UNIVERSAL DIAGONAL QUATERNARY FORMS

STEPHEN ZHOU

1. Introduction

Definition 1.1. A quadratic form f is said to be universal if f represents all positive integers.

Here are some examples of universal and non-universal quadratic forms.

Example. $f(w, x, y, z) = w^2 + x^2 + y^2 + z^2$ is a universal quadratic form.

Example. $f(x, y) = x^2 + y^2$ is not universal by the sum of 2 squares theorem.

Example. $f(x, y, z) = x^2 + y^2 + z^2$ is also not universal.

These examples raise the question of whether there exists a universal quadratic form in less than 4 variables. The answer is no, although we will not prove this. However, we can easily prove this for binary quadratic forms.

Theorem 1.2. *No positive definite binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is universal.*

Proof. We may assume f is reduced since any binary form is equivalent to a reduced form. Then $|b| \leq a \leq c$, and the smallest form represented by f is a. Thus $a = 1$, so $f(x, y) = x^2 + bxy + cy^2$. If $c > 1$, then f does not represent 2, so $c = 1$. Thus the only possible universal quadratic forms are $x^2 + xy + y^2$ and $x^2 + y^2$, neither of which are universal. ∎

It turns out that there are only finitely many universal quaternary (4 variable) quadratic forms. However, for $n \geq 5$, there are infinitely many, since we can add any quadratic form in $n-4$ to a universal quaternary quadratic form in 4 different variables. This motivates the goal of this paper, which is to find all universal quadratic forms of form $ax^2 + by^2 + cz^2 + dw^2$, which are called diagonal quaternary quadratic forms for reasons we will get into later. To find these forms, we will need to prove Legendre's theorem on sums of 3 squares and several analogous theorems.

Theorem 1.3 (Legendre)**.** *An integers n is a sum of 3 squares if and only if n is not of form $4^a(8b + 7)$ for some integers a, b.*

2. Ternary Quadratic Forms

The purpose of the next 2 sections is to prove Legendre's 3 square theorem. We will first prove some facts about ternary forms analogous to those about binary forms.

Theorem 2.1. $f(x, y, z) = x^2 + y^2 + z^2$ *represents all integers excluding those of the form* $4^a(8b + 7)$

Date: October 2023.

Introducing the idea of the symmetric matrix associated with a form makes this easier. Notice that

$$\begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + bxy + cy^2. \tag{2.1}$$

The same thing is also true in higher dimensions. In general, if $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, then

$$\mathbf{x}^T A\mathbf{x} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}x_ix_j = f(x_1, x_2 \ldots x_n). \tag{2.2}$$

Since x_ix_j is $a_{ij} + a_{ji}$ if $j \neq i$, changing the values of the a_{ij} will not affect the matrix as long $a_{ij} + a_{ji}$ is unchanged. Thus there is a unique symmetric matrix corresponding to each form.

Example. The form $f(x, y, z) = x^3 + y^2 + 2z^2 + 3xy + 4xz + 5yz$ corresponds to the matrix

$$\begin{pmatrix} 1 & \frac{3}{2} & 2 \\ \frac{3}{2} & 1 & \frac{5}{2} \\ 2 & \frac{5}{2} & 2 \end{pmatrix} \tag{2.3}$$

Note that A is not integral even though f has all integer coefficients.

Definition 2.2. We call a quadratic form f *integral* if its corresponding symmetric matrix A is integral.

This requires that the coefficients of x_ix_j with $i \neq j$ are even.

Definition 2.3. A quadratic form f is equivalent to g if and only if there exists some matrix P with determinant 1 such that

$$G = P^T F P, \tag{2.4}$$

where F and G are their corresponding matrices. If $|P| = 1$, then f and g are properly equivalent.

It is obvious that this definition is equivalent to one given in class, since an integer linear transformation has integer inverse only if it's determinant is 1. We will now determine when a ternary quadratic form is positive definite.

Definition 2.4. The determinant of a quadratic form f is the determinant of its corresponding matrix A.

Note that the determinant is not the same as the determinant. In the case of a binary form, $disc(A) = -4\det(A)$. Since $h(-4) = 1$, if $|A| = 1$ for a 2×2 matrix A, then $|A|$ is properly equivalent to a sum of 2 squares.

Theorem 2.5. *A ternary quadratic form f represented by A is positive definite if and only if the following 3 properties hold:*
a) $a_{11} > 0$
b) $A_{33} > 0$
c) $\det(A) > 0$,
where A_{ij} is the i, j minor of A.

We need a lemma:

Lemma 2.6. *If f is a positive definite form represented by A, then*

$$a_{11}f(x,y,z) = (a_{11}x^2 + a_{12}y^2 + a_{13}z^2)^2 + g(y,z), \tag{2.5}$$

where

$$g(y,z) = \det(A_{33})y^2 + 2\det(A_{23})yz + \det(A_{22})z^2, \tag{2.6}$$

Furthermore, $\det(g) = a_{11}\det(f)$.

Proof. This is just computation, using the fact that A is symmetric. ■

Proof of Theorem 2.5. Let g be as in lemma 2.3. Then g is positive definite if and only if $\det(A_{33}) \geq 0$, and $\det(g) = a_{11}\det(f) \geq 0$. Thus we need to show that f is positive definite if and only if g is. Assume that g is not symmetric, so that there exists some s, t such that $g(s,g) \leq 0$. Then there exists some r such that $a_{11}r + a_{22}s + a_{33}t = 0$, so $f(r,s,t) = 0 + g(s,t) \leq 0$. Conversely, if f is not positive, then neither is g since $f(x,y,z) = (a_{11}x + a_{22}y + a_{33}z)^2 + g(y,z)$ and squares are always positive. ■

Similarly to binary forms, we can reduce positive definite ternary quadratic forms.

Theorem 2.7. *Every positive definite ternary quadratic form f with determinant D is equivalent to a form $h(x,y,z)$ represented by a matrix A satisfying the following properties:*
a) $0 < a_{11} < \frac{4}{3}\sqrt[3]{D}$
b) $2|a_{12}| \leq a_{11}$
c) $2|a_{13}| \leq a_{11}$

We will first need to prove a lemma:

Lemma 2.8. *Let C be a matrix with* $\gcd(c_{11}, c_{12}, c_{13}) = 1$. *Then the remaining entries of the matrix can be chosen such that* $\det(C) = 1$.

Proof. Let $g = \gcd(c_{11}, c_{21})$. Then there exist integers c_{12}, c_{22}, u, v such that $c_{11}c_{22} - c_{21}c_{12} = g$ and $gu - c_{31}v = 1$, since $\gcd(g, c_{31}) = 1$. Then

$$\begin{vmatrix} c_{11} & c_{12} & \frac{c_{11}v}{g} \\ c_{21} & c_{22} & \frac{c_{21}v}{g} \\ c_{31} & 0 & u \end{vmatrix} = \frac{c_{31}v}{g}(c_{21}c_{12} - c_{11}c_{22}) + u(c_{11}c_{22} - c_{21}c_{12}) = -c_{31}v + gu = 1.$$

■

Now we can prove Theorem 2.4.

Proof of Theorem 2.7. Let a_{11} be the smallest number represented by f. We will first transform f with a coprime matrix C, satisfying $\det(C) = 1$ (So that C has an integer inverse) into a new form g such that the x^2 coefficient of g is a_{11}. Say that $f(c_{11}, c_{21}, c_{31}) = a_{11}$. Then $\gcd(c_{11}, c_{21}, c_{31}) = 1$ by the minimality of a_{11}, so we can choose the 6 other entries of the matrix $C = (c_{ij})$ such that $\det(C) = 1$. Now we will transform g with a matrix

$$N = \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & u & w \end{pmatrix} \tag{2.7}$$

where $\begin{vmatrix} t & u \\ u & v \end{vmatrix} = 1$, so that $\det(N) = 1$. Let $h(x) = f(N(x,y,z))$. Then

$$h(1,0,0) = g(1,0,0) \tag{2.8}$$

so we can let the matrix representing h be $A = (a_{ij})$. We make the substitution

$$\begin{pmatrix} x' & y' & z' \end{pmatrix}^T = N \begin{pmatrix} x & y & z \end{pmatrix}^T, \tag{2.9}$$

so that $g(x', y', z') = h(x, y, z)$. Using the formula for $N = (a_{ij})$,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ r & t & v \\ u & s & w \end{pmatrix} \begin{pmatrix} a_{11} & b_{12} & b_{13} \\ b_{12} & b_{22} & b_{23} \\ b_{13} & b_{23} & b_{33} \end{pmatrix} \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix}. \tag{2.10}$$

Expanding the top row, we get that

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \end{pmatrix} = \begin{pmatrix} a_{11} & b_{12} & b_{13} \end{pmatrix} \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix}.$$

Thus,

$$\begin{pmatrix} a_{11} & b_{12} & b_{13} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_{11} & b_{12} & b_{13} \end{pmatrix} \begin{pmatrix} 1 & r & s \\ 0 & t & u \\ 0 & v & w \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}. \tag{2.11}$$

Using (4), we get that,

(2.12)

$$0 = g(x', y', z') - h(x, y, z) = (a_{11}x' + b_{12}y' + b_{13}z')^2 - (a_{11}x + a_{12}y + a_{13}z)^2 + k(y', z') - l(y, z),$$

where k and l are positive definite binary quadratic forms. Thus $k(y', z') = l(y, z)$, so N transforms l to k. Since t, u, v, w are unspecified, we can choose them such that N transforms l to a reduced binary form.

Since r is arbitrary, the only constraint on the value of

$$a_{12} = a_{11}r + b_{12}t + b_{13}v \tag{2.13}$$

is that $a_{12} \equiv b_{12}t + b_{12}v \pmod{a_{11}}$. Thus r can be chosen such that $2|a_{12}| \leq a_{11}$. Similarly, s can be chosen such that $2|a_{13}| \leq a_{11}$.

The x^2 coefficient of l is $-4|A_{33}|$, so

$$a_{12}a_{13} - a_{22}^2 \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}\det(h)}. \tag{2.14}$$

From this,

$$a_{11}^2 \leq a_{11}a_{22} - a_{12}^2 + a_{12}^2 \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}\det(h)} + \frac{a_{11}^2}{4}. \tag{2.15}$$

Rearranging gives

$$a_{11} \leq \frac{4}{3}\sqrt[3]{\det(h)}, \tag{2.16}$$

as desired. ■

The following theorem is the reason for this section.

Theorem 2.9. *Every positive definite binary form with determinant* 1 *is properly equivalent to a sum of* 3 *squares.*

Proof. By Theorem 2.4, any form with determinant 1 is equivalent to a form f with matrix A satisfying the following:

$$0 \leq a_{11}, 2a_{12} \leq a_{11}, 2a_{13} \leq a_{11}. \tag{2.17}$$

Thus $a_{11} = 0$ and $a_{12} = a_{13} = 0$. By the formula given in Lemma 2.3, $f(x, y, z) = x^2 + g(y, z)$, where $\det(g) = 1$. Every positive definite binary form with determinant 1 is equivalent to a sum of 2 squares since $h(-4) = 1$, so f is equivalent to a sum of 3 squares. ■

We are now ready to prove Legendre's 3 square theorem.

3. Proof of Legendre's 3 Squares Theorem

Proof of Theorem 1.3. We will first show that no integer of form $4^a(8b + 7)$ is a sum of 3 squares. Since the squares modulo 0 are $0, 1, 4$, 3 squares cannot sum to 7 mod 8, no number $8b+7$ is a sum of 3 squares. Now we can induct on a, since $x^2 + y^2 + z^2 \equiv 0 \pmod 4$ implies that x, y, z are even.

For all other integers, we will explicitly find a positive definite ternary form with determinant 1 that represents n for any $n \not\equiv 7 \pmod 8$. Let f be a ternary quadratic form with matrix

$$\begin{pmatrix} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 1 \\ 1 & 0 & n \end{pmatrix}, \tag{3.1}$$

where a_{11}, a_{12}, a_{22} are integers to be determined. Then $f(0, 0, 1) = n$, so f represents n. Let $b = a_{11}a_{22} - a_{12}^2$, so that $\det(f) = bn - a_{22}$. The conditions of theorem 2.2 become that

$$a_{11} > 0, b > 0, a_{22} = bn - 1. \tag{3.2}$$

The case $n = 1$ is obvious, so assume $n > 1$. Then the last 2 conditions imply the first, since the last condition gives that $a_{22} > 0$ and the second condition gives that

$$a_{11} = \frac{b + a_{12}^2}{a_{22}} > 0. \tag{3.3}$$

This also implies that we need to find a b such that $-b$ is a quadratic residue modulo $bn - 1$ in order to prove that some a_{11}, a_{12}, a_{22} exist.

First assume n is even. We can assume that $n \not\equiv 0 \pmod 4$ since we can then divide by 4. Then $4n$ and $n - 1$ are coprime, so there exists some m such that

$$p = 4bm + n - 1 \tag{3.4}$$

is prime. Then $p = bn - 1$ if we let $b = 4m + 1$. Since $b = p = 1 \pmod 4$, quadratic reciprocity gives that

$$\left(\frac{-b}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{bn-1}{b}\right) = \left(\frac{-1}{b}\right) = 1. \tag{3.5}$$

Now assume n is odd, so that $n = 1, 3, 5 \pmod 8$. Let c be the smallest positive integer such that $cn \equiv 3 \pmod 4$. Then $\gcd(4n, \frac{cn-1}{2}) = 1$, so there exists some m such that

$$p = 4nm + \frac{cn - 1}{2} \tag{3.6}$$

is prime. If we let $b = 8m + c$, then $2p = bn - 1$. Thus we need to have $-b$ to be a residue modulo 2 and p. We already know $-b$ is a residue modulo 2 since it is odd. Thus we need to prove that

$$\left(\frac{-b}{p}\right) = 1. \tag{3.7}$$

By casework on the value of $n \pmod 8$, we see that

$$\left(\frac{-b}{p}\right) = \left(\frac{p}{b}\right). \tag{3.8}$$

Note that

$$\left(\frac{-2p}{b}\right) = \left(\frac{1-bn}{b}\right) = 1. \tag{3.9}$$

Thus we need to show that

$$\left(\frac{-2}{b}\right) \equiv 1, \tag{3.10}$$

which follows by casework. ■

4. Diagonal Quadratic Forms

We are now ready to find all universal diagonal quadratic forms. The following proof was discovered by Ramanujan.

Theorem 4.1. *There are exactly* 55 *positive definite quaternary diagonal quadratic forms, down to proper equivalence. These are:*
1) $x^2 + y^2 + z^2 + du^2$ *with* $1 \le d \le 7$,
2) $x^2 + y^2 + 2z^2 + du^2$ *with* $2 \le d \le 14$,
3) $x^2 + y^2 + 3z^2 + du^2$ *with* $3 \le d \le 6$,
4) $x^2 + 2y^2 + 2z^2 + du^2$ *with* $2 \le d \le 7$,
5) $x^2 + 2y^2 + 3z^2 + du^2$ *with* $3 \le d \le 10$,
6) $x^2 + 2y^2 + 4z^2 + du^2$ *with* $4 \le d \le 14$ *and*
7) $x^2 + 2y^2 + 5z^2 + du^2$ *with* $5 \le d \le 10$.

Proof. We will first prove that these are the only possible forms. Let $f(x, y, z, w) = ax^2 + by^2 + cz^2 + du^2$ be a universal diagonal form. We may assume that $a \le b \le c \le d$ because we only care about the equivalence class of f. Then $a = 1$, since f needs to represent 1. $1 \le b \le 2$, since f needs to represent 2. There are now 2 cases depending on the choices for a and b. If $a = b = 1$, then $1 \le c \le 3$, since 3 must be represented. If $a = 1, b = 2$, then $3 \le c \le 5$, since 5 needs to be represented. Considering each of the 7 cases separately, we find the bounds for d.

We now require a lemma:

Lemma 4.2. *The following forms represent the following integers.*
a) $x^2 + y^2 + 2z^2$ *represents all integers not of form* $4^a(16b + 14)$.
b) $x^2 + y^2 + 3z^2$ *represents all integers not of form* $9^a(9b + 6)$.
c) $x^2 + 2y^2 + 2z^2$ *represents all integers not of form* $4^a(8b + 7)$.
d) $x^2 + 2y^2 + 3z^2$ *represents all integers not of form* $4^a(16b + 10)$.
e) $x^2 + 2y^2 + 4z^2$ *represents all integers not of form* $4^a(16b + 14)$.

f) $x^2 + 2y^2 + 5z^2$ *represents all integers not of form* $25^a(25b + 10)$ *or* $25^a(25b + 15)$.

Proof. Most of these can be proved similarly to Theorem 3.1, although the proof is harder since the forms are not the only form in their class group down to proper equivalence.

However, a), c), and e) can be easily proven. Let $f(x, y, z) = x^2 + y^2 + 2z^2$. If $2n = x^2 + y^2 + 2z^2$, then $x \equiv y \pmod 2$, so there exists some x', x' such that $x = x' + y'$ and $y = x' - y'$. Then $n = x'^2 + y'^2 + z^2$, so f cannot represent any integer of form $4^a(16b + 14)$. Conversely, if $n = x'^2 + y'^2 + z^2$, then $2n = (x' + y')^2 + (x' - y')^2 + 2z^2$, so all other even integers are represented by f. In particular, f represents all integers of the form $4n + 2$. Say that $4n + 2 = x^2 + y^2 + 2z^2$. Considering the previous modulo 4, we see that x, y are odd, while z is even. Say that $x' + y' = x$, $x' - y' = y$, and $z = 2z'$. Then $2n + 1 = x'^2 + y'^2 + 2z'^2$. Thus f represents all odd integers, so the only integers not represented are those of form $4^a(16b + 14)$. Cases c) and e) are proved similarly. ∎

We will now prove all forms in a) are universal. Again, the other cases are proved similarly. If $n \neq 4^a(8b + 7)$ for any a, b, then we can represent n with $w = 0$. Assume $n = 4^a(8b + 7)$. Then if we let $w = 2^a$, we get that $4^a(8b + 7 - d)$ must be a sum of 2 squares, which is true unless $d = 3$ or $d = 7$. If $d = 3$ and $b = 0$, then setting $w = 2^a$ gives that 4^{a+1} must be a sum of 3 squares, which is true. If $d = 3$ and $b > 0$, then setting $w = 2^{a+1}$ gives that $4^a(8b - 5)$ must be a sum of 3 squares, which is also true. Similarly, if $d = 7$, we can set $w = 2^{a+1}$ if $b > 2$ and 2^a if $b \leq 2$. ∎

5. The 15 And 290 Theorems

There is actually a general way to check if a quadratic form is universal. Conway proved the following theorem, which provides an easy way to check if an integral form is universal.

Theorem 5.1 (Conway)**.** *A positive definite form with integer matrix is universal if and only if it represents all integers less than or equal to* 15*.*

Bhargava generalized this to all integral quadratic forms.

Theorem 5.2 (Bhargava)**.** *A positive definite integral quadratic form represents all integers if and only if it represents all integers less than or equal to* 290*.*

These theorems give us an easy way to check if a form is universal: just check if it represents all numbers up to 15 or 290. This was used to find all universal quaternary quadratic forms.