HILBERT BASES, CARATHEODORY'S THEOREM AND COMBINATORIAL OPTIMIZATION

András Sebő
IMAG, ARTEMIS, Université Fourier Grenoble 1, BP 53X
38041 GRENOBLE, Cedex, FRANCE

Abstract : A Hilbert basis is a set of vectors with the property that every integer vector in the cone generated by this set is also a nonnegative integer combination of its elements. Hilbert bases were defined by Giles and Pulleyblank (1979) to study total dual integrality. They come up in a natural way in different combinatorial optimization problems from matroid bases through totally dual integral inequality systems to matchings, arborescences or multicommodity flows, and formulate the pure algebraic essence of certain properties of these.

In this paper we are studying some structural properties of Hilbert bases. The main goal is to prove a Caratheodory type statement, a problem raised by a celebrated work of Cook, Fonlupt and Schrijver (1987). Proving it in some special cases we would like to show a new kind of approach to this problem. These special cases include combinatorial examples for which the "integral Caratheodory theorem" may be of interest for its own sake.

We would also like to show that the effect of this problem is beyond the integral Caratheodory problem: the main conjecture contains other results about totally dual integral systems, and more generally would become a basic structural property of combinatorial objects for which integer minimax theorems hold.

1. Introduction

The origins of the problem we are going to study lie in a seemingly innocent question of Cunningham (1987) related to testing membership in matroid polyhedra: *if a vector can be written as a non-negative integer combination of (characteristic vectors of) matroid bases, can it also be expressed as a non-negative integer combination of a small number of matroid bases.* Cunningham gave a first answer to this question that was satisfactory for his goals: if the ground-set of the matroid has n elements, a polynomial number $O(n^4)$ of matroid bases are always enough.

It is an easy consequence of Edmonds' (1970) matroid partition theorem that matroid bases have the property that any vector that can be written both as their non-negative and their integer combination can also be written as their non-negative integer combination. This property turned out to be the only interesting one from the point of view of Cunningham's above mentioned question (see Cook, Fonlupt, Schrijver (1986)). It is actually the algebraic essence of different combinatorial objects as it was shown by the papers referred to above, and as we would like to point out later.

The set of non-negative (real) combinations of the vectors $a_1, ..., a_k$ is called the *cone* generated by these vectors and will be denoted by cone$(a_1,...,a_k)$. "*cone*" will always mean polyhedral (that is finitely generated) cone. A cone is called *pointed*, if it does not contain any linear subspace besides the 0-space, or equivalently, if there exists a hyperplane such that the only element of the cone on the hyperplane is the 0, or equivalently, if the 0 vector cannot be written as a non-negative combination of the coefficient vectors of the linear inequalities describing the cone.

The lattice generated by the vectors $a_1,...,a_k \in \mathbb{Z}^n$ is the set of their integer combinations, and will be denoted by lat$(a_1,...,a_k)$. The *basis* of a lattice is a set of linearly independent vectors which generate the lattice. It is well-known that every lattice has a basis (cf. eg. Schrijver(1986)). $\det(a_1,...,a_n)$ will denote the determinant of the matrix whose columns are a_1, a_2,..., a_n.

The *parallelepiped* defined by the integer vectors $a_1,\ldots,a_k \in \mathbb{Z}^n$ will be the following set $\mathrm{par}(\mathrm{a}_1,\ldots,\mathrm{a}_\mathrm{k})$ of integer vectors:

$$\mathrm{par}(a_1,\ldots,a_k) := \{w = \sum_{i=1}^{k} \lambda_i a_i : 0 \leq \lambda_i < 1 \quad (i = 1,\ldots,k), \quad w \text{ integer } \}.$$

Motivated by total dual integral systems, Giles and Pulleyblank (1979) defined Hilbert bases, they and Schrijver (1981) proved some basic properties of them, and showed their relation to total dual integrality. Later works such as Cunningham (1987), Cook, Fonlupt and Schrijver (1986), or Lovász (1987) show that the significance of Hilbert bases is beyond totally dual integral systems. They play an important role in integer programming in general, for example in the Chvátal closing procedure (cf. Schrijver (1986)).

The finite set H will be called *Hilbert-generating-system*, if every vector in $\mathrm{cone}(\mathrm{a}_1,...,\mathrm{a}_\mathrm{k}) \cap \mathrm{lat}(\mathrm{a}_1,...,\mathrm{a}_\mathrm{k})$ can also be written as a non-negative integer combination of $a_1,...,a_k$. A *Hilbert basis* is a minimal Hilbert-generating-system of a given cone and lattice, that is H is a Hilbert basis if and only if it is a Hilbert generating system, and the cone generated by any proper subset of it is either not a Hilbert-generating-system or generates a smaller lattice or a smaller cone. The above mentioned property of matroid bases means exactly that they form a Hilbert generating system. Furthermore, since no matroid basis can be a non-negative combination of others, they form a Hilbert basis. (We do not distinguish subsets of a set from their characteristic (incidence) vectors).

Remark: This terminology slightly differs from that used in some other papers, but reflects somewhat the present folklore:
1. The term "Hilbert basis" was used earlier for Hilbert generating systems. Since bases in algebra are minimal generating systems, and since Schrijver (1981) has shown that pointed cones have a unique "minimal Hilbert basis" (see below), it was more and

more used for minimal systems as well, which causes some confusion.
2. In some papers Hilbert bases are restricted to satisfy $\mathrm{lat}(H) = \mathbb{Z}^n$, though not all the examples satisfy this restriction (for example matroid bases or matchings do not). This is not bad: if $\mathrm{lat}(H) \neq \mathbb{Z}^n$, use the linear transformation which brings a basis of $\mathrm{lat}(H)$ into the unit vectors. This linear transformation brings H to a Hilbert basis H' "isomorphic" to the original one, and $\mathrm{lat}(H') = \mathbb{Z}^n$. From now on *we shall also suppose that a Hilbert basis H satisfies* $\mathrm{lat}(H) = \mathbb{Z}^n$, and if we want to emphasize that an example does not satisfy this additional restriction we shall signal it.

Les Trotter (1987) has put the question of finding examples of "general TDI-systems" related to Hilbert bases without the assumption $\mathrm{lat}(H) = \mathbb{Z}^n$ in exactly the same way as TDI systems to Hilbert bases with this assumption (see Section 4). He has also found a nice example of "general TDI systems" which are not TDI in the usual sense, shown in Section 4.

We finish this introduction by three simple results and a series of conjectures about Hilbert bases that will play an important role in the sequel.

The *Hilbert generating system* or Hilbert basis of a cone C is a Hilbert generating system, or Hilbert basis of H with $C = \mathrm{cone}(H)$ and $\mathrm{lat}(H) = \mathbb{Z}^n$. In other words a Hilbert generating system of C is a finite set $H \subseteq C$ with the property that every integer vector in C is can be expressed as a non-negative integer combination of H; a Hilbert basis of C is an (inclusionwise) minimal Hilbert generating system of C. (An arbitrary Hilbert basis H (with $\mathrm{lat}(H) = \mathbb{Z}^n$) is the Hilbert basis of $\mathrm{cone}(H)$.) The following result is due to Giles and Pulleyblank (1979) :

Theorem 1.1 *Every cone has a finite Hilbert generating system.*

Proof. Let $C = \mathrm{cone}(a_1, \ldots, a_k)$. $\mathrm{par}(a_1, \ldots, a_k)$ is clearly a finite set, because it is bounded and it contains only integer vectors. But $\{a_1, \ldots, a_k\} \cup \mathrm{par}(a_1, \ldots, a_k)$ is a Hilbert generating system of the cone C, because if $w \in C$, $w = \sum_{i=1}^{k} \lambda_i a_i$, then

$$w - \sum_{i=1}^{k} \lfloor \lambda_i \rfloor a_i = \sum_{i=1}^{k} \{\lambda_i\} a_i \in \mathrm{par}(a_1, \ldots, a_k)$$

where $\lfloor x \rfloor$ denotes the integer part of the number x, and $\{x\}$ denotes its fractional part.
Q.E.D.

Schrijver (1981) proved the following theorem:

Theorem 1.2 *Every pointed cone has a unique Hilbert basis.*

The existence of a Hilbert basis follows from the previous theorem. The following proof of the unicity was pointed out to me by Brahim Chaourar. (I learnt from Les Trotter that Jiyong Liu proved it in a similar way.)

Proof. Suppose the rows of the $k \times n$ matrice P and the $l \times n$ matrix Q both form Hilbert-bases of one and the same pointed cone C: $P = AQ$ and $Q = BP$, where A and B are non-negative integer matrices of size $k \times l$ and $l \times k$ respectively. We can deduce $P = ABP$.

We first show that AB is the identity matrix. Denoting the j-th element of its i-th row by λ_{ij}, our matrix equation is equivalent to the equations $p_i = \sum_{j=1}^{k} \lambda_{ij} p_j$, where p_i is the i-th row of P and $\lambda_{ij} \geq 0$ is integer ($i = 1, \ldots, k$, $j = 1, \ldots, k$). For every $i = 1, \ldots, k$, $\lambda_{ii} = 1$, for say $\lambda_{11} = 0$ would contradict the fact that the p_i-s form a *minimal* Hilbert generating system (we can delete p_1); $\lambda_{11} > 1$ would contradict the *pointedness* of C. Substituting this into our equation we get $0 = \sum_{j \neq i} \lambda_{ij} p_j$ for every i, and since C is pointed, and the coefficients are non-negative, we can deduce $\lambda_{ij} = 0$ if $i \neq j$.

We conclude that A, B are non-negative integer matrices, and AB is the $k \times k$ identity matrix. Since the rows of P and Q form a *minimal* Hilbert generating system, A and B have no zero columns and rows. It follows immediately that both A and B are permutation matrices.

Q.E.D.

From now on *we shall suppose that Hilbert generating systems and Hilbert bases generate pointed cones,* except if we emphasize the countrary. A cone will also automatically mean *pointed cone*. All the examples we shall mention treat only pointed cones as well.

Theorem 1.2 immediately implies the following observation of Schrijver (1981). (This played an important role in his original proof.)

Corollary *The Hilbert basis of the cone* $C = \mathrm{cone}(a_1, \ldots, a_k)$ *is the set*

$$H = \{h \in C \cap \mathbb{Z}^n \setminus \{0\} : h \textit{ is not the sum of two non-zero integer vectors of } C\}.$$

Clearly, $H \subseteq \mathrm{par}(a_1, \ldots, a_k) \cup \{a_1, \ldots, a_k\}$.

Thus the formula in the above corollary is an equivalent definition of the *Hilbert basis of a cone C*, and it will be used as such, without any more reference to it.

Cook, Fonlupt and Schrijver (1986) have proved the following Caratheodory type theorem for Hilbert bases *:

Theorem 1.3 *Let C be a pointed cone, and let $H \subseteq \mathbb{Z}^n$ be its Hilbert basis. If* $w \in \mathrm{cone(H)} \cap \mathbb{Z}^{\mathrm{n}}$ *then w is the positive integer linear combination of at most $2n - 1$*

* Recall Caratheodory's theorem for cones: *every element of a cone can be written as the non-negative linear combination of at most n generating vectors of the cone.*, see Schrijver (1986) Corollary 7.1i.

elements of H. If H consists only of 0-1 *vectors, then this bound can be improved to* $2n-2$.

We have to put the proof here because the proof of Theorem 2.1 will refer to its details.

Proof. Let $H=\{a_1,\dots,a_k\}$, $w=\sum_{i=1}^k \lambda_i a_i$, and suppose $\sum_{i=1}^k \lambda_i$ is maximum among all possible choices. (This maximum is finite because C is pointed.) We know from linear programming that the set $\{a_i : \lambda_i > 0\}$ can be chosen to be linearly independent (a version of Caratheodory's theorem)*. We can thus suppose without loss of generality that $\lambda_i = 0$ if $i > n$, that is $w=\sum_{i=1}^n \lambda_i a_i$.

Let

$$(1.1) \qquad w_0 = w - \sum_{i=1}^n \lfloor \lambda_i \rfloor a_i = \sum_{i=1}^n \{\lambda_i\} a_i \in \mathrm{par}(a_1,\dots,a_n)$$

$w_0 \in C$, and w_0 is an integer vector, whence there exist $\alpha_i \geq 0$ integers such that $w_0 = \sum_{i=1}^k \alpha_i a_i$. Clearly,

$$(1.2) \qquad w = \sum_{i=1}^k \alpha_i a_i + \sum_{i=1}^n \lfloor \lambda_i \rfloor a_i$$

$\sum_{i=1}^k \alpha_i \leq n-1$, for if not, $\sum_{i=1}^k \alpha_i \geq n > \sum_{i=1}^k \{\lambda_i\}$, and thus the sum of the coefficients in (1.2) is greater than $\sum_{i=1}^n \lambda_i$, a contradiction.

Since the α_i-s are integers $|\{i : \alpha_i > 0\}| \leq n-1$ follows, proving that the number of positive coefficients in (1.2) is at most $2n-1$.

Q.E.D.

Cook Fonlupt and Schrijver (1986) add the remark that in 2 dimensions 2 elements are enough, and they do not have any example where n elements would not be enough in general instead of the $2n-1$ above.

Conjecture A *Let $H \subseteq \mathbb{Z}^n$ be a Hilbert basis, and $w \in \mathrm{cone(H)} \cap \mathbb{Z}^{\mathrm{n}}$. Then w is the positive integer linear combination of at most n elements of H, and these can be determined in polynomial time.*

In a lecture, Bill Cook communicated an additional fact which was very important from the point of view of the present work: in the plane, the determinant of neighbouring Hilbert basis elements is ± 1, (equivalently, they generate the lattice of all integers, or just the same lattice as H), for a proof see the end of this introduction. In sections

* In the language of linear programming: there exists an optimal *basic* solution.

2 and 3 we are going to prove generalizations of this fact, in Sections 4 and 5 we shall deduce some consequences for combinatorial problems. These results, many examples and the strong belief in the beauty of nature makes us think that the same is true in general. In other words, if the following conjecture is true, it should be due to Cook Fonlupt and Schrijver (1986), if it is not, the responsibility is the author's.

CONJECTURE B *If $H \subseteq \mathbb{Z}^n$ is a full dimensional pointed Hilbert basis, then* $\mathrm{cone}(H)$ *is covered by cones* $\mathrm{cone}(a_1, \ldots, a_n)$*, where* $\{a_1, \ldots, a_n\} \subseteq H$*, and* $\det(a_1, ..., a_n) = \pm 1$*;* $a_1, \ldots, a_n$ *such that* $\mathrm{cone}(a_1, \ldots, a_n)$ *contains a given element of* $\mathrm{cone}(H) \cap \mathbb{Z}^n$*, and* $\det(a_1, ..., a_n) = \pm 1$ *can be computed in polynomial time.*

It is easy to see that Conjecture B implies Conjecture A. For general Hilbert-bases, instead of "$\mathrm{det}(\mathrm{a}_1, ..., \mathrm{a}_\mathrm{n}) = \pm 1$" we have to write simply that "$(a_1, ..., a_n)$ is a basis of $\mathrm{lat}(\mathrm{a}_1, ..., \mathrm{a}_\mathrm{n})$."

Note that vectors $a_1, \ldots, a_n$ with $\det(\mathrm{a}_1, ..., \mathrm{a}_\mathrm{n}) = 1$ are the minimum cardinality full dimensional Hilbert bases and they are the only linearly independent Hilbert bases. For a not necessarily full dimensional set of linearly independent vectors $\{a_1, \ldots, a_k\}$ the equivalence of the following statements can be shown easily:

(i) $\{a_1, \ldots, a_k\}$ *is linearly independent and is a Hilbert basis.*

(ii) $\mathrm{par}(a_1, ..., a_k) = \{0\}$

(iii) The g.c.d. of the $k \times k$ subdeterminants of the matrix whose columns are $a_1, \ldots, a_k$ is 1. (The equivalence of (ii) with the rest relies however on some knowledge on lattices, see Schrijver (1986). Actually, (iii) will be used only for $k = n$, when it is evident.)

For simplicity, we shall often suppose that our Hilbert basis is of full rank. This is not a restriction of the generality: if the Hilbert basis is in a subspace of rank r, choose a basis of this subspace, and represent the vectors of the subspace in with the coefficient vectors of linear combinations of this basis. This gives a full dimensional representation of the same Hilbert basis in $\mathbb{R}^r$.

This argument permits to extend statements from the full dimensional case to arbitrary Hilbert bases. For example, using that full dimensional linearly independent Hilbert bases are exactly the sets of vectors with determinant ± 1, we get the following obviously equivalent version of Conjecture B, which does not need the assumption about the full rank, and does not speak about determinants:

CONJECTURE C *Let $H \subseteq \mathbb{Z}^n$ be a Hilbert-basis where $\mathrm{cone}(H)$ is pointed. If H is linearly dependent, and $w \in \mathrm{cone}(\mathrm{H}) \cap \mathbb{Z}^\mathrm{n}$, then there exists a Hilbert-basis $H' \subset H$, $(H' \neq H)$, $w \in \mathrm{cone}(\mathrm{H}')$, and H' can be computed in polynomial time.*

The reader may find it useful to study numerical examples of Hilbert bases first in 2 dimensions. Taking two linearly independent relatively prime vectors with non-± 1 determinant, clearly, not every integer vector of the pointed cone C generated by these two vectors is an integer combination of the generating vectors. You can easily find the (uniquely determined) elements of the Hilbert basis of C. The experience aquired through such examples will probably help to follow the proof below, and arguments all along the paper.

Let us finish this introduction by proving these conjectures for $n = 2$. This case is easy, but it isn't a completely banal exercise.

However, short proofs can be given in various ways. Several proofs can be extracted from more general arguments, for example Lemma 1 of Theorem 2.2 below gives a proof. The particularity of this case, exploited by the proofs is that *neighboring Hilbert basis elements have determinant* 1*, or equivalently, if we delete either of the extreme rays, the remaining vectors form a Hilbert basis again.* It is not difficult to prove that the Hilbert basis H of the cone generated by the integer vectors a_1, a_2 lies in $\mathrm{conv}(a_1, a_2, 0)$. (This fact implies immediatly Conjecture C: $H \setminus \{a_1\}$ is a Hilbert basis, for if $v \in \mathrm{conv}(H \setminus \{a_1\})$, and $v = v_1 + v_2$, $v_1, v_2 \in \mathrm{cone}(a_1, a_2)$, then clearly, $v_1, v_2 \in \mathrm{conv}(H \setminus \{a_1\})$.) Our purpose with giving a separate proof here is that some aspects of Hilbert bases might be easier to understand on this simple example. The following version, simplified down to the bare essentials, was exhibited by Péter E. Soltész:

Proof of Conjecture C for $n = 2$. If $|H| \le 2$, the statement is trivial. Let $a_1, a_2 \in H$ be the extreme rays of $\mathrm{cone}(H)$. By our assumptions a_1 and a_2 are linearly independent and $H \setminus \{a_1, a_2\} \ne \emptyset$. It is enough to prove that $H \setminus \{a_1\}$ is a Hilbert basis, for then by symmetry $H \setminus \{a_2\}$ is also a Hilbert basis, and arbitrary $w \in \mathrm{cone}(H)$ is contained in the cone generated by one of these.

One of the extreme rays of $\mathrm{cone}(H \setminus \{a_1\})$ is a_2, let the other be a_1'. Of course $a_1' \in H$. All we have to prove is that every $w \in \mathrm{par}(a_1', a_2)$ is the non-negative integer combination of vectors in $H \setminus \{a_1\}$. We shall actually prove even more. Let $w \in \mathrm{par}(a_1', a_2)$. We know that w can be written as the non-negative integer combination of vectors in H: $w = \sum_{h \in H} \alpha(h) h$, where $\alpha(h) \ge 0$ integer for all $h \in H$. We shall prove that in *every* combination of this form $\alpha(a_1) = 0$. Suppose indirectly that $\alpha(a_1) \ge 1$, and substitute every $h \in H$ by their expression as a nonnegative linear combination of a_1 and a_2: we get that

$$w = \beta_1 a_1 + \beta_2 a_2, \text{ where } \beta_1 \ge 1, \beta_2 \ge 0. \tag{1.3}$$

On the other hand $w = \lambda_1' a_1' + \lambda_2' a_2$ $(0 \le \lambda_1', \lambda_2' < 1)$, where $a_1' = \lambda_1 a_1 + \lambda_2 a_2$

($0 \le \lambda_1, \lambda_2 < 1$), whence

$$w = \lambda_1' \lambda_1 a_1 + (\lambda_1' \lambda_2 + \lambda_2') a_2. \tag{1.4}$$

In (1.3) the coefficient of a_1 is at least 1, whereas in (1.4) it is smaller than 1. This is a contradiction, because there is a unique way to express w in the basis a_1, a_2.

Q.E.D.

The reader could visualize this proof finding the clear geometric meaning of each step.

2. Improving by 1

In this section we improve only by 1 three known bounds. The proofs seem to require new methods though, and may give more general indications for attacking the conjectures A, B, C. Their proofs are strictly related to Conjectures B and C. The main support for the conjectures is just the following fact valid for the whole paper: *in all cases when Conjecture A is true, the stronger Conjectures B and C also hold; the same proofs work for them; furthermore, in most cases, the only way of proving Conjecture A is to prove Conjectures B or C.*

Theorem 2.1 *Let $H \subseteq \mathbb{Z}^n$ be the Hilbert basis of a pointed cone, and $w \in \text{cone}(H) \cap \mathbb{Z}^n$. Then w is the positive integer linear combination of at most $2n-2$ elements of H.*

The proof, in addition to the proof of Theorem 1.3, exploits the symmetry of parallelepipeds:

Proof. Let $H = \{a_1, \ldots, a_k\}$, $w = \sum_{i=1}^k \lambda_i a_i$; $\sum_{i=1}^k \lambda_i$ is maximum; $a_1, \ldots, a_n$ are linearly independent, $\{a_i : \lambda_i > 0\} = \{a_1, \ldots, a_n\}$. (If $|\{i : \lambda_i > 0\}| < n$, then the statement follows already from the proof of Theorem 1.3.) *Assume in addition that* $\text{conv}(a_1, \ldots, a_n) \cap H = \{a_1, \ldots, a_n\}$. We can assume this without loss of generality, for

$$w = \varepsilon h + \sum_{i=1}^n (\lambda_i - \varepsilon \gamma_i) a_i, \tag{2.1}$$

and if $h = \sum_{i=1}^n \gamma_i a_i$ with $\sum_{i=1}^n \gamma_i = 1$, ($0 \le \gamma_i < 1$, $i = 1, \ldots, n$), then the sum of the coefficients in such a combination remains equal to $\sum_{i=1}^n \lambda_i$. The choice $\varepsilon := \min\{\frac{\lambda_i}{\gamma_i} : i = 1, \ldots, n\} =: \frac{\lambda_j}{\gamma_j}$ makes clear that $\text{cone}(a_1, \ldots, a_{j-1}, h, a_{j+1}, \ldots, a_n)$ contains w, and combines it with the same some of coefficients*.

* This is just a "pivot" bringing h into the "basis", without changing the "objective value", because the "relative cost" of h was 0.

Let w_0 be defined by (1.1). We have now

$$\sum_{i=1}^{n}\{\lambda_i\} < n-1. \tag{2.2}$$

Indeed, suppose indirectly that $\sum_{i=1}^{n}\{\lambda_i\} \geq n-1$, *that is, where* $\gamma_i := 1-\{\lambda_i\} > 0$, *(*$i=1,\ldots,n$*)*

$$\sum_{i=1}^{n}\gamma_i \leq 1. \tag{2.3}$$

Let now

$$h := \sum_{i=1}^{n}\gamma_i a_i = a_1 + \ldots + a_n - w_0 \in \text{cone}(a_1,\ldots,a_n)\cap \mathbb{Z}^n,$$

furthermore, if $h \notin H$ substitute h in (2.1) by a non-negative integer combination of Hilbert basis elements. We must have equality in (2.3), because otherwise the sum of the coefficients in (2.1) is bigger than $\sum_{i=1}^{n}\lambda_i$ for any positive ε; $h \in H$ for the same reason. Thus $h \in \text{conv}(a_1,\ldots,a_n)\setminus\{a_1,\ldots,a_n\}$, contradicting the assumption made in the beginning of the proof, and proving (2.2).

After these remarks we proceed in exactly the same way as in the proof of Theorem 1.3. However, because of (2.2), we have now the following tighter bound in the last paragraph of the proof of Theorem 1.3: $\sum_{i=1}^{k}\alpha_i \leq n-2$, for if not, $\sum_{i=1}^{k}\alpha_i \geq n-1 > \sum_{i=1}^{n}\{\lambda_i\}$, and thus the sum of the coefficients in (1.2) is greater than $\sum_{i=1}^{n}\lambda_i$, a contradiction.

Since the α_i-s are integers $|\{i : \alpha_i > 0\}| \leq n-2$ follows, proving that the number of positive coefficients in (1.2) is at most $2n-2$.

Q.E.D.

Remark:

1.Instead of requiring $\text{conv}(a_1,\ldots,a_n)\cap H = \{a_1,\ldots,a_n\}$ in the proof, we could have assumed that $\det(a_1,\ldots,a_n)$ is minimal:

$$\det(a_1,\ldots,a_{j-1},h,a_{j+1},\ldots,a_n) = \det(a_1,\ldots,a_{j-1},\sum_{i=1}^{n}\gamma_i a_i, a_{j+1},\ldots,a_n) = \gamma_j\det(a_1,\ldots,a_n) < \det(a_1,\ldots,a_n).$$

Thus "pivoting" decreases the determinant, if we "bring" an element of the parallelepiped into the basis.

This trick, although it is more technical than the one we used in the above version of the proof, can also be used to prove other statements. For instance *it implies immediately the existence of a Hilbert generating system for which Conjecture B holds*:

by Caratheodory's theorem cone(H) is covered by cones of the type cone(H') (where $H' \subseteq H$ is linearly independent). If for each of these H' we take $h \in \mathrm{par}(H')$ and replace H' by the n cones that have h and $n-1$-elements of H' as extreme rays (we suppose H is full dimensional), we get a new covering by cones, and by the above remark the maximum determinant has decreased. Repeating this a finite number of times, we get the appropriate Hilbert generating system.

2. A third possibility, which is *better from the algorithmic point of view*: let $c_i := 1 - \varepsilon \parallel a_i \parallel$, where ε is "sufficiently small"; it is easy to see that a basis with maximal objective value with respect to this objective function satisfies $\mathrm{conv}(a_1, \dots, a_n) \cap H = \{a_1, \dots, a_n\}$. It follows that the positive linear combination with at most $2n-2$ Hilbert basis elements can be determined in polynomial time.

The following theorem will of course not contain many combinatorial examples. (It could be interesting in itself though from the viewpoint of three dimensional geometry.) However, its proof is probably the one which goes the deepest into the structure of Hilbert bases in general:

Theorem 2.2 *Conjectures A, B, and C are true for $n \leq 3$.*

To prepare the proof we state two lemmata valid in arbitrary dimension:

Lemma 1 *Let $H \subseteq \mathbb{Z}^n$ be the Hilbert basis of a pointed cone, $H = a_1, \dots, a_k$ and $w \in \mathrm{cone(H)} \cap \mathbb{Z}^{\mathrm{n}}$. Then there exist coefficients λ_i such that $w = \sum_{i=1}^k \lambda_i a_i$, and*

(i) $\sum_{i=1}^k \lambda_i$ *is maximum under this constraint.*

(ii) $\{a_i : \lambda_i > 0\}$ *is linearly independent, say* $\{a_i : \lambda_i > 0\} = \{a_1, \dots, a_s\}$, $s \leq n$.

(iii) If $h \in \mathrm{par}(\{a_1, \dots, a_s\} \setminus \{0\}$, $h = \sum_{i=1}^k \gamma_i a_i$, *then*

$$1 < \sum_{i=1}^k \gamma_i < s - 1 \leq n - 1. \tag{2.4}$$

Less formally, there exists an "optimal basis" for which (iii) holds. Note that Conjecture B for $n = 2$ follows immediately.

Proof. Let $H = \{a_1, \dots, a_k\}$, $w = \sum_{i=1}^k \lambda_i a_i$; $\sum_{i=1}^k \lambda_i$ is maximum; $\{a_i : \lambda_i > 0\} = \{a_1, \dots, a_s\}$, and this set is linearly independent (see the proof of Theorem 1.3. *Assume in addition that* $\mathrm{conv}(a_1, \dots, a_s) \cap H = \{a_1, \dots, a_s\}$ like in the proof of Theorem 2.1.

Thus (i) and (ii) hold by the above choice. Let $h \in \mathrm{par}(a_1, \dots, a_s)$, $h = \sum_{i=1}^s \gamma_i a_i$. We have to prove (2.4). Like in the proof of Theorem 2.1, (2.3) cannot hold, whence $\sum_{i=1}^s \gamma_i > 1$. Applying the same to the symmetric $\bar{h} = a_1 + \ldots + a_s - h = \sum_{i=1}^s (1-\gamma_i) a_i$ we get that $\sum_{i=1}^s 1 - \gamma_i > 1$ and (2.4) is proved.

Q.E.D.

The following Lemma is well-known from the geometry of numbers. For the sake of completeness we sketch a proof using the Hermite normal form:

Lemma 2 *Let $a_1, \ldots, a_n \in \mathbb{Z}^n$ be a basis of $\mathbb{R}^n$. Then*
$|\mathrm{par}(a_1, \ldots, a_n)| = |\det(a_1, \ldots, a_n)|$ (For a general set $a_1, \ldots, a_k$ we simply replace the determinant by the greatest common divisor of the $r \times r$ determinants where r is their rank.)

Proof. Let A be the matrix whose columns are $a_1, \ldots, a_n$. Let r_i denote the i-th row of A. Clearly, if we replace a row r_i by $r_i \pm r_j$ $(i \neq j)$, then the set of vectors $\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ for which $A\underline{\lambda}$ is integer remains the same. In particular, the number of elements in the parallelepiped defined by the new column vectors remains the same; the determinant does not change either. With such operations one can arrive to the "Hermite normal form" (see Schrijver (1986) p.45) of the rows. We can thus suppose that A is lower triangular. Let the elements in its main diagonal be $d_1, \ldots d_n$. Clearly, for $A\underline{\lambda}$ to be in $\mathrm{par}(a_1, \ldots, a_n)$ we have d_1 different choices for λ_1: $\frac{t}{d_1}$ $(t = 0, \ldots, d_1 - 1)$. Similarly, if $\lambda_1, \ldots, \lambda_{i-1}$ have already been chosen, and the i-th component of $\sum_{j=1}^{i-1} \lambda_j a_j$ is x, then the possible choices for λ_i are $\frac{\lceil x \rceil - x + t}{d_i}$ $(t = 0, \ldots, d_i - 1)$: for all possible choices of $\lambda_1, \ldots, \lambda_{i-1}$ we have d_i choices for λ_i. We conclude that $\mathrm{par}(a_1, \ldots, a_n)$ has $d_1 \ldots d_n = det(A)$ elements.

Q.E.D.

Proof of Theorem 2.2. Suppose $n = 3$, and let us prove Conjecture C.

Claim 1 *If $H \subseteq \mathbb{Z}^3$ is a Hilbert-basis, and $w \in \mathrm{cone(H)} \cap \mathbb{Z}^3$, then there exist vectors $a_1, a_2, a_3 \in H$ such that $\mathrm{par(a_1, a_2, a_3)} \setminus \{0\} \subseteq \mathrm{H}$, and $w \in \mathrm{cone(a_1, a_2, a_3)}$.*

Indeed, let $\{a_1, a_2, a_3\}$ and $\{\lambda_1, \lambda_2, \lambda_3\}$ be the basis and coefficients provided by Lemma 1 (s=3), and $h \in \mathrm{par}(a_1, a_2, a_3)$, $h = \gamma_1 a_1 + \gamma_2 a_2 + \gamma_3 a_3$. By Lemma 1 (2.4), $\gamma_1 + \gamma_2 + \gamma_3 < 2$. If $h \notin H$, then substituting h with a non-negative integer combination of H, the sum of the coefficients in (2.1) is again bigger than $\lambda_1 + \lambda_2 + \lambda_3$ contradicting Lemma 1 (i).

Claim 2 *If Claim 1 does not hold for any proper subset of H (it must hold then for H, that is $\mathrm{par}(a_1, a_2, a_3) \setminus \{0\} = H$), then it has an element $h = \gamma_1 a_1 + \gamma_2 a_2 + \gamma_3 a_3$ that satisfies the equation*

$$\Delta(\gamma_1 + \gamma_2 + \gamma_3) = \Delta + 1,$$

where $\Delta := \mathrm{det(a_1, a_2, a_3)}$.

Before proving Claim 2, let us summarize our knowledge about the parallelepiped $\mathrm{par}(a_1, a_2, a_3)$: it has $\Delta - 1$ different non-zero elements (see Lemma 2) of the form

$h = \gamma_1 a_1 + \gamma_2 a_2 + \gamma_3 a_3$, where the coefficients are rational numbers all with Δ as denominator (Cramer's rule); denoting the sum of the numerators of the coefficients by $s(h)$,

$$s(h) = \Delta(\gamma_1 + \gamma_2 + \gamma_3). \tag{2.5}$$

On the other hand, (2.4) for $n = 3$ gives $\Delta < s(h) < 2\Delta$, in other words,

(2.6) *$s(h)$ is always one of the values $\Delta + 1, \ldots, 2\Delta - 1$, that is one of $\Delta - 1$ different values.*

We shall prove that

(2.7) *for $h_1 \neq h_2 \in \mathrm{par}(a_1, a_2, a_3)$, $s(h_1) \neq s(h_2)$.*

It follows then by (2.6) that for each $i \in \{\Delta + 1, \ldots, 2\Delta - 1\}$, $s(h) = i$ is satisfied for exactly one $h \in H$, and in particular $s(h) = \Delta + 1$ for some $h \in H$. Because of (2.5) this is just the statement of Claim 2.

Let $h_1, h_2 \in \mathrm{par}(a_1, a_2, a_3)$, $s(h_1) = s(h_2) =: s$. All we have to prove, is $h_1 = h_2$.

For $h \in \mathrm{par}(a_1, a_2, a_3)$ let $\bar{h} := a_1 + a_2 + a_3 - h$. Clearly, $\bar{h} \in \mathrm{par}(a_1, a_2, a_3)$. The identity

$$h_1 + \bar{h}_2 = a_1 + a_2 + a_3$$

is obviously equivalent to $h_1 = h_2$. $s(h_1) + s(\bar{h}_2) = s + 3\Delta - s = 3\Delta$. Thus, in the combination $h_1 + \bar{h}_2 = \delta_1 a_1 + \delta_2 a_2 + \delta_3 a_3$, $\delta_1 + \delta_2 + \delta_3 = \frac{3\Delta}{\Delta} = 3$, and

$$0 < \delta_i < 2, \quad (i = 1, 2, 3). \tag{2.8}$$

Since by (2.6) for every vector in the parallelepiped, the sum of the coefficients is non-integer, the fact that $\delta_1 + \delta_2 + \delta_3$ is integer implies that δ_1, δ_2 and δ_3 are all integers, and using (2.8) we have $\delta_1 = \delta_2 = \delta_3 = 1$. Claim 2 is proved.

We show now how Conjecture C follows from the claims. If H is not of the form $\mathrm{par}(\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3) \setminus \{0\}$ then we are done by Claim 1. Thus we can suppose $H = \mathrm{par}(\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3) \setminus \{0\}$, and that the condition of Claim 2 holds. Clearly, for every $h \in \mathrm{par}(a_1, a_2, a_3)$:

$$\mathrm{par}(a_1, a_2, h) \cup \mathrm{par}(a_1, h, a_3) \cup \mathrm{par}(h, a_2, a_3) \supseteq H \setminus \{h\},$$

and at least the origin is contained in the intersection of the three parallelepipeds on the left hand side, whence:

$$\det(\mathrm{a}_1, \mathrm{a}_2, \mathrm{h}) + \det(\mathrm{a}_1, \mathrm{h}, \mathrm{a}_3) + \det(\mathrm{h}, \mathrm{a}_2, \mathrm{a}_3) - 2 \geq \det(\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3) - 1.$$

If h is now the element guaranteed by Claim 2, we have equality here (the members of the sum at the left hand side are the same as those in Claim 2, through elementary operations on determinants). Consequently we have equality in the above set-containment as well. It follows that $\mathrm{par}(a_1, a_2, h) \setminus \{0\}$, $\mathrm{par(a_1, h, a_3)} \setminus \{0\}$ and $\mathrm{par(h, a_2, a_3)} \setminus \{0\}$ partition H, and are Hilbert bases. The theorem is proved. (The statement about the complexity is clear: the solution of a linear programming problem allows to decrease the size of the problem by 2.)

Q.E.D.

Conjecture A in the following special case has been proved earlier by A. Gerards. The following proof is based on arguments similar to the other two proofs of this section, some elements of which will be useful later:

Theorem 2.3 *Conjectures A, B and C are true for Hilbert bases whose linear rank is one less than their cardinality.*

Proof. We shall prove Conjecture B for the set of vectors $H = \{a_1, \ldots, a_{n+1}\}$ of full rank, forming a Hilbert basis. Clearly, up to a scalar multiple, there exists one unique non-zero linear relation

$$\sum_{i=1}^{n+1} \alpha_i a_i = 0. \tag{2.9}$$

For later convenience we state the following Lemma in a somewhat more general form that we need it here:

Lemma : *If $H = \{a_1, \ldots, a_k\}$ is an arbitrary Hilbert-basis, and the linearly independent vectors $a_1, \ldots, a_s \in H$ do not form a Hilbert basis, then*
a. *There exists an equation of the form*

$$\sum_{i \in I} a_i = \sum_{i \notin I} \alpha_i a_i \tag{2.10}$$

where $I \subseteq \{1, \ldots, s\}$, and $\alpha_i \geq 0$ integers ($i \notin I$).
b. *There exists an equation of the form $\sum_{i \in I} \alpha_i a_i = \sum_{i \notin I} \alpha_i a_i$ where $I \subseteq \{1, \ldots, s\}$, $\alpha_i \geq 0$ integers ($i = 1, \ldots, k$), and* $\max\{\alpha_i : i = 1, \ldots, s\} < \max\{\alpha_i : i = s+1, \ldots, k\}$.

Indeed, $a_1 + \ldots + a_s = h + \bar{h}$, where $0 \neq h \in \mathrm{par}(a_1, \ldots, a_s)$. Since both h and $\bar{h}$ are in $\mathrm{cone}(H)$, they can be expressed as a non-negative integer combination of H. Substitute these expressions for h and $\bar{h}$ into the above equation. In the linear expression we have for h we are sure to have an element different from $a_1, \ldots, a_s$. After eventual simplifications because of elements that occur on both sides we get (2.10) and a. is proved.

To prove Lemma b. take simply $h \in \text{par}(a_1, \dots, a_s)$. Clearly, $h = \frac{1}{q}(p_1 a_1 + \dots + p_s a_s)$, $0 \le p_i < q$ $(i = 1, \dots, s)$. Expressing h as a non-negative integer combination of H, we get that $p_1 a_1 + \dots + p_s a_s = q \sum_{i=1}^{k} r_i a_i$, where r_i is non-negative integer, and there exists $j > s$ with $r_j \ge 1$. Thus, after simplifying because of elements that occur on both sides we get an equation with all coefficients smaller than q on the left hand side; a_j is on the right hand side, and its coefficient is at least q . The Lemma is proved.

The Lemma tells us a lot about the coefficients in (2.9). Suppose $a_1, \dots, a_s$ be independent, but not a Hilbert basis. (Otherwise we are done.) By Lemma a. (2.10) holds, and must coincide with (2.9) up to a scalar multiple. Because of the uniqueness of (2.9), Lemma b. applies to (2.9) as well: (2.9) can be supposed to be identical to (2.10) with the additional property, that there exists j with $\alpha_j \ge 2$. Furthermore,

(2.11) *if* $\{a_j : j \in J\}$, $J \subseteq \{1, \dots, n+1\}$ *is linearly independent and not a Hilbert basis, then* $J \supseteq I$.

(Because J satisfies the same assumption as $\{1, \dots, s\}$ and consequently (2.10) holds if we replace I by $I' \subseteq J$. By the uniqueness of (2.10), using $\alpha_j \ge 2$ as well, we get $I' = I$.)

Let now $w \in \text{cone}(H)$ be arbitrary. By Caratheodory's theorem, $w = \sum_{i=1}^{s} \lambda_i a_i$, $\lambda_i \ge 0$, and we can suppose that $a_1, \dots, a_s$ are those in the Lemma. Let $\lambda := \min\{\lambda_i : i \in I\}$. By (2.10) we have

$$w = \sum_{i \in I} (\lambda_i - \lambda) a_i + \sum_{i \notin I} (\lambda_i + \lambda \alpha_i) a_i \tag{2.12}$$

(define $\lambda_i = 0$ for $i > s$). Since $\lambda_i - \lambda = 0$ for some $i \in I$, in (2.12) the indices of the positive coefficients do not contain I. Thus $\{a_i : a_i$ has positive coefficient in (2.12)$\}$ is linearly independent (because (2.10) is the unique linear relation), and according to (2.11), it is a Hilbert basis.

Q.E.D.

A proof of this theorem also follows from our study of "uncrossable Hilbert bases" (Section 3), and another one from the structure of 1-dimensional Hilbert kernels (see a remark in Section 5 after Conjecture E).

3. Strong and uncrossable Hilbert-bases

An equivalent definition of Hilbert generating systems could be the following: H is a Hilbert generating system if and only if for every $w \in \text{cone(H)} \cap \text{lat(H)}$ there exists a $h \in H$ such that $w - h \in \text{cone(H)}$.

Chandrasekaran and Tamir (1984) studied a property which can be reformulated as follows: for every $w \in \text{cone(H)} \cap \text{lat(H)}$ and $h \in H$, $w - \epsilon h \in \text{cone(H)}$ with $\epsilon > 0$ implies $w - h \in \text{cone(H)}$. The origin of this property lies in Fulkerson's proof (1972) of the Pluperfect Graph Theorem. The same property permitted to Cook, Fonlupt, Schrijver (1986) to prove Conjecture A for the cliques lying on a face of the clique polytope of a perfect graph.

We first suggest a property which will permit to include further combinatorial examples, and is, on the other hand special enough: we will prove Conjectures A, B, C if this property holds. H will be called a *strong Hilbert-basis*, if for every face F of $C := \text{cone(H)}$ there exists an element $h_F \in F$ with the following property: if $w \in C \cap \mathbb{Z}^n$, and F is the minimal face of C containing w, then $w - h_F \in C$. *

h_F with this property will be called a *strong element* of F. (For basic definitions and statements about the structure of polyhedra cf. Schrijver (1986).) The main result of this section is the following theorem:

Theorem 3.1 *If $H \subseteq \mathbb{Z}^n$ is a strong Hilbert basis, then Conjecture A, B, C hold for it.*

Proof. Let $w \in C \cap \mathbb{Z}^n$, and suppose F_1 is the minimal face of C containing w, and $h_1 := h_{F_1}$. Let $\lambda_1 := \max\{\lambda : w - \lambda h_1 \in C\}$. The dimension of the minimal face F_2 cotaining $w - \lambda_1 h_1$ is less than that of F_1. Apply now the same procedure to $w - \lambda h_1 \in C$, and so on. Clearly, we arrive in this way at a series of faces $F_1, \ldots, F_s$ and linearly independent vectors $h_1, \ldots, h_s$ ($h_i = h_{F_i}$, $i = 1, \ldots, s$), $w \in \text{cone}(h_1, \ldots, h_s)$.

We prove now by induction on $\dim(F_1)$ that $h_1, \ldots, h_s$ is a Hilbert basis. If $\dim(F_1) = 1$ the statement is obvious. If $h_1, \ldots, h_s$ is not a Hilbert basis, there exists a $0 \neq h \in \text{par}(h_1, \ldots, h_s)$, $h = \sum_{i=1}^{s} \gamma_i h_i$ $(0 \leq \gamma_i < 1)$. By the induction hypothesis $h_2, \ldots, h_s$ is a Hilbert basis, whence $\gamma_1 \neq 0$. The minimal face containing h is F_1, and because of $\sum_{i=2}^{s} \gamma_i h_i \in F_2$ where $\dim(F_2) < \dim(F_1)$ we see that $\gamma_1 = \max\{\lambda : h - \lambda h_1 \in C\}$. But $0 < \gamma_1 < 1$ contradicts the property of $h_{F_1} = h_1$ in the strong Hilbert basis H.

* Using Chandrasekaran and Tamir's terminology, strong Hilbert bases are exactly those Hilbert bases H, whose elements have an order such that the lexicographically maximal linear expression of every $h \in \text{cone}(H)$ is integer. (Easy to see.) Chandrasekaran and Tamir investigated problems where the same holds for *every* order.

The claim about the complexity is an immediate consequence of the ellipsoid method, see Grötschel, Lovász, Schrijver (1987): $\max\{\lambda : h - \lambda h_1 \in C\}$ can be computed in polynomial time. Another way of applying the ellipsoid method will also be useful: maximize $\lambda_F c(h_F)$ under the constraint $h = \sum\{\lambda_F h_F : F$ face of $C\}$ $c(h_F) := \Delta^{\dim(F)}$, where Δ is the biggest determinant of a square submatrix of H. *

Q.E.D.

A second property that will imply the conjectures: uncrossability. Recall the following from the Lemma a. of Theorem 2.3: *If H is a Hilbert basis, and the linearly independent vectors $a_1, \ldots, a_s \in H$ do not form a Hilbert-basis, then their sum can also be written in another way as a non-negative integer combination of Hilbert-basis elements.* We shall say that H is *uncrossable*, if for some objective function $c : H \longrightarrow \mathbb{R}$ and for every independent subset $\{a_1, \ldots, a_s\} \subseteq H$, among the combinations

$$\sum_{h \in H} \alpha(h) h = a_1 + \ldots + a_s, \tag{3.1}$$

($\alpha(h)$ integer for every $h \in H$), there is one with

$$\sum_{h \in H} \alpha(h) c(h) > c(a_1) + \ldots + c(a_s). \tag{3.2}$$

(This is a generalization of the properties used in "uncrossing procedures" for many combinatorial problems. Eg. the square of the cardinality of a set is often used as objective function.)

CONJECTURE D *Every Hilbert basis is uncrossable, and the objective function c in the definition of uncrossability is computable in polynomial time.*

The reader can check that *in all the special cases for which we proved the conjectures, Conjecture D also holds.* Check it for instance for the example of Theorem 2.3: any function c such that the objective value of the left hand side of (2.10) is smaller than that of the right hand side will obviously do. Thus the proof of Theorem 3.2 below will provide a new proof for Theorem 2.3 . An other example: the choice of the objective function at the end of the proof of Theorem 3.1 prove that *strong Hilbert bases are uncrossable* (Proofs in this paper can be considered to exhibit an appropriate objective function to show uncrossability, and Theorem 3.2 below proves again the conjectures for every case.) Conjecture D is important from the algorithmic point of view.

Theorem 3.2 *Conjectures A, B, C hold for uncrossable Hilbert bases*

---

* It is easy to see that the c-maximum solutions are exactly the lexicographically maximal ones, if we order the variables in the decreasing order of c. In Chandrasekaran and Tamir's terminology our proof means that strong Hilbert bases are exactly those in which lexicographically maximal solutions *with respect to a specific order* are Hilbert bases.

Proof. Let H be an uncrossable Hilbert basis, $c : H \longrightarrow \mathbb{R}$ the function that ensures uncrossability, and $b \in \text{cone}(H)$ arbitrary. Let $B := \{a_1, \dots, a_s\} \subseteq H$ be the vectors which belong to a positive variable β_i in an optimal basic solution for the linear program $\sum_{h \in H} x(h)h = b, \quad x \geq 0, \quad \max \sum_{h \in H} x(h)c(h)$. (The maximum exists because of the pointedness of cone(H).)

B must be a Hilbert basis, because if it were not, then (3.1) holds, that is

$$b = \varepsilon \sum_{h \in H} \alpha(h)h + \sum_{i=1}^{s} (\beta_i - \varepsilon)a_i. \tag{3.3}$$

Because of uncrossability, (3.2) also holds. If ε is sufficiently small, (3.3) also expresses b as a nonnegative combination, and by (3.2), has bigger objective value than $\sum_{i=1}^{s} \beta_i c(a_i)$, a contradiction with the choice of B.

Q.E.D.

The above proof implies that cone(H), where H is an uncrossable Hilbert basis, has a "triangulation" with cones generated by independent Hilbert bases $B \subseteq H$. A *triangulation* of the cone C is a set of cones with linearly independent extreme rays whose union is C, and the intersection of any two of which is a smaller dimensional cone.

4. Combinatorial examples

We have now finished the study of Hilbert bases in general. In this section we sketch some applications, in the following section we make some algorithmic and other remarks. In these two sections the reader will have to be satisfied with a short summary, and sketched proofs because of the lack of place (and time). I hope to write more details in a forthcoming paper.

Hilbert basis constitute an equivalent algebraic language to study TDI systems. A system of inequalities is called *totally dual integral* (or TDI), if any inequality which is their consequence and has an integer coefficient vector, arises as their non-negative integer combination. The first, basic results about TDI systems were proved by Giles and Pulleyblank(1979), Edmonds and Giles (1984), and Schrijver (1981). The translation between TDI systems and Hilbert bases is provided by the following observation of Giles and Pulleyblank (1979) see also Schrijver (1986):

Theorem 4.1 **a**. *The system of inequalities $Ax \leq b$ (A and b are integral) is TDI if and only if for each face F of the polyhedron $\{x : Ax \leq b\}$, the rows of A which are* *active in F form a Hilbert basis.*

b. *The rows of the integer matrix A form a Hilbert basis if and only if $Ax \leq 0$ is TDI.*

A row of a is called *active* in a face (or for an objective function), if it is satisfied with equality by every vector in the face (which is the set of optimal solutions for the given objective function).

Many combinatorial applications of Hilbert bases arise from well-known TDI systems of Combinatorial Optimization, (and as we shall see below, many others arise in a different way). It is an immediate conequence of Theorem 2.1 (through Theorem 4.1) that *for n-dimensional TDI systems there always exists an integer optimal dual solution with at most $2n-2$ nonzero variables.* We list now some Hilbert bases, where we know something better than the bound $2n-2$.

I. Totally unimodular and uncrossable systems

For the Hilbert bases corresponding to many TDI systems all the conjectures we presented hold trivially. Two big classes of them whill let us avoid listing them one by one: integer linear programs with totally unimodular constraint matrices; problems where for example uncrossing procedures lead to a "triangular basic" dual solution. An example to the latter: matroid polyhedra.

II. Perfect Graphs and Matchings

The following Lemma extracts the essence of Fulkerson's proof (1972) of the Pluperfect Graph Theorem:

Lemma *Let $P := \{x : Ax \leq b\}$ be full dimensional (for simplicity), and let $ax \leq \beta$ be an inequality in the system $Ax \leq b$. Suppose furthermore, that $ax \geq \beta - 1$ is valid for every $x \in P$. If for an objective function c $ax \leq \beta$ is active, then there exists a dual solution to the linear program $Ax \leq b$, $\max cx$ where the dual variable corresponding to the row a is at least* 1. .

Theorem 4.2 *The "active rows" (for an arbitrary objective function) of clique polyhedra of perfect graphs and matching polyhedra form a strong Hilbert basis.*

Proof. (Sketch) All the inequalities describing the clique polyhedron of perfect graphs are of the form $ax \leq 1$, and $ax \geq 0$ is valid for them. The Lemma states that such inequalities are "strong" elements of the cone of active rows: it follows that the active rows form a strong Hilbert basis.

For matching polyhedra, inequalities of the type $x_i \geq 0$ and $x(\delta(v)) \leq 1$ satisfy the conditions of the Lemma. So whenever such an inequality is active, it is a strong element. If there are no such inequalities, then it can be shown that one of the "odd set inequalities" is strong. Q.E.D.

For the case of perfect graphs, the above proof is just an equivalent way of presenting Cook, Fonlupt and Schrijver's (1986) proof of Conjecture A.

Corollary *Conjectures A, B, C, D hold for the Hilbert bases in the above theorem*

III. MATROID BASES

It follows from the matroid partition theorem that the (incidence vectors of the) bases of an arbitrary matroid form a Hilbert basis (whose lattice is not $\mathbb{Z}^n$). A. Frank (1984) has proved that *bases of uniform matroids* (the set of all k-tuples of an arbitrary set) form a Hilbert basis for which Conjecture A holds. É Tardos (1984) gave a simple proof that reduced the problem in one step to a smaller dimensional one, actually with a natural choice of a "strong element". This leads to the following:

Theorem 4.3 *The set of all k-tuples of an arbitrary set forms a strong Hilbert basis, where every element is strong (in every face containing it).*

Corollary *Conjectures A, B, C, D hold for the set of all k-tuples of an arbitrary set.*

This is the only result I know about the conjectures on matroid bases.

IV. ARBORESCENCES

It follows from Edmonds' (1967) rooted arborescence theorem that arborescences (as edge-sets) constitute a Hilbert basis.

From Pevsner's (198?) algorithmic considerations one can extract the following theorem:

Theorem 4.4 *: Let G be a directed graph with a root $r \in V(G)$, and w be a vector in the cone C generated by the arborescences of G rooted in r.*
a. *If $w - a \notin C$ for some arborescence a, then there exists an arborescence b such that $w - b \in C$ and the dimension of the minimal face containing $w - b$ is less than that of w.*
b. *There exist two arborescences a and b rooted in r and a non-negative integer α such that $w' := w - (\alpha a + b) \in C$, and the dimension of the minimal face containing w' is less than that of w.*

It is easy to prove Theorem 4.4a using Lovász's proof of Edmonds' theorem, and b is an easy corollary of a.

Theorem 4.4b implies a better bound than the bounds known in general: using two vectors, the dimension can be decreased by one; if Conjecture A is proved for graphs where the linear rank of the arborescences is c, we get that for every w there exists a solution with at most $2(r - c) + c = 2r - c$ positive coefficients, where r is the rank of the arborescences; we get immediately the bound $2r - 3$ (because of Theorem 2.2), that can probably be considerably improved with an analysis of small graphs. We would find it more interesting however, and we hope too, that the strong property exhibited in Theorem 4.4 brings us nearer to the conjectures in this case.

The Conjectures for the "polar" problem (minimum weight rooted arborescence maximum cut packing) are trivial, belong to I.

V. ODD CUTS

The following example was suggested by Les Trotter (1987): *For every objective function, the active rows of T-join polyhedra form a Hilbert basis, if the non-negativity constraints are written in the form $2x_i \geq 0$.* This follows from Seymour's integer minimax theorem (1981a) about minimum T-joins and maximum T-cut packings in graphs with "bipartite" weightings. The lattice generated by the odd cuts and the doubles of the unit vectors is clearly *the set of bipartite weightings*, and not the set of all integer vectors: this case does not fit into the usual definition of TDI-ness, which supposes that the considered lattice is the set of all integers.

Some special cases such as planar graphs are strong Hilbert bases, and thus the conjectures hold for them.

VI. MULTICOMMODITY FLOWS

It is a basic question about graphs whether *the existence of a fractional multicommodity flow implies the existence of an integer one* for arbitrary demands and capacities, see Seymour (1981b), Karzanov (1987), Sebő (1990). Such graphs are called *routing*.

Given a graph G let the *multicommodity cone* of G be the cone generated by the vectors $v_{C,f}$ and $2e_i$, where $C \subseteq E(G)$ is a cycle, $f \in C$, and $v_{C,f}(e)$ is equal to -1 if $e = f$, to 1 if $e \in C \setminus \{f\}$, and 0 otherwise; the e_i-s are the unit vectors on the edges. The extreme rays defined here will be denoted by MH(G). The above mentioned question, and the papers refered to investigate the problem of characterizing when MH(G) or some subcone of it is a Hilbert basis.

It is easy to see that a graph is *routing* if and only if MH(G) is a Hilbert basis. Routing graphs include Seymour's (1981b) class of "cycling" graphs. More generally, all this can be defined in terms of binary matroids. The characterization of routing matroids is open.

We do not require that the generated lattice is the set of all integer vectors: if we require that, it follows from Seymour (1981b) that MH(G) is a Hilbert basis if and only if G is series-parallel. MH(G) generates the lattice of Eulerian weightings. The MH(G) of certain graphs (or matroids), among them that of planar graphs, turns out to be a strong Hilbert basis. Consequently Conjectures A, B, C, D hold for these cases.

The list of the examples seems to be unbounded, actually every TDI system gives an example. On the other hand the list of the solved cases of the conjectures is for the moment poor.

5. Other remarks

I. Testing membership

We first prove that *it is coNP-complete to decide whether a given vector is in the Hilbert basis of a cone given by defining inequalities*, a fact proved first by É. Tardos (1987) with a reduction to the maximum stable set problem of a graph.

Theorem 5.1 *Given two vectors $a, h \in \mathbb{Z}^n$, it is coNP-complete to decide whether h is in the Hilbert basis of the cone $\{x : ax = 0, x \geq 0\}$*

Proof. Let $a_1, \ldots, a_{n-2}$ be an instance of PARTITION (see Garey-Johnson (1979), and $a_{n-1} := a_n := -1/2(a_1 + \ldots + a_{n-2})$, $a := (a_1, \ldots, a_n)$; let h be the n-dimensional all 1 vector. Clearly, $C := \{x : ax = 0, x \geq 0\}$ is a pointed cone, $h \in C$, and h is in the Hilbert basis of C if and only if the answer to the given instance of PARTITION is no.

Q.E.D.

II. Testing TDI-ness, and integral dual solutions

Next we show that *Conjecture B contains Cook, Lovász and Schrijver's result (1984) on testing TDI-ness in fix dimension.* We do not have to use Lenstra's integer programming algorithm (in the test. The key-observation is the following:

Theorem 5.2 *Suppose Conjecture B is true, and $H \subseteq \mathbb{Z}^n$ is full dimensional (and generates a pointed cone). Let $H_1, \ldots, H_p \subseteq H$ be the list of those n-element independent subsets of H whose determinant is* 1. *Then H is a Hilbert basis if and only if* $\mathrm{cone}(H) = \bigcup_{i=1}^{p} \mathrm{cone}(H_i)$.

Proof. The only if part is just Conjecture B. The if part is trivial, since by the constraint $w \in \mathrm{cone}(H)$ is in some of the $\mathrm{cone}(H_i)$-s, and those are Hilbert bases.

Q.E.D.

Let H be like in the theorem, and let n be fixed. (It is easy to see from Theorem 4.1 that in order to check TDI-ness it is enough to test whether a given set of vectors is a Hilbert basis; the assumptions of Theorem 5.2 on H do not restrict the generality, see Schrijver (1986)). Since n is fixed, the facets of $C_0 := \mathrm{cone}(H)$ can be determined in polynomial time. Let now $H_1, \ldots, H_p \subseteq H$ be the list of those n-element independent subsets of H whose determinant is 1. Since n is fixed, this list, and the facets of $C_i :=$ cone(H_i) $(i = 1, \ldots, p)$ can be determined in polynomial time. Let $b_1, \ldots, b_q \in$ cone(H) be the list of all vectors that generate a one-dimensional cone (half line) which is the intersection of n linearly independent facets from among the facets of $C_0, \ldots, C_p$. Since n is fixed, q is still a polynomial of $|H|$, and can be computed in polynomial time.

Now clearly, cone$(H) \neq \bigcup_{i=1}^p$ cone(H_i) *if and only if there exists a linearly independent subset* $\{c_1, \ldots, c_n\} \subseteq \{b_1, \ldots, b_q\}$ *such that no inner (non-facet) point of* cone$(c_1, \ldots, c_n)$ *lies in* $\bigcup_{i=1}^p$ cone(H_i). Thus we "only" have to test for all $\{c_1, \ldots, c_n\} \subseteq \{b_1, \ldots, b_q\}$ whether $c_1 + \ldots + c_n$ (this is an inner point) is contained in at least one of the cones C_i $(i = 1, \ldots, p)$. If yes, then we can conclude cone$(H) = \bigcup_{i=1}^p$ cone(H_i), and H is a Hilbert basis by Theorem 5.3. If $c_1 + \ldots + c_n$ is contained in none of the C_i $(i = 1, \ldots, p)$ for some $\{c_1, \ldots, c_n\} \subseteq \{b_1, \ldots, b_q\}$, then clearly cone$(H) \neq \bigcup_{i=1}^p$ cone(H_i), and according to Theorem 5.2 H is not a Hilbert basis. Q.E.D.

For TDI systems, we are also interested in finding an integer dual solution, and if the conjectures hold, a dual solution whose positive variables belong to linearly independent constraints forming a Hilbert basis. If our TDI system is given explicitly by a system of linear inequalities and Conjecture D holds, even the latter task can be solved easily with the help of Theorem 4.1.

For linear programming problems given by a separation oracle (for the definition see Grötschel Lovász, Schrijver (1987)) we must suppose that the minimal system describing the corresponding polyhedron is TDI, and that for a cone given by a separation oracle, and whose extreme rays constitute a Hilbert basis, $c(h)$ in Conjecture D can be determined in polynomial time. (For most of the TDI systems for which the Conjectures are known, these conditions are satisfied.) With the proof technique used by Grötschel, Lovász and Schrijver (1987) (6.5.14), our problem is reduced to writing a vector w of a cone given by a separation oracle as a non-negative c-maximum linear combination of the extreme rays. (By the proof of Theorem 3.2 every independent subset of a c-optimal solution is a Hilbert basis.)

Compared to (6.5.14) here we have the additional task of optimizing the function c. However, given a separation oracle for the cone $\{yA : y \geq 0\}$, a separation oracle for the polyhedron $\{yA = w : y \geq 0\}$ can be determined in polynomial time, whence the function c can be optimized in polynomial time. (We used the equivalence of optimization and separation several times, see Grötschel, Lovász and Schrijver' book.)

III. Structure

We prove here some weakenings and of Conjecture B, and state a reformulation.

Note first that there exists at least one basis with the property claimed in Conjecture B (Gerards and Sebő (1987)), implying "local strong unimodularity" for totally dual integral systems, that is the existence of active rows whose determinant is 1.

Next we note that *every cone has a finite Hilbert generating system for which Conjectures A, B, C are true*, see Remark 1 after Theorem 2.1, but the number of redundant elements in this construction might be huge. Of course, if we start with a covering of cone(H) by the cones of Conjecture B, then there there is no redundant element. It would be interesting to prove the existence of a Hilbert generating system for which the conjectures hold and does not have many redundant elements.

par(H) is a Hilbert generating system which has many redundant elements, but the conjectures are still interesting and open for it. Liu and Trotter (1990) have put the interesting question of giving a proof at least if "1" is replaced by some bigger, but not very big number in the definition of "par", and they have some results in this direction.

Finally, we sketch our results on Hilbert kernels: they are based on the recognition that for any property of Hilbert bases, only the linear dependencies between Hilbert-basis elements play a role. A linear subspace $S \subseteq \mathbb{R}^k$ is called *Hilbert kernel*, if there exists an $n \times k$ matrix H whose columns constitute a Hilbert basis (of a pointed cone), and $S := \{x : Hx = 0\}$. A great advantage of Hilbert kernels is that they neglect non-essential properties of Hilbert bases, for example their definition does not depend on whether we suppose $\mathrm{lat}(H) = \mathbb{Z}^n$ or not. We present the following characterization of Hilbert kernels without proof, noting that the proof is not difficult.

Theorem 5.3 *Let $S \subseteq \mathbb{R}^k$ be a linear subspace. The following statements are equivalent:*

(i) S *is a Hilbert kernel*

(ii) For every $x \in S$ *there exists* $y \in S$ *so that* $y \equiv x$ *and* $y < 1$

(iii) For every $x \in S$ *there exists* $y \in S$*,* y *integer and* $y \leq \lceil x \rceil$

(iv) $H(S) \cup \{e_1, \ldots, e_k\}$ *is a Hilbert basis, where* $H(S)$ *is a Hilbert basis of* S*, and* e_i *(*$i = 1, \ldots, k$*) is the vector whose* i*-th coordinate is* 1*, and the others are* 0*.*

Let us reformulate Conjecture B in terms of Hilbert kernels (Conjectures A, C, D can be reformulated similarly). The proof of the equivalence is easy.

CONJECTURE E *If* S *is a Hilbert-kernel, then for every* $x \in \mathbb{R}^n, x \geq 0$ *there exists* $y \in S$*, such that* $z \in S$*,* z_i *integer for values* i *with* $x_i = y_i$*, implies* $z \in \mathbb{Z}^n$*.*

The coefficients of the linear equations satisfied by an n-dimensional Hilbert basis of cardinality k form a $k-n$ dimensional subspace of $\mathbb{R}^k$. It is convenient to represent Hilbert-kernels with a basis of $S \cap \mathbb{Z}^k$, $k-n$ linearly independent k-dimensional vectors. The case $k = n+1$ corresponds to 1-dimensional Hilbert-kernels. From Theorem 5.3 it is easy to see that 1-dimensional Hilbert kernels are exactly the lines generated by vectors all positive components of which are 1. Conjecture E is an immidiate consequence, providing a new proof of Theorem 2.3.

At this point, the relation of the different conjectures may appear chaotic. Let us finally summarize the easy implications by the following scheme:

CONJECTURE D $\Longrightarrow$ CONJECTURE B $\Longleftrightarrow$ CONJECTURE C $\Longleftrightarrow$ CONJECTURE E $\Longrightarrow$ CONJECTURE A.

We do not know anything about the other implications.

Acknowledgment: I owe a lot to Bill Cook, Bert Gerards and Éva Tardos: most of the above results were first written down in letters to them, and would not have been proved without their permanent interest and encouragement. Many thanks are due to Brahim Chaourar and Kazuo Murota for various suggestions.

References:

Chandrasekaran, Tamir (1984), On the integrality of an extreme solution to pluperfect graph and balanced systems, Operations Research Letters, **3**,4, 215–218 137–145

W. Cook, J. Fonlupt, A. Schrijver (1986), An integer analogue of Carathéodory's theorem, Journal of Combinatorial theory (B) **40** (1986) 63–70

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

W. Cunningham (1987) Testing membership in matroid polyhedra, J. Combinatorial Theory B 36, 161-188

J. Edmonds (1967) Edge-disjoint branchings, in: Combinatorial algorithms, Academic Press, New York

J. Edmonds (1970) Submodular functions, matroids and certain polyhedra, in: Combinatorial Structures and their Applications, Gordon and Breach, New York, pp 69–87

J. Edmonds R. Giles (1984) Total dual integrality of linear inequality systems, in: Progress in Combinatorial Optimization, Jubilee Conference, W.R. Pulleyblank ed., Academic Press, Toronto

A. Frank (1984) private communication

A. Frank (1987) Graph connectivity and network flows, to appear in the Handbook of Combinatorics, R. Graham, M. Grötschel, L. Lovász eds.

D.R. Fulkerson, Antiblocking Polyhedra, J. of Comb. Theory,**12** (B), pp 50–71

M.R. Garey, and D.S. Johnson (1979), Computers and Intractability: a Guide to the Theory of NP-completeness, Freeman, San Francisco

A. Gerards, A. Sebő (1987), Total dual integrality implies local strong unimodularity, Mathematical Programming, **38**, 69–73

Giles, Pulleyblank (1979), Total dual integrality and integer polyhedra, Linear algebra and its applications, 25, 191–196

Grötschel, Lovász, Schrijver (1987) The ellipsoid method and combinatorial optimization, Springer, Heidelberg

A.V. Karzanov (1987)Half integral five-terminus flows, Discrete Applied Mathematics, 18, 263–278

J. Liu and L. Trotter (1990) private communication

L. Lovász (1976) On two minimax theorems in graph, J. Comb Theory, B, **2**, 96–103

L. Lovász (1987) Matching Theory, Lecture at the seventh Hungarian Colloquium on Combinatorics, Finite and Infinite sets, Eger, July 5-10

A. Hoffmann and R. Oppenheim (1978), Local unimodularity in the matching polytope, Annals of Discrete Mathematics, 2, 201–209

P. A. Pevsner (198?) Effektivnyi algoritm upakovki vetvlenii vo vzveshennom grafe (in Russian)

A. Schrijver (1981), On total dual integrality, Linear algebra and its applications, **38**, 27–32

A. Schrijver (1986), Theory of linear an integer programming, Wiley, Chichester

A. Sebő (1990) The cographic multiflow problem: an epilogue, to appear in DIMACS (W. Cook and P. Seymour eds.)

P.D. Seymour (1981a), On odd cuts and plane multicommodity flows, Proc. London Math. Soc. **(3) 42**, 1981, 178–192

P.D. Seymour (1981b), Matroids and multicommodity flows, European Journal of Combinatorics **(2)** , 257–290

É. Tardos (1984), (1987) private communication

L. Trotter (1987) private communication