On Hilbert bases of polyhedral cones

Martin Henk and Robert Weismantel

Preprint SC96-12 (April 1996)

ON HILBERT BASES OF POLYHEDRAL CONES

MARTIN HENK AND ROBERT WEISMANTEL

Abstract. For a polyhedral cone $C = \text{pos}\{a^1, \ldots, a^m\} \subset \mathbb{R}^d$, $a^i \in \mathbb{Z}^d$, a subset of integral vectors $\mathcal{H}(C) \subset C \cap \mathbb{Z}^d$ is called a Hilbert basis of C iff (i) each element of $C \cap \mathbb{Z}^d$ can be written as a non-negative integer combination of elements of $\mathcal{H}(C)$ and (ii) $\mathcal{H}(C)$ has minimal cardinality with respect to all subsets of $C \cap \mathbb{Z}^d$ for which (i) holds.

We show that various problems related to Hilbert bases are hard in terms of computational complexity. However, if the dimension and the number of elements of the Hilbert basis are fixed, a Hilbert basis can always be computed in polynomial time.

Furthermore we introduce an algorithm for computing the Hilbert basis of a polyhedral cone. The finiteness of this method is deduced from a result about the height of a Hilbert basis which, in particular, improves on former estimates.

1. Introduction

Throughout the paper $\mathbb{R}^d$ denotes the d-dimensional Euclidean space and $\text{pos}S, \text{lin}S, \text{conv}S$ denote the positive, linear and convex hull of a subset $S \subset \mathbb{R}^d$, respectively. The cardinality of a set S is denoted by $\#S$ and for a vector $x \in \mathbb{R}^d$ its i-th coordinate is denoted by x_i. The i-th unit vector is represented by e^i. $|\cdot|$ denotes the Euclidean norm and the maximum norm is denoted by $|\cdot|_\infty$. A cone $C \subset \mathbb{R}^d$ is a set with the properties that $x + y \in C$ if $x, y \in C$ and $\lambda x \in C$ if $x \in C$, $\lambda \geq 0$. A cone C is called pointed if the set $C \backslash \{0\}$ is strictly contained in an open halfspace, i.e., there exists $c \in \mathbb{R}^d$ such that $c^T x < 0$ for all $x \in C \backslash \{0\}$. If $C = \text{pos}\{a^1, \ldots, a^m\}$ with vectors a^i, $1 \leq i \leq m$, then C is called a polyhedral cone or a finitely generated cone.

Here we are studying polyhedral cones $C \subset \mathbb{R}^d$ that can be represented as

$$C = \text{pos}\{a^1, \ldots, a^m\},$$

where $a^i \in \mathbb{Z}^d$ for all $1 \leq i \leq m$. We remark that such a cone can also be described by a system of inequalities $C = \{x \in \mathbb{R}^d : Ax \leq 0\}$ with a suitable matrix $A \in \mathbb{Z}^{l \times d}$ (cf. [Min96]). To avoid some trivial cases we always assume $C \neq \{0\}$.

It is well known that for every polyhedral cone C there exists a set $\mathcal{H}_{\mathbb{Z}^d}(C) \subset C \cap \mathbb{Z}^d$ such that (cf. [Hil90], [Sch86])

The work of the first author is supported by the Gerhard-Hess Forschungs-Förderpreis of the German Science Foundation (DFG) awarded to Günter M. Ziegler (Zi 475/1-1).

1. each $z \in C \cap \mathbb{Z}^d$ can be expressed as a positive integer combination of elements in $\mathcal{H}_{\mathbb{Z}^d}(C)$, i.e. $z = \sum_{h \in \mathcal{H}_{\mathbb{Z}^d}(C)} z_h h$, $z_h \in \mathbb{N}$.
2. $\mathcal{H}_{\mathbb{Z}^d}(C)$ has minimal cardinality with respect to all subsets of $C \cap \mathbb{Z}^d$ for which (1) holds.

The set $\mathcal{H}_{\mathbb{Z}^d}(C)$ is called the **Hilbert basis** of C. If the cone is pointed it is uniquely determined by the following characterization (cf. [Sch86])

$$\mathcal{H}_{\mathbb{Z}^d}(C) = \Big\{ h \in C \cap \mathbb{Z}^d \backslash \{0\} : h \text{ is not the sum of two other vectors in } C \cap \mathbb{Z}^d \backslash \{0\} \Big\}. \tag{1.1}$$

It is easy to see that the Hilbert basis is contained in the parallelepiped spanned by $a^1, \dots, a^m$, that is

$$\mathcal{H}_{\mathbb{Z}^d}(C) \subset \mathcal{P}_{\mathbb{Z}^d}(C) := \{a^1, \dots, a^m\} \cup \left\{ a \in C \cap \mathbb{Z}^d \backslash \{0\} : a = \sum_{i=1}^{m} \lambda_i a^i, 0 \leq \lambda_i < 1,\, 1 \leq i \leq m \right\}. \tag{1.2}$$

Hilbert bases are strongly related to the theory of integer programming. Without claiming completeness we list three areas in which Hilbert bases play a central role.

- A rational system $Ax \leq b$ is total dual integrality (TDI) if and only if for each face F of the polyhedron $P = \{x : Ax \leq b\}$, the rows $(a^1)^T, \dots, (a^k)^T$ of A satisfied with equality by all $x \in F$ contain the Hilbert basis of the cone $C_F = \text{pos}\{a^1, \dots, a^k\}$ [Sch86].
- Universal test sets of integer programs can be constructed from Hilbert bases of certain cones, see [Gra75], [Tho94], [UWZ94].
- In polyhedral combinatorics one is often interested in deriving an inequality description of a polyhedron that is given as the convex hull of its vertices. Sometimes such an inequality system can be explained via Hilbert bases as in the case of the 0/1 knapsack polytope $\sum_{i=1}^{n} a_i x_i \leq b$ when $\#\{a_i : 1 \leq i \leq n\} = 2$, see [Wei94].

We also want to remark that Hilbert bases are related to the theory of desingularizations of toric varieties (cf. [Dai95], [DHZ96], [Stu96]). In this context it is an interesting question to bound the so called height of a Hilbert basis. We study this problem in the next section and apply it later to prove the finiteness of an algorithm for computing a Hilbert basis (see section 4). In section 3 we deal with complexity issues for problems about Hilbert bases. We also show that a Hilbert basis can be found in polynomial time provided, the dimension and the cardinality of the Hilbert basis is fixed.

2. The height of a Hilbert basis

Before making precise our problem let us extend the notion of Hilbert bases to arbitrary lattices. To this end we replace the standard lattice $\mathbb{Z}^d$

by an arbitrary d-dimensional lattice $\Lambda \subset \mathbb{R}^d$. For a pointed cone $C = \mathrm{pos}\{a^1, \dots, a^m\}$ with $a^i \in \Lambda$ the Hilbert basis is denoted by $\mathcal{H}_\Lambda(C)$.

If $l^1, \dots, l^d$ is a basis of Λ, i.e., $\Lambda = \{z_1 l^1 + \cdots + z_d l^d : z_i \in \mathbb{Z}\}$ and $l^1, \dots, l^d$ are linearly independent, then $\det(\Lambda) = |\det(l^1, \dots, l^d)|$ is called the determinant of the lattice. For a subset $\{a^1, \dots, a^d\}$ of d linearly independent lattice points $a^i \in \Lambda$ the quotient $|\det(a^1, \dots, a^d)|/\det(\Lambda) \in \mathbb{N}$ is called the index of $\{a^1, \dots, a^d\}$ with respect to Λ. This value equals the number of cosets of the lattice $\{z_1 a^1 + \cdots + z_d a^d : z_i \in \mathbb{Z}\}$ in the additive group Λ. For more information about lattices we refer to [GL87].

Let $C = \{a^1, \dots, a^m\}$, $a^i \in \Lambda$ be a pointed cone. For $h \in \mathcal{H}_\Lambda(C)$ the number

$$g_C(h) := \min\left\{ \sum_{i=1}^m \lambda_i : h = \sum_{i=1}^m \lambda_i a^i,\ \lambda_i \geq 0,\ 1 \leq i \leq m \right\}$$

is called the **height** of h. By (1.2) we have a trivial upper bound of $g_C(h) \leq m$. This bound can be improved easily, since by Carathéodory's Theorem, there are d vectors $a^{i_1}, \dots, a^{i_d}$ such that $h \in C' = \mathrm{pos}\{a^{i_1}, \dots, a^{i_d}\}$. Thus $h \in \mathcal{H}_\Lambda(C')$ and (1.2) yields $g_C(h) \leq d$. Indeed, it is well known that $g_C(h) < d - 1$, $d \geq 2$. This was first proved by Ewald&Wessels [EW91] in the context of complete toric varieties. A simpler proof can be found in [LTZ93].

Asymptotically the bound $d - 1$ is best possible. Let $\Lambda = \mathbb{Z}^d$ and let $e^i \in \mathbb{R}^d$ be the i-th unit vector. For $r \in \mathbb{N}\backslash\{0\}$ let

$$C(d,r) = \mathrm{pos}\left\{ e^1, \dots, e^{d-1}, re^d + \sum_{i=1}^{d-1} e^i \right\}.$$

$h = (1, \dots, 1)^T$ is an element of the Hilbert basis of height $(d-1)\cdot(r-1)/r + 1/r = (d-1) - (d-2)/r$. If r goes to infinity the height of $h = (1, \dots, 1)^T$ converges to the value $d - 1$.

One can also derive a sharp bound on the height of Hilbert basis elements. More precisely, we show

Theorem 2.1. *Let $\Lambda \subset \mathbb{R}^d$ be a lattice with $\det(\Lambda) > 0$ and let $C = \mathrm{pos}\{a^1, \dots, a^d\}$, $a^i \in \Lambda$, be a pointed cone with $|\det(a^1, \dots, a^d)| > 0$. For $h \in \mathcal{H}_\Lambda(C)$ one has*

$$g_C(h) \leq (d-1) - (d-2)\frac{\det(\Lambda)}{|\det(a^1, \dots, a^d)|}.$$

As an immediate consequence we obtain with Carthéodory's Theorem

Corollary 2.1. *Let $\Lambda \subset \mathbb{R}^d$ be a lattice with $\det(\Lambda) > 0$ and let $C = \mathrm{pos}\{a^1, \dots, a^m\}$ be a pointed cone with $\dim(C) = d$. For $h \in \mathcal{H}_\Lambda(C)$ one has*

$$g_C(h) \leq (d-1) - (d-2)\frac{\det(\Lambda)}{|\det(a^{i_1}, \dots, a^{i_d})|},$$

where $\{a^{i_1},\ldots,a^{i_d}\}$ *is a subset of* d *linearly independent lattice vectors with minimal index such that* $h \in \mathrm{pos}\{a^{i_1},\ldots,a^{i_d}\}$.

Furthermore, we get from Theorem 2.1 with the notation of (1.2) (cf. Theorem 2.3.2. ii) in [Liu91])

Corollary 2.2. *Let* $\Lambda \subset \mathbb{R}^d$ *be a lattice with* $\det(\Lambda) > 0$ *and let* $C = \mathrm{pos}\{a^1,\ldots,a^d\}$, $a^i \in \Lambda$, *be a pointed cone with* $|\det(a^1,\ldots,a^d)| > 0$. *If* $\mathcal{H}_\Lambda(C) = \mathcal{P}_\Lambda(C)$ *then for* $h \in \mathcal{H}_\Lambda(C)$ *satisfying*

$$h = \sum_{i=1}^{d} \lambda_i a^i, \quad \text{with} \quad 0 < \lambda_i < 1, \quad i = 1,\ldots,d, \tag{2.1}$$

one has

$$1 + (d-2)\frac{\det(\Lambda)}{|\det(a^1,\ldots,a^d)|} \le g_C(h).$$

Proof. Assume that there exists a vector $h \in \mathcal{H}_\Lambda(C)$ satisfying (2.1), but with $g_C(h) < 1 + (d-2)\det(\Lambda)/|\det(a^1,\ldots,a^d)|$. Then $\overline{h} = \sum_{i=1}^{d} a^i - h \in \mathcal{P}(C) = \mathcal{H}_\Lambda(C)$ and

$$g_C(\overline{h}) = d - g_C(h) > (d-1) - (d-2)\det(\Lambda)/|\det(a^1,\ldots,a^d)|.$$

This is a contradiction to Theorem 2.1. □

Remark. In [Liu91] it is claimed that $1 + (d-2)\det(\Lambda)/|\det(a^1,\ldots,a^d)|$ is a lower bound on the height of Hilbert bases elements even if they lie on the boundary of C. This is however not true for the following reason. Assume that there is a cone $C^d = \mathrm{pos}\{a^1,\ldots,a^d\}$ in $\mathbb{R}^d$ with respect to the integer lattice $\mathbb{Z}^d$ such that each $h \in \mathcal{H}_{\mathbb{Z}^d}(C^d) = \mathcal{P}_{\mathbb{Z}^d}(C^d)$ satisfies this lower bound. Then we can embed C^d in $\mathbb{R}^{d+n}$ and by adding the new generating vectors $e^{d+1},\ldots,e^{d+n}$ to C^d we obtain a new cone $C^{d+n} = \mathrm{pos}\{(a^1,0)^T,\ldots,(a^d,0)^T,e^{d+1},\ldots,e^{d+n}\}$ with

$$|\det((a^1,0)^T,\ldots,(a^d,0)^T,e^{d+1},\ldots,e^{d+n})| = |\det(a^1,\ldots,a^d)|.$$

In particular we have

$$\mathcal{H}_{\mathbb{Z}^{d+n}}(C^{d+n}) = \{(h,0)^T : h \in \mathcal{H}_{\mathbb{Z}^d}(C^d)\} \cup \{e^{d+1},\ldots,e^{d+n}\}$$

and thus $\mathcal{P}_{\mathbb{Z}^{d+n}}(C^{d+n}) = \mathcal{H}_{\mathbb{Z}^{d+n}}(C^{d+n})$. Hence the height of each $h \in \mathcal{H}_{\mathbb{Z}^d}(C^d)$ is even bounded from below by $1 + (d+n-2)/\det(C^d)$, for all $n \in \mathbb{N}$. Thus the assumption (2.1) is necessary indeed.

The proof of Theorem 2.1 is based on two lemmas that we present next. For two integers p, r we denote by $[p]_r$ the least integer $m \ge 0$ such that $p \equiv m \mod r$.

Lemma 2.1. *Let* $p, r \in \mathbb{N}$, $1 \le p \le r-1$, *and let* $\mathcal{M}(p,r) = \{j \in \{1,\ldots,r-1\} : [j \cdot p]_r \le p\}$. *Then* $\#\mathcal{M}(p,r) = p + \gcd(p,r) - 1$.

Proof. First assume $\gcd(p,r)=1$. Then $[kp]_r \neq [lp]_r$ for $1 \leq k \neq l \leq r-1$ and thus $\{[jp]_r : 1 \leq j \leq r-1\} = \{1,\dots,r-1\}$. Since $p \leq r-1$ we have $\#\mathcal{M}(p,r) = p$.

Next assume $\gcd(p,r) = q > 1$. By the first case we have $\#\mathcal{M}(p/q, r/q) = p/q$. Let $j \in \mathcal{M}(p/q, r/q)$ and $0 \leq i \leq q-1$. It is easy to see that $[(j+i\cdot r/q)p]_r = q[j\cdot p/q]_{r/q}$ and thus $[(j+i\cdot r/q)p]_r \leq p$. So

$$\mathcal{M}_*(p,r) := \{(j+i\cdot r/q) : j \in \mathcal{M}(p/q,r/q), i \in \{0,\dots,q-1\}\} \subset \mathcal{M}(p,r).$$

For $1 \leq j \leq (r/q)-1$ the numbers $(j+i\cdot r/q)$, $j \in \mathcal{M}(p/q,r/q)$, $i \in \{0,\dots,q-1\}$ are pairwise disjoint and this implies $\#\mathcal{M}_*(p,r) = p$.

Now, let $\mathcal{M}_0(p,r) = \{j \in \{1,\dots,r-1\} : [j\cdot p]_r = 0\}$. Obviously, $\mathcal{M}_0(p,r) = \{j\cdot r/q : j \in \{1,\dots,q-1\}\}$ and since $[j\cdot p]_r > 0$ for $j \in \mathcal{M}_*(p,r)$ we get

$$\#\mathcal{M}(p,r) \geq \#\mathcal{M}_*(p,r) + \#\mathcal{M}_0(p,r) = p + \gcd(p,r) - 1. \tag{2.2}$$

On the other hand it is not hard to see that $[j]_{r/q} \in \mathcal{M}(p/q,r/q)$ for $j \in \mathcal{M}(p,r)\backslash\mathcal{M}_0(p,r)$ and this shows that equality holds in (2.2). $\square$

Lemma 2.2. *Let $m,n \in \mathbb{N}$ and let $\mathcal{N}_i \subset \{1,\dots,n\}$ for $1 \leq i \leq m$. If $\sum_{i=1}^m \#\mathcal{N}_i \geq (m-1)\cdot n + k$, $k \in \{1,\dots,n\}$, then*

$$\#\left(\bigcap_{i=1}^m \mathcal{N}_i\right) \geq k.$$

Proof. We use induction on m. For $m=1$ there is nothing to prove. Hence let $m>1$ and without loss of generality let $\mathcal{N}_m = \{1,\dots,\#\mathcal{N}_m\}$ with $\#\mathcal{N}_m \geq k$. Since $\sum_{i=1}^{m-1}\#\mathcal{N}_i \geq (m-2)\cdot n + n + k - \#\mathcal{N}_m$ we have $\#(\cap_{i=1}^{m-1}\mathcal{N}_i) \geq n + k - \#\mathcal{N}_m$. Obviously, $\cap_{i=1}^{m-1}\mathcal{N}_i \subset \{1,\dots,n\}$ and thus

$$\#\left(\left(\bigcap_{i=1}^{m-1}\mathcal{N}_i\right) \cap \{1,\dots,\#\mathcal{N}_m\}\right) \geq k.$$

$\square$

We are now ready for the proof of Theorem 2.1.

Proof of Theorem 2.1. By (1.2) it suffices to consider a vector h of the form $h = \sum_{i=1}^d \lambda_i a^i \in \mathcal{H}_\Lambda(C)$ with $0 \leq \lambda_i < 1$, $1 \leq i \leq d$. Let $l = |\det(a^1,\dots,a^d)|/\det(\Lambda)$ be the index of C with respect to Λ. If $l=1$ then the vectors $a^1,\dots,a^d$ form a basis of Λ. This implies $\mathcal{H}_\Lambda(C) = \{a^1,\dots,a^d\}$. Otherwise we may assume that $l>1$. Then it is not too difficult to see that the coefficients λ_i have a representation as

$$\lambda_i = \frac{p_i}{r},\ p_i \in \{0,\dots,r-1\},\ 1 \leq i \leq d, \tag{2.3}$$

with $\gcd(p_1,\dots,p_d,r) = 1$ where $2 \leq r$ and r is a divisor of l. To verify this, let A be the matrix with columns $a^1,\dots,a^d$ and let L be a matrix whose columns form a basis of the lattice Λ. Then there exists a matrix $Z \in \mathbb{Z}^{d\times d}$

such that $A = LZ$ and $|\det(Z)| = l$. With $\lambda = (\lambda_1, \dots, \lambda_d)^T$ we obtain $A\lambda = h = Lz$ for a certain $z \in \mathbb{Z}^d$. This yields $\lambda = Z^{-1}z$. From this a representation of the desired form can be derived, see [GLS88] for details.

Next we transform the lattice and the cone into the "right" position. Let $\Lambda_h \subset \Lambda$ be the lattice generated by $a^1, \dots, a^d$ and h. Obviously, $h \in \mathcal{H}_{\Lambda_h}(C)$ and since $\det(\Lambda_h) \geq \det(\Lambda)$ it suffices to consider the cone C with respect to the lattice Λ_h. Let $A_* = (1/r) \cdot A$ be the matrix with columns $a^1, \dots, a^d$ scaled by $1/r$ and let $\Lambda_* = A_*^{-1}\Lambda$, $C_* = A_*^{-1}C = \text{pos}\{re^1, \dots, re^d\}$. Λ_* is the lattice generated by the elements $re^1, \dots, re^d$ and $p = (p_1, \dots, p_d)^T$. Clearly, $p \in \mathcal{H}_{\Lambda_*}(C_*)$ and we have to show $\sum_{i=1}^d p_i \leq (d-1)r - (d-2)(r/l)$ (cf. (2.3)). Since $r \leq l$ it is enough to prove $\sum_{i=1}^d p_i \leq (d-1)r - (d-2) = (d-1)(r-1)+1$. Assume the opposite, i.e.

$$\sum_{i=1}^{d} p_i \geq (d-1)(r-1) + 2. \tag{2.4}$$

In the following we show that under this assumption p can be written as the sum of two elements in $C_* \cap \Lambda_* \backslash \{0\}$ which contradicts property (1.1) of an element of a Hilbert basis. For $1 \leq j \leq r-1$ let $p^j = ([jp_1]_r, \dots, [jp_d]_r)^T \in C_* \cap \Lambda_*$. Since $\gcd(p_1, \dots, p_d, r) = 1$ we also have $p^j \neq 0$, $1 \leq j \leq r-1$. Now, let $\mathcal{M}(p_i, r) = \{j \in \{1, \dots, r-1\} : [j \cdot p_i]_r \leq p_i\}$, $1 \leq i \leq d$. By Lemma 2.1 we have $\#\mathcal{M}(p_i, r) \geq p_i$ and by (2.4)

$$\sum_{i=1}^{d} \#\mathcal{M}(p_i, r) \geq (d-1)(r-1) + 2.$$

Applying Lemma 2.2 to the sets $\mathcal{M}(p_i, r) \subset \{1, \dots, r-1\}$ yields

$$\#\left(\bigcap_{i=1}^{d} \mathcal{M}(p_i, r)\right) \geq 2.$$

For $j \in \cap_{i=1}^d \mathcal{M}(p_i, r)$ with $j \neq 1$ we consider the point $p^j + p^{r+1-j}$. The i-th component of this vector is given by $[j \cdot p_i]_r + [(r+1-j) \cdot p_i]_r$. Let $j \cdot p_i = l_{i,j} r + [j \cdot p_i]_r$ for some $l_{i,j} \in \{0, \dots, p_i - 1\}$. We get $(r+1-j)p_i = (p_i - l_{i,j})r + p_i - [j \cdot p_i]_r$. As $j \in \mathcal{M}(p_i, r)$ holds, we obtain $[(r+1-j)p_i]_r = p_i - [j \cdot p_i]_r$. This shows $p = p^j + p^{r+1-j}$. □

3. Complexity issues for Hilbert bases problems

This section treats algorithmic questions for problems about the Hilbert basis of a pointed cone $C_A \neq \{0\}$. We assume throughout that C_A is given in the form

$$C_A = \{x \in \mathbb{R}^d : Ax \leq 0\}, \tag{3.1}$$

with $A \in \mathbb{Z}^{m \times d}$ consisting of rows $(a^i)^T$, $1 \leq i \leq m$. For abbreviation we use the notation $\mathcal{H}(C_A)$ for the Hilbert basis of C_A with respect to the lattice

$\mathbb{Z}^d$. One constructive approach for Hilbert bases is based on a solution of the following problem.

The Hilbert Basis Problem (HBP). *Given a pointed cone $C_A \subset \mathbb{R}^d$ and vectors $h^1, \ldots, h^k \in \mathcal{H}(C_A)$, either*

i) *assert that $h^1, \ldots, h^k$ is the Hilbert basis of C_A, or*
ii) *find a point $h \in \mathcal{H}(C_A) \backslash \{h^1, \ldots, h^k\}$.*

For $k = 0$ HBP reduces to the problem of finding one member of the Hilbert basis. We remark

Proposition 3.1. *Let $C_A \subset \mathbb{R}^d$ be a pointed cone. There exists a polynomial time algorithm that determines one element $h \in \mathcal{H}(C_A)$.*

Proof. Let $c = \sum_{i=1}^m a^i$ and $P_A = C_A \cap \{x \in \mathbb{R}^d : c^T x \geq -1\}$. Since C_A is pointed, P_A is a polytope of which we can find a vertex $v \neq 0$ in polynomial time, see [GLS88]. Then there exists a system of d linearly independent rows $(a^{j_i})^T$, $1 \leq i \leq d$ such that

$$\mathrm{lin}(v) = \bigcap_{i=1}^{d-1} \left\{ x \in \mathbb{R}^d : (a^{j_i})^T x = 0 \right\}$$

and $(a^{j_d})^T v < 0$. Let u be the solution of

$$(a^{j_d})^T u = -1, \quad (a^{j_i})^T u = 0, \quad 1 \leq i \leq d-1. \tag{3.2}$$

We have $u \in \mathrm{pos}\{v\}$ and u may be written as

$$u = \frac{1}{q}(p_1, \ldots, p_d)^T, \quad q \in \mathbb{N},\ p_i \in \mathbb{Z} \text{ and } |p_i|, q \leq |\det(A^j)|, \tag{3.3}$$

where A^j denotes the matrix with rows $(a^{j_i})^T$, $1 \leq i \leq d$ (cf. [GLS88]). It is well known that the gcd of d numbers can be calculated in polynomial time and hence, $h = q \cdot u / \gcd(p_1, \ldots, p_d)$ can be constructed in polynomial time. We now claim that $h \in \mathcal{H}(C_A)$. First notice that $h \in C_A \cap \mathbb{Z}^d$. On account of (1.1) it suffices to show that h cannot be written as a nontrivial sum of two elements in $C_A \cap \mathbb{Z}^d$. Suppose $h = f + g$ with $f, g \in C_A \cap \mathbb{Z}^d \backslash \{0\}$. By (3.2) we get $f, g \in \mathrm{pos}\{v\} = \mathrm{pos}\{h\}$. Since by our construction $\mathrm{pos}\{h\} \cap \mathbb{Z}^d \backslash \{0\} = \{n \cdot h : n \in \mathbb{N}\}$, the statement follows. □

The proof of the proposition shows that one can find in polynomial time an element of the Hilbert basis belonging to the boundary of the cone C_A. However, the problem to decide whether $\mathcal{H}(C_A)$ contains a (relative) interior point of C_A is $\mathcal{NP}$-hard. This result will be derived next. We start with a proof that it is $\mathcal{NP}$-complete to decide whether a point $g \in C_A \cap \mathbb{Z}^d \backslash \{0\}$ can be written as the sum of two elements in $C_A \cap \mathbb{Z}^d \backslash \{0\}$.

Theorem 3.1. The Decomposition Problem (DP)*: For a pointed cone $C_A \subset \mathbb{R}^d$ and a vector $g \in C_A \cap \mathbb{Z}^d$ it is $\mathcal{NP}$-complete to decide whether $g \notin \mathcal{H}(C_A)$,* *Proof.* If $g \notin \mathcal{H}(C_A)$ then there exist two elements $v, w \in C_A \cap \mathbb{Z}^d \backslash \{0\}$ with $g = v + w$ (cf. (1.1)). Thus the problem is in $\mathcal{NP}$. In the following we give a polynomial time reduction of the subset sum problem to the decomposition problem: The subset sum problem is known to be $\mathcal{NP}$-complete (cf. [Kar72]) and is the task:

The Subset Sum Problem (`SSP`). *Let $a_1, \dots, a_d$, b be positive integers; decide whether there exists a subset $J \subset \{1, \dots, d\}$ with $\sum_{i \in J} a_i = b$.*

For an instance of `SSP` defined by the data $a = (a_1, \dots, a_d)^T \in \mathbb{N}^d$, $b \in \mathbb{N}$ let $P(a, b) = \{x \in \{0,1\}^d : a^T x = b\}$. Our task is to decide whether $P(a, b) \neq \emptyset$. First we may assume that $b \leq \sum_{i=1}^d a_i$ since otherwise we have $P = \emptyset$. Let $e = (1, \dots, 1)^T$ be the vector of all-ones. Then $x \in P(a, b) \Leftrightarrow (e - x) \in P(a, \sum_{i=1}^d a_i - b)$ and thus

$$P(a, b) \neq \emptyset \Longleftrightarrow P(a, \sum_{i=1}^{d} a_i - b) \neq \emptyset.$$

Hence we may even assume that $b \leq (\sum_{i=1}^d a_i)/2$.

Now we claim that the given instance of `SSP` can be transformed in polynomial time to an instance of `SSP` with input parameters $\tilde{a} = (\tilde{a}_1, \dots, \tilde{a}_n)^T$, $\tilde{b}$ such that

$$P(a, b) \neq \emptyset \Longleftrightarrow P(\tilde{a}, \tilde{b}) \neq \emptyset \text{ and } \sum_{i=1}^{n} \tilde{a}_i = 2\tilde{b}.$$

The correctness of the claim follows from the following arguments. If $b = (\sum_{i=1}^d a_i)/2$, then we may set $n = d$, $\tilde{a}_i = a_i$ for all $i = 1, \dots, d$ and $\tilde{b} = b$. If $b < (\sum_{i=1}^d a_i)/2$, we define $n = d + 1$, $\tilde{a} = (\tilde{a}_1, \dots, \tilde{a}_{d+1})^T = (a_1, \dots, a_d, \sum_{i=1}^d a_i - 2b)^T \in \mathbb{N}^{d+1}$ and $\tilde{b} = \sum_{i=1}^d a_i - b \in \mathbb{N}$.

From now on we assume that we are given an instance of a `SSP` with input parameters $\tilde{a} = (\tilde{a}_1, \dots, \tilde{a}_n)^T$, $\tilde{b}$ satisfying

$$\sum_{i=1}^{n} \tilde{a}_i = 2\tilde{b}. \tag{3.4}$$

For the parameters $\tilde{a} = (\tilde{a}_1, \dots, \tilde{a}_n)^T$, $\tilde{b}$ let C_A be the pointed cone given by

$$C_A = \left\{ x \in \mathbb{R}^{n+1} : \sum_{i=1}^{n} \tilde{a}_i x_i - \tilde{b} x_{n+1} = 0, \quad x \geq 0 \right\}. \tag{3.5}$$

We claim

$$P(\tilde{a}, \tilde{b}) \neq \emptyset \Longleftrightarrow (1, \dots, 1, 2)^T \notin \mathcal{H}(C_A). \tag{3.6}$$

By (3.4) we have $h = (1, \dots, 1, 2)^T \in C_A \cap \mathbb{Z}^{n+1}$. Suppose $h \notin \mathcal{H}(C_A)$. In this case we can find two elements $v, w \in C_A \cap \mathbb{Z}^{n+1} \backslash \{0\}$ with $h = v + w$. Obviously, $v_i, w_i \in \{0, 1\}$, $1 \leq i \leq n$ and since $\tilde{a}_1, \dots, \tilde{a}_n$ are positive we have $v_{n+1} = w_{n+1} = 1$. Thus $(v_1, \dots, v_n)^T, (w_1, \dots, w_n)^T \in P(\tilde{a}, \tilde{b})$.

For the other direction let $\tilde{v} \in P(\tilde{a}, \tilde{b})$. Then $v = (\tilde{v}_1, \ldots, \tilde{v}_n, 1) \in C_A$ and also $\tilde{w} = h - \tilde{v} \in C_A$. This shows $h \notin \mathcal{H}(C_A)$. □

An immediate consequence of this proof is

Corollary 3.1. *Let $C_A \subset \mathbb{R}^d$ be a pointed cone. The problem to find a point $h \in \mathcal{H}(C_A)$ contained in the relative interior of C_A or to assert that no such point exists, is $\mathcal{NP}$-hard.*

Proof. Again we consider an instance of the subset sum problem SSP. We use the notation in the proof of Theorem 3.1. In particular, $\tilde{a}, \tilde{b}$ defines the instance of SSP satisfying (3.4) and $C_A \subset \mathbb{R}^{n+1}$ is the cone defined via (3.5). We have $\dim(C_A) = n$ and $h = (1, \ldots, 1, 2)^T$ is contained in the relative interior of C_A. If no point of $\mathcal{H}(C_A)$ belongs to the relative interior of C_A, then $h \notin \mathcal{H}(C_A)$ and by (3.6) we know that SSP has a solution. On the other hand if $g \in \mathcal{H}(C_A)$ is contained in the relative interior of C_A then $g_i \geq 1$, $1 \leq i \leq n$, and $g_{n+1} \geq 2$. Suppose that $\tilde{v} \in P(\tilde{a}, \tilde{b})$. Then $v = (\tilde{v}_1, \ldots, \tilde{v}_n, 1) \in C_A$. As $\tilde{v}_i \in \{0, 1\}$ for all $i = 1, \ldots, n$ we obtain that $\tilde{w} = g - \tilde{v} \in C_A$, a contradiction that $g \in \mathcal{H}(C_A)$. Therefore SSP does not have a solution in this case. □

Next we investigate the problem HBP. It seems quite likely that this problem is $\mathcal{NP}$-hard, but we did not succeed in proving this. In the following we show that HBP can be solved in polynomial time provided that the dimension d is fixed.

For an instance $A \in \mathbb{Z}^{m \times d}$, $h^1, \ldots, h^k \in \mathcal{H}(C_A)$ of HBP let

$$F_A(h^1, \ldots, h^k) = \{f \in C_A \cap \mathbb{Z}^d \backslash \{0\} : f - h^j \notin C_A \text{ for all } j = 1, \ldots, k\}. \tag{3.7}$$

If $k = 0$ we set $F_A(\emptyset) = C_A \cap \mathbb{Z}^d \backslash \{0\}$. Obviously, $f - h^j \notin C_A$ implies that this point violates a restriction $(a^{j_i})^T x \leq 0$ of $Ax \leq 0$. Hence

$$\begin{aligned} f \in F_A(h^1, \ldots, h^k) \iff & f \in C_A \cap \mathbb{Z}^d \backslash \{0\} \text{ and } \forall j \in \{1, \ldots, k\} \\ & \exists\, j_i \in \{1, \ldots, m\} \text{ with } (a^{j_i})^T f \geq (a^{j_i})^T h^j + 1. \end{aligned} \tag{3.8}$$

Let $h \in \mathcal{H}(C_A) \backslash \{h^1, \ldots, h^k\}$. By (1.1) we have $h \in F_A(h^1, \ldots, h^k)$ and thus $F_A(h^1, \ldots, h^k) \neq \emptyset$. On the other hand if $\mathcal{H}(C_A) = \{h^1, \ldots, h^k\}$ then each $z \in C_A \cap \mathbb{Z}^d \backslash \{0\}$ can be written as $z = \sum_{i=1}^k z_i h^i$ with $z_i \in \mathbb{N} \cup \{0\}$ and $\sum_{i=1}^k z_i \geq 1$, implying that $F_A(h^1, \ldots, h^k) = \emptyset$. Therefore we have the relation

$$\{h^1, \ldots, h^k\} = \mathcal{H}(C_A) \iff F_A(h^1, \ldots, h^k) = \emptyset. \tag{3.9}$$

Proposition 3.2. *Let $C_A = \{x \in \mathbb{R}^d : Ax \leq 0\}$, $A \in \mathbb{Z}^{m \times d}$, be a pointed cone and let $c = \sum_{i=1}^m (a^i)^T$ be the sum of the rows of A. If the problem*

$$\max c^T z, \quad z \in F_A(h^1, \ldots, h^k).$$

is infeasible then $\mathcal{H}(C_A) = \{h^1, \dots, h^k\}$*. Otherwise, each optimal solution belongs to* $\mathcal{H}(C_A) \backslash \{h^1, \dots, h^k\}$*.*

Proof. If $\max c^T z, \quad z \in F_A(h^1, \dots, h^k)$ is infeasible, then (3.9) implies that $\{h^1, \dots, h^k\} = \mathcal{H}(C_A)$. Otherwise, we conclude that $c^T z \leq -1$ for all $z \in C_A \cap \mathbb{Z}^d \setminus \{0\}$, because C_A is a pointed cone. This shows that there exists an optimal solution $z^* \in F_A(h^1, \dots, h^k)$. It is also clear that $z^* \notin \{h^1, \dots, h^k\}$. What is not so clear is that $z^* \in \mathcal{H}(C_A)$. Assume the opposite, i.e., $z^* = v + w$ with $v, w \in C_A \cap \mathbb{Z}^d \backslash \{0\}$. Since z^* is optimal and C_A is pointed, neither v nor w are members of $F_A(h^1, \dots, h^k)$. Then there exists a vector h^i, $i \in \{1, \dots, k\}$ such that $v - h^i \in C_A \cap \mathbb{Z}^d$. Then, $z^* - h^i = (v - h^i) + w \in C_A$, a contradiction that $z^* \in F_A(h^1, \dots, h^k)$. □

Taking this proposition into account, we see that one can solve HBP if one is able to optimize c over $F_A(h^1, \dots, h^k)$. In order to get a more tractable description of $F_A(h_1, \dots, h^k)$ we resort to a lemma that bounds the size of all the vectors in $\mathcal{H}(C_A)$.

Lemma 3.1. *Let* C_A *be a pointed cone. For* $h = (h_1, \dots, h_d)^T \in \mathcal{H}(C_A)$ *one has*

$$|h_i| < 2^{\langle A \rangle}, \quad 1 \leq i \leq d,$$

where $\langle A \rangle$ *denotes the encoding length of the matrix* A *(cf.* [GLS88]*).*

Proof. Let $\{u^1, \dots, u^l\} \subseteq \mathbb{R}^d$ be a minimal set with $C_A = \text{pos}\{u^1, \dots, u^l\}$. For each u^j there exists a system of d linearly independent rows $(a^{j_i})^T$ of A such that u^j is the solution of the system (cf. (3.2) and [Zie95])

$$(a^{j_d})^T u^j = -1, \quad (a^{j_i})^T u^j = 0, \quad 1 \leq i \leq d-1.$$

By (3.3) we may assume $u^j \in \mathbb{Z}^d$ with $|u_i^j| < 2^{\langle A \rangle - d^2}$ (cf. [GLS88]). Let $h \in \mathcal{H}(C_A)$. By Carathéodory's theorem there exist d vectors $u^{j_1}, \dots, u^{j_d}$ such that $h \in C_h = \text{pos}\{u^{j_1}, \dots, u^{j_d}\}$. Obviously, h belongs to the Hilbert basis of the cone C_h, and applying Theorem 2.1 to h and C_h with respect to the space generated by $\text{lin} C_h$ gives

$$|h_i| \leq g_{C_h}(h) \max\{|u_i^{j_k}| : 1 \leq k \leq d\} < (d-1) 2^{\langle A \rangle - d^2}.$$

□

Now, let

$$\tilde{F}_A(h^1, \dots, h^k) = F_A(h^1, \dots, h^k) \cap \{z \in \mathbb{Z}^d : |z|_\infty \leq 2^{\langle A \rangle}\}. \tag{3.10}$$

On account of Proposition 3.2 and Lemma 3.1 we have

$$\begin{aligned} &\{z^* : c^T z^* = \max\, c^T z, \quad z \in F_A(h^1, \dots, h^k)\} \\ = &\{z^* : c^T z^* = \max\, c^T z, \quad z \in \tilde{F}_A(h^1, \dots, h^k)\} \end{aligned}$$

and we can replace in Proposition 3.2 $F_A(h^1, \dots, h^k)$ by $\tilde{F}_A(h^1, \dots, h^k)$, i.e.,

Remark 3.1. *Let* $C_A = \{x \in \mathbb{R}^d : Ax \leq 0\}$*,* $A \in \mathbb{Z}^{m\times d}$*, be a pointed cone and let* $c = \sum_{i=1}^m (a^i)^T$ *be the sum of the rows of* A*. If the problem*

$$\max c^T z, \quad z \in \tilde{F}_A(h^1, \dots, h^k)$$

is infeasible then $\mathcal{H}(C_A) = \{h^1, \dots, h^k\}$*. Otherwise, each optimal solution belongs to* $\mathcal{H}(C_A) \backslash \{h^1, \dots, h^k\}$*.*

The next step is to show that the set of all vectors in $\tilde{F}_A(h^1, \dots, h^k)$ is equal to the set of integral points that satisfy a system of inequalities in integer variables.

Proposition 3.3. *Let* $C_A = \{x \in \mathbb{R}^d : Ax \leq 0\}$ *with* $A \in \mathbb{Z}^{m\times d}$ *be a pointed cone and* $c = \sum_{i=1}^d (a^i)^T$ *be the sum of the row vectors of* A*. An integral vector* $z \in C_A \cap \mathbb{Z}^d$ *is in the set* $\tilde{F}_A(h^1, \dots, h^k)$ *if and only if there exists a* $0/1$*-matrix* $\lambda \in \{0,1\}^{m\times k}$ *such that* $\sum_{i=1}^m \lambda_{i,j} \geq 1$ *for every* $1 \leq j \leq k$ *satisfying the following conditions:*

$$(a^i)^T z \geq \lambda_{i,j}\left((a^i)^T h^j + 1\right) - (1 - \lambda_{i,j})2^{2\langle A\rangle} \text{ for all } 1 \leq i \leq m,\ 1 \leq j \leq k.$$

Proof. For $f \in \tilde{F}_A(h^1, \dots, h^k)$ and $j \in \{1, \dots, k\}$ let j_i be the index in $\{1, \dots, m\}$ with $(a^{j_i})^T f \geq (a^{j_i})^T h^j + 1$, see (3.8). With $\lambda_{i,j} = 0$ for all $i \in \{1, \dots, m\} \backslash \{j_i\}$ and $\lambda_{j_i,j} = 1$ we have $\lambda_{i,j} \in \{0,1\}$, $\sum_{i=1}^m \lambda_{i,j} \geq 1$. Moreover, for $1 \leq i \leq m$ we obtain

$$(a^i)^T f \geq \lambda_{i,j}\left((a^i)^T h^j + 1\right) - (1 - \lambda_{i,j})2^{2\langle A\rangle},$$

where we use the estimate $|(a^i)^T f| \leq |a^i| \cdot |f| < 2^{\langle a^i\rangle - d}(d2^{\langle A\rangle}) < 2^{2\langle A\rangle}$ (cf. [GLS88]).

Conversely, let $z \in C_A \cap \mathbb{Z}^d$ and $\lambda \in \{0,1\}^{m*k}$ satisfy $\sum_{i=1}^m \lambda_{i,j} \geq 1$ for all $1 \leq j \leq k$ and the system of inequalities outlined above. For every $1 \leq j \leq k$ there exists a parameter $\lambda_{j_i,j} = 1$. Then

$$(a^{j_i})^T z \geq \lambda_{j_i,j}\left((a^{j_i})^T h^j + 1\right) - (1 - \lambda_{j_i,j})2^{2\langle A\rangle} = (a^{j_i})^T h^j + 1.$$

So $z - h^j \notin C_A$, $z \neq 0$ and we have $z \in \tilde{F}_A(h^1, \dots, h^k)$. □

The optimization problem $\max c^T z, z \in \tilde{F}_A(h^1, \dots, h^k)$ gives rise to a linear integer program in dimension $d + mk$. Therefore, we cannot simply apply Lenstra's algorithm [Len83] to this integer program in order to terminate with a solution of HBP in polynomial time for fixed d. In order to end up with a polynomial time algorithm we split the set $\tilde{F}_A(h^1, \dots, h^k)$ into a polynomial number of subsets each of which is easy to describe. Then we apply Lenstra's algorithm to each subset separately. A similar trick was used in [CLS84], see also [Sch86].

Theorem 3.2. *For fixed dimension* d *there exists a polynomial time algorithm that solves* HBP*.*

Proof. Let $A \in \mathbb{Z}^{m\times d}$ and $h^1, \dots, h^k \in \mathcal{H}(C_A)$ be an input of HBP. Again, we denote by $(a^i)^T$ the rows of A, $1 \leq i \leq m$. By Theorem 3.1 we may assume $k \geq 1$.

Let $\mathcal{Z}$ be the collection of vectors $u \in C_A \cap \{x \in \mathbb{R}^d : |x|_\infty \leq 2^{\langle A \rangle}\}$ determined by d linearly independent equations from the following list:

$$\begin{aligned} (e^i)^T u &= 2^{\langle A \rangle}, \quad i = 1, \dots, d, \\ (e^i)^T u &= -2^{\langle A \rangle}, \quad i = 1, \dots, d, \\ (a^i)^T u &= 0, \quad i = 1, \dots, m \\ (a^i)^T u &= (a^i)^T h^j + 1/2, \quad i = 1, \dots, m, \ j = 1, \dots, k. \end{aligned} \tag{3.11}$$

Since d is fixed we can find and store $\mathcal{Z}$ in polynomial time. Let r be the maximal cardinality of a set of linearly independent vectors from $\mathcal{Z}$. Obviously, $r = \dim(C_A)$. Now, we determine all affinely independent subsets $u^1, \dots, u^{r+1}$, $u^i \in \mathcal{Z}$, such that for all $j \in \{1, \dots, k\}$ there exists an index $j_i \in \{1, \dots, m\}$ with

$$(a^{j_i})^T u^l \geq (a^{j_i})^T h^j + 1/2, \quad 1 \leq l \leq r+1. \tag{3.12}$$

Let $\mathcal{S}$ be the collection of all these subsets. We claim

$$\tilde{F}_A(h^1, \dots, h^k) = \bigcup_{\{u^1, \dots, u^{r+1}\} \in \mathcal{S}} \left(\operatorname{conv}\{u^1, \dots, u^{r+1}\} \cap \mathbb{Z}^d \backslash \{0\} \right). \tag{3.13}$$

Let $f \in \tilde{F}_A(h^1, \dots, h^k)$. Since $f - h^j \notin C_A$ for each $j \in \{1, \dots, k\}$ there exists a $j_i \in \{1, \dots, m\}$ such that $(a^{j_i})^T f \geq (a^{j_i})^T h^j + 1$ (cf. (3.8)). Hence f is contained in the polytope

$$P_f = \{x \in \mathbb{R}^d : Ax \leq 0, \, (a^{j_i})^T x \geq (a^{j_i})^T h^j + 1/2, \, 1 \leq j \leq k, \, |x|_\infty \leq 2^{\langle A \rangle}\}.$$

Since $\dim(C_A) = r$ and $(a^{j_i})^T f \geq (a^{j_i})^T h^j + 1$ we have $\dim(P_f) = r$. By Carathéodory's Theorem f can be written as a convex combination of $(r+1)$ affinely independent vertices of P_f. Since each vertex of P_f is contained in $\mathcal{Z}$, there exists a set $\{u^1 \dots, u^{r+1}\} \in \mathcal{S}$ with $f \in \operatorname{conv}\{u^1, \dots, u^{r+1}\} \cap \mathbb{Z}^d \backslash \{0\}$.

On the other hand let $\{u^1, \dots, u^{r+1}\} \in \mathcal{S}$ and $z \in \operatorname{conv}\{u^1, \dots, u^{r+1}\} \cap \mathbb{Z}^d \backslash \{0\}$. Then we may write $z = \sum_{i=1}^{r+1} \lambda_i u^i$ with $\sum_{i=1}^{r+1} \lambda_i = 1$, $\lambda_i \geq 0$, $1 \leq i \leq r+1$. From (3.12) we get for $j \in \{1, \dots, k\}$

$$(a^{j_i})^T z = \sum_{l=1}^{r+1} \lambda_i (a^{j_i})^T u^l \geq (a^{j_i})^T h^j + \frac{1}{2}.$$

Hence $(a^{j_i})^T z \geq (a^{j_i})^T h^j + 1$. Since $z \in C_A \cap \mathbb{Z}^d \backslash \{0\}$, $|z|_\infty \leq 2^{\langle A \rangle}$ we have $z \in \tilde{F}_A(h^1, \dots, h^k)$.

Now, let $c = \sum_{i=1}^m a^i$. For each $S = \{u^1, \dots, u^{r+1}\} \in \mathcal{S}$ we consider the integer linear program

$$(IP_S) \qquad \max c^T z, \, c^T z \leq -1, z \in \operatorname{conv} S \cap \mathbb{Z}^d.$$

An integer program of this form can be solved by Lenstra's algorithm [Len83]. If for every $S \in \mathcal{S}$ the program (IP_S) is infeasible, then $\mathcal{H}(C_A) = \{h^1, \dots, h^k\}$ by (3.13) and Remark 3.1. Otherwise, let z^S denote an optimal solution of a feasible problem (IP_S). Let z^* be one of these optimal solutions that maximizes the objective function c. It follows that z^* is a solution of $\max c^T z, z \in \tilde{F}_A(h^1, \dots, h^k)$. Therefore $z^* \in \mathcal{H}(C_A) \setminus \{h^1, \dots, h^k\}$. $\square$

From this Theorem we may deduce

Corollary 3.2. *Let $C_A = \{x \in \mathbb{R}^d : Ax \leq 0\}$ be a pointed cone and $k = \#\mathcal{H}(C_A)$. For fixed d and k there exists a polynomial algorithm which determines the Hilbert basis of C_A.*

4. An algorithm to compute Hilbert Bases

Throughout this section we assume that A is a fixed m times d matrix of integer coefficients with rows $(a^1)^T, \dots, (a^m)^T$ and $C = \{x \in \mathbb{R}^d_+ : Ax \leq 0\}$ is the polyhedral cone associated with A. For a vector v, v^+ is the vector with components $v_i^+ = \max\{0, v_i\}$ and $v^- = (-v)^+$. In the following we present a procedure that computes an integral Hilbert basis of C that we denote by $\mathcal{H}$. For related algorithms see [Stu96], [Pot96], [Tho94], [UWZ94].

There are two ingredients that will be presented first and turn out to be crucial for the proof of correctness of the algorithm: one is the notion of reducibility and the other one is the definition of m total orders on $\mathbb{Z}^d$.

Definition 4.1. *We say that $v \in \mathbb{Z}^d$* **reduces** *$w \in \mathbb{Z}^d$ if the following four properties hold:*

$$v^+ \leq w^+, \quad v^- \leq w^-, \quad (Av)^+ \leq (Aw)^+, \quad (Av)^- \leq (Aw)^-.$$

v is called **reducible** *in this case. If there does not exist $w \in \mathbb{Z}^d$ reducing v, we say that v is* **irreducible**.

In words, if v reduces w, then for $i \in \{+, -\}$ both w^i and $(Aw)^i$ can be written as the sum of two integral vectors that lie in the same orthant as w^i and $(Aw)^i$, respectively. In particular, if w is an integral point in C and an integral point $v \in C$ reduces w, then $w - v$ belongs to C.

Next we define m total orders on $\mathbb{Z}^d$ that we denote by the symbol $\succ_1$, $\succ_2$, ..., $\succ_m$. The symbol $\succ_{lex}$ is used for the lexicographic order between the lattice points in $\mathbb{Z}^d$. For $x, y \in \mathbb{Z}^d$ we define

$$x \prec_i y \qquad \Longleftrightarrow \qquad \begin{cases} (a^i)^T x < (a^i)^T y, & \text{or} \\ (a^i)^T x = (a^i)^T y & \text{and } x \prec_{lex} y. \end{cases}$$

We are now ready to outline an algorithm that computes an integral Hilbert basis $\mathcal{H}$ of C and verify its correctness.

Algorithm 4.1. to compute a minimal integral Hilbert basis $\mathcal{H}$ of the cone C.

(1) *Set $\mathcal{G} := \{e^1, \dots, e^d\}$ and $\mathcal{G}_{old} := \emptyset$.*
(2) *While $\mathcal{G}$ and $\mathcal{G}_{old}$ differ perform the following steps:*
  (2.1) *Set $\mathcal{G}_{old} := \mathcal{G}$.*
  (2.2) *For every $v, u \in \mathcal{G}$ with $|u + v|_\infty \leq 2^{\langle A \rangle}$ set $w := u + v$.*

a) *As long as possible find* $z \in \mathcal{G}$ *reducing* w *and update* $w := w - z$.

b) *If* $w \neq 0$, *set* $\mathcal{G} := \mathcal{G} \cup \{w\}$.

(3) *Set* $\mathcal{H} := \mathcal{G}$.

(4) *As long as there exists* $w \in \mathcal{H}$ *such that* $Aw \not\leq 0$ *set* $\mathcal{H} := \mathcal{H} \setminus \{w\}$.

(5) *As long as there exists* $w \in \mathcal{H}$ *that is reducible by some* $v \in \mathcal{H}$ *set* $\mathcal{H} := \mathcal{H} \setminus \{w\}$.

The algorithm terminates in finite time and outputs an integral Hilbert basis of the cone. This will be shown in two steps. We start with a lemma saying that every integral vector $x \in C \setminus \mathcal{G}$ can be reduced by integral vectors.

Lemma 4.1. *Let* $x \in C \cap \mathbb{N}^d$ *such that* $x \notin \mathcal{G}$. *For every* $i \in \{0, \dots, m\}$ *there exist* $z^1, \dots, z^k \in \mathcal{G}$ *satisfying*

$$\text{(I)} \quad x = \sum_{v=1}^{k} z^v \qquad \textit{and} \qquad \text{(II)} \quad z^v \prec_t 0 \textit{ for } 1 \leq t \leq i,\ 1 \leq v \leq k.$$

Proof. Let $x \in C \cap \mathbb{N}^d$ and assume that $x \notin \mathcal{G}$. On account of Lemma 3.1 we know that the Hilbert basis of C is contained in the cube with edge length $2 * 2^{\langle A \rangle}$. Therefore, we can assume that $|x|_\infty \leq 2^{\langle A \rangle}$. We use induction on i in order to verify the lemma. If $i = 0$ we only need to verify the property that there exist non-negative integral vectors $z^1, \dots, z^k \in \mathcal{G}$ that satisfy (I) of Lemma 4.1. For example μ_1 copies of e^1, μ_2 copies of e^2, ..., μ_d copies of e^d satisfy this requirement since $e^1, \dots, e^d \in \mathcal{G}$ are irreducible. We now assume that the lemma is correct for a given value of i and show the correctness for the index $i+1$.

Let $x = \sum_{j=1}^{d} \mu_j e^j$ be given with $\mu_j \in \mathbb{N}$ for all $j = 1, \dots, d$. By assumption of the induction there exist non-negative integral vectors $z^1, \dots, z^k \in \mathcal{G}$ that satisfy property (I) of Lemma 4.1 and condition (II) for all values of $t \in \{0, \dots, i\}$, i.e., $z^v \prec_t 0$ for every $t \in \{0, \dots, i\}$ and $v \in \{1, \dots, k\}$. With every family $z^1, \dots, z^k \in \mathcal{G}$ of non-negative integral vectors that satisfy property (I) and condition (II) for all values of $t \in \{0, \dots, i\}$ we associate a special point z^* that is defined as the sum of vectors in the sequence that are negative with respect to the order $\succ_{i+1}$. In formulas, let $v_0 \in \{1, \dots, k\}$ be the index such that

$$z^v \prec_{i+1} 0 \text{ for all } v = 1, \dots, v_0 - 1 \qquad \text{and} \qquad z^v \succ_{i+1} 0 \text{ for all } v = v_0, \dots, k,$$

then $z^* = \sum_{v=1}^{v_0-1} z^v$. (Note that $x \in C \cap \mathbb{N}^d$ and so $v_0 \geq 2$).

Choose vectors $z^1, \dots, z^k \in \mathcal{G}$ that satisfy property (I) and (II) for all values of $t \in \{0, \dots, i\}$ such that the special point $z^* := \sum_{v=1}^{v_0-1} z^v$ is maximal with respect to the order $\succ_{i+1}$. If $v_0 = k+1$, then $z^1, \dots, z^k$ satisfy property (II) of Lemma 4.1 for all values of $t \in \{0, \dots, i+1\}$ and we are done. Otherwise, $v_0 \leq k$ holds implying that $z := z^{v_0-1} + z^{v_0} \in \mathbb{N}^d$. Since $|z|_\infty \leq |x|_\infty \leq 2^{\langle A \rangle}$ the point z was computed in Step (2.2) of Algorithm 4.1. Hence, there exists a representation of z in the form

$$z = g^1 + \ldots + g^a,$$

where $g^1, \ldots, g^a \in \mathcal{G}$ reduce z. Let $b \leq a$ be the index with

$$g^1 \prec_{i+1} 0, \ldots, g^b \prec_{i+1} 0 \text{ and } g^{b+1} \succ_{i+1} 0, \ldots, g^a \succ_{i+1} 0.$$

Then $z^1, \ldots, z^{v_0-2}, g^1, \ldots, g^b, g^{b+1}, \ldots g^a, z^{v_0+1} \ldots, z^k$ is also a sequence of non-negative integral points that satisfy condition (I) and condition (II) for all values of $t \in \{0, \ldots, i\}$. Yet, the special point z^* of this new sequence is

$$\sum_{v=1}^{v_0-2} z^v + g^1 + \ldots g^b.$$

As $z^{v_0-1} \prec_{i+1} z^{v_0-1} + z^{v_0} = z = g^1 + \ldots g^b + g^{b+1} + \ldots + g^a$ and as each g^j reduces z we obtain $z^{v_0-1} \prec_{i+1} g^j$ for $j = 1, \ldots, b$. It then follows that the special point in this new sequence is greater than the special point of the original sequence $z^1, \ldots, z^k$ with respect to $\succ_{i+1}$. We obtain a contradiction that the sequence $z^1, \ldots, z^k$ was chosen such that the specified point z^* is maximal with respect to $\succ_{i+1}$. □

Theorem 4.1. *Algorithm 4.1 terminates after a finite number of steps and the output $\mathcal{H}$ is a Hilbert basis of C.*

Proof. Finiteness of the algorithm follows from the fact that the number of integral points in the set $\mathcal{G}$ that we compute in Steps (1) and (2) is always finite. Each performance of Step (2) adds at least one element to the current set $\mathcal{G}$.

Furthermore, Lemma 4.1 with $i = m$ shows that each $x \in C \cap \mathbb{N}^d$ can be written as the sum of elements in $\mathcal{G}$. Thus

$$C \cap \mathbb{N}^d = \{\sum_{i=1}^{k} n_i g^i \,:\, n_i \in \mathbb{N},\, g^i \in \mathcal{G} \cap C, 1 \leq i \leq k,\, k \in \mathbb{N}\}.$$

Hence it should be clear that steps (4) and (5) reduce $\mathcal{G}$ to the Hilbert basis $\mathcal{H}$.

□

Example 4.1. *Let $w_1, \ldots w_d$, $w_{d+1}, \ldots, w_l$ be non-negative integers such that each w_{d+j}, $j = 1, \ldots, l$ is an integer multiple of each w_i, $i = 1, \ldots, d$, and set*

$$C := \{x \in \mathbb{R}_+^{d+l} \,:\, \sum_{i=1}^{d} w_i x_i - \sum_{j=1}^{l} w_{d+j} x_{d+j} \leq 0\}.$$

Algorithm 4.1 starts with $\mathcal{G} = \bigcup_{i=1}^{d}\{e^i\} \cup \bigcup_{j=1}^{l}\{e^{d+j}\}$. Note that $\bigcup_{j=1}^{l}\{e^{d+j}\} \subseteq C$. Next we perform steps (2.1) and (2.2'). After performing Step 2, $\mathcal{G}$ is of the form $\mathcal{G} = \{e^1, \ldots, e^d\} \cup \{e^i + e^{d+j} \,:\, i = 1, \ldots, d,\ j = 1, \ldots, l\} \cup \{e^{d+1}, \ldots, e^{d+l}\}$ because for every $i, j \in \{1, \ldots, d\}$ or $i, j \in \{d+1, \ldots, d+l\}$ the vector $e^i + e^j$ is reducible by e^i. As $w_i - w_{d+j} < 0$, the set $\{e^i + e^{d+j}\,:$

$i = 1, \dots, d,\ j = 1, \dots, l\}$ is contained in C. Moreover, every vector of the form $e^i + e^{d+j_1} + e^{d+j_2}$ with $i \in \{1, \dots, d\}$ and $j_1, j_2 \in \{1, \dots, l\}$ is reducible by $e^i + e^{d+j_1}$. Therefore, performing Steps (2.1) and (2.2') a second time yields an updated set $\mathcal{G}$ of the form $\mathcal{G} = \{e^{d+j} : j = 1, \dots, l,\ \ e^i + e^{d+j} : i = 1, \dots, d,\ j = 1, \dots, l,\ \ e^{i_1} + e^{i_2} + e^{d+j} : i_1, i_2 = 1, \dots, d,\ j = 1, \dots, l\} \cup \{e^1, \dots, e^d\}$.

Iterating these arguments shows that an irreducible vector is always of the form $\sum_{i \in S} e^i + e^{d+j}$ with $S \subseteq \{1, \dots, d\}$ and $j \in \{1, \dots, l\}$. The fact that each w_{d+j}, $j = 1, \dots, l$ is an integer multiple of each w_i, $i = 1, \dots, d$ implies that a vector $\sum_{i \in S} e^i + e^{d+j}$ such that $S \subseteq \{1, \dots, d\}$, $j \in \{1, \dots, l\}$ and $\sum_{i \in S} w_i - w_{d+j} > 0$ can be reduced by a vector $\sum_{i \in \bar{S}} e^i + e^{d+j}$ where $\bar{S} \subset S$ and $\sum_{i \in \bar{S}} w_i - w_{d+j} = 0$.

It follows that we terminate with Step 2 of Algorithm 4.1 when $\mathcal{G}$ is equal to the union of $\{e^1, \dots, e^d\}$ and the set

$$\{\sum_{i \in S} e^i + e^{d+j} : S \subseteq \{1, \dots, d\}, \sum_{i \in S} w_i \leq w_{d+j},\ j = 1, \dots, l\}.$$

After performing Steps (3), (4) and (5) we end with

$$\mathcal{H} = \{\sum_{i \in S} e^i + e^{d+j} : S \subseteq \{1, \dots, d\},\ j = 1, \dots, l,\ \sum_{i \in S} w_i \leq w_{d+j}\}.$$

This is by our Theorem the Hilbert basis of the cone C. The number of times Step 2 is performed is equal to the ratio $\frac{\max\{w_{d+j} : j=1,\dots,l\}}{\min\{w_i : i=1,\dots,d\}}$.

Throughout this section we were dealing with cones that are contained in one orthant of $\mathbb{R}^d$. For polyhedral cones of the form $C = \{x \in \mathbb{R}^d : Ax \leq 0\}$ a slight modification of Algorithm 4.1 will still compute an integral Hilbert basis of the associated cone. We replace the initial Step (1) by

(1') Set $\mathcal{G} := \{e^1, -e^1, \dots, e^d, -e^d\}$ and $\mathcal{G}_{old} := \emptyset$.

Then by applying the same techniques as we did in the proof of Lemma 4.1 we obtain

Lemma 4.2. *Let $x \in \{x \in \mathbb{R}^d : Ax \leq 0\} \cap \mathbb{Z}^d$ such that $x \notin \mathcal{G}$ where G is the set that we computed via the modified Algorithm 4.1 with Steps (1'), (2) - (5). For every $i \in \{1, \dots, m\}$ there exist $z^1, \dots, z^k \in \mathcal{G}$ satisfying*

$$\text{(I)} \quad x = \sum_{v=1}^{k} z^v \quad \textit{and} \quad \text{(II)} \quad z^v \prec_t 0 \textit{ for } 1 \leq t \leq i,\ 1 \leq v \leq k.$$

As a consequence of Lemma 4.2 we obtain that the modified Algorithm computes an integral Hilbert basis of the cone $\{x \in \mathbb{R}^d : Ax \leq 0\}$.

References

[CLS84] W. Cook, L. Lovász, and A. Schrijver, *A polynomial-time test for total dual integrality in fixed dimension*, Mathematical Programming Study **22** (1984), 64–69.

[Dai95] D. Dais, *Enumerative combinatorics of invariants of certain complex threefolds with trivial canonical bundle*, Bonner Math. Schriften **279** (1995).

[DHZ96] D. Dais, M. Henk, and G.M. Ziegler, *On the existence of crepant resolutions of Gorenstein abelian quotient singularities in dimensions* ≥ 4, in preperation (1996).

[EW91] G. Ewald and U. Wessels, *On the ampleness of invertible sheaves in complete projective toric varieties*, Results in Mathematics **19** (1991), 275–278.

[GL87] P.M. Gruber and C.G. Lekkerkerker, *Geometry of numbers*, 2nd ed., North-Holland, Amsterdam, 1987.

[GLS88] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer, New-York, 1988.

[Gra75] J.E. Graver, *On the foundations of linear and integer linear programming I*, Math. Program. **8** (1975), 207–226.

[Hil90] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.

[Kar72] R.M. Karp, *Reducibilty among combinatorial problems*, Complexity of Computer Computations (New York) (R.E. Miller and J.W. Thatcher, eds.), Plenum Press, New York, 1972, pp. 85–103.

[Len83] H.W. Lenstra, Jr., *Integer programming with a fixed number of variables*, Mathematics of Operation Research **8** (1983), 538–548.

[Liu91] J. Liu, *Hilbert Bases with the Carathéodory Property*, Ph. D.Thesis, Cornell University, Ithaca NY, 1991.

[LTZ93] J. Liu, L.E. Trotter, Jr., and G.M. Ziegler, *On the Height of the Minimal Hilbert Basis*, Results in Mathematics **23** (1993), 374–376.

[Min96] H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1896.

[Pot96] L. Pottier, *Euclide algorithm in dimension n*, Preprint, Université de Nice-Sophia Antipolis, Valbonne (1996).

[Sch86] A. Schrijver, *Theory of Linear and Integer Programming*, John Wiley and Sons, Chichester, 1986.

[Stu96] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, AMS, Providence, R. I., 1996.

[Tho94] R. Thomas, *A geometric Buchberger algorithm for integer programming*, Mathematics of Operations Research (1994), to appear.

[UWZ94] R. Urbaniak, R. Weismantel, and G.M. Ziegler, *A variant of Buchberger's algorithm for integer programming*, Preprint (Konrad-Zuse-Zentrum Berlin) SC 94-29 (1994).

[Wei94] R. Weismantel, *Hilbert bases and the facets of special knapsack polytopes*, submitted (1994).

[Zie95] G.M. Ziegler, *Lectures on Polytopes*, Springer, New York, 1995.

Technische Universität Berlin, Sekr. MA 6-1, Strasse des 17. Juni 136, D-10623 Berlin, Germany

E-mail address: henk@math.tu-berlin.de

Konrad-Zuse-Zentrum für Informationstechnik (ZIB), Heilbronner Strasse 10, D-10711 Berlin, Germany

E-mail address: weismantel@zib.berlin.de