Universal quadratic forms and the 290-Theorem

Manjul Bhargava and Jonathan Hanke

1 Introduction

In 1993, Conway formulated a remarkable conjecture regarding universal quadratic forms, i.e., integer-coefficient, positive-definite quadratic forms representing all positive integers. Based on theoretical evidence and computations performed by his students Miller, Schneeberger, and Simons, Conway conjectured that such a quadratic form represents all positive integers if and only if it represents all positive integers up to 290. In fact, he conjectured that for such a quadratic form to be universal, it is necessary and sufficient for the form to represent a certain specified set of 29 integers, the largest of which is 290.

The purpose of the present article is to prove this conjecture.

Theorem 1 ("The 290-Theorem") *If a positive-definite quadratic form with integer coefficients represents the twenty-nine integers*

$$\begin{array}{c} 1,2,3,5,6,7,10,13,14,15,17,19,21,22,23,26, \\ 29,30,31,34,35,37,42,58,93,110,145,203, \textit{and } 290 \end{array} \tag{1}$$

then it represents all positive integers.

We call the integers listed in (1) the **critical integers**. To show that these integers are indeed critical in the 290-Theorem, we prove:

Theorem 2 *For each of the twenty-nine critical integers t, there exists a positive definite quadratic form with integer coefficients which fails to represent t but represents every other positive integer.*

The following result shows that the number 290 plays a rather special role among the critical numbers:

Theorem 3 *If a positive-definite quadratic form with integer coefficients represents every positive integer below* 290*, then it represents every integer above* 290*.*

One of the historical motivations for proving a result in the spirit of Theorem 1 was to determine all universal quadratic forms in four variables (four being the minimal number of variables possible for a universal quadratic form). The first result in this direction is due to Lagrange [17], who showed that every positive integer can be expressed as the sum of four squares; i.e., the form $a^2 + b^2 + c^2 + d^2$ is universal. Other universal forms were later investigated by Waring [27], Jacobi [13], and Liouville [18], among others.

The first systematic investigation of universal quaternary forms was carried out by Ramanujan [19], who determined all universal quaternary diagonal forms. (There are 54 of them.) Ramanujan's assertions were later given detailed proofs by Dickson, while various other authors attempted to extend Ramanujan's list to non-diagonal forms. In this regard, Willerding exhibited 168 quaternary universal forms having integer-matrix. In [1], it was shown that there are exactly 204 universal forms having integer-matrix. The 290-Theorem at last allows us to completely solve the problem of determining all universal quaternary forms. We prove:

Theorem 4 *There are exactly* 6436 *universal quaternary forms.*

The proofs of Theorems 1–4 require the confluence of several recent theoretical and computational advances in the arithmetic of quadratic forms—along with a bit of good luck. The theoretical advances include the escalation method (cf.§2–§4.1) as well as new effective bounds on the Fourier coefficients of weight 2 theta functions (cf. §4.2). The computational advances include efficient new ways to check representability of eligible numbers and rapidly compute arbitrary local densities of a number by a quadratic form (cf. §4.3). The bit of good luck includes an arithmetic trick (the "10-14 switch"—cf. §5.2) which allows us to reduce the proofs of Theorems 1–4 almost entirely to the study of quadratic forms in four variables.

We introduce the escalation method in §2, and compute the necessary small-dimensional escalator lattices in §3 and §4.1. In §4.2–§4.4 we determine the integers represented by the four-dimensional escalators, and we describe the new arithmetic, analytic, and computational techniques that lie behind these determinations. In §5 we study all higher-dimensional escalators. Finally, in §6, we use this information to complete the proofs of Theorems 1–4.

2 Preliminaries

The proof of the 290-Theorem is perhaps best enunciated geometrically using the language of lattices. As is well-known, there is a natural bijection between equivalence classes of integer-coefficient quadratic forms and lattices having integer norms; precisely, a quadratic form f can be regarded as the norm form for a corresponding lattice $L(f)$. Hence we shall freely move between the language of forms and the language of lattices. For brevity, by a "form" we shall always mean a positive-definite quadratic form $\sum_{1\leq i\leq j\leq n} c_{ij}\, x_i x_j$ having integer coefficients c_{ij}, and by a "lattice" we shall always mean a lattice having integer norms.

A form (or its corresponding lattice) is said to be **universal** if it represents every positive integer. If a form f happens not to be universal, define the **truant** of f (or of its corresponding lattice $L(f)$) to be the smallest positive integer not represented by f.

Important in the proof of the 290-Theorem is the notion of "escalator lattice." An **escalation** of a nonuniversal lattice L is defined to be any lattice which is generated by L and a vector whose norm is equal to the truant of L. An **escalator lattice** is a lattice which can be obtained as the result of a sequence of successive escalations of the zero-dimensional lattice.

3 Small-dimensional escalators

The unique escalation of the zero-dimensional lattice is the lattice generated by a single vector of norm 1. This lattice corresponds to the form x^2 (or, in matrix form, $[1]$) which fails to represent the number 2. Hence every escalation of $[1]$ has inner product matrix of the form

$$\begin{bmatrix} 1 & a \\ a & 2 \end{bmatrix}.$$

By the Cauchy-Schwartz inequality, $a^2 \leq 2$, and since a must be an integer or half-integer, we conclude that $a = 0$, $\pm 1/2$ or ± 1. The choices $a = \pm 1/2$ lead to isometric lattices, as do the choices $a = \pm 1$, so we obtain only three nonisometric two-dimensional escalators, namely those lattices having Minkowski-reduced Gram matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 \\ 1/2 & 2 \end{bmatrix}, \text{ and } \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

The truants of these three escalators are 3, 3, and 5 respectively. Escalating each of these three two-dimensional escalators in the same manner, we find exactly 34 new nonisometric escalator lattices, namely those having Minkowski-reduced Gram matrices

$$\begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 1 & 1/2 \\ 0 & 1/2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 1 & 1/2 \\ 0 & 1/2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1/2 \\ 0 & 1/2 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 1 & 1/2 \\ 1/2 & 1/2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 1/2 \\ 1/2 & 2 & -1/2 \\ 1/2 & -1/2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 1 & 0 \\ 1/2 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1/2 & 1/2 \\ 1/2 & 2 & 1/2 \\ 1/2 & 1/2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 2 & 1/2 \\ 0 & 1/2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1/2 \\ 0 & 1/2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1/2 & -1/2 \\ 1/2 & 2 & 1/2 \\ -1/2 & 1/2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 1/2 \\ 1/2 & 2 & 0 \\ 1/2 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 2 & 1/2 \\ 0 & 1/2 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1/2 & 0 \\ 1/2 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1/2 \\ 1/2 & 1/2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 0 \\ 1/2 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1/2 \\ 0 & 1/2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1/2 \\ 1/2 & 1/2 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1/2 \\ 0 & 1/2 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 5 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1/2 \\ 1/2 & 1/2 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 0 \\ 1/2 & 0 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1/2 \\ 0 & 1/2 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 5 \end{bmatrix}, \text{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{bmatrix}.$$

It is easy to see that these 34 escalators are all nonuniversal, and their truants are given respectively by

$$\begin{array}{c} 14,\quad 7,\quad 5,\quad 10,\quad 21, \\ 14,\quad 6,\quad 10,\quad 22,\quad 6, \\ 6,\quad 13,\quad 5,\quad 10,\quad 7, \\ 17,\quad 14,\quad 10,\quad 5, \\ 6,\quad 7,\quad 10,\quad 23,\quad 10, \\ 7,\quad 29,\quad 31,\quad 14,\quad 10, \\ 7,\quad 29,\quad 10,\quad 13,\quad \text{and}\quad 10. \end{array}$$

4 The basic four-dimensional escalators

Escalating now each of the above 34 three-dimensional escalators, we obtain 6560 nonisomorphic four-dimensional escalator lattices. We call these the **basic** four-dimensional escalators. We note that other four-dimensional escalators can be obtained as the result of a sequence of escalations of these basic escalators; however, since every four-dimensional escalator contains a basic escalator—and since most of these basic four-dimensional escalators are either universal or represent all but a sparse set of positive integers—it will suffice for us to consider only the basic escalators in dimension four.

4.1 Arithmetic methods

For each basic four-dimensional escalator L_4, we wish to determine *exactly* the set of positive integers represented by L_4. In many cases, this can be accomplished through arithmetic methods as in [1]. Namely, in each such L_4, we look for a 3-dimensional sublattice L_3 which is known to represent some large set of integers. Typically, we choose L_3 to be unique in its genus, in which case L_3 represents all integers that it represents locally (i.e., over each p-adic ring $\mathbb{Z}_p$). With this knowledge of L_3, we then show that the direct sum of L_3 with its orthogonal complement in L_4 represents all sufficiently large integers n locally represented by L_4. A check of representability for small n reveals exactly those numbers represented by L_4.

For example, let us consider the escalations L_4 of the escalator lattice L_3 corresponding to Legendre's three squares form $x^2 + y^2 + z^2$. This 3-dimensional lattice L_3 is well-known to be unique in its genus, and it represents all positive integers not of the form $4^a(8k + 7)$ for some integer a. Suppose $[m]$ is the Gram matrix of the orthogonal complement of L_3 in L_4. We wish to show that $L_3 \oplus [m]$ represents all sufficiently large integers.

To this end, suppose L_4 is not universal, and let u be the first integer not represented by L_4. Then, in particular, u is not represented by L_3, so u must be of the form $4^a(8k+7)$. Moreover u must be squarefree (by minimality), so $a = 0$ and $u \equiv 7 \pmod 8$.

Now if $m \not\equiv 0$, 3 or 7 (mod 8), then clearly $u - m$ is not of the form $4^a(8k+7)$. Similarly, if $m \equiv 3$ or 7 (mod 8), then $u - 4m$ cannot be of the form $4^a(8k + 7)$. Thus if $m \not\equiv 0$ (mod 8), and if $u \geq 4m$, then either $u - m$ or $u - 4m$ is represented by L_3, so u is represented by $L_3 \oplus [m]$ for all $u \geq 4m$. For all escalations L_4 of L_3 it is easy to see that the associated m never exceeds 27, and one checks that eash such L_4 represents all integers less than $4 \times 27 = 108$. It follows that any such escalator L_4 is universal when its associated value of m is not a multiple of 8. Fortunately, the values $m = 8, 16$, and 24 do not arise, proving the universality of all escalations of $x^2 + y^2 + z^2$. (In particular, this includes a proof of Lagrange's four squares theorem.)

Of the 34 three-dimensional escalator lattices, 20 of them are unique in their genus; thus they too represent all numbers they locally represent, and most of their escalations can be handled similarly. In fact, *all* escalations of 17 of these 20 three-dimensional escalators can be handled in this way, namely #'s 1–8, 10–12, 17, 19, 21, 22, 24, and 34 on the list of ternary escalators in Section 3. This determines what numbers are represented by 1658 of the 6560 basic four-dimensional escalators.

If we allow other values for L_3, then many more basic four-dimensional escalators can be handled, but not all of them. In fact, one can show that more than 2300 of the 6560 contain *no* three-dimensional form of class number one! Although more sophisticated arithmetic techniques can be applied to some of these, it quickly becomes clear that an alternative method is necessary to effectively deal with the remaining four-dimensional escalators.

4.2 Analytic methods

In 1929 Tartakowsky [26] established the first analytic result about the numbers represented by an integral quadratic form, proving that any form of dimension ≥ 5 represents all sufficiently large integers that it locally represents. A similar result due to Kloosterman [16] holds for 4-dimensional forms, assuming possibly that the integer is not too divisible by finitely many **anisotropic primes**.* In all of our basic 4-dimensional escalators, there are no anisotropic primes, so in principle we can use this result to understand which numbers are represented by each them. However to apply this idea in practice, one needs an *effective* version which says how large is "sufficiently large", and this bound needs to be reasonably small.

General effective versions of the Tartakowsky-Kloosterman theorem have been obtained by several authors, such as by Watson [29] and Hsia and Icaza [11] † (in dimension ≥ 5) and by Fomenko [7] and Schulze-Pillot [23] (in dimension 4). However, even the best of these effective results have not been of much practical use. For example, the best of these bounds for representing prime numbers p by the Kneser form $x^2 + 3y^2 + 5z^2 + 7w^2$ of level $N = 420$ requires that one check the representability of all $p < 3.73 \times 10^{34}$. Even assuming N is squarefree (which always gives a substantial improvement), we would still need to check all $p < 5.13 \times 10^{12}$.

The difficulty with these previous approaches is that they treat all modular forms/theta functions of a given level simultaneously, and use estimates for all forms of a given level. Although they are the best known uniform estimates, their uniformity comes at the price of accuracy for individual forms. By studying individual forms Q, practical versions of the Tartakowsky-Kloosterman theorem for Q can be achieved using the theory of modular forms. We note that modular forms are secretly present in the works of Tartakowsky and Kloosterman, and explicitly appear in Schulze-Pillot's formulation, so it is natural

*In fact they prove more, namely that if m is locally represented then $r_Q(m) \to \infty$ as $m \to \infty$, which as a special case gives $r_Q(m) > 0$ if m is sufficiently large. For a more detailed exposition of the history, see the survey papers [5], [9], [25], [20] and [12].

†by arithmetic methods

to guess that a more detailed study of their properties would yield improved bounds for representability. This direction was recently pursued by the second author in [8], where the integers represented by the Kneser form $x^2 + 3y^2 + 5z^2 + 7w^2$ were explicitly determined.

Modular forms arise because for any positive definite integer-valued quadratic form Q in n variables, the Fourier series generating function

$$\Theta_Q(z) = \sum_{m \geq 0} r_Q(m)\, e^{2\pi i m z}$$

is a modular form of weight $n/2$ for some congruence subgroup $\Gamma_0(N) \subseteq SL(2, \mathbb{Z})$. From the general theory of such modular forms, we can decompose $\Theta_Q(z)$ naturally as a sum of an **Eisenstein series** $E(z)$ and a **cusp form** $f(z)$, whose Fourier coefficients have different growth rates as $m \to \infty$. In particular, the Eisenstein coefficients $a_E(m)$ are always non-negative and grow more quickly than the cusp form coefficients $a_f(m)$. By establishing an effective lower bound for $a_E(m)$ and an effective upper bound for $|a_f(m)|$ we may obtain an effective version of the Tartakowsky-Kloosterman result.

4.2.1 The Eisenstein coefficients $a_E(m)$

The Eisenstein coefficients $a_E(m)$ have a very natural meaning in terms of the local behavior of the quadratic form Q, due to Siegel [22], which gives

$$a_E(m) = \prod_v \beta_v(m)$$

as a product of local densities $\beta_v(m)$. Here each $\beta_v(m)$ measures the number of local (integral) representations of m by Q_v at each completion v of $\mathbb{Q}$. The real local density at $\beta_\infty(m)$ is easily computed as the volume of the real ellipsoid $Q(x) = m$, while the local density at each prime p is given as

$$\beta_p(m) = \lim_{r \to \infty} \frac{\#\{\vec{x} \in (\mathbb{Z}/p^r\mathbb{Z})^n \mid Q(\vec{x}) \equiv m \pmod{p^r}\}}{p^{n(r-1)}}$$

which roughly counts the (normalized) number of representations of m by Q over the p-adic integers $\mathbb{Z}_p$.

Because of the local multiplicative nature of $a_E(m)$, an effective lower bound for $a_E(m)$ follows from reasonable lower bounds for each of the local densities $\beta_v(m)$, which reflect an understanding of how the number of solutions of $Q(x) = m \pmod{p^r}$ grows as $r \to \infty$. For most primes p this solution counting is fairly straightforward, but if $p \mid \det(2Q)$ then the answer may additionally involve solutions of several simpler auxilary quadratic forms, whose densities must also be computed to obtain the desired lower bound. Combining these local estimates in the case of a quaternary form Q gives an effective bound

$$a_E(m) \geq C_E\, m \prod_{\substack{p \nmid N,\, p \mid m \\ \chi(p) = -1}} \frac{p-1}{p+1}$$

for all numbers m locally represented by Q. An exact formula for the constant $C_E > 0$ is described in Theorems 5.7(b) and 6.3 of [8], though computing it for any given form is extremely complicated. It requires knowing all possible local densities $\beta_p(m)$ at all primes! When $p \mid 2\det(2Q)$ this is accomplished using the explicit reduction maps (with congruence conditions) described in [8, §3], while for $p = 2$ we additionally must count points on certain ellipsoids (with congruence conditions) over $\mathbb{Z}/8\mathbb{Z}$.

4.2.2 The cusp form coefficients $a_f(m)$

The nature of the cusp form $f(z)$ appearing in the theta function $\Theta_Q(z)$ and its precise relationship with Q are more mysterious. To obtain an upper bound for the size of its Fourier coefficients $a_f(m)$, we appeal to the general theory of Hecke eigenforms and write

$$f(z) = \sum_{i=1}^{r} \gamma_i \, f_i(z) \qquad \text{for some } \gamma_i \in \mathbb{C}$$

as a linear combination of Hecke eigenforms $f_i(z)$ normalized so that each of their first Fourier coefficients $a_i(m) = 1$. By applying the weight 2 Ramanujan bound to the normalized eigenforms $f_i(z)$, we obtain the explicit upper bound

$$|a_f(m)| \leq C_f \, 2^{P(m)} \tau(m) \sqrt{m}$$

where $C_f = \sum |\gamma_i|$, $P(m)$ is the number of distinct prime divisors of m, and $\tau(m)$ is the number of (positive) divisors of m.

To find the γ_i's, we write the new part $f^{\mathrm{new}}(z)$ of $f(z)$ as a sum over Galois-conjugate newforms $f_j(z)$. Since all $a_f(m) \in \mathbb{Q}$, $\gamma_{i'} = \gamma_i^\sigma$ whenever $f_{i'} = f_i^\sigma$ for some embedding $\sigma : K_j := \mathbb{Q}(a_i(m)) \to \bar{\mathbb{Q}}$, and we have that

$$f(z) = \sum_j \sum_{\sigma : K_j \to \bar{\mathbb{Q}}} (\gamma_j f_j(z))^\sigma = \sum_{m>0} \sum_j \mathrm{Tr}_{K_j/\mathbb{Q}}(\gamma_j \, a_j(m)).$$

By regarding both γ_j and $a_j(m)$ as vectors over $\mathbb{Q}$ in the basis given by powers of some α_j such that $K_j = \mathbb{Q}(\alpha_j)$, and finding the (rational) trace matrix for this basis, we can exactly determine the γ_i's by simultaneously solving these rational linear equations for sufficiently many m. By repeating this procedure to solve for the components of $f - f^{\mathrm{new}}$ in $\mathrm{Span}\{f_j(d\,z)\}$ for each possible $d \mid N$, we can completely decompose f into its Galois-conjugate components. We then find C_f by summing the absolute values of all embeddings γ_i^σ over all possible d.

4.2.3 The explicit bound for representability

By combining the bounds for $a_E(m)$ and $a_f(m)$, we know that any number m which is locally represented by Q and satisfies

$$\frac{\sqrt{m}}{\tau(m)} \prod_{\substack{p \nmid N,\, p \mid m \\ \chi(p) = -1}} \frac{p-1}{p+1} < M \tag{2}$$

must be represented by Q, where $M = C_E/C_f$. Since the right side of (2) is an increasing function as m becomes more divisible, we see that there are only finitely many numbers whose representability by Q is in question. In practice this bound may still be quite large, but the multiplicative nature of this bound allows us to avoid checking all numbers for which (2) fails.

In general the size of the Eisenstein bound C_E is small, with the overall difficulty of our computation – governed by the size of M – coming from the presence of many "large" cusp forms. This parallels the difficulties appearing in the arithmetic method, where such erratic behavour of $r_Q(m)$ makes it difficult to find embeddings of known regular forms, and often indicates that Q has many classes in its genus.

As an example, of our 6560 quaternaries the largest bound comes from (Form #6414) $Q(\vec{x}) = x^2 + 2y^2 + 4z^2 + 31w^2 + yz - yw + 3zw$, which has level $N = 3744$ and $\chi(\cdot) = (\frac{104}{\cdot})$. For this form, we find that $C_E = 36/125$ and $C_f \approx 2331.99 < 2332.99$, giving the overall bound $M < 8100.65$.

4.3 Computational methods

We say that an integer m is **eligible** for a quaternary quadratic form Q if m is locally represented by Q but (2) does not hold. In the previous section we saw that there are finitely many (though possibly a very large number of) eligible numbers, and our task in this section is to quickly determine which of them are represented by Q. To do this in practice for large sets of eligible numbers, several additional computational ideas are needed.

4.3.1 Generating eligible numbers

For convenience, we let $B(m)$ denote the left side of (2). Since $B(m)$ is multiplicative, and $B(p) > 1$ for all primes $p > 7$, all prime divisors p of an eligible number m must satisfy

$$B(p) < \frac{M}{B(2)\, B(3)\, B(5)\, B(7)},$$

giving an explicit set of possible prime divisors for m. We call such primes p **eligible primes**, although they may not themselves be eligible numbers! It is also useful at this point to slightly reorder the eligible primes, so their "size" refers to the size of their $B(p)$.

We then determine the maximum possible number of (distinct) prime divisors in any eligible number m by taking the product of the smallest eligible primes p_i and checking how many primes are needed to ensure that $p_1 \cdots p_{s+1}$ is not eligible. This gives us a very efficient way of generating all eligible numbers as products of at most s eligible primes.

To generate a list of square-free eligible numbers $t = p_1 \cdots p_r$ arising as products of exactly r eligible primes, we start by taking the p_i to be the smallest r eligible primes, and increase p_r until t is no longer eligible. When this happens, we increment p_{r-1} to the next eligible prime, and set p_r to be the first eligible prime $> p_{r-1}$. If this t is eligible then we keep increasing p_r as before, but if not, then we increment p_{r-2} and set p_{r-1} and p_r equal to the next two eligible primes $> p_{r-2}$. Continuing in this way for each $r \leq s$, we produce all square-free eligible numbers t.

In practice, we precompute the set of eligible primes p and store their associated values $B(p)$ for quick computations of the values $B(m)$. Because it is time-consuming to compute the exact value of $B(p)$ for all eligible primes p, we only do this for all $p < 10^4$ and use the approximation $B(p) \approx \frac{\sqrt{p}}{2}(1-\frac{1}{p}) < B(p)$ for $p > 10^4$. To reduce memory requirements, we generate only a million eligible square-free numbers at a time, and check their representability before proceeding to the next million numbers.

4.3.2 Checking eligible numbers

After generating a set of eligible numbers m, we must quickly check if each m is represented by Q. An obvious way of doing this is to compute the theta function of Q up to some precision $\geq m$ (i.e. the first $m+1$ Fourier coefficients) by finding the lengths of all vectors in some large ellipsoid, and then checking whether the coefficient $r_Q(m) = 0$ for each m. However this is not very practical for two reasons. The first problem is that computing the theta function in this way up to precision X takes time $\approx X^{\dim(Q)/2} = X^2$, which is rather slow for large precisions. The second problem is that the precision we need may itself be extremely large, so that even if we could quickly compute the theta function, it would be too large to reasonably store.

We reduce the required theta function precision by finding a **split local cover** for each quaternary Q, by which we mean a sublattice of L on which the quadratic form Q splits as $Q' = dx^2 \oplus T$ for some $d \in \mathbb{N}$ and some ternary form T, with the additional property that Q and Q' represent the same numbers locally. In fact, we will always choose a split local cover for which d is minimal. We then look to see if each m is represented by Q' (hence also by Q), and then test the remaining (very small) set of possible exceptions of Q' for representability by Q. For our 4-dimensional forms we do this by naively computing $\Theta_Q(z)$ up to precision 10,000, which suffices for all possible exceptions that arise.

Given a split local cover Q', we check if Q' represents m by finding the largest value $dx_0^2 < m$ and then check if $m - dx_0^2$ is represented by T. If not, we decrement x_0 and repeat, until we either find that m is represented by Q' or we exceed the precomputed precision Y of the ternary theta function $\Theta_T(z)$. To ensure that $m - dx_0^2 < Y$, we require ternary precision $Y \approx 2d\sqrt{X}$. However since we may need several attempts to verify $r_{Q'}(m) > 0$, we compute $\Theta_T(z)$ to precision $\approx 10d\sqrt{X}$ which allows at least 5 attempts for each eligible number m.

To decrease the time needed to compute the ternary theta functions $\Theta_T(z)$ (which naively is $\approx Y^{\frac{3}{2}}$ for precision up to Y), we instead compute an **approximate boolean theta function**, which keeps a single bit describing whether $T(\vec{y}) = m$ has a solution in an appropriately chosen small rectangular cylinder in the ellipsoid $T(\vec{y}) \leq Y$. By the equidistribution results of Duke and Schulze-Pillot [6, Theorems 1 and 3], we expect that the intersection of this cylinder with the ellipsoid $T(x) = m$ should have a roughly constant number of integer points, and so there are $\approx Y^{\frac{1}{2}}$ vectors we need to check.* By choosing the short dimensions of the cylinder to be large enough, we are able to detect most of the numbers represented by T, though a few may be missed. However because we get several attempts to verify the representability of each m, these few omissions are unimportant.

The combined use of a split local cover and an approximate boolean theta function to check representability of all $m < X$ by Q requires us to store $\sqrt{X}$ bits and takes $O(X^{\frac{1}{4}})$

*This assumes we are considering numbers which are primitively represented by the spinor genus of T, meaning they have a priori bounded divisibility at the anisotropic primes, and avoid the certain numbers in finitely many "spinor square classes". This is discussed explicitly in [9, §5 and §7], [24, §4] and [8, §4].

time. This provides a *substantial* savings over the naive method, which would store X bits and take $O(X^2)$ time!

4.3.3 Error checking and precision issues

As with any large computation, the possibility of error is a real issue. This is especially true when using a computer, whose operation can only be viewed intermittently and whose accuracy depends on the reliability of many layers of code beneath the view of all but the most proficient computer scientist. We have taken many steps to ensure the accuracy of our computations, the most important of which are described below.

Open source code in established languages – The code for this project was written in Magma (for escalations and embeddings) and in C++ (for the analytic method), and its source code can be freely downloaded from the authors' websites. We hope that other researchers may find this code useful in their own work, and through a desire to extend or improve it, will notice and report any possible bugs or inefficiencies. Additionally, to reach the widest possible audience, this code will be included in the SAGE software package which has a very friendly Magma-like user interface and uses the Python scripting language.

Local density and lower bound accuracy checking – The local density computations used to find the Eisenstein constant C_E are quite involved when $p \mid 2\det(2Q)$, hence prone to subtle errors. Therefore for each form Q and all $m < 100$ we have verified Siegel's formula by computing the (infinite) product of local densities (in C++) and checking that this agrees with $E(z)$ computed as the weighted average of theta functions over all classes in the genus of Q (in Magma).

The lower bound constant C_E is further checked for accuracy by comparing it with the naive constant satisfied by the first 10,000 coefficients of $E(z)$. In all cases, this naive constant is $\geq C_E$ as expected, and their difference is $< 10^{-3}$.

Roundoff error tolerance – All C++ integer computations with the potential to be large have used the GMP arbitrary precision integer type `mpz_class`, and all local densities and Eisenstein coefficients are computed exactly with the corresponding rational number type `mpq_class`. The cuspidal constants C_f were computed exactly over $\mathbb{Q}$ in MAGMA until the very last step, where the complex embeddings were found. Though the accuracy of the embedding appears to be valid to at least 150 decimal places, to be on the safe side we use instead the more permissive bound $C_f + 1$. When the degree of the coefficient fields K_j are > 100, it is quite time-consuming to solve for the exact coefficients in K_j, and we use the approximate cuspidal constants kindly provided to us by William Stein with an accuracy of 3 decimal places.

4.3.4 The largest example

To see how these techniques work in practice, we give the details of the computation for the locally universal form (Form #6414) $Q(\vec{x}) = x^2 + 2y^2 + 4z^2 + 31w^2 + yz - yw + 3zw$, which has the largest overall bound $M < 8100.65$. This form has 36,795,947 eligible primes and its squarefree eligible numbers m can have at most 14 prime factors. By looking at the orthogonal complements of small vectors, and checking local conditions, we compute (obviously) that $Q' = x^2 \oplus T$ where $T = 2y^2 + 4z^2 + 31w^2 + yz - yw + 3zw$ is a minimal split local cover, and estimate the largest eligible m to be $< 8.17 \times 10^{16}$ by solving for m in (2). We then compute an approximate boolean theta function of T to precision 5.14×10^9 by performing LLL-reduction on T (which in this case leaves T unchanged) and finding the lengths of all vectors $\vec{v} = (y, z, w)$ in the rectangular cylinder $0 \leq y, z \leq 800$ and $w \geq 0$, inside the ellipsoid $T(\vec{v}) < 5.14 \times 10^9$. This computation took approximately 200 minutes.

With this, we generate the 28 billion eligible squarefree numbers m (a million at a time) and check that some $m - x^2$ is represented by T. This checking took a little under 1.5 days, and verified that there are no square-free exceptions. Therefore Q has no exceptions, and represents all non-negative integers. †

It is interesting to see how this concrete example relates to the analytic bounds previously mentioned in §4.2. To compare these estimates, suppose we were only interested in knowing which prime numbers p are represented by Form #6414. The bound in [23] would require us to check all primes $p < 5.43 \times 10^{49}$, compared to checking all $p < 2.63 \times 10^8$ from (2).

4.4 Summary

The above arithmetic, analytic, and computational methods thus allow us to determine exactly which integers are represented by each of the basic four-dimensional escalators. It turns out that these 6560 basic escalator lattices L may be naturally partitioned into three types:

- Type I: L is universal.
- Type II: L is not universal but misses at most three positive integers, each of which appears on the critical list.
- Type III: L is not locally universal, but is regular, and represents all integers not of the form $4^a(16k + 14)$.

We find that of the 6560 basic four-dimensional escalators, 6402 of them are of Type I, 153 are of Type II, and 5 are of Type III.

5 Higher escalators

By a **higher escalator** we mean any escalator resulting from a sequence of escalations of some basic four-dimensional escalator. The set of all higher escalators has cardinality in the millions, so treating each higher escalator individually would be a daunting task!

Fortunately, escalations of Type II forms may be disposed of easily (see §5.1), since they each miss only finitely many integers. More miraculously, we may also handle the

†For this form, there is an interesting trick of W. Jagy one can use to check that Q represents all positive integers $< X$ *without* checking all eligible numbers individually or storing a boolean ternary theta function for T. This involves finding a split sublattice of the form $221x^2 \oplus T'$ for which d is odd and T' locally represents all (positive) odd integers. One then checks that T' has no odd exceptions $< 6 \times 10^9$ larger than 48563 by keeping track of the largest exception in the current ellipsoid. Using a simple implementation of this idea, Jagy verified that Q has no exceptions $48767 < m < 10^{16}$ in about one month. See [14] for details.

escalations of Type III forms in a uniform manner using a trick we call the "10-14 switch" (see §5.2). This trick allows us to study only about 100 quaternary forms instead of millions of higher-dimensional forms.

5.1 Escalations of Type II forms

Among the 6560 basic four-dimensional escalators, those of Type I do not escalate and thus do not need to be considered. As for the Type II forms, each misses at most three integers; therefore, any basic escalator of Type II will become universal in at most three escalation steps. In particular, any sequence of escalations of a Type II form will result again in a form of Type II or (in at most three escalation steps) will be of Type I and cannot be escalated further.

5.2 Escalations of Type III forms and the 10-14 switch

It remains to consider the escalations of the five basic Type III quaternary escalators, whose Gram matrices are given explicitly by

$$\begin{bmatrix} 1 & 0 & -1/2 & -3 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 1 \\ -3 & 0 & 1 & 10 \end{bmatrix}, \begin{bmatrix} 1 & 0 & -1/2 & -2 \\ 0 & 2 & 1 & -2 \\ -1/2 & 1 & 5 & 3 \\ -2 & -2 & 3 & 10 \end{bmatrix}, \begin{bmatrix} 1 & 0 & -1/2 & -2 \\ 0 & 2 & 1 & -2 \\ -1/2 & 1 & 5 & 1 \\ -2 & -2 & 1 & 10 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & -1/2 & -1 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 3 \\ -1 & 0 & 3 & 10 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 1 & 0 & -1/2 & -1 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 2 \\ -1 & 0 & 2 & 10 \end{bmatrix}.$$

Each of these forms has truant 14, and each happens to arise as an escalation of the three-dimensional escalator L_3 given by $\begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 5 \end{bmatrix}$ which has truant 10.

The total number of escalations of these five basic four-dimensional escalators is found to be 14221, each of which has dimension four or five (mostly dimension five). The key idea that allows us to treat these forms uniformly is the observation that each of these escalators is obtained by escalating L_3 first by a vector of norm 10, and then again by a vector of length 14.

The latter two operations commute, however, which leads to the idea of the "10-14 switch". Namely, let us consider first all possible lattices generated by L_3 and a vector of norm 14 (i.e., consider first the "escalations of L_3 by 14" instead of by its truant 10). This leads to 330 quaternary forms, which we call the **auxiliary quaternaries**. Any of the 14221 escalators referred to above must clearly contain one of these 330 auxiliary quaternaries.

Remarkably, one finds that 226 of these 330 auxiliary quaternary forms already occurred among the 6555 basic four-dimensional escalators of Type I or II as given in Section 4.4, and hence they need not be reconsidered. Thus only 104 of the 330 auxiliary quaternaries are new. To these, we apply the techniques of Section 4.2.

In the end, we find that each of these 104 forms L is either of Type I, Type II, or exhibits a slightly new behavior, namely that of

- Type IV: L represents all integers except perhaps for those of the form $10n^2$ and $13n^2$.

5.3 Summary

It follows from the above discussion that it is not possible to escalate the zero lattice more than seven times.

Proposition 1 *The zero lattice can be escalated at most seven times.*

Corollary 1 *There is no escalator of dimension greater than seven.*

We are not aware of the existence of any seven-dimensional escalators. On the other hand, one can easily construct millions of escalators that achieve dimension six; for example, any escalation of the 5-dimensional escalator lattice (which has truant 290)

$$\begin{bmatrix} 1 & 0 & -1/2 \\ 0 & 2 & -1/2 \\ -1/2 & -1/2 & 4 \end{bmatrix} \oplus [29] \oplus [145] \qquad (3)$$

is a (universal) six-dimensional escalator.

Thus the escalation story ends by the seventh step. Although we have seen that millions of escalators exist, the Cauchy-Schwartz inequality implies that any lattice will have at most finitely many escalations. Moreover, a look at the list of possible integers missed by the basic quaternary escalators and by the auxiliary quaternaries shows that any escalator—in any dimension—must have a truant contained in the set of 29 critical integers. We summarize this discussion as follows.

Proposition 2 *There are only finitely many escalator lattices, each of which is either universal, or has truant which is contained in the list of* 29 *critical integers.*

6 Proofs of Theorems 1–4

We are now ready to prove Theorems 1–4.

Proof of Theorem 1: We claim that all information about universality of lattices is contained in our study of escalator lattices. To make this precise, we make two observations:

(i) Any universal lattice L must contain a universal escalator,

(ii) The truant of a nonuniversal lattice L must be the truant of some nonuniversal escalator.

To see (i), notice that if L is universal then we may construct within L an escalation sequence $\{0\} \subset L_1 \subset L_2 \subset \cdots$. In at most seven steps, we obtain a universal escalator, by Proposition 1. The same argument applies to (ii): construct a maximal escalation sequence $\{0\} \subset L_1 \subset L_2 \subset \cdots \subset L_k$ $(k \leq 7)$ within L. Then evidently truant(L) =truant(L_k).

On the other hand we have classified all escalator lattices, and the only truants that arise for escalator lattices are contained in the list of 29 critical integers by Proposition 2. Theorem 1 follows. □

Proof of Theorem 2: We first show that for every critical integer t, there actually exists an escalator lattice L such that truant$(L) = t$. The truant 1 occurs for the zero lattice, the truant 2 for the unique one-dimensional escalator, while the truants 3 and 5 arise in the case of the three two-dimensional escalators. The truants that arise for the 34 three-dimensional escalators are 5, 6, 7, 10, 13, 14, 17, 21, 22, 23, 29, 31, while the truants that arise for the basic four-dimensional escalators are 10, 13, 14, 15, 19, 21, 23, 26, 30, 34, 35, 37, 42, 58, 93, 110, and 145.

In (3) we have already seen a 5-dimensional escalator with truant 290. Since

$$L_{145} := \begin{bmatrix} 1 & 0 & -1/2 \\ 0 & 2 & -1/2 \\ -1/2 & -1/2 & 4 \end{bmatrix} \oplus [29] \qquad (4)$$

is the only basic quaternary escalator missing the integer 203, we now use it to produce an escalator with truant 203. First, we note that L_{145} has truant 145; we claim that $L_{203} := L_{145} \oplus [58]$ has truant 203. This is because the only square multiples of 58 less than 203 are 0 and 58, and L_{145} represents neither 203 nor 145, so L_{203} cannot represent 203. However since L_{145} has truant 145, L_{203} represents $\{0, \dots, 144\} \cup \{0+58, \dots, 144+58\} = \{0, \dots, 202\}$. Thus L_{203} has truant 203, proving the claim.

Since L_{203} must contain a vector $\vec{v}$ of norm 145, the lattice L'_{203} generated by L_{145} and $\vec{v}$ in L_{203} must be an escalator with truant 203. Moreover, since $\vec{v}$ must take the form $(*, *, *, 1)$, we actually have $L'_{203} = L_{203}$. Thus every critical integer t occurs as the truant of some escalator.

Finally, given any critical integer t, let L be an escalator with truant t, and consider the lattice $L \oplus [t+1]^{\oplus 4} \oplus [2t+1]$. Then this lattice represents all positive integers except for t, as desired. □

Proof of Theorem 3: We have seen that any escalator L having truant 290 must arise as the result of a sequence of escalations of the escalator L_{145} given in (4), which fails to represent just the three integers 145, 203, and 290. It is evident that any such L having truant 290 will represent every positive integer greater than 290, yielding the desired conclusion. □

Proof of Theorem 4: We observe that a universal quaternary form must have successive minima that are smaller than 1, 2, 5, and 31 respectively (the fastest growing minima for any four-dimensional escalator). Searching through all Minkowski-reduced quaternary quadratic forms having such successive minima, and systematically applying the 290-Theorem, yields the desired result. □

Acknowledgments

The authors thank John Conway, William Jagy, Irving Kaplansky, and William Stein for many helpful discussions and their continued interest in our work. We are especially grateful to William Jagy for his many efforts to understand the basic quaternary escalator #6414, and to William Stein for using his expertise in computing modular forms to find the cuspidal constants C_f for all 6664 of our quaternary escalators.

The authors' source code used to verify all computational statements made in this article may be found at:

`http://www.math.duke.edu/~jonhanke/290/Universal-290.html`

Computations were carried out in C++, Python, Pari/GP, and Magma, and often used the GNU Multiple Precision Arithmetic Library (GMP).

The first author was supported by a Clay Mathematics Institute Long-Term Prize Fellowship. The second author was partially supported by NSA Award H98230-04-1-0076.

References

[1] M. Bhargava, On the Conway-Schneeberger Fifteen Theorem. *Quadratic forms and their applications* (*Dublin, 1999*), 27–37, Contemp. Math., **272**, Amer. Math. Soc., Providence, RI, 2000.

[2] J. H. Conway, Universal quadratic forms and the Fifteen Theorem. *Quadratic forms and their applications* (*Dublin, 1999*), 23–26, Contemp. Math., **272**, Amer. Math. Soc., Providence, RI, 2000. Proceedings.

[3] J. H. Conway and N. A. Sloane, *Sphere packings, lattices and groups*. Third edition. Grundlehren der Mathematischen Wissenschaften **290**, Springer-Verlag, New York, 1999.

[4] L. E. Dickson, Quaternary quadratic forms representing all integers. *Amer. J. of Math.* **49** (1927), 35–56.

[5] W. Duke, Some old problems and new results about quadratic forms. *Notices Amer. Math. Soc.* **44** (1997), no. 2, 190–196.

[6] W. Duke and R. Schulze-Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids. *Invent. Math.* **99** (1990), no. 1, 49–57.

[7] O. M. Fomenko, Estimates of Petersson's inner product with an application to the theory of quaternary quadratic forms. (Russian) *Dokl. Akad. Nauk SSSR* **152** (1963), 559–562.

[8] J. Hanke, Local densities and explicit bounds for representability by a quadratric form. *Duke Math. J.* **124** (2004), no. 2, 351–388.

[9] J. Hanke, Some recent results about (ternary) quadratic forms. *Number theory*, 147–164, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI, 2004.

[10] J. Hanke, On a Local-Global Principle for Integral Quadratic Forms. (preprint).

[11] J. Hsia and M. I. Icaza, Effective version of Tartakowsky's theorem. *Acta Arith.* **89** (1999), no. 3, 235–253.

[12] H. Iwaniec, Spectral theory of automorphic forms and recent developments in analytic number theory. *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Berkeley, Calif., 1986), 444–456, Amer. Math Soc, Providence, RI, 1987.

[13] H. Jacobi, *Jour. für Math.* **21** (1840), 13–32.

[14] W. Jagy, personal communication.

[15] W. Jagy, I. Kaplansky, and A. Schiemann, There are 913 regular ternary forms. *Mathematika* **44** (1997), no. 2, 332–341.

[16] 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.

[17] J. L. Lagrange, Nouveau Mém. Acad. Roy. Sci. Berlin (1772) 123; *Oevres.* vol. 3 1869, pp. 189–201.

[18] J. Liouville, *Jour. de Math.* (2) **1** (1856), 230.

[19] S. Ramanujan, On the expression of a number in the form $ax^2+by^2+cz^2+du^2$. *Proc. Camb. Phil. Soc.* **19** (1916), 11–21.

[20] P. Sarnak, Kloosterman, quadratic forms and modular forms. *Nieuw Arch. Wiskd* (5) **1** (2000), no. 4, 385–389.

[21] W. A. Schneeberger, *Arithmetic and Geometry of Integral Lattices*, Ph.D. Thesis, Princeton University, 1995.

[22] C. L. Siegel, Über die Analytische Theorie der quadratischen Formen. *Ann. of Math.* **36** (1935), 527–606; Gestammelte Abhandlungen, band I, 1966, pp. 326–405.

[23] R. Schulze-Pillot, On explicit versions of Tartakovski's theorem. *Arch. Math.* (*Basel*) **77** (2001), no. 2, 129–137.

[24] R. Schulze-Pillot, Exceptional integers for genera of integral ternary positive definite quadratic forms. *Duke Math. J.* **102** (2000), no. 2, 351–357.

[25] R. Schulze-Pillot, Representation by integral quadratic forms—a survey. *Algebraic and arithmetic theory of quadratic forms*, 303–321, Contemp. Math., 344, Amer. Math. Soc., Providence, RI, 2004.

[26] W. Tartakowsky, *Die Gesamthieit der Zahlen, die durch eine positive quadratische Form* $F(x_1, x_2, \ldots, x_s)\,(s \geq 4)$ *darstellbar sind.* I, II. Bull. Ac. Sc. Leningrad (7) **2** (1929); 111–122, 165–196.

[27] E. Waring, *Meditationes algebraicae.* Cambridge, ed. 3, 1782, 349.

[28] G. L. Watson, One-class genera of positive ternary quadratic forms-II. *Mathematika* **22**, no. 43, 1–11.

[29] G. L. Watson, Quadratic Diophantine equations. *Philos. Trans. Roy. Soc. London Ser. A* **253** 1960/1961 227–254.

[30] M. E. Willerding, *Determination of all classes of positive quaternary quadratic forms which represent all* (*positive*) *integers*, Ph.D. Thesis, St. Louis University, 1948.