What is the probability that a random integral quadratic form in \( n \) variables is isotropic?

Manjul Bhargava, John Cremona, and Tom Fisher

November 22, 2013

Abstract

We show that the density of quadratic forms in \( n \) variables over \( \mathbb{Z}_p \) that are isotropic is a rational function in \( p \), where the rational function is independent of \( p \), and we determine this rational function explicitly. As a consequence, for each \( n \), we determine the probability that a random integral quadratic form in \( n \) variables is isotropic. In particular, we show that the probability that a random integral quaternary quadratic form is isotropic is \( \approx 97.0\% \), in the case where the coefficients of the quadratic form are independently and uniformly distributed in the range \([-X, X]\) with \( X \to \infty \). When random integral quaternary quadratic forms are chosen with respect to the Gaussian Orthogonal Ensemble (GOE), the probability of isotropy increases to \( \approx 98.3\% \).

1 Introduction

An integral quadratic form \( Q \) in \( n \) variables takes the form

\[
Q(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j, \tag{1}
\]

where all coefficients \( a_{ij} \) lie in \( \mathbb{Z} \). The quadratic form \( Q \) is said to be isotropic if it represents 0, i.e., if there exists a nonzero \( n \)-tuple \((k_1, \ldots, k_n) \in \mathbb{Z}^n\) such that \( Q(k_1, \ldots, k_n) = 0 \). In this paper, we wish to determine the answer to the question: what is the probability that a random integral quadratic form in \( n \) variables is isotropic?

More precisely, let us define the height \( h(Q) \) of the quadratic form \( Q \) in (1) by \( h(Q) = \max\{|a_{ij}|\} \). Then we may define the probability that a random integral quadratic form \( Q \) in \( n \) variables has a given property \( P \) by

\[
\lim_{X \to \infty} \frac{\#\{Q(x_1, \ldots, x_n) : Q \text{ has property } P \text{ and } h(Q) < X\}}{\#\{Q(x_1, \ldots, x_n) : h(Q) < X\}}, \tag{2}
\]

if this limit exists. In particular, the probability \( \rho_n \) that a random quadratic form in \( n \) variables is isotropic is defined by

\[
\rho_n = \lim_{X \to \infty} \frac{\#\{Q(x_1, \ldots, x_n) : Q \text{ is isotropic and } h(Q) < X\}}{\#\{Q(x_1, \ldots, x_n) : h(Q) < X\}}. \tag{3}
\]
As we will see, this limit always exists. We will evaluate it explicitly in terms of $\rho_n(\infty)$, the probability that a (real or integral) quadratic form in $n$ variables is indefinite (this probability being defined again as in (2)).

It is quite easy to handle the problem for most values of $n$. Indeed, if $n \geq 5$, then it is well-known that a rational quadratic form in $n$ variables is always isotropic over $\mathbb{Q}_p$ for all primes $p$, and hence by the Hasse–Minkowski Theorem it is isotropic if and only if it is indefinite. Therefore $\rho_n = \rho_n(\infty)$ if $n \geq 5$.

Small values of $n$ can also be handled relatively easily. If $n = 1$, then $Q$ is certainly anisotropic unless $a_{11} = 0$; thus $\rho_1 = 0$. If $n = 2$, then we simply note that $Q$ is isotropic implies that $Q$ is isotropic modulo $p$. But a binary quadratic form is isotropic modulo $p$ if and only if it is zero or reducible modulo $p$. The number of such binary forms over $\mathbb{F}_p$ is $p^3 - (p - 1)(p^2 - p)/2 = (p^3 + 2p^2 - p)/2$. Therefore, by the Chinese Remainder Theorem, the probability that a random integral binary quadratic form is isotropic is at most

$$\prod_{p < Y} \frac{p^3 + 2p^2 - p}{2p^3},$$

for any $Y > 0$. Letting $Y$ tend to infinity shows that $\rho_2 = 0$.

The case $n = 3$ may also be handled similarly. Again, if an integral ternary quadratic form $Q$ is isotropic, then it is also isotropic modulo $p$. If the determinant of $Q$ is prime to $p$, then it is isotropic over $\mathbb{F}_p$ (and indeed over $\mathbb{Q}_p$). The number of ternary quadratic forms $Q$ over $\mathbb{F}_p$, with vanishing determinant is $O(p^5)$. Such a form is generically of rank 2, i.e., a binary quadratic form, which is anisotropic $1/2 + O(1/p)$ of the time by the $n = 2$ case. We conclude, by the Chinese Remainder Theorem, that the probability that a random integral ternary quadratic form is isotropic is at most

$$\prod_{p < Y} \frac{p^6 - \frac{1}{2}p^5 + O(p^4)}{p^6},$$

for any $Y > 0$. Letting $Y$ tend to infinity shows also that $\rho_3 = 0$.

The only (more nontrivial) case that remains is $n = 4$, i.e. the case of quaternary quadratic forms. In this case, it has been shown by Poonen and Voloch [5, Thm. 3.6], using the sieve of Ekedahl [4], that $\rho_4$ exists, and that

$$\rho_4 = \rho_4(\infty) \prod_p \rho_4(p),$$

where the product is over all primes $p$, and $\rho_4(p)$ corresponds to the probability (with respect to the standard additive $\mathbb{Z}_p$-measure) that a quaternary quadratic form over $\mathbb{Z}_p$ is isotropic. Thus, to compute $\rho_4$ (in terms of $\rho_4(\infty)$), it suffices to compute $\rho_4(p)$ for all primes $p$.

In this paper we show that, for each $n$, the quantity $\rho_n(p)$ is a rational function in $p$ that is independent of $p$ (this even includes the case $p = 2$), and we determine these rational functions explicitly. Specifically, we prove the following theorem.

**Theorem 1** Let $\rho_n(p)$ denote the probability that a quadratic form $Q$ in $n$ variables over $\mathbb{Z}_p$ is isotropic. Then

$$\rho_1(p) = 0, \quad \rho_2(p) = \frac{1}{2}, \quad \rho_3(p) = 1 - \frac{p}{2(p + 1)^2}, \quad \rho_4(p) = 1 - \frac{p^3}{4(p + 1)^2(p^4 + p^3 + p^2 + p + 1)}.$$
and $\rho_n(p) = 1$ for all $n \geq 5$.

As a consequence, we obtain the following theorem giving the probability $\rho_n$ that a random integral quadratic form in $n$ variables is isotropic.

**Theorem 2** The probability $\rho_n$ that a random integral quadratic form in $n$ variables is isotropic is

$$
\begin{aligned}
\rho_n = \begin{cases}
0 & \text{if } n \leq 3 \\
\frac{p^3}{4(p+1)^2(p^4+p^3+p^2+p+1)} & \text{if } n = 4 \\
\rho_n(\infty) & \text{if } n \geq 5.
\end{cases}
\end{aligned}
$$

Note that, for all $n$, we may write more simply

$$
\rho_n = \rho_n(\infty) \prod_p \rho_n(p)
$$

where the values of $\rho_n(p)$ are provided in Theorem 1.

The quantities $\rho_n(\infty)$ can easily be expressed as explicit definite integrals; however, it seems unlikely that these integrals can be evaluated in compact and closed form for general $n$. Using the numerical integration function NIntegrate (or via a Monte Carlo integration with $10^{10}$ trials) in Mathematica, we easily compute $\rho_n(\infty) \approx 0.627, 0.901, 0.982, 0.998,$ and $> 0.999$ for $n = 1, 2, 3, 4, 5,$ and $6$, respectively. It is known (see, e.g., [1, Thm. 2.3.5]) that $1 - \rho_n(\infty)$ decays faster than $e^{-cn}$ for some constant $c > 0$; the actual rate of decay is likely even faster than that.

In particular, we have

$$
\prod_p \rho_4(p) = \prod_p \left(1 - \frac{p^3}{4(p+1)^2(p^4+p^3+p^2+p+1)}\right) \approx 98.74\%.
$$

Since numerically $\rho_4(\infty) \approx 0.9823$, we obtain $\rho_4 \approx 0.9823 \times 0.9874 \approx 97.0\%$.

We remark that, more generally, rather than taking the distribution on the space of real quadratic forms where the coefficients are independently distributed in the interval $(-X, X)$, we may use instead other nice distributions $D$, such as the Gaussian Orthogonal Ensemble (GOE), whose definition we recall below. Let $D$ be a piecewise smooth rapidly decaying function $D$ on the vector space $\mathbb{R}^{n(n+1)/2}$ of real quadratic forms in $n$ variables satisfying $\int_Q D(Q) dQ = 1$. Then we may define the probability, with respect to the distribution $D$, that a random integral quadratic form $Q$ in $n$ variables has a property $P$ by

$$
\lim_{X \to \infty} \frac{\sum_{Q} Q(x_1, \ldots, x_n) \text{ integral with property } p D(Q/X)}{\sum_{Q} Q(x_1, \ldots, x_n) \text{ integral } D(Q/X)}.
$$

Let $\rho_n^D$ (resp. $\rho_n^D(\infty)$) denote the probability with respect to the distribution $D$ that a random integral quadratic form in $n$ variables is isotropic (resp. indefinite). For example, if $D$ is the distribution on real quadratic forms where each coefficient is independently distributed uniformly in the interval $[-1/2, 1/2]$, then $\rho_n^D = \rho_n$ and $\rho_n^D(\infty) = \rho_n(\infty)$. If $D = \text{GOE}$ is the distribution on symmetric
matrices \( AA^t \) where each entry of \( A \) is an identical and independently distributed Gaussian, i.e., the Gaussian Orthogonal Ensemble, then we use \( \rho_{n}^{\text{GOE}} \) (resp. \( \rho_{n}^{\text{GOE}}(\infty) \)) to denote the probability, with respect to the GOE distribution, that a random \( n \)-ary quadratic form is isotropic (resp. indefinite). Then, by the same arguments as in [5], we conclude that Theorem 2 holds also with each occurrence of \( \rho \) replaced more generally by \( \rho^D \).

It has been shown in [3, (7)] that

\[
\rho_1^{\text{GOE}}(\infty) = 0, \quad \rho_2^{\text{GOE}}(\infty) = \frac{\sqrt{2}}{2}, \quad \rho_3^{\text{GOE}}(\infty) = \frac{\pi + 2\sqrt{2}}{2\pi},
\]

and in [2] it is shown that \( 1 - \rho_n^{\text{GOE}}(\infty) \) decays like \( 2e^{-n^2(\log 3)/4} \). It is natural to expect similar behavior for \( \rho_n(\infty) \), although this seems to be an open question. Numerically, we have \( \rho_n^{\text{GOE}}(\infty) = 0, .707, .950, .995, \) and > .999 for \( n = 1, 2, 3, 4, \) and 5, respectively.

We summarize the values of \( \rho_n^D \), and list numerical values in the cases of the uniform and GOE distributions, in Table 1.

Our method to prove Theorem 1 is as follows. We note that a quadratic form in \( n \) variables defined over \( \mathbb{Z}_p \) can be anisotropic only if its reduction modulo \( p \) has either two conjugate linear factors over \( \mathbb{F}_{p^2} \) or a repeated linear factor over \( \mathbb{F}_p \). We first compute the probability of each of these cases occurring, which is elementary. We then determine the probabilities of isotropy in each of these two cases by developing recursive formulae for these probabilities, in terms of other suitable quantities, which consequently allow us to solve and obtain exact algebraic expressions for these probabilities for each value of \( n \). We note that our general argument shows in particular that quadratic forms in \( n \geq 5 \) variables over \( \mathbb{Q}_p \) of nonzero discriminant are always isotropic, thus giving a new recursive proof of this well-known fact.

We note that Theorems 1 and 2 also hold over a general local or global field, respectively (where we define general densities of quadrics as in [5, §4]). Indeed, the analogue of Theorem 1 holds over any finite extension of \( \mathbb{Q}_p \) (with the same proof), provided that when making substitutions in the proofs we replace \( p \) by a uniformiser, and when computing probabilities we replace \( p \) by the order of the residue field.

| \( n \) | \( \rho_n^D \) | \( \rho_n \) | \( \rho_n^{\text{GOE}} \) |
|---|---|---|---|
| 1 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 |
| 4 | \( \rho_4^{\text{GOE}}(\infty) \prod_p \left( 1 - \frac{p^3}{4(p+1)^2(p^4+p^3+p^2+p+1)} \right) \approx 97.0\% \approx 98.3\% \) |
| 5 | \( \rho_5^{\text{GOE}}(\infty) \approx 99.8\% > 99.9\% \) |
| \( \geq 6 \) | \( \rho_n^{\text{GOE}}(\infty) \) | > 99.9\% | > 99.9\% |

Table 1: Probability that a random integral quadratic form in \( n \) variables is isotropic, for a general distribution \( D \), for the uniform distribution, and for the GOE distribution.
2 Preliminaries

Fix a prime $p$. For any free $\mathbb{Z}_p$-module $V$ of finite rank, there is a unique additive $p$-adic Haar measure $\mu_V$ on $V$ which we always normalize so that $\mu_V(V) = 1$. All densities/probabilities are computed with respect to this measure. In this section, we take $V = V_n$ to be the $n(n+1)/2$-dimensional $\mathbb{Z}_p$-module of $n$-ary quadratic forms over $\mathbb{Z}_p$. We then work out the density $\rho_n(p)$ (i.e. measure with respect to $\mu_V$) of the set of $n$-ary quadratic forms over $\mathbb{Z}_p$ that are isotropic.

We start by observing that a primitive $n$-ary quadratic form over $\mathbb{Z}_p$ can be anisotropic only if, either: (I) the reduction mod $p$ factors into two conjugate linear factors defined over a quadratic extension of $\mathbb{F}_p$, or (II) the reduction mod $p$ is a constant times the square of a linear form over $\mathbb{F}_p$. Let $\xi_1^{(n)}$ and $\xi_2^{(n)}$ be the probabilities of Cases I and II, i.e. the densities of these two types of quadratic forms in $V_n$. Then

$$\xi_0^{(n)} = 1 - \xi_1^{(n)} - \xi_2^{(n)} - \frac{1}{p^{n(n+1)/2}}$$

is the probability that a form is primitive, but not in Cases I or II. Let $\alpha_1^{(n)}$ (resp. $\alpha_2^{(n)}$) be the probability of isotropy for quadratic forms in Case I (resp. Case II). Then

$$\rho_n(p) = \xi_0^{(n)} + \xi_1^{(n)} \alpha_1^{(n)} + \xi_2^{(n)} \alpha_2^{(n)} + \frac{1}{p^{n(n+1)/2}} \rho_n(p),$$

implying

$$\rho_n(p) = \frac{p^{n(n+1)/2}}{p^{n(n+1)/2} - 1} \left( \xi_0^{(n)} + \xi_1^{(n)} \alpha_1^{(n)} + \xi_2^{(n)} \alpha_2^{(n)} \right). \quad (5)$$

3 Some counting over finite fields

Let $\eta_1^{(n)}$ (resp. $\eta_2^{(n)}$) be the probability that a quadratic form is in Case I (resp. Case II) given the “point condition” that the coefficient of $x_1^2$ is a unit. Similarly, let $\nu_1^{(n)}$ be the probability that a quadratic form is in Case I given the “line condition” that the binary quadratic form $Q(x_1, x_2, 0, \ldots, 0)$ is irreducible modulo $p$. Note that it is impossible to be in Case II given the line condition, but we may also define $\nu_2^{(n)} = 0$. Set $\eta_0^{(n)} = 1 - \eta_1^{(n)} - \eta_2^{(n)}$ and $\nu_0^{(n)} = 1 - \nu_1^{(n)} - \nu_2^{(n)} = 1 - \nu_1^{(n)}$. The values of $\xi_j^{(n)}$, $\eta_j^{(n)}$, $\nu_j^{(n)}$, are given by the following easy lemma.

**Lemma 3** The probability that a random quadratic form over $\mathbb{Z}_p$ is in Cases I or II is as follows.

- **Case I (all; relative to point condition; relative to line condition)**

  $$\xi_1^{(n)} = \frac{(p^n - 1)(p^n - p)}{2(p + 1)p^{n(n+1)/2}}, \quad \eta_1^{(n)} = \frac{p^{n-1} - 1}{2p^{n(n-1)/2}}, \quad \nu_1^{(n)} = \frac{1}{p^{(n-1)(n-2)/2}}.$$

- **Case II (all; relative to point condition; relative to line condition)**

  $$\xi_2^{(n)} = \frac{p^n - 1}{p^{n(n+1)/2}}, \quad \eta_2^{(n)} = \frac{1}{p^{n(n-1)/2}}, \quad \nu_2^{(n)} = 0.$$
**Proof:** Case I: There are \((p^{2n} - 1)/(p^2 - 1)\) linear forms over \(\mathbb{F}_p^2\) up to scaling; subtracting the \((p^n - 1)/(p - 1)\) which are defined over \(\mathbb{F}_p\), dividing by 2 to count conjugate pairs and then multiplying by \(p - 1\) for scaling gives \(\frac{(p^n - 1)(p^{n-1} - 1)}{2(p+1)}\) Case I forms, and hence the value of \(\xi_1^{(n)}\).

Similarly, the number of Case I quadratic forms satisfying the point condition is \((p^{2(n-1)} - p^{n-1})(p-1)/2\). Dividing by the probability \(1 - 1/p\) of the point condition holding gives \(p^n(p^{n-1} - 1)/2\) and hence the value of \(\eta_1^{(n)}\).

Lastly, the number of Case I quadratic forms satisfying the line condition is \(p^{2n-3}(p - 1)^2/2\); dividing by the probability \(\xi_1^{(2)}\) of the line condition holding gives \(p^{2n-1}\) and hence the value of \(\nu_1^{(n)}\).

Case II is similar and easier: the number of Case II quadratic forms is \(p^n - 1\), of which \(p^n - p^{n-1}\) satisfy the point condition and none satisfy the line condition, from which the formulae given follow easily. \(\square\)

### 4 Recursive formulae

We now outline our strategy for computing the densities \(\rho_n(p)\) using (5), by evaluating \(\alpha_j^{(n)}\) for \(j = 1, 2\). If a quadratic form is in Case I, then we may make a (density-preserving) change of variables, transforming it so that its reduction is an irreducible binary form in only two variables. Now isotropy forces the values of those variables, in any primitive vector giving a zero, to be multiples of \(p\). Now isotropy makes those variables multiples of \(p\), and we may scale those variables by \(p\) and divide the form by \(p\). Similarly, if a form is in Case II, then we transform it so that its reduction is the square of a single variable, scale that variable and divide out. After carrying out this process once, we again divide into cases and repeat the procedure, which leads us back to an earlier situation with either the line or point conditions, which we need to allow for.

To make this precise, we introduce some extra notation for the probability of isotropy for quadratic forms which are in Case I or Case II after the initial transformation: let \(\beta_1^{(n)}\) (resp. \(\beta_2^{(n)}\)) be the probability of being in Case I (resp. Case II) after one step when the original quadratic form was in Case I, and similarly \(\gamma_1^{(n)}\) (resp. \(\gamma_2^{(n)}\)) the probability of being in Case I (resp. Case II) after one step when the original quadratic form was in Case II.

**Lemma 4**

1. \(\alpha_1^{(2)} = 0, \text{ and for } n \geq 3,\)

\[
\alpha_1^{(n)} = \xi_0^{(n-2)} + \xi_1^{(n-2)}\beta_1^{(n)} + \xi_2^{(n-2)}\beta_2^{(n)} + \frac{1}{p^{(n-1)(n-2)/2}}(\nu_0^{(n)} + \nu_1^{(n)}\alpha_1^{(n)} + \nu_2^{(n)}\alpha_2^{(n)}).
\]

2. \(\alpha_2^{(1)} = 0, \text{ and for } n \geq 2,\)

\[
\alpha_2^{(n)} = \xi_0^{(n-1)} + \xi_1^{(n-1)}\gamma_1^{(n)} + \xi_2^{(n-1)}\gamma_2^{(n)} + \frac{1}{p^{n(n-1)/2}}(\eta_0^{(n)} + \eta_1^{(n)}\alpha_1^{(n)} + \eta_2^{(n)}\alpha_2^{(n)}).
\]
Lemma 5. Since into cases as before, with the probabilities of being in each case given by $\beta_1, \beta_2$.

Proof: We have $\alpha_1^{(2)} = 0$ since a binary quadratic form that is irreducible over $\mathbb{F}_p$ is anisotropic. Now assume that $n \geq 3$, and (for Case I) $Q(x_1, \ldots, x_n) \mod p$ has two conjugate linear factors. Without loss of generality, the reduction mod $p$ is a binary quadratic form in $x_1$ and $x_2$. Now any primitive vector giving a zero of $Q$ must have its first two coordinates divisible by $p$, so replace $Q(x_1, \ldots, x_n)$ by $\frac{1}{p} Q(px_1, px_2, x_3, \ldots, x_n)$. The reduction mod $p$ is now a quadratic form in $x_3, \ldots, x_n$. If the new $Q$ is identically zero then, after dividing it by $p$, we obtain a new integral form that lands in Cases I and II with probabilities $\nu_1^{(n)}$ and $\nu_2^{(n)}$, respectively, since it satisfies the line condition; otherwise, we divide into cases as before, with the probabilities of being in each case given by $\xi_j^{(n-1)}$.

The result for $\alpha_2^{(n)}$ is proved similarly: without loss of generality the reduction mod $p$ is a quadratic form in $x_1$ only, we replace $Q(x_1, \ldots, x_n)$ by $\frac{1}{p} Q(px_1, x_2, \ldots, x_n)$, whose reduction mod $p$ is a quadratic form in $x_2, \ldots, x_n$. If the new $Q$ is identically zero then, after dividing it by $p$, we have a new integral form that lands in Cases I and II with probabilities $\eta_1^{(n)}$ and $\eta_2^{(n)}$, respectively, since it satisfies the point condition; otherwise, we divide into cases as before, with probabilities $\xi_j^{(n-1)}$. □

It remains to compute $\beta_1^{(n)}$ (for $n \geq 4$), $\beta_2^{(n)}$ (for $n \geq 3$), $\gamma_1^{(n)}$ (for $n \geq 3$) and $\gamma_2^{(n)}$ (for $n \geq 2$). Since $\xi_1^{(1)} = 0$, we do not need to compute $\beta_1^{(3)}$ or $\gamma_1^{(2)}$, which are in any case undefined.

Lemma 5.

(i) If $n \geq 4$ then $\beta_1^{(n)} = \nu_0^{(n-2)} + \nu_1^{(n-2)} \beta_1^{(n)}$; also, $\beta_1^{(4)} = 0$.

(ii) If $n \geq 3$ then $\beta_2^{(n)} = \nu_0^{(n-1)} + \nu_1^{(n-1)} \gamma_1^{(n)}$; also, $\beta_2^{(3)} = 0$.

(iii) If $n \geq 3$ then $\gamma_1^{(n)} = \eta_0^{(n-2)} + \eta_1^{(n-2)} \beta_1^{(n)} + \eta_2^{(n-2)} \beta_2^{(n)}$; also, $\gamma_1^{(3)} = 0$.

(iv) If $n \geq 2$ then $\gamma_2^{(n)} = \eta_0^{(n-1)} + \eta_1^{(n-1)} \gamma_1^{(n)} + \eta_2^{(n-1)} \gamma_2^{(n)}$; also, $\gamma_2^{(2)} = 0$.

Proof: In Case I, the initial transformation leads to a quadratic form for which the valuations of the coefficients satisfy

\begin{align*}
\geq 1 & \geq 1 \geq 1 \geq 1 \geq 1 \ldots \geq 1 \\
\geq 1 & \geq 1 \geq 1 \geq 1 \geq 1 \ldots \geq 1 \\
\geq 0 & \geq 0 \geq 0 \ldots \geq 0 \\
\geq 0 & \geq 0 \ldots \geq 0 \\
\geq 0 & \ldots \geq 0 \\
& \vdots \\
& \geq 0
\end{align*}

(6)

and $\beta_1^{(n)}$ (resp. $\beta_2^{(n)}$) are the probabilities of isotropy given that the reduction modulo $p$ of the form in $x_3, x_4, \ldots, x_n$ is in Case I (resp. Case II).

1In this and the similar arrays which follow, we put into position $(i, j)$ the known condition on $v(a_{i,j})$, so the top left entry refers to the coefficient of $x_1^2$, the top right to $x_1x_n$ and the bottom right to $x_n^2$. 

7
Similarly, in Case II the initial transformation leads to

\[
\begin{array}{cccccccc}
= 1 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \ldots & \geq 1 \\
\geq 0 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \ldots & \geq 1 \\
\geq 0 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \ldots & \geq 1 \\
\geq 0 & \geq 1 & \ldots & \geq 1 \\
\geq 1 & \ldots & \geq 1 \\
\geq 0 & \ldots & \geq 0 \\
\geq 0 & \ldots & \geq 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\geq 0 & \ldots & \geq 0 \\
\geq 0 & \ldots & \geq 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\geq 0 \\
\end{array}
\]

(7)

and \(\gamma_1^{(n)}\) (resp. \(\gamma_2^{(n)}\)) are the probabilities of isotropy given that the reduction modulo \(p\) of the form in \(x_2, x_3, \ldots, x_n\) is in Case I (resp. Case II).

(i) To evaluate \(\beta_1^{(n)}\) we may assume, after a second linear change of variables, that we have

\[
\begin{array}{cccccccc}
\geq 1 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \ldots & \geq 1 \\
\geq 1 & \geq 1 & \geq 1 & \\
\geq 0 & \geq 1 & \geq 1 & \\
\geq 0 & \geq 1 & \ldots & \geq 1 \\
\geq 0 & \ldots & \geq 1 \\
\geq 0 & \ldots & \geq 0 \\
\geq 0 & \ldots & \geq 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\geq 0 \\
\end{array}
\]

and that the reductions mod \(p\) of both \(\frac{1}{p}Q(x_1, x_2, 0, \ldots, 0)\) and \(Q(0, 0, x_3, x_4, 0, \ldots, 0)\) are irreducible binary quadratic forms. Any zero of \(Q\) must satisfy \(x_3 \equiv x_4 \equiv 0 \pmod{p}\). This gives a contradiction when \(n = 4\), so that \(Q(x_1, \ldots, x_4)\) is anisotropic, and \(\beta_1^{(4)} = 0\). Otherwise, replacing \(Q(x_1, \ldots, x_n)\) by \(\frac{1}{p}Q(x_3, x_4, px_1, px_2, x_5, \ldots, x_n)\) brings us back to the situation in (6). Now, however, the line condition holds, so that Cases I and II occur with probabilities \(\nu_1^{(n-2)}\) and \(\nu_2^{(n-2)} = 0\) instead of \(\xi_1^{(n-2)}\) and \(\xi_2^{(n-2)}\).

(ii) To evaluate \(\beta_2^{(n)}\), we may assume that the valuations of the coefficients satisfy

\[
\begin{array}{cccccccc}
\geq 1 & \geq 1 & \geq 1 & \geq 1 & \geq 1 & \ldots & \geq 1 \\
\geq 1 & \geq 1 & \geq 1 & \ldots & \geq 1 \\
0 & \geq 1 & \ldots & \geq 1 \\
\geq 0 & \ldots & \geq 1 \\
\geq 0 & \ldots & \geq 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\geq 0 \\
\end{array}
\]

and that the reduction mod \(p\) of \(\frac{1}{p}Q(x_1, x_2, 0, \ldots, 0)\) is an irreducible binary quadratic form. If \(n = 3\) then \(Q\) is anisotropic, and \(\beta_2^{(3)} = 0\). Otherwise, replacing \(Q(x_1, \ldots, x_n)\) by \(\frac{1}{p}Q(x_2, x_3, px_1, x_4, \ldots, x_n)\) brings us back to the situation in (7) but with the line condition, so that Cases I and II occur with probabilities \(\nu_1^{(n-1)}\) and \(\nu_2^{(n-1)}\) instead of \(\xi_1^{(n-1)}\) and \(\xi_2^{(n-1)}\).
(iii) For $\gamma_1^{(n)}$, we may assume that the valuations of the coefficients satisfy

\[
\begin{array}{ccccccccc}
= 1 & \geq 1 & \geq 1 & \cdots & \geq 1 \\
\geq 0 & \geq 0 & \geq 1 & \cdots & \geq 1 \\
\geq 0 & \geq 1 & \cdots & \geq 1 \\
\geq 1 & \cdots & \geq 1 \\
\cdots & \cdots & \cdots & \cdots \\
\geq 1
\end{array}
\]

and the reduction of $Q(0, x_2, x_3, 0, \ldots, 0) \mod p$ is irreducible. Any zero of $Q$ now satisfies $x_2 \equiv x_3 \equiv 0 \pmod p$. When $n = 3$ this gives a contradiction, so $Q(x_1, x_2, x_3)$ is anisotropic, and $\gamma_1^{(3)} = 0$. Otherwise, replacing $Q(x_1, \ldots, x_n)$ by $\frac{1}{p}Q(x_3, px_1, px_2, x_4, \ldots, x_n)$ brings us back to the situation in (6) but with the point condition, so that Cases I and II occur with probabilities $\eta_1^{(n-2)}$ and $\eta_2^{(n-2)}$.

(iv) Lastly, for $\gamma_1^{(n)}$, we may assume that the valuations of the coefficients satisfy

\[
\begin{array}{ccccccccc}
= 1 & \geq 1 & \geq 1 & \cdots & \geq 1 \\
= 0 & \geq 1 & \cdots & \geq 1 \\
\geq 1 & \cdots & \geq 1 \\
\cdots & \cdots & \cdots & \cdots \\
\geq 1
\end{array}
\]

If $n = 2$ then $Q(x_1, x_2)$ is anisotropic, and $\gamma_2^{(2)} = 0$. Otherwise, replacing $Q(x_1, \ldots, x_n)$ by $\frac{1}{p}Q(x_2, px_1, x_3, \ldots, x_n)$ brings us back to the situation in (7) but with the point condition. □

5 Conclusion

Using Lemmas 3 and 5 we can compute $\beta_j^{(n)}$ and $\gamma_j^{(n)}$ for $j = 1, 2$ and all $n$: we first determine $\beta_1$ from Lemma 5 (i), then $\beta_2^{(n)}$ and $\gamma_1^{(n)}$ together using Lemma 5 (ii,iii), and finally $\gamma_2^{(n)}$ using Lemma 5 (iv). The following table gives the result:

| $n$   | $\beta_1^{(n)}$ | $\beta_2^{(n)}$ | $\gamma_1^{(n)}$ | $\gamma_2^{(n)}$ |
|-------|-----------------|-----------------|-----------------|-----------------|
| $n = 2$ | $-$             | $-$             | $-$             | $0$             |
| $n = 3$ | $-$             | $0$             | $0$             | $1/2$           |
| $n = 4$ | $0$             | $(2p+1)/(2p+2)$ | $(p+2)/(2p+2)$  | $1 - (p/(4(p^2+p+1))$ |
| $n \geq 5$ | $1$             | $1$             | $1$             | $1$             |

Now, using Lemma 4, we compute $\alpha_1^{(n)}$ and $\alpha_2^{(n)}$:

| $n$   | $\alpha_1^{(n)}$ | $\alpha_2^{(n)}$ |
|-------|-----------------|-----------------|
| $n = 2$ | $0$             | $1/(2p+2)$     |
| $n = 3$ | $1/(p+1)$       | $(p+2)/(2p+2)$ |
| $n = 4$ | $1 - (p^3/(2(p+1)(p^2+p+1)))$ | $1 - (p^3/(4(p+1)(p^3+p^2+p+1)))$ |
| $n \geq 5$ | $1$             | $1$             |
Finally, we compute $\rho_n(p)$ using (5), yielding the values stated in Theorem 1.

Note that our proof of Theorem 1 also yields a (recursive) algorithm to determine whether a quadratic form over $\mathbb{Q}_p$ is isotropic. Tracing through the algorithm, we see that, for a quadratic form of nonzero discriminant, only finitely many recursive iterations are possible (since we may organize the algorithm so that at each such iteration the discriminant valuation is reduced), i.e., the algorithm always terminates. In particular, when $n \geq 5$, our algorithm always yields a zero for any $n$-ary quadratic form of nonzero discriminant; hence every nondegenerate quadratic form in $n \geq 5$ variables is isotropic.

Acknowledgments

We thank Jonathan Hanke and Terence Tao for helpful conversations. The first author was supported by a Simons Investigator Grant and NSF grant DMS-1001828.

References

[1] G. W. Anderson, A. Guionnet, and O. Zeitouni, An Introduction to Random Matrices, Cambridge Studies in Advanced Mathematics 118, Cambridge University Press, 2009.

[2] D. Dean and S. Majumdar, Extreme Value Statistics of Eigenvalues of Gaussian Random Matrices, http://arxiv.org/abs/0801.1730.

[3] J-P. Dedieu and G. Malajovich, On the number of minima of a random polynomial, http://arxiv:math/0702360.

[4] T. Ekedahl, An infinite version of the Chinese remainder theorem, Comment. Math. Univ. St. Paul. 40 (1991), 53–59.

[5] B. Poonen and P. Voloch, Random Diophantine equations, Arithmetic of Higher-Dimensional Algebraic Varieties, 175–184, Progress in Mathematics 226, 2004, Birkhäuser, Boston, MA.