Primitive Lattice Polytopes

Antoine Deza[a], George Manoussakis[b], and Shmuel Onn[c]

[a]McMaster University, Hamilton, Ontario, Canada
[b]Université de Paris Sud, Orsay, France
[c]Technion - 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 a parameter controlling 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 lattice polytopes* can be seen as a generalization of the permutahedron of type B_d. We note that, besides a large symmetry group, primitive lattice polytopes have a large diameter and many vertices relative to their grid size embedding. The article is structured as follows. In Section 2, we introduce the primitive lattice polytopes and some of their properties. In Section 3, respectively Section 4, lower bounds for the diameter of lattice polytopes, respectively lower and upper bounds for a parameter studied in convex matroid optimization, are derived.

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, 20, 23, 25] and references therein. For convex matroid optimization, we refer to [17, 19] and references therein.

2 Primitive lattice polytopes

2.1 Zonotopes generated by short primitive vectors

The convex hull of integer-valued points is called a lattice polytope and, if all the vertices are drawn from $\{0, 1, \ldots, k\}^d$, is refereed 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 lattice polytope* $Z_q(d, p)$ defined as the zonotope generated by the primitive integer vectors of q-norm at most p:

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

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. In Section 3, we consider $H_q(d, p)$ which is, up to translation, the image of $Z_q(d, p)$ by the 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 $Z_q(d, p)$. In Section 4, we consider the *positive primitive lattice polytope* $Z_q^+(d, p)$ 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 $\mathbb{Z}_+ = \{0, 1, \ldots\}$. Similarly, one can 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 lattice polytopes with a few examples:

(*i*) $Z_1(2, 2)$ 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.

(*ii*) $Z_1(3, 2)$ 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*) $Z_\infty(3, 1)$ is congruent to the truncated small rhombicuboctahedron 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.

(*iv*) For finite q, $Z_q(d,1)$ is generated by the d unit vectors and forms the $\{-1,1\}^d$-cube, and $H_q(d,1)$ is the $\{0,1\}^d$-cube.

(*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.

(*vi*) $Z_1(d,2)$ 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.

(*vii*) $H^+_1(d,2)$ 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 $\binom{d+1}{2}$.

2.2 Combinatorial properties of the primitive lattice polytopes

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 [26] 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, and 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 $v_1 \geq \cdots \geq v_d > 0$. 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 $c_1 > c_2 > \cdots > c_d > 0$.*

(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 with are the $2d!$ permutations of $\pm\sigma(d)$ where $\sigma(d)$ is a vertex with pairwise distinct coordinates, and the 2 vertices $\pm\sigma^+_\infty(d,1)$.*

3 Primitive lattice polytopes with 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 $\delta(d,k) \leq kd - \lceil 2d/3 \rceil$ 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 [24], 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 [24], Balog and Bárány [3], and Acketa and Žunić [1]. This question can be found in Ziegler's book [26] as Exercise 4.15. The answer is summarized in Proposition 3.1 where $\phi(j)$ is the Euler totient function counting positive integers less 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 $k = \sum_{1 \leq j \leq p} j\phi(j)$ where $\phi(j)$ denotes the Euler totient function. The diameter of $H_1(2,p)$ is $2 \sum_{1 \leq j \leq p} \phi(j)$ 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 $k = \sum_{1 \leq j \leq p} j\phi(j)$ for some p, one can show that $\delta(2,k)$ is achieved uniquely by a translation of $H_1(2,p)$. For $k \neq \sum_{1 \leq j \leq p} j\phi(j)$ for any p, $\delta(2,k)$ is achieved by a translation of a Minkowski sum of an appropriate subset of the generators of $H_1(2,p)$ including all generators of $H_1(2,p-1)$ for an appropriate p. For the order of $\sum_{1\le j\le p}\phi(j)$, respectively $\sum_{1\le j\le p} j\phi(j)$, 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
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 appropriate $k<d$ 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, we slightly generalize this approach and show that a Minkowski sum of a proper subset of the generators of $H_1(d,2)$ yields $\delta(d,k)\ge\lfloor(k+1)d/2\rfloor$ for all $k\le 2d-1$.

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

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 $[i,j]$. The first perfect matching is $[1,2],[3,d],[4,d-1],\dots,[d/2,d/2+1]$. 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 cercle around 1 where the edge $[1,2]$ is vertical and the edges $[3,d],[4,d-1],\dots,[d/2,d/2+1]$ 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 $(\ldots,1,\ldots,1,\ldots)$ 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 $\delta(d,3)=2d$.

	$\delta(d,k)$	k: 1	2	3	4	5	6	7	8	9	10
d	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 [22] considered the Minkowski length $L(P)$ of a lattice polytope P; that is, the largest number of lattice segments whose Minkowski sum is contained in P. Considering the special case when P is the $\{0,k\}^d$-cube, let $L(d,k)$ denote the Minkowski length of $\{0,k\}^d$-cube. For example, the Minkowski length of the $\{0,1\}^d$-cube satisfies $L(d,1)=d$. 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 3.2 implies that $L(2,k)=\delta(2,k)$ and $L(d,k)=\lfloor (k+1)d/2 \rfloor$ for $k \leq 2d-1$.

4 Primitive lattice polytopes with many vertices

In this section, we recall the setting of convex matroid optimization and show that $H_q(d,p)$, respectively $H_q^+(d,p)$, yields upper, respectively lower, bounds for a parameter studied by Melamed, Onn, and Rothblum [17, 19] and controlling the computational complexity of multi-criteria matroid optimization.

Call $S \subset \{0,1\}^n$ a *matroid* if it is the set of the indicators of bases of a matroid over $\{1,\ldots,n\}$. For a $d \times n$ matrix W, let $WS = \{Wx : x \in S\}$, and let $\mathrm{conv}(WS) = W\mathrm{conv}(S)$ be the projection to $\mathbb{R}^d$ of $\mathrm{conv}(S)$ by W. Given a convex function $f : \mathbb{R}^d \to \mathbb{R}$, *convex matroid optimization* deals with maximizing the composite function $f(Wx)$ over S; that is, max $\{f(Wx) \ : \ x \in S\}$, and is concerned with $\mathrm{conv}(WS)$; that is, the projection of the set of the feasible points. The maximization problem can be interpreted as a problem of multicriteria optimization, where each row of W gives a linear criterion $W_i x$ and f compromises these criteria. Thus, W is called the *criteria* matrix or *weight* matrix. The projection polytope $\mathrm{conv}(WS)$ and its vertices play a key role in solving the maximization problem as, for any convex function f, there is an optimal solution x whose projection $y = Wx$ is a vertex of $\mathrm{conv}(WS)$. In particular, the enumeration of all vertices of $\mathrm{conv}(WS)$ enables to compute the optimal objective value by picking a vertex attaining the optimal value $f(y) = f(Wx)$. Thus, it suffices that f is presented by a *comparison oracle* that, queried on vectors $y, z \in \mathbb{R}^d$, asserts whether or not $f(y) < f(z)$. *Coarse* criteria matrices; that is, W whose entries are small or in $\{0,1,\ldots,p\}$, are of particular interest. In multicriteria combinatorial optimization, this case corresponds to the weight $W_{i,j}$ attributed to element j of the ground set $\{1,\ldots,n\}$ under criterion i being small or in $\{0,1,\ldots,p\}$ for all i,j. In the reminder of Section 4, we only consider $\{0,1,\ldots,p\}$-valued W. We refer to Melamed and Onn [17], and references therein, for convex integer optimization and for convex matroid optimization in particular.

Recall that the *normal cone* of a polytope $P \subset \mathbb{R}^n$ at its vertex v is the relatively open cone of of vectors $c \in \mathbb{R}^n$ such that v is the unique maximizer of $\{\max c^T x : x \in P\}$. A polytope P is a *refinement* of a polytope Q if the normal cone of P at every vertex of P is contained in the normal cone of Q at some vertex of Q.

Proposition 4.1. *For positive integers d,p,n, a matroid $S \subset \{0,1\}^n$, and a $d \times n$ criteria matrix W with entries in $\{0,1,\ldots,p\}$, $H_\infty(d,p)$ is a refinement of* $\mathrm{conv}(WS)$*. Thus, the maximum number $m(d,p)$ of vertices of* $\mathrm{conv}(WS)$ *is independent of n, S, and W. In addition, $m(d,p)$ is at most the number of vertices of $H_\infty(d,p)$.*

Proof. For a matroid $S \subset \{0,1\}^n$, any edge of $\mathrm{conv}(S)$ is parallel to the difference $\mathbf{1}_i - \mathbf{1}_j$ between a pair of unit vectors in $\mathbb{R}^n$, see [17, 19]. Therefore, any edge of the projection $\mathrm{conv}(WS)$ by W is parallel to the difference $W^i - W^j$ between a pair of columns of W belonging to $\{0, \pm 1, \cdots \pm p\}^d$. Hence, $\sum [0,1]G$ where $G = \{v \in \mathbb{Z}^d : \|v\|_\infty \leq p\}$ is a refinement of $\mathrm{conv}(WS)$, see [11, 19]. Note that the generators of $H_\infty(d,p)$ form a maximal subset of G without pair of linearly dependent elements. Thus, $H_\infty(d,p)$ is equivalent to $\sum [0,1]G$ and hence a refinement of $\mathrm{conv}(WS)$. Thus, the maximum number $m(d,p)$ of vertices of $\mathrm{conv}(WS)$ is independent of n, S, and W, and satisfies $m(d,p) \leq f_0(H_\infty(d,p))$. $\square$

Proposition 4.2. *For positive integers d and p, there exist a positive integer n, a matroid $S \subset \{0,1\}^n$, and a $d \times n$ criteria matrix W with entries in $\{0,1,\dots,p\}$ such that* $\mathrm{conv}(WS) = H_\infty^+(d,p)$*. Thus, the maximum number $m(d,p)$ of vertices of* $\mathrm{conv}(WS)$ *is at least the number of vertices of $H_\infty^+(d,p)$.*

Proof. Let m denotes the number of generators of $H_\infty^+(d,p)$, and let W be the $d \times 2m$ matrix whose first m columns are the generators of $H_\infty^+(d,p)$, say, ordered lexicographically, and last m columns consist of zeros. Let S be the (set of indicators of bases of the) uniform matroid U_{2m}^m – that is, S consists of all vectors in $\{0,1\}^{2m}$ with exactly m zeros and m ones. One can check that $\mathrm{conv}(WS) = \sum[0,1]\{v \in \mathbb{Z}_+^d : \|v\|_\infty \leq p, \gcd(v) = 1\} = H_\infty^+(d,p)$. □

Theorem 4.3. *The following inequalities hold for $d \geq 3$:*

$$2 + 2d! \leq f_0(H_\infty^+(d,1)) \leq m(d,1) \leq f_0(H_\infty(d,1)) \leq 2\sum_{i=0}^{d-1}\binom{(3^d-3)/2}{i} - 2\binom{(3^{d-1}-3)/2}{d-1}.$$

Proof. The inequalities $2 + 2d! \leq f_0(H_\infty^+(d,1)) \leq m(d,1) \leq f_0(H_\infty(d,1))$ restate Property 2.3 item (iii) and Propositions 4.1 and 4.2 for $p = 1$. The last inequality is obtained by exploiting the structure of the generators of $H_\infty(d,1)$. One can check that $H_\infty(d,1)$ has $(3^d-1)/2$ generators and that removing the first zero of the generators of $H_\infty(d,1)$ starting with zero yields exactly the $(3^{d-1}-1)/2$ generators of $H_\infty(d-1,1)$. We recall that the number of vertices $f_0(Z)$ of a d-dimensional zonotope Z generated by m generators is bounded by $\bar{f}(d,m) = 2\sum_{0\leq i\leq d-1}\binom{m-1}{i}$. By duality, the number $f_0(Z)$ of vertices of a zonotope Z is equal to the number $f_{d-1}(\mathcal{A})$ of cells of the associate hyperplane arrangement $\mathcal{A}$ where each generator m^j of Z corresponds to an hyperplane h^j of $\mathcal{A}$, see [10, 26]. The inequality $f_0(Z) \leq \bar{f}(d,m)$ is based on the inequality $f_{d-1}(\mathcal{A}) \leq f_{d-1}(\mathcal{A} \setminus h^j) + f_{d-1}(\mathcal{A} \cap h^j)$ for any hyperplane h^j of $\mathcal{A}$ where $\mathcal{A} \setminus h^j$ denotes the arrangement obtained by removing h^j from $\mathcal{A}$, and $\mathcal{A} \cap h^j$ denotes the arrangement obtained by intersecting $\mathcal{A}$ with h^j. Recursively applying this inequality to the arrangement $\mathcal{A}_\infty(d,1)$ associated to $H_\infty(d,1)$ till the remaining $(3^{d-1}-1)/2$ hyperplanes form a $(d-1)$-dimensional arrangement equivalent to $\mathcal{A}_\infty(d-1,1)$ yields: $f_{d-1}(\mathcal{A}_\infty(d,1)) \leq \bar{f}(d,(3^d-1)/2) - \big(\bar{f}(d,(3^{d-1}-1)/2) - \bar{f}(d-1,(3^{d-1}-1)/2)\big)$ which completes the proof since $f_{d-1}(\mathcal{A}_\infty(d,1)) = f_0(H_\infty(d,1))$ and $\bar{f}(d,m) - \bar{f}(d-1,m) = 2\binom{m-1}{d}$. In other words, the inequality is based on the inductive build-up of $H_\infty(d,1)$ starting with the $(3^{d-1}-3)/2$ generators with zero as first coordinate, and noticing that these $(3^{d-1}-3)/2$ generators belong to a lower dimensional space. □

In order to tighten the lower bound for $m(d,1)$, we consider a family of lattice polytopes introduced in [17] and defined as $M(d,r,s) = \mathrm{conv}(W_d^s S_r^{s2^d})$ where W is the $\{0,1\}$-valued $d \times s2^d$ matrix whose $s2^d$ columns consist of s copies of the 2^d elements of $\{0,1\}^d$, and S is the (set of indicators of bases of the) uniform matroid $U_{s2^d}^r$ of rank r and order $s2^d$; that is, S consists of all vectors in $\{0,1\}^{s2^d}$ with exactly r ones. We illustrate the $M(d,r,s)$ family with a few examples:

(i) $M(d,r,s \geq r)$ is the $\{0,s\}^d$-cube,

(ii) $M(d,2,1)$ is the truncated $\{0,2\}^d$-cube, *(iii)* $M(d, s+1, s \geq 2)$ is the truncated $\{0, s\}^d$-cube,

(vi) $M(3, 5, 2)$ is congruent to $H_1(3, 2)$.

Observation 4.4.

(i) $m(2, 1) = 8$ *as* $f_0(M(2, 3, 2)) = f_0(H_\infty(2, 1)) = 8$,

(ii) $48 \leq m(3, 1) \leq 96$ *as* $f_0(M(3, 5, 2)) = 48$ *and* $f_0(H_\infty(3, 1)) = 96$,

(iii) $672 \leq m(4, 1) \leq 5\,376$ *as* $f_0(M(4, 11, 2)) = 672$ *and* $f_0(H_\infty(4, 1)) = 5\,376$,

(iv) $11\,292 \leq m(5, 1) \leq 1\,981\,440$ *as* $f_0(H^+_\infty(5, 1)) = 11\,292$ *and* $f_0(H_\infty(5, 1)) = 1\,981\,440$.

Enumerative questions concerning $H_q(d, p)$ and $H^+_q(d, p)$ have been studied in various settings. For example, $f_0(H^+_\infty(d, 1))$ corresponds to the OEI sequence A034997 giving the number of generalized retarded functions in quantum field theory, and $f_0(H_\infty(d, 1))$, which is the number of regions of hyperplane arrangements with $\{-1, 0.1\}$-valued normals in dimension d, corresponds to the OEI sequence A009997 giving $f_0(H^+_\infty(d, 1))/(2^d d!)$, see [21] and references therein.

Acknowledgment. The authors thank Johanne Cohen, Nathann Cohen, Komei Fukuda, and Aladin Virmaux for valuable comments and suggestions and for informing us of reference [24], Emo Welzl and Günter Ziegler for helping us access Thorsten Thiele's Diplomarbeit, Dmitrii Pasechnik for pointing out reference [22] and the concept of Minkowski length, and Vincent Pilaud for pointing out graphical zonotopes yielding a lower bound of $kd/2$ for $\delta(d, k)$ for $k < d$, and that $Z_1(d, 2)$ is the permutahedron of type B_d. This work was supported by the Natural Sciences and Engineering Research Council of Canada Discovery Grant program (RGPIN-2015-06163) and by the Digiteo Chair C&O program.

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 Hearth-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 and Uriel G. Rothblum. Convex combinatorial optimization. *Discrete and Computational Geometry*, 32:549–566, 2004.

[20] Francisco Santos. A counterexample to the Hirsch conjecture. *Annals of Mathematics*, 176:383–412, 2012.

[21] Neil Sloane (editor). The on-line encyclopedia of integer sequences. `https://oeis.org`.

[22] Ivan Soprunova and Jenya Soprunova. Eventual quasi-linearity of the Minkowski length. *European Journal of Combinatorics*, 58:110–117, 2016.

[23] Noriyoshi Sukegawa. Improving bounds on the diameter of a polyhedron in high dimensions. *arXiv:1604.04338*, 2016.

[24] Torsten Thiele. Extremalprobleme für Punktmengen. *Diplomarbeit, Freie Universität Berlin*, 1991.

[25] Michael Todd. An improved Kalai-Kleitman bound for the diameter of a polyhedron. *SIAM Journal on Discrete Mathematics*, 28:1944–1947, 2014.

[26] 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