Semigroups of Polyhedra with Prescribed Number of Lattice Points and the k-Frobenius Problem

Iskander Aliev, Jesús A. De Loera, and Quentin Louveaux

[1] Cardiff University, UK,
AlievI@cardiff.ac.uk,
[2] University of California, Davis
deloera@math.ucdavis.edu
[3] Université de Liège, Belgium
q.louveaux@ulg.ac.be

Abstract. The well-studied semigroup $\mathrm{Sg}(A) = \{b : b = Ax,\ x \in \mathbb{Z}^n, x \geq 0\}$ can be stratified by the sizes of the polyhedral fibers $IP_A(b) = \{x : Ax = b, x \geq 0, x \in \mathbb{Z}^n\}$. The key theme of this paper is a structure theory that characterizes precisely the set $\mathrm{Sg}_{\geq k}(A)$ of all vectors $b \in \mathrm{Sg}(A)$ such that their fiber $IP_A(b)$ has *at least* k-solutions. We demonstrate that this set is finitely generated, a union of translated copies of a semigroup which can be computed explicitly via Hilbert bases computations. Related results can be derived for those right-hand-side vectors b for which $IP_A(b)$ has *exactly* k solutions or *fewer than* k solutions. We also show that, when n, k are fixed natural numbers, one can compute in polynomial time an encoding of $\mathrm{Sg}_{\geq k}(A)$ as a generating function, using a short sum of rational functions. As a consequence, one can identify all right-hand-side vectors that have at least k solutions. Using this tool we prove that for fixed n, k the k-Frobenius number can be computed in polynomial time, generalizing a well-known result of R. Kannan.

1 Introduction

An *affine semigroup* is a semigroup (always containing a zero element) which is finitely generated and can be embedded in $\mathbb{Z}^n$ for some n. We study here a special kind of affine semigroups that appears in many interesting problems in combinatorics, commutative algebra, and number theory and that can be described in very explicit terms. Given an integer matrix $A \in \mathbb{Z}^{d\times n}$ and a vector $b \in \mathbb{Z}^d$, we study the semigroup $\mathrm{Sg}(A) = \{b : b = Ax,\ x \in \mathbb{Z}^n, x \geq 0\}$. Geometrically it can be described as *some* of the lattice points inside the convex polyhedral cone $\mathrm{cone}(A)$ of non-negative linear combinations of the columns of A. It is well-known that $\mathrm{Sg}(A) \subset \mathrm{cone}(A) \cap \mathbb{Z}^n$, but the equality is not always true. It is also well-known that $\mathrm{cone}(A) \cap \mathbb{Z}^n$ is a finitely generated semigroup, this time with generators given by the *Hilbert bases* of $\mathrm{cone}(A)$ [30, 39]. The study of the difference between $\mathrm{Sg}(A)$ and $\mathrm{cone}(A) \cap \mathbb{Z}^n$ is quite interesting (e.g., has been part of many papers in commutative algebra about semigroups and their rings. See e.g., [8, 18, 42, 43] and the references therein). Practically speaking, membership of b in the semigroup $\mathrm{Sg}(A)$ reduces to the challenge, given a vector b, to find whether the linear Diophantine system

$$Ax = b, \quad x \geq 0, \quad x \in \mathbb{Z}^n\,, \tag{1}$$

has a solution or not. We will denote the problem (1) by $IP_A(b)$. Geometrically, $IP_A(b)$ asks whether there is at least one lattice point inside the *parametric polyhedron* $P_A(b) = \{x : Ax = b, x \geq 0\}$.

Now, for a given integer k there are three natural interesting variations of the classical feasibility problem above that in a natural way measure the number of solutions of $IP_A(b)$:

– Are there *at least* k distinct solutions for $IP_A(b)$? If yes, we say that the problem is $\geq k$*-feasible*.

– Are there *exactly* k distinct solutions for $IP_A(b)$? If yes, we say that the problem is $=$ *k-feasible*.
– Are there *less than* k distinct solutions for $IP_A(b)$? If yes, we say that the problem is $<$ *k-feasible*.

We call these three problems, *the fundamental problems of k-feasibility*. Given the integer k one can decompose $\mathrm{Sg}(A)$ taking into account the number of solutions for $IP_A(b)$. The original feasibility problem is just the problem of deciding whether $IP_A(b)$ is ≥ 1-feasible. This shows directly that k-feasibility problems are NP-hard in complexity. Recently Eisenbrand and Hänhle [26] showed that the related problem of finding the right-hand-side vector b that maximizes the number of lattice points solutions, when b is restricted to take values in a polyhedron, is NP-hard.

This paper investigates the question of, given an integral matrix A, determining for which right-hand-side vectors b are the problems $IP_A(b) \geq k$-feasible, $= k$-feasible, or $< k$-feasible. In what follows we say that b is $\geq k$-feasible, or respectively, $= k$-feasible or $< k$-feasible if the corresponding $IP_A(b)$ is. The first part of this paper is about a decomposition of the semigroup $\mathrm{Sg}(A)$ into translated semigroups that group together all elements $b \in \mathrm{Sg}(A)$ that are $\geq k$-feasible (similarly for the other cases). The second part is about the theoretical and practical complexity of algorithms for finding such decomposition of $\mathrm{Sg}(A)$ in practice. A key application is the study of the k-Frobenius number, a number of interest in combinatorial number theory.

The theory of k-feasibility is useful in applications where a given number of solutions k needs to be achieved to consider the problem solved or where one cannot allow too many solutions. Naturally k-feasibility problems have interesting applications in combinatorics and statistics: Consider first the widely popular recreational puzzle *sudoku*, each instance can be thought of as an integer linear program where the hints provided in some of the entries are the given right-hand-sides of the problem. Of course in that case newspapers wish to give readers a puzzle where the solution is unique ($k = 1$). It is not difficult to see that this is a special case of a *3-dimensional transportation problem* that is, the question to decide whether the set of *integer* feasible solutions of the $r \times s \times t$-transportation problem

$$\left\{ x \in \mathbb{Z}^{rst} : \sum_{i=1}^{r} x_{ijk} = u_{jk}, \sum_{j=1}^{s} x_{ijk} = v_{ik}, \sum_{k=1}^{t} x_{ijk} = w_{ij}, x_{ijk} \geq 0 \right\}$$

has a unique solution given right-hand sides u, v, w. Another application of k-feasibility appears in statistics, concretely in application in the data security problem of *multi-way contingency tables*, because when the number of solutions is small, e.g. unique, the margins of the statistical table may disclose personal information which is illegal [24]. Polyhedra with fixed number of (interior) lattice points play a role in many areas of pure mathematics including representation theory, algebraic geometry and combinatorial geometry. Indeed, there has been a lot of work, going back to classical results of Minkowski and van der Corput, to show that the volume of a lattice polytope P with $k = \mathrm{card}(\mathbb{Z}^n \cap \mathrm{int}\, P) \geq 1$ is bounded above by a constant that only depends in n and k (see e.g., [33, 35]). Similarly, the supremum of the possible number of points of $\mathbb{Z}^n$ in a lattice polytope in $\mathbb{R}^n$ containing precisely k points of $\mathbb{Z}^n$ in its interior, can be bounded by a constant that only depends in n and k. Such results play an important role in the theory of toric varieties and the structure of lattice polyhedra (see e.g., [28, 18, 43] and the references therein). The k-feasibility problems also relate to the growth of the values of Littlewood-Richardson coefficients through the polyhedral interpretations of those numbers (see [34] and its references).

Finally, our work is a generalization of a classical problem in combinatorial number theory. Let a be a positive integral n-dimensional primitive vector, i.e., $a = (a_1, \dots, a_n)^T \in \mathbb{Z}^n_{>0}$ with $\gcd(a_1, \dots, a_n) = 1$. For a positive integer k the *k-Frobenius number* $\mathrm{F}_k(a)$ is the largest number which cannot be represented in *at least* k different ways as a non-negative integral combination of the a_i's. Thus, putting $A = a^T$,

$$\mathrm{F}_k(a) = \max\{b \in \mathbb{Z} : IP_A(b) \text{ is } < k- \text{ feasible}\}. \tag{2}$$

When $k = 1$ this has been studied by a large number of authors and both the structure and algorithmic properties are well-understood. Computing $\mathrm{F}_1(a)$ when n is not fixed is an NP-hard problem (Ramirez Alfonsin [37]). On the other hand, for any fixed n the classical Frobenius number can be found in polynomial time by sophisticated deep algorithms due to Kannan [31] and later Barvinok and Woods [12]. The general problem of finding $\mathrm{F}_1(a)$ has been traditionally referred to as the *Frobenius problem*. There is a rich literature on the various aspects of this question. For a comprehensive and extensive survey we refer the reader to the book of Ramirez Alfonsin [38]. The k-feasibility generalization of the Frobenius number was introduced and studied by Beck and Robins in [14]. They gave formulas for $n = 2$ of the k-Frobenius number, but for general n and k only bounds on the k-Frobenius number $\mathrm{F}_k(a)$ are available (see [3],[5] and [27] for prior work).

Our Results

This paper has five contributions to the study of k-feasibility, the semigroup $\mathrm{Sg}(A)$, and the associated polyhedra.

Throughout the paper we assume that the cone $\mathrm{cone}(A)$ is pointed. The five topics indicate the structure of this paper:

1. First, we prove a structural result that implies that the set $\mathrm{Sg}_{\geq k}(A)$ of b's inside the semigroup $\mathrm{Sg}(A)$ that provide $\geq k$-feasible fibers $IP_A(b)$ is finitely generated.
   Let $\mathrm{Sg}_{\geq k}(A)$ (respectively $\mathrm{Sg}_{=k}(A)$ and $\mathrm{Sg}_{<k}(A)$) be the set of right-hand side vectors $b \in \mathrm{cone}(A) \cap \mathbb{Z}^d$ that make $IP_A(b) \geq k$-feasible (respectively $= k$-feasible, $< k$-feasible). Note that $\mathrm{Sg}_{\geq 1}(A)$ is equal to $\mathrm{Sg}(A)$, the semigroup generated by the column vectors of the matrix A.
   Our first structural theorem gives an algebraic description of the sets $\mathrm{Sg}_{\geq k}(A)$ and $\mathrm{Sg}_{<k}(A)$. Let $e_1, \ldots, e_n$ be the standard basis vectors in $\mathbb{Z}^n_{\geq 0}$. We define the *coordinate subspace of* $\mathbb{Z}^n_{\geq 0}$ of dimension $r \geq 1$ determined by $e_{i_1}, \ldots, e_{i_r}$ with $i_1 < \cdots < i_r$ as the set $\{e_{i_1} z_1 + \cdots + e_{i_r} z_r : z_j \in \mathbb{Z}_{\geq 0} \text{ for } 1 \leq j \leq r\}$. By the 0-dimensional coordinate subspace of $\mathbb{Z}^n_{\geq 0}$ we understand the origin $0 \in \mathbb{Z}^n_{\geq 0}$.

   Theorem 1. *(i) There exists a monomial ideal $I^k(A) \subset \mathbb{Q}[x_1, \ldots, x_n]$ such that*

   $$\mathrm{Sg}_{\geq k}(A) = \{A\lambda : \lambda \in E^k(A)\}\,, \tag{3}$$

   where $E^k(A)$ is the set of exponents of monomials in $I^k(A)$.
   (ii) The set $\mathrm{Sg}_{<k}(A)$ can be written as a finite union of translates of the sets $\{A\lambda : \lambda \in S\}$, where S is a coordinate subspace of $\mathbb{Z}^n_{\geq 0}$.

   By the Gordan-Dickson lemma, the ideal $I^k(A)$ is finitely generated, thus one can conclude

   Corollary 1. $\mathrm{Sg}_{\geq k}(A)$ *is a finite union of translated copies of the semigroup $A\mathbb{Z}^n_{\geq 0}$.*

   The proof of Theorem 1 relies on some basic facts on lattice points when we think of them as generators of monomial ideals. The basic tool is a characterization of the complement of a monomial ideal (see [20]). Some of the arguments are of interest for the study of affine semigroups and toric varieties [17, 43].
   Theorem 1 extends the earlier decomposition theorem of Hemmecke, Takemura and Yoshida [29] for $k = 1$. They investigated the semigroup $\mathrm{Sg}(A)$ and the vectors that are *not* in the semigroup but still lie within the cone $\mathrm{cone}(A)$ generated by the columns of A. Note even

when there exists a real nonnegative solution for $Ax = b$, there may not exist an *integral* nonnegative solution. Those authors studied $Q_{\mathrm{sat}} = \mathrm{cone}(A) \cap \mathrm{lattice}(A)$, where $\mathrm{lattice}(A)$ is the lattice generated by the columns of A. They called $H = Q_{\mathrm{sat}} \setminus \mathrm{Sg}(A)$ the set of *holes* of $\mathrm{Sg}(A)$ (in the context of numeric semigroups and the Frobenius number, holes have also been called *gaps*, see [36]) The set of holes H may be finite or infinite, but their main result is to give a finite description of the holes as a finitely-generated set. Our Theorem 1 was inspired by theirs. For us the holes of [29] are just a special case for $k = 1$. We can generalize this notion to consider *k-holes*, namely those right hand-sides b for which $Ax = b$ has *less than k* non-negative integer solutions.
Section 2 gives a proof of Theorem 1 that relies on basic commutative algebra.

2. Second, although traditionally the Frobenius problem has been studied for $1 \times n$ matrices, in Sections 3-5 we discuss $\mathrm{F}_k(A)$, a generalization of k-Frobenius number, but this time applicable to all matrices. We explain the meaning of this generalized k-Frobenius number to the structure of the set $\mathrm{Sg}_{\geq k}(A)$ when seen far away from the origin moving toward asymptotic directions inside the $\mathrm{cone}(A)$. Essentially, the set $\mathrm{Sg}_{\geq k}(A)$ can be decomposed into the set of all integer points in the interior of a certain translated cone and a smaller complex complementary set. We discuss the location of such a cone along a given direction c in the interior of $\mathrm{cone}(A)$.
The key goal of Sections 3-5 is to derive the lower and upper bounds for $\mathrm{F}_k(A)$ under some mild assumptions for the matrix A. Based on the results obtained in [4], [5] we show that $\mathrm{F}_k(A)$ is bounded from above in terms of $\det(AA^T)$ and k.

Theorem 2. *Let A be a matrix in $\mathbb{Z}^{d\times n}$, $1 \leq d < n$, satisfying*

$$\begin{aligned} &\text{i) } \gcd\left(\det(A_{I_d}) : A_{I_d} \textit{ is an } d\times d \textit{ minor of } A\right) = 1,\\ &\text{ii) } \{x \in \mathbb{R}^n_{\geq 0} : A\,x = 0\} = \{0\}\,. \end{aligned} \tag{4}$$

Then the k-Frobenius number associated with A satisfies the inequality

$$\mathrm{F}_k(A) \leq \frac{n-d}{2(n-d+1)^{1/2}}\det(AA^T) + \frac{(k-1)^{1/(n-d)}}{2(n-d+1)^{1/2}}(\det(AA^T))^{1/2+1/(2(n-d))}\,. \tag{5}$$

In addition, the structural Theorem 1 allows us to obtain the lower and upper bounds for $\mathrm{F}_k(A)$ in terms of a finite basis of the monomial ideal $I^k(A)$. Let $||\cdot||_\infty$ denote the maximum norm.

Theorem 3. *Let $x^{g_1}, \ldots, x^{g_t}$ be a finite basis for the ideal $I^k(A)$ and let $m(A) = \min_{1\leq i\leq t}||g_i||_\infty$ and $M(A) = \max_{1\leq i\leq t}||g_i||_\infty$. The number $\mathrm{F}_k(A)$ satisfies the inequalities*

$$m(A) - 1 \leq \mathrm{F}_k(A) \leq \frac{n-d}{2(n-d+1)^{1/2}}\det(AA^T) + M(A)\left(\frac{\det(AA^T)}{n-d+1}\right)^{1/2}\,. \tag{6}$$

3. Third. In Section 6, we propose a way to compute the k-holes, i.e., $\mathrm{Sg}_{<}(A)$, of the semigroup $\mathrm{Sg}(A)$. We give a natural generalization of the proof techniques used in [29] for 1-holes that relies on Hilbert bases to obtain the following theorem:

Theorem 4. *There exists an algorithm that computes for an integral matrix A a finite explicit representation for the set H of k-holes of the semigroup $\mathrm{Sg}(A)$. The algorithm computes (finitely many) vectors $h_i \in \mathbb{Z}^d$ and monoids M_i, each given by a finite set of generators in $\mathbb{Z}^d$, $i \in I$, such that*

$$H = \bigcup_{i\in I}\left(\{h_i\} + M_i\right).$$

Here M_i could be trivial, that is, $M_i = \{0\}$.

4. Our fourth contribution improves on the computational complexity of the earlier sections. For n and k fixed integer numbers, we establish an efficient way to detect all the $\geq k$-feasible vectors b's, not explicitly one by one (as we did in inefficiently in previous sections), but rather the entire set of k-feasible vectors is encoded as a single multivariate *generating function*, $\sum_{\geq k-\text{feasible}} t^b$.

Theorem 5. *Let $A \in \mathbb{Z}^{d\times n}$, let M be a positive integer. Assuming that n and k are fixed, there is a polynomial time algorithm to compute a short sum of rational functions $G(t)$ which efficiently represents a formal sum*

$$\sum_{b:\,\geq k-feasible\ in\ A,\ b_i\leq M} t^b.$$

Moreover, from the algebraic formula, one can perform the following tasks in polynomial time:
(a) Count how many such b's are there (finite because M provides a box).
(b) Extract the lexicographic-smallest such b, $\geq k$-feasible vector.
(c) Find the $\geq k$-feasible vector b that maximizes the dot product $c^T b$.
(d) Identical results hold for the problem of the form $Ax \leq b,\ x \in \mathbb{Z}^n$.

Let us explain a bit the philosophy of such theorem using generating functions for those not familiar with this point of view: In 1993 A. Barvinok [11] gave an algorithm for counting the lattice points in inside a polyhedron P in polynomial time when the dimension of P is a constant. The input of the algorithm is the inequality description of P, the output is a polynomial-size formula for the multivariate generating function of all lattice points in P, namely $f(P) = \sum_{a\in P\cap\mathbb{Z}^n} x^a$ where x^a is an abbreviation of $x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$. Hence, a long polynomial with exponentially many monomials is encoded as a much shorter sum of rational functions of the form

$$f(P) \quad = \quad \sum_{i\in I} \pm \frac{x^{u_i}}{(1-x^{c_{1,i}})(1-x^{c_{2,i}})\ldots(1-x^{c_{n-d,i}})}. \tag{7}$$

Later on Barvinok and Woods [12] developed a set of powerful manipulation rules for using these short rational functions in Boolean constructions on various sets of lattice points, as well as a way to recover the lattice points inside the image of a linear projection of a convex polytope. It is very interesting that to prove the last item of the theorem we will use a generalization of a famous results in the theory of integer programming, the theorem of Doignon [25] and Bell and Scarf [13, 40]. In this paper we rely on Barvinok's theory to prove Theorem 5.
It must be remarked that from the results of Barvinok [11] for fixed n, but not necessarily fixed k, one can decide whether a particular b is k-feasible in polynomial time, but more strongly, as a corollary of Theorem 5, one can prove the following theorem for the computation of the k-Frobenius number. Recall that given a vector $(a_1, a_2, \ldots, a_n)$ and a positive integer b a *knapsack problem* is a linear Diophantine problem of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ with $x_i \geq 0$. The questions about finding the k-Frobenius number is a query over a parametric family of knapsack problems.

Corollary 2. *Consider the parametric knapsack problem $a^T x = b$, $x \geq 0$ associated with the vector $a = (a_1, \ldots, a_n)^T \in \mathbb{Z}^n_{>0}$ with $\gcd(a_1, \ldots, a_n) = 1$. For a fixed positive integers k and n, the k-Frobenius number can be computed in polynomial time.*

This result is a key contribution of this paper. Corollary 2 greatly generalizes a similar celebrated theorem of R. Kannan [31]. Section 7 gives proofs of Theorem 5 and its Corollary 2.

5. The fifth and final contribution of our article is about practical computation and experimental exploration of the behavior of the k-Frobenius number. In the Section 8 we report on the fast practical computation of the k-Frobenius number of parametric knapsacks using ideas from dynamic programming. Using a simple implementation we manage to compute k-Frobenius numbers in several instances with good time performance (see report on our experiments). From Corollary 2 one can ask: What is the computational complexity of computing the k-Frobenius when the dimension n is fixed but k is part of the input? On the basis of the results of [26] one can suspect that this is an NP-hard problem, but we do not know of the answer. It is then of interest to experiment with the values of $\mathrm{F}_k(a)$ to see the growth for fixed values of n. The authors of [3] proved that on average $\mathrm{F}_k(a_1, \dots, a_n)$ equals to $c_{k,n}(a_1 \cdots a_n)^{1/(n-1)}$ where $c_{k,n}$ is a constant that depends on n and k. But we do not know the size of that constant $c_{n,k}$ for $k > 1$. Our final experiments with knapsacks of three variables ($n = 3$) provided support for a conjecture on properties for $\mathrm{F}_k((a_1, a_2, a_3))$ and $c_{3,k}$.

In what follows we assume that the reader has some familiarity with polyhedral convexity, monomial ideals, toric ideals, semigroup rings, and Gröbner bases as presented in [12] and [20, 43].

2 Proof of Theorem 1

For $f \in \mathrm{cone}(A) \cap \mathbb{Z}^d$ define

$$L^k_{A,f} = \{\lambda \in \mathbb{Z}^n_{\geq 0} : IP_A(f + A\lambda) \text{ is } \geq k \text{ feasible}\},$$

so that $\mathrm{Sg}_{\geq k}(A) = \{A\lambda : \lambda \in L^k_{A,0}\}$. Define then the monomial ideal $I^k(A)$ as follows (with its set of exponent vectors denoted by $E^k(A)$).

$$I^k(A) := \langle x^\lambda : \lambda \in L^k_{A,0} \rangle .$$

To see that the equation $\mathrm{Sg}_{\geq k}(A) = \{A\lambda : \lambda \in E^k(A)\}$, is satisfied it is enough to check that for any $\lambda_0 \in L^k_{A,0}$ the inclusion $\lambda_0 + \mathbb{Z}^n_{\geq 0} \subset L^k_{A,0}$ holds. We will prove the following more general statement.

Lemma 1. *For any $f \in \mathrm{cone}(A) \cap \mathbb{Z}^d$ and $\lambda_0 \in L^k_{A,f}$ we have the inclusion*

$$\lambda_0 + \mathbb{Z}^n_{\geq 0} \subset L^k_{A,f} . \tag{8}$$

Proof. Let $\lambda_0 \in L^k_{A,f}$, so that there exist k distinct vectors $\lambda_1, \dots, \lambda_k \in \mathbb{Z}^n_{\geq 0}$ with

$$f + A\lambda_0 = A\lambda_1 = \cdots = A\lambda_k .$$

Take any vector $\mu \in \mathbb{Z}^n_{\geq 0}$ and set $\nu = \lambda_0 + \mu$. Then, clearly, we have

$$f + A\nu = A(\lambda_1 + \mu) = \cdots = A(\lambda_{k-1} + \mu) ,$$

where all vectors $\lambda_1 + \mu, \dots, \lambda_k + \mu \in \mathbb{Z}^n_{\geq 0}$ are distinct. Consequently, $IP_A(f + A\nu)$ is $\geq k$ feasible and, thus, $\nu \in L^k_{A,f}$. Hence (8) holds and the lemma is proved.

Lemma 1 with $f = 0$ clearly implies the first claim of Theorem 1. Let us now prove the second claim. Recall that the elements of the set $\mathrm{Sg}_{<k}(A)$ are also called *k-holes.* A k-hole f is *fundamental* if there is no other k-hole $h \in \mathrm{Sg}_{<k}(A)$ such that $f - h \in \mathrm{Sg}_{\geq 1}(A)$.

Lemma 2. *The set of fundamental k-holes is a subset of the zonotope*

$$P = \{A\lambda : \lambda \in [0, 1)^n\} .$$

Proof. Let $f \in \mathrm{Sg}_{<k}(A)$ be a fundamental hole. We can write

$$f = A\lambda\,,\ \lambda \in \mathbb{Q}^n_{\geq 0}\,.$$

Suppose $f \notin P$. Then for some j we must have $\lambda_j \geq 1$. Thus, denoting by A_j the jth column vector of A, the element $f' = f - A_j$ is a k-hole as any k distinct solutions for $IP_A(f')$ would correspond to k distinct solutions for $IP_A(f)$. Thus we get a contradiction with our choice of f as a fundamental k-hole. This implies $\lambda_j < 1$ for all j and, consequently, $f \in P$. The lemma is proved.

Lemma 2 shows, in particular, that the number of fundamental k-holes is finite. Let us fix a fundamental k-hole f. If the set $L^k_{A,f}$ is empty then $f + A\lambda$ is a k-holes for all $\lambda \in \mathbb{Z}^n_{\geq 0}$. Assume now that $L^k_{A,f}$ is not empty and consider the monomial ideal $I^k_{A,f} \subset \mathbb{Q}[x_1, \dots, x_n]$ defined as

$$I^k_{A,f} = \langle x^\lambda : \lambda \in L^k_{A,f}\rangle\,.$$

Then, in view of (8), $f + A\lambda$ is not a k-hole if and only if $x^\lambda \in I^k_{A,f}$.

Thus we need to write down the set $C(I^k_{A,f})$ of exponents of *standard monomials* for the ideal $I^k_{A,f}$. Any such exponent $\lambda \in C(I^k_{A,f})$ corresponds to the k-hole $f + A\lambda$.

By Theorem 3 in Chapter 9 of [20], the set $C(I^k_{A,f})$ can be written as a finite union of translates of coordinate subspaces of $\mathbb{Z}^n_{\geq 0}$. Since the number of fundamental k-holes is finite, the second claim of Theorem 1 is proved.

3 Asymptotic structure of $\mathrm{Sg}_{\geq k}(A)$

In this section we assume that $A \in \mathbb{Z}^{d\times n}$, $1 \leq d < n$, is an integral $d \times n$ matrix satisfying

$$\begin{array}{l} \text{i)}\ \gcd\left(\det(A_{I_d}) : A_{I_d} \text{ is an } d\times d \text{ minor of } A\right) = 1,\\ \text{ii)}\ \{x \in \mathbb{R}^n_{\geq 0} : A\,x = 0\} = \{0\}\,. \end{array} \tag{9}$$

In the important special case $d = 1$ the matrix $A = a^T$ is just a row vector with $a = (a_1, a_2, \dots, a_n)^T \in \mathbb{Z}^n$ and (9) i) says that $\gcd(a_1, a_2, \dots, a_n) = 1$. Due to the second assumption (9) ii) we may assume that all entries of the vector a are positive. It follows that the largest integral value b such that the problem $IP_A(b)$ is $< k$-feasible, the k-Frobenius number $\mathrm{F}_k(a)$, is well-defined. Clearly, for $d = 1$ we have the inclusion

$$\mathrm{int}(\mathrm{F}_k(a) + \mathbb{R}_{\geq 0}) \cap \mathbb{Z} \subset \mathrm{Sg}_{\geq k}(a^T)\,, \tag{10}$$

where $\mathrm{int}(\cdot)$ denotes the interior of the set.

In general, the structure of the set $\mathrm{Sg}_{\geq k}(A)$, apart from a few special cases, is not well understood. It is known that, in analogy with (10), $\mathrm{Sg}_{\geq k}(A)$ can be decomposed into the set of all integer points in the interior of a certain translated cone and a complex complementary set. More recent results (see [5]) attempt to estimate the location of such a cone along the fixed direction vector $v = A\,\mathbf{1}$, where $\mathbf{1}$ is the all-1-vector, in the interior of $\mathrm{cone}(A)$. The choice of v as the direction vector is dated back to the paper of Khovanskii [32] for $k = 1$.

In this paper we consider a generalization of the Frobenius number that reflects $\geq k$-feasibility properties of the whole family of the problems $IP_A(b)$, when b runs over all integer vectors in the interior of the cone $\mathrm{cone}(A)$. Given a direction vector $b \in \mathrm{int}(\mathrm{cone}(A)) \cap \mathbb{Z}^d$ put

$$\mathrm{g}_k(A, b) = \min\{t \geq 0 : \mathrm{int}(tb + \mathrm{cone}(A)) \cap \mathbb{Z}^n \subseteq \mathrm{Sg}_{\geq k}(A)\}.$$

We define the *k-Frobenius number associated with* A as

$$\mathrm{F}_k(A) = \max\{\mathrm{g}_k(A, b) : b \in \mathrm{int}(\mathrm{cone}(A)) \cap \mathbb{Z}^d\}\,.$$

The number $\mathrm{g}_k(A) = \mathrm{g}_k(A, v)$ was called in [5] the *diagonal k-Frobenius number* $\mathrm{g}_k(A)$ *of* A. A lower bound for $\mathrm{g}_k(A)$ (and thus, by definition of $\mathrm{g}_k(A)$, for $\mathrm{F}_k(A)$) was given in [5, Theorem 1.3]. Next we derive the lower and upper bounds for $\mathrm{F}_k(A)$ presented in Theorem 2 and Theorem 3.

Before we start the proofs it is worth remarking they will be based on the results obtained in [4], [5] and the structural Theorem 1.

4 Proof of Theorem 2

First we show that the k-Frobenius number $\mathrm{F}_k(A)$ is bounded from above by the (suitably normalized) number $\mathrm{g}_k(A)$.

Lemma 3.

$$\mathrm{F}_k(A) \le \left(\frac{\det(AA^T)}{n-d+1}\right)^{1/2} \mathrm{g}_k(A)\,. \tag{11}$$

Proof. Put for convenience $\gamma = \left(\frac{\det(AA^T)}{n-d+1}\right)^{1/2}$. As it was shown in the proof of Lemma 1.1 in [4], for any $b \in \mathrm{int}(\mathrm{cone}(A)) \cap \mathbb{Z}^d$ the vector γb is contained in $v + \mathrm{cone}(A)$. Therefore $\gamma b + \mathrm{cone}(A) \subset v + \mathrm{cone}(A)$ and, consequently,

$$\mathrm{int}(\mathrm{g}_k(A)\gamma b + \mathrm{cone}(A)) \cap \mathbb{Z}^n \subset \mathrm{int}(\mathrm{g}_k(A)v + \mathrm{cone}(A)) \cap \mathbb{Z}^n \subset \mathrm{Sg}_{\ge k}(A)\,.$$

Hence for any $b \in \mathrm{int}(\mathrm{cone}(A)) \cap \mathbb{Z}^d$ we have $\mathrm{g}_k(A, b) \le \mathrm{g}_k(A)\gamma$. Therefore $\mathrm{F}_k(A) \le \mathrm{g}_k(A)\gamma$ and the lemma is proved.

The diagonal k-Frobenius number $\mathrm{g}_k(A)$ in its turn is bounded from above in terms of A and k due to the following result.

Theorem 6 (Theorem 1.2 in [5]). *The diagonal k-Frobenius number associated with A satisfies the inequality*

$$\mathrm{g}_k(A) \le \frac{n-d}{2}(\det(AA^T))^{1/2} + \frac{(k-1)^{1/(n-d)}}{2}\left(\det(AA^T)\right)^{1/(2(n-d))}\,. \tag{12}$$

Combining (11) and (12) we obtain the inequality (5).

5 Proof of Theorem 3

Recall that by Theorem 1 (i), we have

$$E^k(A) = \{\lambda \in \mathbb{Z}^n_{\ge 0} : A\lambda \in \mathrm{Sg}_{\ge k}(A)\}\,.$$

This implies the following observation.

Lemma 4. *For any $\mu \in \mathbb{Z}^n_{\ge 0} \setminus E^k(A)$ we have $A\mu \in \mathrm{Sg}_{<k}(A)$*

The set of exponents $E^k(A)$ of the monomial ideal $I^k(A) = \langle x^{g_1}, \dots, x^{g_t} \rangle$ has the form

$$E^k(A) = \bigcup_{i=1}^{t} (g_i + \mathbb{Z}^n_{\geq 0})\,. \tag{13}$$

By (13), any $g \in E^k(A)$ has $||g||_\infty \geq m(A)$. Therefore the point $(m(A)-1)\mathbf{1} \notin E^k(A)$ and, by Lemma 4, we obtain $A((m(A)-1)\mathbf{1}) = (m(A)-1)v \notin \mathrm{Sg}_{\geq k}(A)$. Therefore, by the definition of $\mathrm{g}_k(A)$,

$$m(A) - 1 \leq \mathrm{g}_k(A) \leq \mathrm{F}_k(A)\,.$$

This proves the lower bound in (6).

To derive the upper bound, we will show first that $\mathrm{g}_k(A)$ satisfies the inequality

$$\mathrm{g}_k(A) \leq \mathrm{g}_1(A) + M(A)\,. \tag{14}$$

Let us choose any $y \in ((\mathrm{g}_1(A) + M(A))v + \mathrm{cone}(A)) \cap \mathbb{Z}^d$. To prove (14), it is enough to show that $y \in \mathrm{Sg}_{\geq k}(A)$. Consider the point $y' = y - M(A)v$. Since $y' \in (\mathrm{g}_1(A)v + \mathrm{cone}(A)) \cap \mathbb{Z}^d$, we have $y' \in \mathrm{Sg}_{\geq 1}(A)$. Therefore, there exists $z \in \mathbb{Z}^n_{\geq 0}$ such that $Az = y'$. Hence $A(z + M(A)\mathbf{1}) = Az + M(A)v = y$. Finally, observe that $M(A)\mathbf{1} \in E^k(A)$, and hence $z + M(A)\mathbf{1} \in M(A)\mathbf{1} + \mathbb{Z}^n \subset E^k(A)$. Consequently, $y = A(z + M(A)\mathbf{1}) \in \mathrm{Sg}_{\geq k}(A)$ and the inequality (14) is proved. The upper bound in (6) now follows from (11), (14) and (12) with $k = 1$.

6 Computing *k*-holes via Hilbert bases

In this section we combine the results of Hemmecke et al. [29] with our techniques to compute the elements of $\mathrm{Sg}_{<k}(A)$ proving Theorem 4. In contrast to the *implicit* representation via rational generating functions that we saw in Section 7, we now present an algorithm to compute an *explicit* representation of $\mathrm{Sg}_{\geq k}(A)$, even for an infinite case using semigroups. We remark that this explicit representation need not be of polynomial size in the input size of A.

In view of the proof of Theorem 1 (ii), it is enough to compute all fundamental k-holes and then for each fundamental k-hole f compute the standard monomials of the ideal $I^k_{A,f}$. In view of Lemma 2, all fundamental k-holes are located in a zonotope $P = \{A\lambda : \lambda \in [0,1)^n\}$. Thus, with a straightforward generalization of the approach proposed in Hemmecke et al. [29], the fundamental k-holes the can be computed by using a Hilbert basis of the cone $\mathrm{cone}(A)$. In the special case $k = 1$ Hemmecke et al. [29] obtained the following result:

Lemma 5. *There exists an algorithm that computes for an integral matrix A a finite explicit representation for the set H of holes of the semigroup Q generated by the columns of A. The algorithm computes (finitely many) vectors $h_i \in \mathbb{Z}^d$ and monoids M_i, each given by a finite set of generators in $\mathbb{Z}^d$, $i \in I$, such that*

$$H = \bigcup_{i \in I} (\{h_i\} + M_i)\,.$$

Here M_i could be trivial, that is, $M_i = \{0\}$.

Let f be a fundamental k-hole. Recall that for a nonempty set $L^k_{A,f}$ the monomial ideal $I^k_{A,f} \subset \mathbb{Q}[x_1, \dots, x_n]$ is defined as

$$I^k_{A,f} = \langle x^\lambda : \lambda \in L^k_{A,f} \rangle$$

and $f + A\lambda$ is not a k-hole if and only if $x^\lambda \in I^k_{A,f}$.

Thus we need to compute the exponents of standard monomials for the ideal $I^k_{A,f}$. Any such exponent $\lambda \in \mathbb{Z}^n_{\geq 0}$ corresponds to the k-hole $f + A\lambda$.

The exponents of standard monomials can be computed explicitly from a set of generators of the ideal. Hence, it is enough to find the generators of $I^k_{A,f}$. Let us fix an ordering $\prec$ in $\mathbb{Z}^n_{\geq 0}$. The minimal generators for the ideal $I^k_{A,f}$ correspond to the $\prec$-minimal elements of the set

$$L^k_{A,f} = \{\lambda \in \mathbb{Z}^n_{\geq 0} : \exists \text{ distinct } \mu_1, \dots, \mu_k \in \mathbb{Z}^n_{\geq 0} \text{ such that } \\ f + A\lambda = A\mu_1 = \dots = A\mu_k\}\,.$$

For computational purposes it is enough to compute a set of vectors of $L^k_{A,f}$ that contains all the $\prec$-minimal elements. We will proceed as follows. Let K be a complete graph with the vertex set $V = \{1, 2, \dots, k\}$. By a weighted orientation H of K we will understand a weighted directed graph $H = (V, E)$ such that any two vertices of H are connected by a directed edge $e \in E$ with a weight $w(e) \in \{1, \dots, n\}$.

Let $\mathcal{S}$ be set of all weighted orientations of K. For each $H \in \mathcal{S}$ we construct the following two auxiliary sets: the set

$$L_H = \{\lambda \in \mathbb{Z}^n_{\geq 0} : \exists \mu_1, \dots, \mu_k \in \mathbb{Z}^n_{\geq 0} \text{ such that } f + A\lambda = A\mu_1 = \dots = A\mu_k \\ \text{and } (\mu_i)_{w(e)} \leq (\mu_j)_{w(e)} - 1 \text{ for each } e = (i,j) \in E\,\}$$

and the set

$$M_H = \{(\lambda, \mu_1, \dots, \mu_k) \in \mathbb{Z}^{(k+1)n}_{\geq 0} : f + A\lambda = A\mu_1 = \dots = A\mu_k \\ \text{and } (\mu_i)_{w(e)} \leq (\mu_j)_{w(e)} - 1 \text{ for each } e = (i,j) \in E\}\,.$$

Then, in particular, $L^k_{A,f} = \bigcup_{H \in \mathcal{S}} L_H$, where the union is taken over all orientations in $H \in \mathcal{S}$.

We will need the following result.

Lemma 6. *Let λ_0 be a $\prec$-minimal element of L_H. Then there exists a $\prec$-minimal element of M_H of the form $(\lambda_0, \hat{\mu}_1, \dots, \hat{\mu}_k)$.*

Let λ_0 be a $\prec$-minimal element of L_H. Suppose on contrary, for every $(\mu_1, \dots, \mu_k) \in \mathbb{Z}^{kn}_{\geq 0}$ the vector $(\lambda_0, \mu_1, \dots, \mu_k)$ is not a $\prec$-minimal element of M_H. Let $(\hat{\mu}_1, \dots, \hat{\mu}_k)$ be a $\prec$-minimal element of the set

$$M_H|_{\lambda=\lambda_0} = \{(\mu_1, \dots, \mu_k) \in \mathbb{Z}^{kn}_{\geq 0} : f + A\lambda_0 = A\mu_1 = \dots = A\mu_k \\ \text{and } (\mu_i)_{w(e)} \leq (\mu_j)_{w(e)} - 1 \text{ for each } e = (i,j) \in E\}\,.$$

By the assumption, there exists a vector $(\lambda', \mu'_1, \dots, \mu'_k) \in M_H$ such that $(\lambda', \mu'_1, \dots, \mu'_k) \prec (\lambda_0, \hat{\mu}_1, \dots, \hat{\mu}_k)$ and $(\lambda', \mu'_1, \dots, \mu'_k) \neq (\lambda_0, \hat{\mu}_1, \dots, \hat{\mu}_k)$. If $\lambda' \neq \lambda_0$ we get a contradiction to the $\prec$-minimality of λ_0 in L_H. On the other hand, if $\lambda' = \lambda_0$ we get a contradiction to the $\prec$-minimality of $(\hat{\mu}_1, \dots, \hat{\mu}_k)$ in $M_H|_{\lambda=\lambda_0}$.

In view of Lemma 6, to compute a generating set for $L^k_{A,f}$ (or to determine that $L^k_{A,f}$ is empty) it is now enough to compute the set of all minimal elements for $M_H, H \in \mathcal{S}$ and remove the last kn components from each of them.

7 Proof of Theorem 5

We use the technic of rational generating functions developed by Barvinok and Woods in [11, 12] (see also the book [10]). We wish to prove a representation theorem of a set of lattice points as a sum $\sum_{\geq k-\text{feasible}} t^b$. First we need a lemma

Lemma 7. *Let n be a constant. Given a positive integer M and the associated n-dimensional box $B_M = [0,M]^n$, there exist an integer linear objective function $\bar{c}_M^{\intercal} x$ such that $\bar{c}_M^{\intercal}(y_i - y_j) \neq 0$ for all pairs of non-zero lattice points y_i, y_j inside the box B_M. One can find one such vector in polynomial time.*

Proof: Let s be a single auxiliary (real) variable and the associated vector $\mathbf{c}(\mathbf{s}) = (1, s, s^2, s^3, \ldots, s^{n-1})^T$. Now for each of the $L = M^n(M^n-1)/2$ pairs of non-zero lattice vectors $y_i - y_j$ we construct one univariate polynomial $f_{i,j}(s) = \mathbf{c}(\mathbf{s})^{\intercal}(y_i - y_j)$ (since y_i, y_j are distinct the polynomial $f_{i,j}$ is not identically zero). These are polynomials of degree $n-1$ so they can only have at most $n-1$ real roots each. Note also that these are polynomials all of whose coefficients are integer numbers between $-M$ and M, that means, by the famous Cauchy bound on the absolute values of roots of univariate polynomials that any of the real roots of any $f_{i,j}(s)$ must be bounded in above by $1+M$. Thus taking, for example, the value $s_0 = M+2$ gives $\bar{c}_M = \mathbf{c}(s_0)$ as an integer vector that totally orders all lattice points in the box B_M. Note that the bit-size description of $\bar{c}_M$ is polynomial in the input namely n, and $\log(M)$ because the entries are the first $(n-1)$ powers of M.

Now, recall that A is an integral $d \times n$ matrix and n, k are constants. Let M be an integer that bounds the k-Frobenius number of A. We can define the polyhedron (note X_i denotes an n-dimensional vector so this polytope lives in nk-dimensional space):

$Q(A,k,M) = \big\{(X_1, X_2, \ldots, X_k) : \; AX_1 = \cdots = AX_k,\ \bar{c}_M^{\intercal} X_i \geq \bar{c}_M^{\intercal} X_{i+1} + 1, \text{ for } i = 1, \ldots, k-1 \text{ and } X_i \geq 0,\ M \geq AX_1 \geq 0\big\}$.

One can use Barvinok's algorithm to compute the generating function of the lattice points of $Q(A,k,M)$. This is a polytope that has the key property that all its integer points represent *distinct* k-tuples of integer points that are in some polytope $P_A(b) = \{x : Ax = b, x \geq 0\}$. When we turn to monomials, $z_1^{X_1} z_2^{X_2} \ldots z_k^{X_k}$ has only those where $X_i \neq X_j$. Namely, this is precisely the set of all monomials coming from k-tuples of distinct vectors in $\mathbb{Z}^n_{\geq 0}$ that give the same value $AX_1 = AX_2 = \cdots = AX_k$.

We can do Boolean operations on the generating functions representing sets of lattice points by the following result:

Lemma 8 (Corollary 3.7 in [12]). *Let us fix l (the number of sets $S_i \subset \mathbb{Z}^d$) and r (the number of binomials in each fraction of the generating function $f(S_i)$). Then there exists an $s = s(l,r)$ and a polynomial time algorithm, which, for any l (finite) sets of lattice points $S_1, \ldots, S_l \subset \mathbb{Z}^d$ given by their generating functions $f(S_i)$ and a set $S \subset \mathbb{Z}^n$ defined as a Boolean combination of $S_1, \ldots, S_m$, computes $f(S)$ in the form*

$$f(S) = \sum_{i \in I} \gamma_i \frac{x^{u_i}}{(1 - x^{v_{i1}}) \cdots (1 - x^{v_{is}})},$$

where $\gamma_i \in \mathbb{Q}$, $u_i, v_{ij} \in \mathbb{Z}^n$ and $v_{ij} \neq 0$ for all i, j.

Finally another key subroutine introduced by Barvinok and Woods is the following *Projection Theorem*. In both Lemmas 8 and 9, the dimension n is assumed to be fixed.

Lemma 9 (Theorem 1.7 in [12]). *Assume the dimension n is a fixed constant. Consider a rational polytope $P \subset \mathbb{R}^n$ and a linear map $T : \mathbb{Z}^n \to \mathbb{Z}^k$. There is a polynomial time algorithm which computes a short representation of the generating function $f\big(T(P \cap \mathbb{Z}^n), x\big)$.*

In this case we apply a very simple linear map $T(X_1, X_2, \ldots, X_k) = AX_1$, by multiplication with A. This yields of course for each k-tuple (which has $X_i \neq X_j$) the corresponding right-hand side vector $b = AX_1$ that has at least k-distinct solutions. The final generating expression will be

$$f = \sum_{b \in \text{projection of } Q(A,k,M) : \text{with at least } k\text{-representations}} t^b.$$

Which is the desired short rational function which efficiently represents the sum $\sum_{\geq k-\text{feasible}} t^b$. This proves the main result in the body of the paper for $\geq k$-feasible. Because if one knows a description for $\mathrm{Sg}_{\geq k}(A)$ and $\mathrm{Sg}_{\geq k+1}(A)$ one knows $\mathrm{Sg}_{=k}(A) = \mathrm{Sg}_{\geq k}(A) \backslash \mathrm{Sg}_{\geq k+1}(A)$ and $\mathrm{Sg}_{<k}(A) = \mathrm{Sg}(A) \backslash \mathrm{Sg}_{\geq k}(A)$, the Boolean properties of generating functions in Lemma 8 give the theorem in all three cases.

Now we move to prove Parts (a) to (d) of the theorem.

Part (a) If we have a generating function representation of

$$\sum_{\geq k-\text{feasible}} t^b,$$

it has the form

$$f(t) = \sum_{i \in I} \alpha_i \frac{t^{p_i}}{(1 - t^{a_{i1}}) \cdots (1 - t^{a_{ik}})}.$$

Note that by specializing at $t = (1, \ldots, 1)$, we can count how many b's are $\geq k$-feasible (again the set is finite because it fits inside a box). Remark the substitution is not immediate since $t = (1, \ldots, 1)$ is a pole of each fraction in the representation of f. This problem is solvable because it has been shown by Barvinok and Woods that this computation can be handled efficiently (see Theorem 2.6 in [12] for details) and this proves Part (a).

Part (b) This item is a direct corollary of the following extraction lemma.

Lemma 10 (Lemma 8 in [22] or Theorem 7.5.2 in [23]). *Assume the dimension n is fixed. Let $S \subset \mathbb{Z}_+^n$ be nonempty and finite set of lattice points. Suppose the polynomial $f(S; z) = \sum_{\beta \in S} z^\beta$ is represented as a short rational function and let c be a cost vector. We can extract the (unique) lexicographic largest leading monomial from the set $\{x^\alpha : \alpha \cdot c = M, \alpha \in S\}$, where $M := \max\{\alpha \cdot c : \alpha \in S\}$, in polynomial time.*

Part (c) Barvinok and Woods developed a way to do monomial substitutions (not just $t_i = 1$ as we used in Part (a)), where the variable t_i in the current series, is replaced by a new monomial $z_1^{a_1} z_2^{a_2} \cdots z_r^{a_r}$. Note that the rational generating function $f = \sum_{b \in Q \cap \mathbb{Z}^d} b^b$ can give the evaluations of the b's for a given objective function $c \in \mathbb{Z}^d$. If we make the substitution $t_i = z^{c_i}$, the above equation yields a *univariate* rational function in z:

$$f(z) = \sum_{i \in I} E_i \frac{z^{c \cdot u_i}}{\prod_{j=1}^{d} (1 - z^{c \cdot v_{ij}})}. \tag{15}$$

Moreover $f(z) = \sum_{b \in Q \cap \mathbb{Z}^d} z^{c \cdot b}$. Thus we just need to find the (lexicographically) largest monomial in the sum in polynomial time. But this follows from Part (b).

Part (d) To prove this result we will use a recent generalization of Doignon-Bell-Scarf's theorem [6]. Any problem of the form $Ax \leq b$ can be transferred to a problem of the form $Ax + Is = b$ by adding slack variables s. Then such a system is in the shape of the main part of Theorem 5 except we need a fixed number of columns. To see this is possible, by Theorem 1 in [6], if $Ax \leq b$ has k-solutions then, exactly the same integer solutions appear in a subsystem $A_S x \leq b$ with no more than a constant $c(n, k)$ rows. Thus when we add slacks we will only add a constant number of slacks, only $n + c(k, n)$ many of them. Of course we do not know which rows form the system but there are only $\binom{d}{c(k,n)}$ possibilities for subsystems $A_S x + Is = b$ (each subsystem has a fixed number of columns now, thus it can be solved in polynomial time). Therefore, we can also decide for which b's the polyhedron has k points $Ax \leq b$ in polynomial time (again when encoded in a rational function format).

To conclude we see how to compute the k-Frobenius number efficiently.
Proof of Corollary 2:

We start by observing that there is an upper bound for the k-Frobenius number. Indeed Theorem 1.1 in [3] gives already an upper bound on that is certainly smaller than $M = k(n-1)!a_1a_2\cdots a_n$. The k-Frobenius number must be smaller and thus we will use in the bounding box created in our Theorem 5.

Next we claim the same generating function descriptions obtained in Theorem 5 exist also for the sets those b which are $= k$-feasible, $\geq k$-feasible, or $< k$-feasible with the added condition that $b_i \leq M$. This is because the generating functions of those sets of b's can be obtained from the set of b's encoded by Theorem 5 through Boolean operations (intersection, unions, complements). Indeed using Barvinok Woods theory about such Boolean expressions, and the fact that $\mathrm{Sg}_{\geq k+1}(A) \setminus \mathrm{Sg}_{\geq k}(A) = \mathrm{Sg}_{=k}(A)$ and that $\mathrm{Sg}_{<k}(A) = \mathrm{Sg}_{\geq k}(A) \setminus \mathrm{Sg}_{=k}(A)$. The same identities hold under the intersection with the box $B_M = [0, M]^d$, thus the claim follows.

We may see now that Corollary 2 follows directly from what we achieved in Theorem 5 and the Boolean operation Lemma of Barvinok and Woods. Indeed, from Theorem 5 we have a rational function representation of the k-feasible b for the Knapsack problem $f(t) = \sum_{i\in I} E_i \frac{t^{c\cdot u_i}}{\prod_{j=1}^{d}(1-t^{c\cdot v_{ij}})} = \sum_{b\in \text{projection of} Q(A,k,M)\cap\mathbb{Z}^d,\, \geq k-\text{feasible}} t^{c\cdot b}$. Clearly the k-Frobenius number is simply the largest (lexicographic) b, such that t^b is **not** in $f(t)$, it is in its complement. Note the choice of bound M is such that we indeed have the k-Frobenius number inside. Then, for the complement $\overline{S} = \mathbb{Z}_+ \setminus S$, we compute the generating function $f(\overline{S}; x) = (1-t)^{-1} - f(t)$ and then we compute the largest such t^b in the complement using Lemma 10.

8 Computing the k-Frobenius number by dynamic programming

In this section, we propose a dynamic programming algorithm to compute the k-Frobenius number in practice. We run some experiments with the algorithm. We first describe the algorithm. There is a lot of prior work for the computation of $F_1(a)$ (see [9] and references therein).

8.1 A simple dynamic programming algorithm for $F_k(a)$

Definition 1. *Given $a_1, \ldots, a_n \in \mathbb{Z}_+$, we introduce $T_i(b)$ as denoting the number of integral solutions of the knapsack $\sum_{l=1}^{n} a_l x_l = b$ satisfying $x_j = 0$ for $j < i$ and $x_i \geq 1$, i. e. $T_i(b)$ counts the number of integral solutions of the knapsack where the smallest nonzero index is i.*

The idea of the algorithm is to update an array $T_i(b)$ for increasing b and for all i. The following observation allows us to initialize the dynamic programming approach.

Lemma 11. *$T_i(a_i) = 1$ and $T_i(b) = 0$ for all $0 \leq b \leq a_i - 1$.*

The following lemma explains how to update the function T.

Lemma 12. *Given $b \neq a_i$,*

$$T_i(b) = \sum_{j=i}^{n} T_j(b - a_i). \tag{16}$$

Proof. We first prove that (16) holds with $\geq$ instead of $=$. Indeed consider any solution $\bar{x}$ of $\sum_{l=1}^{n} a_l x_l = b - a_i$ with $\bar{x}_j = 0$ for all $1 \leq j \leq i-1$, it can be transformed into a solution for

$\sum_{l=1}^{n} a_l x_l = b$ by considering $\bar{x} + e_i$. Obviously the first $(i-1)$ components are still zero and the i^{th} component is positive.

We now prove that (16) holds with $\leq$. Consider a solution $\hat{x} \in \mathbb{Z}_+^n$ with $\hat{x}_j = 0$ for all $1 \leq j \leq i-1$ and $\hat{x}_i \geq 1$ to $\sum_{l=1}^{n} a_l x_l = b$. By subtracting 1 from the first component, we obtain a solution to $\sum_{l=1}^{n} a_l x_l = b - a_i$ where the first $i-1$ components are zero.

Using Lemma 11 and Lemma 12, we can fill in an array $T_i(b)$ starting from $b = 0$ for increasing values of b. Obtaining the array T allows us to count the number of different solutions.

Lemma 13. *The number of integral solutions to* $\sum_{l=1}^{n} a_l x_l = b$ *is equal to* $\sum_{i=1}^{n} T_i(b)$.

Proof. This follows from the fact that any integral solution to $\sum_{l=1}^{n} a_l x_l = b$ is counted exactly one in one set corresponding to the smallest index for which x_i is nonzero.

To determine the k-Frobenius number, we need to know the largest b that is $<$ k-feasible. It is therefore important to determine a stopping criterion for the dynamic programming algorithm. A first obvious criterion is to use the upper bound for b given in Section 4. It turns out that this upper bound is very often too large compared to the actual k-Frobenius number and leads to longer computation times. The following lemma allows us to interrupt the computation with the guarantee for a k-Frobenius number earlier.

Lemma 14. *Assume that* $a_1 < a_2 < \cdots < a_n$ *and that* $\sum_{i=1}^{n} a_i x_i = b$ *has at least* k *integral solutions for all* $\bar{b} \leq b \leq \bar{b} + a_1$. *Then* $\sum_{i=1}^{n} a_i x_i = b$ *has at least* k *integral solutions for all* $b \geq \bar{b}$.

Proof. This follows from the fact that $T_1(b) = \sum_{i=1}^{n} T_i(b - a_1)$ and that the number of integral solutions of $\sum_{i=1}^{n} a_i x_i = b$ is at least $T_1(b)$.

We now have all the necessary ingredients to describe a dynamic programming-based algorithm.

Algorithm 1 DP algorithm for the k-Frobenius number

```
Require: a_1 < a_2 ··· < a_n, k ≥ 1
  T_i(a_i) = 1 for all i = 1, ..., n
  T_i(b) = 0 for i = 1, ..., n and b < a_i
  b := a_1 + 1
  while ∃b̄ ∈ [b − a_1, b − 1] with Σ_{i=1}^{n} T_i(b̄) < k do
    for i := 1 to n do
      T_i(b) := Σ_{j=i}^{n} T_j(b − a_i)
    end for
    b := b + 1
  end while
  Return the largest b that has less than k solutions
```

8.2 Empirical complexity of the dynamic programming algorithm

In the following, we report on some experiments carried out by implementing the dynamic programming algorithm. We want to check the average time needed to compute the k-Frobenius number for some common values of n and a_1 as well as the dependency on k. We also want to see an average measure of the k-Frobenius number. Our implementation of the algorithm is in standard C code

CPU	Intel Core i7-975, 4 cores, 8 threads
CPU clock	3.33 GHz
Installed RAM	12 Gb DDR3-1333 SDRAM
Compiler	GCC 4.6.3 20120306 (Red Hat 4.6.3-2)
Environment	GNU/Linux (Fedora 15)
Kernel	linux 2.6.43.8-1.fc15.x86_64

Table 1. Conditions of the experiments

and does not allow for arbitrarily large integers. The conditions of our experiments are detailed in Table 1.

The first set of experiments aims at evaluating the running time of the algorithm. We ran the algorithm for different values of n, the number of variables of the knapsack. For each value of n, we create 20 knapsacks with coefficients in the range $[2^{16}, 2^{18}]$ and compute the 32-Frobenius number. In Table 2, we report on the average running time in seconds as well as the average maximum right-hand-side reached before the stopping criterion (given by Lemma 14) is met. We observe that

Dimension	5	10	15	20	25	30
Average time (s)	12	2	2	3	3	4
Average max rhs ($\times 10^6$)	63.8	2.5	1.5	1.2	0.98	0.89

Table 2. Dependency on the dimension n

the larger n is, the fewer iterations are needed since in this case, the number of solutions grows quickly. The total time however increases slightly with n as the array T is larger to fill. At some point, we may expect memory issues as the array T becomes too large to store when n increases.

In the second set of experiments, we investigate the complexity dependent on the value a_1. In particular, we fix $k = 32$ and the dimension to either 3, 6 or 12. We let the coefficients vary in an increasing range. For each given interval, we again run 20 different instances and compute the average running time as well as the maximum right-hand-side reached before the stopping criterion (given by Lemma 14) is met. The summary of the experiment is reported in Table 3. We observe a strong dependency on the size of the coefficients. The largest range reported is, for each given dimension, the largest for which we did not run into memory issues. We observe again that the k-Frobenius number is larger when the dimension is smaller.

Finally we want to check the dependency on k. We fix the dimension to $n = 10$ and the range of values for a_i to $[2^{14}, 2^{16}]$. For each value of k, we run 20 experiments. In this set of experiments, we also want to report on how the k-Frobenius number varies with increasing k. We show both results for $n = 5$ and $n = 10$. The summary of the results are reported in Table 4. We observe that it is not much more complicated to compute a larger value of k with our approach and that the algorithm is slightly dependent on that parameter (in particular when $n = 10$). We can also observe that for a given k, we also automatically compute all smaller values of k during the algorithm. In particular the 1-Frobenius number is the usual Frobenius number. We refer to [15] for extensive computational experiments and a survey on most existing algorithms for the Frobenius number in the usual sense.

Dimension $n = 3$						
Range a_i	$[2^6, 2^7]$	$[2^8, 2^9]$	$[2^{10}, 2^{11}]$	$[2^{12}, 2^{13}]$	$[2^{14}, 2^{15}]$	$[2^{16}, 2^{17}]$
Average time (s)	0	0	0	1	13	32
Max rhs ($\times 10^6$)	0.008	0.08	0.8	13	163	359
Dimension $n = 6$						
Range a_i	$[2^{10}, 2^{11}]$	$[2^{12}, 2^{13}]$	$[2^{14}, 2^{15}]$	$[2^{16}, 2^{17}]$	$[2^{18}, 2^{19}]$	$[2^{20}, 2^{21}]$
Average time (s)	0	0	0	1	7	52
Max rhs ($\times 10^6$)	0.03	0.2	1	5	28	194
Dimension $n = 12$						
Range a_i	$[2^{10}, 2^{11}]$	$[2^{12}, 2^{13}]$	$[2^{14}, 2^{15}]$	$[2^{16}, 2^{17}]$	$[2^{18}, 2^{19}]$	$[2^{20}, 2^{21}]$
Average time (s)	0	0	0	1	6	28
Max rhs ($\times 10^6$)	0.01	0.06	0.3	1.4	7	32

Table 3. Dependency on the range of a

Dimension $n = 10$									
k	1	4	16	64	256	1024	2^{12}	2^{14}	2^{16}
Average time (s)	0	0	0	0	0	0	1	1	1
Average max rhs ($\times 10^6$)	0.39	0.42	0.47	0.54	0.62	0.73	0.91	1.1	1.3
Average k-Frob ($\times 10^6$)	0.34	0.36	0.42	0.49	0.59	0.7	0.84	1.0	1.2
Dimension $n = 5$									
k	1	4	16	64	256	1024	2^{12}	2^{14}	2^{16}
Average time (s)	0	0	0	0	0	0	1	1	1
Average max rhs ($\times 10^6$)	0.79	0.99	1.3	1.7	2.4	3.4	4.9	6.9	9.8
Average k-Frob ($\times 10^6$)	0.78	0.95	1.2	1.6	2.3	3.2	4.6	6.5	9.2

Table 4. Dependency on k

8.3 Experiments about the k-Frobenius number $\mathrm{F}_k(a_1, a_2, a_3)$

We now want to make several experiments concerning the k-Frobenius number $\mathrm{F}_k(a)$ and express some interesting conjectures for future work. The case of $n = 2$, i.e., knapsacks with exactly two variables, is well known and has been studied by Beck and Robins [14]. They prove the following theorem.

Theorem 7. *Given a two-dimensional knapsack $a_1x_1 + a_2x_2$, the k-Frobenius number is*

$$g_{k-1}(a_1, a_2) = ka_1a_2 - a_1 - a_2,$$

where $g_k(a_1, a_2)$ is the largest right-hand-side b such that $a_1x_1 + a_2x_2 = b$ has exactly k integral solutions.

Note that one can easily express $\mathrm{F}_k(a)$ in terms of $g_k(a)$. Indeed $\mathrm{F}_k(a) = \max\{g_i(a) : i \leq k-1\}$. One can then wonder about the behavior of the sequence $\{g_i(a)\}_{i=0}^{\infty}$. For $n = 2$, [14] shows the sequence is increasing with respect to i for all index values.

The situation changes drastically for $n = 3$. There is no known explicit formula for $\mathrm{F}_k(a_1, a_2, a_3)$. It has also been proven that $g_i(a_1, a_2, a_3)$ is not necessarily increasing with i. For example, Brown et al. [16] indicated that $g_{14}(3, 5, 8) = 52$ whereas $g_{15}(3, 5, 8) = 51$ and therefore in that particular case $g_{14} > g_{15}$. Furthermore Shallit and Stankewicz [41] proved that for $i > 0$ and $n = 5$, the quantity $g_0 - g_i$ is arbitrarily large and positive. They also give an example of $g_0 > g_1$ for $n = 4$. In contrast, we prove the following theorem that, for $n = 3$, such a discrepancy does not exist and we always have $g_0 < g_1$.

Theorem 8. *Given $a_1 < a_2 < a_3 \in \mathbb{Z}_+$, we have*

$$g_0(a_1, a_2, a_3) < g_1(a_1, a_2, a_3).$$

To prove this theorem, we first consider the case in which all coefficients are pairwise relatively prime.

Lemma 15. *Let $a_1 < a_2 < a_3 \in \mathbb{Z}_+$ be such that all coefficients are pairwise relatively prime. Then*

$$g_0(a_1, a_2, a_3) < g_1(a_1, a_2, a_3).$$

Proof. Let us denote $f := g_0(a_1, a_2, a_3)$ as the Frobenius-number of the knapsack. This implies that

$$a_1x_1 + a_2x_2 + a_3x_3 = f \tag{17}$$

has no integral solution. On the other hand

$$a_1x_1 + a_2x_2 + a_3x_3 = f + a_1 \tag{18}$$

has at least one integral solution. We will prove that it cannot have two or more integral solutions. Let $\bar{x}$ be any integral solution to (18). Observe that $\bar{x}_1 = 0$, otherwise we could trivially construct an integral solution for (17). Therefore $\bar{x} = (0, \bar{x}_2, \bar{x}_3)$. Consider by contradiction that $\tilde{x} = (0, \tilde{x}_2, \tilde{x}_3)$ is another integral solution to (18). Then $a_2(\bar{x}_2 - \tilde{x}_2) + a_3(\bar{x}_3 - \tilde{x}_3) = 0$. In particular, since $\gcd(a_2, a_3) = 1$, this implies $|\bar{x}_2 - \tilde{x}_2| = la_3$ with l a natural number, which in turn implies that either $\bar{x}_2 \geq a_3$ or $\tilde{x}_2 \geq a_3$. Assume wlog that $\bar{x}_2 \geq a_3$, and since $\bar{x}_2$ is an integral solution to (18), this implies that $f + a_1 \geq a_2a_3$ and hence $f \geq a_2a_3 - a_1$ which is in contradiction with the fact that $f = g_0(a_1, a_2, a_3) \leq g_0(a_2, a_3) \leq g_0(a_2, a_3) = a_2a_3 - a_2 - a_3$.

The following theorem has been proven by Brown et al. [16] and we use it to our benefit:

Lemma 16. *Let $d = gcd(a_2, a_3)$ and $j \in \mathbb{Z}_+$ then either $g_j = dg_j(a_1, \frac{a_2}{d}, \frac{a_3}{d}) + (d-1)a_1$ or g_j is not defined, i.e. no right-hand-side achieves exactly j integral solutions.*

Proof. (of Theorem 7) Consider a triple (a_1, a_2, a_3). If the coefficients are pairwise relatively prime, the result follows from Lemma 15. Assume that there is some gcd different from 1 for a pair of coefficients. From Lemma 16, we can get rid of the gcd and that does not change the relative order between g_0 and g_1. By applying at most three times Lemma 16, we come back to the case where all coefficients are pairwise relatively prime and the result follows.

We now know that $g_0 < g_1$ when $n = 3$. We use our computational tool to conjecture what is the smallest j such that an inversion $g_j > g_{j+1}$ (monotonicity is broken) occurs for some triple of coefficients. We have drawn 10000 triples of coefficients in the range $[2, 42]$. In 54% of the cases, the g_j's were increasing with j until $j = 1000$. The minimum j reached for which $g_j > g_{j+1}$ is $j = 14$. This occurred in 15 cases. But all of these cases can be proven to be equivalent, from Lemma 16, to the case of the triple $(3, 5, 8)$. The same conclusion was reached on another test with coefficients in the range $[2, 1000]$. Interestingly, the second smallest j for which $g_j > g_{j+1}$ was $j = 17$ and all triples can be proven to be equivalent to $(2, 5, 7)$. Thus we conjecture:

Conjecture: *For any triple of positive integers $a = (a_1, a_2, a_3)$ the sequence of numbers the sequence $\{g_i(a)\}_{i=0}^{\infty}$ is monotonically increasing with i, for $i \leq 14$.*

Finally we evaluate empirically how the k-Frobenius number evolves. In particular, it is known that $F_k(a_1, a_2, a_3) \approx c_{3,k}\sqrt{a_1 a_2 a_3}$. We now use the code to observe this behaviour and empirically obtain a value for $c_{3,k}$. We have drawn 1000 triples of coefficients in the range $[2, 1000]$. For each triple, we have computed the k-Frobenius number for $k = 1, 2, 16, 1024, 65536$. We observe in this case that $F_k \approx c_{3,k}\sqrt{a_1 a_2 a_3}$ as expected. In Figure 1, we represent, with a logarithmic scale, the product $a_1 a_2 a_3$ on the x-axis and the k-Frobenius on the y-axis for the respective values of k. In

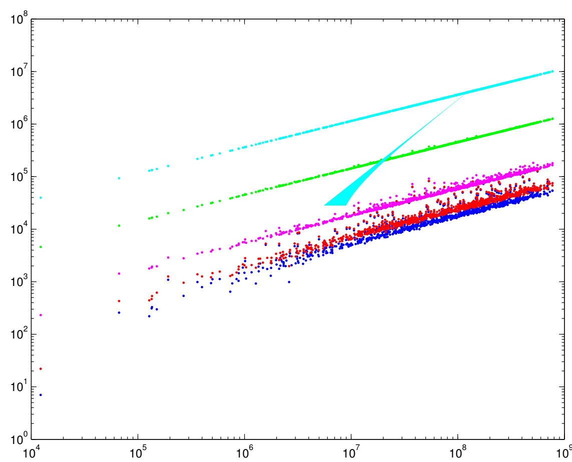

Fig. 1. Value of the k-Frobenius (over the y-axis) with respect to the product $a_1 a_2 a_3$ for $a_i \in [2, 1000]$ for $k = 1, 2, 16, 1024, 65536$.

order to assess an approximate value for $c_{3,k}$ we now perform a linear regression over $\log(a_1 a_2 a_3)$ and $\log(F_k(a_1, a_2, a_3))$ whose results is shown in the following table.

$F_k(a_1,a_2,a_3) \approx c_{3,k}(a_1a_2a_3)^{r_k}$		
k	$c_{3,k}$	r_k
1	0.67	0.56
2	1.12	0.55
16	4.54	0.52
1024	44.7	0.5
65536	362	0.5

Finally, we want to empirically compare the behaviour of $F_k(a_1, a_2, a_3)$ with respect to $g_{k-1}(a_1, a_2, a_3)$. For 1000 triples of coefficients respectively drawn in the interval $[2, 100]$ and $[2, 1000]$, we count the proportion of times that g_k is undefined and the proportion of times that $F_k(a_1, a_2, a_3) = g_{k-1}(a_1, a_2, a_3)$ for different values of k. The results are proposed in the following table.

		Proportion of times that		
a	k	g_k undefined	$F_k = g_{k-1}$	$F_k \neq g_{k-1}$
$[2, 100]$	100	6%	93%	1%
$[2, 100]$	1000	19%	78%	3%
$[2, 100]$	10000	43%	53%	4%
$[2, 100]$	30000	53%	44%	3%
$[2, 100]$	60000	63%	35%	2%
$[2, 1000]$	100	0.1%	99.9%	0
$[2, 1000]$	1000	1.3%	98.2%	0.5%
$[2, 1000]$	10000	5%	92%	3%
$[2, 1000]$	30000	7%	89%	4%
$[2, 1000]$	60000	9%	85%	6%

Finally in Figure 2, we report the difference $F_{60000} - g_{59999}$ for all cases in which the two values are different and where the coefficients are drawn in $[2, 1000]$. The x-axis is again the product $a_1a_2a_3$. We observe that the difference is very often very small with respect to F_k.

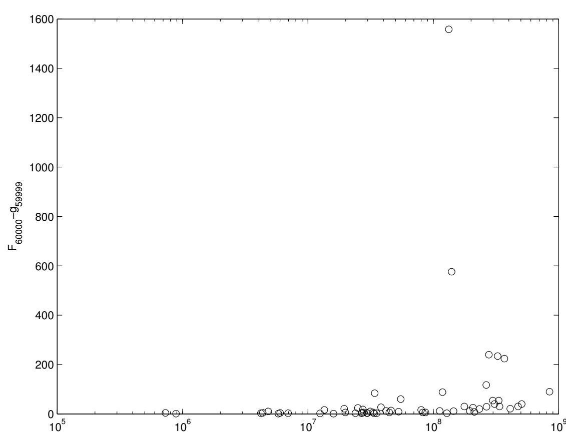

Fig. 2. Value of $F_{60000} - g_{59999}$ with respect to $a_1a_2a_3$ in 59 cases (over 1000) in which it is nonzero

9 Acknowledgements

We are truly grateful to Lenny Fukshansky, Martin Henk, and Matthias Köppe for their comments, encouragement and corrections that improve the paper we present today. Some of our results were announced in [7].

References

1. 4ti2 team. `4ti2`–Software package for algebraic, geometric and combinatorial problems on linear spaces. Available at `http://www.4ti2.de/`.
2. K. Aardal and A. K. Lenstra. Hard equality constrained integer knapsacks. In *Integer programming and combinatorial optimization, Lecture Notes in Comput. Sci. Springer*. (2002), 350–366.
3. I. Aliev, L. Fukshansky and M. Henk, Generalized Frobenius Numbers: Bounds and Average Behavior, *Acta Arith.*, 155 (2012), 53–62.
4. I. Aliev and M. Henk, Feasibility of integer knapsacks, *SIAM J. Optimization*, 20 (2010), 2978–2993.
5. I. Aliev, M. Henk and E. Linke, Integer Points in Knapsack Polytopes and s-covering Radius, *Electron. J. Combin.*, 20 (2013), no. 2, Paper 42, 17 pp.
6. I. Aliev, R. Bassett, J. A. De Loera, Q. Louveaux. A Quantitative Doignon-Bell-Scarf Theorem. Available at ArXiv:1405.2480.
7. I. Aliev, J. A. De Loera, Q. Louveaux. Integer Programs with Prescribed Number of Solutions and a Weighted Version of Doignon-Bell-Scarf's Theorem, to appear in the Proceedings of IPCO 2014.
8. V. Barucci, Numerical semigroup algebras. In Multiplicative Ideal Theory in Commutative Algebra (J.W. Brewer, S. Glaz, H. Heinzer and B. Olberding eds.) Springer (2006), p. 39-53.
9. D. Beihoffer, J. Hendry, A. Nijenhuis and S. Wagon, Faster Algorithms for Frobenius Numbers, Electronic Journal of Combinatorics, Volume 12 (2005), Research paper #R27
10. Barvinok, A.I. *A course in convexity*, American Math. Soc., Graduate studies in Mathematics, Providence RI, vol. 54, (2002).
11. A. I. Barvinok. Polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Math. of Operations Research* **19** (1994), 769–779.
12. A. I. Barvinok and K. Woods. Short rational generating functions for lattice point problems. *J. Amer. Math. Soc.* **16** (2003), 957–979.
13. D.E. Bell (1977). A theorem concerning the integer lattice. *Studies in Applied Mathematics*, 56(1).
14. M. Beck, S. Robins, A formula related to the Frobenius problem in two dimensions, *Number theory* (New York, 2003), 171-23, Springer, New York, 2004.
15. D. Beihoffer, J. Hendry, A. Nijenhuis, S. Wagon. Faster algorithms for Frobenius numbers, *Electron. J. Combin*, 12(1), 2005.
16. A. Brown, E. Dannenberg, J. Fox, J. Hanna, K. Keck, A. Moore, Z. Robbins, B. Samples, J. Stankewicz, On a generalization of the Frobenius number. *Journal of Integer Sequences*, 13(2), 3, 2010.
17. W. Bruns, J. Gubeladze and N. V. Trung. Problems and algorithms for affine semigroups. *Semigroup Forum* **64** (2002), 180–212.
18. B. Nill. Lattice polytopes having h^*-polynomials with given degree and linear coefficient, *European Journal of Combinatorics*, 29: 1596–1602, 2008.
19. W. Bruns and R. Koch. `NORMALIZ`, computing normalizations of affine semigroups, Available from `ftp://ftp.mathematik.uni-osnabrueck.de/pub/osm/kommalg/software/`.
20. D. Cox, J. Little, and D. O'Shea Ideals, Varieties and Algorithms, Undergraduate Texts in Mathematics, Springer, New York, 1992.
21. J. A. De Loera, R. Hemmecke, J. Tauzer, and R. Yoshida. Effective lattice point counting in rational convex polytopes, *Journal of Symbolic Computation*, 38(4):1273–1302, 2004.
22. J. A. De Loera, D. C. Haws, R. Hemmecke, P. Huggins, B. Sturmfels, and R. Yoshida. Short rational functions for toric algebra and applications. *Journal of Symbolic Computation*, 38(2):959–973, 2004.
23. J.A. De Loera, R. Hemmecke, M. Köppe, Algebraic and geometric ideas in the theory of discrete optimization. MOS-SIAM Series on Optimization, 14. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA; Mathematical Optimization Society, Philadelphia, PA, 2013. xx+322 pp.

24. A. Dobra, A. F. Karr, and P. A. Sanil, Preserving confidentiality of high-dimensional tabulated data: statistical and computational issues. *Stat. Comput.* **13** (2003), 363–370.
25. J-P. Doignon, Convexity in cristallographical lattices, *Journal of Geometry* 3.1 (1973): 71–85.
26. F. Eisenbrand and N. Hähnle, Minimizing the number of lattice points in a translated polygon in *Proceedings of SODA* (2013),1123–1130.
27. L. Fukshansky, A. Schürmann, Bounds on generalized Frobenius numbers, *European J. Combin.*, 3 (2011), 361–368.
28. C. Haase, B. Nill, and S. Payne, Cayley decompositions of lattice polytopes and upper bounds for h^*-polynomials, *J. Reine Angew. Math.* 637 (2009), 207–216.
29. R. Hemmecke, A. Takemura, and R. Yoshida Computing holes in semi-groups and its application to transportation problems. *Contributions to Discrete Mathematics*, 4 (2009), 81–91.
30. M. Henk, R. Weismantel, On Hilbert bases of polyhedral cones, Preprint SC 96-12, Konrad-Zuse-Zentrum fr Informationstechnik, Berlin, April 1996. www.zib.de/bib/pub/pw/index.en.html.
31. R. Kannan, Lattice translates of a polytope and the Frobenius problem, *Combinatorica*, **12**(2)(1992), 161–177.
32. A. G. Khovanskii, *The Newton polytope, the Hilbert polynomial and sums of finite sets* , Funktsional. Anal. i Prilozhen. **26** (1992), no. 4, 57–63.
33. J.C. Lagarias and G.M. Ziegler, Bounds for lattice polytopes containing a fixed number of interior points in a sublattice. *Canad. J. Math.* 43 (1991), no. 5, 1022–1035.
34. I. Pak and E. Vallejo, Combinatorics and geometry of Littlewood-Richardson cones, *Europ. J. Combinatorics*, vol. 26 (2005), 995–1008
35. O. Pikhurko, Lattice points in lattice polytopes. *Mathematika* 48 (2001), no. 1-2, 1524 (2003).
36. J.L. Ramírez Alfonsín, Gaps in semigroups, *Discrete Mathematics*, 308 (18) (2008), 4177–4184
37. J. L. Ramírez Alfonsín, Complexity of the Frobenius problem, *Combinatorica*, **16** (1996), no. 1, 143–147.
38. J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem, Oxford Lecture Series in Mathematics and Its Applications, Oxford University Press, New York, 2006.
39. A. Schrijver, Theory of linear and integer programming. Wiley, 1998.
40. H.E. Scarf, An observation on the structure of production sets with indivisibilities, *Proceedings of the National Academy of Sciences* 74.9 (1977): 3637–3641.
41. J. Shallit, J. Stankewicz, Unbounded discrepancy in Frobenius numbers. *Integers*, 11(1), 27-34, 2011.
42. R.P. Stanley Combinatorics and Commutative Algebra. Second edition. Progress in Mathematics, 41. Birkhäuser, Boston, 1996.
43. B. Sturmfels Gröbner Bases and Convex Polytopes, University Lecture Series, vol. 8, AMS, Providence RI, 1995.
44. A. Takemura and R. Yoshida. A generalization of the integer linear infeasibility problem. *Discrete Optimization.* **5** (2008), 36–52.