Lattice polytopes with distinct pair-sums

M. D. Choi
University of Toronto
Toronto, M5S 3G3, Canada

T. Y. Lam
University of California
Berkeley, CA 94720

Bruce Reznick
University of Illinois
Urbana, IL 61801

May 29, 2001

Let $\mathcal{P}$ be a lattice polytope in $\mathbb{R}^n$, the convex hull of a finite set in $\mathbb{Z}^n$, and let

$$\mathcal{L}(\mathcal{P}) := \mathcal{P} \cap \mathbb{Z}^n = \{v_1, \dots, v_N\},$$

where $N = N(\mathcal{P}) := |\mathcal{L}(\mathcal{P})|$. Suppose the $N + \binom{N}{2}$ points in $\mathcal{L}(\mathcal{P}) + \mathcal{L}(\mathcal{P})$,

$$2v_1, \dots, 2v_N;\ v_1 + v_2,\ v_1 + v_3, \dots, v_{N-1} + v_N$$

are distinct. In this case, we say that $\mathcal{P}$ is a *distinct pair-sum* or *dps* polytope. Our interest in dps polytopes comes from the study of the representation of polynomials as a sum of squares of polynomials.

The following lemma offers two other geometrical characterizations of dps polytopes.

Lemma 1. *Let $\mathcal{P}$ be a lattice polytope. Then the following are equivalent:*
(1) *$\mathcal{L}(\mathcal{P})$ is a dps polytope.*
(2) *$\mathcal{L}(\mathcal{P})$ does not contain the vertices of a (nondegenerate) parallelogram, and does not contain three collinear points.*
(3) *Suppose $v \neq v'$ and $w \neq w'$ are in $\mathcal{L}(\mathcal{P})$. Then $v' - v$ and $w' - w$ are parallel only if $\{v, v'\} = \{w, w'\}$.*

Proof. (1) $\Rightarrow$ (2). Suppose $v_1, v_2, v_3, v_4 \in \mathcal{L}(\mathcal{P})$ are the vertices of a parallelogram. Then $v_1 - v_2 = v_3 - v_4$ implies $v_1 + v_4 = v_2 + v_3$, so that $\mathcal{P}$ is not dps. Now suppose $v_1, v_2, v_3 \in \mathcal{L}(\mathcal{P})$, and v_2 is interior to the line segment $\overline{v_1 v_3}$. If v_2 is the midpoint of the segment, then $v_2+v_2=v_1+v_3$, so $\mathcal{P}$ is not dps. Otherwise, we may assume that v_2 is closer to v_1 than to v_3. Then $v_4=v_2+(v_2-v_1)$ will also be a lattice point on the line segment $\overline{v_1v_3}$, and v_2 is the midpoint of $\overline{v_1v_4}$; again, $\mathcal{P}$ is not dps.

(2) $\Rightarrow$ (3). For $u\in\mathbb{Z}^n$, let $g(u)=\gcd(u_1,\ldots,u_n)$. Suppose $g(u'-u)=d>1$. Then $u'-u=du''$ for $u''\in\mathbb{Z}^n$, and the line segment $\overline{u\,u'}$ contains the lattice points u, $u+u''$, …, $u+du''=u'$. Thus, if (2) holds and $u,u'\in\mathcal{L}(\mathcal{P})$, $u\neq u'$, we have $g(u'-u)=1$. Suppose $w'-w=\alpha\cdot(v'-v)$. Then $\alpha=p/q$ for nonzero integers p, q, and $q(w'-w)=p(v'-v)$. Hence $|q|=g(q(w'-w))=g(p(v'-v))=|p|$, so $\alpha=\pm1$. Now the parallelogram condition in (2) implies that $\{v,v'\}=\{w,w'\}$.

(3) $\Rightarrow$ (1). If (3) holds for $\mathcal{P}$, and $v_i,v_j,v_k,v_\ell\in\mathcal{L}(\mathcal{P})$ with $i\notin\{k,\ell\}$, then $v_i-v_k\neq v_\ell-v_j$, and so $v_i+v_j\neq v_k+v_\ell$. This proves (1). $\square$

Our main results are these: if $\mathcal{P}$ in $\mathbb{R}^n$ is a dps polytope, then $N(\mathcal{P})\le 2^n$, and, for every n, we construct dps polytopes in $\mathbb{R}^n$ for which $N(\mathcal{P})=2^n$.

Example 1. Let $\mathcal{P}\subset\mathbb{R}^2$ be the triangle with vertices $\{(0,1),(1,2),(2,0)\}$. Then $\mathcal{P}$ is a dps polytope, because

$$\mathcal{L}(\mathcal{P})=\{(0,1),\ (1,2),\ (2,0),\ (1,1)\},$$

and

$$\mathcal{L}(\mathcal{P})+\mathcal{L}(\mathcal{P})=\{(0,2),(1,2),(1,3),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(4,0)\}.$$

We can view $\mathcal{P}$ as the projection onto the first two coordinates of the triangle with vertices $\{(0,1,2),(1,2,0),(2,0,1)\}$, which lies in the hyperplane $x_1+x_2+x_3=3$. (In this example, we could have just as well taken the triangle with vertices $\{(0,0),(1,2),(2,1)\}$; again, $\mathcal{L}(\mathcal{P})$ will consist of the vertices of $\mathcal{P}$ and $(1,1)$.)

Example 2. Let

$$\begin{aligned}\mathcal{A}&=\{(4,1,0,0),(0,4,1,0),(0,0,4,1),(1,0,0,4)\},\\ \mathcal{B}&=\{(2,1,1,1),(1,2,1,1),(1,1,2,1),(1,1,1,2)\};\end{aligned}$$

and let $\mathcal{P}=cvx(\mathcal{A}\cup\mathcal{B})\subset\mathbb{R}^4$ be the convex hull of $\mathcal{A}\cup\mathcal{B}$. By construction, $\mathcal{P}$ is cyclically symmetric with respect to its coordinates. It is not hard to show that $\mathcal{L}(\mathcal{P})=\mathcal{A}\cup\mathcal{B}$. Suppose $w=(w^{(1)},w^{(2)},w^{(3)},w^{(4)})\in\mathcal{L}(\mathcal{P})$. Since w is a convex combination of $\mathcal{A}\cup\mathcal{B}$, we have $w^{(i)}\ge 0$ and $\sum_i w^{(i)}=5$. If $w^{(i)}\ge 1$ for all i, then w must be a permutation of $(2,1,1,1)$ and so lies in $\mathcal{B}$. Otherwise, $w^{(i)}=0$ for some i, and by cycling the coordinates, we may assume that $w^{(1)}=0$. But then w must be a convex combination of $(0,4,1,0)$ and $(0,0,4,1)$ and so $w\in\mathcal{A}$. A routine check, which we omit, shows that the $8+\binom{8}{2}=36$ sums in $\mathcal{L}(\mathcal{P})+\mathcal{L}(\mathcal{P})$ are distinct. By projecting $\mathcal{P}$ onto its first three coordinates, we obtain a dps polytope in $\mathbb{R}^3$ with $N(\mathcal{P})=8$.

Theorem 2. *Suppose $\mathcal{P}$ is a dps polytope in $\mathbb{R}^n$. Then $N(\mathcal{P}) \leq 2^n$.*

Proof. If $N(\mathcal{P}) > 2^n$, then by the Pigeonhole Principle, there exist $v_i \neq v_j$ so that v_i and v_j are component-wise congruent modulo 2. This means that $v_k = \frac{1}{2}(v_i + v_j) = v_i + \frac{1}{2}(v_j - v_i)$ is also a lattice point, and it follows from Lemma 1 that $\mathcal{P}$ is not a dps polytope. $\square$

This argument is essentially the same one used to solve Putnam Problem 1971-A1 (see [**?**]): "Let there be given nine lattice points (points with integral coordinates) in three dimensional Euclidean space. Show that there is a lattice point on the interior of one of the line segments joining two of these points." The proof of Theorem 2 also applies to the less restrictive class of convex polytopes which do not contain three lattice points on a line. One such polytope is the n-cube $\mathcal{C}_n = \{0,1\}^n$, which has many lattice parallelograms.

We shall say that a dps polytope $\mathcal{P} \subset \mathbb{R}^n$ for which $N(\mathcal{P}) = 2^n$ is *maximal.* The proof of Theorem 2 implies that no two points in a dps polytope are component-wise congruent modulo 2; hence a maximal dps polytope contains one representative from every congruence class modulo 2 (and at most one representative from every congruence class modulo m, $m \geq 3$).

Suppose M is an $n \times n$ unimodular matrix with integer entries. Then M defines a linear mapping on $\mathbb{R}^n$ (viewed as column vectors) by matrix multiplication. Since linear mappings preserve inclusions and both M and M^{-1} have integer entries, it is easy to see that $\mathcal{L}(M(\mathcal{P})) = M(\mathcal{L}(\mathcal{P}))$ for any lattice polytope $\mathcal{P}$, and since linear mappings preserve sums, it is then clear that $\mathcal{P}$ is dps if and only if $M(\mathcal{P})$ is dps.

Theorem 3. *There exist maximal dps polytopes in $\mathbb{R}^n$ for every n.*

Proof. For $n = 1$, let $\mathcal{P} = [0,1]$; for $n = 2, 3$, consider Examples 1 and 2. Suppose now that $\mathcal{P}$ is a maximal dps polytope in $\mathbb{R}^n$, $n \geq 3$. Write $\mathcal{L} = \mathcal{L}(\mathcal{P})$ and define the (finite) set of differences

$$\mathcal{D} = (\mathcal{L} - \mathcal{L})^* := \{v - v' : \, v, v' \in \mathcal{L}, \, v \neq v'\}.$$

Let M be a unimodular integer matrix such that if $u \in \mathcal{D}$, then $M(u) \notin \mathcal{D}$. (We shall construct such an M below.)

We define the polytope $\mathcal{P}'$ in $\mathbb{R}^{n+1}$ as follows. Let

$$\mathcal{A} = \{(v, 0) \in \mathbb{R}^{n+1} : v \in \mathcal{L}(\mathcal{P})\}, \qquad \mathcal{B} = \{(M(v), 1) \in \mathbb{R}^{n+1} : v \in \mathcal{L}(\mathcal{P})\},$$

and let $\mathcal{P}' = cvx(\mathcal{A} \cup \mathcal{B})$. If $w = (w^{(1)}, \ldots, w^{(n+1)}) \in \mathcal{L}(\mathcal{P}')$, then $0 \leq w^{(n+1)} \leq 1$, hence $w^{(n+1)}$ equals 0 or 1. Thus, w lies either on the face determined by $\mathcal{A}$, in which case $w = (v, 0)$, or on the face determined by $\mathcal{B}$, in which case $w = (M(v), 1)$. It follows that $\mathcal{L}(\mathcal{P}') = \mathcal{A} \cup \mathcal{B}$, so $N(\mathcal{P}') = 2^{n+1}$.

Now consider $\mathcal{L}(\mathcal{P}') + \mathcal{L}(\mathcal{P}')$; this consists of three disjoint sets of points:

$$\{(v_i, 0) + (v_j, 0)\}, \qquad \{(v_i, 0) + (M(v_j), 1)\}, \qquad \{(M(v_i), 1) + (M(v_j), 1)\},$$

where $v_i, v_j \in \mathcal{L}(\mathcal{P})$. Since both $\mathcal{P}$ and $M(\mathcal{P})$ are dps, the sums in the first and the third set are distinct. For the second set, we suppose that

$$(v_i, 0) + (M(v_j), 1) = (v_k, 0) + (M(v_\ell), 1), \tag{1}$$

or equivalently,

$$v_i - v_k = M(v_\ell) - M(v_j) = M(v_\ell - v_j).$$

If $j = \ell$, then $v_i - v_k = 0$, so $i = k$, which is the only possible way for (**??**) to hold in a dps polytope. Otherwise, $j \neq \ell$, so $M(v_\ell - v_j) = v_i - v_k \in \mathcal{D}$, a contradiction to the choice of M. Thus, $\mathcal{P}'$ is a maximal dps polytope in $\mathbb{R}^{n+1}$.

We now construct a matrix M with the desired properties. First, let

$$R = \max\{|u_j^{(k)}| : u_j \in \mathcal{D},\ 1 \leq k \leq n\}.$$

and let M be the $n \times n$ matrix given below:

$$M = \begin{pmatrix} 1+(R+1)^2 & R+1 & 0 & 0 & \dots & 0 & 0 \\ R+1 & 1 & R+1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & R+1 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 1 & R+1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

(In words, the only non-zero entries in M are the diagonal, the superdiagonal, and the first entry in the second row.) It is easy to see that M is unimodular.

We show now that for every $u \in \mathcal{D}$, at least one entry of $w = M(u)$ has absolute value greater than R. This implies that $M(u) \notin \mathcal{D}$, and will complete the proof. Write $u = (u^{(1)}, \dots, u^{(n)})$ and suppose that k is the smallest index such that $u^{(k)} \neq 0$. (Such an index exists because $0 \notin \mathcal{D}$.)

If $k = 1$, then $w^{(1)} = (1 + (R+1)^2)u^{(1)} + (R+1)u^{(2)}$, and hence

$$|w^{(1)}| \geq |(1 + (R+1)^2)u^{(1)}| - (R+1)|u^{(2)}| \geq 1 + (R+1)^2 - R(R+1) = R + 2.$$

If $k \geq 2$, then $u^{(1)} = \dots = u^{(k-1)} = 0$, so $w^{(k-1)} = (R+1)u^{(k)}$ and $|w^{(k-1)}| \geq R+1$. Finally, we remark that the same proof applies in the case $n = 2$, if we take as our matrix the 2×2 submatrix at the upper left of M. $\square$

Example 3. We illustrate the last construction by applying it to the polytope in Example 1, for which

$$\mathcal{D} = \{\pm(0,1), \pm(1,-2), \pm(1,-1), \pm(1,0), \pm(1,1), \pm(2,-1)\},$$

so $R = 2$ and

$$M = \begin{pmatrix} 10 & 3 \\ 3 & 1 \end{pmatrix}.$$

Thus, $cvx(\mathcal{A}\cup\mathcal{B})$ is a maximal dps polytope in $\mathbb{R}^3$, where

$$\mathcal{A} = \{(0,1,0),(1,1,0),(1,2,0),(2,0,0)\},$$
$$\mathcal{B} = \{(3,1,1),(13,4,1),(16,5,1),(20,6,1)\}.$$

We could now apply the shear $(x_1,x_2,x_3)\mapsto(x_1-3x_2-5x_3+5, x_2-x_3, x_3)$, which maps $\mathcal{A}$ and $\mathcal{B}$ to

$$\mathcal{A}' := \{(2,1,0),(3,1,0),(0,2,0),(7,0,0)\}$$

and

$$\mathcal{B}' := \{(0,0,1),(1,3,1),(1,4,1),(2,5,1)\},$$

respectively, in order to reduce the magnitude of the coordinates in the example.

Since any translate of a dps polytope is also dps, we may always assume, as we have done in the examples, that $\mathcal{P}$ lies in the non-negative orthant of $\mathbb{R}^n$. In this case, we define $s(\mathcal{P})$, the *size* of $\mathcal{P}$:

$$s(\mathcal{P}) = \max\{v_j^{(1)}+\cdots+v_j^{(n)} :\ v_j\in\mathcal{L}(\mathcal{P})\}.$$

If $s = s(\mathcal{P})$, then $\mathcal{P}$ can be viewed as a projection onto the first n coordinates of a polytope in $\mathbb{R}^{n+1}$ which lies in the simplex

$$\Delta_{n+1}(s) := \{u = (u^{(1)},\ldots,u^{(n+1)}) :\ u^{(i)}\geq 0,\ \sum_{i=1}^{n+1} u^{(i)} = s\}.$$

Let s_n denote the minimum size of any maximal dps polytope in $\mathbb{R}^n$. Examples 1 and 2 show that $s_2\leq 3$ and $s_3\leq 5$. It is not difficult to show that these estimates are sharp. The first case can be done by hand: if $\mathcal{P}$ is a maximal dps polytope with size 2 in $\mathbb{R}^2$, then $\mathcal{L}(\mathcal{P})$ must consist of four points chosen from

$$\{(0,0),(0,1),(0,2),(1,0),(1,1),(2,0)\}.$$

Since each congruence class is represented in $\mathcal{L}(\mathcal{P})$, it must contain $(0,1)$, $(1,0)$ and $(1,1)$. These three points form a parallelogram with each of the points $(0,0)$, $(0,2)$ and $(2,0)$. Hence no fourth point can exist in $\mathcal{L}(\mathcal{P})$ while preserving the dps property. The second case is similar, but much more complicated. Computer-aided calculations can be used to conclude that no dps polytope in $\mathbb{R}^3$ has size 4 or less. (We thank Dr. Bruce Carpenter for doing the Mathematica coding.)

It can also be shown, using the style of argument of [?, Ch. 3], that every maximal dps polytope in $\mathbb{R}^2$ is the image of the triangle in Example 1 under an affine unimodular linear mapping, and consists of a triangle with area 3/2, and a single lattice point inside, which will always be the centroid of the triangle. The tetrahedron determined by $\mathcal{B}$ in Example 2 lies within the tetrahedron determined by $\mathcal{A}$, whereas in Example 3, each point in $\mathcal{L}$ is on the boundary of the polytope.

Thus there are at least two distinct combinatorial types of maximal dps polytopes in $\mathbb{R}^3$.

We make no serious conjecture about the growth of s_n. On the one hand, any maximal dps polytope must contain a lattice point with odd coordinates, so $s_n \geq n$. In the other direction, it is not difficult to use the proof of Theorem 3 to obtain a doubly-exponential bound for s_n. Since this bound is likely to be very crude, we do not present it explicitly. Another open question is to determine the minimum volume of a maximal dps polytope in $\mathbb{R}^n$ for $n \geq 3$. We also do not know the answer to the following question: is every dps polytope a subset of a maximal dps polytope?"

We now discuss our original interest in this subject. Given $u \in \mathbb{Z}_+^n$, define the monomial $x^u \in \mathbb{R}[x_1, \ldots, x_n]$ by

$$x^u = x_1^{u(1)} \ldots x_n^{u(n)}.$$

Suppose $\mathcal{U} \subseteq \mathbb{Z}_+^n$ and consider the polynomial

$$p(x_1, \ldots, x_n) = \sum_{u \in \mathcal{U}} b_u x^u.$$

In [?], the present authors developed an algorithm for determining whether p can be written as a sum of squares of polynomials. A necessary condition is that p is psd; that is, $p(x_1, \ldots, x_n) \geq 0$ for all $x \in \mathbb{R}^n$. Suppose p is psd and let

$$\mathcal{C}(p) = cvx\{u : b_u \neq 0\}.$$

Then $\mathcal{C}(p)$ is a lattice polytope; in fact it can be shown that the vertices of $\mathcal{C}(p)$ lie in $(2\mathbb{Z})^n$, so that $\mathcal{P} := \frac{1}{2}\mathcal{C}(p)$ is a lattice polytope. Let

$$\mathcal{L}(\mathcal{P}) = \{v_1, \ldots, v_N\},$$

and for $u \in \mathcal{C}(p)$, let $D(u) = \{(i,j) : v_i + v_j = u\}$. It is proved in [?, Thm. 2.4] that p can be written as a sum of at most r squares of polynomials if and only if there is a real $N \times N$ symmetric psd matrix $A = [a_{ij}]$ of rank at most r, so that

$$\sum_{(i,j) \in D(u)} a_{ij} = b_u \qquad \text{for all } u \in \mathcal{C}(p).$$

If $\mathcal{P}$ is a dps polytope in $\mathbb{R}^n$, then either $|D(u)| \leq 1$ or $D(u) = \{(i,j),(j,i)\}$. In either case, a_{ij} is completely determined by b_u. In particular, if

$$h_{\mathcal{P}}(x_1, \ldots, x_n) := \sum_{i=1}^{N} (x^{v_i})^2, \tag{2}$$

then A must equal I_N, the $N \times N$ identity matrix, so that p is a sum of N squares, and no fewer.

Finally, we note that the homogenization of polynomials with n variables into forms with $n+1$ variables is precisely analogous to the embedding of polytopes in $\mathbb{R}^n_+$ into the hyperplane $\Delta_{n+1}(s)$.

Example 4. (See [**?**, Ex. 3.9])

We return to Example 1, in its homogeneous version. Let $A = [a_{ij}]$ be a real symmetric 4×4 matrix and let

$$f(t_1, t_2, t_3, t_4) = \sum_{i=1}^{4} \sum_{j=1}^{4} a_{ij} t_i t_j$$

be its associated quadratic form. We use the substitution suggested by $\mathcal{L}(\mathcal{P})$ and define the ternary sextic form

$$p(x_1, x_2, x_3) = f(x_2 x_3^2, x_1 x_2^2, x_1^2 x_3, x_1 x_2 x_3).$$

Then p is a sum of squares of polynomials (cubic forms) if and only if f is a psd quadratic form; that is,

$$f(t_1, t_2, t_3, t_4) \geq 0 \qquad \text{for all } (t_1, t_2, t_3, t_4) \in \mathbb{R}^4.$$

Since $t_4^3 = t_1 t_2 t_3$, the condition for p to be a psd form is weaker:

$$f(t_1, t_2, t_3, (t_1 t_2 t_3)^{1/3}) \geq 0 \qquad \text{for all } (t_1, t_2, t_3) \in \mathbb{R}^3.$$

If $f(t_1, t_2, t_3, t_4) = t_1^2 + t_2^2 + t_3^2 - 3t_4^2$, then f is not psd, but $f(t_1, t_2, t_3, (t_1 t_2 t_3)^{1/3}) \geq 0$ by the arithmetic-geometric inequality. It follows that

$$p(x_1, x_2, x_3) = x_2^2 x_3^4 + x_1^2 x_2^4 + x_1^4 x_3^2 - 3x_1^2 x_2^2 x_3^2$$

is a form which is psd, but not a sum of squares of polynomials. This particular example was discussed in [**?**]. For a history and bibliography of this subject and its relation to Hilbert's 17th Problem, see [**?**].

More generally, the *Pythagoras number* of a ring A, $P(A)$, is the smallest number $n \leq \infty$ such that any sum of squares in A can be expressed as a sum of at most n squares in A. Pfister [**?**] proved in 1967 that $P(\mathbb{R}(x_1, \ldots, x_n)) \leq 2^n$. It is easy to see that $P(\mathbb{R}[x_1]) = 2$. Since maximal dps polytopes exist in $\mathbb{R}^n$ for every n, a consideration of $h_{\mathcal{P}}$ (c.f. (**??**)) shows that $P(\mathbb{R}[x_1, \ldots, x_n]) \geq 2^n$. This is not the strongest result possible: in [**?**, p.60], using other methods, Dai and the present authors have shown that $P(\mathbb{R}[x_1, \ldots, x_n]) = \infty$ for $n \geq 2$.

References

[1] G. L. Alexanderson, L. F. Klosinski, L. C. Larson (eds.), *The William Lowell Putnam Mathematical Competition, Problems and Solutions: 1964–1984*, Mathematical Association of America, 1985.

[2] M. D. Choi, Z. D. Dai, T. Y. Lam and B. Reznick, *The pythagoras number of some affine algebras and local algebras*, J. Reine. Angew. Math. **336** (1982), 45–82.

[3] M. D. Choi and T. Y. Lam, *An old question of Hilbert*, Queen's Papers in Pure and Appl. Math. (Proceedings of Quadratic Forms Conference, Queen's University (G. Orzech ed.)) **46** (1976), 385–405.

[4] M. D. Choi, T. Y. Lam and B. Reznick, *Sums of squares of real polynomials*, Proc. Symp. Pure Math. **58.2** (1995), 103–126.

[5] A. Pfister, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Invent. Math. **4** (1967), 229–237.

[6] B. Reznick, *Lattice point simplices*, Discrete Math. **60** (1986), 219–242.

[7] B. Reznick, *Some concrete aspects of Hilbert's 17th Problem*, Contemp. Math. **253** (2000), 251–272.