

McMaster University
Advanced Optimization Laboratory



Title:

Primitive Zonotopes

Authors:

Antoine Deza, George Manoussakis, and Shmuel Onn

AdvOL-Report No. 2015/5

December 2015, Hamilton, Ontario, Canada
(revised January 2017)

Primitive Zonotopes

Antoine Deza^a, George Manoussakis^b, and Shmuel Onn^c

^aMcMaster University, Hamilton, Ontario, Canada

^bUniversité de Paris Sud, Orsay, France

^cTechnion - Israel Institute of Technology, Haifa, Israel

Abstract

We introduce and study a family of polytopes which can be seen as a generalization of the permutahedron of type B_d . We highlight connections with the largest possible diameter of the convex hull of a set of points in dimension d whose coordinates are integers between 0 and k , and with the computational complexity of multicriteria matroid optimization.

Keywords: Lattice polytopes, matroid optimization, diameter, primitive integer vectors

1 Introduction

We introduce and study lattice polytopes generated by the primitive vectors of bounded norm. These *primitive zonotopes* can be seen as a generalization of the permutahedron of type B_d . We note that, besides a large symmetry group, primitive zonotopes have a large diameter and many vertices relative to their grid embedding size. The article is structured as follows. In Section 2, we introduce the primitive zonotopes and some of their properties. In Section 3 we derive lower bounds for the diameter of lattice polytopes, and in Section 4 we determine the computational complexity of multicriteria matroid optimization.

Finding a good bound on the maximal edge-diameter of a polytope in terms of its dimension and the number of its facets is not only a natural question of discrete geometry, but also historically closely connected with the theory of the simplex method. Recent results dealing with the combinatorial, geometric, and algorithmic aspects of linear optimization include Santos' counterexample to the Hirsch conjecture, and Allamigeon, Benchimol, Gaubert, and Joswig's counterexample to a continuous analogue of the polynomial Hirsch conjecture. Kalai and Kleitman's upper bound for the diameter of polytopes was strengthened by Todd, and then by Sukegawa. Kleinschmidt and Onn's upper bound for the diameter of lattice polytopes was strengthened by Del Pia and Michini, and then by Deza and Pournin. For more details and additional results such as the validation that transportation polytopes satisfy the Hirsch bound, see [2, 5, 6, 7, 8, 15, 21, 24, 26] and references therein.

Multicriteria matroid optimization is a generalization of standard linear matroid optimization where each basis is evaluated according to several, rather than one, criteria, and these values are traded-in by a convex function, see [17, 19, 20] and references therein. It turns out

that multicriteria matroid optimization can be reduced to solve several linear counterparts. In Section 4, the largest number of such counterparts is shown to be precisely the number of vertices of a primitive zonotope.

2 Primitive zonotopes

2.1 Definition

The convex hull of integer-valued points is called a lattice polytope and, if all the vertices are drawn from $\{0, 1, \dots, k\}^d$, is referred to as a lattice (d, k) -polytope. For simplicity, we only consider full dimensional lattice (d, k) -polytopes. Given a finite set G of vectors, also called the generators, the zonotope generated by G is the convex hull of all signed sums of the elements of G . Searching for lattice polytopes with a large diameter for a given k , natural candidates include zonotopes generated by short integer vectors in order to keep the grid embedding size relatively small. In addition, we restrict to integer vectors which are pairwise linearly independent in order to maximize the diameter. Thus, for $q = \infty$ or a positive integer, and d, p positive integers, we consider the *primitive zonotope* $Z_q(d, p)$ defined as the zonotope generated by the primitive integer vectors of q -norm at most p :

$$\begin{aligned} Z_q(d, p) &= \sum [-1, 1] \{v \in \mathbb{Z}^d : \|v\|_q \leq p, \gcd(v) = 1, v \succ 0\} \\ &= \text{conv} \left(\sum \{ \lambda_v v : v \in \mathbb{Z}^d, \|v\|_q \leq p, \gcd(v) = 1, v \succ 0\} : \lambda_v = \pm 1 \right) \end{aligned}$$

where $\gcd(v)$ is the largest integer dividing all entries of v , and \succ the lexicographic order on \mathbb{R}^d , i.e. $v \succ 0$ if the first nonzero coordinate of v is positive. Similarly, we consider $H_q(d, p)$ which is, up to translation, the image of $Z_q(d, p)$ by a homothety of factor $1/2$:

$$H_q(d, p) = \sum [0, 1] \{v \in \mathbb{Z}^d : \|v\|_q \leq p, \gcd(v) = 1, v \succ 0\}.$$

In other words, $H_q(d, p)$ is the Minkowski sum of the generators of $Z_q(d, p)$. We also consider the *positive primitive zonotope* $Z_q^+(d, p)$ defined as the zonotope generated by the primitive integer vectors of q -norm at most p with nonnegative coordinates:

$$Z_q^+(d, p) = \sum [-1, 1] \{v \in \mathbb{Z}_+^d : \|v\|_q \leq p, \gcd(v) = 1\}$$

where $\mathbb{Z}_+ = \{0, 1, \dots\}$. Similarly, we consider the Minkowski sum of the generators of $Z_q^+(d, p)$:

$$H_q^+(d, p) = \sum [0, 1] \{v \in \mathbb{Z}_+^d : \|v\|_q \leq p, \gcd(v) = 1\}.$$

We illustrate the primitive zonotopes with a few examples:

- (i) For finite q , $Z_q(d, 1)$ is generated by the d unit vectors and forms the $\{-1, 1\}^d$ -cube. $H_q(d, 1)$ is the $\{0, 1\}^d$ -cube.
- (ii) $Z_1(d, 2)$ is the permutahedron of type B_d and thus, $H_1(d, 2)$ is, up to translation, a lattice $(d, 2d - 1)$ -polytope with $2^d d!$ vertices and diameter d^2 . For example, $Z_1(2, 2)$

is generated by $\{(0, 1), (1, 0), (1, 1), (1, -1)\}$ and forms the octagon whose vertices are $\{(-3, -1), (-3, 1), (-1, 3), (1, 3), (3, 1), (3, -1), (1, -3), (-1, -3)\}$. $H_1(2, 2)$ is, up to translation, a lattice $(2, 3)$ -polygon. $Z_1(3, 2)$ is congruent to the truncated cuboctahedron – which is also called great rhombicuboctahedron – and is the Minkowski sum of an octahedron and a cuboctahedron, see for instance Eppstein [9]. $H_1(3, 2)$ is, up to translation, a lattice $(3, 5)$ -polytope with diameter 9 and 48 vertices.

- (iii) $H_1^+(d, 2)$ is the Minkowski sum of the permutahedron with the $\{0, 1\}^d$ -cube. Thus, $H_1^+(d, 2)$ is a lattice (d, d) -polytope with diameter $\binom{d+1}{2}$.
- (iv) $Z_\infty(3, 1)$ is congruent to the truncated small rhombicuboctahedron, see Figure 1 for an illustration, which is the Minkowski sum of a cube, a truncated octahedron, and a rhombic dodecahedron, see for instance Eppstein [9]. $H_\infty(3, 1)$ is, up to translation, a lattice $(3, 9)$ -polytope with diameter 13 and 96 vertices.

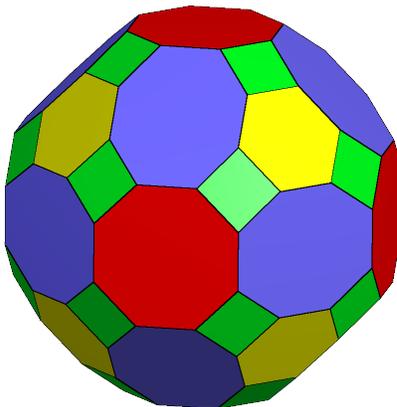


Figure 1: $Z_\infty(3, 1)$ is congruent to the truncated small rhombicuboctahedron

- (v) $Z_\infty^+(2, 2)$ is generated by $\{(0, 1), (1, 0), (1, 1), (1, 2), (2, 1)\}$ and forms the decagon whose vertices are $\{(-5, -5), (-5, -3), (-3, -5), (-3, 1), (-1, 3), (1, -3), (3, -1), (3, 5), (5, 3), (5, 5)\}$. $H_\infty^+(2, 2)$ is a lattice $(2, 5)$ -polygon.

2.2 Combinatorial properties

We provide properties concerning $Z_q(d, p)$ and $Z_q^+(d, p)$, and in particular their symmetry group, diameter, and vertices. $Z_1(d, 2)$ is the permutahedron of type B_d as its generators form the root system of type B_d , see [14]. Thus, $Z_1(d, 2)$ has $2^d d!$ vertices and its symmetry group is B_d . The properties listed in this section are extensions to $Z_q(d, p)$ of known properties of $Z_1(d, 2)$, and thus given without proof. We refer to Fukuda [10], Grünbaum [12], and Ziegler [27] for polytopes and, in particular, zonotopes.

Property 2.1.

- (i) $Z_q(d, p)$ is invariant under the symmetries induced by coordinate permutations and the reflections induced by sign flips.

- (ii) The sum $\sigma_q(d, p)$ of all the generators of $Z_q(d, p)$ is a vertex of both $Z_q(d, p)$ and $H_q(d, p)$. The origin is a vertex of $H_q(d, p)$, and $-\sigma_q(d, p)$ is a vertex of $Z_q(d, p)$.
- (iii) The coordinates of the vertices of $Z_q(d, p)$ are odd. Thus, the number of vertices of $Z_q(d, p)$ is a multiple of 2^d .
- (iv) $H_q(d, p)$ is, up to translation, a lattice (d, k) -polytope where k is the sum of the first coordinates of all generators of $Z_q(d, p)$.
- (v) The diameter of $Z_q(d, p)$, respectively $Z_q^+(d, p)$, is equal to the number of its generators.

Property 2.2.

- (i) $Z_q^+(d, p)$ is centrally symmetric and invariant under the symmetries induced by coordinate permutations.
- (ii) The sum $\sigma_q^+(d, p)$ of all the generators of $Z_q^+(d, p)$ is a vertex of both $Z_q^+(d, p)$ and $H_q^+(d, p)$. The origin is a vertex of $H_q^+(d, p)$, and $-\sigma_q^+(d, p)$ is a vertex of $Z_q^+(d, p)$.

A vertex v of $Z_q(d, p)$ is called *canonical* if $v_1 \geq \dots \geq v_d > 0$. Property 2.1 item (i) implies that the vertices of $Z_q(d, p)$ are all the coordinate permutations and sign flips of its canonical vertices.

Property 2.3.

- (i) A canonical vertex v of $Z_q(d, p)$ is the unique maximizer of $\{\max c^T x : x \in Z_q(d, p)\}$ for some vector c satisfying $c_1 > c_2 > \dots > c_d > 0$.
- (ii) $Z_1(d, 2)$ has $2^d d!$ vertices corresponding to all coordinate permutations and sign flips of the unique canonical vertex $\sigma_1(d, 2) = (2d - 1, 2d - 3, \dots, 1)$.
- (iii) $Z_\infty^+(d, 1)$ has at least $2 + 2d!$ vertices including the $2d!$ permutations of $\pm\sigma(d)$ where $\sigma(d)$ is a vertex with pairwise distinct coordinates, and the 2 vertices $\pm\sigma_\infty^+(d, 1)$.

Enumerative questions concerning $H_q(d, p)$ and $H_q^+(d, p)$ have been studied in various settings. For example, the number of vertices of $H_\infty^+(d, 1)$ corresponds to the OEI sequence A034997 giving the number of generalized retarded functions in quantum field theory, and the number of vertices of $H_\infty(d, 1)$, which is the number of regions of hyperplane arrangements with $\{-1, 0, 1\}$ -valued normals in dimension d , corresponds, up to a factor of $2^d d!$, to the OEI sequence A009997, see [22] and references therein.

3 Large diameter

Let $\delta(d, k)$ be the maximum possible edge-diameter over all lattice (d, k) -polytopes. Naddef [18] showed in 1989 that $\delta(d, 1) = d$, Kleinschmidt and Onn [16] generalized this result in 1992 showing that $\delta(d, k) \leq kd$. In 2016, Del Pia and Michini [7] strengthened the upper bound to $\delta(d, k) \leq kd - \lceil d/2 \rceil$ for $k \geq 2$, and showed that $\delta(d, 2) = \lfloor 3d/2 \rfloor$. Pursuing Del Pia and Michini's approach, Deza and Pournin [8] showed that $\delta(d, k) \leq kd - \lceil 2d/3 \rceil - (k - 3)$ for $k \geq 3$, and that $\delta(4, 3) = 8$. Del Pia and Michini conclude their paper noting that the current lower bound

for $\delta(d, k)$ is of order $k^{2/3}d$ and ask whether the gap between the lower and upper bounds could be closed, or at least reduced. The order $k^{2/3}d$ lower bound for $\delta(d, k)$ is a direct consequence of the determination of $\delta(2, k)$ which was investigated independently in the early nineties by Thiele [25], Balog and Bárány [3], and Acketa and Žunić [1]. In this section, we highlight that $H_1(2, p)$ is the unique polygon achieving $\delta(2, k)$ for a proper k , and that a Minkowski sum of a proper subset of the generators of $H_1(d, 2)$ achieves a diameter of $\lfloor (k+1)d/2 \rfloor$ for all $k \leq 2d-1$.

3.1 $H_1(2, p)$ as a lattice polygon with large diameter

Finding lattice polygons with the largest diameter; that is, to determine $\delta(2, k)$, was investigated independently in the early nineties by Thiele [25], Balog and Bárány [3], and Acketa and Žunić [1]. This question can be found in Ziegler's book [27] as Exercise 4.15. The answer is summarized in Proposition 3.1 where $\phi(j)$ is the Euler totient function counting positive integers less than or equal to j and relatively prime with j . Note that $\phi(1)$ is set to 1.

Proposition 3.1. *$H_1(2, p)$ is, up to translation, a lattice $(2, k)$ -polygon with $k = \sum_{j=1}^p j\phi(j)$ where $\phi(j)$ denotes the Euler totient function. The diameter of $H_1(2, p)$ is $2 \sum_{j=1}^p \phi(j)$ and satisfies $\delta(H_1(2, p)) = \delta(2, k)$. Thus, $\delta(2, k) = 6(\frac{k}{2\pi})^{2/3} + O(k^{1/3} \log k)$.*

Note that lattice polygons can be associated to set of integer-valued vectors adding to zero and such that no pair of vectors are positive multiples of each other. Such set of vectors forms a $(2, k)$ -polygon with $2k$ being the maximum between the sum of the norms of the first coordinates of the vectors and the sum of the norms of the second coordinates of the vectors. Then, for $k = \sum_{j=1}^p j\phi(j)$ for some p , one can show that $\delta(2, k)$ is achieved uniquely by a translation of $H_1(2, p)$. For $k \neq \sum_{j=1}^p j\phi(j)$ for any p , $\delta(2, k)$ is achieved by a translation of a Minkowski sum of a proper subset of the generators of $H_1(2, p)$ including all generators of $H_1(2, p-1)$ for a proper p . For the order of $\sum_{j=1}^p \phi(j)$, respectively $\sum_{j=1}^p j\phi(j)$, being $\frac{3p^2}{\pi^2} + O(p \ln p)$, respectively $\frac{2p^3}{\pi^2} + O(p^2 \ln p)$, we refer to [13]. The first values of $\delta(2, k)$ are given in Table 1.

p of $H_1(2, p)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	4
k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
$\delta(2, k)$	2	3	4	4	5	6	6	7	8	8	8	9	10	10	10	11	12	

Table 1: Relation between $H_1(2, p)$ and $\delta(2, k)$

3.2 $H_1(d, 2)$ as a lattice polytope with large diameter

As pointed out by Vincent Pilaud, a lower bound of $kd/2$ for $\delta(d, k)$ for $k < d$ can be achieved by considering a graphical zonotope $H_{\mathcal{G}}$; that is, the Minkowski sum of the line segments $[e_i, e_j]$ for all edges ij of a given graph \mathcal{G} . Consider the graphical zonotope $H_{\mathcal{C}(d,k)}$ associated to the circulant graph $\mathcal{C}(d, k)$ of degree k on d nodes. One can check that $H_{\mathcal{C}(d,k)}$ is a lattice (d, k) -polytope with diameter $kd/2$. In this section, pursuing this approach, we show that a Minkowski sum of a proper subset of the generators of $H_1(d, 2)$ yields $\delta(d, k) \geq \lfloor (k+1)d/2 \rfloor$ for all $k \leq 2d-1$.

Theorem 3.2. *For $k \leq 2d - 1$, there is a subset of the generators of $H_1(d, 2)$ whose Minkowski sum is, up to translation, a lattice (d, k) -polytope with diameter $\lfloor (k + 1)d/2 \rfloor$. So for $k \leq 2d - 1$ we have $\delta(d, k) \geq \lfloor (k + 1)d/2 \rfloor$. For instance, $H_1^+(d, 2)$ is a lattice (d, d) -polytope with diameter $\binom{d+1}{2}$, and $H_1(d, 2)$ is, up to translation, a lattice $(d, 2d - 1)$ -polytope with diameter d^2 .*

Proof. We first note that the number of generators of $H_1(d, 2)$ is d^2 . The generators of $H_1(d, 2)$ are $\{-1, 0, 1\}$ -valued d -tuples: d permutations of $(1, 0, \dots, 0)$, $\binom{d}{2}$ permutations of $(1, 1, 0, \dots, 0)$, and $\binom{d}{2}$ permutations of $(1, -1, 0, \dots, 0)$. Thus, $\delta(H_1(d, 2)) = d^2$ by Property 2.1 item (v). As the sum of the first coordinates of the generators of $H_1(d, 2)$ is $2d - 1$, $H_1(d, 2)$ is, up to translation, a lattice $(d, 2d - 1)$ -polytope by Property 2.1 item (iv). Consider first the case when d is even. The first $d - 1$ subsets are obtained by removing from the current subset of generators of $H_1(d, 2)$ a set of $d/2$ generators taken among the $\binom{d}{2}$ permutations of $(1, -1, 0, \dots, 0)$. The removed $d - 1$ subsets correspond to $d - 1$ disjoint perfect matchings of the complete graph K_d where the nonzero i^{th} and j^{th} coordinates of a generator $(\dots, 1, \dots, -1, \dots)$ correspond to the edge $[i, j]$ of K_d . The first perfect matching is $[1, 2], [3, d], [4, d - 1], \dots, [d/2 + 1, d/2 + 2]$. The next perfect matching is obtained by changing d to 2, and i to $i + 1$ for all other entries except 1 which remains unchanged. This procedure yields $d - 1$ disjoint perfect matchings as, placing the vertices 2 to d on a circle around 1 where the edge $[1, 2]$ is vertical and the edges $[3, d], [4, d - 1], \dots, [d/2 + 1, d/2 + 2]$ are horizontal, the procedure corresponds to the $d - 1$ rotations of the initial perfect matching, see [4, Chapter 12]. As these $d - 1$ perfect matchings correspond to all the generators of $H_1(d, 2)$ which are permutations of $(1, -1, 0, \dots, 0)$, the procedure ends with a subset of the generators of $H_1(d, 2)$ forming the $\binom{d+1}{2}$ generators of $H_1^+(d, 2)$. We can then repeat the same procedure where the nonzero i^{th} and j^{th} coordinates of a generator $(\dots, 1, \dots, 1, \dots)$ correspond to the edge $[i, j]$ of K_d , and similarly obtain $d - 1$ disjoint perfect matchings. The procedure now ends with a subset of the generators of $H_1(d, 2)$ forming $H_1(d, 1)$; that is the unit cube. One can check that if the Minkowski sum H of the current subset of generators of $H_1(d, 2)$ is a lattice (d, k) -polytope of diameter $\delta(H)$, removing the $d/2$ generators corresponding to a perfect matching yields a lattice $(d, k - 1)$ -polytope of diameter $\delta(H) - d/2$. Thus, starting from $H_1(d, 2)$ which is a $(d, 2d - 1)$ -polytope with diameter d^2 , we obtain a (d, k) -polytope with diameter $(k + 1)d/2$ for all $k \leq 2d - 1$. The case when d is odd is similar. The removed subsets are of alternating sizes $\lceil d/2 \rceil$ and $\lfloor d/2 \rfloor$. Adding a dummy vertex $d + 1$ to K_d , we consider the d disjoint perfect matching of K_{d+1} described for even d . The first subset consists of the $\lceil d/2 \rceil$ edges where $[3, d + 1]$ is replaced by $[3, 5]$, the second subset consists of the $\lfloor d/2 \rfloor$ edges where $[5, d + 1]$ is removed, the third subset consists of the $\lceil d/2 \rceil$ edges where $[7, d + 1]$ is replaced by $[7, 9]$, and so forth. As for even d , one can check that if the Minkowski sum H of the current subset of generators of $H_1(d, 2)$ is a lattice (d, k) -polytope of diameter $\delta(H)$, removing the described $\lceil d/2 \rceil$, respectively $\lfloor d/2 \rfloor$, generators yields a lattice $(d, k - 1)$ -polytope of diameter $\delta(H) - \lceil d/2 \rceil$, respectively $\delta(H) - \lfloor d/2 \rfloor$. Thus, starting from $H_1(d, 2)$ which is a $(d, 2d - 1)$ -polytope with diameter d^2 , we obtain a (d, k) -polytope with diameter $\lfloor (k + 1)d/2 \rfloor$ for all $k \leq 2d - 1$. \square

Conjecture 3.3. $\delta(d, k) \leq \lfloor (k + 1)d/2 \rfloor$, and $\delta(d, k)$ is achieved, up to translation, by a Minkowski sum of lattice vectors.

Note that Conjecture 3.3 holds for all known values of $\delta(d, k)$ given in Table 2, and hypothesizes, in particular, that $\delta(d, 3) = 2d$. Note that $\delta(d, 3) = 2d$ for $d \leq 4$, $2d \leq \delta(d, 3) \leq \lceil 7d/3 \rceil - 1$ when $d \not\equiv 2 \pmod{3}$, and $\delta(d, 3) \leq \lceil 7d/3 \rceil$ when $d \equiv 2 \pmod{3}$, see [8].

$\delta(d, k)$	k									
	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	3	4	4	5	6	6	7	8	8
3	3	4	6							
4	4	6	8							
\vdots	\vdots	\vdots								
d	d	$\lfloor 3d/2 \rfloor$								

Table 2: Largest diameter $\delta(d, k)$ over all lattice (d, k) -polytopes

Soprunov and Soprunova [23] considered the Minkowski length of a lattice polytope P ; that is, the largest number of lattice segments whose Minkowski sum is contained in P . For example, the Minkowski length of the $\{0, k\}^d$ -cube is kd . We consider a variant of the Minkowski length and the special case when P is the $\{0, k\}^d$ -cube. Let $L(d, k)$ denote the largest number of pairwise linearly independent lattice segments whose Minkowski sum is contained in the $\{0, k\}^d$ -cube. One can check that the generators of $H_1(d, 2)$ form the largest, and unique, set of primitive lattice vectors which Minkowski sum fits within the $\{0, k\}^d$ -cube for $k = 2d - 1$; that is, for k being the sum of the first coordinates of the d^2 generators of $H_1(d, 2)$. Thus, $L(d, 2d - 1) = \delta(H_1(d, 2)) = d^2$. Similarly, the constructions used in Proposition 3.1 and Theorem 3.2 imply that $L(2, k) = \delta(2, k)$ for all k , and $L(d, k) = \lfloor (k + 1)d/2 \rfloor$ for $k \leq 2d - 1$.

4 Multicriteria matroid optimization

We consider the convex multicriteria matroid optimization framework of Melamed, Onn and Rothblum, see [17, 19, 20], and show that $H_\infty(d, p)$ settles its computational complexity.

Call $S \subset \{0, 1\}^n$ a *matroid* if it is the set of the indicators of bases of a matroid over $\{1, \dots, n\}$. For instance, S can be the set of indicators of spanning trees in a connected graph with n edges. We assume that the matroid is presented by an *independence oracle* that, queried on $y \in \{0, 1\}^n$, asserts whether or not $y \leq x$ for some $x \in S$. The standard linear optimization problem over the matroid S is: given a *utility vector* $w \in \mathbb{Z}^n$, find a basis which maximizes the utility $w^T x$, that is, solve $\{\max w^T x : x \in S\}$. This problem is known to be easily solvable by the *greedy algorithm*. Generalizing this problem to d criteria, we are given a $d \times n$ integer *utility matrix* W whose i^{th} row W_i gives the utility $W_i x$ of basis $x \in S$ under criterion i , so the vector $Wx \in \mathbb{Z}^d$ represents the d utility values of basis x under the d criteria. These values are then traded-in by a convex function $f : \mathbb{R}^d \rightarrow \mathbb{R}$. We assume that f is presented by a *comparison oracle* that, queried on vectors $x, y \in \mathbb{Z}^d$, asserts whether or not $f(x) < f(y)$. The *multicriteria matroid optimization problem* is then: find a basis which maximizes the traded-in utility $f(Wx)$; that is, solve $\{\max f(Wx) : x \in S\}$, making use of the oracle presentations of S and f .

Let $\text{conv}(WS) = \text{conv}\{Wx : x \in S\}$ be the projection to \mathbb{R}^d of $\text{conv}(S)$ by W . As detailed in [19, Chapter 2], the projection polytope $\text{conv}(WS)$ and its vertices play a key role in solving our optimization problem since for any convex function f there is an optimal solution $x \in S$ whose projection $u = Wx$ is a vertex of $\text{conv}(WS)$. Thus, the convex multicriteria problem

can be solved by enumerating the set of vertices of $\text{conv}(WS)$, picking a vertex u attaining a maximum value $f(u)$, and finding $x \in S$ with $Wx = u$. However, direct computation of $\text{conv}(WS)$ and enumeration of its vertices are intractable since, typically, S has exponentially many points.

Following [17], we consider nonnegative utilities, so that, for some positive integer p , for all i, j , the utility $W_{i,j}$ of element j of the ground set of the matroid under criterion i is in $\{0, 1, \dots, p\}$. We call such utility matrices *p-bounded*. Let $m(d, p)$ denote the number of vertices of $H_\infty(d, p)$. Theorem 4.1 settles the computational complexity of the multicriteria optimization problem by showing that the maximum number of vertices of the projection polytope $\text{conv}(WS)$ of any matroid S on n elements and any d -criteria p -bounded utility matrix; that is, $W \in \{0, 1, \dots, p\}^{d \times n}$, is equal to $m(d, p)$, and hence is in particular *independent* of n, S , and W . Below, we use the following. The *normal cone* of polytope $P \subset \mathbb{R}^n$ at its vertex v is the relatively open cone of vectors $h \in \mathbb{R}^n$ such that v is the unique maximizer of $h^T x$ over P . A polytope H *refines* a polytope P if the normal cone of H at every vertex of H is contained in the normal cone of P at some vertex of P . Then, the closure of each normal cone of P is the union of closures of normal cones of H , and P has no more vertices than H .

Theorem 4.1. *Let d, p be any positive integers. Then, for any positive integer n , any matroid $S \subset \{0, 1\}^n$, and any d -criteria p -bounded utility matrix W , the primitive zonotope $H_\infty(d, p)$ refines $\text{conv}(WS)$. Moreover, $H_\infty(d, p)$ is a translation of $\text{conv}(WS)$ for some matroid S and d -criteria p -bounded utility matrix W . Thus, the maximum number of vertices of $\text{conv}(WS)$ for any n , any matroid $S \subset \{0, 1\}^n$, and any d -criteria p -bounded utility matrix W , equals the number $m(d, p)$ of vertices of $H_\infty(d, p)$, and hence is independent of n, S , and W . Also, for any fixed d and convex $f : \mathbb{R}^d \rightarrow \mathbb{R}$, the multicriteria matroid optimization problem can be solved using a number of arithmetic operations and queries to the oracles of S and f which is polynomial in n and p using $m(d, p)$ greedily solvable linear matroid optimization counterparts.*

Proof. We show first that $H_\infty(d, p)$ refines $\text{conv}(WS)$ for every matroid S . It is known that if G is a finite set of vectors such that every edge in a polytope P is parallel to some $g \in G$, then the zonotope $H = \sum[0, 1]G$ refines P , see [11, 20]. Now, for any matroid $S \subset \{0, 1\}^n$, any edge of $\text{conv}(S)$ is parallel to the difference $\mathbf{1}_i - \mathbf{1}_j$ between a pair of unit vectors in \mathbb{R}^n , see [19, Chapter 2]. Therefore, any edge of the projection $\text{conv}(WS)$ is parallel to the difference $W^i - W^j$ between a pair of columns of W . Note that $W^i - W^j \in \{0, \pm 1, \dots, \pm p\}^d$ since $W^i, W^j \in \{0, 1, \dots, p\}^d$. Thus, every edge of $\text{conv}(WS)$ is parallel to some vector in

$$G(d, p) = \{v \in \mathbb{Z}^d : \|v\|_\infty \leq p, \text{gcd}(v) = 1, v \succ 0\}.$$

Therefore, the primitive zonotope $H_\infty(d, p) = \sum[0, 1]G(d, p)$ refines $\text{conv}(WS)$. Next, we construct a matroid S and a d -criteria p -bounded utility matrix such that $H_\infty(d, p)$ is a translation of $\text{conv}(WS)$. For a vector $g \in \mathbb{Z}^d$ let $g^+, g^- \in \mathbb{Z}_+^d$ be its *positive* and *negative parts*; that is, the unique nonnegative vectors with disjoint support satisfying $g = g^+ - g^-$. Order arbitrarily the vectors $\{g_1, \dots, g_r\}$ of $G(d, p)$ and let $n = 2r$. Consider the graph which is a path of length r whose edges are labeled by g_1, \dots, g_r . Then, replace each edge g_i by two parallel edges labeled by g_i^+ and g_i^- . Let $S \subset \{0, 1\}^n$ be the graphic matroid of the resulting graph on n edges. Let W be the d -criteria p -bounded matrix $W = [g_1^+, g_1^-, \dots, g_r^+, g_r^-]$. Now, there is a bijection between bases $x \in S$ and subsets $I \subseteq \{1, \dots, r\}$ where we put i in I if x chooses g_i^+ from the parallel

pair $\{g_i^+, g_i^-\}$. Then, for corresponding x and I :

$$Wx = \sum_{i \in I} g_i^+ + \sum_{i \notin I} g_i^- = \sum_{i=1}^r g_i^- + \sum_{i \in I} (g_i^+ - g_i^-) + \sum_{i \notin I} (g_i^- - g_i^-) = \sum_{i=1}^r g_i^- + \sum_{i \in I} g_i.$$

Thus,

$$\begin{aligned} \text{conv}(Wx : x \in S) &= \text{conv} \left(\sum_{i=1}^r g_i^- + \sum_{i \in I} g_i : I \subseteq \{1, \dots, r\} \right) \\ &= \sum_{i=1}^r g_i^- + \text{conv} \left(\sum G : G \subseteq G(d, p) \right) = \sum_{i=1}^r g_i^- + H_\infty(d, p). \end{aligned}$$

We conclude that this implies that the maximum number of vertices of $\text{conv}(WS)$ for any n , any matroid $S \subset \{0, 1\}^n$, and any d -criteria p -bounded utility matrix W , equals the number $m(d, p)$ of vertices of $H_\infty(d, p)$. Indeed, for every W and S , the number of vertices of $\text{conv}(WS)$ is at most $m(d, p)$ since $H_\infty(d, p)$ refines $\text{conv}(WS)$. In addition, $m(d, p)$ is attained as the number of vertices of the translation $\text{conv}(WS)$ of $H_\infty(d, p)$ for S and W constructed above.

We proceed with the algorithmic complexity of the multicriteria matroid optimization problem. Let d be fixed, the number $g(d, p)$ of generators of $H_\infty(d, p)$ satisfies $g(d, p) = O(p^d)$. Thus, as detailed in [19, Chapter 2], the number of vertices of $H_\infty(d, p)$ satisfies $m(d, p) = O(g(d, p)^d) = O(p^{d^2})$ which is polynomial in p , and in that much time, all vertices of $H_\infty(d, p)$ can be enumerated along with, for each vertex $v \in \mathbb{Z}^d$, a vector h_v in the normal cone of $H_\infty(d, p)$ at v . This preprocessing depends only on p .

Now, let n , a matroid $S \subset \{0, 1\}^n$, and a d -criteria p -bounded utility matrix W be given. For each of the $m(d, p) = O(p^{d^2})$ vertices v of $H_\infty(d, p)$ we solve the standard linear optimization problem over S with utility vector $w_v = h_v^T W \in \mathbb{Z}^n$ by the greedy algorithm using the independence oracle of S and find an optimal basis $x_v \in S$. We collect the projections Wx_v of all these optimal bases x_v corresponding to the vertices v of $H_\infty(d, p)$ in a set $U \subset \mathbb{Z}^d$. We now claim that every vertex u of $\text{conv}(WS)$ lies in U . Consider such a vertex u and let $x \in S$ be such that $u = Wx$. Since $H_\infty(d, p)$ refines $\text{conv}(WS)$, there is a vertex v of H such that the normal cone of H at v is contained in the normal cone of $\text{conv}(WS)$ at u . Therefore, h_v is maximized over $\text{conv}(WS)$ uniquely at $u = Wx$. We claim that $u = Wx_v \in U$. Assume that not, then we get $w_v^T x = h_v^T Wx > h_v^T Wx_v = w_v^T x_v$. hence a contradiction. Thus, we find a vertex v of $H_\infty(d, p)$ such that $u = Wx_v$ maximizes $f(u)$ over U using the comparison oracle of f , and conclude that $x_v \in S$ is the optimal solution to the multicriteria matroid problem. \square

Example 4.2. Let $(d, p) = (2, 1)$, we describe $H_\infty(2, 1)$, the matroid S , and the matrix W constructed in the proof of Theorem 4.1 such that $H_\infty(2, 1)$ is a translation of $\text{conv}(WS)$: $G(2, 1) = \{(0, 1), (1, -1), (1, 0), (1, 1)\}$, $n = 8$, and

$$S = \{x \in \{0, 1\}^8 : x_{2i-1} + x_{2i} = 1, \quad i = 1, 2, 3, 4\}, \quad W = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

See Figure 2 for an illustration of $\text{conv}(WS) = (0, 1) + H_\infty(2, 1)$ with its $m(2, 1) = 8$ vertices, and a vector h_v in the normal cone of $H_\infty(2, 1)$ at each vertex v of $\text{conv}(WS)$.

Now consider the following bicriteria matroid optimization problem with $f = \|\cdot\|_2^2$; that is, $f(y_1, y_2) = y_1^2 + y_2^2$, over a uniform matroid and 2-criteria 1-bounded utility matrix given by

$$U_{12}^6 = \{x \in \{0, 1\}^{12} : \sum_{i=1}^{12} x_i = 6\}, \quad W = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We solve the problem using the algorithm provided in the proof of Theorem 4.1. For each of the $m(2, 1) = 8$ vectors h_v in normal cones in Figure 2, we solve the linear optimization counterpart over U_{12}^6 with utility vector $w_v = h_v^T W \in \mathbb{Z}^{12}$ by the greedy algorithm and find an optimal basis $x_v \in U_{12}^6$. For instance, for $h_v = (1, 2)$, greedily found w_v and x_v are:

$$w_v = (0 \ 2 \ 1 \ 3 \ 0 \ 2 \ 1 \ 3 \ 0 \ 2 \ 1 \ 3), \quad x_v = (0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1).$$

Then, $Wx_v = (3, 6)$ so x_v has objective value $f(Wx_v) = 45$. We repeat this for all 8 vectors h_v and find the best. Here, the x_v above is indeed an optimal solution to the bicriteria problem. Note that U_{12}^6 has $\binom{12}{6} = 924$ bases and, for matroids on ground sets with larger n , the number of bases typically grows exponentially. Thus, solving our problem by exhaustive search is unreasonable. Instead, our algorithm solves any bicriteria 1-bounded matroid problem in polynomial time by always greedily solving only 8 linear counterparts, each in time linear in n .

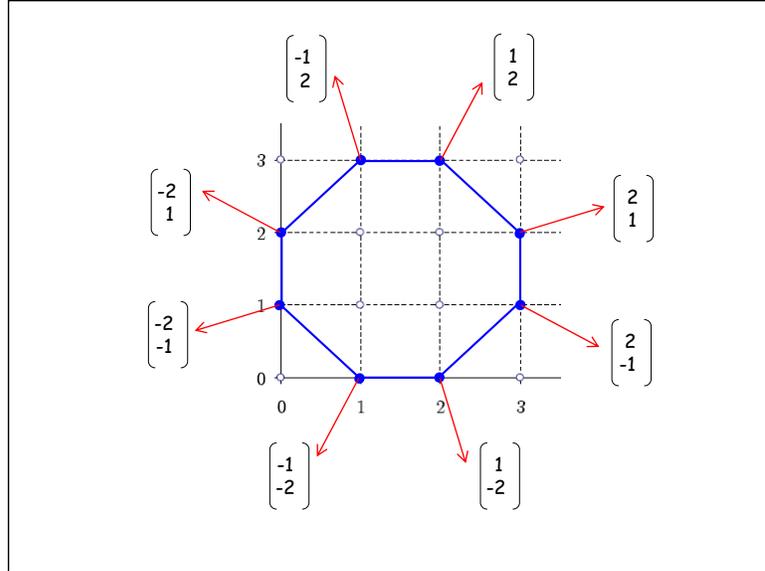


Figure 2: $\text{conv}(WS) = (0, 1) + H_\infty(2, 1)$ and associated vectors h_v

Theorem 4.1 asserts that the number $m(d, p)$ of vertices of $H_\infty(d, p)$ is the largest number of linear counterparts needed to solve any d -criteria p -bounded problem. While we do not know much about the exact value of $m(d, p)$, we examine $m(d, p)$ for small d or p in the rest of this section: $m(1, p)$ is trivially equal to 2, $m(2, p)$ is given in Proposition 4.3, and the first values of $m(d, 1)$ are given after Proposition 4.3.

Proposition 4.3. *The number of vertices of $H_\infty(2, p)$ satisfies $m(2, p) = 8 \sum_{j=1}^p \phi(j)$ where $\phi(j)$ is the Euler totient function counting positive integers less than or equal to j and relatively prime with j .*

Proof. Since the generators of $H_q(d, p)$ are pairwise linearly independent, the diameter of $H_q(d, p)$ equals the number of generators. For $d = 2$, the number of vertices of $H_q(2, p)$ is twice the diameter. Thus, $m(2, p)$ is twice the number of generators of $H_\infty(2, p)$. Now, $H_\infty(2, p)$ has $4\phi(1)$ generators $(1, 0), (0, 1), (1, 1), (1, -1)$. In addition, for $p \geq 2$, $H_\infty(2, p)$ has the $4\phi(j)$ generators $(i, j), (i, -j), (j, i), (j, -i)$ for $j = 2, \dots, p$ where i runs through all positive integers less than or equal to j and relatively prime with j . So $H_\infty(2, p)$ has $4 \sum_{j=1}^p \phi(j)$ generators and $m(2, p) = 8 \sum_{j=1}^p \phi(j)$ vertices. \square

For instance, the first values of $m(2, p)$ are:

$$m(2, 1) = 8, \quad m(2, 2) = 16, \quad m(2, 3) = 32, \quad m(2, 4) = 48, \quad m(2, 5) = 80, \quad m(2, 6) = 96.$$

Turning to the number $m(d, 1)$ of vertices of $H_\infty(d, 1)$, no closed-form expression is known but, as mentioned at the end of Section 2, $m(d, 1)$ corresponds to the OEI sequence A009997, up to a factor of $2^d d!$. The first values are:

$$m(2, 1) = 8, \quad m(3, 1) = 96, \quad m(4, 1) = 5\,376, \quad m(5, 1) = 1\,981\,440, \quad m(6, 1) = 5\,722\,536\,960.$$

To solve a 6-criteria 1-bounded matroid problem may require about 6 billion linear counterparts!

Acknowledgment

The authors thank the anonymous referees, Johanne Cohen, Nathann Cohen, Komei Fukuda, and Aladin Virmaux for valuable comments and for informing us of reference [25], Emo Welzl and Günter Ziegler for helping us access Thorsten Thiele's Diplomarbeit, Dmitrii Pasechnik for pointing out reference [23] and the concept of Minkowski length, and Vincent Pilaud for pointing out graphical zonotopes and that $Z_1(d, 2)$ is the permutahedron of type B_d . This work was partially supported by the Natural Sciences and Engineering Research Council of Canada Discovery Grant program (RGPIN-2015-06163), by the Digiteo Chair C&O program, and by the Dresner Chair at the Technion.

References

- [1] Dragan Acketa and Joviša Žunić. On the maximal number of edges of convex digital polygons included into an $m \times m$ -grid. *Journal of Combinatorial Theory A*, 69:358–368, 1995.
- [2] Xavier Allamigeon, Pascal Benchimol, Stéphane Gaubert, and Michael Joswig. Long and winding central paths. *arXiv:1405.4161*, 2014.
- [3] Antal Balog and Imre Bárány. On the convex hull of the integer points in a disc. In *Proceedings of the Seventh Annual Symposium on Computational Geometry*, pages 162–165, 1991.

- [4] Claude Berge. *Graphes*. Gauthier-Villars, 1983.
- [5] Nicolas Bonifas, Marco Di Summa, Friedrich Eisenbrand, Nicolai Hähnle, and Martin Niemeier. On sub-determinants and the diameter of polyhedra. *Discrete and Computational Geometry*, 52:102–115, 2014.
- [6] Steffen Borgwardt, Jesús De Loera, and Elisabeth Finhold. The diameters of transportation polytopes satisfy the Hirsch conjecture. *arXiv:1603.00325*, 2016.
- [7] Alberto Del Pia and Carla Michini. On the diameter of lattice polytopes. *Discrete and Computational Geometry*, 55:681–687, 2016.
- [8] Antoine Deza and Lionel Pournin. Improved bounds on the diameter of lattice polytopes. *arXiv:1610.00341*, 2016.
- [9] David Eppstein. Zonohedra and zonotopes. *Mathematica in Education and Research*, 5:15–21, 1996.
- [10] Komei Fukuda. Lecture notes: Polyhedral computation. <http://www-oldurls.inf.ethz.ch/personal/fukudak/lect/pclect/notes2015/>.
- [11] Peter Gritzmann and Bernd Sturmfels. Minkowski addition of polytopes: complexity and applications to Gröbner bases. *SIAM Journal on Discrete Mathematics*, 6:246–269, 1993.
- [12] Branko Grünbaum. *Convex Polytopes*. Graduate Texts in Mathematics. Springer, 2003.
- [13] Godfrey Hardy, Edward Wright, David Heath-Brown, and Joseph Silverman. *An introduction to the theory of numbers*. Clarendon Press Oxford, 1979.
- [14] James Humphreys. *Reflection groups and Coxeter groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1990.
- [15] Gil Kalai and Daniel Kleitman. A quasi-polynomial bound for the diameter of graphs of polyhedra. *Bulletin of the American Mathematical Society*, 26:315–316, 1992.
- [16] Peter Kleinschmidt and Shmuel Onn. On the diameter of convex polytopes. *Discrete Mathematics*, 102:75–77, 1992.
- [17] Michal Melamed and Shmuel Onn. Convex integer optimization by constantly many linear counterparts. *Linear Algebra and its Applications*, 447:88–109, 2014.
- [18] Dennis Naddef. The Hirsch conjecture is true for $(0, 1)$ -polytopes. *Mathematical Programming*, 45:109–110, 1989.
- [19] Shmuel Onn. *Nonlinear Discrete Optimization*. Zurich Lectures in Advanced Mathematics. European Mathematical Society, 2010.
- [20] Shmuel Onn and Uriel G. Rothblum. Convex combinatorial optimization. *Discrete and Computational Geometry*, 32:549–566, 2004.

- [21] Francisco Santos. A counterexample to the Hirsch conjecture. *Annals of Mathematics*, 176:383–412, 2012.
- [22] Neil Sloane (editor). The on-line encyclopedia of integer sequences. <https://oeis.org>.
- [23] Ivan Soprunov and Jenya Soprunova. Eventual quasi-linearity of the Minkowski length. *European Journal of Combinatorics*, 58:110–117, 2016.
- [24] Noriyoshi Sukegawa. Improving bounds on the diameter of a polyhedron in high dimensions. *arXiv:1604.04338*, 2016.
- [25] Torsten Thiele. Extremalprobleme für Punktmengen. *Diplomarbeit, Freie Universität Berlin*, 1991.
- [26] Michael Todd. An improved Kalai-Kleitman bound for the diameter of a polyhedron. *SIAM Journal on Discrete Mathematics*, 28:1944–1947, 2014.
- [27] Günter Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics. Springer, 1995.

Antoine Deza, Advanced Optimization Laboratory, Faculty of Engineering
McMaster University, Hamilton, Ontario, Canada.
Email: deza@mcmaster.ca

George Manoussakis, Laboratoire de Recherche en Informatique
Université de Paris Sud, Orsay, France.
Email: george@lri.fr

Shmuel Onn, Operations Research, Davidson faculty of IE & M
Technion Israel Institute of Technology, Haifa, Israel.
Email: onn@ie.technion.ac.il