Rose-Hulman Undergraduate Mathematics Journal

Volume 17
Issue 1

Article 1

Unique minimal forcing sets and forced representation of integers by quadratic forms

Tahseen Rabbani
University of Virginia

Rose-Hulman Undergraduate Mathematics Journal

Unique minimal forcing sets and forced representation of integers by quadratic forms

Tahseen Rabbani[a]

Volume 17, No. 1, Spring 2016

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]University of Virginia

Rose-Hulman Undergraduate Mathematics Journal
Volume 17, No. 1, Spring 2016

Unique minimal forcing sets and forced representation of integers by quadratic forms

Tahseen Rabbani

Abstract. For $S, W \subseteq \mathbb{N}$, we say S forces W, denoted $S \rightarrowtail W$, if any integer-matrix positive definite form which represents every element of S over $\mathbb{Z}$ also represents every element of W over $\mathbb{Z}$. In the context of a superset S^*, S is referred to as a unique minimal forcing set of W if for any $S_0 \subseteq S^*$ we have that $S_0 \rightarrowtail W$ if and only if $S \subseteq S_0$. In 2000, Manjul Bhargava used his own novel method of "escalators" to prove the unique minimal forcing set of $\mathbb{N}$ is $T = \{1, 2, 3, 5, 6, 7, 10, 14, 15\}$, which was a refinement of the celebrated Conway-Schneeberger Fifteen Theorem. We use Bhargava's theory of escalators to develop an algorithm which determines whether a positive integer, interpreted as a singleton in $\mathbb{N}$, has a unique minimal forcing set within T and to establish several infinite families of positive integers without unique minimal forcing sets in T.

Acknowledgements: I thank my advisor, Dr. Andrew Obus, for guiding me through all the necessary background theory and posing questions which provided the framework for my research. A great deal of gratitude is also due towards Dr. Chris Laumann for graciously providing a Magma program which was used for the bulk of escalator calculations presented in this paper.

1 Introduction

Representation of integers by quadratic forms is a well-studied topic which extends back several centuries. Informally, a quadratic form is a polynomial with only degree-two terms. Among the more famous results is Lagrange's Four Squares Theorem, which states that any positive integer can be represented by the form $x^2 + y^2 + z^2 + w^2$ over the integers, $\mathbb{Z}$, that is, using integral inputs. Fermat's theorem on sums of two squares, which states that an odd prime p is representable by $x^2 + y^2$ over $\mathbb{Z}$ if and only if $p \equiv 1 \mod 4$, is also a well-known result which is often covered in elementary number theory courses.

It is not always feasible to provide a complete characterization of the integers a given quadratic form can represent over $\mathbb{Z}$. However, given a subset of integers the form is known to represent, it is often possible to deduce what other integers it will be forced to represent. We shall focus our attention on a special class of quadratic forms known as integer-matrix positive definite forms. If every one of these forms which represents all the elements of some $S \subseteq \mathbb{Z}$ also represents every element of some $W \subseteq \mathbb{Z}$, then we say S forces W, or that S is a forcing set of W.

By studying subsets represented by a form in the context of forcing, we can drastically reduce the complexity of determining what other integers the form must represent. For example, the representation of positive integers up to 15 forces representation of all positive integers [1], a result known as the Conway-Schneeberger 15 Theorem. Also, Manjul Bhargava determined that $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$ is a forcing set of all primes and that $\{1, 3, 5, 7, 11, 15, 33\}$ is a forcing set of all positive odd integers (although both of these results extend to a class of forms wider than just integer-matrix positive definite) [7].

This paper is designed to fluidly build appropriate background knowledge of quadratic forms, culminating in a discussion of forcing sets, although the reader is expected to be familiar with abstract algebra, elementary number theory, and p-adic numbers. Sections 2 and 3 introduce fundamental properties of quadratic forms and theorems relating to integer representation. In Sections 4.1-4.2, we present an introduction to Manjul Bhargava's theory of escalators, followed by an algorithm which will determine whether an integer has a unique minimal forcing set using the escalation method. The final section, 4.3, establishes several results on infinite families of positive integers without unique minimal forcing sets.

Much of this paper uses terminology and notation unique to J.H. Conway's works [3] [4], so for further work, it is encouraged that the reader additionally consult the texts of T.Y. Lam [8] and O. Timothy O'Meara [9] for alternative and more standard descriptions of quadratic form theory.

2 A First Definition of Quadratic Forms

In this section, we will define and discuss the connection between quadratic forms and lattices. Let R be a ring (respectively K, a field) not of characteristic 2. A **quadratic form** over R or K is a homogeneous polynomial of degree 2 in any number of variables. Throughout this paper, we shall use "quadratic form" and "form" interchangeably. For a quadratic form

$$f(x_1, x_2, \dots, x_n) = \sum_{1\le i\le j\le n} a_{ij}x_ix_j,$$

by letting $x = [x_1\ x_2 \dots\ x_n]$, we may represent f as xM_fx^T where M_f is the $n \times n$ symmetric matrix given by

$$M_f(i,j) = \begin{cases} a_{ii} & i = j \\ \frac{1}{2}a_{ij} & i < j \end{cases}$$

For example, the form $f = x_1^2 + 3x_2^2 + 2x_1x_2$ is associated with the matrix $\begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix}$. If the polynomial representation of a form has only integer coefficients then it is referred to as an **integral form**. If $a_{ij} = 0$ for $i \neq j$, then f is referred to as a diagonal form and expressed as

$$[a_{11},\ a_{22},\ a_{33},\ \dots\ ,\ a_{nn}].$$

The determinant of f, denoted by $\det(f)$, refers to the determinant of the matrix associated with f.

Let f be a quadratic form with coefficients in a ring R. We refer to an element of $r \in R$ as **representable** if there exists $v \in R^n$ such that $f(v) = r$.

If the associated matrix of a form contains only integer entries, then it is referred to as an **integer-matrix** form. Relating back to the polynomial representation, a form f is integer-matrix if and only if the a_{ii} are integers and a_{ij} is even for $i \neq j$. For a ring $R \subseteq \mathbb{R}$, a form f is **positive definite** if for all $v \neq 0$, where $v \in R^n$, $f(v) > 0$. The matrix of a positive definite form will have only positive eigenvalues. Integer-matrix positive definite forms will be the primary focus of this paper.

A **lattice** L is a group isomorphic to $(\mathbb{Z}^n, +)$ with an inner product $\langle\cdot,\cdot\rangle$. A subgroup of L is referred to as a sublattice (L is respectively referred to as the **superlattice** of the subgroup). A quadratic form f over $\mathbb{Z}$ in n variables with matrix M_f may be interpreted as the lattice $(\mathbb{Z}^n, +)$ with inner product $\langle x, y\rangle = xM_fy^T$ for $x,\ y \in \mathbb{Z}^n$. The length or **norm** of a vector x is the inner product of x with itself. Hence, this lattice contains vectors of squared lengths equivalent to the integers represented by f. Henceforth, quadratic forms and their associated matrices will often be referred to as lattices.

3 Integral Representation

Classifying the set of integers represented by a quadratic form is a process with no general optimial strategy, but studying representation over the p-adics often proves to be illuminating.

3.1 Equivalence

It is possible for a quadratic form to be represented in more than one way, so we must define an equivalence class of some sort for differing representations. For an arbitrary ring R, we say two quadratic f and g forms over R of the same dimension (number of variables) are **R-equivalent** (for lattices, **R-isometric**) if there exists some invertible linear change of variables that transforms either form into the other. In other words, if M_f and M_g are the matrices of f and g respectively, then f and g are R-equivalent if and only if there exists some invertible R-matrix A such that $AM_fA^T = M_g$. For example, $p(x, y) = x^2 + y^2$ is $\mathbb{Z}$-equivalent to $q(s, t) = 5s^2 + 6st + 2t^2$ (also called integral equivalence), since

$$p(s + t, 2s + t) = s^2 + 2st + 2t^2 + 4s^2 + 4st + t^2 = g(s, t)$$

and

$$q(x-y, 2y-x) = 5x^2 - 10xy + 5y^2 - 6x^2 + 18xy - 12y^2 + 8y^2 - 8xy + 2x^2 = x^2 + y^2 = f(x, y).$$

In terms of matrices, we have that $M_p = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_q = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$, $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$, and $AM_pA^T = M_q$. More specifically, f and g are integrally equivalent if and only if there exists some integer matrix A such that $AM_fA^T = M_g$ and $\det(A) = \pm 1$.

If f is an integral form, several types of elementary manipulations will give rise to an integrally equivalent form. The rearrangement of variables trivially gives rise to equivalent forms. If M_f is the matrix of f, any integral multiple of a row may be added to another, as long as the transpose operation is also performed, to produce an integrally equivalent form. That is, if a multiple of the i^{th} row is added to the j^{th} row, then the same multiple of the i^{th} column must be added to the j^{th} column. Generalizing to an arbitrary ring R, we define **permissible** operations on the matrix M of a quadratic form over R as those which give rise to equivalent forms. In particular, any permissible operation may be represented as a conjugation of M by some invertible R-matrix A and its transpose, that is, AMA^T. We say a property is **invariant** if it is preserved over equivalent forms, with respect to a ring.

3.2 Genus and p-adic symbols

We will now consider equivalence over $\mathbb{Z}_p$, the p-adic integers, including $\mathbb{Z}_\infty = \mathbb{R}$, which is referred to as **p-adic equivalence**. The bulk of the machinery used in the next three sections is derived from Conway and Sloane's *Sphere Packings, Lattices, and Groups* [4, §15]. Results not otherwise cited may be found there. The reader is also encouraged to see Conway and Fung's *The Sensual (Quadratic) Form* [3], pp. 91-115, for a less rigorous treatment of these topics in the same language presented.

We first introduce the direct sum notation $\oplus$. The direct sum of two forms $f \oplus g$ corresponds to the form with matrix $\begin{bmatrix} M_f & 0 \\ 0 & M_g \end{bmatrix}$, where M_f, M_g are the matrices of f and g, respectively.

To determine whether two forms are p-adically equivalent, one only needs to calculate their **p-adic symbols**, which are invariant for p-adically equivalent forms. Let M be the matrix of a quadratic form over $\mathbb{Z}$. In Conway and Sloane's aforementioned text [4], pp. 369-370, it is demonstrated that M is diagonalizable over $\mathbb{Z}_p$ for $p \neq 2$ using the permissible operations described at the end of section 3.1.

Let N be the diagonalization of M over $\mathbb{R}$. Then the -1-adic symbol of M is expressed as $(+)^{n_+}(-)^{n_-}$, where n_+ and n_- are respectively the number of positive and negative entries along the diagonal of N.

For $p \neq -1, 2$, M may be p-adically diagonalized to the shape

$$[a, b, c, \dots, pa', pb', \dots, p^2 a'', \dots, \dots]$$

where $a, b, c, \dots, a', b', c', \dots, a'', b'', \dots$ are relatively prime to p. The diagonal forms

$$\begin{aligned} f_1 &= [a, b, c, \dots], \\ f_p &= [a', b', c', \dots], \\ f_{p^2} &= [a'', b'', c'', \dots], \\ &\dots \end{aligned}$$

are referred to as the Jordan constituents of f and the expression

$$f_1 \oplus p f_p \oplus p^2 f_{p^2} \oplus \cdots \oplus p^r f_{p^r} \oplus \cdots$$

is referred to as the **Jordan decomposition** of f. The determinant of each f_{p_i} is a p-adic unit, meaning its determinant, the product of all entries, is not divisible by p. The p-adic symbol is then expressed as

$$1^{\pm n_0} p^{\pm n_1} p^{2^{\pm n_2}} \cdots p^{r^{\pm n_r}} \cdots$$

where n_i is the dimension of f_{p^i}, and the sign is the value of the Legendre symbol $(\frac{\det(f_q)}{p})$. For example, to compute the 5-adic symbol of the diagonal form $[1, 2, 3, 5, 10, 25]$, we first decompose it into the constitutents $f_1 = [1, 2, 3]$, $f_5 = [1, 2]$, $f_{25} = [1]$, resulting in the symbol $1^{+3}5^{-2}25^{+1}$.

The 2-adic symbol is calculated in a different manner since not every form may be diagonalized over the 2-adics. In any case, there is a method by which to produce a Jordan decomposition of 2-adic unit forms, which is not explained in this paper. See Conway and Sloane's aforementioned text [4], pp. 380-383 for an explanation.

Although not shown here, the p-adic symbol is an invariant property over $\mathbb{Z}_p$, and it exactly characterizes p-adic equivalence. For p not dividing $2\det(f)$, the p-adic symbol is equivalent to $1^{\pm \dim(f)}$, so this allows us to easily compare the p-adic symbols between two forms. We say a collection of integral quadratic forms are within the same **genus** if they are p-adically equivalent for every p. Therefore, we have the following:

Theorem 3.1 *Two integral quadratic forms f and g are in the same genus if and only if they have the same p-adic symbols for every p.*

Consequently, a genus may be denoted by the p-adic symbols shared by every form within the genus.

3.3 Global Relation

We will now look at forms which satisfy the **global relation**. As we will see in the next section, the notions of genus and the global relation play an important role in integral representation. Consider the prime factorization of an integer n (including $p = -1$). Define the p**-part** of n as the maximal p power contained as a factor. For example, the 5-part of 50 is 25 since $50 = 5^2 \cdot 2$. Let $n = p^r a$, where a is coprime to p. We refer to n as a p-adic antisquare if r is odd and a is not a quadratic residue modulo p.

Let f be a diagonal form. For $p \neq -1, 2$, the p**-signature** of f, denoted $\sigma_p(f)$, is the sum of the p-parts in every entry and the addition of 4 for each antisquare, taken modulo 8. The -1- signature is calculated by adding 1 for every positive entry and -1 for every negative entry, but not taken modulo 8 this time. The 2-signature is the sum of the odd parts of every entry and an additional 4 for every entry of the form $2^r(8k \pm 3)$ for r odd (referred to as 2-adic antisquares), taken modulo 8. For p not dividing $2\det(f)$, we have $\sigma_p(f) \equiv \dim(f)$ mod 8.

For example, the 3-signature of $[10, 9, -3]$ is $1 + 9 + 3 + 4 \equiv 1 \mod 8$, since -3 is an antisquare. The 2- signature is $5 + 9 + (-3) + 4 \equiv 15 \mod 8$, since 10 is a 2-adic antisquare. The -1-signature is $1 + 1 + (-1) = 1$.

For a p-adically diagonalized diagonal form f, we define the p**-excesses** $e_p(f)$ as

$$\begin{aligned} e_p(f) &= \sigma_p(f) - \dim(f) \qquad \text{if } p \neq 2 \\ e_2(f) &= \dim(f) - \sigma_2(f). \end{aligned}$$

A form f satisfies the **global relation** if the sum of its p-excesses for every prime p is a multiple of 8.

Conveniently enough, for p odd, the p-adic symbol of a form also encodes the value of its p-signature and p-excess. Let $1^{\pm n_0} p^{\pm n_1} \cdots q^{\pm n_r} \cdots$ be the p-adic symbol of f, then

$$\sigma_p(f) = \sum p^i n_i + 4k \mod 8$$

where $k = 1$ if the number of negative exponents for odd powers of p is odd and $k = 0$ if this number is even. It is clear then that the p-excess may be obtained as well. We have a similar encoding in the 2-adic symbol, but this will not be demonstrated – once again, we encourage the reader to see Conway and Sloane's text [4]. Thus, if we are given an arbitrary p-adic symbol, we may determine if forms contained in the genus denoted by this symbol satisfy the global relation.

3.4 Local versus Global Representation

In this section, we will establish a powerful theorem about genuses containing a form which satisfies the global relation. Representation of an integer over $\mathbb{Z}_p$, for a particular prime p, will be referred to as **local representation**. The strong Hasse-Minkowski theorem asserts that a rational form f represents a rational number q over $\mathbb{Q}$ if and only if f represents q

over $\mathbb{Q}_p$ for all p. Unfortunately, we are not always afforded the same relation between $\mathbb{Z}$ and $\mathbb{Z}_p$, although representation over $\mathbb{Z}_p$ can relay a great deal of information, as demonstrated by the following theorem.

Theorem 3.2 *Given a genus G with a p-adic symbol that satisfies the global relation,*

1. *There exists an integral form in G.*
2. *If some form $f \in G$ represents a positive integer n over $\mathbb{Z}_p$ for all p, then at least one integral form $f' \in G$ represents n over $\mathbb{Z}$.*

If a genus contains only one form up to integral equivalence, we refer to such a form as **class number one**. There is an obvious consequence of Theorem 3.2 for class number one forms which satisfy the global relation:

Corollary 3.3 *If a class number one form represents a positive integer n over $\mathbb{Z}_p$ for all p, then it represents n over $\mathbb{Z}$.*

It is convenient to test local representation over $\mathbb{Q}_p$ modulo squares, that is, to check whether square classes in $(\mathbb{Q}_p^\times)/(\mathbb{Q}_p^\times)^2$ are represented, where $\mathbb{Q}_p^\times$ denotes the multiplicative group. For an odd prime p, let $p^e u_+$ and $p^e u_-$ denote the product of an even power of p with a quadratic residue and nonresidue modulo p, and $p^e u_+$ and $p^e u_-$ denote the same except for an odd power of p. Let $2^e u_i$ and $2^d u_i$ respectively denote product of an even and odd power of 2 with u_i congruent i modulo 8. Then we have the following:

Proposition 3.4 *The congruence classes of $(\mathbb{Q}_p^\times)/(\mathbb{Q}_p^\times)^2$ consist of $p^e u_+$, $p^d u_+$, $p^e u_-$, and $p^d u_-$.*

Proposition 3.5 *The congruence classes of $(\mathbb{Q}_2^\times)/(\mathbb{Q}_2^\times)^2$ consist of $2^e u_1$, $2^e u_3$, $2^e u_5$, $2^e u_7$, $2^d u_1$, $2^d u_3$, $2^d u_5$, and $2^d u_7$.*

Furthermore, the following lemma reduces the process of characterization considerably.

Lemma 3.6 *If a form f fails to locally represent a p-adic integer, then $p \mid 2\det(f)$.*

There are several methods by which to characterize integers represented by a form which is not class number one, such as searching for a class number one sublattice. There are also **regular** forms which are not class number one, but which represent every integer locally represented by the genus, hence finding an embedding of a regular form can be just as useful as finding a class number one form. See Jagy, Kaplansky, and Schiemann's paper "There are 913 regular ternary forms" for a classification of ternary (3 variable) regular forms [5].

4 Forcing Sets

Using the techniques and theorems we have learned in the previous sections, we are finally prepared to discuss **forcing sets**. In these remaining sections, we will assume representation by quadratic forms to be over $\mathbb{Z}$. In 1993, Conway and W.A. Schneeberger presented an important result on quadratic forms which represent every positive integer.

Theorem 4.1 (The Fifteen Theorem) *If an integer-matrix positive definite quadratic form represents every positive integer up to 15 then it represents every positive integer.*

The original proof was never published due to its length and complexity, but in 2000 M. Bhargava provided an elegant proof using the novel method of **escalators**. Bhargava was also able to refine the Fifteen Theorem.

Theorem 4.2 *If an integer-matrix positive definite quadratic form represents 1, 2, 3, 5, 6, 7, 10, 14, and 15, then it represents every positive integer.*

For the proof of the above theorem and a detailed description of escalation, see Bhargava's paper, "On the Conway-Schneeberger Fifteen Theorem. [1]"

4.1 Escalators

Let $S = \{a_1, a_2, a_3, \dots\}$ be a possibly infinite set of positive integers ordered from least to greatest. We will construct the set of integer-matrix positive definite forms which represent every element S, termed S-universal, up to equivalence over $\mathbb{Z}$ using a technique established by Bhargava known as **escalation**.

Formally, we begin with the zero-dimensional lattice $[0]$. We define the S-**truant** of a lattice L to be the first element of S not represented by L. For brevity, we will just say truant when the set in question is apparent. The truant of the zero-dimensional lattice is a_1. An **escalation** of L is a superlattice generated by L and a vector with norm equal to the truant. So, we escalate the zero-dimensional lattice and obtain $L_1 = [a_1]$, which is referred to as the 1-dimensional escalator. The 1-dimensional escalator is unique. If $L_1 = [a_1]$ has no truant, then it is S-**universal**. Otherwise let a_{i_1} be the truant of L_1. The escalations of L_1 consist of the lattices with integer matrix of the form $\begin{bmatrix} a_1 & b \\ b & a_{i_1} \end{bmatrix}$ which have only positive eigenvalues. These lattices are referred to as the 2-dimensional escalators. If any particular lattice $\begin{bmatrix} a_1 & b_1 \\ b_1 & a_{i_1} \end{bmatrix}$ has truant a_{i_2}, escalations of L_2 will appear as integerl matrices of the form $\begin{bmatrix} a_1 & b_1 & c \\ b_1 & a_{i_1} & d \\ c & d & a_{i_2} \end{bmatrix}$ with strictly positive eigenvalues. The set of all escalations of 2-dimensional escalators with truants constitute the 3-dimensional escalators. This process of escalation is continued until a complete set of S-universal nonisometric lattices is constructed. Any lattice obtained by escalation on S is referred to as an **escalator lattice**.

If $S = \{1, 3, 7\}$, we find the set of S-universal S-escalator lattices. The 1-dimensional lattice is $[1]$, which corresponds to the form x^2. The truant of this form is 3, so we escalate, and our 2-dimensional escalators are $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$. It is imporant to reiterate that we are determining escalators up to integral equivalence, so while $\begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix}$ is a valid escalator, it is $\mathbb{Z}$-equivalent to the first lattice. The truant of the first lattice is 7 while the second is universal. The 3-dimensional escalators are the following:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 7 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 7 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

The 3-dimensional escalators together with $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$ make up the $\{1, 3, 7\}$-universal escalator lattices.

Bhargava proved the modified version of the 15-theorem by attempting to produce the set of escalator lattices representing $\mathbb{N}$ and found that the only truants which appeared were $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$. As an algorithmic consideration it is worth noting that for any set of positive integers, even one which is infinite, the set of escalator lattices may be determined in a finite number of steps. In fact, for a given set of positive integers, there is no non-universal escalator of dimension greater than 7. See Bhargava and Hanke's "Universal quadratic forms and the 290-theorem" for a detailed proof [2].

4.2 Forced Representation

Henceforth, we may interpret representation of a set to mean representation of every element within the set. For S, $W \subset \mathbb{N}$, we say W is **forced** by S, denoted $S \rightarrowtail W$, if any integer-matrix positive definite form which represents S also represents every element of W. This is as simple as determining whether every S-universal escalator lattice also represents W. If a non-S-universal escalator represents W, then so do all escalations coming from it, so we need not check these escalators in order to confirm whether $S \rightarrowtail W$. We may also study whether a set force a positive integer n, denoted $S \rightarrowtail n$, by interpreting n as a singleton in $\mathbb{N}$.

In the context of a superset S^*, if a particular subset $S \subseteq S^*$ forces W and no proper subset of S forces W, we say S is a **minimal forcing set** of W in S^*. For any given subset $S_0 \subseteq S^*$, we have $S_0 \rightarrowtail W$ if and only if $S \subseteq S_0$, then S is referred to as a **unique minimal forcing set** of W in S^*.

Now, we present an algorithm which determines whether a positive integer n has a unique minimal forcing set within $T = \{1, 2, 3, 5, 6, 7, 10, 14, 15\}$, which is Bhargava's unique minimal forcing set of $\mathbb{N}$:

1. Check if $\{1\}$ forces n, which will only occur if n is a square. If this is not the case, use escalation to check if $\{1, 2\}$ forces n. If this fails, check $\{1, 2, 3\}$, $\{1, 2, 3, 5\}$, and so on until a subset (in sequential order) of T forces n. Such a subset must exist by the

Fifteen Theorem. Let T_1 be this subset ordered from least to greatest. If $T_1 = \{1\}$ then this is a minimal forcing set, so denote it as T_{min} and proceed to step 3. Otherwise, proceed to Step 2.

2. Let $T_1 = \{a_1, a_2, \ldots, a_l\}$. This is a labeling for convenience since we know, in fact, $T_1 = \{1, 2, 3, 5, 6, \ldots, t\}$, where $t \leq 15$. Use the method of escalators to check if $T_1 \setminus \{a_{l-1}\}$ forces n. If so, replace T_1 by $T_1 \setminus \{a_{l-1}\}$. Then check if $T_1 \setminus \{a_{l-2}\}$ forces n. If so, replace T_1 by $T_1 \setminus \{a_{l-2}\}$. Continue this process all the way down through a_1, and denote the maximally sieved version of T_1 as T_{min}. This is a candidate for a unique minimal forcing set. Also note that if the process of singular removal fails to force n for every a_i, $1 \leq i \leq l-1$, then the original T_1 is already minimal. In any case, proceed to Step 3.

3. For each $c_i \in T_{min}$, check if $T \setminus \{c_i\}$ forces n. If any removal forces n, then n has no unique minimal forcing set. If every singular removal fails to force n, we have that T_{min} must be entirely contained in a subset of T to force n, proving it is a unique minimal forcing set of n in T. Proceed to Step 4 if n does not have a unique minimal forcing set, but a calculation of all minimal sets forcing n is desired.

4. Let T^* be the collection of sets $T \setminus c_i$ which force n, where $c_i \in T_{min}$. For each set of T^*, remove elements in descending order, and continually sieve through progressively smaller subsets using the process described in Step 2 until a minimal set is acquired. These minimal subsets along with T_{min} make up the minimal forcing sets of n in T.

As an example, we will perform the process on the number 11 to determine if it has a unique minimal forcing set in T. If a truant is mentioned, we mean a T-truant.

We begin with [1], which clearly fails to represent 11. The truant of this form is 2, so we escalate, and our 2-dimensional escalators are $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ and $\begin{bmatrix}1 & 0\\0 & 2\end{bmatrix}$. The first lattice fails to represent 11, while the second does. So we escalate the first lattice by its truant 3 to obtain,

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

All 3 of these lattices represent 11, thus $T_1 = \{1, 2, 3\}$, and we proceed to Step 2.

Now we check if $\{1, 3\} \rightarrowtail 11$. The 1-dimensional escalation lattices of $\{1, 3\}$ consist of $\begin{bmatrix}1 & 0\\0 & 2\end{bmatrix}$ and $\begin{bmatrix}1 & 0\\0 & 3\end{bmatrix}$, but the second one fails to represent 11, so $\{1, 3\} \not\rightarrowtail 11$. Now we check if $\{2, 3\} \rightarrowtail 11$. The 2-dimensional escalation lattices consist of

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

While the first and third lattices represent 11, the second lattice fails, so $\{2, 3\} \not\rightarrowtail 11$. We have established that $T_{min} = \{1, 2, 3\}$, so we proceed to Step 3.

We will begin by checking if $T \setminus \{1\} \rightarrowtail 11$. We begin with [2], which clearly does not represent 11, so we escalate by the truant 3, which results in 2-dimensional lattices we have already calculated in (1). Only the second lattice fails to represent 11, so we escalate by its truant 5. One of the escalator lattices $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 5 \end{bmatrix}$, fails to represent 11 but represents $T \setminus \{1\}$, thus $T \setminus \{1\} \not\rightarrowtail 11$.

Next we check if $T \setminus \{2\} \rightarrowtail 11$. Beginning with [1], we escalate by 3, and find $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$ fails to represent 11, so we escalate by its truant 5. One of the escalator lattices $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 1 & 4 \end{bmatrix}$ fails to represent 11 but it represents $T \setminus \{2\}$, thus $T \setminus \{2\} \not\rightarrowtail 11$.

Lastly, we check if $T \setminus \{3\} \rightarrowtail 11$. We begin with [1] and escalate by 2, resulting in the lattice $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which does not represent 11, so we escalate by the truant 6. One of the 3-dimensional escalators $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix}$ fails to represent 11 but it represents $T \setminus \{3\}$, hence $T \setminus \{3\} \not\rightarrowtail 11$. Thus, we have proven 11 has a unique minimal forcing set: {1, 2, 3}.

4.3 Families of Numbers Without Unique Minimal Forcing Sets

In this final section, we will look at families of infinite numbers without unique minimal forcing sets. We begin with a useful lemma.

Lemma 4.3 *Let S be a set of positive integers and $n \in \mathbb{N}$ such that n has a unique minimal forcing set $S_0 \subseteq S$. If S_1, $S_2 \subseteq S$ such that $S_1 \neq S_2$, and both subsets force n, then $S_1 \cap S_2 \rightarrowtail n$.*

Proof. By definition of a unique minimal forcing set, S_1 and S_2 must both contain S_0, so the lemma immediately follows. ■

Using this fact, we can devise a method for discovering a family of numbers without unique minimal forcing sets in $T = \{1, 2, 3, 5, 6, 7, 10, 14, 15\}$. Let S_1 and S_2 be distinct but not disjoint subsets of T. Suppose $S_1 \rightarrowtail W$, $S_2 \rightarrowtail Z$, and let V be a set of positive integers, none of which is forced by $S_1 \cap S_2$. Then by Lemma 4.3, we have that if $n \in W \cap Z$, but also $n \in V$, then n does not have a unique minimal forcing set. Using this fact, we establish the main result of this paper. Let the **order** of p in n, denoted $ord_p(n)$, represent the highest power of the prime p dividing a fixed positive integer n.

Theorem 4.4 *Let $n \in \mathbb{N}$. If n is not of the following forms,*

1. *$2^k u_7$, for any integer $k \geq 0$.*
2. *$2^e u_3$, for even $e \geq 0$.*
3. *$3^d u_+$, for odd $d \geq 0$.*
4. *$3^d u_-$, for odd $d \geq 0$.*
5. *$\prod_{i=1}^{j} p_i^{a_i}$ for primes p_i with a_i odd for some $p_i \equiv 5, 7 \mod 8$.*

but has $\mathrm{ord}_p(n)$ *odd for some* $p \equiv 3 \mod 4$*, then* n *does not have a unique minimal forcing set in* T*.*

Proof. For such n, we will show that for $\{1,2,6\} \rightarrowtail n$ and $\{1,2,3,5,7,10,14\} \rightarrowtail n$, but n is not represented by any $\{1,2\}$-escalator. We first determine the integers forced by $\{1, 2, 6\}$. We begin with [1] and escalate by the truant 2 to obtain the 2-dimensional escalators $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. The first is has truant 6, while second is universal over our set. We will escalate the first form and then classify integers represented by the second.

The complete set of 3-dimensional $\{1,2,6\}$-escalators of $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ consist of the diagonal forms $[1,1,1]$, $[1,1,2]$, $[1,1,4]$, $[1,1,5]$, and $[1,1,6]$. All 5 forms are class number one [10], so by Corollary 3.3 it is good enough to check which numbers are locally represented. The first two forms are addressed by Bhargava [1]. They respectively represent numbers not of the form $2^e u_7$ and $2^d u_7$. The third form represents numbers not of the form $2^e u_3$ and $2^e u_7$. The fourth form represents numbers not of the form $2^e u_3$. The last form represents numbers not of the form $3^d u_+$.

Returning to the second lattice, it can be shown that it represents any positive integer n without $\mathrm{ord}_p(n)$ odd for $p \equiv 5,7 \mod 8$. For this result and more concerning representation of primes by binary (2 variable) quadratic forms, see Spearman and Williams' "Representing Primes by Binary Quadratic Forms [11]."

Next, we check the positive integers forced by $\{1,2,3,5,7,10,14\}$. The escalation of this set is near-identical to the process used by Bhargava in [1] to find a forcing set for $\mathbb{N}$ over $\mathbb{Z}$, with the exception of the non-escalation of the lattice $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}$, which is in fact, universal over our set. This form represents numbers not of the form $3^d u_-$. The other escalator lattices will represent every positive integer except possibly 15.

Consolidating all these classes together, we arrive at conditions 1-5. Lastly, we check the numbers forced by the intersection of both sets, $\{1, 2\}$. The escalation lattices consist of the two familiar lattices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. The second form we have dealt with, while the first form $x^2 + y^2$ has been famously proven by Fermat to represent a positive integer n if and only if it does not have $\mathrm{ord}_p(n)$ odd for $p \equiv 3 \mod 4$. See Jones and Jones' text *Elementary Number Theory*, Theorem 10.3 for a proof [6]. Thus, we find the numbers forced by $\{1, 2, 6\}$ and $\{1, 2, 3, 5, 7, 10, 14\}$ equivalent to those numbers not satisfying conditions 1-5, and numbers not represented by the intersection $\{1,2\}$ of both sets to be those with a prime factor $\mathrm{ord}_p(n)$ odd for $p \equiv 3 \mod 4$, completing the proof. ∎

Corollary 4.5 *If* n *is a positive integer such that*

$$n = 2^e \prod_{i=1}^{j} p_i^{2a_i} \prod_{i=1}^{2l} {p'_i}^{b_i} \prod_{i=1}^{m} q_i^{c_i} \prod_{i=1}^{v} g_i^{2f_i},$$

for even $e \geq 0$*,* $a_i \geq 0$*, odd* $b_i > 0$*,* $c_i \geq 0$*,* $f_i \geq 0$*, and distinct primes* $p_i \equiv 3 \mod 8$*,* $3 \neq {p'}_i \equiv 3 \mod 8$*,* $q_i \equiv 1 \mod 8$*, and* $g_i \equiv 5,7 \mod 8$*, then* n *does not have a unique minimal forcing set in* T*.*

Proof. We have that n is in the 2-adic squareclass $2^e u_1$, since $\prod_{i=1}^{j} p_i^{2a_i} \equiv \prod_{i=1}^{2l} {p'}_i^{b_i} \equiv \prod_{i=1}^{m} q_i^{c_i} \equiv \prod_{i=1}^{v} g_i^{2f_i} \equiv 1 \mod 8$. We also know that n is not of the form $3^d u_+$ or $3^d u_-$, since we only allow 3 to be in the class of primes p_i which are raised to even powers. Furthermore, n is not divisible by a prime factor $p \equiv 5$ or $7 \bmod 8$ such that $\text{ord}_n(p)$ is odd. Thus, it satisfies conditions 1-5 of Theorem 4.4. Since it has prime factor $p \equiv 3 \mod 4$ such that $\text{ord}_n(p)$ is odd, the result follows. ∎

Corollary 4.6 *If n is a positive integer such that*

$$n = 2^d \prod_{i=1}^{j} p_i^{2a_i} \prod_{i=1}^{l} {p'}_i^{b_i} \prod_{i=1}^{m} q_i^{c_i} \prod_{i=1}^{v} g_i^{2f_i},$$

for odd $d > 0$, $a_i \geq 0$, odd $b_i > 0$, $c_i \geq 0$, $f_i \geq 0$, and distinct primes $p_i \equiv 3 \mod 8$, $3 \neq {p'}_i \equiv 3 \mod 8$, $q_i \equiv 1 \mod 8$, and $g_i \equiv 5, 7 \mod 8$, then n does not have a unique minimal forcing set in T.

Proof. We have that n is in the 2-adic squareclass $2^d u_1$ or $2^d u_3$, since $\prod_{i=1}^{j} p_i^{2a_i} \equiv \prod_{i=1}^{m} q_i^{c_i} \equiv \prod_{i=1}^{v} g_i^{2f_i} \equiv 1 \mod 8$ and $\prod_{i=1}^{2l} {p'}_i^{b_i} \equiv 1, 3 \mod 8$. If l is even then it is congruent to 1 modulo 8 and if l is odd, it is congruent to 3 modulo 8. We also have that n is not of the form $3^d u_+$ or $3^d u_-$, since we only allow 3 to be in the class of primes p_i which are raised to even powers. Furthermore, n is not divisible by a prime factor $p \equiv 5$ or $7 \bmod 8$ such that $\text{ord}_n(p)$ is odd. Thus, it satisfies conditions 1-5 of Theorem 4.4. Since it has a prime factor congruent to 3 modulo 4 whose order in n is odd, the result follows. ∎

It is also worth noting that by Dirichlet's theorem, we are guaranteed infinitely such p_i, ${p'}_i$, q_i, and g_i.

References

[1] M. Bhargava, "On the Conway-Schneeberger Fifteen Theorem." *Quadratic forms and their applications.* Contemp. Math, Vol. 272, p.p. 27-37, 2000.

[2] M. Bhargava and J. Hanke, "Universal quadratic forms and the 290-theorem." *Invent. Math.* (to appear). Preprint available @ http://www.wordpress.jonhanke.com/wp-content/uploads/2011/09/290-Theorem-preprint.pdf

[3] J.H. Conway and F. Fung, *The Sensual (Quadratic) Form.* The Carus Mathematical Monographs, Number 26, 1997.

[4] J.H. Conway and N.J.A Sloane, *Sphere Packings, Lattices and Groups.* Springer-Verlag New York Inc., 1988.

[5] W.C. Jagy, I. Kaplansky, and A. Schiemann, "There are 913 regular ternary forms." *Mathematika.* Cambridge University Press, Vol. 44, Issue 02, p.p. 332-341, 1997.

[6] G.A. Jones and J.M. Jones, *Elementary Number Theory.* London: Springer, 1998.

[7] M.-H. Kim, "Recent developments on universal forms." *Algebraic and arithmetic theory of quadratic forms.* Contemp. Math, Vol. 344, p.p. 215-228.

[8] T.Y. Lam, *Introduction to Quadratic Forms over Fields.* American Mathematical Society, 2004.

[9] O. Timothy O'Meara, *Introduction to Quadratic Forms.* Springer, 2000.

[10] G. Nebe and N.J.A. Sloane, "The Brandt-Intrau-Schiemann Table of Odd Ternary Quadratic Forms." Available @ `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_1.html`

[11] B. Spearman and K.S. Williams, "Representing Primes by Binary Quadratic Forms." *The American Mathematical Monthly.* Math. Assoc. America, Vol. 99, No. 5, p.p. 423-426, 1992.