The height of minimal Hilbert bases

Martin Henk and Robert Weismantel

Abstract

For an integral polyhedral cone $C = \text{pos}\{a^1, \ldots, a^m\}$, $a^i \in \mathbb{Z}^d$, a subset $\mathcal{B}(C) \subset C \cap \mathbb{Z}^d$ is called a minimal Hilbert basis of C iff (i) each element of $C \cap \mathbb{Z}^d$ can be written as a non-negative integral combination of elements of $\mathcal{B}(C)$ and (ii) $\mathcal{B}(C)$ has minimal cardinality with respect to all subsets of $C \cap \mathbb{Z}^d$ for which (i) holds. We give a tight bound for the so-called height of an element of the basis which improves on former results.

1 Introduction

Throughout the paper $\mathbb{R}^d$ denotes the d-dimensional Euclidean space, and $\text{pos}\, S$ the positive hull of a subset $S \subset \mathbb{R}^d$. The cardinality of a (finite) subset $S \subset \mathbb{R}^d$ is denoted by $\#S$ and the i-th unit vector is represented by e^i. 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 $a^i \in \mathbb{R}^d$, $1 \leq i \leq m$, then C is called a polyhedral cone or a finitely generated cone.

Here we are studying integral polyhedral cones $C \subset \mathbb{R}^d$, i.e, there exist vectors $a^i \in \mathbb{Z}^d \backslash \{0\}$ for $1 \leq i \leq m$ such that $C = \text{pos}\{a^1, \ldots, a^m\}$, or equivalently, $C = \{x \in \mathbb{R}^d : Ax \leq 0\}$ for an appropriate matrix $A \in \mathbb{Z}^{n \times d}$.

From Gordan's lemma (cf. [1], [2]) we know that for every integral polyhedral cone C there exists a set $\mathcal{B}(C) \subset C \cap \mathbb{Z}^d$ such that

1. each $z \in C \cap \mathbb{Z}^d$ can be expressed as a non-negative integral combination of elements in $\mathcal{B}(C)$, i.e., $z = \sum_{b \in \mathcal{B}(C)} z_b\, b$, $z_b \in \mathbb{N}$.

2. $\mathcal{B}(C)$ has minimal cardinality with respect to all subsets of $C \cap \mathbb{Z}^d$ for which (1) holds.

$\mathcal{B}(C)$ is called a minimal Hilbert basis of C. For short we just say basis of C. If C is a pointed cone then $\mathcal{B}(C)$ is uniquely determined (cf. [3], [2]),

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

1991 Mathematics Subject Classification. Primary 52B20, 90C21; Secondary 11P21.

Key words and Phrases. Hilbert bases, rational polyhedral cones, integer programming.

This implies that the basis $\mathcal{B}(C)$ is contained in the zonotope generated by $a^1, \ldots, a^m$. More precisely, we have

$$\begin{aligned}\mathcal{B}(C) \subset \{a^1, \ldots, a^m\} \cup \\ \left\{ a \in C \cap \mathbb{Z}^d \backslash \{0\} : a = \sum_{i=1}^{m} \lambda_i a^i, 0 \leq \lambda_i < 1, \, 1 \leq i \leq m \right\}.\end{aligned} \tag{1.2}$$

We want to remark that (minimal) Hilbert bases occur under many different names in various fields of mathematics such as integer programming (cf. [2], [4], [5], [6]) or in the context of special desingularizations of toric varieties (cf. [7], [8], [9],[10]). However, very little is known about the geometrical structure of the basis elements. Here we focus on the height of the Hilbert basis.

Definition 1. *Let $C = \mathrm{pos}\{a^1, \ldots, a^m\}$, $a^i \in \mathbb{Z}^d$, be a pointed cone. For $b \in \mathcal{B}(C)$ the number*

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

is called the height of the basis element b.

It is straightforward to see that for dimension 2 the height is not greater than 1 and from Caratheodory's theorem and (1.2) one easily derives the bound $h_C(b) < d$, $b \in \mathcal{B}(C)$, $C \subset \mathbb{R}^d$. Indeed, it was proven by Ewald & Wessels [11] that

$$h_C(b) < d - 1, \quad b \in \mathcal{B}(C), \qquad d \geq 3,$$

is an asymptotically tight upper bound for the height (see also [12]). Here we sharpen the bound in the following way.

Theorem 1. *Let $C = \mathrm{pos}\{a^1, \ldots, a^m\}$, $a^i \in \mathbb{Z}^d$, be a d-dimensional pointed cone. For $b \in \mathcal{B}(C)$ one has*

$$h_C(b) \leq (d-1) - \frac{d-2}{|\det(a^{i_1}, \ldots, a^{i_d})|},$$

where $\{a^{i_1}, \ldots, a^{i_d}\} \subset \{a^1, \ldots, a^m\}$ is a subset of d linearly independent integral points such that $b \in \mathrm{pos}\{a^{i_1}, \ldots, a^{i_d}\}$.

This bound is tight for various families of cones. For example, let $r \in \mathbb{N}\backslash\{0\}$ and let (cf. [11])

$$C_r^d = \mathrm{pos} \left\{ e^1, \ldots, e^{d-1}, re^d + \sum_{i=1}^{d-1} e^i \right\}.$$

The point $b = (1, \ldots, 1)^T$ is an element of the basis with

$$h_C(b) = (d-1) \cdot \frac{r-1}{r} + \frac{1}{r} = d - 1 - \frac{d-2}{|\det(e^1, \ldots, e^{d-1}, re^d + \sum_{i=1}^{d-1} e^i)|}.$$

2 Proof of Theorem 1

The proof is prepared by the next two simple lemmas.

Lemma 1. *Let $p, r \in \mathbb{N}$ such that $1 \le p \le r-1$. We define $\mathcal{M}(p,r) = \{j \in \{0,\dots,r-1\} : (j\cdot p) \bmod r \le p\}$. Then $\#\mathcal{M}(p,r) = p + \gcd(p,r)$.*

Proof. Obviously, if $\gcd(p,r) = 1$ then $\{(j\cdot p) \bmod r : 0 \le j \le r-1\} = \{0,\dots,r-1\}$ and the statement is true. Hence $\#\mathcal{M}(p/q, r/q) = p/q + 1$ where $q = \gcd(p,r)$. Since

$$\left(j + i\cdot\frac{r}{q}\right)\cdot p \bmod r = q\cdot\left(j\cdot\frac{p}{q} \bmod \frac{r}{q}\right),\ 0\le j\le \frac{r}{q}-1,\ 0\le i\le q-1,$$

we get $\#\mathcal{M}(p,r) = q\cdot\#\mathcal{M}(p/q,r/q) = p+\gcd(p,r)$. □

The next lemma is quite obvious and can easily be proved by induction on the number n.

Lemma 2. *Let m, n be positive integers and let $\mathcal{N}_i \subset \{1,\dots,n\}$ for $1 \le i \le m$. If $\sum_{i=1}^m \#\mathcal{N}_i \ge (m-1)\cdot n + k$, $k \in \{1,\dots,n\}$, then $\#\left(\bigcap_{i=1}^m \mathcal{N}_i\right) \ge k$.*

□

We are now ready for the proof of Theorem 1.

Proof of Theorem 1. Let $b \in \mathcal{B}(C)$ and w.l.o.g. let $\{a^1,\dots,a^d\}$ be a subset of the generators $a^1,\dots,a^m$ of the cone C such that $a^1,\dots,a^d$ are linearly independent and $b \in \mathrm{pos}\{a^1,\dots,a^d\}$. Let $\Lambda \subset \mathbb{Z}^d$ be the lattice generated by $\{a^1,\dots,a^d,b\}$, $\det(\Lambda)$ its determinant and

$$r = |\det(a^1,\dots,a^d)|/\det(\Lambda) \in \mathbb{N}$$

be the index of the sublattice generated by $a^1,\dots,a^d$ w.r.t. Λ (cf. [13]). In the following we show

$$h_C(b) \le (d-1) - (d-2)\frac{\det(\Lambda)}{|\det(a^1,\dots,a^d)|} = (d-1) - \frac{d-2}{r}, \tag{2.1}$$

which is a slightly stronger inequality as posed in Theorem 1. To this end let $b \notin \{a^1,\dots,a^d\}$. Furthermore, since b is also contained in the minimal Hilbert basis of the cone $\mathrm{pos}\{a^1,\dots,a^d\}$ we may assume by (1.2) that $b = \sum_{i=1}^d \lambda_i a^i$ with $0 \le \lambda_i < 1$. It is quite easy to see that the coefficients λ_i have a representation as

$$\lambda_i = \frac{p_i}{r},\quad p_i \in \{0,\dots,r-1\},\ 1\le i\le d,$$

with $\gcd(p_1,\dots,p_d,r) = 1$ and that

$$\left\{\sum_{i=1}^d \left(\frac{(j\cdot p_i) \bmod r}{r}\right) a^i : 1 \le j \le r-1\right\} \subset C \cap \mathbb{Z}^d\backslash\{0\}. \tag{2.2}$$

Now, by definition we have $h_C(b) \le \sum_{i=1}^d (p_i/r)$ and thus it suffices to show $\sum_{i=1}^d \frac{p_i}{r} \le (d-1) - (d-2)/r$ (cf. (2.1)). Assume the contrary, i.e.,

$$\sum_{i=1}^d p_i \ge (d-1)(r-1) + 2. \tag{2.3}$$

Then $r \ge 3$ and we show that b can be written as the sum of two elements contained in the set on the left hand side of (2.2). This contradicts (1.1).

For $1 \le i \le d$ let

$$\mathcal{M}(p_i,r) = \{j \in \{0,\dots,r-1\} : jp_i \bmod r \le p_i\}.$$

Lemma 1 yields the bound $\#\mathcal{M}(p_i, r) \geq p_i + 1$ and by (2.3) we get

$$\sum_{i=1}^{d} \#\mathcal{M}(p_i, r) \geq (d-1)r + 3.$$

Lemma 2 says that the intersection $\cap_{i=1}^{d} \mathcal{M}(p_i, r)$ contains an element $k \in \{2, \ldots, r-1\}$, say. By the definition of the sets $\mathcal{M}(p_i, r)$ we have

$$p_i = \Big((k \cdot p_i) \bmod r\Big) + \Big(((r-1-k) \cdot p_i) \bmod r\Big), \quad 1 \leq i \leq d,$$

and we get the desired contradiction

$$b = \sum_{i=1}^{d} \left(\frac{(k \cdot p_i) \bmod r}{r}\right) a^i + \sum_{i=1}^{d} \left(\frac{((r-1-k) \cdot p_i) \bmod r}{r}\right) a^i.$$

□

3 Some consequences of Theorem 1

Theorem 1 may be used to derive the following lower bound.

Corollary 1. *Let $C = \operatorname{pos}\{a^1, \ldots, a^d\}$ be a pointed cone such that $a^1, \ldots, a^d \in \mathbb{Z}^d$ are linearly independent. If $\mathcal{B}(C) = \{a^1, \ldots, a^d\} \cup \{z \in \mathbb{Z}^d : z = \sum_{i=1}^{d} \lambda_i a^i,\ 0 \leq \lambda_i < 1\}$ then for $b \in \mathcal{B}(C)$ contained in the interior of C one has*

$$h_C(b) \geq 1 + \frac{d-2}{|\det(a^1, \ldots, a^d)|}.$$

Proof. Since b is contained in the interior of C the lattice point $\bar{b} = \sum_{i=1}^{d} a^i - b$ is contained in the half open parallelepiped generated by $a^1, \ldots, a^d$. Hence, by assumption $\bar{b} \in \mathcal{B}(C)$ and Theorem 1 yields

$$h_C(\bar{b}) = d - h_C(b) \geq 1 + (d-2)/|\det(a^1, \ldots, a^d)|.$$

□

The next corollary shows an application of Theorem 1 in integer programming.

Corollary 2. *Let $A \in \mathbb{Z}^{m \times d}$ with all subdeterminants at most α in absolute value and let $b \in \mathbb{Z}^m$, $c \in \mathbb{Z}^d$ be given vectors. If $\widetilde{z}$ is a feasible, non-optimal solution of the program $\max\{c^T z : Az \leq b,\ z \in \mathbb{Z}^d\}$, then there exists a feasible solution $\widehat{z}$ such that $c^T\widehat{z} > c^T\widetilde{z}$ and*

$$|\widehat{z} - \widetilde{z}|_\infty \leq (d-1)\alpha - \frac{d-2}{d^{d/2}\alpha^{d-2}},$$

where $|\cdot|_\infty$ denotes the maximum norm.

Proof. Let z^* be a feasible solution with $c^T z^* > c^T \widetilde{z}$. We split the system $Ax \leq b$ into subsystems $A_1 x \leq b_1$, $A_2 x \leq b_2$ such that $A_1 \widetilde{z} \leq A_1 z^*$ and $A_2 \widetilde{z} \geq A_2 z^*$. Let C be the cone

$$C = \{x \in \mathbb{R}^d : A_1 x \leq 0,\ A_2 x \geq 0\}$$

and $w^1, \ldots, w^n \in \mathbb{Z}^d$ such that $C = \text{pos}\{w^1, \ldots, w^n\}$. Using Cramer's rule we obtain that $|w^j|_\infty \leq \alpha$, $1 \leq j \leq n$. Since $z^* - \widetilde{z} \in C$ there exist $l \leq d$ linearly independent vectors $w^{i_1}, \ldots, w^{i_l}$ such that $z^* - \widetilde{z} \in \overline{C} = \text{pos}\{w^{i_1}, \ldots, w^{i_l}\}$. It follows that

$$z^* - \widetilde{z} = \sum_{i=1}^{k} n_i b^i, \quad n_i \in \mathbb{N}\backslash\{0\}$$

for some $b^1, \ldots, b^k \in \mathcal{B}(\overline{C})$. It is easy to see that $\widetilde{z} + b^i$, $i \in \{1, \ldots, k\}$, is a feasible solution. On account of the condition $c^T z^* > c^T \widetilde{z}$ we may assume that $c^T(\widetilde{z} + b^1) > c^T \widetilde{z}$. We define $\widehat{z} := \widetilde{z} + b^1$ and write b^1 as

$$b^1 = \sum_{j=1}^{l} \lambda_j w^{i_j}$$

with $\lambda_1, \ldots, \lambda_l \geq 0$. Applying Theorem 1 to the l-dimensional cone $\overline{C}$ together with the Hadamard inequality gives

$$|\widehat{z} - \widetilde{z}|_\infty \leq \alpha \left(\sum_{j=1}^{l} \lambda_j \right) \leq \alpha \left((l-1) - \frac{l-2}{|w^{i_1}| \cdots |w^{i_l}|)} \right).$$

As $|w^{i_j}| \leq d^{1/2}\alpha$, we obtain

$$|\widehat{z} - \widetilde{z}|_\infty \leq (l-1)\alpha - \frac{l-2}{d^{l/2}\alpha^{l-1}} \leq (d-1)\alpha - \frac{d-2}{d^{d/2}\alpha^{d-1}},$$

where the last inequality can be verified with elementary algebra. □

We remark that the bound of Corollary 2 strengthens the bound of $d\alpha$ given in [14].

We are grateful to Les Trotter jr. and Günter M. Ziegler for helpful discussions and comments.

References

[1] P. Gordan, *Über die Auflösung linearer Gleichungen mit reellen Coefficienten*, Math. Ann. **6** (1873), 23–28.

[2] A. Schrijver, *Theory of linear and integer programming*, John Wiley and Sons, Chichester, 1986.

[3] J.G. van der Corput, *Über Systeme von linear-homogenen Gleichungen und Ungleichungen*, Proceedings Koninklijke Akademie van Wetenschappen te Amsterdam **34** (1931), 368–371.

[4] A. Sebö, *Hilbert bases, Caratheodory's Theorem and combinatorial optimization*, Proc. of the IPCO conference, Waterloo, Canada, 1990, 431–455.

[5] R. Urbaniak, R. Weismantel, and G.M. Ziegler, *A variant of Buchberger's algorithm for integer programming*, SIAM J. Discrete Math., to appear.

[6] R. Weismantel, *Hilbert bases and the facets of special knapsack polytopes*, Math. Oper. Res. **21**(4) (1996), 896–904.

[7] C. Bouvier and G. Gonzalez-Springberg, *G-désingularisations de variétés toriques*, C. R. Acad.Sci. Paris, t.315, Série I, (1992), 817–820.

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

[9] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, Graduate Texts in Mathematics Vol. 168, Springer, Berlin, 1996.

[10] T. Oda, *Convex bodies and algebraic geometry*, Springer, New-York, 1985.

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

[12] J. Liu, L.E. Trotter, Jr., and G.M. Ziegler, *On the Height of the minimal Hilbert basis*, Result. Math. **23** (1993), 374–376.

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

[14] W. Cook, A.M.H. Gerards, A. Schrijver, and É. Tardos, *Sensitivity theorems in integer programming problems*, Math. Programming **34** (1986), 63–70.

Martin Henk, Robert Weismantel
Konrad-Zuse-Zentrum für Informationstechnik (ZIB) Berlin
Takustraße 7
D-14195 Berlin-Dahlem, Germany
E-mail: henk@zib.de, weismantel@zib.de

Eingegangen am 30. April 1997.