On the Complexity of Recognizing the Hilbert Basis of a Linear Diophantine System ⋆

Arnaud Durand [a,1], Miki Hermann [b,2], and Laurent Juban [b,3]

[a] *Department of Computer Science, Université Paris 12, 94010 Créteil, France.*

[b] *LORIA (CNRS and Université Henri Poincaré Nancy 1), BP 239, 54506 Vandœuvre-lès-Nancy, France.*

Abstract

The problem of computing the Hilbert basis of a homogeneous linear Diophantine system over nonnegative integers is often considered in automated deduction and integer programming. In automated deduction, the Hilbert basis of a corresponding system serves to compute the minimal complete set of associative-commutative unifiers, whereas in integer programming the Hilbert bases are tightly connected to integer polyhedra and to the notion of total dual integrality. In this paper, we sharpen the previously known result that the problem, asking whether a given solution belongs to the Hilbert basis of a given system, is coNP-complete. We show that the problem has a pseudopolynomial algorithm if the number of equations in the system is fixed, but it is coNP-complete in the strong sense if the given system is unbounded. This result is important in the scope of automated deduction, where the input is given in unary and therefore the previously known coNP-completeness result was unusable. Moreover, we show that, from the complexity standpoint, it is not important to know the underlying homogeneous linear Diophantine system when we ask whether a given set of vectors constitutes a Hilbert basis.

Key words: Computational complexity, homogeneous linear Diophantine system, Hilbert basis, coNP-completeness, completeness in the strong sense.

⋆ A preliminary version of this paper appeared in *Proceedings 24th International Symposium on Mathematical Foundations of Computer Science (MFCS'99), Szklarska Poręba (Poland)*, M. Kutyłowski, L. Pacholski, and T. Wierzbicki, editors, volume 1672 of *Lecture Notes in Computer Science*, pages 92–102. Springer-Verlag, September 1999. Part of this work was done while the first author was a lecturer (ATER) at IUT A of the Université Nancy 2, France.

[1] e-mail: durand@univ-paris12.fr

[2] Corresponding author. e-mail: hermann@loria.fr

[3] e-mail: juban@loria.fr

1 Introduction and Summary of Results

The Hilbert basis of a homogeneous system of linear Diophantine equations over the nonnegative integers is the set of all non-zero vectors that are *minimal* solutions with respect to the pointwise ordering. This set forms a basis of the space of solutions of the system, that is, every solution can be written as a nonnegative linear combination of vectors from the Hilbert basis, and no vector of the Hilbert basis can be expressed as a positive linear combination of other vectors. Moreover, the Hilbert basis is always finite and unique. The concept of a Hilbert basis was studied as early as the second half of the 19th century by Gordan [Gor73] and Hilbert [Hil90]. Since that time, it has received considerable attention in linear algebra and integer programming.

Computing the Hilbert basis of a homogeneous system of linear Diophantine equations over nonnegative integers has turned out to be one of the key problems in automated deduction. Its importance in this area emerged through the work of Stickel [Sti81], who designed the first algorithm for unification in the presence of associative-commutative (AC) function symbols. Stickel showed that the minimal complete set of unifiers of a simultaneous elementary AC-unification problem can be obtained from the Hilbert basis of an associated homogeneous system of linear Diophantine equations over nonnegative integers. In integer programming, Hilbert bases are strongly related to total dual integrality. Universal test sets of integer programs can be constructed from Hilbert bases. Hilbert bases play also an important rôle in various fields of mathematics, like combinatorial convexity, toric varieties, and in polynomial rings and ideals (see [Sch86] for an excellent overview).

Finding the Hilbert basis is a hard problem, since its presence allows us to solve the corresponding integer programming problem easily. Recall that integer programming is NP-complete. The complexity of counting the cardinality of the Hilbert basis was studied by Hermann, Juban, and Kolaitis in [HJK99]. They determined the Hilbert basis cardinality counting problem to be in the counting class #NP by testing whether a candidate for a solution belongs to the witness set with a coNP-algorithm. Once the membership in a counting class is determined, we may ask whether the membership of the Hilbert basis cardinality problem cannot be showed for a lower class. An insight to this question is given by the complexity analysis of the problem whether a solution s of a homogeneous linear Diophantine system S over nonnegative integers belongs to the Hilbert basis of S. This problem was already considered by Sebő [Seb90], and by Henk and Weismantel [HW96], where they show that the problem is coNP-complete. However, the coNP-completeness proof is done in both cases by a reduction from a pseudopolynomial algorithm. This is a problem when the coefficients are given in unary notation. Indeed, when the Hilbert basis is computed for associative-commutative unification, the co-

efficients are written in unary notation since the underlying AC-unification problem in automated deduction is always given in unary. In this paper, we properly analyze the complexity of recognizing minimal solutions of homogeneous linear Diophantine systems S over nonnegative integers when their coefficients are written in unary notation. We also analyze the case when the number of equations in a system S is bounded.

There are two subsequent natural questions for Hilbert basis recognition that we analyze in this paper. The first problem, given a system S and a set of solutions C of S, asks whether C forms the Hilbert basis of S. The complexity of this problem was left as an open question in [HW96]. The second problem is just a generalization of the previous one. Given a set of integral vectors C, it asks whether C constitutes the Hilbert basis for an unknown system. This problem was proved to be in coNP by Edmonds and Giles [EG82], but it is unknown whether it is coNP-complete (see Schrijver [Sch86] for an overview and references). In this paper, we show that these two problems are polynomially equivalent.

2 Basic Notions and Definitions

We assume that the reader is familiar with some basics of computational complexity and integer programming. Additional material on these topics can be found in the monographs [Pap94,Sch86].

A homogeneous linear Diophantine system over nonnegative integers is a system of equations $S\colon Ax = 0$, where $A = (a_i^j)_k^n$ is a $k \times n$ integer matrix and $x = (x_1, \ldots, x_n)$ is a vector of variables over nonnegative integers. We say that a solution s of S is *nontrivial* if it is different from the all-zero solution $(0, \ldots, 0)$. We say that a solution $s = (s_1, \ldots, s_n)$ of S is *smaller* than a solution $s' = (s'_1, \ldots, s'_n)$, and write $s < s'$, if $s \neq s'$ and, for all $i = 1, \ldots, n$, the relation $s_i \leq s'_i$ holds. The relation $<$ is called the *pointwise ordering* on solutions. A solution s is *minimal* if it is nontrivial and there is no smaller nontrivial solution s'', i.e., $s'' < s$ is false for every nontrivial solution s'' of S.

The *Hilbert basis* $H(S)$ of the system S is the set of all minimal solutions of S. This set is indeed a *basis* for the space of nontrivial solutions of S, since no minimal solution can be expressed as a positive linear combination of the other minimal solutions, whereas every nontrivial solution can be expressed as a positive linear combination of minimal solutions. The Hilbert basis $H(S)$ is finite and it is the unique basis of the space of nontrivial solutions of S.

In this paper, we are concerned with the computational complexity of deciding whether a given solution belongs to the Hilbert basis $H(S)$. To prove lower

bounds of the considered problems, we need NP-complete problems from which we perform a polynomial-time reduction. We will use the following two NP-complete problems (see [GJ79]).

PARTITION
Input: Finite set A of positive integers $a \in \mathbb{Z}^+$.
Question: Is there a subset $A' \subseteq A$ such that $\sum_{a \in A'} a = \sum_{a \in A - A'} a$?

Note that PARTITION remains NP-complete even if the elements in A are ordered as $a_1 > a_2 > \cdots > a_{2n}$ and A' is required to contain exactly one of each pair of consecutive elements a_{2i-1}, a_{2i}, for each $i = 1, \ldots, n$.

However, PARTITION can be solved by a pseudopolynomial algorithm. This means that PARTITION can be solved in polynomial time if the values in A are given in unary notation. We need an NP-complete problem in the strong sense if we want to prove completeness results even if the input of our problems is given in unary. The following problem is NP-complete in the strong sense.

3-PARTITION
Input: Set $A = \{a_1, \ldots, a_{3m}\}$ of $3m$ positive integer elements $a_i \in \mathbb{Z}^+$ and a bound $B \in \mathbb{Z}^+$, such that $B/4 < a_i < B/2$ and $a_1 + \cdots + a_{3m} = mB$.
Question: Can A be partitioned into m disjoint sets A_1, A_2, ..., A_m such that $\sum_{a \in A_i} a = B$ for each $i = 1, \ldots, m$?

In the sequel, we consider the following decision problems concerning minimal solutions of a homogeneous linear Diophantine system. The first problem checks whether a solution of a given system S belongs to the Hilbert basis $H(S)$. This problem is related to the problem of counting the cardinality of the Hilbert basis of a given homogeneous linear Diophantine system over nonnegative integers.

MINIMAL SOLUTION
Input: Homogeneous linear Diophantine system $S\colon Ax = 0$ over nonnegative integers and an integral vector s.
Question: Is s a minimal solution of the system S?

We denote by MINIMAL SOLUTION(k) the instance of the decision problem with a fixed number k of equations in the system S.

The second problem checks whether a given set of solutions C equals the Hilbert basis $H(S)$ of a given system S. This problem is essentially the same as the Hilbert basis problem (HBP) formulated in [HW96], whose complexity was left open.

HILBERT BASIS CHECKING
Input: Homogeneous linear Diophantine system $S\colon Ax = 0$ over nonnegative integers and a set of integral vectors C.
Question: Is C the Hilbert basis of S?

The third problem checks whether a given set of integral vectors C constitutes the Hilbert basis of an unknown system. This problem is known to be in coNP [EG82], but its exact complexity is unknown.

HILBERT BASIS RECOGNITION
Input: Set of integral vectors C.
Question: Is C the Hilbert basis of some homogeneous linear Diophantine system?

We must make clear what we mean by the *size* of the input in the above decision problems. This involves the question whether the coefficients of the system $S\colon Ax = 0$, in the solution s, and in the set of solutions C are all written in unary or binary notation. Note that equational unification problems in automated deduction are given in unary notation, i.e., each monomial ax counts for a occurrences of the variable x, since the inputs in automated deduction are considered to be terms over the alphabet of variables and function symbols. Since our decision problems are derived from similar problems in elementary AC-unification, it is quite natural to assume that the coefficients of the linear Diophantine systems are written in unary. However, in integer programming, coefficients of linear systems are usually written in binary. For this reason, we consider in the sequel both variants of the mentioned Hilbert basis recognition problems. The *size* of the system $Ax = 0$ is kna in unary notation and $kn \log a$ in binary notation, where a is the maximum absolute value of the coefficients in the $k \times n$ matrix A. An upper bound for a problem given in binary holds also for the same problem written in unary. Similarly, a lower bound for a problem given in unary holds also for the same problem written in binary.

3 Recognizing Vectors of the Hilbert Basis

In this section, we investigate the complexity of recognizing elements of the Hilbert basis. This problem was already considered by Sebő [Seb90] and by Henk and Weismantel [HW96]. Both mention the following results, for which we give a new simpler proof.

Theorem 1 MINIMAL SOLUTION(1) *in binary is* coNP*-complete.*

PROOF. Membership in coNP is clear. We guess a vector s' pointwise smaller than the given vector s and verify that it is *not* a solution of S.

For coNP-hardness, we construct a polynomial reduction from the complement of PARTITION. Recall that PARTITION remains NP-complete even if the elements in A are ordered as $a_1 > a_2 > \cdots > a_{2n}$ and A' is required to contain exactly one of each pair of consecutive elements a_{2i-1}, a_{2i}, for each $i = 1, \ldots, n$. The PARTITION problem with the additional special condition is expressed in arithmetic form by the equation

$$\begin{aligned} & x_1 a_1 + (1 - x_1)a_2 + \cdots + x_n a_{2n-1} + (1 - x_n)a_{2n} \\ = \; & (1 - x_1)a_1 + x_1 a_2 + \cdots + (1 - x_n)a_{2n-1} + x_n a_{2n}. \end{aligned}$$

Consider the case when each variable x_i is instantiated by the values $\{0, 1\}$. Setting $x_i = 1$ has the effect to put a_{2i-1} into A' and a_{2i} into $A - A'$.

Note that each variable x_i has four occurrences. The two on the left-hand side in the expression $x_i a_{2i-1} + (1 - x_i)a_{2i}$ and the two on the right in the expression $(1 - x_i)a_{2i-1} + x_i a_{2i}$. After regrouping variables and factoring the previous expressions, we obtain the summand

$$2x_i(a_{2i-1} - a_{2i}) - (a_{2i-1} - a_{2i})$$

for each i. Summing up these expressions for $i = 1, \ldots, n$ and multiplying the right-hand side by a new variable y gives the equation E:

$$2\sum_{i=1}^{n} x_i(a_{2i-1} - a_{2i}) \;=\; y\sum_{i=1}^{n}(a_{2i-1} - a_{2i}).$$

This equation has always the solution $y = 2$ and $x_i = 1$ for each i. We claim that $s = \{y = 2, x_i = 1 \mid i = 1, \ldots, n\}$ is *minimal* for E if and only if the corresponding instance of PARTITION has no nontrivial solution. Indeed, if PARTITION has a nontrivial solution, then there are two possibilities for each i. Either $a_{2i-1} \in A'$ and $a_{2i} \in A - A'$, then we set $x_i = 1$. Otherwise, $a_{2i-1} \in A - A'$ and $a_{2i} \in A'$, then we set $x_i = 0$. This assignment to the variables x_i, together with setting $y = 1$, constitutes a solution s' of the equation E that is smaller than s. Conversely, each nontrivial solution s', smaller than s, must have $y = 1$ and $x_i \in \{0, 1\}$. The assignment of the values $\{0, 1\}$ to the variables x_i indicates the distribution of the values between A' and $A - A'$. If $x_i = 1$ then $a_{2i-1} \in A'$ and $a_{2i} \in A - A'$. Otherwise, if $x_i = 0$ then $a_{2i-1} \in A - A'$ and $a_{2i} \in A'$ for each $i = 1, \ldots, n$. $\square$

A natural question is to ask what happens when the previous problem is written in unary notation. If the problem remained coNP-complete also in the unary notation, this would mean that we used a problem not strong enough to prove the lower bound. On the other hand, the considered problem can be really pseudopolynomial. We can enlarge this question to any fixed number of equations, asking whether the decision problem MINIMAL SOLUTION(k) given in unary can be solved in polynomial time for any fixed k.

Theorem 2 MINIMAL SOLUTION(k) *in unary notation can be solved in polynomial time for any fixed k.*

PROOF. Let $S\colon Ax = 0$ be the considered system and s the nonnegative integral vector. We check first in polynomial time whether s is a solution of the system S. Afterwards, we move the monomials with negative coefficients in S to the other side, forming an equivalent system $S'\colon A'x = A''x$, where A' and A'' are integral matrices with nonnegative coefficients. Instantiate the variables x in S' by the solution s and compute the vector of values $b = (b_1, \ldots, b_k) = A's = A''s$. Let $c = (c_1, \ldots, c_k)$ be a vector of nonnegative integers, different from the all-zero vector $(0, \ldots, 0)$ and pointwise smaller than the vector b. The solution s is *not minimal* for S if and only if there exists a vector c, smaller than b, such that the system of equations $\{A'x = c\} \cup \{A''x = c\}$ has a solution satisfying the relation $0 \leq x_i \leq s_i$ for each $i = 1, \ldots, n$. Let $s^* = \max\{s_1, \ldots, s_n\}$ be the maximum coefficient in the vector s. There are $(b_1+1)\cdots(b_k+1)-1 = \mathcal{O}((nas^*)^k)$ possibilities to choose the vector c, where a is the maximum absolute value of the coefficients of the matrix A. Since $(nas^*)^k$ is polynomial in the size of the input, we have at most a polynomial number of systems to solve. A nonnegative solution of the system $\{A'x = c\} \cup \{A''x = c\}$ subject to the constraints $0 \leq x_i \leq s_i$, can be found in polynomial time, following the result of Papadimitriou in [Pap81]. Hence, the whole problem can be solved in polynomial time for a fixed k. □

The situation changes radically if there is no bound on the number of equations in the system $S\colon Ax = 0$ with the coefficients of A written in unary. The following theorem shows that we cross the tractability boundary in this case.

Theorem 3 MINIMAL SOLUTION *is* coNP*-complete in the strong sense.*

PROOF. Membership in coNP is proved the same way as in Theorem 1. Guess a vector s' pointwise smaller than the given vector s and verify that it is *not* a solution of S.

For the lower bound, we exhibit a reduction from the complement of 3-PARTITION, a strongly coNP-complete problem. We will form a homogeneous

linear Diophantine system S composed of four parts S_1, S_2, S_3, and S_4. The first part S_1 is

$$\begin{aligned} a_1 x_1^1 + a_2 x_2^1 + \cdots + a_{3m} x_{3m}^1 &= By \\ &\vdots \\ a_1 x_1^m + a_2 x_2^m + \cdots + a_{3m} x_{3m}^m &= By \end{aligned}$$

The j-th line of this system corresponds to one set A_j, where setting $x_i^j = 1$ corresponds to $a_i \in A_j$. The second part S_2 is

$$\begin{aligned} x_1^1 + x_2^1 + \cdots + x_{3m}^1 &= 3y \\ &\vdots \\ x_1^m + x_2^m + \cdots + x_{3m}^m &= 3y \end{aligned}$$

This part assures that each A_i contains three elements when $y = 1$. We will force the assignment $y = 1$ later. The third part S_3 is

$$\begin{aligned} x_1^1 + x_1^2 + \cdots + x_1^m &= y \\ &\vdots \\ x_{3m}^1 + x_{3m}^2 + \cdots + x_{3m}^m &= y \end{aligned}$$

The i-th line of this part forces the element a_i to be in only one set A_j.

The idea is now to add sufficiently many variables and homogeneous equations in the fourth part to force y to have only the solutions 0, 1, $m-1$, m, or greater than m. Naturally, the solution of the whole system for $y = 1$ must be pointwise smaller than the solution for $y = m$. The fourth part S_4 consists only of the single equation

$$z_1 + (m-1)z_2 = y.$$

Hence, we get the solutions of S for $y = 0, 1, m-1, m$, and maybe greater, but we do not need to consider those with $y > m$.

The solution with $y = 0$ is the trivial all-zero solution of S. The solution with $y = m$, $z_1 = 1$, $z_2 = 1$, and $x_i^j = 1$ for each i and j is always a solution of S. We claim that the instance of 3-PARTITION has a solution if and only if there exists a solution with $y = 1$, $z_1 = 1$, and $z_2 = 0$, and $x_i^j \in \{0, 1\}$. In this case, $x_i^j = 1$ indicates that the element a_j is in the set A_i, and $x_i^j = 0$ otherwise. However, the two solutions, one for $y = 1$, the other for $y = m$, indicate that there must be always a third solution for $y = m - 1$ that is complementary

to the solution for $y = 1$. The solution with $y = m - 1$ has the values $z_1 = 0$, $z_2 = 1$, and $x_i^j \in \{0, 1\}$. In this case, $x_i^j = 0$ indicates that the element a_j is in the set A_i, and $x_i^j = 1$ otherwise.

Set $S = S_1 \cup S_2 \cup S_3 \cup S_4$ and take for vector s the solution

$$s \;=\; \{y = m, z_1 = 1, z_2 = 1, x_i^j = 1 \mid i = 1, \ldots, 3m; j = 1, \ldots, m\}.$$

There exists a pointwise smaller nontrivial solution of the system S than the solution s if and only if the corresponding instance of the 3-PARTITION has a solution. In other words, the vector s is a minimal solution of the system S if and only if the corresponding instance of 3-PARTITION has no solution. This proves that testing for minimality of a solution of a homogeneous linear Diophantine system is coNP-complete in the strong sense. □

Remark 4 *The complexity of the considered problems* MINIMAL SOLUTION(1) *in binary,* MINIMAL SOLUTION(k) *in unary for fixed* k*, and* MINIMAL SOLUTION *remains the same even if the given vector* s *is known to be a solution of the system* S*.*

4 Checking the Hilbert Basis

The results of the previous section naturally extend to problems where we check whether a set of vectors C is a subset of the Hilbert basis $H(S)$ of a given system S. In this section, we investigate the question whether the set of vectors C equals the Hilbert basis $H(S)$ for both cases when the system S is known as well as when S is unknown. The complexity of the first problem was left open by Henk and Weismantel in [HW96].

Proposition 5 HILBERT BASIS CHECKING *belongs to* coNP*.*

PROOF. Let $S\colon Ax = 0$ be the homogeneous linear Diophantine system over nonnegative integers and C the set of vectors. First, we check in polynomial time whether each vector in C is a solution of S. If $s = (s_1, \ldots, s_n)$ is a minimal solution of S, then each coordinate s_i satisfies the inequality $s_i < n(ka)^{2k+1}$, where a is the maximum absolute value of the coefficients in A. This result was proved independently by several authors, among them Papadimitriou [Pap81] and Lambert [Lam87]. Now, membership in coNP is easy to show. Guess a vector $s = (s_1, \ldots, s_n)$ within the bounds $s_i < n(ka)^{2k+1}$ for each i and not greater or equal to any vector $c \in C$, and verify that s is *not* a solution of S. □

The problem HILBERT BASIS RECOGNITION was studied by Edmonds and Giles in [EG82], where they showed that the problem is in coNP. We will show that this problem is polynomially equivalent to HILBERT BASIS CHECKING.

Let us introduce the concept of the *canonical form* of an integral matrix, to be able to compare homogeneous linear Diophantine systems over nonnegative integers. Each integral matrix A can be seen as a set of integral vectors represented by the rows a_i.

Definition 6 *The* ***canonical form*** $A^\perp$ *of an integral matrix* A *is the smallest* $k \times n$ *integral matrix, with respect to the number of rows* k*, such that the sets of nonnegative integral solutions* $\{x \in \mathbb{Z}_0^+ \mid Ax = 0\}$ *and* $\{x \in \mathbb{Z}_0^+ \mid A^\perp x = 0\}$ *are equal, and each row* a_i *of* $A^\perp$ *has the following properties:*

(1) $a_i^j = 0$ *for* $j = 1, \ldots, i-1$*, i.e., the coefficients below the main diagonal are equal to 0;*
(2) $a_i^i > 0$*, i.e., the main diagonal coefficients are positive;*
(3) $a_i^j = 0$ *for* $j = i+1, \ldots, k$*, i.e., the coefficients above the main diagonal are equal to 0;*
(4) $\gcd(a_i^1, \ldots, a_i^n) = 1$*, i.e., the greatest common divisor of the coefficients of* a_i *is equal to 1;*
(5) either there exists a negative coefficient $a_i^j < 0$ *or all coefficients* a_i^j *are equal to 0, for some* $j \in \{k+1, \ldots, n\}$.

Hence, the canonical matrix $A^\perp$ has the form $(U_k \; A^\perp_{n-k})$, where U_k is a positive integral $k \times k$ matrix, such that $u_i^i > 0$ for $i = 1, \ldots, k$ and $u_i^j = 0$ for $i \neq j$. More precisely, the matrix $A^\perp$ has the following form

$$A^\perp = \left(\begin{array}{cccccc|ccccc} + & 0 & 0 & 0 & \cdots & 0 & * & * & * & \cdots & * \\ 0 & + & 0 & 0 & \cdots & 0 & * & * & * & \cdots & * \\ \vdots & \ddots & \ddots & \ddots & \cdots & 0 & \vdots & \vdots & \vdots & & * \\ \vdots & & \ddots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & * \\ \vdots & & & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & * \\ 0 & \cdots & \cdots & \cdots & 0 & + & * & * & * & \cdots & * \end{array}\right)$$

where $+$ corresponds to a positive coefficient and $*$ means an arbitrary coefficient. The canonical form $A^\perp$ resembles to the Smith normal form of an integral matrix A. It can be constructed by the following algorithm.

Algorithm $\mathcal{A}$

Input: Integral matrix A.
Output: Canonical form $A^{\perp}$ of A.
Method: Perform the following rules, with the precedence

$$\textbf{Combine} \succ \textbf{Zero} \succ \textbf{Negative} \succ \textbf{Gcd} \succ \textbf{Row} \succ \textbf{Column} \succ \textbf{Below} \succ \textbf{Above} \succ \textbf{Separate}$$

on a given integral matrix A, while one of the conditions is satisfied.

Combine: If there exists a row a_i in A that can be written as a linear combination with rational coefficients of the other rows in A, then remove the row a_i from A.

Zero: Remove each all-zero row $a_i = (0, \ldots, 0)$ from A.

Negative: If there exists a row a_i in A and a positive integer m, such that $a_i^1 = \cdots = a_i^{m-1} = 0$ and $a_i^m < 0$, then replace the row a_i in A by the new row $a_i' = -a_i$. This means that we multiply the row a_i by the coefficient -1.

Gcd: If there exists a row a_i in A, such that $\gcd(a_i^1, \ldots, a_i^n) > 1$, then replace the row a_i in A by the new row b_i, where we set $b_i^j = a_i^j / \gcd(a_i^1, \ldots, a_i^n)$. This rule forces the greatest common divisor of a row to be equal to 1.

Row: If there exists two rows a_i and a_j in A, where $i < j$, and two positive integers m_i, m_j, such that $m_i > m_j$, $a_i^{m_i} \neq 0$, $a_j^{m_j} \neq 0$, $a_i^l = 0$ for all $l = 1, \ldots, m_i - 1$, and $a_j^p = 0$ for all $p = 1, \ldots, m_j - 1$, then permute the rows a_i and a_j in A.

Column: If there exists a row a_i where $a_i^j = 0$ for each $j = 1, \ldots, i$, then permute the column a^i with another column a^m, such that $a_i^m \neq 0$ and $m > i$.

Below: If there exist two rows a_i and a_j in A, where $i < j$, and a positive integer m, such that $a_i^m \neq 0$, $a_j^m \neq 0$, and $a_i^l = 0$ for all $l = 1, \ldots, m - 1$, then replace the row a_j in A by the new row $a_j' = a_i^m a_j - a_j^m a_i$. This rule forces the coefficients below the main diagonal of A to be equal to 0.

Above: If there exists two rows a_i and a_j in A, where $i < j$, and a positive integer m, such that $a_i^m \neq 0$, $a_j^m \neq 0$, and $a_j^l = 0$ for all $l = 1, \ldots, m - 1$, then replace the row a_i in A by the new row $a_i' = a_j^m a_i - a_i^m a_j$. This rule forces the coefficients above the main diagonal of A to be equal to 0.

Separate: If there exists a row a_i with the coefficients $a_i^j \geq 0$ for each $j = 1, \ldots, n$, then add for each positive coefficient $a_i^j > 0$ the row $\varepsilon^j = (\varepsilon_1^j, \ldots, \varepsilon_n^j)$ to A, where $\varepsilon_i^j = 1$ if $i = j$ and $\varepsilon_i^j = 0$ otherwise. This transformation corresponds to the idea that a row a_i with nonnegative coefficients forces the variables x_j in the system $Ax = 0$ to be assigned the value $x_j = 0$ if the coefficient a_i^j is positive, since we consider systems over nonnegative integers.

End of algorithm

Algorithm $\mathcal{A}$ deletes redundancies in an integral matrix. It is clear that the systems $S\colon Ax = 0$ and $S'\colon A'x = 0$ over nonnegative integers have the same

set of solutions if A' can be constructed from A by a successive application of the rules from the algorithm $\mathcal{A}$. Unrestricted application of the rules from Algorithm $\mathcal{A}$ may result in exponentially big intermediate coefficients of the constructed matrix, even if the resulting canonical form $A^{\perp}$ is polynomial. To avoid this problem, we must apply the rules **Above**, **Below**, and **Row**, **Column** in the same way as it was proposed by Kannan and Bachem in [KB79]. This method consist of computing the normal form $A_i^{\perp}$ of the first i rows and columns before treating the $(i+1)$-th row and column of the matrix A. Under these circumstances, the Algorithm $\mathcal{A}$ runs in polynomial time and the intermediate coefficients are of polynomial size.

Lemma 7 *The algorithm $\mathcal{A}$ always terminates and computes in polynomial time for each integral matrix A the unique canonical matrix $A^{\perp}$.*

PROOF. This proof is similar to the termination proof within polynomial bounds for the coefficients for computing of the Smith normal form of an integral matrix, presented by Kannan and Bachem in [KB79].

Suppose that the matrix A contains only a single row. Then it is easy to transform this matrix to the canonical form $A^{\perp}$. We apply the rules **Zero**, **Negative**, **Gcd**, and **Column**. The rules **Row**, **Below**, and **Above** do not need to be applied. Afterwards, if all coefficients of the produced row are positive, we apply the **Separate** rule , followed by the rules **Row** and **Column** to obtain the required canonical form. Hence, we can compute the canonical form of a matrix formed by a single row in polynomial time.

To prove that the algorithm $\mathcal{A}$ is polynomial, we need to show that when we add a new row to a canonical matrix, we can compute the canonical form of the enlarged matrix in polynomial time. This coincides with the basic idea of the algorithm to compute the canonical form of the first i rows before considering the $(i+1)$-st row.

Let A' be a matrix with i rows in canonical form. For adding the $(i+1)$-st row, we will proceed the same way as it was proposed by Kannan and Bachem in [KB79]. We can ignore the application of certain rules, like **Gcd**, since they do not introduce a possibility of exponential explosion, and focus more on the crucial rules, namely **Below** and **Above**. The enlarged matrix A'' to be

transformed to the canonical form has the following form:

$$
\begin{array}{ccccccccccccc}
+ & 0 & 0 & 0 & \cdots & 0 & * & * & * & \cdots & * \\
0 & + & 0 & 0 & \cdots & 0 & * & * & * & \cdots & * \\
\vdots & \ddots & \ddots & \ddots & \cdots & 0 & \vdots & \vdots & \vdots & & * \\
\vdots & & \ddots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & * \\
\vdots & & & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & * \\
0 & \cdots & \cdots & \cdots & & 0 & + & * & * & \cdots & * \\
* & * & * & * & \cdots & * & * & * & * & \cdots & *
\end{array}
$$

After the application of the **Below** rule to the first i rows of the matrix with the row $(i+1)$, we obtain the following matrix:

$$
\begin{array}{ccccccccccccc}
+ & 0 & 0 & 0 & \cdots & 0 & * & * & * & \cdots & * \\
0 & + & 0 & 0 & \cdots & 0 & * & * & * & \cdots & * \\
\vdots & \ddots & \ddots & \ddots & \cdots & 0 & \vdots & \vdots & \vdots & & * \\
\vdots & & \ddots & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & * \\
\vdots & & & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & * \\
0 & \cdots & \cdots & \cdots & & 0 & + & * & * & \cdots & * \\
0 & 0 & 0 & 0 & \cdots & 0 & * & * & * & \cdots & *
\end{array}
$$

This transformation can be done in polynomial time. Afterwards, we apply the **Above** rule to get in the $(i+1)$-st column all coefficients equal to zero except in the last row. If the coefficient a_{i+1}^{i+1} is equal to zero, we apply the **Column** rule before the application of **Above**. If however there is no non-zero coefficient among a_{i+1}^{i+1}, ..., a_{i+1}^{n}, then the last row contains only zeros and can be therefore discarded by the **Zero** rule.

Now, the application of the **Above** rule between the rows a_{i+1} and a_j for each $j = 1, \ldots, i$, we get a matrix in the following form:

$$\begin{array}{cccccccccccc}
+ & 0 & 0 & 0 & \cdots & 0 & 0 & * & * & \cdots & * \\
0 & + & 0 & 0 & \cdots & 0 & 0 & * & * & \cdots & * \\
\vdots & \ddots & \ddots & \ddots & \cdots & 0 & 0 & \vdots & \vdots & & * \\
\vdots & & \ddots & \ddots & \ddots & 0 & 0 & \vdots & \vdots & & * \\
\vdots & & & \ddots & \ddots & 0 & 0 & \vdots & \vdots & & * \\
0 & \cdots & \cdots & \cdots & \cdots & 0 & + & 0 & * & \cdots & * \\
0 & 0 & 0 & 0 & \cdots & 0 & * & * & * & \cdots & *
\end{array}$$

This matrix can be easily transformed in the required canonical form by an application of the rules **Column** and **Negative**, if necessary.

The **Row** rule must be used when we apply the **Separate** rule on a row that contains only nonnegative coefficients. The number of added rows by a successive application of the **Separate** rule is necessarily polynomial, since each application of this rule adds at most n new rows, whereas it cannot be applied more than k times on a $k \times n$ matrix A.

The intermediate coefficients are never exponentially bigger than the maximum absolute value of the coefficients in A, since we follow exactly the approach of Kannan and Bachem [KB79], and therefore their proof is applicable on our case. The uniqueness of the canonical form $A^{\perp}$ follows from the uniqueness of the Smith normal form and the fact that the **Separate** rule decomposes a row in a deterministic way. $\square$

Definition 8 *Two integral matrices A and B are **equivalent**, if their canonical forms $A^{\perp}$ and $B^{\perp}$ are equal. In the same spirit, two systems $S\colon Ax = 0$ and $S'\colon Bx = 0$ are **equivalent** if their matrices A and B are equivalent and they have a nontrivial solution, i.e., their Hilbert bases are nonempty.*

The following proposition shows that there is a one-to-one correspondence between equivalent systems and nonempty Hilbert bases.

Proposition 9 *Let $S\colon Ax = 0$ and $S'\colon Bx = 0$ be two homogeneous linear Diophantine systems over nonnegative integers with nonempty Hilbert bases. The systems S and S' are equivalent if and only if they have the same Hilbert basis, i.e., $H(S) = H(S')$.*

PROOF. The only-if direction is clear. Two equivalent systems S and S' have the same set of solutions and, consecutively, also the same Hilbert basis.

For the if direction, assume that the systems S and S' are *not* equivalent, but both have the same nonempty Hilbert basis

$$H(S) \;=\; H(S') \;=\; \{h_1, \ldots, h_q\}.$$

Hence, the canonical matrices $A^{\perp}$ and $B^{\perp}$ are *not* equal. Therefore there must be a row b in B that cannot be written as a linear combination of the rows from $A^{\perp}$. Let $a_1, \ldots, a_m$ be the rows of the canonical matrix $A^{\perp}$. Note that the integral vectors a_i are linearly independent. From the Fundamental Theorem of Linear Inequalities (see Schrijver [Sch86], pages 85-86) follows, that there exists an integral vector $\alpha = (\alpha_1, \ldots, \alpha_n)$ that satisfies the system $A^{\perp}x = 0$, such that $b\alpha < 0$ holds. We will show that the vector α can be assumed to have only nonnegative coefficients.

Suppose that there exists a negative coefficient $\alpha_i < 0$ in α. Then we can construct a new vector

$$\alpha' \;=\; \alpha + \lambda_1 h_1 + \cdots + \lambda_q h_q$$

by adding to α a linear combination of the Hilbert basis vectors $H(S) = \{h_1, \ldots, h_q\}$ with nonnegative integer coefficients $\lambda_j \in \mathbb{Z}_0^+$ for each $j = 1, \ldots, q$, such that we get a positive coefficient $\alpha'_i > 0$. Recall that the Hilbert basis contains only nonnegative integral vectors. Indeed, each coefficient α'_i in α' can be made positive, since the condition $\alpha'_i = \alpha_i < 0$ implies that each nonnegative linear combination of the Hilbert basis is equal to 0 in the i-th coordinate. This can happen if and only if $h^i_j = 0$ holds for each vector h_j in the Hilbert basis $H(S)$.

The condition $h^i_j = 0$ for each j implies that the system $A^{\perp}x = 0$ contains the row $x_i = 0$. Without loss of generality, we assume that $h^1_1 = \cdots = h^1_q = 0$, i.e., that the first coefficient of the vectors h_i from the Hilbert basis $H(S)$ is equal to 0, otherwise we permute the coordinates. The first row of the matrix $A^{\perp}$ is equal to

$$a_1 \;=\; (a^1_1, 0, \ldots, 0, a^{k+1}_1, \ldots, a^n_1).$$

Since the first coordinate of the vectors h_i is equal to 0, the vector

$$a' \;=\; (0, \ldots, 0, a^{k+1}_1, \ldots, a^n_1)$$

has the property that $a'h_i = 0$ for each $h_i \in H(S)$. From the Fundamental Theorem of Linear Inequalities follows that a' is a nonnegative linear combination of the linearly independent rows $a_1, \ldots, a_k$ of the matrix $A^{\perp}$. Indeed, the set of vectors $\{a_1, \ldots, a_k, a'\}$ cannot be linearly independent, since each vector β, that satisfies the system $A^{\perp}x = 0$, can be produced as a linear combination of the vectors $H(S)$, and this implies $\beta a' = 0$. The rows $a_2, \ldots, a_k$ cannot participate in the nonnegative linear combination to produce the vector a', since the coefficients $a_i^i \neq 0$ at the main diagonal of $A^{\perp}$ are different from 0 for each $i = 2, \ldots, k$. Hence, there exists a positive coefficient λ, such that $\lambda a_1 = a'$. This is true either if $\lambda a_1^1 = 0$ or if a' is the all-zero vector $(0, \ldots, 0)$. The first case is impossible since $a_1^1 \neq 0$. The second case implies

$$a_1^{k+1} = \cdots = a_1^n = 0.$$

Therefore the first row of $A^{\perp}$ is equal to $a_1 = (a_1^1, 0, \ldots, 0)$. The coefficient a_1^1 must be equal to 1, since the greatest common divisor of the coefficients of the row a_1 is equal to 1. This implies that the first row of the system $A^{\perp}x = 0$ is equal to $x_1 = 0$.

Since the vector α satisfies the system $A^{\perp}x = 0$, the coordinate α_i must be equal to 0, but this contradicts the initial condition $\alpha_i < 0$. The inequation $b\alpha' < 0$ is satisfied by the constructed vector α', too, since the equality $\lambda_j b h_j = 0$ for each $j = 1, \ldots, q$ follows from the fact that $\{h_1, \ldots, h_q\}$ is also the Hilbert basis of the system S'.

Hence, there exists a *nonnegative* integral vector α that is a solution of the system $S\colon Ax = 0$ and therefore also of the system $A^{\perp}x = 0$, such that $b\alpha < 0$ holds. The vector α can be written as a linear combination with nonnegative integer coefficients of the Hilbert basis $H(S)$. The vector α is *not* a solution of the system $S'\colon Bx = 0$, following the relation $b\alpha < 0$, therefore it cannot be written as a linear combination with nonnegative integer coefficients of the Hilbert basis $H(S')$. Hence, the Hilbert bases $H(S)$ and $H(S')$ must be different. This produces a contradiction with the initial hypothesis. $\square$

Given a set of nonnegative vectors $C = \{c_1, \ldots, c_m\}$, we need to reconstruct a homogeneous linear Diophantine system $S'\colon Bx = 0$ over nonnegative integers, such that each vector $c_i \in C$ is a solution of S'. The system S' is constructed in the following way.

Let d be the dimension of the vectors $C = \{c_1, \ldots, c_m\}$. Start with $S' = \emptyset$. First of all, we must look for the coordinates that are equal to zero for each vector $c_i \in C$, $i = 1, \ldots, m$. For each coordinate $j \in \{1, \ldots, d\}$, such that $c_i^j = 0$ for all vectors $c_i \in C$, put the equation $x_j = 0$ into S'. This creates

the rows with one coefficient equal to 1 and the other equal to zero in the matrix B. Now, form the equation

$$E(x,y)\colon x_1y_1 + \cdots + x_dy_d = 0.$$

Substitute into $E(x,y)$ consecutively the vectors $c_i = (c_i^1, \ldots, c_i^d)$ from C for the variable vector $x = (x_1, \ldots, x_d)$, forming the equations

$$E(c_1,y), E(c_2,y), \ldots, E(c_m,y).$$

This creates a new homogeneous linear Diophantine system $S''\colon Dy = 0$ over integers. Solve the system $S''\colon Dy = 0$ by known methods from linear algebra, e.g., by computing the Smith normal form of the matrix D. If the system S'' has no solution then there is no system S' with solutions including the set of vectors C. Let

$$Y(p_1, \ldots, p_q) \;=\; \{y_i = l_i(p_1, \ldots, p_q) \mid i = 1, \ldots, d\}$$

be the parametric solution of the system S'' with parameters $p = (p_1, \ldots, p_q)$, where l_i are linear Diophantine expressions over p. We substitute consecutively the orthonormal basis $\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)\}$ for p into the parametric solution $Y(p_1,\ldots,p_q)$, producing the particular solutions

$$Y_1 = Y(1,0,\ldots,0), \quad Y_2 = Y(0,1,0,\ldots,0), \quad \ldots, \quad Y_q = Y(0,\ldots,0,1)$$

of the system S''. Clearly, each solution of S'' can be written as a linear combination with integer coefficients of the solution $Y_1, \ldots, Y_q$. Now, we substitute consecutively the solutions $Y_1, \ldots, Y_q$ into the equation $E(x,y)$ for the variables y. We add the equation $E(x,Y_j)$ to the constructed system S', for each $j = 1, \ldots, q$. This terminates the construction of the system S'. The system S' can be constructed in polynomial time, because we can find the parametric solution $Y(p)$ of the homogeneous linear Diophantine system S'' over integers in polynomial time. This is based on the fact that the Smith normal form of an integer matrix can be computed in polynomial time.

Example 10 Let

$$\{100100,\ 010010,\ 001010,\ 100020,\ 020100,\ 011100,\ 002100\}$$

be the set of vectors C for which we want to reconstruct a homogeneous linear Diophantine system $S'\colon Bx = 0$ over nonnegative integers. The 6th coordinate

of the vectors C is always equal to 0, therefore we set $x_6 = 0$. Form the equation

$$E(x,y)\colon x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 + x_6y_6 = 0.$$

Substitute consecutively the vectors C for the variable x into $E(x,y)$, forming the equations $E(c_1,y)$, ..., $E(c_7,y)$. This results in the homogeneous linear Diophantine system S''

$$\begin{array}{rrrrrrrrrrrr}
y_1 & & + y_4 & & & = & 0 & & y_2 & & + y_5 & = & 0 \\
 & y_3 & & + y_5 & & = & 0 & y_1 & & & + 2y_5 & = & 0 \\
2y_2 & & + y_4 & & & = & 0 & & y_2 & + y_3 & + y_4 & = & 0 \\
 & 2y_3 & + y_4 & & & = & 0 & & & & & &
\end{array}$$

over integers. A parametric solution of the system S' is the set

$$Y(p) \;=\; \{y_1 = 2p,\ y_2 = p,\ y_3 = p,\ y_4 = -2p,\ y_5 = -p\}.$$

Instantiating $p = 1$ and adding the set of equations $Y(1)$ to the reconstructed system results in the following final system

$$S' \;=\; \{2x_1 + x_2 + x_3 - 2x_4 - x_5 = 0,\ x_6 = 0\}.$$

It can be easily seen that each solution of the system S' is a linear combination with positive integer coefficients of the vectors C. This is not surprising, since the set C is the Hilbert basis of the reconstructed system S'. $\square$

Suppose now that C is the Hilbert basis of an unknown system. Following the Farkas-Minkowski-Weyl theorem (see Corollaries 7.1a and 7.1b in [Sch86]), the polyhedron $P = \{x \in \mathbb{Z}_0^+ \mid Bx \leq 0\}$ associated with the reconstructed system S' is equal to the set of nonnegative integral vectors

$$cone(G) \;=\; \{\lambda_1 g_1 + \cdots + \lambda_t g_t \in (\mathbb{Z}_0^+)^d \mid g_i \in G,\ \lambda_j \in \mathbb{Q}_0^+\}$$

formed as linear combinations of nonnegative integer vectors $G = \{g_1, \ldots, g_t\}$ with nonnegative rational coefficients λ_j, called also the smallest convex *cone* generated by nonnegative integer vectors G. Since each vector from C is a solution of the reconstructed system $S'\colon Bx = 0$, the set C must be a subset of the polyhedron P. Since $P = cone(G)$, each vector $c_i \in C$ can be written as a linear combination with nonnegative rational coefficients of the vectors G. The

cone $cone(G)$ can be seen also as a linear combination with rational coefficients of the vectors C, i.e.,

$$cone(G) \;=\; \{\mu_1 c_1 + \cdots + \mu_m c_m \mid c_i \in C,\ \mu_j \in \mathbb{Q}\}.$$

Following Theorem 16.4 in [Sch86, page 233], each polyhedral cone is generated by an integral Hilbert basis. Therefore there exists integral vectors $u_1, \ldots, u_t$, $v_1, \ldots, v_s$, such that

$$\begin{aligned} cone(G) \;=\; \{&\lambda_1 u_1 + \cdots + \lambda_t u_t + \mu_1 v_1 + \cdots + \mu_s v_s \\ &\mid \lambda_i \in \mathbb{Z}_0^+, \lambda_1 + \cdots + \lambda_t = 1\}. \end{aligned}$$

If we know that the set of vectors C is a Hilbert basis of an unknown homogeneous linear Diophantine system over nonnegative integers, then it must also generate the cone $cone(G)$ and henceforth the polyhedron P. Otherwise, it could not be the Hilbert basis of a system. Therefore the set of vectors $\{u_1, \ldots, u_t, v_1, \ldots, v_s\}$ must be the Hilbert basis. The cone can be written then as the set

$$cone(G) \;=\; \{\nu_1 c_1 + \cdots + \nu_m c_m \mid c_i \in C, v_j \in \mathbb{Z}_0^+\}.$$

Therefore, we have that $t = m$ and $G = C$, since the Hilbert basis is unique. Therefore C must be also the Hilbert basis of the reconstructed system

$$S'\colon Bx \;=\; 0.$$

Combining it with Proposition 9, we obtain the following result.

Proposition 11 *Let S be a homogeneous linear Diophantine system over nonnegative integers. Let C be the Hilbert basis of an unknown homogeneous linear Diophantine system over $\mathbb{Z}_0^+$. The set C is the Hilbert basis of the system S if and only if the system S' reconstructed from C is equivalent to S.*

We are able now to prove the polynomial equivalence of the problems of HILBERT BASIS CHECKING and HILBERT BASIS RECOGNITION.

Theorem 12 *The problems* HILBERT BASIS CHECKING *and* HILBERT BASIS RECOGNITION *are polynomially equivalent.*

PROOF. To show that the two problems are polynomially equivalent, we present two polynomial-time reductions: one from HILBERT BASIS CHECKING

to HILBERT BASIS RECOGNITION, the other from HILBERT BASIS RECOGNITION to HILBERT BASIS CHECKING.

The reduction from HILBERT BASIS CHECKING to HILBERT BASIS RECOGNITION consists just of forgetting the system S. We must prove that the set of solutions C is the Hilbert basis of the system S if and only if C is the Hilbert basis of some unknown system. From Proposition 9 follows that the set C is the Hilbert basis of the system S if and only if the set C is the Hilbert basis of an unknown system equivalent to S. If the set of vectors C is the Hilbert basis of an unknown system, we reconstruct a homogeneous linear Diophantine system S' over integers, such that all vectors c_i from C are solutions of S'. Following Proposition 11, the set of vectors C is the Hilbert basis of the system S' if and only if the systems S and S' are equivalent.

For the other reduction, if the set C is the Hilbert basis of an unknown system, we can reconstruct a system S' for C in polynomial time. Following Proposition 11, the set C is the Hilbert basis of the known system S in the problem HILBERT BASIS CHECKING if and only if the system S is equivalent to the reconstructed system S'. □

5 Concluding Remarks

We showed that the problem, given a homogeneous linear Diophantine system S over nonnegative integers, asking whether a given solution s belongs to the Hilbert basis of S, is coNP-complete in the strong sense, but it has a pseudopolynomial algorithm if the number of equations in the system S is fixed. This sharpens previous complexity results on recognizing Hilbert basis vectors by Sebő [Seb90] and by Henk and Weismantel [HW96].

Moreover, the coNP-completeness in the strong sense of MINIMAL SOLUTION indicates that the problem of counting the cardinality of the Hilbert basis, considered in [HJK99], is very unlikely to be in #P, unless P = coNP or unless there exists another witness set than the set of minimal solutions of the linear Diophantine system that would allow us to check the witnesses of the Hilbert basis in polynomial time.

We also showed that the problem, given a homogeneous linear Diophantine system S and a set of vectors C, asking whether C is the Hilbert basis of S, is polynomially equivalent to the version of this problem, where the system S is unknown. The former was stated as an open problem by Henk and Weismantel in [HW96], whereas the latter was stated as an open problem by Edmonds and Giles in [EG82]. Our result shows that the presence or absence of a homogeneous linear Diophantine system is not significant for recognizing a Hilbert

basis.

References

[EG82] J. Edmonds and R. Giles. Total dual integrality of linear inequality systems. In W. R. Pulleyblank, editor, *Proceedings Progress in Combinatorial Optimization, Jubilee Conference, Waterloo (Ontario, Canada)*, pages 324–333. Academic Press, 1982.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and intractability: A guide to the theory of NP-completeness.* W.H. Freeman and Co, 1979.

[Gor73] P. Gordan. Ueber die Auflösung linearen Gleichungen mit reellen Coefficienten. *Mathematische Annalen*, 6:23–28, 1873.

[Hil90] D. Hilbert. Ueber die Theorie der algebraischen Formen. *Mathematische Annalen*, 36:473–534, 1890.

[HJK99] M. Hermann, L. Juban, and P. G. Kolaitis. On the complexity of counting the Hilbert basis of a linear Diophantine system. In H. Ganzinger, D. McAllester, and A. Voronkov, editors, *Proceedings 6th International Conference on Logic for Programming and Automated Reasoning (LPAR'99), Tbilisi (Republic of Georgia)*, volume 1705 of *Lecture Notes in Computer Science (in Artificial Intelligence)*, pages 13–32, September, 1999. Springer-Verlag.

[HW96] M. Henk and R. Weismantel. On Hilbert bases of polyhedral cones. Preprint SC 96-12, Konrad-Zuse-Zentrum für Informationstechnik, Berlin, April 1996. URL = http://www.zib.de/bib/pub/pw/index.en.html.

[KB79] R. Kannan and A. Bachem. Algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM Journal on Computing*, 8(4):499–507, 1979.

[Lam87] J.-L. Lambert. Une borne pour les générateurs des solutions entières positives d'une équation diophantienne linéaire. *Compte-rendus de l'Académie des Sciences de Paris*, 305(1):39–40, 1987.

[Pap81] C. H. Papadimitriou. On the complexity of integer programming. *Journal of the Association for Computing Machinery*, 28(4):765–768, 1981.

[Pap94] C. H. Papadimitriou. *Computational complexity.* Addison-Wesley, 1994.

[Sch86] A. Schrijver. *Theory of linear and integer programming.* John Wiley & Sons, 1986.

[Seb90] A. Sebő. Hilbert bases, Carathéodory's theorem and combinatorial optimization. In R. Kannan and W. R. Pulleyblank, editors, *Proceedings 1st Integer Programming and Combinatorial Optimization Conference, Waterloo (Ontario, Canada)*, pages 431–455. University of Waterloo Press, May 1990.

[Sti81] M. Stickel. A unification algorithm for associative-commutative functions. *Journal of the Association for Computing Machinery*, 28(3):423–434, 1981.