Note

Testing Hilbert bases in fixed co-dimension

FRIEDRICH EISENBRAND[1], ANDRÁS SEBŐ[2], AND GENNADY SHMONIN[1]

[1] *EPFL SB MA, Station 8, CH-1015, Lausanne, Switzerland*
[2] *Laboratoire G-SCOP , 46, Avenue Félix Viallet , 38000 Grenoble , France*

Abstract

We show that the problem of testing whether a given set of $n+k$ rational vectors in $\mathbb{R}^n$ forms a Hilbert basis can be solved in polynomial time if k is fixed.

1 Introduction

Given rational vectors $a_1,\dots,a_m \in \mathbb{R}^n$, the *cone* generated by $a_1,\dots,a_m$ is the set of all non-negative linear combinations of these vectors:

$$\operatorname{cone}(a_1,\dots,a_m) := \left\{\sum_{i=1}^{m} \lambda_i a_i : \lambda_i \geqslant 0,\ i=1,\dots,m\right\}.$$

It is the Farkas–Minkowski–Weyl theorem (see, e.g., Schrijver [9]) that each cone generated by finitely many vectors is *polyhedral*, i.e., can be represented in the form

$$\operatorname{cone}(a_1,\dots,a_m) = \left\{x : Bx \leqslant 0\right\} \tag{1}$$

for some rational matrix B; and conversely, each cone of the form (1) is generated by finitely many rational vectors. The cone is called *pointed* if it does not contain any linear subspace besides the 0-space, or equivalently, if there exists a half-space whose intersection with the cone is $\{0\}$.

The set of all non-negative integral linear combinations of $a_1,\dots,a_m$,

$$\operatorname{int.cone}(a_1,\dots,a_m) := \left\{\sum_{i=1}^{m} \lambda_i a_i : \lambda_i \geqslant 0,\ \lambda_i \in \mathbb{Z},\ i=1,\dots,m\right\},$$

is called the *integer cone* generated by $a_1,\dots,a_m$. The *lattice* generated by $a_1,\dots,a_m$ is the set of all integral linear combinations of $a_1,\dots,a_m$:

$$\operatorname{lat}(a_1,\dots,a_m) := \left\{\sum_{i=1}^{m} \lambda_i a_i : \lambda_i \in \mathbb{Z},\ i=1,\dots,m\right\}.$$

A *basis* of the lattice $\mathrm{lat}(a_1,\ldots,a_m)$ is the set of linearly independent vectors that generates $\mathrm{lat}(a_1,\ldots,a_m)$. Since $a_1,\ldots,a_m$ are rational vectors, $\mathrm{lat}(a_1,\ldots,a_m)$ has a basis; see, e.g., Schrijver [9].

Let $a_1,\ldots,a_m \in \mathbb{Q}^n$ be linearly independent vectors, hence they form a basis of the lattice $\mathrm{lat}(a_1,\ldots,a_m)$. The set

$$\mathrm{par}(a_1,\ldots,a_m) := \left\{\sum_{i=1}^{m} \lambda_i a_i : 0 \leqslant \lambda_i < 1,\, i = 1,\ldots,m\right\}$$

is called the *fundamental parallelepiped* of vectors $a_1,\ldots,a_m$. It is well-known that the volume of the fundamental parallelepiped is an invariant of the lattice, i.e., does not depend on the choice of a basis. This volume is called the *determinant* of the lattice.

A finite set of vectors $a_1,\ldots,a_m$ forms a *Hilbert basis* if

$$\mathrm{int.cone}(a_1,\ldots,a_m) = \mathrm{cone}(a_1,\ldots,a_m) \cap \mathrm{lat}(a_1,\ldots,a_m),$$

i.e., each vector of the lattice $\mathrm{lat}(a_1,\ldots,a_m)$ in the cone $\mathrm{cone}(a_1,\ldots,a_m)$ can be expressed as a non-negative integral combination of $a_1,\ldots,a_m$.

The concept of Hilbert bases was introduced by Giles and Pulleyblank [5] in the context of totally dual integral systems. They proved that each cone has a finite Hilbert basis. Schrijver [8] showed that each pointed cone has a *unique* minimal Hilbert basis.

Cook *et al.* [2] proved the following analogue of Carathéodory's theorem for Hilbert bases: if $H = \{a_1,\ldots,a_m\}$ is a Hilbert basis and the cone $\mathrm{cone}(H)$ is pointed, then each vector $b \in \mathrm{int.cone}(a_1,\ldots,a_m)$ can be expressed as a non-negative integral linear combination of at most $2n-1$ vectors vectors from H. Later, Sebő [10] improved this bound to $2n-2$. On the other hand, Bruns *et al.* [1] showed that the bound n (as for traditional Carathéodory's theorem) is not valid in general.

In this note we consider the problem of recognizing Hilbert bases: Given rational vectors $a_1,\ldots,a_m \in \mathbb{Q}^n$, do they form a Hilbert basis? The problem belongs to coNP, but it is open whether or not it belongs to NP.[1] If the rank of $a_1,\ldots,a_m$ is fixed, the problem can be solved in polynomial time; see Cook *et al.* [3].

We consider the case when the difference $m-n$ is fixed. The approach is based on studying so-called "Hilbert kernels", briefly introduced by Sebő [10]. This is mostly based on the observation that for any property of a Hilbert basis, only the linear dependencies between its elements are important.

2 Hilbert kernels

A linear subspace $L \subseteq \mathbb{R}^m$ is called a *Hilbert kernel* if there is a matrix

$$H = [\,h_1,\ldots,h_m\,] \in \mathbb{Q}^{n\times m}$$

[1] Recently, J. Pap showed that the problem is coNP-complete.

such that

$$L = \{x : Hx = 0\} \tag{2}$$

and the columns of H, i.e., vectors $h_1, \ldots, h_m$ form a Hilbert basis. We remark that we do not specify the dimension n of vectors $h_1, \ldots, h_m$ here—it can be chosen arbitrarily. It is easy to see that if

$$H' = [\, h'_1, \ldots, h'_m \,] \in \mathbb{Q}^{n' \times m}$$

is *any* other matrix satisfying (2), then the columns of H' also form a Hilbert basis.

Theorem 2.1. *A linear subspace $L \subseteq \mathbb{R}^m$ is a Hilbert kernel if and only if for each vector $x \in L$, there is an integral vector $y \in L$ such that $y \leqslant \lceil x \rceil$.*

Proof. Suppose that L is a Hilbert kernel and let $H \in \mathbb{Q}^{n \times m}$ be a matrix satisfying (2). Then the columns of H form a Hilbert basis and $Hx = 0$, which is equivalent to

$$H\lceil x \rceil = H(\lceil x \rceil - x). \tag{3}$$

The vector

$$b := H(\lceil x \rceil - x)$$

clearly belongs to the cone generated by the columns of H. By (3), it is also in the lattice $\mathrm{lat}(H)$, and therefore, since H is a Hilbert basis, b must belong to the integer cone generated by H; that is,

$$b = H(\lceil x \rceil - x) = Hz$$

for some non-negative integral vector $z \in \mathbb{Z}^m$. It follows that $y = \lceil x \rceil - z$ belongs to L and satisfies $y \leqslant \lceil x \rceil$.

For the converse, let $b \in \mathrm{cone}(H) \cap \mathrm{lat}(H)$, where H is a matrix satisfying (2). Equivalently, we have

$$b = Hx = Hy$$

for some non-negative vector $x \in \mathbb{R}^m$ and some integral vector $y \in \mathbb{Z}^m$. Then $y - x \in L$, and therefore, there is an integral $z \in L$ such that

$$z \leqslant \lceil y - x \rceil = y - \lfloor x \rfloor.$$

Therefore,

$$b = Hy = H(y - z), \quad y - z \geqslant \lfloor x \rfloor \geqslant 0,$$

that is, b belongs to the integer cone generated by H. $\square$

Thus, in order to check whether the columns of a matrix H form a Hilbert bases, we can consider the linear subspace $L = \{x : Hx = 0\}$ and check the following statement:

$$\forall x \in L \quad \exists y \in L \cap \mathbb{Z}^m : \quad y \leqslant \lceil x \rceil,$$

or equivalently,

$$\forall x \in L \quad \exists y \in L \cap \mathbb{Z}^m : \quad y < x + \mathbf{1}, \tag{4}$$

where $\mathbf{1}$ denotes the all-one vector.

3 Testing Hilbert bases

The question (4) is closely related to parametric integer programming. A typical parametric integer programming problem can be stated as follows: Given a polyhedron $Q \subseteq \mathbb{R}^m$ and a rational matrix $A \in \mathbb{Q}^{m\times n}$, find a vector b such that the system $Ax \leqslant b$ has no integral solution.

Kannan [6] established an algorithm that solves parametric integer programming in case when n and m are fixed. The main techniques used in the proof were actually developed by Kannan [7]. Eisenbrand and Shmonin [4] improved that algorithm to run in polynomial time for variable m (while n is still to be fixed).

Let us consider the question (4) in more detail, under the assumption that the dimension of L, $k = m - \operatorname{rank}(H)$, is fixed. We can efficiently find a basis $a_1, \dots, a_k$ of the lattice $L \cap \mathbb{Z}^m$; see [11] and [12]. Now, (4) is equivalent to

$$\forall \lambda \in \mathbb{R}^k \quad \exists \mu \in \mathbb{Z}^n : \quad \sum_{i=1}^{k} \mu_i a_i < \sum_{i=1}^{k} \lambda_i a_i + \mathbf{1}.$$

The number of integer variables here is fixed, and therefore, the problem can be solved by exploiting an algorithm for parametric integer programming. Thus, we have proved the following theorem.

Theorem 3.1. *Let k be a constant. There is a polynomial algorithm that, provided $n + k$ rational vectors of dimension n, checks if they form a Hilbert basis.*

References

[1] W. Bruns, J. S. Gubeladze, M. Henk, A. Martin, and R. Weismantel. A counterexample to an integer analogue of Carathéodory's theorem. *Journal für die reine und angewandte Mathematik*, 510:179–185, May 1999.

[2] W. J. Cook, J. Fonlupt, and A. Schrijver. An integer analogue of Carathéodory's theorem. *Journal of Combinatorial Theory, Series B*, 40(1):63–70, Feb. 1986.

[3] W. J. Cook, L. Lovász, and A. Schrijver. A polynomial-time test for total dual integrality in fixed dimension. In B. H. Korte and K. Ritter, editors, *Mathematical programming at Oberwolfach II*, volume 22 of *Mathematical Programming Study*. North-Holland, Amsterdam, 1984.

[4] F. Eisenbrand and G. Shmonin. Parametric integer programming in fixed dimension, 2007. To appear in *Mathematics of Operations Research*.

[5] F. R. Giles and W. R. Pulleyblank. Total dual integrality and integer polyhedra. *Linear Algebra and its Applications*, 25:191–196, June 1979.

[6] R. Kannan. Test sets for integer programs, ∀∃ sentences. In W. J. Cook and P. D. Seymour, editors, *Polyhedral Combinatorics*, volume 1 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 39–47. American Mathematical Society, Providence, RI, 1990.

[7] R. Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, June 1992.

[8] A. Schrijver. On total dual integrality. *Linear Algebra and its Applications*, 38:27–32, June 1981.

[9] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley, Chichester, 1986. A Wiley-Interscience publication.

[10] A. Sebő. Hilbert bases, Carathéodory's theorem and combinatorial optimization. In R. Kannan and W. R. Pulleyblank, editors, *Proceedings of the 1st Integer Programming and Combinatorial Optimization Conference, Waterloo, Ontario, Canada, May 28–30, 1990*, pages 431–455, Waterloo, Ontario, 1990. University of Waterloo Press.

[11] J. von zur Gathen and M. Sieveking. Weitere zum Erfüllungsproblem polynomial äquivalente kombinatorische Aufgaben. In E. P. Specker and V. Strassen, editors, *Komplexität von Entscheidungsproblemen: Ein Seminar*, volume 43 of *Lecture Notes in Computer Science*, pages 49–71, Berlin, 1976. Springer.

[12] A. A. Votyakov and M. A. Frumkin. An algorithm for finding the general integer solution of a system of linear equations. In A. A. Fridman, editor, *Issledovaniya po diskretnoi optimizatsii*, pages 128–140, Moscow, 1976. Izdatelstvo "Nauka".