JOURNAL OF NUMBER THEORY 4, 330–341 (1972)

On Voronoi Reduction of Positive Definite Quadratic Forms

T. J. DICKSON*

Department of Mathematics, Ohio State University, Columbus, Ohio 43210

Communicated by R. P. Bambah

Received May 26, 1970

There are two methods of reduction of positive definite quadratic forms due to Voronoi. One of these methods is based on the perfect forms and the other on the type of Voronoi polyhedra associated with the form. It was conjectured by Voronoi that these two methods are strongly connected.

It is shown in this paper that the two reductions coincide only in the case of the set of forms referred to by Voronoi as the principal cone.

1. *Introduction.* Voronoi [3, 4], outlined two methods of partitioning the $\frac{1}{2}n(n+1)$-dimensional space of positive definite quadratic forms in n variables into polyhedral cones with the origin as vertex, where the cones possess the following properties:

(i) They fill the space simply, i.e. any two cones are disjoint or have a common face.

(ii) An integral unimodular transformation either leaves a cone invariant or transforms it into another cone of the system.

(iii) There exists a finite number of the cones, say $\Delta_0, \Delta_1, \ldots, \Delta_\tau$ such that any positive form is equivalent to a form lying in some Δ_i $(0 \leqslant i \leqslant \tau)$.

These two partitions were arrived at by widely differing methods and yet the resulting cones, in the known cases, are very similar. Voronoi conjectured a strong connection between the two methods.

Let $\phi(\mathbf{x}) = \sum a_{ij}x_ix_j$ be a positive definite quadratic form in n variables

* Current address: University of Western Australia, Nedlands, W. A., 6009, Australia.

and let M be the minimum value of $\phi(\mathbf{x})$ for integral $\mathbf{x} \neq \mathbf{0}$. Let this minimum be attained at the $2s$ points,

$$\mathbf{x} = \pm\mathbf{m}_k \qquad (k = 1,..., s).$$

Now ϕ is said to be *perfect* if it is uniquely determined by its minimum M and its s minimal vectors, i.e., if these is no nontrivial quadratic form Ψ such that

$$\Psi(\mathbf{m}_k) = 0 \qquad (k = 1,..., s).$$

Obviously, $s \geqslant \frac{1}{2}n(n+1)$.

Corresponding to the perfect form ϕ we associate the cone Δ in the $\frac{1}{2}n(n+1)$-dimensional space of n-ary quad. forms where

$$\Delta = \left\{ f \mid f(\mathbf{x}) = \sum_{k=1}^{s} \rho_k(\mathbf{m}_k'\mathbf{x})^2,\ \rho_k \geqslant 0\ (k = 1,..., s) \right\},$$

i.e., the cone whose edge forms are $(\mathbf{m}_k'\mathbf{x})^2$ $(k = 1,..., s)$.

These cones partition the space of positive forms with the properties stated above and this was Voronoi's first method. We will call these cones *type* I *cones.*

The form

$$\phi_0(\mathbf{x}) = \sum_{i=1}^{n} x_i^2 + \sum_{i<j} x_i x_j$$

is easily shown to be perfect for all n and the corresponding cone is found to be

$$\Delta_0 = \left\{ f \mid f(\mathbf{x}) = \sum_{i=1}^{n} \rho_i x_i^2 + \sum_{i<j} \rho_{ij}(x_i - x_j)^2;\ \rho_i \geqslant 0,\ \rho_{ij} \geqslant 0 \right\}.$$

This was called the principal cone by Voronoi. When $n = 2, 3$, all perfect forms are equivalent to $\phi_0(\mathbf{x})$ and hence all type I cones are equivalent to Δ_0.

The *Voronoi polyhedron* Π_f corresponding to a positive definite quadratic form f is defined as

$$\Pi_f = \{\mathbf{x} \mid f(\mathbf{x}) \leqslant f(\mathbf{x} - \boldsymbol{l}) \text{ for all integral } \boldsymbol{l}\}.$$

A given $\boldsymbol{l}$ defines a proper (i.e., $(n-1)$-dimensional) face of Π_f if and only if

$$f(\boldsymbol{l}) = \min_{\mathbf{x} \equiv \boldsymbol{l} (\mathrm{mod}\ 2)} f(\mathbf{x})$$

and this minimum is attained only at $\mathbf{x} = \pm\boldsymbol{l}$. Let S be the set of such $\boldsymbol{l}$. We call such $\boldsymbol{l}$ *unique* mod 2 *minima* of f.

Π_f is called *primitive* if each vertex lies on exactly n proper faces of Π_f. Thus for each vertex of Π_f there corresponds an n-subset of S. When Π_f is *primitive*, $|S| = 2(2^n - 1)$, and hence we have $2^n - 1$ pairs of opposite parallel faces.

Two primitive polyhedra are of the same type if the set S and the n-subsets of S corresponding to the vertices are the same for each. Voronoi showed that the set of all forms corresponding to a particular type of primitive polyhedra is the interior of a polyhedral cone in the space of positive forms with vertex the origin. All such cones form a partition of the space of positive forms again with the properties outlined above and this was Voronoi's second method. We will call these cones *type* II *cones*.

It should be noted that although all forms in the interior of a given cone have the same set S of unique mod 2 minima, the set S does not completely specify the cone as it is possible for neighboring cones to have the same set S but the subsets corresponding to the vertices are different in each cone.

Voronoi's algorithm for finding the type II cones is very cumbersome and these cones are only known completely for $n \leqslant 4$ but the known results are very similar to the results for the partition into type I cones.

Voronoi showed the following:

(i) The cone Δ_0 is also a type II cone for all n and hence when $n = 2, 3$ the two sets of cones are identical.

(ii) When $n = 4$, there are two equivalence classes of type I cones and three classes of type II cones. Let Δ_0, Δ_1 and Δ_0, Δ_1', Δ_1'' be representatives of these classes. Then Δ_1 may be partitioned into cones each of which is equivalent to Δ_1', Δ_1''. Thus the second partition is a refinement of the first.

Reduction of quadratic forms using type II cones is extremely important in lattice covering problems [1, 2] and if it were true that in general the partition into type II cones is a refinement of the partition into type I cones then it would provide a simpler way of finding the inequivalent type II cones for $n > 4$.

In this paper we prove the following

THEOREM 1. *Let* $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_s$ *be* s *primitive integral vectors which span* R_n *and let*

$$\Delta = \left\{ f \mid f(\mathbf{x}) = \sum_{k=1}^{s} \rho_k (\mathbf{m}_k' \mathbf{x})^2;\ \rho_k > 0\ (k = 1, \ldots, s) \right\}.$$

Then $\mathbf{l}$ *is a unique* mod 2 *minimum of* Δ *(i.e., for all* f *in* Δ*) if and only if*

$$|\mathbf{m}_k'\mathbf{l}| \leqslant 1 \qquad \text{for all} \quad k = 1,..., s,$$

and there does not exist an integral $\mathbf{a} \neq \pm\mathbf{l}$ *such that*

$$|\mathbf{m}_k'\mathbf{a}| \leqslant |\mathbf{m}_k'\mathbf{l}| \qquad \text{for all} \quad k = 1,..., s.$$

Further, if Δ *has* $2^n - 1$ *pairs of unique* mod 2 *minima then* $S \leqslant \frac{1}{2}n(n+1)$ *with equality only when* Δ *is equivalent under integral unimodular transformation to* Δ_0.

THEOREM 2. *The only cones of positive definite quadratic forms which are both type* I *and type* II *cones are those equivalent to* Δ_0, *the principal cone.*

2. In this section we prove three combinatorial lemmas necessary for the proof of Theorem 1.

We will be concerned in these lemmas with ordered n-tuples of 0's and 1's and also ordered n-tuples of 0's and ± 1's which we will call $(0, 1)n$*-vectors* and $(0, \pm 1)n$*-vectors*, respectively.

If $\mathbf{a} = (a_1, a_2,..., a_n)$ is any n-vector we will denote by $\mathbf{a}^*$ the $(n-1)$-vector $(a_1, a_2,..., a_{n-1})$ and $\mathbf{a}$ is any $(0, \pm 1)n$-vector denote by $\mathbf{a}^+$ the $(0, 1)n$-vector obtained by replacing all -1's by 1's.

LEMMA 1. *Let* n, k *be positive integers with* $k \leqslant n$ *and*

$$A = \{(i_1, i_2,..., i_k) \mid 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n\}.$$

Let ϕ *be any mapping from* A *to the set of all* $(0, 1)k$*-vectors.*

Let B *be the set of* $(0, 1)n$*-vectors* $\mathbf{x}$ *satisfying the property that for all* $(i_1, i_2,..., i_k) \in A$ *the ordered* k *tuple of entries in* $\mathbf{x}$ *in the* $i_1, i_2,..., i_k$*-th positions is not* $\phi(i_1, i_2,..., i_k)$ *(i.e., we are forming* $(0, 1)n$*-vectors and for each* k *positions there is a "forbidden" set of entries).*

Then

$$|B| \leqslant \sum_{i=0}^{k-1} \binom{n}{i}.$$

Proof. Let S be the set of all (a, b) such that the result is true when $k = a, n = b$.

It is easily seen that $(1, n) \in S$ and $(n, n) \in S$ for all positive integers n.

We will assume that $(k-1, n-1) \in S$ and $(k, n-1) \in S$ where k, n are positive integers such that $k \leqslant n - 1$ and show that this implies $(k, n) \in S$. This will give the required result by induction.

Let

$$B^* = \{\mathbf{b}^* \mid \mathbf{b} \in B\}.$$

As $(k, n-1) \in S$, then

$$|B^*| \leqslant \sum_{i=0}^{k-1} \binom{n-1}{i}.$$

Now, given any $\mathbf{b}^* \in B^*$, this may arise from either one or two possible $\mathbf{b} \in B$ (n-th position may be 0 or 1). Let C be the set of all $\mathbf{b}^*$ in B^* arising from two vectors in B. So $|B| = |B^*| + |C|$.

Consider all $\phi\ (i_1, i_2, i_3, \ldots, i_{k-1}, n)$ where $1 \leqslant i_1 < i_2 < \cdots < i_{k-1} \leqslant n-1$. These must differ with each vector in C in at least one of the $i_1, i_2, \ldots, i_{k-1}$ positions and so, as $(k-1, n-1) \in S$,

$$|C| \leqslant \sum_{i=0}^{k-2} \binom{n-1}{i} = \sum_{i=1}^{k-1} \binom{n-1}{i-1}.$$

Thus

$$|B| \leqslant \sum_{i=0}^{k-1} \binom{n-1}{i} + \sum_{i=1}^{k-1} \binom{n-1}{i-1} = \sum_{i=0}^{k-1} \binom{n}{i},$$

which is the required result.

We see that if B is maximal, i.e., equality holds, then B^* and C are maximal.

We shall only use this lemma for $k = 2, 3$ but for the sake of completeness we have proved the more general result.

We note that

(i) if $k = 2$ then $|B| \leqslant n + 1$,

(ii) if $k = 3$ then $|B| \leqslant \frac{1}{2}n(n+1) + 1$.

We note also that this upper bound can be easily realized if we take any $(0, 1)n$-vector $\mathbf{x}$ and choose $\phi(i_1, \ldots, i_k)$ to be the $(0, 1)k$-vector of entries in the $i_1, i_2, \ldots, i_k$-th positions in $\mathbf{x}$, i.e., all $\phi(i_1, \ldots, i_k)$ will agree in common positions.

However, it is possible for B to be maximal in other situations, too. For instance, if $k = 2$, $n = 4$, $\phi(1, 2) = (1, 1)$, $\phi(1, 3) = (1, 1)$, $\phi(1, 4) = (0, 1)$, $\phi(2, 3) = (0, 1)$, $\phi(2, 4) = (1, 1)$, $\phi(3, 4) = (1, 1)$, then

$$B = \{(1, 0, 0, 0), (0, 0, 0, 0), (0, 1, 0, 0), (1, 0, 0, 1), (0, 1, 1, 0)\},$$

and B is maximal.

LEMMA 2. *If, in Lemma* 1, $k = 2$, B *is maximal and contains* $\mathbf{0}$ *(say* $B = \{\mathbf{0}, \boldsymbol{l}_1, ..., \boldsymbol{l}_n\}$*), then*

$$\det[\boldsymbol{l}_1, ..., \boldsymbol{l}_n] = \pm 1.$$

Proof. We will prove by induction.

When $n = 2$, the result is easily verified.

Consider now $n > 2$. We see that, by the argument in the proof of Lemma 1, $|B^*| = n$ and also $|C| = 1$, i.e., there is exactly one pair $\mathbf{b}_1, \mathbf{b}_2 \in B$ such that $\mathbf{b}_1^* = \mathbf{b}_2^*$. We must consider two cases.

Case (i). $\mathbf{0} \in \{\mathbf{b}_1, \mathbf{b}_2\}$. Without loss of generality let $\{\mathbf{b}_1, \mathbf{b}_2\} = \{\mathbf{0}, \boldsymbol{l}_1\}$ Then $\boldsymbol{l}_1^* = \mathbf{0}^*$ and

$$\det[\boldsymbol{l}_1, \boldsymbol{l}_2, ..., \boldsymbol{l}_n] = \begin{vmatrix} \mathbf{0}^* & \boldsymbol{l}_2^* & \boldsymbol{l}_3^* & & \boldsymbol{l}_n^* \\ 1 & a_2 & a_3 & & a_n \end{vmatrix}$$

where the a_i are 0 or 1.

Now $B^* = \{\mathbf{0}^*, \boldsymbol{l}_2^*, \boldsymbol{l}_3^*, ..., \boldsymbol{l}_n^*\}$ is maximal set of (0, 1) $(n-1)$ vectors and by induction hypothesis

$$\det[\boldsymbol{l}_2^*, ..., \boldsymbol{l}_n^*] = \pm 1$$

and result follows

Case (ii). $\mathbf{0} \notin \{\mathbf{b}_1, \mathbf{b}_2\}$. Without loss of generality, let $\{\mathbf{b}_1, \mathbf{b}_2\} = \{\boldsymbol{l}_1, \boldsymbol{l}_2\}$. Then

$$\det[\boldsymbol{l}_1, ..., \boldsymbol{l}_n] = \pm \begin{vmatrix} \boldsymbol{l}_1^* & \boldsymbol{l}_1^* & \boldsymbol{l}_3^* & \boldsymbol{l}_4^* & & \boldsymbol{l}_n^* \\ 1 & 0 & a_3 & a_4 & & a_n \end{vmatrix},$$

where the a_i are 0 or 1.

Now $B^* = \{\mathbf{0}^*, \boldsymbol{l}_1^*, \boldsymbol{l}_3^*, \boldsymbol{l}_4^*, ..., \boldsymbol{l}_n^*\}$ is maximal set of (0, 1) $(n-1)$ vectors and by induction hypothesis result again follows.

LEMMA 3. *Let* A *be a set of* $(0, \pm 1)n$*-vectors* $(\neq \mathbf{0})$ *such that no two members of* A *are congruent modulo* 2 *and* $|A| = 2^n - 1$ *(i.e., containing a representative of each nonzero congruence class).*

Let B *be a set of* $(0, \pm 1)n$*-vectors* $\mathbf{b}$ *for which* $|\mathbf{a}'\mathbf{b}| \leqslant 1$ *for all* $\mathbf{a} \in A$*, including in* B *at most one of each pair* $\pm\mathbf{b}$*. Then* $|B| \leqslant \frac{1}{2}n(n+1) + 1$.

Proof. We will prove by induction. The case $n = 2$ is easily verified.

For $n > 2$, choose any 3 integers h, i, j such that $1 \leqslant h < i < j \leqslant n$.

Let there exist 4 vectors $\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$, $\mathbf{b}_4$ in B such that the entries in the h-, i-, j-th positions in $\mathbf{b}_1^+$, $\mathbf{b}_2^+$, $\mathbf{b}_3^+$, $\mathbf{b}_4^+$ are, respectively, (0, 1, 1), (1, 0, 1), (1, 1, 0), (1, 1, 1).

Let $\mathbf{a} \in A$ be nonzero only in h-, i-, j-th positions. Without loss of generality we can assume these entries are all 1 (we can change sign in a particular position in all vectors in A and B without affecting hypothesis).

Referring only to the h-, i-, j-th positions we must have, as $|\mathbf{a}'\mathbf{b}_i| \leqslant 1$ for all i, $\mathbf{a} = (1, 1, 1)$, $\mathbf{b}_1 = \pm(0, 1, -1)$, $\mathbf{b}_2 = \pm(1, 0, -1)$, $\mathbf{b}_3 = \pm(1, -1, 0)$. $\mathbf{b}_4$ must have 2 entries of one sign and the other opposite in sign. Without loss of generality we may assume $\mathbf{b}_4 = \pm(1, 1, -1)$.

Now consider $\mathbf{a}_1 \in A$ which is nonzero only in h- and i-th positions. As $|\mathbf{a}_1'\mathbf{b}_4| \leqslant 1$, then $\mathbf{a}_1 = \pm(1, -1, 0)$ but then $|\mathbf{a}_1'\mathbf{b}_3| = 2$ which is a contradiction.

Thus there is a (0, 1)3-vector which does not appear in the h-, i-, j-th positions in any $\mathbf{b}^+$ where $\mathbf{b} \in B$ and this 3-vector has at least two nonzero entries. As this is true for all choices of h, i, j, then B^+ satisfies the conditions of Lemma 1 with $k = 3$, where

$$B^+ = \{\mathbf{b}^+ \mid \mathbf{b} \in B\}.$$

Thus

$$|B^+| \leqslant \tfrac{1}{2}n(n+1) + 1.$$

Assume B contains two vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ such that $\mathbf{b}_1^+ = \mathbf{b}_2^+$. Then $\mathbf{b}_1 \equiv \mathbf{b}_2 \pmod 2$. As $\mathbf{b}_1 \neq \pm\mathbf{b}_2$, there exists i, j such that $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, the i-th and j-th entries in $\mathbf{b}_1$ and $\mathbf{b}_2$ are all nonzero, the i-th entries being of the same sign and the j-th entries of opposite sign. Choose $\mathbf{a}$ as the vector in A which is nonzero in only the i-th and j-th position. Then we cannot have

$$|\mathbf{a}'\mathbf{b}_1| \leqslant 1 \qquad \text{and} \qquad |\mathbf{a}'\mathbf{b}_2| \leqslant 1,$$

which contradicts hypothesis.

Thus B contains no two vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ such that $\mathbf{b}_1^+ = \mathbf{b}_2^+$. So

$$|B| = |B^+| \leqslant \tfrac{1}{2}n(n+1) + 1.$$

LEMMA 4. *If equality holds in Lemma* 3, *then after replacing* $\mathbf{b}$ *by* $-\mathbf{b}$ *for some* $\mathbf{b} \in B$ *if necessary, there exists an integral unimodular transformation* T *such that*

$$TB = D_n = \{\mathbf{e}_i \mid i = 1,\ldots, n\} \cup \{\mathbf{e}_i - \mathbf{e}_j \mid 1 \leqslant i < j \leqslant n\} \cup \{0\},$$

where $\mathbf{e}_i$ *is vector with* 1 *in* i*-th position and* 0 *elsewhere.*

Proof. We note firstly that we can replace any vector in A or B by its negative without affecting the conditions of the Lemma and we will in fact do this throughout the proof without any further comment.

We will again prove by induction.

The result is easily shown for $n = 2$ as there is essentially only two possible A and these are easily checked.

Consider now $n > 2$. B^+ satisfies conditions of Lemma 1 with $k = 3$ and $|B^+|$ is maximum possible, so from the statement at the end of Lemma 1, we have

(i) B^{+*} is maximal and $|B^{+*}| = |B^*| = \frac{1}{2}n(n-1) + 1$ and

(ii) if C is the set of vectors $\mathbf{b}^* \in B^*$ arising from two vectors in B then C^+ is maximal and $|C^+| = |C| = n$.

Obviously $\mathbf{0}, \mathbf{e}_n$ belong to B so $\mathbf{0} \in C$.

Let

$$C = \{\mathbf{0}, \boldsymbol{l}_1^*, \boldsymbol{l}_2^*, \ldots, \boldsymbol{l}_{n-1}^*\}.$$

By Lemma 2,

$$\det[\boldsymbol{l}_1^{+*}, \boldsymbol{l}_2^{+*}, \ldots, \boldsymbol{l}_{n-1}^{+*}] = \pm 1.$$

Consider now $\det[\boldsymbol{l}_1^*, \boldsymbol{l}_2^*, \ldots, \boldsymbol{l}_{n-1}^*]$. Expanding this determinant fully this must have the same number of nonzero terms as $\det[\boldsymbol{l}_1^{+*}, \boldsymbol{l}_2^{+*}, \ldots, \boldsymbol{l}_{n-1}^{+*}]$ which are all ± 1. There must be an odd number of such terms and hence $\det[\boldsymbol{l}_1^*, \boldsymbol{l}_2^*, \ldots, \boldsymbol{l}_{n-1}^*] \neq 0$ making $\{\boldsymbol{l}_1^*, \boldsymbol{l}_2^*, \ldots, \boldsymbol{l}_{n-1}^*\}$ linearly independent.

Let $A = A' \cup A''$ where A' is the set of all vectors in A with 0 in the n-th position and A'' the set of those with ± 1 in n-th position.

Now A'^* and B^* obviously satisfy the conditions of Lemma 3 with B^* of maximum cardinality so by the induction hypothesis there exists an integral unimodular transformation U^* on R_{n-1} such that $U^*B^* = D_{n-1}$.

Examination of D_{n-1} shows that the determinant of any $(n-1)$ linearly independent vectors in U^*B^* is ± 1 so there exists an integral unimodular transformation W^* such that

$$W^*U^*\boldsymbol{l}_i^* = \mathbf{e}_i^* \qquad (i = 1, \ldots, n-1).$$

Let U be the transformation on R_n which leaves the n-th coordinate fixed and whose action on the first $(n-1)$ coordinates is W^*U^* and consider UB. UB will contain $\mathbf{0}, \mathbf{e}_i$ $(i = 1, \ldots, n)$ and $\mathbf{e}_i + \mathbf{h}_i$ $(i = 1, \ldots, n-1)$ where $\mathbf{h}_i$ is either $\mathbf{e}_n$ or $-\mathbf{e}_n$.

Applying integral unimodular transformation

$$x_n \to x_n - x_i$$
$$x_j \to x_j \qquad (j \neq n),$$

if necessary, we may ensure that $\mathbf{h}_i = -\mathbf{e}_n$ for all i. So we may assume UB contains $\mathbf{0}$, $\mathbf{e}_i$ $(i = 1,..., n)$ and $\mathbf{e}_i - \mathbf{e}_n$ $(i = 1,..., n-1)$.

Consider now $(U^{-1})'A$. As $|((U^{-1})'\mathbf{a})'(U\mathbf{b})| = |\mathbf{a}'\mathbf{b}|$ and $\boldsymbol{l}_i \in UB$ for all i then all vectors in $(U^{-1})'A$ are $(0, \pm 1)n$-vectors. We note also that $(U^{-1})'\mathbf{a}_i \equiv (U^{-1})'\mathbf{a}_2 \pmod 2 \Rightarrow \mathbf{a}_1 \equiv \mathbf{a}_2 \pmod 2$ as $(U^{-1})'$ is integral unimodular. So $(U^{-1})'A$ and UB satisfy conditions of Lemma 3 with UB of maximum cardinality. For the rest of the proof let us just refer to these as A and B respectively.

We now make extensive use of the fact that $|\mathbf{a}'\mathbf{b}| \leqslant 1$ for all $\mathbf{a} \in A$ and $\mathbf{b} \in B$ to determine the possibilities for the remaining vectors of B and the vectors of A.

As B contains $\mathbf{e}_i - \mathbf{e}_n$ $(i = 1,..., n)$ then the vectors of A'' will have all nonzero elements of the same sign. Without loss of generality we assume they are all 1. Consider now the remaining vectors in B. These will be $\frac{1}{2}(n-1)(n-2)$ of them. Using the vectors of A'' we find they must be of two types. If they are nonzero in the n-th position then they are of the form $\mathbf{e}_n - \mathbf{e}_i - \mathbf{e}_j$, where $1 \leqslant i < j \leqslant n-1$. If they are zero in the n-th position they are of the form $\mathbf{e}_i - \mathbf{e}_j$, where $1 \leqslant i < j \leqslant n-1$. Considering now a vector in A' which is nonzero in the i-th and j-th positions we see that we cannot have both of the above for a given i, j. As the number of choices for i, j is $\frac{1}{2}(n-1)(n-2)$ then we have exactly one of these for a given i, j.

Let i, j, k be any integers between 1 and $n-1$. By considering a vector in A' which is nonzero in i-th, j-th and k-th positions we see that

(i) $\mathbf{e}_n - \mathbf{e}_i - \mathbf{e}_j \in B$, $\mathbf{e}_n - \mathbf{e}_j - \mathbf{e}_k \in B \Rightarrow \mathbf{e}_n - \mathbf{e}_i - \mathbf{e}_k \notin B$,

(ii) $\mathbf{e}_i - \mathbf{e}_j \in B$, $\mathbf{e}_j - \mathbf{e}_k \in B \Rightarrow \mathbf{e}_n - \mathbf{e}_i - \mathbf{e}_k \notin B$.

Thus the set $\{1, 2,..., n-1\}$ partitions into two subsets S_1 and S_2 such that for any $i, j \in \{1, 2,..., n-1\}$,

(i) $i \in S_1$, $j \in S_1 \Rightarrow \mathbf{e}_n - \mathbf{e}_i - \mathbf{e}_j \notin B$,

(ii) $i \in S_2$, $j \in S_2 \Rightarrow \mathbf{e}_n - \mathbf{e}_i - \mathbf{e}_j \notin B$,

(iii) $i \in S_1$, $j \in S_2 \Rightarrow \mathbf{e}_i - \mathbf{e}_j \notin B$.

We can easily see now that the transformation

$$\begin{aligned} x_i &\to -x_i, && i \in S_1, \\ x_i &\to x_i, && i \in S_2, \\ x_n &\to x_n + \sum_{i \in S_1} x_i, \end{aligned}$$

transforms B into D_n and our proof is complete.

3. We now prove the theorems stated in Section 1.

Proof of Theorem 1. If $\boldsymbol{l}$ is a unique mod 2 minima for all f in Δ then $f(\boldsymbol{l}) < f(\boldsymbol{l} + 2\mathbf{a})$ for all integral $\mathbf{a} \neq -\boldsymbol{l}$ and for all f in Δ. This means that

$$\sum_{k=1}^{s} \rho_k(\mathbf{m}_k'\boldsymbol{l})^2 < \sum_{k=1}^{s} \rho_k(\mathbf{m}_k'(\boldsymbol{l} + 2\mathbf{a}))^2$$

for all integral $\mathbf{a} \neq -\boldsymbol{l}$ and all $\rho_i > 0$.

Now this is true if and only if, for each $k = 1,..., s$,

$$(\mathbf{m}_k'\boldsymbol{l})^2 \leqslant (\mathbf{m}_k'(\boldsymbol{l} + 2\mathbf{a}))^2 \qquad \text{for all } \mathbf{a} \tag{1}$$

and for each $\mathbf{a} \neq -\boldsymbol{l}$ there is strict inequality for at least one k.

Now (1) is equivalent to

$$(\mathbf{m}_k'\mathbf{a})^2 \geqslant -(\mathbf{m}_k'\boldsymbol{l})(\mathbf{m}_k'\mathbf{a}) \qquad \text{for all } \mathbf{a},$$

i.e.,

$$(\mathbf{m}_k'\mathbf{a})^2 \geqslant |(\mathbf{m}_k'\boldsymbol{l})(\mathbf{m}_k'\mathbf{a})| \qquad \text{for all } \mathbf{a} \tag{2}$$

(making use of both $\pm\mathbf{a}$) and this is equivalent to

$$|\, \mathbf{m}_k'\boldsymbol{l} \,| \leqslant 1$$

as $\mathbf{m}_k$ is primitive and we can choose $\mathbf{a}$ such that $\mathbf{m}_k'\mathbf{a} = 1$.

If for some $\mathbf{a}$ there is strict inequality in (1) and hence also 2 we see that

(i) $|\, \mathbf{m}_k'\boldsymbol{l} \,| = 1 \Rightarrow |\, \mathbf{m}_k'\mathbf{a} \,| \neq 0, 1,$

(ii) $|\, \mathbf{m}_k'\boldsymbol{l} \,| = 0 \Rightarrow |\, \mathbf{m}_k'\mathbf{a} \,| \neq 0,$

and so $|\, \mathbf{m}_k'\mathbf{a} \,| > |\, \mathbf{m}_k'\boldsymbol{l} \,|$ and this is obviously sufficient for strict inequality.

This gives us the first part of our theorem.

For the second part, let $S = \{\pm\boldsymbol{l}_i \mid i = 1,..., 2^n - 1\}$ be the set of unique mod 2 minima of Δ and let $\mathbf{m}_1,..., \mathbf{m}_n$ be linearly independent.

Let $\boldsymbol{l}_i, \boldsymbol{l}_j \in S(\boldsymbol{l}_i \neq \pm\boldsymbol{l}_j)$ be such that

$$|\, \mathbf{m}_k'\boldsymbol{l}_i \,| = |\, \mathbf{m}_k'\boldsymbol{l}_j \,| \qquad \text{for all } \; k = 1,..., n.$$

Then

$$\mathbf{m}_k'\boldsymbol{l}_i \equiv \mathbf{m}_k'\boldsymbol{l}_j \pmod 2,$$

i.e.,

$$\mathbf{m}_k'(\boldsymbol{l}_i - \boldsymbol{l}_j) \equiv 0 \pmod 2 \qquad \text{for all } \; k = 1,..., n.$$

So for all $\boldsymbol{l} \equiv \boldsymbol{l}_i - \boldsymbol{l}_j \pmod 2$ we have

$$\begin{aligned} \mathbf{m}_k'\boldsymbol{l} &= 2\mathbf{m}_k'\mathbf{a} + \mathbf{m}_k'(\boldsymbol{l}_i - \boldsymbol{l}_j) \qquad \text{for some integral } \mathbf{a} \\ &\equiv 0 \pmod 2. \end{aligned}$$

But at least one such $\boldsymbol{l}$ is in S and we have $|\ \mathbf{m}_k'\boldsymbol{l}\ | \leqslant 1$. This means $\boldsymbol{l} = \mathbf{0}$ which is a contradiction as $\boldsymbol{l}_i \not\equiv \boldsymbol{l}_j \pmod 2$.

So if we let

$$\mathbf{a}_j = (\mathbf{m}_1'\boldsymbol{l}_j\ ,\ \mathbf{m}_2'\boldsymbol{l}_j\ ,\ldots,\ \mathbf{m}_n'\boldsymbol{l}_j) \qquad (j = 1, 2,\ldots, 2^n - 1),$$

then we will have $2^n - 1$ different $\mathbf{a}_j^+$. Thus all possible $(0, 1)n$-vectors $(\neq \mathbf{0})$ will appear among the $\mathbf{a}_j^+$.

Without loss of generality we can let $\mathbf{a}_j^+ = \mathbf{e}_j$ $(j = 1, 2,\ldots, n)$. This implies that $|\det(\mathbf{m}_1\ ,\ \mathbf{m}_2\ ,\ldots,\ \mathbf{m}_n)| = 1$ and so if we let

$$\mathbf{m}_k = b_{k1}\mathbf{m}_1 + b_{k2}\mathbf{m}_2 + \cdots + b_{kn}\mathbf{m}_n \qquad (k = 1, 2,\ldots, s),$$

then all the b_{kj} are integers. Also, as $|\ b_{kj}\ | = |\ \mathbf{m}_k'\boldsymbol{l}_j\ |$ for all k and all $j = 1, 2,\ldots, n$, then we have $|\ b_{kj}\ | \leqslant 1$.

Let $\mathbf{b}_k = (b_{k1}\ ,\ b_{k2}\ ,\ldots,\ b_{kn})$ $(k = 1, 2,\ldots, s)$ and we have $|\ \mathbf{a}_j'\mathbf{b}_k\ | = |\ \mathbf{m}_k'\boldsymbol{l}_j\ | \leqslant 1$. Thus $A = \{\mathbf{a}_j \mid j = 1,\ldots, 2^n - 1\}$ and $B = \{\mathbf{b}_k \mid k = 1, 2,\ldots, s\}$ satisfy the conditions of Lemma 3 and $\mathbf{0} \notin B$ so

$$|\ B\ | = s \leqslant \tfrac{1}{2}n(n + 1).$$

If $s = \frac{1}{2}n(n + 1)$, then by Lemma 4 there exists an integral unimodular transformation such that B is transformed into $D_n - \{\mathbf{0}\}$. As $|\det(\mathbf{m}_1\ ,\ldots,\ \mathbf{m}_n)| = 1$, this means there exists an integral unimodular transformation taking $\{\mathbf{m}_1\ ,\ \mathbf{m}_2\ ,\ldots,\ \mathbf{m}_s\}$ into $D_n - \{\mathbf{0}\}$ and hence Δ is equivalent to Δ_0.

Proof of Theorem 2. Let Δ be a type I cone. Then

$$\Delta = \left\{ f \mid f(\mathbf{x}) = \sum_{k=1}^{s} \rho_k(\mathbf{m}_k'\mathbf{x})^2;\ \rho_k \geqslant 0 \right\},$$

where $s \geqslant \frac{1}{2}n(n + 1)$, $\mathbf{m}_k$ is a primitive integral vector for all k and $\{\mathbf{m}_1\ ,\ \mathbf{m}_2\ ,\ldots,\ \mathbf{m}_k\}$ spans R_n (otherwise the forms in the interior of Δ would not be positive definite).

Now if Δ is also a type II cone then the interior of Δ has $2^n - 1$ pairs of unique mod 2 minima and so by Theorem 1, $s = \frac{1}{2}n(n + 1)$ and Δ is equivalent to Δ_0, the principal cone.

References

1. E. S. Barnes and T. J. Dickson, Extreme coverings of n-space by spheres, *J. Aust. Math. Soc.* **7** (1967), 115–127.
2. T. J. Dickson, A sufficient condition for an extreme covering of n-space by spheres, *J. Aust. Math. Soc.* **8** (1968), 56–62.

3. G. VORONOI, Sur quelques propriétés des formes quadratique positives parfaites, *J. Reine Angew. Math.* **133** (1906), 97–178.
4. G. VORONOI, Recherches sur les paralléloèdres primitifs *J. Reine Angew. Math.* (Part I), **134** (1908), 198–287; (Part II) **136** (1909), 67–181.