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

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

[1] LACL, Department of Computer Science, Université Paris 12, 61, av. gen. de Gaule, 94010 Créteil, France. durand@univ-paris12.fr

[2] LORIA (CNRS and Université Henri Poincaré Nancy 1), BP 239, 54506 Vandœuvre-lès-Nancy, France. {hermann,juban}@loria.fr

Abstract. The problem of computing the Hilbert basis of a 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 prove that, given a linear Diophantine system and a set of solutions, asking whether this set constitutes the Hilbert basis of the system, is also coNP-complete in the strong sense, answering this way an open problem formulated by Henk and Weismantel in 1996. Our result also allows us to solve another open problem, formulated by Edmonds and Giles in 1982, where we prove that asking whether a given set of vectors constitutes the Hilbert basis of an unknown linear Diophantine system, is coNP-complete in the strong sense.

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

* Part of this work was done while the first author was a lecturer (ATER) at IUT A of the Université Nancy 2, France.

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. This naturally invokes the question on the complexity of counting the cardinality of the Hilbert basis. 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).

Following the articles showing its importance, researchers in the fields of automated deduction and integer programming became interested in algorithms computing the Hilbert basis of a system. Huet [Hue78], as well as Clausen and Fortenbacher [CF89] described algorithms working for one equation. These papers assume that the computation of the Hilbert basis of a system can be reduced to successive computations of the Hilbert basis of single equations, interlaced with substitutions of the result into the rest of the system. This approach entails an exponential blow-up during the transformation. Several researchers, including Contejean and Devie [CD94], Lankford [Lan89], Domenjoud [Dom91], Henk and Weismantel [HW96], have also developed direct algorithms for computing the Hilbert basis of systems with an arbitrary number of equations.

We may ask several questions in connection with the Hilbert basis and integer programming problems. These questions represent several variants of the Hilbert basis recognition problem. Usually, the upper bound of the Hilbert basis cardinality counting problem is determined by testing whether a candidate for a solution belongs to the witness set. If 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. The answer 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 coefficients are written in unary notation since the underlying AC-unification problem in automated deduction is always given in unary. In this paper, we properly analyse 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 analyse 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 was unknown whether it is coNP-complete (see Schrijver [Sch86] for an overview and references). In this paper, we completely settle the complexity of these two decision problems.

Due to the page limit, some proofs can be found in the Appendix.

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 is the unique basis of the space of nontrivial solutions of S.

In this paper, we are essentially concerned with the computational complexity of deciding whether a given solution belongs to the Hilbert basis $H(S)$, whether a given set of solutions C constitutes the Hilbert basis $H(S)$ of a given homogeneous linear Diophantine system $S\colon Ax = 0$, and whether a given set of integral vectors C constitutes the Hilbert basis of an unknown system 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 $A_1, A_2, \ldots, A_m$ such that $\sum_{a \in A_i} a = B$ for each $i = 1, \ldots, m$?

Note that each set A_i in 3-PARTITION must contain exactly three elements from A.

In the sequel, we consider the following decision problems. 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.

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?

This problem is essentially the same as the Hilbert basis problem (HBP) formulated in [HW96], whose complexity was left open.

The third problem checks whether a given set of integral vectors C constitutes the Hilbert basis of an unknown system.

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

The third problem is known to be in coNP [EG82], but its exact complexity was unknown.

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.*

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.*

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.*

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].

Theorem 5. HILBERT BASIS CHECKING *is* coNP*-complete in the strong sense.*

Note that the HILBERT BASIS CHECKING problem remains coNP-complete in the strong sense even if C is known to be a set of solutions of the system S.

At last, we consider the HILBERT BASIS RECOGNITION problem stated by Edmonds and Giles in [EG82], where they showed that the problem is in coNP. We will prove a tight lower bound for this problem.

We 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, where $j \in \{k+1, \ldots, n\}$.

Hence, the canonical matrix $A^\perp$ has the form $(U_k \; A_{n-k}^\perp)$, where U_k is a positive integral diagonal $k \times k$ matrix.

The canonical form $A^\perp$ ressembles 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 **Combine** $\succ$ **Zero** $\succ$ **Negative** $\succ$ **Gcd** $\succ$ **Exchange** $\succ$ **Below** $\succ$ **Above** $\succ$ **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.

Exchange: 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 *exchange* the rows a_i and a_j in A.

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 $\epsilon^j = (\epsilon_1^j, \ldots, \epsilon_n^j)$ to A, where $\epsilon_i^j = 1$ if $i = j$ and $\epsilon_i^j = 0$ 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 **Exchange** 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 before treating the

$(i+1)$-th row 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 $A^{\perp}$.*

We define two integral matrices A and B to be *equivalent*, if their canonical forms $A^{\perp}$ and $B^{\perp}$ are equal. In the same spirit, we define two systems $S: Ax = 0$ and $S': Bx = 0$ to be *equivalent* if their matrices A and B are equivalent and they have a nontrivial solution. The following proposition shows that there is a one-to-one correspondence between equivalent systems and nonempty Hilbert bases.

Proposition 8. *Let $S: Ax = 0$ and $S': Bx = 0$ 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 $H(S) = H(S')$.*

Given a set of nonnegative vectors $C = \{c_1, \ldots, c_m\}$, we need to reconstruct a homogeneous linear Diophantine system $S': Bx = 0$ 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 $E(x, y): x_1 y_1 + \cdots + x_d y_d = 0$. 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 $E(c_1, y)$, $E(c_2, y)$, …, $E(c_m, y)$. This creates a new homogeneous linear Diophantine system $S'': Dy = 0$ over integers. Solve the system $S'': Dy = 0$ 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 the 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 $Y_1 = Y(1, 0, \ldots, 0)$, $Y_2 = Y(0, 1, 0, \ldots, 0)$, …, $Y_q = Y(0, \ldots, 0, 1)$ of the system S''. Clearly, each solution of S'' can be written as a linear combination with integer coefficients of the solution Y_1, …, Y_q. Now, we substitute consecutively the solutions Y_1, …, 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 9. 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 $E(c_1,y), \ldots, E(c_7,y)$. This results in the homogeneous linear Diophantine system S''

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

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. In fact, this is not a surprise, since the set C is the Hilbert basis of the reconstructed system S'.

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., $cone(G) = \{\mu_1 c_1 + \cdots + \mu_m c_m \in (\mathbb{Z}_0^+)^d \mid c_i \in C,\ \mu_j \in \mathbb{Q}\}$. 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. 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 8, we obtain the following result.

Proposition 10. *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 complexity result concerning the HILBERT BASIS RECOGNITION problem.

Theorem 11. HILBERT BASIS RECOGNITION *is strongly* coNP*-complete.*

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].

We also proved 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 coNP-complete in the strong sense. This result answers an open problem stated by Henk and Weismantel in [HW96]. Moreover, the aforementioned problem represents an intermediate step for proving the lower bound of the problem whether a given set of integral vectors constitutes the Hilbert basis of an unknown homogeneous linear Diophantine system over nonnegative integers. Essentially the same problem was stated by Edmonds and Giles in [EG82], where they showed that it belongs to coNP, but the lower bound was unknown. We proved that the problem is coNP-complete in the strong sense, what completely settles the complexity of the considered problem.

References

[CD94] E. Contejean and H. Devie. An efficient incremental algorithm for solving systems of linear Diophantine equations. *Information and Computation*, 113(1):143–172, 1994.

[CF89] M. Clausen and A. Fortenbacher. Efficient solution of linear Diophantine equations. *Journal of Symbolic Computation*, 8(1-2):201–216, 1989.

[Dom91] E. Domenjoud. Solving systems of linear Diophantine equations: An algebraic approach. In A. Tarlecki, ed., *Proceedings 16th MFCS, Kazimierz Dolny (Poland)*, *LNCS* 520, pages 141–150. Springer, 1991.

[EG82] J. Edmonds and R. Giles. Total dual integrality of linear inequality systems. In W. R. Pulleyblank, ed., *Proceedings Progress in Combinatorial Optimization, 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.

[Hue78] G. Huet. An algorithm to generate the basis of solutions to homogeneous linear Diophantine equations. *Inf. Proc. Letters*, 7(3):144–147, 1978.

[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 J. 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.

[Lan89] D. Lankford. Non-negative integer basis algorithms for linear equations with integer coefficients. *Journal of Automated Reasoning*, 5(1):25–35, 1989.

[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.* Wiley, 1986.

[Seb90] A. Sebő. Hilbert bases, Carathéodory's theorem and combinatorial optimization. In R. Kannan and W. R. Pulleyblank, eds., *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.

Appendix

Proof of Theorem 1: 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 the lower bound, we construct a polynomial reduction from the complement of PARTITION. The PARTITION problem with the additional special condition is expressed in arithmetic form by the equation $x_1a_1 + (1-x_1)a_2 + \cdots + x_na_{2n-1} + (1-x_n)a_{2n} = (1-x_1)a_1 + x_1a_2 + \cdots + (1-x_n)a_{2n-1} + x_na_{2n}$. 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 $A - A'$. Regrouping variables in the previous equation results in the summand $x_ia_{2i-1} + (1-x_i)a_{2i} - ((1-x_i)a_{2i-1} + x_ia_{2i}) = 2x_i(a_{2i-1} - a_{2i}) - (a_{2i-1} - a_{2i})$ 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 $i = 1, \ldots, n$. $\square$

Proof of Theorem 2: 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 $0 \le x_i \le s_i$ 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 $0 \le x_i \le s_i$, 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. $\square$

Proof of Theorem 3: 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

$$x_1^1 + x_2^1 + \cdots + x_{3m}^1 = 3y$$

$$\vdots$$
$$x_1^m + x_2^m + \cdots + x_{3m}^m = 3y$$

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

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

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. ◻

Proof of Theorem 5: 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.

For the lower bound, we exhibit a polynomial reduction from the problem MINIMAL SOLUTION. Given a system $S: Ax = 0$ and a vector s, we enlarge the system S by a new system $Bx = 0$ that will restrict the solutions of the enlarged system $S': S \cup \{Bx = 0\}$ to the multiples of s. Since s is a minimal solution of S, it will constitute the Hilbert basis of S', i.e., we will force $H(S') = \{s\}$.

We construct the matrix B in the following way. It will be an $(n-1) \times n$ integral matrix, where

$$b_i^j = \begin{cases} 0 & \text{if } i \neq j,\ j < n \\ y_i & \text{if } i = j,\ j < n \\ z_i & \text{if } j = n \end{cases}$$

with the coefficients y_i on the main diagonal, the coefficients z_i in the last column, and zeros everywhere else. The coefficients y_i and z_i are computed as the minimal solutions of the equations $y_i s_i + z_i s_n = 0$ over integers, for each $i = 1, \ldots, n-1$. Hence, the coefficients are $y_i = s_n / \gcd(s_i, s_n)$ and $z_i = -s_i / \gcd(s_i, s_n)$. Indeed, only the multiples of s are solutions of the constructed system $Bx = 0$ which equals $\{(s_n / \gcd(s_i, s_n))x_i - (s_i / \gcd(s_i, s_n))x_n = 0 \mid i = 1, \ldots, n-1\}$. Since s is a minimal solution of S, the set $\{s\}$ is the Hilbert basis of the combined system S'. □

Proof of Proposition 8: 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 $h_j^i = 0$ holds for each vector h_j in the Hilbert basis $H(S)$.

The condition $h_j^i = 0$ for each j implies that the system $A^\perp x = 0$ contains the row $x_i = 0$. Without loss of generality, we assume that $h_1^1 = \cdots = h_q^1 = 0$, 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 $a_1 = (a_1^1, 0, \ldots, 0, a_1^{k+1}, \ldots, a_1^n)$. Since the first coordinate of the vectors h_i is equal to 0, the vector $a' = (0, \ldots, 0, a_1^{k+1}, \ldots, a_1^n)$ 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. Contradiction. □

Proof of Theorem 11: The problem belongs to coNP, as it was proved by Edmonds and Giles in [EG82].

For the lower bound, we perform a reduction from the variant of the HILBERT BASIS CHECKING problem, where C is known to be a set of solutions of the system S. The reduction consists of simply *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. The only-if implication is always trivially satisfied, since C is the Hilbert basis of some system if it is the Hilbert basis of 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 10, the set of vectors C is the Hilbert basis of the system S if and only if the systems S and S' are equivalent. □