An introduction to empty lattice-simplices

András Sebő
CNRS, Laboratoire Leibniz-IMAG, Grenoble, France
http://www-leibniz.imag.fr/DMD/OPTICOMB *

March 15, 1999

Abstract

We study simplices whose vertices lie on a lattice and have no other lattice points. Such 'empty lattice simplices' come up in the theory of integer programming, and in some combinatorial problems. They have been investigated in various contexts and under varying terminology by Reeve, White, Scarf, Kannan and Lovász, Reznick, Kantor, Haase and Ziegler, etc.

Can the 'emptiness' of lattice simplices be 'well-characterized' ? Is their 'lattice-width' small ? Do the integer points of the parallelepiped they generate have a particular structure ?

The 'good characterization' of empty lattice simplices occurs to be open in general ! We provide a polynomial algorithm for deciding when a given integer 'knapsack' or 'partition' lattice simplex is empty. More generally, we ask for a characterization of linear inequalities satisfied by the lattice points of a lattice parallelepiped. We state a conjecture about such inequalities, prove it for $n \leq 4$, and deduce several variants of classical results of Reeve, White and Scarf characterizing the emptiness of small dimensional lattice simplices. For instance, a three dimensional integer simplex is empty if and only if all its faces have width 1. Seemingly different characterizations can be easily proved from one another using the Hermite normal form.

In fixed dimension the width of polytopes can be computed in polynomial time (see the simple integer programming formulation of Haase and Ziegler). We prove that it is already NP-complete to decide whether the width of a very special class of integer simplices is 1, and we also provide for every $n \geq 3$ a simple example of n-dimensional empty integer simplices of width $n-2$, improving on earlier bounds.

1 Introduction

Let $V \subseteq \mathbb{R}^n$ ($n \in \mathbb{N}$) be a finite set. A *polytope* is a set of the form $\mathrm{conv}(V) := \{\sum_{v\in V} \lambda_v v : \sum_{v\in V} \lambda_v = 1\}$. If V is linearly independent, then $S := \mathrm{conv}(V \cup \{0\})$ is called a *simplex.* (It will be assumed that that $0 \in \mathbb{R}^n$ is one of the vertices of S.) The (linear or affine) *rank* $r(S)$ is the linear rank of V. A polytope is said to be *integer* if its vertices are integer vectors. More generally, fixing an arbitrary 'lattice' L, a lattice polytope is a polytope whose vertices are in L. The results we are proving in this paper do hold for arbitrary lattices, but this general case can always be obviously reduced to $L = \mathbb{Z}^n$. Therefore we will not care about more general lattices.

A set of the form $\mathrm{cone}(V) := \{\sum_{v\in V} \lambda_v v : \lambda_v \geq 0\}$ is a *cone*; if V is linearly independent, the cone is called *simplicial.*

*Research developed partly during a visit in the Research Institute for Mathematical Sciences, Kyoto University.

We refere to Schrijver [13] for basic facts about polytopes, cones and other notions of polyhedral combinatorics, as well as for standard notations such as the affine or linear hull of vectors, etc.

Let us call an integer polytope P *empty*, if it is integer, and denoting the set of its vertices by V, $(P \cap \mathbb{Z}^n) \setminus V = \emptyset$. (The definition is similar for arbitrary lattice L instead of $\mathbb{Z}^n$.) Empty lattice polytopes have been studied in the past four decades, let us mention as landmarks Reeve [11], White [15], Reznick [10], Scarf [12] and Haase, Ziegler [5]. (However, there is no unified terminology about them: the terms range from 'lattice-point-free lattice polytopes' to 'elementary or fundamental lattice polytopes'.) The latter paper is devoted to the volume and the width of empty lattice simplices.

In this paper we study the structure of empty lattice simplices, the correlation of emptiness and the width of lattice simplices, including the computational complexity of both. (Note that deciding whether a (not necessarily integer) simplex contains an integer point is trivially NP-complete, since the set of feasible solutions of the knapsack problem $K := \{x \in \mathbb{R}^n : ax = b, x \geq 0\}$ ($a \in \mathbb{N}^n, b \in \mathbb{N}$) is a simplex. However, in Section 2 we will decide whether a knapsack lattice simplex is empty in polynomial time.)

Deciding whether a lattice simplex is empty is the simplest of a possible range of problems that can be formulated as follows: given linearly indepedent integer vectors $a_1, \ldots, a_n \in \mathbb{Z}^n$ is there an integer vector v in the cone they generate such that the uniquely determined coefficients $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}_+$ for which $\lambda_1 a_1 + \ldots + \lambda_n a_n = v$ satisfy some given linear inequalities. The problem investigated here corresponds to the inequality $\lambda_1 + \ldots \lambda_n \leq 1$. Another interesting variant is the existence of an integer point where the λ_i $(i = 1, \ldots, n)$ satisfy some lower and upper bounds. For instance the 'Lonely Runner Problem' (or 'View Obstruction Problem') for velocity vector $v \in \mathbb{R}^n$ (see [4]) can be restated as the problem of the existence of an integer vector with $1/(n+1) \leq \lambda_i \leq n/(n+1)$ for all $i = 1, \ldots, n$ in $\mathrm{cone}(e_1, \ldots, e_n, (v, d))$, where the e_i $(i = 1, \ldots, n)$ are unit vectors and d is the least common multiple of all the vectors $v_i + v_j$, $(i, j = 1, \ldots, n)$.

The *width* $W(S)$ *in* $\mathbb{R}^n$ of a set $S \subseteq \mathbb{R}^n$ is the minimum of $\max\{w^T(x - y) : x, y \in S\}$ over all vectors $w \in \mathbb{Z}^n \setminus \{0\}$. If the rank of S is $r < n$, then the width of S in $\mathbb{R}^n$ is 0, and it is more interesting to speak about its *width in* $\mathrm{aff}(S) = \mathrm{lin}(S)$ defined as the minimum of $\max\{w^T(x - y) : x, y \in S\}$ over all vectors $w \in \mathbb{Z}^n$ not orthogonal to $\mathrm{lin}(S)$. Shortly, the *width* of S will mean its width in $\mathrm{aff}(S)$.

If $0 \notin V \subseteq \mathbb{Z}^n$, and V is linearly independent, then define $\mathrm{par}(V) := \{x \in \mathbb{Z}^n : x = \sum_{v \in V} \lambda_v v; 1 > \lambda_v \geq 0\ (v \in V)\}$ and call it a *parallelepiped*. If in addition $|V| = n$, then $|\mathrm{par}(V)| = \det(V)$, where $\det(V)$ denotes the *absolute value of the determinant* of the matrix whose rows are the elements of V (see for instance Cassels [3], or for an elementary proof see Sebő [14]). In particular, $\mathrm{par}(V) = \{0\}$ if and only if $\det(V) = 1$.

The problem of deciding the emptiness of parallelepipeds generated by integer vectors is therefore easy. On the other hand the same problem is still open for simplices, and that is the topic of this paper.

If $n \leq 3$, it is well-known [15], that the width of an empty integer simplex is 1 (the reverse is even easier – for both directions see Corollary 4.5 below).

The following example shows that in general the width of empty integer simplices can be large. The problem might have been overlooked before: the simple construction below is apparently the first explicit example of empty integer simplices of arbitrary high width. The best result known so far was Kantor's non-constructive proof [8] for the existence of integer simplices of width n/e. For a survey concerning previous results on the correlation of the width and the volume of empty lattice simplices see Haase, Ziegler [5].

It is easy to construct integer simplices of width n without integer points at all (not even the vertices), for instance by the following well-known example, [6]: for arbitrary $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, the simplex $\{x \in \mathbb{R}^n : \sum_{i=1}^n x_i \leq n - \varepsilon/2, x_i \geq \varepsilon/2$ for all $i = 1, \ldots, n\}$ has width $n - \varepsilon$ and no integer point. The vertices of this simplex have exactly one big coordinate. We define an integer simplex which is 'closest possible' to this one:

Let $k \in \mathbb{N}$ (the best choice will be $k = n-2$). $S_n(k) := \mathrm{conv}(s_0, s_1, ..., s_n)$, $s_0 := 0$, $s_1 := (1, k, 0, \ldots, 0)$, $s_2 := (0, 1, k, 0, \ldots, 0)$, $\ldots$, $s_{n-1} := (0, \ldots, 0, 1, k)$, $s_n := (k, 0, \ldots, 0, 1)$. Let $s_{i,j}$ denote the j-th coordinate of s_i, that is, $s_{i,j} = 0$ if $|i-j| \geq 2$, $s_{i,i} = 1$, $s_{i,i+1} = k$, $(i, j \in \{1, \ldots, n\})$. The notation $i+1$ is understood mod n.

(1.1) *The width of $S_n(k)$ is k, unless both $k = 1$ and n is even.*

Indeed, since $0 \in S_n(k)$, the width is at least k if and only if for arbitrary nonzero integer n-dimensional w there exists $i \in \{1, \ldots, n\}$ so that $|w^T s_i| \geq k$. The polytope $S_n(k)$ is a simplex if $s_1, \ldots, s_n$ are linearly independent, which is automatic if $W(S_n(k)) = k > 0$ holds.

Let $w \in \mathbb{Z}^n$, $w \neq 0$. If $w_i = 0$ for some $i \in \{1, \ldots, n\}$, then there also exists one such that $w_i = 0$ and $w_{i+1} \neq 0$. But then $|w^T s_i| \geq s_{i,i+1} = k$, and we are done. So suppose w has full support. If there exists an $i = 1, ..., n$ such that $|w_i| < |w_{i+1}|$, then $|w^T s_i| = |w_i + w_{i+1} k| \geq |w_{i+1} k| - |w_i| > (k-1)|w_i| \geq k - 1$, and we are done again.

Hence, we can suppose that $|w_i| \geq |w_{i+1}|$ holds for all $i = 1, ..., n$. But then the equality follows throughout, and we can suppose $|w_i| = 1$ for all $i = 1, ..., n$. If there exists an $i \in \{1, \ldots, n\}$ so that w_i, w_{i+1} have the same sign, then $w^T s_i = k + 1$. If the signs of the w_i are cyclically alternating, then $w^T s_i$ is also alternating between $(k-1)$ and $-(k-1)$ and then $w^T(s_i - s_{i+1}) = 2k - 2$. In this case n is even, and $2k - 2 \geq k$ unless $k = 1$.

So the width is at least k, unless n is even, and $k = 1$. Choosing w to be any of the n unit vectors we see that the width of $S_n(k)$ is k. □

(1.2) *If $k + 1 < n$, then $S_n(k)$ is an empty integer simplex.*

Indeed, for a contradiction, let $z = (z_1, \ldots, z_n) \in S_n(k)$ be an integer vector different from s_i $(i = 1, ..., n)$, $z = \sum_{i=0}^n \lambda_i s_i$, $\lambda_i \in \mathbb{R}_+$, $\sum_{i=0}^n \lambda_i = 1$.

Claim: $\lambda_i > 0$ for all $i = 1, \ldots, n$.

Indeed, if not, there exists an $i \in \{1, \ldots, n\}$ so that $\lambda_i = 0$, $\lambda_{i+1} \neq 0$. Then $z_{i+1} = \lambda_{i+1}$. Since $\lambda_{i+1} > 0$ by assumption, and $\lambda_{i+1} < 1$ since z is different from s_{i+1}, we have: z_{i+1} is not integer, contradicting the integrality of z. The claim is proved.

The claim immediately implies $z > 0$ and hence $z \geq 1$. Therefore $\sum_{i=1}^n z_i \geq n$. On the other hand, for all the vertices x of $S_n(k)$, $\sum_{i=1}^n x_i \leq k + 1$. Thus, if $k + 1 < n$, then $z \notin S_n(k)$. □

Hence, *for $n \geq 3$, $S_n(n-2)$ is an integer simplex of width $n-2$ by (1.1), and is empty by (1.2).* The volume (determinant) of $S_n(n-2)$ is also high among empty simplices in $\mathbb{R}^n$. This example is not best possible : for small n there exist empty integer simplices of larger width, see [5]. Moreover Imre Bárány pointed out that in the above example, for odd n, the facet of $S_n(k)$ not containing 0 has still the same width as $S_n(k)$, providing an empty integer simplex of width $n-1$ if $n \geq 4$ is even; Bárány also noticed that the volume can be increased by a constant factor by changing one entry in the example. However, it still seems to be reasonable to think that the maximum width of an empty integer simplex $S \subseteq \mathbb{R}^n$ is $n +$ constant. Kannan and Lovász [6] implies that the width of an arbitrary empty integer polytope is at most $O(n^2)$; in [1] this is improved to $O(n^{3/2})$, where for empty integer simplices $O(n \log n)$ is also proved.

The main question we are interested in is the following:

Question: *Is there a simple 'good-characterization' theorem or even a polynomial algorithm deciding the emptiness of integer simplices ? How are the emptiness and the width correlated ? Is there any relation between their computational complexity ?*

It is surprising that the literature does not make any claim about these problems in general. In the present paper we state some questions and provide some simple answers whenever we can. Unfortunately we do not yet know what is the complexity of deciding the emptiness of integer simplices, nor the complexity of computing the width of empty integer simplices !

In Section 2 we describe a good-characterization theorem and polynomial algorithm deciding if an integer knapsack (or 'partition') polytope is empty.

In Setion 3 and Section 4 we show a possible good certificate for certain lattice simplices to be empty. As a consequence, a simple new proof is provided for facts well-known from [15], [12].

Deciding whether a lattice polytope is empty can be trivially reduced to the existence of an integer point in a slightly perturbed polytope. The result of Section 2 suggests that a reduction in the opposite direction could be more difficult, and is impossible in some particular cases.

This reduction implies that in fixed dimension it can be decided in polynomial time whether a lattice polytope is empty by Lenstra [9]. More generally, Barvinok [2] developped a polynomial algorithm for counting the number of integer points in polytopes when the dimension is fixed.

We do not care about how the simplices are given, since the constraints can be computed from the vertices in polynomial time, and vice versa.

In Section 5 we explore the complexity of computing the width of simplices.

2 Knapsack simplices

If $a, b \in \mathbb{Z}$, $\mathrm{lcm}(a, b)$ denotes the least common multiple of a and b, that is, the smallest nonnegative number which is both a multiple of a and of b.

Theorem 2.1 *Let $K := \{x \in \mathbb{R}^n : a^T x = b, x \geq 0\}$, $(a \in \mathbb{N}^n,\ b \in \mathbb{N})$ be an integer polytope. Then K is empty, if and only if $\mathrm{lcm}(a_i, a_j) = b$ for all $i \neq j = 1, \ldots, n$.*

Proof. Clearly, K is an $n-1$-dimensional simplex whose vertices are $v_i := k_i e_i$, where $k_i := b/a_i$. Since K is an integer polytope, $k_i \in \mathbb{Z}$, that is, $a_i | b$ $(i = 1, \ldots, n)$.

Let us realize that K contains no integer points besides the vertices, if and only if $\gcd(k_i, k_j) = 1$ for all $i, j \in 1, \ldots, n$.

Indeed, if say $\gcd(k_1, k_2) = d > 1$ then $(1/d)v_1 + ((d-1)/d)v_2$ is an integer point. Conversely, suppose that there exists an integer vector $w = \sum_{i=1}^n \lambda_i v_i$ $(\lambda_i \geq 0, i = 1, \ldots, n)$, $\sum_{i=1}^n \lambda_i = 1$, and say $\lambda_1 > 0$. Let $\lambda_i := p_i/q_i$, where p_i, q_i are relatively prime nonzero integers whenever $\lambda_i \neq 0$. Since $\lambda_2 + \ldots + \lambda_n = 1 - \lambda_1$, an arbitrary prime factor p of q_1 occurs also in q_i for some $i \in \{2, \ldots, n\}$. Since $w_i = \lambda_i k_i$ is integer, the denominator of λ_i divides k_i, that is, $p | k_1$, $p | k_i$, proving $\gcd(k_1, k_i) \geq p > 1$.

Now it only remains to notice that for any $i, j = 1, \ldots, n$, $\gcd(k_i, k_j) = 1$ if and only if $\mathrm{lcm}(a_i, a_j) = \mathrm{lcm}(b/k_i, b/k_j) = b$. $\square$

This assertion does not generalize, the simplex K is quite special :

Corollary 2.2 *The integer knapsack polytope $K := \{x \in \mathbb{R}^n : a^T x = b, x \geq 0\}$, $(a \in \mathbb{N}^n,\ b \in \mathbb{N})$ is empty, if and only if all its two dimensional faces are empty.*

3 Parallelepiped Structure and Jump Coefficients

In this section we are stating two lemmas that will be needed in the sequel. The first collects some facts about the structure or parallelepipeds. The second is a result of number theoretic character. The structure provided by the first raises the problem solved by the second.

A *unimodular transformation* is a linear transformation defined by an integer matrix whose determinant is 1. An equivalent definition: a unimodular transformation is the composition of a finite number of reflections $f_i(x) := (x_1, \ldots, -x_i, \ldots, x_n)$, and sums $f_{i,j} := (x_1, \ldots, x_{i-1}, x_i + x_j, x_{i+1}, \ldots, x_n)$,
$(i, j = 1, \ldots, n)$. The equivalence of the two definitions is easy to prove in knowledge of the Hermite normal form (see the definition in [13]).

We will use unimodular transformations of a set of vectors V by putting them into a matrix M as rows, and then using column operations to determine the Hermite normal form M' of M. Then the rows of M' can be considered to provide an 'isomorphic' representation of V.

The residue of $x \in \mathbb{R}$ mod $d \in \mathbb{N}$ will be denoted by $\mathrm{mod}(x, d)$, $0 \le \mathrm{mod}(x, d) < d$.

Let $V := \{v_1, \ldots, v_n\} \subseteq \mathbb{Z}^n$ be a basis of $\mathbb{R}^n$, and $d := \det(v_1, \ldots, v_n)$. By Cramer's rule every integer vector is a linear combination of V with coefficients that are integer multiples of $1/d$. For $x \in \mathbb{R}^n$ the coefficient vector $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ defined by the unique combination $x = (\lambda_1 v_1 + \ldots + \lambda_n v_n)/d$, will be called the V-coefficient vector of x. In other words $\lambda = dV^{-1}x$ (where V denotes the $n \times n$ matrix whose n-th column is v_n). If $x \in \mathbb{Z}^n$ then all V-coefficients of x are integer.

Clearly, V-coefficient vectors are unchanged by linear transformations, and the width is unchanged under unimodular transformations. (The inverse of a unimodular transformation is also unimodular. Unimodular transformations can be considered to be the 'isomorphisms' of polytopes with respect to their integer vectors.)

A $\mathrm{par}(V)$-*coefficient vector* is a vector $\lambda \in \mathbb{R}^n$ which is the V-coefficient vector of some $x \in \mathrm{par}(V)$. We will often exploit the fact that parallelepipeds are *symmetric* objects: if $x \in \mathrm{par}(v_1, \ldots, v_n)$, then $v_1 + \ldots + v_n - x \in \mathrm{par}(v_1, \ldots, v_n)$. In other words, if $(\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n$ is a $\mathrm{par}(V)$-coefficient vector, then $(d - \lambda_1, \ldots, d - \lambda_n)$ is also one (extensively used in [10] and [14]).

We will use $\mathrm{par}(V)$-coefficients and some basic facts in the same way as we did in [14]. These have been similarly used in books, for $n = 3$ in White's paper [15], or in Reznick [10] through 'barycentric coordinates', whose similarity was kindly pointed out to the author by Jean-Michel Kantor.

An important part of the literature is in fact involved more generally with the number of integer points in three (or higher) dimensional simplices. Our ultimate goal is to find only simple general 'good certificates' (or polynomial algorithms) for deciding when this number is *zero*, and $\mathrm{par}(V)$-coefficients seem to be helpful to achieve this task. We are able to achieve only much less: we treat small dimensional cases in a simple new way, bringing to the surface some more general facts and conjectures.

If $x \in \mathbb{R}^n$, then clearly, there exists a unique integer vector p so that $x + p \in \mathrm{par}(V)$. If $x \in \mathbb{Z}^n$ and $\lambda \in \mathbb{Z}^n$ is the V-coefficient vector of x, then the V-coefficient vector of $x + p$ is $(\mathrm{mod}(\lambda_1, d)/d, \ldots, \mathrm{mod}(\lambda_n, d)/d)$. The $\mathrm{par}(V)$-coefficient vectors form a group $G = G(V)$ with respect to $\mathrm{mod}\, d$ addition. This is the factor-group of the additive group of integer vectors with respect to the subgroup generated by V, moreover the following well-known facts hold:

Lemma 3.1 *Let* $V := v_1, \ldots, v_n \in \mathbb{Z}^n$. *Then:*

(a) $\mathrm{par}(V \setminus v_n) = \{0\}$ *if and only if there exists a unimodular transformation (and possibly*

permutation of the coordinates) such that $v_i := e_i$ $(i = 1, \dots, n-1)$, $v_n = (a_1, \dots, a_{n-1}, d)$, *where* $d = \det(v_1, \dots, v_n)$ *and* $0 < a_i < d$ *for all* $i = 1, \dots, n-1$.

(b) If $\mathrm{par}(V \setminus v_n) = \{0\}$, *then* $G(V)$ *is a cyclic group.*

(c) If $\mathrm{par}(V \setminus v_n) = \{0\}$ *then* $\mathrm{par}(V \setminus v_i) = \{0\}$ *for some* $i \in \{1, \dots, n-1\}$ *if and only if in (a)* $\gcd(a_i, d) = 1$.

Indeed, let the rows of a matrix M be the vectors $v_i \in \mathbb{Z}^n$ $(i = 1, \dots, n)$ and consider the Hermite normal form of (the column lattice of) M. If $\mathrm{par}(V \setminus v_n) = \{0\}$, then deleting the last row and column we get an $(n-1) \times (n-1)$ identity matrix, and (a), follows. Now (b) is easy, since $\mathrm{par}(V) = \{0\} \cup \{\lceil i/d(a_1, \dots, a_{n-1}, d) \rceil : i = 1, \dots, d-1\}$, that is, the $\mathrm{par}(V)$-coefficients are equal to $\{\mathrm{mod}(ih, d) : i = 1, \dots, d-1\}$, where $h := (d - a_1, \dots, d - a_n, 1)$. Statement (c) is also easy, since $\gcd(a_i, d) = \gcd(d - a_i, d) > 1$ if and only if there exists $j \in \mathbb{N}$, $j < d$ so that the i-th coordinate of $\mathrm{mod}(jh, d)$ is 0.

Statement (b) is very useful for proving properties forr *all* the parallelepiped P: one can generate the $V := \{v_1, \dots, v_n\}$-coefficients of all the $d-1$ nonzero points of P by taking the $\mathrm{mod}\, d$ multiples of the V-coefficient vector of some generator $h = (h_1, \dots, h_n) \in P$ (cf. [10], or [14]). *If the polytope we are considering is described in terms of inequalities satisfied by a function of the* $\mathrm{par}(V)$*-coefficients*, then it is useful to understand how the $\mathrm{par}(V)$-coefficient vector $\mathrm{mod}((i+1)h, d)$ changed comparing to $\mathrm{mod}(ih, d)$.

For instance, for the simplex $S := \mathrm{conv}(v_1, \dots, v_n)$ to be empty means exactly that the sum of the V-coefficients of any vector in P is strictly greater than d. For any coordinate $0 < a \le d-1$ of h one simply has $\mathrm{mod}((i+1)a, d) = \mathrm{mod}(ia, d) + a$, unless the interval $(\mathrm{mod}(ia, d), \mathrm{mod}(ia, d) + a]$ contains a multiple of d, that is, if and only if $\mathrm{mod}(ia, d) + a \ge d$. In this latter case $\mathrm{mod}((i+1)a, d) = \mathrm{mod}(ia, d) + a - d$, and we will say that i is a *jump-coefficient of* a $\mathrm{mod}\, d$.

Hence $\mathrm{mod}\, d$ inequalities can be treated as ordinary inequalities, corrected by controling of jump-coefficients. We will need only the following simply stated Lemma 3.2, relating containment relations between the sets of jump coeffients, to divisibility relations.

We say that $i \in \{1, \dots, d-1\}$ is a *jump-coefficient* of $a \in \mathbb{N}$ $\mathrm{mod}\, d$ $(1 \le a < d)$, if $\lfloor (i+1)a/d \rfloor > \lfloor ia/d \rfloor$ (equivalently, if $\mathrm{mod}((i+1)a, d) < \mathrm{mod}(ia, d)$). If $a = 1$, then $J_a(d) = \emptyset$, and if $a \ge 2$, the set of jump-coefficients of $a \,\mathrm{mod}\, d$ is

$(*)$ $\quad J_a(d) := \{\lfloor id/a \rfloor : i = 1, \dots, a-1\}$.

Let us illustrate our goal and the statement we want to prove on the easy example of $a = 2$ and d odd: let us show that $J_a(d) \subseteq J_b(d)$ if and only if b is even. Indeed, 2 has just one jump-coefficient, $\lfloor d/2 \rfloor$. So $J_a(d) \subseteq J_b(d)$ if and only if $\lfloor d/2 \rfloor \in J_b$, that is, if and only if the interval $(\lfloor d/2 \rfloor b, (\lfloor d/2 \rfloor + 1)b]$ contains a multiple of d. It does contain a multiple of $d/2$: $bd/2$, and since $b/2 < d/2$ this is the only multiple of $d/2$ it contains. But $bd/2$ is a multiple of d if and only if b is even, as claimed.

Lemma 3.2 states a generalization of this statement for arbitrary a. Let us first visualise the statement, and $(*)$ – a basic tool in the proof :

Let $d \in \mathbb{N}$ be arbitrary, and $0 < a, b < d$. The points $A := \{id/a : i = 1, \dots, a-1\}$ divide the interval $[0, d]$ into a equal parts. Each of these parts has length bigger than 1, so the points of A lie in different intervals $(i, i+1]$. Now $(*)$ means exactly that

$(**)$ $i \in J_a$ *if and only if the interval* $(i, i+1]$ *contains an element of* A.

If $b > a$, then clearly, there is an interval $(i, i+1]$ containing a point of B and not caintaining a point of A. If b is a multiple of a, then obviously, $B \supseteq A$. If $d - a$ is a multiple of $d - b$, then again $B \supseteq A$ is easy to prove (see the Fact below).

If $a, b \leq d/2$, then $d-b \,|\, d-a$ cannot hold. The following lemma states that under this condition the above remark can be reversed: if a does not divide b, then $A \setminus B \neq \emptyset$. If $a \leq d/2$ and $b > d/2$, then $J_a(d) \subseteq J_b(d)$ can hold without any of $a|b$ or $d-b \,|\, d-a$ being true (see example below).

Let us first note the following statement that will be frequently used in the sequel:

Fact: $\{J_a(d), J_{d-a}(d)\}$ is a bipartition of $\{1, \ldots, d-1\}$. (Easy.)

The following lemma looks like a simple and quite basic statement :

Lemma 3.2 *Let d, $a, b \in \mathbb{N}$, $0 < a, b < d/2$, $\gcd(a, d) = \gcd(b, d) = 1$. If $J_a(d) \subseteq J_b(d)$, then $a|b$.*

Proof. Let $a, b \in \mathbb{N}$, $0 < a, b < d/2$, $J_a(d) \subseteq J_b(d)$. Then $a \leq b$. Suppose a does not divide b, and let us show $J_a \setminus J_b \neq \emptyset$. We have then $2 \leq a < b$, and $J_a \setminus J_b \neq \emptyset$ means exactly the existence of $k \in \{1, \ldots, a-1\}$ such that $\lfloor kd/a \rfloor \notin J_b$ (see $(*)$).
Claim : Let $k \in \{1, \ldots, a-1\}$. Then $\lfloor kd/a \rfloor \notin J_b$ if and only if both

$$\frac{\mathrm{mod}(kd, a)}{\mathrm{mod}(kb, a)} < \frac{d}{b}\ , \text{ and } \frac{a - \mathrm{mod}(kd, a)}{a - \mathrm{mod}(kb, a)} < \frac{d}{b} \text{ hold.}$$

This statement looks somewhat scaring, but we will see that it expresses exactly what $\lfloor kd/a \rfloor \notin J_b$ means if one exploits $(*)$ for b, and $(**)$ for a:

Indeed, then $\lfloor kd/a \rfloor \notin J_b$ if and only if for all $i = 1, \ldots, b-1$: $id/b \notin (\lfloor kd/a \rfloor, \lfloor kd/a \rfloor + 1]$. Let us realize, that instead of checking this condition for all i, it is enough to check it for those possibilities for i for which id/b has a chance of being in $(\lfloor kd/a \rfloor, \lfloor kd/a \rfloor + 1]$:

Since $\frac{kd}{a} = \frac{kb}{a}\frac{d}{b}$ and hence $\lfloor \frac{kb}{a} \rfloor \frac{d}{b} \leq \frac{kd}{a} \leq \lceil \frac{kb}{a} \rceil \frac{d}{b}$, there are only two such possibilities for i: $\lfloor \frac{kb}{a} \rfloor$ and $\lceil \frac{kb}{a} \rceil$. In other words, $\lfloor \frac{kd}{a} \rfloor \notin J_b$ if and only if

$$\lfloor \frac{kb}{a} \rfloor \frac{d}{b} < \lfloor \frac{kd}{a} \rfloor, \text{ or } \lceil \frac{kb}{a} \rceil \frac{d}{b} > 1 + \lfloor \frac{kd}{a} \rfloor.$$

Subtract from these inequalities the equality $\frac{kb}{a}\frac{d}{b} = \frac{kd}{a}$, and apply $\lfloor p/q \rfloor = \frac{p - \mathrm{mod}(p,q)}{q}$:

$$-\frac{\mathrm{mod}(kb, a)}{a}\frac{d}{b} < -\frac{\mathrm{mod}(kd, a)}{a},$$

which is the first inequality of the claim, and

$$\frac{a - \mathrm{mod}(kb, a)}{a}\frac{d}{b} > 1 - \frac{\mathrm{mod}(kd, a)}{a},$$

which is the second inequality. The claim is proved.

Let $g := \gcd(a, b)$. The values $\mathrm{mod}(ib, a)$ $(i \in \{0, 1, \ldots, a-1\})$ are from the set $\{jg : j = 0, \ldots, (a/g) - 1\}$, and each number in this set is taken g times. Depending on whether a/g is even or odd, $a/2$ or $a - g/2$ is in this set.

So there exist g different values of i for which $a/2 - g/2 \leq \mathrm{mod}(ib, a) \leq a/2$ and since for all of these g values $\mathrm{mod}(id, a)$ is different (because of $\gcd(a, d) = 1$), for at least one of them $\mathrm{mod}(id, a) \leq a - g$. For this i we have $\frac{\mathrm{mod}(id,a)}{\mathrm{mod}(ib,a)} \leq \frac{a-g}{a/2-g/2} = 2$, and since $a - \mathrm{mod}(ib, a) \geq a/2$, $\frac{a-\mathrm{mod}(id,a)}{a-\mathrm{mod}(ib,a)} \leq 2$ holds as well. Since $d/b > 2$ by assumption, the condition of the claim is satisfied and we conclude $\lfloor id/a \rfloor \notin J_b$. $\square$

Corollary 3.3 *Let d, $a, b \in I\!N$, $d/2 < a, b < d$, $\gcd(a,d) = \gcd(b,d) = 1$. If $J_a(d) \subseteq J_b(d)$, then $d - b \mid d - a$.*

Indeed, according to the Fact proved before the Lemma, $J_a(d) \subseteq J_b(d)$ implies $J_{d-b}(d) \subseteq J_{d-a}(d)$, and clearly, $0 < d-b, d-a < d/2$ $\gcd(d-b, d) = \gcd(d-a, d) = 1$. Hence the Lemma can be applied to $d-b, d-a$ and it establishes $d - b \mid d - a$.

The following example shows that the Lemma or its corollary are not necessarily true if $a < d/2$, $b > d/2$, even if the condition of the lemma is 'asymptotically true' ($\lim d/b = 2$ if $k \to \infty$): let $k \in \mathbb{N}$, $k \geq 3$; $d := 6k - 1$, $a = 3$, $b = 3k + 4$.

Then $J_a = \{2k-1, 4k-1\} \subseteq J_b$ – let us check for instance $2k - 1 \in J_b$: $(2k-1)b = 6k^2 + 5k - 4 = (6k-1)k + 6k - 4 \equiv 6k - 4 \bmod 6k - 1$. Since $3k + 4 > (6k-1) - (6k-4) = 3$, $2k - 1$ is a jump coefficient of $b = 3k + 4 \bmod d$.

For $k = 2$ we do not get a real example: $a = 3$, $b = 10$, $d = 11$; $J_a \subseteq J_b$ is true, and 3 is not a divisor of 10, but the corollary applies to $d - a = 8$ and $d - b = 1$. One gets the smallest example with $J_a \subseteq J_b$ and neither $a|b$ nor $d - b \mid d - a$ by substituting $k = 3$: then $a = 3$, $b = 13$, $d = 17$.

4 A polynomial certificate

In the introduction we formulated a somewhat more general question than the emptiness of lattice simplices: *given a linearly independent set $V := \{v_1, \ldots, v_n\}$ of integer vectors, is there a* $\mathrm{par}(V)$*-coefficient vector whose (weighted) sum is smaller than a pre-given value.* If all the coefficients are 1, and the pregiven value is $d := \det(V)$ we get back the problem of the nonemptiness of $\mathrm{conv}(0, v_1, \ldots, v_n)$.

For integer weights $0 \leq a_1, \ldots, a_n \leq d - 1$, *the congruence* $\sum_{i=1}^n a_i\lambda_i \equiv 0 \bmod d$ $(\lambda_1, \ldots, \lambda_n \in I\!N)$ *implies* $\sum_{i=1}^n a_i\lambda_i \geq d$, unless $a_i\lambda_i = 0$ for all $i = 1, \ldots, n$. If the congruence holds for all $(\lambda_1, \ldots, \lambda_n) \in \mathrm{par}(V)$, then the inequality also holds, except if $\lambda_i = 0$ for all $i = 1, \ldots, n$ for which $a_i > 0$. We suppose that this exception does not occur. (This is automatically the case if all proper faces of $\mathrm{par}(V)$ are empty, or if $a_i > 0$ for all $i = 1, \ldots, n$.) Then, in order to certify the validity of the above inequality for the entire $\mathrm{par}(V)$, one only has to check the congruence to hold for a generating set.

Such inequalities (induced exactly by the 'orthogonal' space to $G(V) \bmod d$) can then be combined in the usual way of linear (or integer) programming, in order to yield new inequalities. We do not have an example where this procedure would not provide a 'short' certificate for a lattice simplex to be empty, or more generally, for the inequality $\sum_{i=1}^n \lambda_i/d > k$ $(k \in \mathbb{N})$ to hold.

By the symmetry of the parallelepiped, the maximum of k for which such an inequality can be satisfied is $k = n/2$.

For this extreme case (which occurs in the open cases of the integer Caratheodory property – and slightly changes for odd n) we conjecture that the simplest possible 'good certificate' can work:

Conjecture 4.1 *Let $e \in \{0, 1\}$, $e \equiv n \bmod 2$, and $V = \{v_1, \ldots, v_n\} \subseteq Z\!\!Z^n$ be linearly independent. Then $\sum_{i=1}^n \lambda_i \geq \lfloor n/2 \rfloor d + 1 - e$ holds for every $\lambda = (\lambda_1, \ldots, \lambda_n) \in G(V)$, if and only if there exists $\alpha = (\alpha_1, \ldots, \alpha_n) \in G(V)$, $\gcd(\alpha_i, d) = 1$ $(i = 1, \ldots, n)$, and a set $\mathcal{P}$ of $\lfloor n/2 \rfloor$ disjoint pairs in $\{1, \ldots, n\}$ such that for each pair $\{p, q\} \in \mathcal{P}$: $\alpha_p + \alpha_q = d$.*

The sufficiency of the condition is easy: α is a generator; for all $\lambda \in G(V)$, $\lambda > 0$; then $0 < \lambda_p + \lambda_q < 2d$ for every $\{p, q\} \in \mathcal{P}$, and $d \mid \lambda_p + \lambda_q$, so $\lambda_p + \lambda_q = d$ for every $\lambda \in G(V)$; $\sum_{i=1}^n \lambda_i \geq |\mathcal{P}| + 1 - e = \lfloor n/2 \rfloor d + 1 - e$ follows.

Conversely, if $\sum_{i=1}^{n} \lambda_i \geq \lfloor n/2 \rfloor d + 1 - e$ for every $\lambda \in G(V)$, then $\mathrm{par}(V \setminus v_i) = \{0\}$ $(i = 1, \ldots, n)$ is obvious: if say $\mathrm{par}(V \setminus v_n) \neq \{0\}$, then by symmetry, there exists $\lambda \in \mathrm{par}(V \setminus e_n) \neq \{0\}$, $\sum_{i=1}^{n} \lambda_i / d \leq (n-1)/2$, a contradiction. So $G(V)$ is cyclic. In order to prove the conjecture, we have to prove that $\sum_{i=1}^{n} \lambda_i \geq \lfloor n/2 \rfloor d + 1 - e$ for every $\lambda = (\lambda_1, \ldots, \lambda_n) \in G(V)$ implies $\lambda_p + \lambda_q = d$ for all $\mathrm{par}(V)$ coefficient, or equivalently, for a generator.

We show this Conjecture in the special case $n \leq 4$, when it is equivalent to a celebrated result of White [15]. Instead of using White's theorem, we provide a new, simpler proof based on Lemma 3.2. We hope that these results will be also useful in more general situations.

An integer simplex $S \subseteq \mathbb{R}^2$ is empty if and only if its two nonzero vertices form an empty parallelepiped, that is, if and only if they define a unimodular matrix. (This is trivial from the Hermite normal form, or just by the symmetry of parallelepipeds.)

Let now $n = 3$, and let $A, B, C \in \mathbb{Z}^3$ be the nonzero vertices of the simplex $S \subseteq \mathbb{R}^3$. It follows from the result on $n \leq 2$ applied to the facets of S after applying Lemma 3.1, that $G(V)$ is cyclic, and then the input of the problem can be given in a shorter and more symmetric form: we suppose that the input consists of only three numbers, the $V := \{A, B, C\}$-coordinates of a generator (α, β, γ) of $G(V)$ (instead of the vectors A, B, C themselves). White's theorem (see [15] or [10]) can be stated as follows:

Theorem 4.2 *Let $S \subseteq \mathbb{R}^3$ be an integer simplex with vertices $O = 0 \in \mathbb{R}^3$, and A, B, C linearly independent vectors, $d := \det(A, B, C)$, $V := \{A, B, C\}$. The following statements are equivalent:*

(i) $\mathrm{par}(A, B) = \mathrm{par}(B, C) = \mathrm{par}(A, C) = \{0\}$, *and there exists a* $\mathrm{par}(V)$*-coefficient vector* (α, β, γ) *such that* $\gcd(\alpha, d) = \gcd(\beta, d) = \gcd(\gamma, d) = 1$, *moreover the sum of two of α, β, γ is equal to d, and the third is equal to 1.*

(ii) $\mathrm{par}(A, B) = \mathrm{par}(B, C) = \mathrm{par}(A, C) = \{0\}$, *and for every* $\mathrm{par}(V)$*-coefficient vector (α, β, γ), after possible permutation of the coordinates*
$mod\ (\alpha, d)$ + $mod\ (\beta, d) = d$ $(i = 1, \ldots, d-1)$.

(iii) S is empty.

Proof. If (i) holds, then $(\alpha, \beta, \gamma) \in G(V)$ is a generator, so (ii) also holds. If (ii) holds, then for all $x \in \mathrm{par}(A, B, C)$ the sum of the first two V-coefficients is divisible by, and it follows that it is equal to d; since $\mathrm{par}(A, B) = \{0\}$, the third V-coordinate of x is nonzero, so the sum of the V-coefficients is greater than d which means exactly that $x \notin S$. So S is empty.

The main part of the proof is (iii) implies (i). We follow the proof of [14] Theorem 2.2:

Let $S \subseteq \mathbb{R}^3$ be an empty integer simplex. Then every face of S is also integer and empty. Therefore (since the faces are two-dimensional) $\mathrm{par}(V') = \{0\}$ for every proper subset $V' \subset V$. Now by Lemma 3.1, the group $G(V)$ is cyclic. Let the $\mathrm{par}(V)$-coefficient (α, β, γ) be a generator.

Claim 1: $d < \mathrm{mod}(i\alpha, d) + \mathrm{mod}(i\beta, d) + \mathrm{mod}(i\gamma, d) < 2d \quad (i = 1, \ldots, d-1)$.

Indeed, since S is empty, $\mathrm{mod}(i\alpha, d) + \mathrm{mod}(i\beta, d) + \mathrm{mod}(i\gamma, d) > d$, and $(d - \mathrm{mod}(i\alpha, d)) + d - \mathrm{mod}(i\beta, d) + d - \mathrm{mod}(i\gamma, d) > d$, for all $i = 1, \ldots, d-1$.

Claim 2: There exists a generator $(\alpha, \beta, \gamma) \in G(V)$ such that $\alpha + \beta + \gamma = d + 1$.

Note that $\mathrm{mod}(i\alpha, d) + \mathrm{mod}(i\beta, d) + \mathrm{mod}(i\gamma, d)$ is mod d different for different $i \in \{1, \ldots, d-1\}$, because if for j, k, $0 \leq j < k \leq d-1$ the values are equal, then for $i = k - j$ the expression would be divisibile by d, contradicting Claim 1. So $\{\mathrm{mod}(i\alpha, d) + \mathrm{mod}(i\beta, d) + \mathrm{mod}(i\gamma, d) : i = 1, \ldots, d-1\}$ is the same as the set $\{d+1, \ldots, 2d-1\}$, in particular there exists $k \in \{1, \ldots, d-1\}$ such that mod $(k\alpha, d) + mod\ (k\alpha, d) + mod\ (k\gamma, d) = d+1$. Then clearly, mod $(ik\alpha, d) + mod\ (ik\alpha, d) + mod\ (ik\gamma, d) = d+i$, so $(k\alpha, k\beta, k\gamma)$ is also a generator, and the claim is proved.

Choose now (α, β, γ) be like in Claim 2.

Claim 3. Each $i = 1, \dots, d-1$ is jump-coefficient of exactly one of α, β and γ.

Indeed, because of Claim 1 we have $\mathrm{mod}((i+1)\alpha, d) + \mathrm{mod}((i+1)\beta, d) + \mathrm{mod}((i+1)\gamma, d) = \mathrm{mod}(i\alpha, d) + \mathrm{mod}(i\beta, d) + \mathrm{mod}(i\gamma, d) + \alpha + \beta + \gamma - d$ and the claim follows.

Fix now the notation so that $\alpha \geq \beta \geq \gamma$. If we apply Claim 3 to $i = 1$ we get that $\alpha > d/2$, $\beta < d/2$, $\gamma < d/2$.

Hence Lemma 3.2 can be applied to $d - \alpha, \beta, \gamma$: Claim 3 means $J_\beta \cap J_\alpha = \emptyset$, $J_\gamma \cap J_\alpha = \emptyset$, whence, because of the Fact noticed before Lemma 3.2 $J_\beta, J_\gamma \subseteq J_{d-\alpha}$. So by Lemma 3.2 $\beta, \gamma \mid d - \alpha$. If both β and γ are proper divisors, then they are both smaller than the half or $d - \alpha$, that is, $\beta + \gamma \leq d - \alpha$, contradicting $\alpha + \beta + \gamma = d + 1$.

So $\beta = d - \alpha$, and then $\gamma = 1$ finishing the proof of the theorem. □

Note that the above proof contains most of the proof of [14] Theorem 2.2 and more: the key-statement of that proof is the existence of a par(V)-coefficient (α, β, γ) such that $\alpha+\beta+\gamma = d+1$. The above proof sharpens that statement by adding that $\gamma = 1$ in this par(V)-coefficient. This additional fact implies some simplifications for proving the main result of [14]. Here we omit these, we prefere to deduce the following, in fact equivalent versions of Theorem 4.2 ([11],[15],[12]). It turns out that the various versions are the same modulo row permutations in the Hermite normal form of a 3×3 matrix that has two different types of rows:

Corollary 4.3 *$S = conv(0, A, B, C) \subseteq \mathbb{R}^3$, $(A, B, C \in \mathbb{Z}^3)$ is empty if and only if the Hermite normal form of one of the (six) 3×3 matrices M whose rows are A, B, C in some order has rows $(1, 0, 0)$, $(0, 1, 0)$, $(a, d-a, d)$, $(\gcd(a, d) = 1)$.*

Proof. The if part is obvious, since for an arbitrary par(V)-coefficient vector (α, β, γ): $\alpha+\beta = d$ and $\gamma > 0$, so $\alpha/d + \beta/d + \gamma/d > 1$.

The only if part is an obvious consequence of the theorem: let the two particular rows mentioned in Theorem 4.2 (i) be the first two rows of a matrix M, and let the remaining row be the third. Then M is a 3×3 matrix, and with the notation of Theorem 4.2, the rows of the Hermite normal form of M are the following : the first two rows are $(1, 0, 0)$, $(0, 1, 0)$ since the parallelepiped generated by any two nonzero extreme rays is $\{0\}$; the third is $(d - \alpha, d - \beta, d)$. Since by Theorem 4.2 $\alpha + \beta = d$, the statement follows. □

Corollary 4.4 *$S = conv(0, A, B, C) \subseteq \mathbb{R}^3$ $(A, B, C \in \mathbb{Z}^3)$ is empty if and only if the Hermite normal form of one of the (six) 3×3 matrices M whose rows are A, B, C in some order has rows $(1, 0, 0)$, $(0, 1, 0)$ and $(1, b, d)$, $(\gcd(b, d) = 1)$.*

Proof. Again, the if part is obvious, because in an arbitrary par(V)-coefficient vector the sum of the first and third coordinate is d, and the second coordinate is positive.

The proof of the only if part is also the same as that of the previous corollary, with the only difference that now we let the two particular rows mentioned in Theorem 4.2 (i) be the first and third row of M. □

Corollary 4.5 *The integer simplex $S \subseteq \mathbb{R}^n$, $n \leq 3$ is empty, if and only if $W(P) = 1$ for all faces P of S (that is, for $P = S$ and for all P which is any of the facets or edges of S).*

Proof. If $n \leq 2$ the statement is obvious (see above). The only if part follows from the previous corollary: after applying a unimodular transformation, the three nonzero vertices of S will be $(1,0,0)$, $(0,1,0)$ and $(1,b,d)$. The vector $w := (1,0,0)$ shows that the width of S is 1.

Conversely, suppose $W(P) = 1$ for every face P of the integer simplex S. Suppose indirectly $v \in S \cap \mathbb{Z}^n$ is not a vertex of S. Because of the statement for $n \leq 2$, v does not lie on a face $P \subset S$, $P \neq S$. For a vector $w \in \mathbb{Z}^n$ defining the width, $\min\{w^T x : x \in S\} < w^T v < \max\{w^T x : x \in S\}$, because the vectors achieving the minimum or the maximum constitute a face of S. But then $W(S) = \max\{w^T x : x \in S\} - \min\{w^T x : x \in S\} = \max\{w^T x : x \in S\} - w^T v + w^T v - \min\{w^T x : x \in S\} \geq 1 + 1 = 2$, a contradiction. $\square$

Corollary 4.6 *Conjecture 4.1 is true for* $n \leq 4$.

Proof. For $n \leq 3$ the statement is a consequence of Theorem 4.2.

Let $n = 4$. As noticed after Conjecture 4.1, we only have to prove that $\sum_{i=1}^{n} \lambda_i \geq 2d$ for every $\lambda \in G(V)$ implies that for some generator α (possibly after permuting the coordinates) $\alpha_1 + \alpha_2 = d$, $\alpha_3 + \alpha_4 = d$.

Let $\alpha \in G(V)$ be a generator, and suppose without loss of generality $\alpha_4 = d - 1$. (This holds after multiplying α by a number relatively prime to d.) Then Claim 2 and 3 of the proof of Theorem 4.2 hold with the choice $\alpha := \alpha_1$, $\beta := \alpha_2$, $\gamma := \alpha_3$, and the proof can be finished in the same way. $\square$

This argument can be copied for proving that Conjecture 4.1 holds true for $n = 2k - 1$ if and only if it is true for $n = 2k$.

5 Computing the width of polytopes

In spite of some counterexamples (see Section 1), the width and the number of lattice points of a lattice simplex are correlated, and some of the remarks above are about this relation. It is interesting to note that the complexity of computing these two numbers seem to show some analogy: it is hard to compute the number of integer points of a polytope, but according to a recent result of Barvinok[2] this problem is polynomially solvable if the dimension is bounded; we show below that to compute the width of quite particular simplices is already NP-hard, however, there is a simple algorithm that finds the width in polynomial time if the dimension is fixed. The proofs are quite easy:

Theorem 5.1 *Let* $a \in \mathbb{N}^n$. *It is NP-complete to decide whether the width of* $\mathrm{conv}(e_1, \ldots, e_n, a)$ *is at most* 1.

Proof. The defined problem is clearly in NP. We reduce PARITION to this problem. Let the input of a PARTITION problem be a vector $a \in \mathbb{N}^n$, where $-a_n := \sum_{i=1}^{n-1} a_i/2$ and we can suppose without loss of generality, $a_i > 3$ $(i = 1, \ldots, n)$. (We multiply by 4 an arbitrary instance of PARTITION. The question of PARTITION is whether there exists a subset $I \subseteq \{1, \ldots, n-1\}$ such that $\sum_{i \in I} a_i = -a_n$, and this is unchanged under multiplication of all the data by a scalar.)

It is easy to see that the width of $P := \mathrm{conv}(e_1, \ldots, e_n, a)$ is at most 1 if and only if the defined PARTITION problem has a solution.

Indeed, if $I \subseteq \{1, \ldots, n-1\}$ is a solution, then for the vector $w \in \mathbb{Z}^n$ defined by $w_i := 1$ if $i \in I \cup \{n\}$, and $w_i := 0$ if $i \notin I \cup \{n\}$ we have $w^T e_i \leq 1$ $(i = 1, \ldots, n)$, $w^T a = 0$.

Conversely, let $W(P) \leq 1$, and let $w \in \mathbb{N}^n$ be the vector defining the width. Then $|w^T x - w^T y| \leq 1$, $x, y \in \{e_1, \ldots, e_n\}$ means that the value of w_i $(i = 1, \ldots, n)$ is one of two consecutive integers, and these are nonnegative without loss of generality: for some $k \in \mathbb{N}$ and $K \subseteq \{1, \ldots, n\}$, $w_i := k + 1$ if $i \in K$ and $w_i := k$ if $i \notin K$; but then $w^T a = k \sum_{i=1}^{n} a_i + \sum_{i \in K} a_i$. Since w defines the width, $|w^T a| \in \{k, k+1\}$, and an easy computation shows that this is possible only if $k = 0$ and $K \setminus \{n\}$ is a solution of the partition problem. $\square$

Let us consider a polytope $P := \{x \in \mathbb{R}^n : Ax \leq b\}$ where A is a matrix with n columns. Denote the i-th row of A by a_i, and the corresponding right hand side by b_i. For simplicity (and without loss of generality) suppose that P is full dimensional. If v is a vertex of P, denote $C_v := \text{cone}(a_i : a_i^T v = b_i)$ and let $X_{u,v}$ denote the set of extreme rays of the cone $C_u \cap -C_v$ so that for every $x \in X_{u,v} : x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, $x_i \in \mathbb{Z}$, $(i = 1, \ldots, n)$, and $\gcd(x_1, \ldots, x_n) = 1$. Let

$$Z_{u,v} := \bigcup \{\text{conv}(X \cup \{0\}) : X \subseteq X_{u,v},\ X \text{ is a basis of } \mathbb{R}^n\} \cap \mathbb{Z}^n.$$

Theorem 5.2 *$W(P) = \min w^T(u - v)$ over all pairs of vertices u, v of S, and all $w \in Z_{u,v}$.*

Proof. By definition, the width of P is the minimum of $\max\{c^T(u-v) : u, v \in P\}$ over all vectors $c \in \mathbb{Z}^n \setminus \{0\}$. Let w be the minimizing vector. It follows from the theory of linear programming, that u, v can be chosen to be vertices of P which maximize and respectively minimize the linear objective function $w^T x$; moreover, by the duality theorem of linear programming, w is then a nonnegative combination of vectors in C_u and also a nonnegative combination of vectors in $-C_v$; that is, $w \in C_u \cap -C_v$. Fix now u and v to be these two vertices of P. All that remains to be proved is:

Claim. For some linearly independent subset $X \subseteq X_{u,v}$, $w \in \text{conv}(X \cup \{0\}) \cap \mathbb{Z}^n$.

Indeed, since $w \in C_u \cap -C_v$, we know by Caratheodory's theorem that $w = \sum_{x \in X} \lambda_x x$ for some linearly independent $X \subseteq X_{u,v}$ and $\lambda_x \in \mathbb{R}$, $(x \in X)$. In order to prove the claim, we have to prove that $\sum_{x \in X} \lambda_x \leq 1$. If not: $w^T(u - v) = (\sum_{x \in X} \lambda_x x)^T (u - v) \geq (\sum_{x \in X} \lambda_x)(\min_{x \in X} x^T(u - v) > \min_{x \in X} x^T(u - v)$.

Let this minimum be achieved in $x_0 \in X$, so we proved $w^T(u - v) > x_0^T(u - v)$. Since $x_0 \in C_u \cap -C_v$, $\max\{x_0^T(u' - v') : u', v' \in P\}$ is achieved for $u' = u$ and $v' = v$. But then $w^T(u - v) > x_0^T(u - v)$ contradicts the definition of w. $\square$

Theorem 5.2 provides a polynomial algorithm for computing the width if n is fixed: all the extreme rays and facets of $C_u \cap -C_v$ can be computed in polynomial time; since $|X_{u,v}|$ is bounded by a polynomial, it contains a polynomial number of subsets X of fixed size n; for every X we solve a mixed integer program searching for an integer point in $\text{conv}(X \cup \{0\})$ but not in $X \cup \{0\}$. Mixed integer programs can be solved in polynomial time by Lenstra [9], see also Schrijver [13], page 260.

Haase and Ziegler [5] present $W(S)$ where S is a lattice simplex as the optimal value of a direct integer linear program. Their method is much simpler, and probably quicker. The finite set of points ('finite basis') provided by Theorem 5.2 can be useful for presenting a finite list of vectors that include a width-defining $w \in \mathbb{Z}^n$, for arbitrary polytopes.

The negative results of the paper do not exclude that the emptiness of integer simplices, and the width of empty integer simplices are decidable in polynomial time. The positive results show some relations between these notions, involving both complexity and bounds.

Acknowledgment: I am thankful to Jean-Michel Kantor for introducing me to the notions and the references of the subject; to Imre Bárány and Bernd Sturmfels for further helpful discussions.

References

[1] W. Banaszczyk, A.E. Litvak, A. Pajor, S.J Szarek, The flatness theorem for non-symmetric convex bodies via the local theory of Banach spaces, Preprint 1998.

[2] A. Barvinok, A polynomial time algorithm for counting integral point in polyhedra when the dimension is fixed, *Math. Oper. Res.*, 19 (1994), 769–779.

[3] J.W.S. Cassels, An Introduction to the Geometry of Numbers, Springer, Berlin, 1959.

[4] W. Bienia, L. Goddyn, P. Gvozdjak, A. Sebő, M. Tarsi, Flows, View Obstructions, and the Lonely Runner, J. Comb. Theory/B, Vol 72, No 1, 1998.

[5] C. Haase, G. Ziegler, On the maximal width of empty lattice simplices, preprint, July 1998/January 1999, 10 pages, European Journal of Combinatorics, to appear.

[6] R. Kannan, L. Lovász, Covering minima and lattice-point-free convex bodies, Annals of Mathematics, 128 (1988), 577-602.

[7] L. Lovász and M. D. Plummer, *Matching Theory*, Akadémiai Kiadó, Budapest, 1986.

[8] J-M. Kantor, On the width of lattice-free simplices, Composition Mathematica, 1999.

[9] H.W. Lenstra Jr., Integer programming with a fixed number of variables, Mathematics of Operations Research, 8, (1983), 538–548.

[10] B. Reznick, Lattice point simplices, Discrete Mathematics, 60, 1986, 219–242.

[11] J.E.Reeve, On the volume of lattice polyhedra, Proc. London Math. Soc. (3) 7 (1957), 378–395.

[12] H. Scarf, Integral polyhedra in three space, Math. Oper. Res., 10 (1985), 403–438.

[13] A. Schrijver, 'Theory of Integer and Linear Programming', Wiley, Chichester,1986.

[14] A. Sebő, Hilbert bases, Caratheodory's theorem and Combinatorial Optimization, IPCO1, (R. Kannan and W. Pulleyblank eds), University of Waterloo Press, Waterloo 1990, 431–456.

[15] G. K. White, Lattice tetrahedra, Canadian J. Math. 16 (1964), 389–396.