[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 $i = 1, \ldots, n$. □

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 $0 \leq x_i \leq s_i$ 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. □

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 $S\colon Ax = 0$ and a vector s, we enlarge the system S by a new system $Bx = 0$ that will restrict the solutions of the enlarged system $S'\colon S \cup \{Bx = 0\}$ 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. □