Linear Transformations Preserving the Voronoi Polyhedron

Kirsten Wickelgren

today

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

Def 1. *Let* $\{\mathbf{e}_i : 1 \leq i \leq n\}$ *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 $\mathrm{Sym}_n(\mathbb{R})$. $\mathrm{Sym}_n(\mathbb{R}) \cong \mathbb{R}^N$.

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

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

Lemma 2. *Given any two nonzero vectors* $\mathbf{u}$ *and* $\mathbf{v}$ *in* $\mathbb{Z}^n$*, there exists a linear transformation* L *in* $GL_n(\mathbb{Z})$*, such that* $L\mathbf{u}$ *and* $L\mathbf{v}$ *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 negetive 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

$$F = \begin{matrix} a^2 & \mathrm{c} \\ \mathrm{c} & b^2 \end{matrix} \tag{1}$$

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

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

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

$$f(x, y) - (ax + qy)^2 = (b^2 - q^2)y^2 + rxy \geq 2(ax + qy) + 1 \tag{3}$$

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

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

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

and

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

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 $f(x_1, 0, \dots, 0, x_n)$ 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 $f(\mathbf{e}_1 + x_k\mathbf{e}_k + \mathbf{e}_n) - f(x_k\mathbf{e}_k)$ 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 $V : \mathbb{R}^n \to Sym_n(\mathbb{R})$ *by*

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

where $\cdot$ *denotes the normal inner product on* $\mathbb{R}^n$ *and* $\mathbf{x}$ *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 $\mathbf{x}$ *in* $\mathbb{R}^n$*, let* X *denote the* $n \times n$ *matrix:*

$$X = \begin{matrix} x_1 & x_1 & \dots & x_1 \\ x_2 & x_2 & \dots & x_2 \\ & & \dots & \\ x_n & x_n & \dots & x_n \end{matrix}. \tag{4}$$

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

$$V(\mathbf{x}) = \frac{1}{n} X X^t.$$

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

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

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* $\pi_{ij}(\mathbf{a})$ *for* $\mathbf{a} \in \mathbb{Z}^N$ *be half of the coeficient of* $x_i x_j$ *in the quadratic form* $\mathbf{a}$ *or the* ij*-entry of the symmetric matrix* A*. For instance, the definition of the Voronoi map reads* $\pi_{ij}(V(\mathbf{a})) = a_i a_j$ *and we have* $\pi_{ij} = \pi_{ji}$*. To avoid writing lots of* $\pi_{ij}s$*, if we have* $\mathbf{a} \in \mathbb{Z}^N$ *we write* $\mathbf{a}_{ij}$ *for* $\pi_{ij}(\mathbf{a})$*. This causes some confusion when we also have an indexed set of vectors,* $\mathbf{w}_i$ *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, $\mathbf{x} \in \mathbb{Z}^n$*, under the Voronoi map, i.e.* $V(\mathbf{x})$.

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 Vornonoi 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* $\mathbf{x}$ *in* $\mathbb{Z}^N$ *is a Voronoi point if and only if* x_{ii} *is the square of an integer and* $x_{ij}x_{kk} = x_{ik}x_{jk}$ *for all* i, j, k.

Proof. The forward direction follows from the definition of a Voronoi point. In the other direction, define $\mathbf{a} \in \mathbb{Z}^n$ 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

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

In other words, $V(\mathbf{a}) = \mathbf{x}$. $\square$

Linear maps in $GL_n(\mathbb{Z})$ *induce linear maps on* $\mathbb{Z}^N$ *by changing the basis of the symmetric bilinear maps 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 invertable 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 defininition, although of course the image need not be in* $GL_N(\mathbb{Z})$. *Note that*

$$\begin{aligned} V(L)V(\mathbf{x}) &= \frac{1}{n}LXX^tL^t = V(L\mathbf{x}) \\ V(L)V(\mathbf{x},\mathbf{y}) &= \frac{1}{2n}L(XY^t + YX^t)L^t = V(L\mathbf{x}, L\mathbf{y}). \end{aligned} \tag{5}$$

This relation justifies the abuse of the name Voronoi map and implies that $V(L)$ *leaves the Voronoi polyhedron invarient, 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* τ *is in* $GL_N(\Pi(n))$ *and* τ *is the Voronoi image of some linear map* L, $L \in Mat_{n\times n}(\mathbb{R})$, *then* L *is integral and integraly 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 $V(L\mathbf{e}_i)$ is in the image of τ restricted to the Voronoi polyhedron. Because $\tau \in GL_N(\Pi(n))$, this means $L(\mathbf{e}_i)$ is integral. The same reasoning shows that L^{-1} is integral.

$\square$

Because $V(\mathbb{Z}^n)$ *spans* $\mathbb{Z}^N$, *for* τ *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 invovle ourselves with binary quadratic forms so we establish the following lemma.*

Lemma 8. *Let τ be in $GL_N(\Pi(n))$. τ is in the image of $Mat_{n\times n}(\mathbb{R})$ if and only if for any $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$, there exist vectors $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{Z}^n$ such that*

$$\begin{aligned} \tau \circ V(\mathbf{u}_i) &= V(\mathbf{w}_i) && (6)\\ \tau \circ V(\mathbf{u}_1, \mathbf{u}_2) &= V(\mathbf{w}_1, \mathbf{w}_2). && (7) \end{aligned}$$

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 τ preserves the Voronoi polyhedron ensures that there are two choices for $\mathbf{w}_1$ (or $\mathbf{w}_2$) satisfying (6) and they are negatives of each other. The substance of this equivalence is that if we choose the signs of the $\mathbf{w}_i$ pairwise, we will never run into trouble constructing the linear map whose image under the Voronoi map is τ.

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 $L(\mathbf{e}_i) = \mathbf{w}_i$ where $\mathbf{w}_i$ is as in (*) on the pair $(\mathbf{e}_1, \mathbf{e}_i)$. Because $V(\mathbf{e}_i)$ and $V(\mathbf{e}_i, \mathbf{e}_j)$ form a spanning set of $\mathbb{R}^N$, it only remains to check that for all pairs (i,j), $\tau \circ V(\mathbf{e}_i, \mathbf{e}_j) = V(\mathbf{w}_i, \mathbf{w}_j)$. 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 $\tau \circ V(\mathbf{e}_i, \mathbf{e}_j) = -V(\mathbf{w}_i, \mathbf{w}_j)$.

It will be convenient to have that none of the coordinates of $\mathbf{w}_1$ or $\mathbf{w}_2$ vanish, so we arrange this. By Lemma 2 there exists a linear transformation T in $GL_n(\mathbb{Z})$ such that $T(\mathbf{w}_1)$ and $T(\mathbf{w}_2)$ have all coordinates nonzero. Replace τ by $V(T) \circ \tau$ and by abuse of notation relabel the latter function τ and let $\mathbf{w}_1$ and $\mathbf{w}_2$ be $T(\mathbf{w}_1)$ and $T(\mathbf{w}_2)$ respectively.

Now consider the teranary quadratic form $q(x,y,z) := \tau \circ V(x\mathbf{e}_1 + y\mathbf{e}_i + z\mathbf{e}_j)$. Because $\tau \circ V$ represents only Voronoi points, $\pi_{ii}(q)$ represents only squares, so Lemma 3 implies that $\pi_{kk}(q)$ is the square of a linear functional. By the definition of $\mathbf{w}_i$, $\pi_{kk}(q(x,y,0)) = (xw_{k1} + yw_{ki})^2$, $\pi_{kk}(q(x,0,z)) = (xw_{k1} + zw_{kj})^2$, and $\pi_{kk}(q(0,y,z)) = (yw_{ki} - zw_{kj})^2$. Since both w_{ki} and w_{kj} are nonzero for all k, the previous comments imply that $\pi_k(\mathbf{w}_1) = 0$ for all k. This however is a contradiction because $\mathbf{0}$ is not a Voronoi point.

□

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 $\Pi(n)$ invarient, as previously commented. Because $V(L)V(\mathbf{x}) = V(L\mathbf{x})$, if $V(L) = V(L')$ we must have $V(L\mathbf{x}) = V(L'\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}^n$. This implies $L = \pm L'$. So $\mathrm{Ker}(V) = \pm 1$. 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 τ in $GL_N(\Pi(n))$ satisfy condition (*). Assume to the contrary that we had vectors $\mathbf{u}_1$ and $\mathbf{u}_2$ in $\mathbb{Z}^n$ and $\tau \in GL_N(\Pi(n))$ that did not satisfy (*).

Consider the binary quadratic form f defined

$$f(x,y) := \tau \circ V(x\mathbf{u}_1 + y\mathbf{u}_2). \tag{8}$$

Because $\tau \in GL_N(\Pi(n))$, $\tau \circ V(\mathbf{u}_1)$ and $\tau \circ V(\mathbf{u}_2)$ are Voronoi points, i.e. we have vectors $\mathbf{w}_1$ and $\mathbf{w}_2$, determined up to sign, such that

$$\tau \circ V(\mathbf{u}_1) = V(\mathbf{w}_1)$$
$$\tau \circ V(\mathbf{u}_2) = V(\mathbf{w}_2).$$

As before, Lemma 2 allows us to assume that $\mathbf{w}_i$ and $\mathbf{w}_j$ have no zero coordinates. Expanding the right hand side of equation (8) and using the definitions above, we see that

$$f(x,y) = x^2V(\mathbf{w}_1) + y^2V(\mathbf{w}_2) + 2xy(\tau \circ V(\mathbf{u}_1,\mathbf{u}_2)).$$

For convenience, define σ by $\sigma = \tau \circ V(\mathbf{u}_1,\mathbf{u}_2)$. We may then express f

$$f(x,y) = x^2V(\mathbf{w}_1) + y^2V(\mathbf{w}_2) + 2xy\sigma. \tag{9}$$

Since f only represents Voronoi points, $\pi_{ii}f$ is a binary quadratic form which only represents squares. By Lemma 3, we have that $\sigma_{ii} = \pm w_{i1}w_{i2}$. Let $(-1)^{\eta_i}$ 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 η_i,

$$f_{ii} = (xw_{i1} + (-1)^{\eta_i}yw_{i2})^2. \tag{12}$$

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

$$(xw_{i1} + (-1)^{\eta_i}yw_{i2})(xw_{j1} + (-1)^{\eta_j}yw_{j2}) = \pm(x^2w_{i1}w_{j1} + y^2w_{i2}w_{j2} + 2xy\sigma_{ij}). \tag{13}$$

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 η_i can be chosen independently of i. Replace w_2 by $-w_2$, if necessary, to have $\eta_i = 1$. Equation (12) now becomes

$$f_{ii} = (xw_{i1} + yw_{i2})^2, \tag{14}$$

or equivalently

$$\sigma_{ii} = w_{i1}w_{i2}. \tag{15}$$

Equation (14) transforms equation (13) into

$$(xw_{i1} + yw_{i2})(xw_{j1} + yw_{j2}) = \pm(x^2 w_{i1}w_{j1} + y^2 w_{i2}w_{j2} + 2xy\sigma_{ij}). \tag{16}$$

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

$$(xw_{i1} + yw_{i2})(xw_{j1} + yw_{j2}) = x^2 w_{i1}w_{j1} + y^2 w_{i2}w_{j2} + 2xy\sigma_{ij}, \tag{17}$$

which gives that

$$\sigma_{ij} = \frac{1}{2}(w_{i1}w_{j2} + w_{i2}w_{j1}). \tag{18}$$

This however implies that $\sigma = V(\mathbf{w}_1, \mathbf{w}_2)$, which is condition (*), and we have a contradiction.

$\square$

5 References

1. E.S. Barnes and M.J. Cohn, On the Inner Product of Positive Quadratic Forms, Journal of London Mathematical Society (2), 12 (1975), 32-36.

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