 1.2) for representations of binary by quaternary quadratic forms is very closely related to the mixing conjecture of Michel and Venkatesh [28]. The mixing conjecture has seen striking progress in recent years with works of Khayutin [24], Blomer and Brumley [1], Blomer, Brumley, and Khayutin [2], as well as Blomer, Brumley, Radziwiłł. The differing methods in these works rely on underlying product structure that is unavailable for the problem of the present article. Correspondingly, there are currently no viable analytic approaches to the local-global principle for $m = 2, n = 4$. An interesting result based on analytic methods is due to Schulze-Pillot [35], who shows that a positive proportion of binary quadratic forms of discriminant $\operatorname{disc}(q)$ are represented.

In the remainder of this announcement, we will present ideas of the proof for Theorem 1.3. As mentioned, our approach is influenced by Linnik's method [26] as reinterpreted in [16, 41] and we will point out similarities and differences.

Acknowledgments: The authors are grateful towards Manfred Einsiedler, Elon Lindenstrauss, Peter Sarnak, and Akshay Venkatesh for their interest in this project and for their encouragement. We also thank Menny Aka, Farrell Brumley, Zhizhong

Huang, Ilya Khayutin, Rainer Schulze-Pillot, Per Salberger, Ye Tian, and Katherine Woo for fruitful discussion on various topics. Last but not least, we thank the Forschungsinstitute für Mathematik at ETH Zurich, the Institute for Advanced Study, the Korea Institute for Advanced Study, the Morningside Center of Mathematics at CAS, and the Simons-Laufer Institute for providing an excellent work environment.

2. Ideas of the proof

2.1. **Density of toral periods.** We begin by reinterpreting our goal in terms of certain adelic periods. Denote by $\mathbf{G} = \mathrm{Spin}_Q$ the spin group of the quadratic form Q. By definition, $\mathbf{G}$ is the universal cover of SO_Q and we denote by $\rho : \mathbf{G} \to \mathrm{SO}_Q$ the covering map. Note that $\mathbf{G}$ is a $\mathbb{Q}$-anisotropic $\mathbb{Q}$-form of $\mathrm{SL}_2 \times \mathrm{SL}_2$. One can show that $\mathbf{G}$ is an inner form if and only if the discriminant $\mathrm{disc}(Q)$ is a rational square; this should be seen as the 'atypical' case (also in view of earlier comments on the mixing conjecture). Define the compact space

$$X = \mathrm{SO}_Q(\mathbb{Q})\rho(\mathbf{G}(\mathbb{A})) \subset \mathrm{SO}_Q(\mathbb{Q})\backslash \mathrm{SO}_Q(\mathbb{A}) \tag{2.1}$$

and let μ_X be the unique $\rho(\mathbf{G}(\mathbb{A}))$-invariant probability measure on X.

Suppose now that we are given a sequence of binary quadratic forms q_i with $\min(q_i) \to \infty$ such that $-\mathrm{disc}(q_i)\,\mathrm{disc}(Q)$ is a non-zero square modulo p_1, p_2. We may assume that Q primitively represents each q_i and show instead that, for large enough i, any element of the spin genus of Q also primitively represents q_i.

For each i, let ι_i be a primitive representation of q_i by Q and define the $\mathbb{Q}$-torus

$$\mathbf{T}_i = \{g \in \mathbf{G} : g.\iota_i(x) = \iota_i(x) \text{ for all } x \in \mathbb{Z}^2\}.$$

These are one-dimensional $\mathbb{Q}$-anisotropic tori.

Remark 2.1. If $\mathbf{G}$ is an inner form of $\mathrm{SL}_2 \times \mathrm{SL}_2$, we may write $\mathbf{G} = \mathbf{B}^1 \times \mathbf{B}^1$ where $\mathbf{B}$ is a quaternion algebra over $\mathbb{Q}$ ramified at the infinite place and where $\mathbf{B}^1$ is the group of norm one units. In this case, one may verify that $\mathbf{T}_i$ projects non-trivially to both factors of $\mathbf{G}$.

Define the adelic toral periods

$$Y_i = \mathrm{SO}_Q(\mathbb{Q})\rho(\mathbf{T}_i(\mathbb{A})) \subset X$$

and let ν_i be the $\rho(\mathbf{T}_i(\mathbb{A}))$-invariant probability measure on Y_i.

Theorem 2.2. *There exists $\delta > 0$ absolute with the following property. Let ν be any weak*-limit of the measures ν_i. Then $\nu \geq \delta\mu_X$.*

In particular, this shows that the sequence Y_i is asymptotically dense i.e. given any open set $\mathcal{O} \subset X$ there exists i_0 so that $Y_i \cap \mathcal{O} \neq \emptyset$ for all $i \geq i_0$. The deduction of our main theorems from Theorem 2.2 is fairly standard and appears in a similar form already in [18, 17]. We will therefore focus on outlining the proof of Theorem 2.2 from now on.

When $\min(q_i)$ grows much slower than the discriminants $\mathrm{disc}(q_i)$, one can apply an argument known as 'equidistribution in stages', among other names. In this situation, one obtains equidistribution of the measures ν_i, which implies, for instance, exact asymptotics in Theorem 1.4. To briefly outline the argument for equidistribution, suppose $v_i \in \iota_i(\mathbb{Z}^2)$ is a shortest vector (with Q-value $\min(q_i)$) and let $\mathbf{H}_i = \{g \in \mathbf{G} : g.v_i = v_i\}$. Then the adelic period $Z_i = \mathrm{SO}_Q(\mathbb{Q})\rho(\mathbf{H}_i(\mathbb{A}))$

has volume polynomial in $\min(q_i)$ and one may apply equidistribution of Y_i in Z_i and of Z_i in X. The former is a version of Duke's equidistribution theorem [6] and its variants, see e.g. [15, §4] and the references therein. The latter follows from recent progress on effective equidistribution of semisimple adelic periods; see [10, 17]. (Note that if $\mathbf{G}$ is an inner form of $\mathrm{SL}_2 \times \mathrm{SL}_2$ this is a version of effective equidistribution of Hecke points proven earlier in [4]).

As the above argument is relatively standard, we will assume from now on that

$$\min(q_i) \geq |\operatorname{disc}(q_i)|^{\eta} \tag{2.2}$$

for some $\eta > 0$.

2.2. **Applying measure rigidity results.** Recall our splitting assumptions at the primes p_1, p_2 in Theorem 1.3. These imply that the tori $\mathbf{T}_i$ split over $\mathbb{Q}_{p_1}$ and $\mathbb{Q}_{p_2}$. To unify the invariance at p_1, p_2, we may pick a bounded sequence $k_i \in \mathbf{G}(\mathbb{Q}_{p_1}) \times \mathbf{G}(\mathbb{Q}_{p_2})$ such that $A = k_i^{-1}(\mathbf{T}_i(\mathbb{Q}_{p_1}) \times \mathbf{T}_i(\mathbb{Q}_{p_2}))k_i$ does not depend on i. Set $Y_i' = Y_i k_i$ and let ν_i' be the Haar probability measure on Y_i'. It is sufficient to show that any weak*-limit ν' of the measures ν_i' satisfies the conclusion of Theorem 2.2. Clearly, ν' is A-invariant.

In a series of fundamental works including [12, 11, 13, 14], Einsiedler and Lindenstrauss have successfully classified, in many instances, probability measures on homogeneous spaces invariant and ergodic under higher-rank diagonalizable actions, assuming positive entropy. Most recently, they resolved in [9] a first instance of this broad program when the action is non-maximal, specifically for actions on irreducible quotients of products of SL_2's. Suppose for simplicity that $\mathbf{G}$ is an outer form of $\mathrm{SL}_2 \times \mathrm{SL}_2$ (as always compact over $\mathbb{R}$). By [9], for any ergodic component μ of ν' we have that either

- μ is homogeneous or
- $h_\mu(a) = 0$ for any $a \in A$.

Here, $h_\mu(a)$ denotes the entropy of μ with respect to a. The homogeneous measures are easily analyzed in our setting and one can verify that any homogeneous measure μ with positive entropy satisfies either $h_\mu(a) = \frac{1}{2} h_{\mu_X}(a)$ (in which case μ is the homogeneous measure for an intermediate period) or $\mu = \mu_X$. In summary, the above application of [9] yields the following

Conclusion: It suffices to show that for some $a \in A$ we have

$$h_{\nu'}(a) > \tfrac{1}{2} h_{\mu_X}(a). \tag{2.3}$$

We establish (2.3) by an argument similar to the aforementioned approach of Linnik e.g. equidistribution of integer points on spheres. Fix $a \in A$. Choose an open neighborhood $B \subset \mathbf{G}(\mathbb{A})$ of the identity and define, for any $n \geq 0$, the two-sided Bowen balls

$$\mathrm{Bow}_n = \bigcap_{|k| \leq n} a^k B a^{-k}.$$

If there is $\delta > 0$ and a sequence $n_i \to \infty$ for which the self-correlation estimate

$$\nu_i' \times \nu_i'\big(\{(x,y) \in X^2 : y \in x\rho(\mathrm{Bow}_{n_i})\}\big) \leq \mathrm{e}^{-2n_i(\frac{1}{2}+\delta)h_{\mu_X}(a)} \tag{2.4}$$

holds, then $h_{\nu'}(a) \geq (\frac{1}{2} + \delta) h_{\mu_X}(a)$ and (2.3) follows.

2.3. **A counting problem.** It remains to prove a self-correlation estimate of the shape in (2.4). An estimate of this type typically corresponds to a counting problem. As (2.4) is a statement about an individual period, we write $q = q_i$ for simplicity. Set $p := p_1$. With a suitable choice of $a \in A$, the counting problem in our setting is given as follows.

Write $q(x,y) = Ax^2 + Bxy + Cy^2$ and set $D = \mathrm{disc}(q) = AC - \frac{1}{4}B^2$. For any $n \geq 1$, consider the set $\mathcal{X}(n)$ of pairs (ι_1, ι_2) with the following properties:

- ι_1, ι_2 are primitive representations of q by Q with distinct images.
- There exists an rotation k in the plane $\iota_1(\mathbb{Q}_p^2)$ (that is, $k \in \mathrm{SO}_Q(\mathbb{Z}_p)$ with $k|_{\iota_1(\mathbb{Q}^2)^\perp} = \mathrm{id}$) such that
$$\iota_2(x) \equiv k\iota_1(x) (\bmod p^{2n})$$
for all $x \in \mathbb{Z}^2$.

Then (2.4) amounts to showing for some n with $p^{(2+\delta)n} \leq D^{1/4}$ (and with $n \to \infty$ as $D \to \infty$)

$$\#\mathcal{X}(n) \ll_\varepsilon \frac{D^{1+\varepsilon}}{p^{(4+2\delta)n}}. \tag{2.5}$$

We note that, more precisely, the left-hand side of (2.4) for time n is bounded by $\ll_\varepsilon D^\varepsilon(\frac{1}{\sqrt{D}} + \frac{1}{D}\#\mathcal{X}(n))$ where the first summand is the 'diagonal' contribution. For the above implicit choice of $a \in A$, the Ad-eigenvalues are $p^{\pm 2}$ and, correspondingly, the maximal entropy is $h_{\mu_X}(a) = 4\log(p)$.

Remark 2.3. For Linnik-type problems such as Theorem 1.1 with a splitting condition at a prime p, one counts, given a positive definite ternary integral quadratic form Q and $D > 0$, the number of pairs (v, w) where $v, w \in \mathbb{Z}^3$ are primitive with $Q(v) = Q(w) = D$ and $v \equiv w \bmod p^n$. See for example [16, 41], where good estimates are obtained using the Siegel mass formula.

We now discuss how to obtain an estimate as in (2.5). A crucial application of the Siegel mass formula [36, 37, 38] implies that it suffices to count all possible quadratic forms attainable on the sublattice $\iota_1(\mathbb{Z}^2) + \iota_2(\mathbb{Z}^2)$. For the purposes of this outline, we focus on the 'generic' case where $\iota_1(\mathbb{Z}^2) + \iota_2(\mathbb{Z}^2)$ is a rank 4 lattice. Define the half-integers

$$x_1 = \langle \iota_1(e_1), \iota_2(e_1)\rangle_Q,\ x_2 = \langle \iota_1(e_1), \iota_2(e_2)\rangle_Q,$$
$$x_3 = \langle \iota_1(e_2), \iota_2(e_1)\rangle_Q,\ x_4 = \langle \iota_1(e_2), \iota_2(e_2)\rangle_Q.$$

Thus, the quadratic form on $\iota_1(\mathbb{Z}^2) + \iota_2(\mathbb{Z}^2) = \mathbb{Z}\iota_1(e_1) + \mathbb{Z}\iota_1(e_2) + \mathbb{Z}\iota_2(e_1) + \mathbb{Z}\iota_2(e_2)$ is given by

$$\begin{pmatrix} A & B/2 & x_1 & x_2 \\ B/2 & C & x_3 & x_4 \\ x_1 & x_3 & A & B/2 \\ x_2 & x_4 & B/2 & C \end{pmatrix}.$$

Note that the determinant of the above symmetric matrix is the determinant of Q times the square of the index $x_0 = [\mathbb{Z}^4 : \iota_1(\mathbb{Z}^2) + \iota_2(\mathbb{Z}^2)]$. In other words, the tuple $(x_0, x_1, \ldots, x_4)$ is a point on the variety

$$\begin{aligned} \mathrm{disc}(Q)x_0^2 = {} & (x_1x_4 - x_2x_3 - D)^2 - (Cx_1 - Ax_4)^2 \\ & - (Bx_1 - A(x_2 + x_3))(Bx_4 - C(x_2 + x_3)). \end{aligned} \tag{2.6}$$

The tuple $(x_0, x_1, \dots, x_4)$ satisfies further restrictions and we summarize all the information in the following definition.

Definition 2.4. *For any $n \in \mathbb{N}$ the subset $\mathcal{S}(n) \subset \frac{1}{2}\mathbb{Z}^5$ is the set of tuples $x = (x_0, \dots, x_4)$ satisfying (2.6) as well as the following constraints:*

- $|x_1| \le A$, $|x_2|, |x_3| \le \sqrt{AC}$, *and* $|x_4| \le C$.
- *We have*

$$\begin{aligned} x_1x_4 - x_2x_3 &\equiv D \bmod p^{4n}, \\ Cx_1 - Ax_4 &\equiv 0 \bmod p^{4n}, \\ C(x_2+x_3) - Bx_4 &\equiv 0 \bmod p^{4n}, \\ A(x_2+x_3) - Bx_1 &\equiv 0 \bmod p^{4n}. \end{aligned} \tag{2.7}$$

- *If $x_1 = A$ or $x_4 = C$ then $x_0 = 0$, $x_2 = x_3 = \frac{B}{2}$. If $x_1 = -A$ or $x_4 = -C$ then $x_0 = 0$, $x_2 = x_3 = -\frac{B}{2}$.*

Here, the first and third bullet points are a simple consequence of the Cauchy-Schwarz inequality while (2.7) is a consequence of the congruence condition in the definition of $\mathcal{X}(n)$.

A 'trivial' bound on the size of $\mathcal{S}(n)$ is given by roughly $\frac{D^2}{p^{12n}}$. This amounts to having at least one half of the maximal entropy (i.e. non-strict inequality in (2.3)) and does not invoke (2.6) meaningfully. It remains to improve on this trivial bound. To that end, we use the determinant method developed by Bombieri and Pila [3], Heath-Brown [21], and Salberger [33]. Specifically, we use a variant of the result of Bombieri and Pila [3] counting integral points on a rational planar curve; the variant can be established using Heath-Brown's p-adic approach from [21]. In the following we outline our argument in more detail.

We choose p^n to be close to $D^{\frac{1}{8}}$, though slightly smaller by a gap in the exponent. With this choice, we need to show that

$$\#\mathcal{S}(n) \ll \sqrt{D}.$$

We note that to leverage (2.6) geometric information on the variety $\mathbf{V}$ cut out by (2.6) has to be used. For instance, affine subspaces of low height contained in $\mathbf{V}$ can be potentially problematic, or more generally low degree subvarieties. This is reflected in our application of the determinant method, where the following two examples take a special role.

Example 2.5. $\mathbf{V}$ contains the affine linear subvariety cut out by $x_1 = A$, $x_2 = x_3 = \frac{B}{2}$, and $x_0 = 0$, on which there are $\gg \frac{C}{p^{4n}}$ many points of $\mathcal{S}(n)$. In view of (2.2), this subset of $\mathcal{S}(n)$ is not problematic.

Example 2.6. If $\operatorname{disc}(Q) = d_0^2$ for some d_0, the variety $\mathbf{V}$ contains the subvariety cut out by $Cx_1 = Ax_4$, $Bx_1 = A(x_2+x_3)$, and $d_0x_0 = x_1x_4 - x_2x_3 - D$. Our assumption that q be primitive implies that (x_1, x_2+x_3, x_4) is a multiple of (A, B, C) and, in particular, the subvariety does not contribute meaningfully.

For the opposite extreme, if for instance $q(x, y) = A(x^2 + y^2)$ then $x_1 = x_4$ and $x_2 + x_3 = 0$. There are $\asymp A$ choices for x_1 and, by the quadratic congruence condition in (2.7), around Ap^{-4n} choices for x_2 so that the total number of points of $\mathcal{S}(n)$ on this subvariety is $\asymp A^2p^{-4n} = Dp^{-4n}$. This is strictly larger than our desired bound for $\mathcal{S}(n)$ and illustrates the role of our primitivity assumption on q.

To restrict the following argument to the most interesting case, we assume henceforth that the quadratic form q is 'balanced' i.e. $\min(q) \gg \sqrt{D}$. We also assume that q is reduced so that $A = \min(q)$; this latter assumption does not restrict the generality.

We begin by linearizing the quadratic equation in (2.7). Thus, we fix a solution $w' = (w_1, \dots, w_4)$ of (2.7) modulo p^{2n} (there are $\ll p^{2n}$ many such classes) and wish to count all the points $x \in \mathcal{S}(n)$ for which $x' = (x_1, \dots, x_4)$ reduces to w modulo p^{2n}. The congruence condition (2.7) in the new coordinates $(y_1, \dots, y_4)$ given by $x_i = w_i + p^{2n} y_i$ translate to

$$\begin{aligned} w_4 y_1 + w_1 y_4 - w_2 y_3 - w_3 y_2 &\equiv 0 \bmod p^{2n}, \\ C y_1 - A y_4 &\equiv 0 \bmod p^{2n}, \\ C(y_2 + y_3) - B y_4 &\equiv 0 \bmod p^{2n}, \\ A(y_2 + y_3) - B y_1 &\equiv 0 \bmod p^{2n}. \end{aligned} \tag{2.8}$$

We may assume that w' lifts to (the last four coordinates of) an element of $\mathcal{S}(n)$ as otherwise $\mathcal{S}(n)$ contains no points in the fiber above w'. In particular, we have

$$|y_1|, |y_2|, |y_3|, |y_4| \ll \sqrt{D} p^{-2n}.$$

The congruence equations in (2.8) are the desired linearized congruence equations. They cut out a sublattice Λ_w of $\frac{1}{2}\mathbb{Z}^4$ of index expected to be around p^{6n}. More precisely, the index is at least $p^{6n-\nu}$ if $p^{\nu+1} \nmid (w_2 - w_3)$. The set of w with $p^{\nu+1} \mid (w_2 - w_3)$ is a smaller set and can be removed from consideration. For simplicity, we suppose here $p \nmid (w_2 - w_3)$.

Let $v_1, \dots, v_4$ denote a Minkowski reduced basis of Λ_w with respect to the usual Euclidean norm. In particular, $\|v_1\| \cdots \|v_4\| \asymp p^{6n}$ and $\|v_1\| \le \|v_2\| \le \|v_3\| \le \|v_4\|$. We can write

$$y' = (y_1, \dots, y_4) = z_1 v_1 + z_2 v_2 + z_3 v_3 + z_4 v_4$$

for new variables $z_1, \dots, z_4$ with $|z_i| \le B_i$ where $B_i \asymp \sqrt{D} p^{-2n} \|v_i\|^{-1}$. Observe that $B_i \gg 1$ as $\|v_4\| \le p^{2n}$.

Generically, our argument now proceeds as follows. Insert the above new coordinates $(z_1, \dots, z_4)$ into (2.6) and fix z_2, z_3, z_4. The so-obtained equation ought to be an irreducible planar curve and the number of points on it is bounded by $B_1^{1/2}$ using the aforementioned variant of the result of Bombieri-Pila in [3]. This yields a saving of $B_1^{1/2} \ge D^{\frac{1}{16}}$ which suffices for our purposes. We observe the following problems with this argument:

- The above equation in x_0, z_4 might not be irreducible or, equivalently, the right-hand side of (2.6) might be a square as a function in z_4. One shows that this can only happen for few values of z_2, z_3, z_4.
- If $B_2 \le D^{\delta}$ for some very small $\delta > 0$, then we only consider few values of z_1, z_2, z_3 and the information of the previous bullet point is not useful. In this case where the lattice Λ_w has a very short vector v_1 we invoke (2.8) again to show that w' is significantly restricted, and obtain a gain in the count of these 'bad' w'.

Overall, the above analysis completes our outline showing $\#\mathcal{S}(n) \ll \sqrt{D}$. As explained, this establishes more than one half of maximal entropy and, with it, Theorem 2.2.

References

[1] Valentin Blomer and Farrell Brumley. Simultaneous equidistribution of toric periods and fractional moments of L-functions. *J. Eur. Math. Soc. (JEMS)*, 26(8):2745–2796, 2024.

[2] Valentin Blomer, Farrell Brumley, and Ilya Khayutin. The mixing conjecture under GRH. *arXiv preprint 2212.06280*, 2022.

[3] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.

[4] Laurent Clozel, Hee Oh, and Emmanuel Ullmo. Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2):327–351, 2001.

[5] James W. Cogdell. On sums of three squares. volume 15, pages 33–44. 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[6] W. Duke. Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92(1):73–90, 1988.

[7] William Duke and Rainer Schulze-Pillot. Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids. *Invent. Math.*, 99(1):49–57, 1990.

[8] Martin Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.*, 195:127–151 (1956), 1955.

[9] M. Einsiedler and E. Lindenstrauss. Rigidity of non-maximal torus actions, unipotent quantitative recurrence, and diophantine approximations. *arXiv preprint, arXiv:2307.04163*, 2023.

[10] M. Einsiedler, G. Margulis, A. Mohammadi, and A. Venkatesh. Effective equidistribution and property (τ). *J. Amer. Math. Soc.*, 33(1):223–289, 2020.

[11] Manfred Einsiedler and Elon Lindenstrauss. On measures invariant under diagonalizable actions: the rank-one case and the general low-entropy method. *J. Mod. Dyn.*, 2(1):83–128, 2008.

[12] Manfred Einsiedler and Elon Lindenstrauss. On measures invariant under tori on quotients of semisimple groups. *Ann. of Math. (2)*, 181(3):993–1031, 2015.

[13] Manfred Einsiedler and Elon Lindenstrauss. Symmetry of entropy in higher rank diagonalizable actions and measure classification. *J. Mod. Dyn.*, 13:163–185, 2018.

[14] Manfred Einsiedler and Elon Lindenstrauss. Joinings of higher rank torus actions on homogeneous spaces. *Publ. Math. Inst. Hautes Études Sci.*, 129:83–127, 2019.

[15] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Distribution of periodic torus orbits and Duke's theorem for cubic fields. *Ann. of Math. (2)*, 173(2):815–885, 2011.

[16] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. The distribution of closed geodesics on the modular surface, and Duke's theorem. *Enseign. Math. (2)*, 58(3-4):249–313, 2012.

[17] Manfred Einsiedler, Elon Lindenstrauss, Amir Mohammadi, and Andreas Wieser. Effective equidistribution of semisimple adelic periods and representations of quadratic forms. *arXiv preprint 2503.21068*, 2025.

[18] Jordan S. Ellenberg and Akshay Venkatesh. Local-global principles for representations of quadratic forms. *Invent. Math.*, 171(2):257–279, 2008.

[19] Alex Gorodnik and Hee Oh. Rational points on homogeneous varieties and equidistribution of adelic periods. *Geom. Funct. Anal.*, 21(2):319–392, 2011. With an appendix by Mikhail Borovoi.

[20] Jonathan Hanke. Local densities and explicit bounds for representability by a quadratric form. *Duke Math. J.*, 124(2):351–388, 2004.

[21] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. of Math. (2)*, 155(2):553–595, 2002.

[22] John S. Hsia, Yoshiyuki Kitaoka, and Martin Kneser. Representations of positive definite quadratic forms. *J. Reine Angew. Math.*, 301:132–141, 1978.

[23] Henryk Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Invent. Math.*, 87(2):385–401, 1987.

[24] Ilya Khayutin. Joint equidistribution of CM points. *Ann. of Math. (2)*, 189(1):145–276, 2019.

[25] H. D. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.

[26] Yu. V. Linnik. *Ergodic properties of algebraic fields*, volume 45 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, New York, 1968. Translated from the Russian by M.S. Keane.
[27] G. A. Margulis and G. M. Tomanov. Invariant measures for actions of unipotent groups over local fields on homogeneous spaces. *Invent. Math.*, 116(1-3):347–392, 1994.
[28] Ph. Michel and A. Venkatesh. The subconvexity problem for GL_2. *Publ. Math. Inst. Hautes Études Sci.*, (111):171–271, 2010.
[29] Shahar Mozes and Nimish Shah. On the space of ergodic invariant measures of unipotent flows. *Ergodic Theory Dynam. Systems*, 15(1):149–159, 1995.
[30] Ken Ono and K. Soundararajan. Ramanujan's ternary quadratic form. *Invent. Math.*, 130(3):415–454, 1997.
[31] Marina Ratner. On Raghunathan's measure conjecture. *Ann. of Math. (2)*, 134(3):545–607, 1991.
[32] Marina Ratner. Raghunathan's conjectures for Cartesian products of real and p-adic Lie groups. *Duke Math. J.*, 77(2):275–382, 1995.
[33] Per Salberger. Counting rational points on projective varieties. *Proc. Lond. Math. Soc. (3)*, 126(4):1092–1133, 2023.
[34] Rainer Schulze-Pillot. On explicit versions of Tartakovski's theorem. *Arch. Math. (Basel)*, 77(2):129–137, 2001.
[35] Rainer Schulze-Pillot. Averages of Fourier coefficients of Siegel modular forms and representation of binary quadratic forms by quadratic forms in four variables. *Math. Ann.*, 368(3-4):923–943, 2017.
[36] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen. *Ann. of Math. (2)*, 36(3):527–606, 1935.
[37] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen. II. *Ann. of Math. (2)*, 37(1):230–263, 1936.
[38] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen. III. *Ann. of Math. (2)*, 38(1):212–291, 1937.
[39] W. Tartakowskii. Die Gesamtheit der Zahlen, die durch eine positive quadratische Form $F(x_1, x_2, \ldots, x_s)$ (s≥4) darstellbar sind. I & II. *Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya*, 7(2):111–122, 165–196, 1929.
[40] G. L. Watson. *Integral quadratic forms*, volume No. 51 of *Cambridge Tracts in Mathematics and Mathematical Physics*. Cambridge University Press, New York, 1960.
[41] Andreas Wieser. Linnik's problems and maximal entropy methods. *Monatsh. Math.*, 190(1):153–208, 2019.