Abstract

We find the group of linear transformations which preserve the Voronoi polyhedron in arbitrary dimension; or equivalently, we find the linear transformations of the space of symmetric matrices which preserve the integer semi-definite ones, proving a conjecture of Ryshkov.

1 Notation and a Couple Remarks

Definition 1. Let \( \{ e_i : 1 \leq i \leq n \} \) denote the standard basis of \( \mathbb{R}^n \).

We will be concerned with the quadratic forms in \( n \) variables, which are determined by \( N = n(n + 1)/2 \) coefficients. Denote the real linear space of symmetric matrices by \( \text{Sym}_n(\mathbb{R}) \). \( \text{Sym}_n(\mathbb{R}) \cong \mathbb{R}^N \).

Let \( \pi_i \) be the \( i^{th} \) coordinate projection. If we have a vector \( x \in \mathbb{Z}^n \) abbreviate \( \pi_i(x) \) by \( x_i \). Furthermore, if we have an indexed set of vectors \( x_i \in \mathbb{Z}^n \) denote \( \pi_j(x_i) \) by \( x_{ji} \).

The proof of the following lemma is straightforward and we omit it.

Lemma 2. Given any two nonzero vectors \( u \) and \( v \) in \( \mathbb{Z}^n \), there exists a linear transformation \( L \) in \( \text{GL}_n(\mathbb{Z}) \), such that \( Lu \) and \( Lv \) have no coordinates which are 0.

We call a quadratic form integer if its coefficients are integral. It will be important for our purposes to establish the following:

Lemma 3. An integer quadratic form that represents only squares is the square of a linear form.

Proof. Let \( f \) be a quadratic form in \( n \) variables (with real symmetric matrix \( F \)) that represents only squares. Note that all the diagonal entries of \( F \) must be squares. We proceed by induction on \( n \).

Let \( n = 2 \). Because \( f \) represents no negative values, \( \det F \geq 0 \). If \( \det F = 0 \), then \( f \) is the square of a linear functional by inspection.

Suppose \( f \) is positive definite. Without loss of generality we may assume that \( F \) is a Minkowski reduced form. Then
with $0 \leq c \leq a^2$ and $0 < a < b$. Express $c$ as $c = 2aq + r$ with $0 \leq r < 2a$. Because $c \leq a^2$, $q \leq a < b$.

This implies that

$$f(x, y) - (ax + qy)^2 = (b^2 - q^2)y^2 + rxy \geq 0$$

and when $y > 0$ the inequality is strict. Because $f$ represents only squares,

$$f(x, y) - (ax + qy)^2 = (b^2 - q^2)y^2 + rxy \geq 2(ax + qy) + 1$$

when $y > 0$. Letting $y = 1$ and $x$ approach infinity, we have $r \geq 2a$ which is a contradiction.

Assume inductively that Lemma 3 holds for forms in $n - 1$ variables. Consider the $n$-ary quadratic form $f(x_1, \ldots, x_n)$.

$$f(x_1, \ldots, x_n, 0) = (a_1x_1 + \cdots + a_{n-1}x_{n-1})^2$$

and

$$f(0, x_2, \ldots, x_n) = (b_2x_2 + \cdots + b_nx_n)^2.$$ 

By multiplying by $-1$ if necessary, we may assume that $b_i = a_i$ for $2 \leq i \leq n - 1$. Let $a_n = b_n$. Then $F_{ij}$ is $a_ia_j$ for all $(i, j)$ except $(1, n)$ and $(n, 1)$. By considering the quadratic form $f(x_1, 0, \ldots, 0, x_n)$ we have that $F_{1n} = \pm a_1a_n$. Suppose that $F_{1n} = -a_1a_n$ (with $a_1$ and $a_n$ nonzero) and for some $k$ $a_k$ is nonzero. Then

$$f = (a_1x_1 + \cdots + a_nx_n)^2 - 4a_1a_nx_n.$$ 

As in the 2-dimensional case, by taking a sufficiently high value for $x_k$ we have that $f(e_1 + x_ke_k + e_n) - f(x_ke_k)$ is too small, which is our contradiction.

We refer to the square of a non-zero linear form as a rank one form.

## 2 The Voronoi Map

Define the map $V : \mathbb{R}^n \to \text{Sym}_n(\mathbb{R})$ by

$$V(a)(x) = (a \cdot x)^2,$$

where $\cdot$ denotes the normal inner product on $\mathbb{R}^n$ and $x$ is a variable vector. This map is usually referred to as the Veronese map. The restriction of this map to $\mathbb{Z}^n$ is known in the geometry of numbers as the Voronoi map. We will use the latter term.
For \( x \) in \( \mathbb{R}^n \), let \( X \) denote the \( n \times n \) matrix:

\[
X = \begin{bmatrix}
x_1 & x_1 & \cdots & x_1 \\
x_2 & x_2 & \cdots & x_2 \\
\vdots & \vdots & \ddots & \vdots \\
x_n & x_n & \cdots & x_n
\end{bmatrix}.
\]

(4)

The Voronoi map, when viewed as a map to the space of symmetric matrices, can then be written

\[
V(x) = \frac{1}{n}XX^t.
\]

The Voronoi map is quadratic and the associated symmetric bilinear map will also be denoted by \( V \), explicitly

\[
V(x, y) = \frac{1}{2n}(XY^t + YX^t).
\]

Equate the space of quadratic forms in \( n \) variables, the space of symmetric \( n \times n \) matrices and \( \mathbb{Z}^N \). Label the \( N \) coordinate projections of \( \mathbb{Z}^N \) by letting \( \pi_{ij}(a) \) for \( a \in \mathbb{Z}^N \) be half of the coefficient of \( x_i x_j \) in the quadratic form \( a \) or the \( ij \)-entry of the symmetric matrix \( A \). For instance, the definition of the Voronoi map reads \( \pi_{ij}(V(a)) = a_i a_j \) and we have \( \pi_{ij} = \pi_{ji} \). To avoid writing lots of \( \pi_{ij} \)'s, if we have \( a \in \mathbb{Z}^N \) we write \( a_{ij} \) for \( \pi_{ij}(a) \). This causes some confusion when we also have an indexed set of vectors, \( w_i \) in \( \mathbb{Z}^n \) and we speak of the \( j \)th coordinate of the \( i \)th vector and also denote it by \( w_{ji} \). The space to which the vector belongs, however, determines what is meant by a double subscript, and hopefully this isn’t too confusing.

A Voronoi point is the image of an integral vector, \( x \in \mathbb{Z}^n \), under the Voronoi map, i.e. \( V(x) \).

**Def 4.** The Voronoi polyhedron in \( n \)-variables, denoted \( \Pi(n) \), is the closure of the convex hull of the image of \( \mathbb{Z}^n \) under the Voronoi map. In other words, it is the closure of the convex hull of all Voronoi points in \( \mathbb{Z}^N \).

Barnes and Cohn [1] showed that the Voronoi polyhedron is also the closure of the convex hull of \( \mathbb{Z}^N \) intersect the cone of semi-definite forms \( K \), by showing that for any real positive definite \( n \)-ary form \( f \) and any \( g \in \mathbb{Z}^N \cap K \), the trace of \( FG \) is greater than or equal to the minimum value of \( f \), where \( FG \) denotes the normal matrix multiplication of the symmetric matrices associated with the quadratic forms \( f \) and \( g \).

**Def 5.** Let \( GL_N(\Pi(n)) \) denote the subset of \( Mat_{N \times N}(\mathbb{R}) \) which maps the Voronoi polyhedron bijectively to itself.

In this paper, we find \( GL_N(\Pi(n)) \) for all \( n \).

We would like to know that a vector is a Voronoi point without having to find a vector in \( \mathbb{Z}^n \), so we characterize Voronoi points as follows:
Lemma 6. A point $x$ in $\mathbb{Z}^N$ is a Voronoi point if and only if $x_{ij} = x_{ik}x_{jk}$ for all $i, j, k$.

Proof. The forward direction follows from the definition of a Voronoi point. In the other direction, define $a \in \mathbb{Z}^n$ by: $a_1 = \sqrt{x_{11}}$ and $a_i = \frac{x_{1i}}{a_1}$. Note that the hypothesis implies that $a_i$ is an integer. We then have

$$V(a)_{ij} = \frac{x_{1i}x_{1j}}{a_1} = \frac{x_{1i}x_{1j}}{x_{11}} = x_{ij}.$$ 

In other words, $V(a) = x$.

Linear maps in $GL_n(\mathbb{Z})$ induce linear maps on $\mathbb{Z}^N$ by changing the basis of the symmetric bilinear forms in $\mathbb{Z}^N$. Explicitly, we define the Voronoi map on $GL_n(\mathbb{Z})$ by $V(L)M = LML^t$ for $M \in \mathbb{Z}^N$, where $M$ is interpreted as a symmetric matrix. $V(L)$ is trivially seen to be linear and integrally invertible with inverse $V(L^{-1})$. Likewise, it is seen that the Voronoi map is a homomorphism from $GL_n(\mathbb{Z})$ to $GL_N(\mathbb{Z})$. We can also lift any linear map (invertable /integral or otherwise) by the same definition, although of course the image need not be in $GL_N(\mathbb{Z})$. Note that

$$V(L)V(x) = \frac{1}{n}LXX^tL^t = V(Lx)$$

$$V(L)V(x, y) = \frac{1}{2n}L(XX^t + YY^t)L^t = V(Lx, Ly). \tag{5}$$

This relation justifies the abuse of the name Voronoi map and implies that $V(L)$ leaves the Voronoi polyhedron invariant, i.e. $V(L) \in GL_N(\Pi(n))$. Ryshkov conjectured that all maps in $GL_N(\Pi(n))$ where of this form, and indeed we show this to be the case. To this end, we establish means of recognizing elements of $GL_N(\Pi(n))$ which are the Voronoi images of elements of $GL_n(\mathbb{Z})$ in Section 3. And then in Section 4 we show that these are in fact all of them.

3 Characterizing the Voronoi images of linear maps in $GL_N(\Pi(n))$

Lemma 7. If $\tau$ is in $GL_N(\Pi(n))$ and $\tau$ is the Voronoi image of some linear map $L$, $L \in Mat_{n \times n}(\mathbb{R})$, then $L$ is integral and integrally invertable and thus $\tau \in V(GL_n(\mathbb{Z}))$.

Proof. Note that because the Voronoi polyhedron is full dimensional, elements of $GL_N(\Pi(n))$ are in $GL_N(\mathbb{R})$. The equations (5) imply that $V(Le_i)$ is in the image of $\tau$ restricted to the Voronoi polyhedron. Because $\tau \in GL_N(\Pi(n))$, this means $L(e_i)$ is integral. The same reasoning shows that $L^{-1}$ is integral.

Because $V(\mathbb{Z}^n)$ spans $\mathbb{Z}^N$, for $\tau$ a linear map on $\mathbb{R}^N$ to be the image of a linear map under the Voronoi map, we need only find a linear map $L$ such that $\tau \circ V = V \circ L$ on $\mathbb{Z}^n$. We wish only to involve ourselves with binary quadratic forms so we establish the following lemma.

4
Lemma 8. Let \( \tau \) be in \( GL_N(\Pi(n)) \). \( \tau \) is in the image of \( Mat_{n\times n}(\mathbb{R}) \) if and only if for any \( u_1, u_2 \in \mathbb{Z}^n \), there exist vectors \( w_1, w_2 \in \mathbb{Z}^n \) such that

\[
\begin{align*}
\tau \circ V(u_1) &= V(w_1) \\
\tau \circ V(u_1, u_2) &= V(w_1, w_2).
\end{align*}
\]

The forward direction of Lemma (8) is just an expression of the equations (5). Call the second condition in Lemma (8) condition (*). Note that in condition (*) the fact that \( \tau \) preserves the Voronoi polyhedron ensures that there are two choices for \( w_1 \) (or \( w_2 \)) satisfying (6) and they are negatives of each other. The substance of this equivalence is that if we choose the signs of the \( w_i \), pairwise, we will never run into trouble constructing the linear map whose image under the Voronoi map is \( \tau \).

Proof. By the previous paragraph, we only show that condition (*) implies that \( \tau = V(L) \) for some linear map \( L \) on \( \mathbb{R}^n \). Define \( L \) by \( L(e_i) = w_i \) where \( w_i \) is as in (*) on the pair \((e_1, e_2)\). Because \( V(e_i) \) and \( V(e_i, e_j) \) form a spanning set of \( \mathbb{R}^N \), it only remains to check that for all pairs \((i, j)\), \( \tau \circ V(e_i, e_j) = V(w_i, w_j) \). Assume that for some \( \tau \in GL_N(\Pi(n)) \) and some pair \((i, j)\) this is not the case. Under this assumption, condition (*) implies that \( \tau \circ V(e_i, e_j) = -V(w_i, w_j) \).

It will be convenient to have that none of the coordinates of \( w_1 \) or \( w_2 \) vanish, so we arrange this. By Lemma 2 there exists a linear transformation \( T \) in \( GL_n(\mathbb{Z}) \) such that \( T(w_1) \) and \( T(w_2) \) have all coordinates nonzero. Replace \( \tau \) by \( V(T) \circ \tau \) and by abuse of notation relabel the latter function \( \tau \) and let \( w_1 \) and \( w_2 \) be \( T(w_1) \) and \( T(w_2) \) respectively.

Now consider the ternary quadratic form \( q(x, y, z) := \tau \circ V(xe_1 + ye_1 + ze_2) \). Because \( \tau \circ V \) represents only Voronoi points, \( \pi_{ij}(q) \) represents only squares, so Lemma 3 implies that \( \pi_{kk}(q) \) is the square of a linear functional. By the definition of \( w_i \), \( \pi_{kk}(q(x, y, 0)) = (xw_{k1} + yw_{k2})^2, \pi_{kk}(q(x, 0, z)) = (xw_{k1} + zw_{k2})^2, \) and \( \pi_{kk}(q(0, y, z)) = (yw_{k1} - zw_{k2})^2 \). Since both \( w_{k1} \) and \( w_{k2} \) are nonzero for all \( k \), the previous comments imply that \( \pi_k(w_i) = 0 \) for all \( k \). This however is a contradiction because \( 0 \) is not a Voronoi point.

\[ \square \]

4 \( GL_N(\Pi(n)) \)

Theorem 9. \( GL_N(\Pi(n)) \cong V(\GL_n(\mathbb{Z})) \cong GL_n(\mathbb{Z})/\{\pm 1\} \)

Proof. The image of \( GL_n(\mathbb{Z}) \) under the Voronoi map leaves \( \Pi(n) \) invariant, as previously commented. Because \( V(L)V(x) = V(Lx) \), if \( V(L) = V(L') \) we must have \( V(Lx) = V(L'x) \) for all \( x \in \mathbb{Z}^n \). This implies \( L = \pm L' \). So \( \text{Ker}(V) = \pm 1 \). The claim will therefore follow if we show that \( V \) is surjective on \( GL_N(\Pi(n)) \). By Lemma (8) and Lemma (7), this is equivalent to showing that all \( \tau \) in \( GL_N(\Pi(n)) \) satisfy condition (*). Assume to the contrary that we had vectors \( u_1 \) and \( u_2 \) in \( \mathbb{Z}^n \) and \( \tau \in GL_N(\Pi(n)) \) that did not satisfy (*).

Consider the binary quadratic form \( f \) defined
Because $\tau \in GL_N(\Pi(n))$, $\tau \circ V(u_1)$ and $\tau \circ V(u_2)$ are Voronoi points, i.e. we have vectors $w_1$ and $w_2$, determined up to sign, such that

\[
\tau \circ V(u_1) = V(w_1) \\
\tau \circ V(u_2) = V(w_2).
\]

As before, Lemma 2 allows us to assume that $w_i$ and $w_j$ have no zero coordinates. Expanding the right hand side of equation (8) and using the definitions above, we see that

\[
f(x, y) = x^2V(w_1) + y^2V(w_2) + 2xy(\tau \circ V(u_1, u_2)).
\]

For convenience, define $\sigma$ by $\sigma = \tau \circ V(u_1, u_2)$. We may then express $f$

\[
f(x, y) = x^2V(w_1) + y^2V(w_2) + 2xy\sigma. \tag{9}
\]

Since $f$ only represents Voronoi points, $\pi_i f$ is a binary quadratic form which only represents squares. By Lemma 3, we have that $\sigma_{ii} = \pm w_{i1}w_{i2}$. Let $(-1)^n_i$ be the sign of $\sigma_{ii}/(w_{i1}w_{i2})$. We show that in fact this sign does not depend on $i$: By Lemma 6,

\[
f_{jj}f_{ii} = f_{ij}^2. \tag{10}
\]

\[
f_{ij} = x^2w_{i1}w_{j1} + y^2w_{i2}w_{j2} + 2xy\sigma_{ij}. \tag{11}
\]

by equation (9). By the definition of $\eta_i$,

\[
f_{ii} = (xw_{i1} + (-1)^n_iyw_{i2})^2. \tag{12}
\]

Combining equation (10), equation (11), and equation (12), and taking the square root yields:

\[
(xw_{i1} + (-1)^n_iyw_{i2})(xw_{j1} + (-1)^n_jyw_{j2}) = \pm(x^2w_{i1}w_{j1} + y^2w_{i2}w_{j2} + 2xy\sigma_{ij}). \tag{13}
\]

The right hand side shows that the signs of $x^2w_{j1}w_{i1}$ and $y^2w_{j2}w_{i2}$ must be the same, which implies that $\eta_i$ can be chosen independently of $i$. Replace $w_2$ by $-w_2$, if necessary, to have $\eta_i = 1$. Equation (12) now becomes
\[ f_{ii} = (xw_{i1} + yw_{i2})^2, \]  
\hspace{1cm} (14)

or equivalently

\[ \sigma_{ii} = w_{i1}w_{i2}. \]  
\hspace{1cm} (15)

Equation (14) transforms equation (13) into

\[ (xw_{i1} + yw_{i2})(xw_{j1} + yw_{j2}) = \pm(x^2w_{i1}w_{j1} + y^2w_{i2}w_{j2} + 2xy\sigma_{ij}). \]  
\hspace{1cm} (16)

Comparing the coefficients of \( x^2 \), we see that in fact we must have

\[ (xw_{i1} + yw_{i2})(xw_{j1} + yw_{j2}) = x^2w_{i1}w_{j1} + y^2w_{i2}w_{j2} + 2xy\sigma_{ij}, \]  
\hspace{1cm} (17)

which gives that

\[ \sigma_{ij} = \frac{1}{2}(w_{i1}w_{j2} + w_{i2}w_{j1}). \]  
\hspace{1cm} (18)

This however implies that \( \sigma = V(w_1, w_2) \), which is condition (*), and we have a contradiction.

\[ \square \]

5 References

2. S.S. Ryshkov and E.P. Baranovskii, Classical Methods in the Theory of Lattice Packings, what’s the other info?