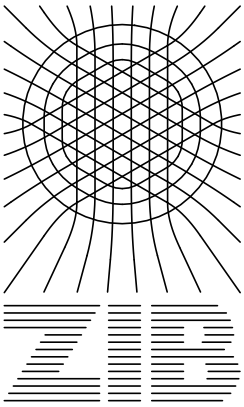
Konrad-Zuse-Zentrum für Informationstechnik Berlin
Takustraße 7, D-14195 Berlin



Test sets of the knapsack problem and simultaneous diophantine approximation

Martin Henk and Robert Weismantel

Preprint SC97-13 (March 1997)

Test sets of the knapsack problem and simultaneous diophantine approximation

Martin Henk* Robert Weismantel†

Abstract

This paper deals with the study of test sets of the knapsack problem and simultaneous diophantine approximation. The Graver test set of the knapsack problem can be derived from minimal integral solutions of linear diophantine equations. We present best possible inequalities that must be satisfied by all minimal integral solutions of a linear diophantine equation and prove that for the corresponding cone the integer analogue of Caratheodory's theorem applies when the numbers are divisible.

We show that the elements of the minimal Hilbert basis of the dual cone of all minimal integral solutions of a linear diophantine equation yield best approximations of a rational vector "from above". A recursive algorithm for computing this Hilbert basis is discussed. We also outline an algorithm for determining a Hilbert basis of a family of cones associated with the knapsack problem.

Keywords: knapsack problem, simultaneous diophantine approximation, diophantine equation, Hilbert basis, test sets.

1 Introduction

This paper deals with the study of test sets of the knapsack problem and simultaneous diophantine approximation. Both topics play a role in various branches of mathematics such as number theory, geometry of numbers and integer programming.

From the viewpoint of integer programming, minimal integral solutions of a linear diophantine equation allow to devise an exact primal algorithm for solving knapsack problems in non-negative integer variables,

$$\max c^T x : \ \alpha^T x = \beta, \ x \in \mathbb{N}^n, \tag{1.1}$$

where $c \in \mathbb{Z}^n$, $\alpha \in (\mathbb{N} \setminus \{0\})^n$ and $\beta \in \mathbb{N}$. More precisely, the primal methods that we consider here are augmentation algorithms, and the question we address is to describe the set of all possible augmentation vectors. This leads us to *test sets*.

*Supported by a "Leibniz Preis" of the German Science Foundation (DFG) awarded to M. Grötschel.

†Supported by a "Gerhard-Hess-Forschungsförderpreis" of the German Science Foundation (DFG).

A test set is a collection of all augmenting directions that one needs in order to guarantee that every non-optimal feasible point of a linear integer program can be improved by one member in the test set. There are various possible ways of defining test sets depending on the view that one takes: the *Graver test set* is naturally derived from a study of the integral vectors in cones [G75]; the *neighbors of the origin* are strongly connected to the study of lattice point free convex bodies [S86]; the so-called *reduced Gröbner basis* of an integer program is obtained from generators of polynomial ideals that is a classical field of algebra, [CT91]. We refrain within this paper from introducing all these three kinds of test sets, but concentrate on the Graver test set, only. In order to introduce the *Graver test set* for the family of knapsack problems with varying $c \in \mathbb{Z}^n$ and $b \in \mathbb{N}$, the notion of a rational polyhedral cone and its Hilbert basis is needed.

Definition 1.1. *For $z^1, \ldots, z^m \in \mathbb{Z}^n$, the set*

$$C := \operatorname{pos}\{z^1, \ldots, z^m\} = \left\{ \sum_{i=1}^{m} \lambda_i z^i : \lambda \in \mathbb{R}^m_{\geq 0} \right\}$$

is called a rational polyhedral cone. It is called pointed *if there exists a hyperplane $\{x \in \mathbb{R}^n : a^T x = 0\}$ such that $\{0\} = \{x \in C : a^T x \leq 0\}$.*

Definition 1.2. *Let $C \subseteq \mathbb{R}^n$ be a rational polyhedral cone. A finite subset $H = \{h^1, \ldots, h^t\} \subseteq C \cap \mathbb{Z}^n$ is a Hilbert basis of C if every $z \in C \cap \mathbb{Z}^n$ has a representation of the form*

$$z = \sum_{i=1}^{t} \lambda_i h^i,$$

with non-negative integral multipliers $\lambda_1, \ldots, \lambda_t$.

The name Hilbert basis was introduced by Giles and Pulleyblank [GP79] in the context of totally dual integral systems. Essential is (see [G1873], [C31])

Theorem 1.1. *Every rational polyhedral cone has a Hilbert basis. If it is pointed, then there exists a unique Hilbert basis that is minimal w.r.t. inclusion.*

In the following by a cone we always mean a rational polyhedral cone.

Let O_j denote the j-th orthant in $\mathbb{R}^n$. For $A \in \mathbb{Z}^{m \times n}$, the set $C_j := \{x \in O_j : Ax = 0\}$ is a pointed cone in $\mathbb{R}^n$. Denoting by H_j the minimal Hilbert basis of C_j, Graver proved the following: The set $H := \bigcup_j H_j$ is a test set for the family of integer programs of the form $\max c^T x : Ax = b,\ x \in \mathbb{N}^n$ for a fixed matrix $A \in \mathbb{Z}^{m \times n}$ and varying $c \in \mathbb{Z}^n$ and $b \in \mathbb{Z}^m$.

This result is the starting point for our discussions. Namely, in order to devise an exact primal algorithm for solving a knapsack problem of the form (1.1), we need to determine, for every orthant O_j in $\mathbb{R}^n$, a Hilbert basis H_j of the so-called *knapsack cone* $C_j = \{x \in O_j : \alpha^T x = 0\}$.

We present in this paper best possible inequalities that must be satisfied by all the elements of the minimal Hilbert basis of C_j and prove that for C_j the integer analogue of Caratheodory's theorem applies when the numbers $\{\alpha_1, \ldots, \alpha_n\}$ are pairwise divisible. We also show that the elements of the minimal Hilbert basis of the dual of C_j yield best approximations of a rational vector "from above". A recursive algorithm for computing this Hilbert basis is discussed. A similar type of procedure applies to the cone C_j. Therefore this method can also be used to find a test set of the knapsack problem.

2 The knapsack cone

Up to a permutation of the coordinates, a knapsack cone C_j can be identified with the set $K_{n,m}$ of all non-negative solutions of a linear diophantine equation, i.e.,

$$K_{n,m} = \left\{ (x,y)^T \in \mathbb{R}^n_{\geq 0} \times \mathbb{R}^m_{\geq 0} : \sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j \right\},$$

where we always assume that $a = (a_1, \ldots, a_n)^T \in \mathbb{N}^n$, $b = (b_1, \ldots, b_m)^T \in \mathbb{N}^m$, $n \geq m \geq 1$ and $a_1 \leq a_2 \leq \cdots \leq a_n$, $b_1 \leq b_2 \leq \cdots \leq b_m$. It is easy to see that

$$K_{n,m} = \text{pos}\left\{ b_j e^i + a_i e^{n+j} : 1 \leq i \leq n,\ 1 \leq j \leq m \right\}, \tag{2.1}$$

where $e^i \in \mathbb{R}^{n+m}$ denotes the i-th unit vector. The minimal Hilbert basis of $K_{n,m}$ is denoted by $\mathcal{H}_{n,m}$.

One of the major results of this paper is to show that every element in $\mathcal{H}_{n,m}$ satisfies $n+m$ special inequalities that generalize the two inequalities $\sum_{i=1}^{n} x_i \leq b_m$ and $\sum_{j=1}^{m} y_j \leq a_n$ proved by Lambert ([L87]) and independently by Diaconis, Graham & Sturmfels [DGS94].

Theorem 2.1. *Every $(x,y)^T \in \mathcal{H}_{n,m}$ satisfies the inequalities*

$$[j_l]: \quad \sum_{i=1}^{n} x_i + \sum_{j=1}^{l-1} \left\lfloor \frac{b_l - b_j}{a_n} \right\rfloor y_j \leq b_l + \sum_{j=l+1}^{m} \left\lceil \frac{b_j - b_l}{a_1} \right\rceil y_j, \quad l = 1, \ldots, m,$$

$$[i_k]: \quad \sum_{j=1}^{m} y_j + \sum_{i=1}^{k-1} \left\lfloor \frac{a_k - a_i}{b_m} \right\rfloor x_i \leq a_k + \sum_{i=k+1}^{n} \left\lceil \frac{a_i - a_k}{b_1} \right\rceil x_i, \quad k = 1, \ldots, n.$$

From an algorithmic point of view Theorem 2.1 allows to assert that an integral point in $K_{n,m}$ does not belong to a minimal Hilbert basis of this cone. This problem is in general $\mathcal{NP}$-complete, see Sebö [S90].

Theorem 2.2 (The Decomposition Problem). *For the pointed cone $K_{n,m}$, and a vector $(x,y)^T \in K_{n,m} \cap \mathbb{Z}^{n+m}$ it is co-$\mathcal{NP}$-complete to decide whether $(x,y)^T$ is contained in $\mathcal{H}_{n,m}$.*

Theorem 2.2 asserts the difficulty of testing for non-membership in $\mathcal{H}_{n,m}$. On the other hand, every integral vector in this cone can be decomposed by vectors of the basis. In fact we can write every integral vector in any pointed cone of dimension n as the non-negative integer combination of at most $2n-2$ vectors from the basis. This was shown by Sebö [S90] and gives currently the best bound in general; it improves the bound given by Cook, Fonlupt & Schrijver [CFS86] by 1, yet is still quite far from what many researchers conjecture to be true, namely: every integral vector in a pointed cone is the non-negative integer combination of at most n vectors of the Hilbert basis. We now prove that this *integer Version of Caratheodory's Theorem* holds for the knapsack cone when the numbers are divisible.

Theorem 2.3. *Let positive integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$ be given such that there exist $p_i, q_j \in \mathbb{N}$ with*

$$a_i = p_i \cdot a_{i-1},\ i = 2, \ldots, n, \quad b_1 = q_1 \cdot a_n,\ b_j = q_j \cdot b_{j-1},\ j = 2, \ldots, m.$$

Every integral point in $K_{n,m}$ can be written as the non-negative integer combination of at most $n+m-1 = \dim(K_{n,m})$ elements of $\mathcal{H}_{n,m}$.

Let us point out that, although Theorem 2.1 gives the best inequalities known so far to assert that an integral point in $K_{n,m}$ does not belong to the minimal Hilbert basis, we believe that a much stronger and more general statement is true: every element in the minimal Hilbert basis of $K_{n,m}$ is a convex combination of 0 and the generators $b_j e^i + a_i e^{n+j}$ of $K_{n,m}$. More formally, let

$$P_{n,m} = \operatorname{conv}\left\{0, b_j e^i + a_i e^{n+j} \,:\, 1 \le i \le n,\, 1 \le j \le m\right\}.$$

One might conjecture that

Conjecture 2.1. $\mathcal{H}_{n,m} \subset P_{n,m}$.[1]

For $m = 1$ Theorem 2.1 implies the inclusion $\mathcal{H}_{n,1} \subset P_{n,1}$. This can easily be read off from the representation

$$P_{n,1} = \left\{(x,y)^T \in \mathbb{R}^n \times \mathbb{R} :\; a^T x = b_1 y; x, y \ge 0, \sum_{i=1}^{n} x_i \le b_1\right\}.$$

One way of verifying the correctness of the conjecture could be to find all facets defining inequalities of $P_{n,m}$ and to check that these inequalities are satisfied by the elements of $H_{n,m}$. A subset of the facets defining inequalities is given by

Proposition 2.1. *For $l = 1, \ldots, m$ let*

$$J_l = \left\{(x,y) \in \mathbb{R}^n \times \mathbb{R}^m : \sum_{i=1}^{n} x_i + \sum_{j=1}^{l-1} \frac{b_l - b_j}{a_n} y_j \le b_l + \sum_{j=l+1}^{m} \frac{b_j - b_l}{a_1} y_j\right\}$$

and for $k = 1, \ldots, n$ let

$$I_k = \left\{(x,y) \in \mathbb{R}^n \times \mathbb{R}^m : \sum_{j=1}^{m} y_j + \sum_{i=1}^{k-1} \frac{a_k - a_i}{b_m} x_i \le a_k + \sum_{i=k+1}^{n} \frac{a_i - a_k}{b_1} x_i\right\}.$$

$P_{n,m} \subset J_l$, $P_{n,m} \subset I_k$. Moreover, the inequalities defining the halfspaces J_l and I_k define facets of $P_{n,m}$, $1 \le l \le m$, $1 \le k \le n$.

Remark 2.4. *Since $P_{n,2} = \{(x,y)^T \in \mathbb{R}^n \times \mathbb{R}^2 : a^T x = b^T y; x, y \ge 0, (x,y)^T \in I_k,\, 1 \le k \le n\}$, Theorem 2.1 shows that the conjecture is "almost true" when $m = 2$.*

3 Best approximations "from above"

In this section we deal with a cone that on the first view seems to be not related to the knapsack cone investigated before.

[1] This conjecture was independently made by Hosten and Sturmfels, private communication

Let $e^1, \ldots, e^n$ denote the n unit vectors in $\mathbb{R}^{n+1}$ having a 1 in coordinate $1, \ldots, n$, respectively. For $p \in \mathbb{Z}^{n+1}$ such that $\gcd(p_1, \ldots, p_{n+1}) = 1$, $p_1, \ldots, p_k > 0$, $p_{k+1}, \ldots, p_n < 0$ and $p_{n+1} > 0$, let

$$C(p) = \operatorname{pos}\{e^1, \ldots, e^n, p\}. \tag{3.1}$$

It turns out that the dual cone $C(p)^*$ of $C(p)$ is "essentially" the knapsack cone. This result builds the bridge towards the previous section. By definition, $C(p)^*$ can be written as $C(p)^* = \{v \in \mathbb{R}^{n+1} : v^T x \geq 0, \ \forall\, x \in C(p)\}$. Since the generators of $C(p)$ consist of the unit vectors $e^1, \ldots, e^n$ plus the vector $p \in \mathbb{Z}^{n+1}$, we obtain

$$C(p)^* = \left\{ v \in \mathbb{R}^n_{\geq 0} \times \mathbb{R} : \sum_{i=1}^{k} v_i \cdot p_i \geq \sum_{i=k+1}^{n} v_i \cdot (-p_i) - v_{n+1} p_{n+1} \right\}.$$

Depending on the sign of v_{n+1}, we partition $C(p)^*$ into the following two cones

$$\begin{aligned} C(p)^*_{\geq} &= \left\{ v \in \mathbb{R}^{n+1}_{\geq 0} : \sum_{i=1}^{k} v_i p_i + v_{n+1} p_{n+1} \geq \sum_{i=k+1}^{n} v_i \cdot (-p_i) \right\}, \\ C(p)^*_{\leq} &= \left\{ v \in \mathbb{R}^n_{\geq 0} \times \mathbb{R}_{\leq 0} : \sum_{i=1}^{k} v_i p_i \geq \sum_{i=k+1}^{n} v_i \cdot (-p_i) + (-v_{n+1}) p_{n+1} \right\}. \end{aligned}$$

Both cones, $C(p)^*_{\geq}$ and $C(p)^*_{\leq}$ may be regarded as "$\geq$-knapsack cones", or, the facet of the cone $C(p)^*_{\geq}$ ($C(p)^*_{\leq}$) induced by the non-trivial inequality is a knapsack cone of the form $K_{k+1,n-k}$ ($K_{k,n-k+1}$) that we studied in Section 2.

In the remainder of this section we study the minimal Hilbert basis of $C(p)$. It turns out that this basis is closely related to the problem of simultaneous diophantine approximation of rational numbers by other rational numbers with an upper bound on the denominator. More precisely, we consider the following approximation problem:

Simultaneous Diophantine Approximation "from above":

Let $p_1, \ldots, p_{n+1} \in \mathbb{Z}$, $p_{n+1} > 0$, and $N \in \mathbb{Z}$, $N > 0$.
Find integers $q_1, \ldots, q_{n+1}$, $N \geq q_{n+1} > 0$ such that $q_i/q_{n+1} \geq p_i/p_{n+1}$, $i = 1, \ldots, n$, and $\sum_{i=1}^{n} (\frac{q_i}{q_{n+1}} - \frac{p_i}{p_{n+1}})$ is as small as possible.
The vector $q' = (\frac{q_1}{q_{n+1}}, \ldots, \frac{q_n}{q_{n+1}})$ is called a best approximation of $p' = (\frac{p_1}{p_{n+1}}, \ldots, \frac{p_n}{p_{n+1}})$ from above with respect to N.

It is clear that if $N \geq p_{n+1}$, then $p' = (\frac{p_1}{p_{n+1}}, \ldots, \frac{p_n}{p_{n+1}})$ itself is its best approximation from above. It is, however, not clear how one can characterize a best approximation of p' from above when $N < p_{n+1}$. We show that a best approximation of p' from above can be read off from the minimal Hilbert basis of $C(p)$.

Theorem 3.1. *Let $p_1, \ldots, p_{n+1} \in \mathbb{Z}$, $p_{n+1} > 0$, and $N \in \mathbb{Z}$, $N > 0$. There exists an element $(q_1, \ldots, q_{n+1})$ of the minimal Hilbert basis of $C(p)$ such that $q' = (\frac{q_1}{q_{n+1}}, \ldots, \frac{q_n}{q_{n+1}})$ is a best approximation of $p' = (\frac{p_1}{p_{n+1}}, \ldots, \frac{p_n}{p_{n+1}})$ from above with respect to N. Moreover, among all such best approximations of p', q' is the unique one with smallest denominator q_{n+1}.*

Instead of restricting our attention to approximations of a rational vector p' from above, one could ask for approximations where, for any of the components of p', one would specify a-priori, whether the approximation should lie below or above the corresponding value of p'. Theorem 3.1 can be extended to this situation.

Theorem 3.2. *Let $\sigma \in \{-1,+1\}^n$ be the sign pattern associated with one orthant of $\mathbb{R}^n$. Let $p_1,\ldots,p_{n+1} \in \mathbb{Z}$, $p_{n+1} > 0$, and $N \in \mathbb{Z}$, $N > 0$. There exists an element $(q_1,\ldots,q_{n+1})$ of the minimal Hilbert basis of $\operatorname{pos}\{\sigma_1 e^1,\ldots,\sigma_n e^n, p\}$ such that*

$$\sum_{i=1}^{n}\left|\frac{q_i}{q_{n+1}}-\frac{p_i}{p_{n+1}}\right| = \min\left\{\sum_{i=1}^{n}\left|\frac{x_i}{x_{n+1}}-\frac{p_i}{p_{n+1}}\right| : x_1,\ldots,x_{n+1}\in\mathbb{Z},\right.$$
$$\left. N \geq x_{n+1} > 0,\ \sigma_i\left(\frac{x_i}{x_{n+1}}-\frac{p_i}{p_{n+1}}\right)\geq 0\right\}.$$

Among all solutions of this diophantine approximation problem, $(\frac{q_1}{q_{n+1}},\ldots,\frac{q_n}{q_{n+1}})$ is the unique one with smallest denominator.

4 A recursive algorithm for the Hilbert basis of $C(p)$ and the knapsack cone

We have motivated in the previous sections why the Hilbert basis of the knapsack cone and the cone of best approximations from above is of particular interest. In this section we treat algorithmic questions related to these bases. We first deal with the cone $C(p) = \operatorname{pos}\{e^1,\ldots,e^n,p\} \subseteq \mathbb{R}^{n+1}$ related to the best approximations from above. Applying a unimodular transformation we may assume that $p = (p_1,\ldots,p_{n+1}) \in \mathbb{N}^{n+1}$.

We remark that it is trivial to find a Hilbert basis of $C(p)$, because it is well known that $\{e^1,\ldots,e^n,p\} \cup \{z \in \mathbb{Z}^{n+1} : z = \sum_{i=1}^{n}\lambda_i e^i + \lambda_{n+1}p, 0 \leq \lambda_i < 1\}$ actually is a Hilbert basis of $C(p)$ (cf. [C31]). All we are left with is to enumerate these integral points. However, in general, the size of this Hilbert basis is exponentially larger than the size of the minimal Hilbert basis, and, of course, we are interested in computing a "small" one.

We proceed in an inductive fashion to compute the basis of $C(p)$: Let H_2 be the minimal Hilbert basis of the 2-dimensional cone

$$C_2 := \operatorname{pos}\{e^1,(p_n,p_{n+1})^T\}.$$

It is clear that $e^1 \in H_2$. Let $(w_1,h_1) < \ldots < (w_m,h_m) \in H_2 \setminus \{e^1\}$ be the remaining elements in H_2. It follows that, for every $x \in C(p)\cap\mathbb{Z}^{n+1}$ with $x_{n+1} > 0$, the coordinate x_{n+1} has a representation of the form $x_{n+1} = \sum_{v=1}^{m}\mu_v h_v$ with $\mu_1,\ldots,\mu_m \in \mathbb{N}$.

Definition 4.1. *For $i,j \in \{1,\ldots,m-1\}$, $i < j$, let*

$$C^{i,j} := \left\{x \in C(p)\cap\mathbb{Z}^{n+1} :\ \exists\,\mu_i,\ldots,\mu_j \in \mathbb{N},\ 0 < x_{n+1} = \sum_{v=i}^{j}\mu_v h_v < h_{j+1}\right\}.$$

We say that $\{g^1,\ldots,g^t\} \subseteq L$ are generators of a set $L \subseteq \mathbb{Z}^n$ if, for every $x \in L$, there exist $\sigma_1,\ldots,\sigma_t \in \mathbb{N}$ such that $x = \sum_{v=1}^{t}\sigma_v g^v$.

Noting that $h_m = p_{n+1}$, the following statement is immediate.

Lemma 4.2. *The union of $\{e^1, \ldots, e^n, p\}$ and a set of generators of $C^{1,m-1}$ defines a Hilbert basis of $C(p)$.*

In fact, an inclusionwise ordering of all the subsets $C^{i,j}$ is possible.

Lemma 4.3. *For every $i' \leq i \leq j \leq j' \in \{1, \ldots, m-1\}$, a minimal set of generators of $C^{i,j}$ (w.r.t. inclusion) defines a subset of any set of generators of $C^{i',j'}$.*

On account of Lemma 4.2 it suffices to find generators of $C^{1,m-1}$ in order to determine a Hilbert basis of $C(p)$. A set of generators of $C^{1,m-1}$ can be computed in a recursive manner.

Algorithm 4.4. Recursion formula to find the generators of $C^{1,m-1}$.

(1) *For $i = 1, \ldots, m-1$ determine generators of $C^{i,i}$.*
(2) *For $i = m-2, \ldots, 1$ determine generators of $C^{i,m-1}$.*

The reason why this recursion makes sense is that the task of finding a set of generators of $C^{i,i}$ can be solved with a procedure to determine the Hilbert basis of a cone similar to $C(p)$, but in one dimension less. Secondly, if one has, for $i = m-2, \ldots, 1$ as input a set of generators of $C^{i,i}$ and $C^{i+1,m-1}$, then one can devise a procedure that returns generators of $C^{i,m-1}$. This is the idea behind the recursion.

Lemma 4.5. *Let $\tilde{p} = (p_1, \ldots, p_{n-1}, h_i p_{n+1}) \in \mathbb{N}^n$ and let $e^1, \ldots, e^{n-1}$ denote the first $n-1$ unit vectors of $\mathbb{R}^n$. For $i \in \{1, \ldots, m-1\}$, let H^i be a Hilbert basis of the n-dimensional cone $C(\tilde{p}) = \operatorname{pos}\{e^1, \ldots, e^{n-1}, \tilde{p}\}$. The set $\{(x_1, \ldots, x_{n-1}, zw_i, zh_i) : (x_1, \ldots, x_{n-1}, z) \in H^i,\ 0 < zh_i < h_{i+1}\}$ is a set of generators of $C^{i,i}$.*

Lemma 4.5 shows that a set of generators of $C^{i,i}$ can easily be reconstructed from a Hilbert basis of the cone $C(\tilde{p})$. This is where the inductive step comes into play. In order to solve Step (2) of Algorithm 4.4 one must be able to turn a set of generators of $C^{i,i}$ and $C^{i+1,m-1}$ into a set of generators of $C^{i,m-1}$. This task may again be solved with a recursive algorithm that would read as follows.

Algorithm 4.6. (Recursion to find $C^{i,m-1}$)

Input: *An ordered set $\{g^1, \ldots, g^t\}$ of generators of $C^{i+1,m-1}$ with $g^1_{n+1} < \ldots < g^t_{n+1}$; a set of generators of $C^{i,i}$.*

Output: *A set of generators of $C^{i,m-1}$;*

For every $v \in \{1, \ldots, t\}$ determine a set of generators of the set $G_v := \{y \in C^{i,m-1} : y_{n+1} < g^v_{n+1}\}$.

Lemma 4.7. *$G_1 = C^{i,i}$ and $G_{t+1} = C^{i,m-1}$.*

Lemma 4.7 shows that when we enter the for-loop of Algorithm 4.6, a set of generators of $C^{i,i}$ is also a set of generators of G_1. Then we proceed through all values of v and determine a set of generators of G_v using a set of generators of G_{v-1}. When v equals $t+1$, we terminate with a set of generators of G_{t+1} that corresponds to a set of generators of $C^{i,m-1}$.

The key of Algorithm 4.6 is a subroutine for returning a set of generators of G_{v+1} whose input consists of a set of generators of G_v. It is not difficult to see that G_{v+1} is equal to the set

$$\begin{aligned} S \;=\; & \{x \in C^{i,m-1} : \exists\, \lambda \in \{0,\ldots,\lambda_v\}, y \in G_v \text{ s.t.} \\ & x_{n+1} = \lambda g^v_{n+1} + y_{n+1} < g^{v+1}_{n+1}\}, \end{aligned} \tag{4.1}$$

where $\lambda_v := \max\{\lambda \in \mathbb{N} :\ \lambda g^v_{n+1} < g^{v+1}_{n+1}\}$ and $g^{t+1}_{n+1} := h_m$. The generators of G_{v+1} are points of the form

$$(x_1,\ldots,x_{n+1}) \in S :\ x_i = \lceil \frac{p_i x_{n+1}}{p_{n+1}} \rceil,\ i = 1,\ldots,n. \tag{4.2}$$

To each point x of the form (4.2) there corresponds a n-dimensional vector of residua of components $x_i p_{n+1} - x_{n+1} p_i$, $i = 1,\ldots,n$. In fact, one can show that the minimal set of generators of G_{v+1} can be characterized as follows: we order the integral points of the form (4.2) w.r.t. increasing last coordinate; the vector of residua of a point that appears later in this sequence is incomparable with the vectors of residua of all points that occur earlier in this sequence. Resorting to appropriate data structures that contain information about the vector of residua for every element in G_v one can determine a set of generators of G_{v+1} without testing every integral point in S.

For precisely this reason, Algorithm 4.4 yields a much more sophisticated algorithm for determining the Hilbert basis of $C(p)$ than the trivial method discussed at the beginning of the section.

We now illustrate the essential steps of Algorithm 4.4 on an example.

Example. Let $n = 2$ and $p = (30, 29, 17)$. The elements of the Hilbert basis of $C(p) = \text{pos}\,\{e^1, e^2, p\}$ that we are interested in consists of integral points of the form $(x_1, x_2, x_3) \in \mathbb{N}^3$ with $x_3 \leq p_{n+1} = 17$ and $x_i = \lceil \frac{p_i x_3}{p_3} \rceil$ for $i = 1, 2$. To each such point x there corresponds the 2-dimensional vector of residua $(x_1 p_3 - x_3 p_1, x_2 p_3 - x_3 p_2)$. Table 4 includes this information.

By $(w_1, h_1), \ldots, (w_m, h_m)$ we denote all elements in the Hilbert basis of the 2-dimensional subcone $C_2 := \{e^1, (29, 17)^T\}$, except for e^1. In our example we have that $m = 4$ and $(w_1, h_1) = (2, 1)$, $(w_2, h_2) = (7, 4)$, $(w_3, h_3) = (12, 7)$ and $(w_4, h_4) = (29, 17)$.

Following Algorithm 4.4 we execute Step (1) to find generators of the sets $C^{1,1}, C^{2,2}, C^{3,3}$. Lemma 4.5 implies that a generator of $C^{1,1}$ is the element $(2, 2, 1)$. Accordingly, we see that a generator of $C^{2,2}$ is the element $(8, 7, 4)$ and that the vectors $(13, 12, 7)$ and $(25, 24, 14)$ define generators of $C^{3,3}$.

With this information we can start Step (2) of Algorithm 4.4. There we first determine generators of $C^{2,3} = \{x \in C \cap \mathbb{Z}^3 :\ \exists\, \mu_2, \mu_3 \in \mathbb{N} \text{ with } p_3 > x_{n+1} = 4\mu_2 + 7\mu_3\}$. The generators of this set coincide with the union of the generators of $C^{2,2}$ and $C^{3,3}$. It remains to find the generators of $C^{1,3}$. To find these, we inspect the generators of $C^{2,3}$ in the following order: first $g^1 = (8, 7, 4)$, then $g^2 = (13, 12, 7)$ and finally $g^3 = (23, 23, 13)$.

For every such element we determine the maximal natural number λ_v such that $\lambda_v g^v_3 < g^{v+1}_3$. The corresponding numbers in this case are $\lambda_1 = \lambda_2 = \lambda_3 = 1$.

For $g^1 = (8, 7, 4)$, we determine the minimal natural number μ such that the residuum of the vector $g^1 + \mu(2, 2, 1)$ exceeds the value of $p_3 = 17$ in one

x_3	vector	residuum	x_3	vector	residuum
1	**(2,2,1)**	$(4,5)$	2	$(4,4,2)$	$(8,10)$
3	$(6,6,3)$	$(12,15)$	4	**(8,7,4)**	$(16,3)$
5	**(9,9,5)**	$(3,8)$	6	$(11,11,6)$	$(7,13)$
7	**(13,12,7)**	$(11,1)$	8	$(15,14,8)$	$(15,6)$
9	**(16,16,9)**	$(2,11)$	10	$(18,18,10)$	$(6,16)$
11	**(20,19,11)**	$(10,4)$	12	$(22,21,12)$	$(14,9)$
13	**(23,23,13)**	$(1,14)$	14	**(25,24,14)**	$(5,2)$
15	$(27,26,15)$	$(9,7)$	16	$(29,28,16)$	$(13,12)$
17	**(30,29,17)**	$(0,0)$			

Table 4
All vectors that are written in bold together with the unit vectors e^1, e^2 define the minimal Hilbert basis of $C(p)$.

component. This gives $\mu = 1$, and the corresponding vector is $(9,9,5)$ that we add to the generators of $C^{1,3}$. For all the other vectors whose 3rd. coordinate is of the form $g_3^1 + \mu < g_3^2$, the associated vectors of residua are greater than the residuum of the point $(9,9,5)$.

Next we proceed to g^2. We know from the previous iteration the generators of $G_2 := \{y \in C^{1,3} : y_3 < g_3^2 = 7\}$. This was the set $\{(2,2,1),(8,7,4),(9,9,5)\}$. On account of (4.1), G_3 is of the form $G_3 = \{x \in C^{1,3} : \exists\, \lambda \in \{0,\ldots,\lambda_2 = 1\}$ and $y \in G$ such that $x_3 = \lambda g_3^2 + y_3 < g_3^3\}$. In order to find generators of G_3 we have to examine the vector of residua of the points $x \in G_3$. There are precisely two additional vectors for which the vector of residua is incomparable with every vector of residua of the generators of G_2: $(16,16,9)$ and $(20,19,11)$. A set of generators of G_3 is

$$\{(2,2,1),(8,7,4),(9,9,5),(13,12,7),(16,16,9),(20,19,11)\}.$$

Next we proceed to g^3. Because $\lambda_3 = 1$ we need to find the set of all points $x \in G_4 = \{x \in C^{1,3} : \exists\, \lambda \in \{0,1\}$ and $y \in G_3$ such that $x_3 = \lambda g_3^3 + y_3 < 17\}$ and the vector of residua is incomparable with every vector of residua associated with the generators of G_3. This yields the vector $(25,24,14)$. On account of lemma 4.7, the sets $C^{1,3}$ and G_4 coincide. The generating set of $C^{1,3}$ consists of the following vectors: $(2,2,1)$, $(8,7,4)$, $(9,9,5)$, $(13,12,7)$, $(16,16,9)$, $(20,19,11)$, $(23,23,13)$, $(25,24,14)$. These vectors plus the vectors e^1, e^2 and p define a Hilbert basis of $C(p)$ in this example.

We want to remark that when $p \in \mathbb{N}^{n+1}$, then $C(p)^*$ partitions into the two cones $\mathbb{R}^{n+1}_{\geq 0}$ and a $\geq$-knapsack cone of the form (cf. Section 2)

$$C(p)^*_{\geq} = \left\{ x \in \mathbb{R}^{n+1}_{\geq 0} : \sum_{i=1}^{n} p_i x_i \geq p_{n+1} x_{n+1} \right\}.$$

There is a similar recursive way of computing a "small" Hilbert basis of $C(p)^*_{\geq}$. Let H_2 be the minimal Hilbert basis of the 2-dimensional cone $C_2 := \{(y,z) \in$

$\mathbb{R}^2_{\geq 0}:\ p_n y \geq p_{n+1} z\}$. Then $e^1 \in H$. Let $(h_1, w_1) < \ldots < (h_m, w_m)$ be all the elements of $H \setminus \{e^1\}$ ordered in this way. For $i \in \{1, \ldots, m-1\}$ we introduce a parameter λ_i to denote the maximal natural number such that $\lambda_i h_i < h_{i+1}$. Then we know that for every $x \in C(p)^*_{\geq} \cap \mathbb{Z}^{n+1}$ with $x_n \neq 0$, x_n can be written as $x_n = \sum_{v=1}^m \mu_v h_v$ with $\mu_1, \ldots, \mu_m \in \mathbb{N}$. We define, for every $i \in \{1, \ldots, m-1\}$, the set $C^i := \{x \in C(p)^*_{\geq} \cap \mathbb{Z}^{n+1}:\ h_{i+1} > x_n = \lambda h_i + y_n > 0,\ y \in \bigcup_{j=1}^{i-1} C^j,\ \lambda \in \{0, \ldots, \lambda_i\}\}$. Realizing that a Hilbert basis of $C(p)^*_{\geq}$ consists of the union of the element $h_m e^n - w_m e^{n+1}$, the set $\{e^1, \ldots, e^{n+1}\}$ and a generating set of C^{m-1}, the following recursive procedure to determine the Hilbert basis of $C(p)^*_{\geq}$ becomes obvious.

Algorithm 4.8. *For $i = 1, \ldots, m-1$ determine a set of generators of C^i.*

Finally, we remark that a similar recursion can be formulated to determine the Hilbert basis of a knapsack cone $K_{n,m}$, see Section 2.

References

[CT91] P. Conti, C. Traverso, *Buchberger algorithm and integer programming*, Proceedings AAECC-9 (New Orleans), Springer LNCS 539, 130 - 139 (1991).

[CFS86] W. Cook, J. Fonlupt, and A. Schrijver, *An integer analogue of Caratheodory's theorem*, J. Comb. Theory (B) **40**, 1986, 63–70.

[C31] J.G. van der Corput, *Über Systeme von linear-homogenen Gleichungen und Ungleichungen*, Proceedings Koninklijke Akademie van Wetenschappen te Amsterdam 34, 368 - 371 (1931).

[DGS94] P. Diaconis, R. Graham, and B. Sturmfels, *Primitive partition identities,* Paul Erdös is 80, Vol. II, Janos Bolyai Society, Budapest, 1-20 (1995).

[GP79] F.R. Giles and W.R. Pulleyblank, *Total dual integrality and integer polyhedra*, Lineare Algebra Appl. 25, 191 - 196 (1979).

[G1873] P. Gordan, *Über die Auflösung linearer Gleichungen mit reellen Coefficienten*, Math. Ann. 6, 23 - 28 (1873).

[G75] J. E. Graver, *On the foundations of linear and integer programming I*, Mathematical Programming 8, 207 - 226 (1975).

[L87] J.L. Lambert, *Une borne pour les générateurs des solutions entiéres postives d'une équation diophnatienne linéaire*, C.R. Acad. Sci. Paris **305**, Série I, 1987, 39–40.

[S86] H. E. Scarf, *Neighborhood systems for production sets with indivisibilities*, Econometrica 54, 507 - 532 (1986).

[S90] A. Sebö, *Hilbert bases, Caratheodory's Theorem and combinatorial optimization*, in Proc. of the IPCO conference, Waterloo, Canada, 1990, 431–455.

Konrad-Zuse-Zentrum für Informationstechnik Berlin, Takustr. 7, D-14195 Berlin-Dahlem, henk@zib.de, weismantel@zib.de.