Forall-exist statements in pseudopolynomial time

Eleonore Bach * Friedrich Eisenbrand † Thomas Rothvoss ‡
Robert Weismantel §

Abstract

Given a convex set $Q \subseteq \mathbb{R}^m$ and an integer matrix $W \in \mathbb{Z}^{m\times n}$, we consider statements of the form $\forall b \in Q \cap \mathbb{Z}^m \ \exists x \in \mathbb{Z}^n$ s.t. $Wx \leq b$. Such statements can be verified in polynomial time with the algorithm of Kannan and its improvements if n is fixed and Q is a polyhedron. The running time of the best-known algorithms is doubly exponential in n. We provide a pseudopolynomial-time algorithm if m is fixed. Its running time is $(m\Delta)^{O(m^2)}$ where Δ is the largest absolute value of an entry in W. Furthermore it applies to general convex sets Q.

1 Introduction

An *integer linear program (ILP)* is a discrete optimization problem of the following kind

$$\max\left\{c^T x : Ax = b,\, x \geq \mathbf{0},\, x \in \mathbb{Z}^n\right\} \tag{1.1}$$

where $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$ and $c \in \mathbb{Z}^n$. Many algorithmic problems can be modeled and solved as an integer program. Integer programming is a showcase of progress and development in the field of *algorithms and complexity*. If the number of variables in (1.1) is fixed, then Lenstra-type algorithms [19, 14] solve integer programming in polynomial time. The recent result of Reis and Rothvoss [21], together with an algorithm of Dadush [7] has a running time of $(\log n)^{O(n)}$ times a polynomial in the binary encoding-length of the input.

In 1982 Papadimitriou [20] has shown that such integer programs in standard form can be solved in pseudopolynomial time, if the number m of rows of $A \in \mathbb{Z}^{m\times n}$ is fixed. The running time of Papadimitriou's algorithm is $(m\Delta)^{O(m^2)}$, where Δ is the largest absolute value of an entry of A. Papadimitriou's algorithms was recently improved. Standard form IPs can be solved in time $(m\Delta)^{O(m)}$, see [9, 13]. Knop, Pilipczuk, and Wrochna [17] showed that this running time is optimal up to constants in the exponent. This lower bound is assuming the exponential-time-hypothesis [12]. In presence of upper bounds on the variables, the best-known pseudopolynomial-time algorithms [9] still have a complexity of $(m\Delta)^{O(m^2)}$. Whether this running time is optimal, is a highly visible open problem.

Central to this paper are *forall-exist statements* of the form

$$\forall b \in Q \cap \mathbb{Z}^m \ \exists x \in \mathbb{Z}^n \quad \text{s.t.} \quad Wx \leq b, \tag{1.2}$$

where $Q \subseteq \mathbb{R}^m$ is a given convex set and $W \in \mathbb{Z}^{m\times n}$ is a given integer matrix.

Forall-exist statements are a substantial generalization of integer programming. For a given right-hand-side $b \in \mathbb{Z}^m$ and $Q = \{b\}$ deciding correctness of the statement (1.2) is an integer feasibility problem. It comes as no surprise that problem (1.2) belongs to the second level of the polynomial hierarchy and is Π_2-complete [23, 24]. Kannan [15] provided an algorithm to decide forall-exist statements that runs in polynomial time if the dimension n (number of columns of W) and m are fixed. Eisenbrand and Shmonin [8] extended this result to the case where only n is assumed to be a constant.

Forall-exist statements are of interest in several scientific disciplines. A classical example from number theory is the *Frobenius problem* [15]. Recently, forall-exist statements are of increasing importance in the field of *fixed-parameter complexity* see, e.g. [10, 16]. A nice application is in the scope of *fair allocations* [4, 5].

*EPFL, Switzerland, eleonore.bach@epfl.ch
†EPFL, Switzerland, friedrich.eisenbrand@epfl.ch
‡University of Washington, USA, rothvoss@uw.edu. Supported by NSF grant 2318620: *The Geometry of Integer Programming and Lattices.*
§ETH Zürich, Switzerland, robert.weismantel@ifor.math.ethz.ch

Contributions Our main result is a pseudopolynomial time algorithm to decide forall-exist statements in the case where the number m of rows of the matrix $W \in \mathbb{Z}^{m\times n}$ is fixed. More precisely, the novel contributions of this paper are the following.

i) We show that a decision problem (1.2) can be decided in time $(m\Delta)^{O(m^2)}$. Here Δ is the largest absolute value of a component of W. In case that the answer is negative, our algorithm provides a $b \in Q \cap \mathbb{Z}^m$ so that the system $Wx \leq b,\ x \in \mathbb{Z}^n$ is infeasible.

This result is via a sequence of reductions that leads to a conjunction of simpler forall-exist statements, for which the domain of the $\exists$-quantifyer is a finite set of integer vectors. The number of such sub-problems itself is

$$\binom{n}{m} \cdot (m\Delta)^{O(m)} = (m\Delta)^{O(m^2)}.$$

The last equality follows form the fact that we can assume that W does not have repeated columns and hence $n \leq (2\Delta + 1)^m$.

This running time is not higher than state-of-the-art algorithms for integer programming with lower and upper bounds on its variables [9] in the pseudopolynomial-time regime where m is fixed. In particular, the algorithm presented here does not show double exponential dependence on the number of variables. The *ETH*-based lower bound of Knop et al. [17] of $(m\Delta)^{\Omega(m)}$ for integer programming problems (1.1) transfers to the same lower bound for forall-exist problems (1.2), by setting $Q = \{b\}$, the right-hand-side of (1.1).

ii) A novel feature of our algorithm is that it applies to general convex sets $Q \subseteq \mathbb{R}^m$, whereas Kannan's algorithm is described and analyzed for polyhedra only.

The analysis of algorithms involving a convex set Q requires a fair amount of technical care, see, e.g. [11]. We need to be able to solve the following problems involving Q. Our algorithm generates rational polyhedra $P \subseteq \mathbb{R}^m$ for which it needs to decide whether $Q \cap P$ contains an integer point, or for a given $x^* \in P$ it has to decide membership in Q. For the latter task, it is enough to have access to Q in form of a *membership oracle* [11]. A query to this oracle has cost 1. The former task is more subtle. Using the state of the art integer programming algorithm [21] this question can be decided in time $(\log m)^{O(m)}$ times a polynomial in $\log(R)$ where $R > 1$ is the radius of a ball containing Q. We abstract from such a detailed running time analysis by accounting cost 1 for this task as well.

We also provide new structural results on specific forall-exist problems that have attracted recent attention [6, 2]. The *diagonal Frobenius number* of a pointed cone $\mathrm{cone}(W) = \{Wx \colon x \in \mathbb{R}^n_{\geq 0}\}$ where $W \in \mathbb{Z}^{m\times n}$, is the smallest $t^* \geq 0$ such that one has the following: For all $c \in \mathrm{cone}(W) \cap \mathbb{Z}^m$ that are conic combinations derived with weights more than t^* in every generator one has that these points are *integer conic combinations* as well.

iii) We show a bound on the diagonal Frobenius number of $(m\Delta)^{O(m)}$ which yields an improvement of the previous-best bound of Aliev and Henk [2] in our parameter setting.

Comparison with the polynomial-time algorithm in fixed dimension The breakthrough of Kannan [15] and its subsequent improvements [8] is a polynomial time algorithm if the dimension n (number of columns of W) is fixed. The running time of these algorithms is doubly exponential in the number of variables n. More precisely, these algorithms require a running time of at least

$$(m \log \Delta)^{2^n}. \tag{1.3}$$

To the best of our knowledge, this is the only algorithm with a nontrivial analysis of its running time that is available for tackling forall-exist statements with fixed m and Δ. If all of n, m and Δ are fixed, a recent paper by Koutecký and Talmon [18] shows that the problem is FPT.

By ignoring the dependence on the binary encoding-length of Δ and dropping constants, the achieved running time (1.3) of Kannan's algorithm [15] can be lower-bounded by $\Omega(m^{2^n})$. Then, up to constant factors, one can see that our algorithm is more efficient in the parameter-range

$$m^2 \log(m\Delta) \leq 2^n \log(m). \tag{1.4}$$

The number m (rows of W) can in principle be exponential in the number of variables n. This is a setting, where Kannan's algorithm is more efficient than our pseudopolynomial-time algorithm. Another interesting setting is when $m \leq n^k$ for some constant k. This applies, for example in the context of fair allocation [4]. To illustrate the efficiency of our algorithm in this case, we can assume that Δ is at least m. If the left-hand-side of (1.4) exceeds the right-hand-side, then

$$2n^{2k}\log(\Delta) > 2^n \quad \iff \quad \log(\Delta) > 2^{n-2k\log n-1}.$$

Since k is a constant, this means that Δ has to be **doubly-exponential** in n. In other words, the number of bits to encode the largest entry of W has to be *exponential* in n. Outside of this regime and under the assumption that m is polynomial in n, the algorithm proposed here is more efficient in terms of worst-case running time.

2 A birds-eye perspective on our approach

Our main result is via a sequence of reductions. The details of this reduction are explained in Section 3. We start here by recalling the starting point and then describe the final problem in this sequence and its solution, thereby providing an overview as well as a first algorithmic result. Throughout $Q \subseteq \mathbb{R}^m$ denotes a convex set and $W \in \mathbb{Z}^{m\times n}$ denotes an integer matrix with $\|W\|_\infty \leq \Delta$. We are concerned with the following decision problem.

Given $Q \subseteq \mathbb{R}^m$ and $W \in \mathbb{Z}^{m\times n}$, decide whether

$$\forall b \in Q \cap \mathbb{Z}^m \quad \text{there exists} \quad x \in \mathbb{Z}^n \quad \text{with} \quad Wx \leq b. \tag{2.5}$$

Our main result is a reduction of problem (2.5) to $\binom{n}{m}\cdot(m\cdot\Delta)^{O(m)}$ many simpler forall-exist problems of the following kind.

Given a convex set $Q \subseteq \mathbb{R}^m$, and a *finite* set $\mathcal{C} \subseteq \mathbb{Z}^m$ with $\|\mathcal{C}\|_\infty \leq (m\cdot\Delta)^{O(m)}$. Decide the validity of the statement

$$\forall b \in Q \cap \mathbb{Z}^m \, \exists c \in \mathcal{C} \colon c \leq b. \tag{2.6}$$

Here $\|\mathcal{C}\|_\infty$ denotes the largest infinity norm of an element in $\mathcal{C}$. Notice that in contrast to the forall-exist statement of our departure, the domain of the variable in the scope of the $\exists$-quantifier at the end-of our reduction is *finite*. In fact $|\mathcal{C}| \leq (m\Delta)^{O(m^2)}$ follows from a counting argument. The running time that is necessary to generate $\binom{n}{m}\cdot(m\cdot\Delta)^{O(m)}$ many simpler forall-exist problems will be $\binom{n}{m}\cdot(m\cdot\Delta)^{O(m)}$ as well. Figure 1 illustrates the exist statement (2.6).

We conclude here by showing that (2.6) can be solved in time $(m\cdot\Delta)^{O(m^2)}$.

THEOREM 2.1. *A forall-exist statement* (2.6) *can be decided in time* $(m\cdot\Delta)^{O(m^2)}$.

Proof. The goal is to find a *counter-example*, i.e., an integer point $b \in Q \cap \mathbb{Z}^m$ such that for every $c \in \mathcal{C}$, there exists an index $i \in \{1,\dots,m\}$ such that $b_i < c_i$. Since all numbers are integers, the latter condition is equivalent to $b_i \leq c_i - (1/2)$. We now consider the hyperplane arrangement defined by the axis-parallel hyperplanes

$$H_c^i = \{x \in \mathbb{R}^m \colon x_i = c_i - (1/2), \quad c \in \mathcal{C}, i \in \{1,\dots,m\}\}. \tag{2.7}$$

This partitions $\mathbb{R}^m$ into finite and infinite cells. Let us describe these cells precisely. For every component $i \in \{1,\dots,m\}$, let $\{c_i \colon c \in \mathcal{C}\}$ be the set of i-th components of elements of $\mathcal{C}$. Let $\ell_i^1 < \cdots < \ell_i^{k_i}$ be an ordering of this set. A cell $\mathcal{V}$ is then determined by a tuple

$$(j_1,\dots,j_m) \in \{0,\dots,k_1\} \times \cdots \times \{0,\dots,k_m\}$$

and it has the form

$$\mathcal{V} = \left\{x \in \mathbb{R}^m \colon \ell_i^{j_1} - (1/2) \leq x_i \leq \ell_i^{j_1+1} - (1/2)\right\},$$

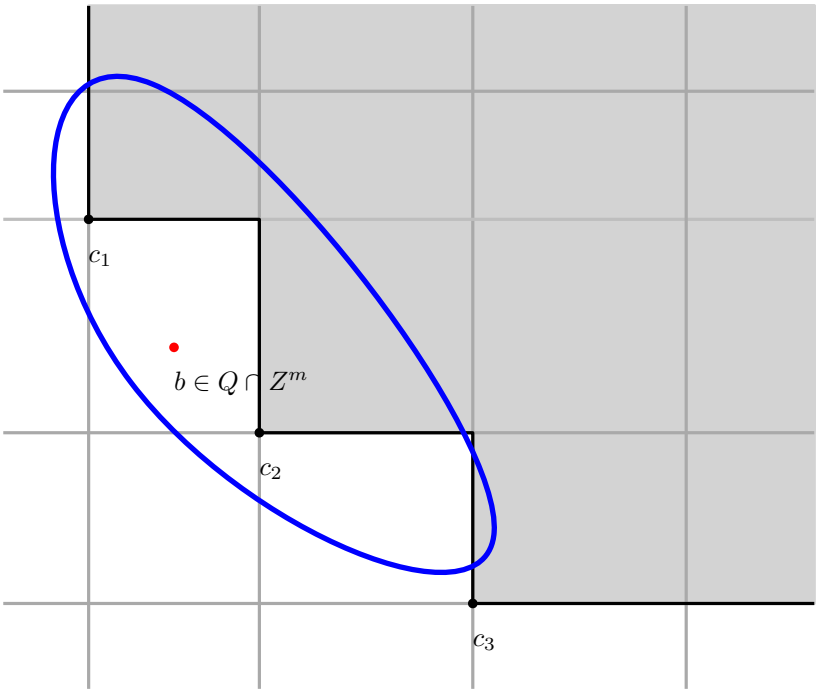

Figure 1: A schematic picture of problem (2.6). The set Q is drawn in blue. The elements of the set $\mathcal{C}$ are c_1, c_2 and c_3. The area in grey corresponds to all points $x \in \mathbb{R}^m$ such that there exists a $c \in \mathcal{C}$ with $c \leq x$. The point b in red is an integral point in Q that is not contained in the grey area and hence is a counter-example of the validity of the corresponding forall-exist statement.

where $\ell_i^0 = -\infty$ and $\ell_i^{k_i+1} = +\infty$. A potential counter-example must lie in the interior of a cell $\mathcal{V}$, since it is integral. Furthermore, the interior of $\mathcal{V}$ either is fully contained in the union of the cones

$$\bigcup_{c \in \mathcal{C}} \left((c - \frac{1}{2}\mathbf{1}) + \mathbb{R}^m_{\geq 0} \right), \tag{2.8}$$

or it is disjoint from this possibly non-convex set. To find a counterexample, we iterate over all cells $\mathcal{V}$. One iteration is as follows.

A) We check whether the interior of $\mathcal{V}$ is contained in the union (2.8). This is the case if and only if an arbitrary point from its interior is contained in one of the cones.

B) In the case in which the interior is not contained in one of the cones, we check whether the integer program

$$\mathcal{V} \cap Q \cap \mathbb{Z}^m \tag{2.9}$$

is feasible. If this is true, a counterexample has been detected and we can stop the process.

The integer program (2.9) can be solved in time $(\log m)^{O(m)}$ [21] which is dominated by our final running time. It remains to be shown that the number of cells is bounded by $(m\Delta)^{O(m^2)}$. Clearly, the number of cells is equal to

$$\prod_{i=1}^{m} (k_i + 1).$$

Since the infinity norm of each $c \in \mathcal{C}$ is bounded by $(m\Delta)^{O(m)}$, one has $k_i \leq (m\Delta)^{O(m)}$ and therefore, the number of cells is bounded by $(m\Delta)^{O(m^2)}$. □

3 The sequence of reductions

The goal of this section is to provide a proof of the following assertion.

THEOREM 3.1. *There exists an algorithm that transforms a forall-exist statement* (1.2) *into an equivalent conjunction of*

$$\binom{n}{m} \cdot (m\Delta)^{O(m)} \tag{3.10}$$

many forall-exist statements (3.12)*. The running time of the algorithm is bounded by* $(m\Delta)^{O(m^2)}$*.*

REMARK 1. *The running time of the algorithm of* $(m\Delta)^{O(m^2)}$ *is potentially higher than the number of problems* (3.12) *in the conjunction. In short, this is because we explicitly enumerate the set* $\mathcal{C}$*. The bound on the infinity norm of* $(m\Delta)^{O(m)}$ *for each element of* $\mathcal{C}$ *yields a straight-forward bound of* $|\mathcal{C}| = (m\Delta)^{O(m^2)}$*.*

We start with a standard transformation that is more convenient for us, as we use the concepts of a finitely generated cone and of a finitely generated integer cone. The *cone* generated by the column vectors of a matrix $C \in \mathbb{Z}^{m\times n}$ is the set $\text{cone}(C) = \{Cx : x \in \mathbb{R}^n_{\geq 0}\}$. The *integer cone* $\text{intcone}(C)$ is defined as $\text{intcone}(C) = \{Cx \colon x \in \mathbb{Z}^n_{\geq 0}\}$. The following is a very important key concept. If $C \in \mathbb{Z}^{m\times m}$ is non-singular, then

$$\text{intcone}(C) = \text{cone}(C) \cap \Lambda(C). \tag{3.11}$$

Here $\Lambda(C) = \{Cx \colon x \in \mathbb{Z}^m\}$ is the *(full-dimensional) lattice* generated by C. The matrix C is called *basis* of $\Lambda(C)$.

We re-write the condition $x \in \mathbb{Z}^n$, $Wx \leq b$ as $x' \in \mathbb{Z}^{n'}_{\geq 0}$, $W'x' = b$. In this way, the latter condition $x' \in \mathbb{Z}^{n'}_{\geq 0}$, $W'x' = b$ can be written as $b \in \text{intcone}(W')$. Notice that $\|W'\|_\infty = \|W\|_\infty$ and that $\text{rank}(W') = m$. We can thus assume, without loss of generality, that our forall-exist statement is as follows.

Given $Q \subseteq \mathbb{R}^m$, $W \in \mathbb{Z}^{m\times n}$ of rank m, decide whether

$$\forall b \in Q \cap \mathbb{Z}^m \colon b \in \text{intcone}(W). \tag{3.12}$$

3.1 Enforcing $\mathbf{Q \subseteq \text{cone}(W)}$ Suppose that there exists an element in $(Q \setminus \text{cone}(W)) \cap \mathbb{Z}^m$. Then this element is a counterexample to (3.12). We begin by excluding such counterexamples that are outside of $\text{cone}(W)$ by preprocessing via integer programming techniques.

More precisely, this is done by solving integer feasibility problems

$$Q \cap \left\{x \in \mathbb{Z}^m \colon a^T x \geq 1\right\} \neq \emptyset$$

for each integral facet-defining inequality $a^T x \leq 0$ of $\text{cone}(W) \subseteq \mathbb{R}^m$. As described in the introduction, we account for a running time of 1 for this test. If Q was explicitly given as a rational polyhedron, then this test can be carried out in time $(\log m)^{O(m)}$ times a polynomial in $\log \Delta$ and the binary encoding length of the description of Q. Apart from the latter factor, this is dominated by our running time.

The number of facets is bounded by $\binom{n}{m}$ and the facets can be enumerated in this time-bound as well, see, e.g. [22]. From now on, we can assume that $Q \subseteq \text{cone}(W)$.

3.2 Reduction to simplicial cones *Carathéodory's theorem*, see, e.g. [22] guarantees that each b in $\text{cone}(W)$ is contained in $\text{cone}(W_B)$ for a basis $B \subseteq \{1, \ldots, n\}$ of W. Here a *basis* W_B of W is a selection of m linearly independent columns of W. Clearly, the forall-exist statement (3.12) over $Q \subseteq \text{cone}(W)$ holds, if and only if it holds over all sets $Q \cap \text{cone}(W_B)$. The number of sets $Q \cap \text{cone}(W_B)$ is bounded by $\binom{n}{m}$.

Our next lemma shows that, in each of these statements over $Q \cap \text{cone}(W_B)$, we can *almost* replace the condition $x \in \text{intcone}(W)$ by $x \in \text{intcone}(W_B)$.

LEMMA 3.1. *Let $b \in \text{cone}(W_B) \cap \mathbb{Z}^m$, then $b \in \text{intcone}(W)$ if and only if there exists an element $v \in \text{intcone}(W)$ of norm $\|v\|_\infty \leq (m\Delta)^{O(m)}$ such that $b - v \in \text{intcone}(W_B)$.*

The proof relies on the following theorem.

THEOREM 3.2. (THEOREM 3.3 IN [9]) *Consider a feasible integer program of the form*

$$\max \left\{ c^T x : Ax = b,\, x \geq \mathbf{0},\, x \in \mathbb{Z}^n \right\} \tag{3.13}$$

where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$ and $c \in \mathbb{Z}^n$ with $\|A\|_\infty \leq \Delta$. Let $x^* \in \mathbb{R}^n_{\geq 0}$ be an optimal fractional vertex solution of the linear programming relaxation. There exists an optimal solution $z^* \in \mathbb{Z}^n_{\geq 0}$ of the integer program (3.13) such that $\|z^* - x^*\|_1 \leq m(2m\Delta + 1)^m$.

Proof. [Proof of Lemma 3.1] If there exists an element $v \in \text{intcone}(W)$ with $b - v \in \text{intcone}(W_B)$, then

$$b \in v + \text{intcone}(W_B) \subseteq \text{intcone}(W).$$

Conversely, let $b \in \text{cone}(W_B)$. Then $b \in \text{intcone}(W)$ is equivalent to the fact that the following integer program is feasible

$$\max \left\{ \mathbf{0}^T x \colon Wx = b,\, x \in \mathbb{Z}^n_{\geq 0} \right\}. \tag{3.14}$$

Since $b \in \text{cone}(W_B)$, there exists an optimal vertex solution $x^* \in \mathbb{R}^n_{\geq 0}$ of the linear programming relaxation of (3.14) has positive entries only in components $i \in B$. With Theorem 3.2 it follows that there exists an integer (optimal) solution $z^* \in \mathbb{Z}^n_{\geq 0}$ with

$$\|z^* - x^*\|_1 \leq m(2m\Delta + 1)^m.$$

This means that b can be decomposed as $b = u + v$, where $u \in \text{intcone}(W_B)$ and $v \in \text{intcone}(W_{NB})$ such that

$$v = W_{NB} \cdot z^*_{NB}.$$

Here we rely on usual notation: W_{NB} is the matrix composed by the columns of W that are indexed by $NB = \overline{B}$ and z^*_{NB} is analogously composed of z^*. Notice that $\|z^*_{NB}\|_1 = \|z^*_{NB} - x^*_{NB}\|_1 \leq (m\Delta)^{O(m)}$. Therefore

$$\|v\|_\infty = \|W_{NB} \cdot z^*_{NB}\|_\infty \leq (m\Delta)^{O(m)}.$$

□

Let us define $\mathscr{C} \subseteq \text{intcone}(W)$ as the set of all elements of $\text{intcone}(W)$ of infinity norm bounded by $(m\Delta)^{O(m)}$. Notice that this set has cardinality $(m\Delta)^{O(m^2)}$. The above discussion shows that the statement (3.12) is equivalent to the conjunction over $\binom{n}{m} \cdot (m\Delta)^{O(m)}$ statements of the following form.

Given $W \in \mathbb{Z}^{m \times m}$ of rank m, $Q \subseteq \text{cone}(W)$ convex and $\mathscr{C} \subseteq \mathbb{Z}^m$, where $\|\mathcal{C}\|_\infty \leq (m\Delta)^{O(m)}$, decide whether

$$\forall b \in Q \cap \mathbb{Z}^m \quad \exists c \in \mathscr{C} \quad \text{such that} \quad b - c \in \text{intcone}(W) \tag{3.15}$$

3.3 Partitioning in residue classes of $\Lambda(W)$ Recall that $\Lambda(W) = \{Wx \colon x \in \mathbb{Z}^m\}$ is the lattice generated by the non-singular and integral matrix $W \in \mathbb{Z}^{m \times m}$. The *fundamental parallelepiped* $\Pi(W)$ is the set

$$\Pi(W) := \{W\lambda \colon \lambda \in [0,1)^m\}.$$

The volume of $\Pi(W)$ is equal to $|\det(W)|$ and corresponds to the number of integer points in $\Pi(W)$. The Hadamard inequality shows that $|\det(W)| \leq (m\Delta)^{O(m)}$. The lattice $\mathbb{Z}^m$ can be partitioned into residue classes modulo $\Lambda(W)$

$$\mathbb{Z}^m = \bigcup_{p \in \Pi(W) \cap \mathbb{Z}^m} (p + \Lambda(W)).$$

See, e.g. [3] for further details. Furthermore, we can assume that each element of $\Pi(W)$ has infinity norm bounded by $m \cdot \Delta$. This shows that the decision problem (3.15) can be reduced to the conjunction of $(m\Delta)^{O(m)}$ decision problems of the following kind, each parameterized by a representative $p \in \Pi(W) \cap \mathbb{Z}^m$ in the fundamental parallelepiped.

Given $W \in \mathbb{Z}^{m\times m}$ of rank m, $p \in \Pi(W) \cap \mathbb{Z}^m$, $Q \subseteq \text{cone}(W)$ convex and $\mathscr{C} \subseteq \mathbb{Z}^m$, decide whether

$$\forall b \in Q \cap (\Lambda(W) + p) \quad \exists c \in \mathscr{C} \quad \text{such that} \quad b - c \in \text{intcone}(W). \tag{3.16}$$

The number of decision problems of the form (3.16) to which (3.12) reduces to is $(m\Delta)^{O(m^2)}$ and the running time involved to arrive at these sub-problems is in the same order of magnitude. This decision problem is now the point of departure of the final reduction step.

3.4 Transforming to $\mathbb{R}^m_{\geq 0}$ Our task is to solve the decision problem (3.16). We begin by recalling that $\text{intcone}(W) = \Lambda(W) \cap \text{cone}(W)$. Hence if $b \in Q \cap (\Lambda(W) + p)$ and $c \in \mathscr{C}$ with $b - c \in \text{intcone}(W)$ one necessarily has

$$c \equiv p \pmod{\Lambda(W)}. \tag{3.17}$$

Therefore, we can delete from $\mathcal{C}$ all elements for which (3.17) does not hold and we can re-write the decision problem (3.16) as follows.

Given $W \in \mathbb{Z}^{m\times m}$ of rank m, $p \in \Pi(W) \cap \mathbb{Z}^m$, $Q \subseteq \text{cone}(W)$ convex and $\mathscr{C} \subseteq \Lambda(W) + p$, decide whether

$$\forall b \in Q \cap (\Lambda(W) + p) \quad \exists c \in \mathscr{C} \quad \text{such that} \quad b \in \text{cone}(W) + c. \tag{3.18}$$

By subtracting p from Q as well as from $\mathcal{C}$, the statement (3.18) is equivalent to the following.

$$\forall b \in Q' \cap \Lambda(W) \quad \exists c \in \mathcal{C}' \quad \text{such that} \quad b - c \in \text{cone}(W), \tag{3.19}$$

where $Q' = Q - p$ and $\mathcal{C}' = \mathcal{C} - p$. Observe that $\mathcal{C}' \subseteq \Lambda(W)$. One has

$$Q' \cap \Lambda(W) = W(W^{-1}Q' \cap \mathbb{Z}^m), \quad \mathcal{C}' = W(W^{-1}\mathcal{C}') \quad \text{and} \quad \text{cone}(W) = W\,\mathbb{R}^m_{\geq 0}.$$

Furthermore, we have $W^{-1}\mathcal{C}' \subseteq \mathbb{Z}^m$. Recall that $\|\mathcal{C}'\|_\infty \leq (m\Delta)^{O(m)}$. The Hadamard inequality implies that the absolute value of each component of W^{-1} is bounded by $(m\Delta)^{O(m)}$. Thus

$$\|W^{-1}\mathcal{C}'\|_\infty \leq (m\Delta)^{O(m)}.$$

By re-defining Q as $W^{-1}Q'$, $\mathcal{C}$ as $W^{-1}\mathcal{C}' \subseteq \mathbb{Z}^m$ we arrive at the desired simple problem (2.6).

Given a convex set $Q \subseteq \mathbb{R}^m$, and a set $\mathcal{C} \subseteq \mathbb{Z}^m$ with $\|\mathcal{C}\|_\infty \leq (m \cdot \Delta)^{O(m)}$. Decide the validity of the statement

$$\forall b \in Q \cap \mathbb{Z}^m \, \exists c \in \mathcal{C} \colon c \leq b.$$

4 Diagonal Frobenius Number

A central element of our sequence of reductions is Lemma 3.1 which is based on proximity between integer and fractional optimal solutions. We conclude this paper with a structural result concerning the following variant of the forall-exist statement (3.12) in which the convex set Q is the entire cone

$$Q = \text{cone}(W).$$

Our technique can be used to describe a subset of $\text{cone}(W) \cap \Lambda(W)$ in which there is no counterexample. In other words, every point belongs to the set $\text{intcone}(W)$.

Similar results of this flavor have appeared in the recent literature. The authors of [6] present a *deep in the cone Lemma* which identifies this set as being those lattice points that are far away from the boundary of $\text{cone}(W)$. The authors note that such a result can also be deduced from Aliev and Henk [2] who provide a bound on their so-called *diagonal Frobenius number*, which is the number t^* below. Given a matrix $W \in \mathbb{Z}^{m\times n}$ such that $\text{cone}(W)$ is pointed, find the smallest natural number t^* such that for all $z \in \{Wx \colon x \geq t\mathbf{1}\} \cap \Lambda(W)$, $z \in \text{intcone}(W)$. Recall that a cone is *pointed* if it does not contain a line, see, e.g. [22]. The upper bound on the diagonal Frobenius number given by Aliev and Henk [2] is as follows.

THEOREM 4.1. ([2]) *Let $W \in \mathbb{Z}^{m\times n}$ such that $\Lambda(W) = \mathbb{Z}^m$ with $\operatorname{cone}(W)$ pointed. Then the diagonal Frobenius number of W is at most*

$$t^* = \frac{(n-m)\sqrt{n}}{2}\sqrt{\det(WW^\top)}.$$

The goal of this section is to provide a simple proof bounding the diagonal Frobenius number in terms of the parameters m (number of rows of W) and Δ (largest absolute value of a component of W). To explain the differences of our bound and the bound in Theorem 4.1 in this setting, we first express the bound above in these parameters.

Each component of WW^T is bounded by $n \cdot \Delta$ in absolute value. Recall that $n \leq (2\Delta+1)^m$. The Hadamard bound implies

$$\sqrt{\det(WW^T)} \leq m^{O(m)}\Delta^{O(m^2)}.$$

Thus, the upper bound [2] on the diagonal Frobenius number is

$$t^* = \Delta^{O(m^2)}.$$

We will show below $t^* = (m\Delta)^{O(m)}$. In a recent paper, Aggarwal et al. [1] have shown that our bound is almost tight.

THEOREM 4.2. *Let $W \in \mathbb{Z}^{m\times n}$ and $\operatorname{cone}(W)$ be pointed. Then*

$$t^* \leq m \cdot (2m\Delta+1)^m.$$

Proof. Let $b \in \Lambda(W)$ with $b = W\lambda$, $\lambda \in \mathbb{R}^n_{\geq 0}$ such that $\lambda \geq \mathbf{1}t$ and $t = m \cdot (2m\Delta+1)^m$. To show is $b \in \operatorname{intcone}(W)$. Let $b' = t \cdot W\mathbf{1} \in \Lambda(W)$. We now consider the integer program

$$\max\left\{\mathbf{0}^T(x^+,x^-)\colon Wx^+ - Wx^- = b - b',\ (x^+,x^-) \geq \mathbf{0},\ (x^+,x^-) \in \mathbb{Z}^{2n}\right\}. \tag{4.20}$$

This integer program is feasible, since $b - b' \in \Lambda(W)$. Since $b - b' \in \operatorname{cone}(W)$, there exists an LP-optimal fractional solution $(y^+, y^-) \geq 0$ such that $y^- = \mathbf{0}$. The proximity Theorem 3.2 implies that there exists an integer solution $(z^+, z^-) \in \mathbb{Z}^{2n}$ such that $\|z^-\|_1 \leq m \cdot (2m\Delta+1)^m$. Notice that

$$W(z^+ - z^- + t\cdot\mathbf{1}) = b \quad \text{ and } z^+ - z^- + t\cdot\mathbf{1} \in \mathbb{Z}^n_{\geq 0}.$$

Hence, $b \in \operatorname{intcone}(W)$. ∎

Acknowledgments We would like to thank the anonymous SODA-reviewers for their very detailed and useful comments and suggestions.

References

[1] Divesh Aggarwal, Antoine Joux, Miklos Santha, and Karol Węgrzycki. Polynomial time algorithms for integer programming and unbounded subset sum in the total regime. *arXiv preprint arXiv:2407.05435*, 2024.

[2] Iskander Aliev and Martin Henk. Feasibility of integer knapsacks. *SIAM Journal on Optimization*, 20(6):2978–2993, 2010.

[3] Alexander Barvinok. *A course in convexity*, volume 54. American Mathematical Soc., 2002.

[4] Robert Bredereck, Andrzej Kaczmarczyk, Dušan Knop, and Rolf Niedermeier. High-multiplicity fair allocation: Lenstra empowered by n-fold integer programming. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, pages 505–523, 2019.

[5] Jason Crampton, Gregory Gutin, Martin Koutecký, and Rémi Watrigant. Parameterized resiliency problems via integer linear programming. In *International Conference on Algorithms and Complexity*, pages 164–176. Springer, 2017.

[6] Jana Cslovjecsek, Martin Koutecký, Alexandra Lassota, Michał Pilipczuk, and Adam Polak. Parameterized algorithms for block-structured integer programs with large entries. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 740–751. SIAM, 2024.

[7] Daniel Nicolas Dadush. *Integer programming, lattice algorithms, and deterministic volume estimation*. Georgia Institute of Technology, 2012.
[8] Friedrich Eisenbrand and Gennady Shmonin. Parametric integer programming in fixed dimension. *Mathematics of Operations Research*, 33(4):839–850, 2008.
[9] Friedrich Eisenbrand and Robert Weismantel. Proximity results and faster algorithms for integer programming using the steinitz lemma. *ACM Transactions on Algorithms (TALG)*, 16(1):1–14, 2019.
[10] Tomáš Gavenčiak, Martin Koutecký, and Dušan Knop. Integer programming in parameterized complexity: Five miniatures. *Discrete Optimization*, 44:100596, 2022.
[11] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2. Springer Science & Business Media, 2012.
[12] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences*, 63(4):512–530, 2001.
[13] Klaus Jansen and Lars Rohwedder. On integer programming, discrepancy, and convolution. *Mathematics of Operations Research*, 48(3):1481–1495, 2023.
[14] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of operations research*, 12(3):415–440, 1987.
[15] Ravi Kannan. Lattice translates of a polytope and the frobenius problem. *Combinatorica*, 12(2):161–177, 1992.
[16] Dušan Knop, Martin Koutecký, and Matthias Mnich. A unifying framework for manipulation problems. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pages 256–264, 2018.
[17] Dušan Knop, Michał Pilipczuk, and Marcin Wrochna. Tight complexity lower bounds for integer linear programming with few constraints. *ACM Transactions on Computation Theory (TOCT)*, 12(3):1–19, 2020.
[18] Martin Koutecký and Nimrod Talmon. Multi-party campaigning. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 35, pages 5506–5513, 2021.
[19] Hendrik W Lenstra Jr. Integer programming with a fixed number of variables. *Mathematics of operations research*, 8(4):538–548, 1983.
[20] Christos H Papadimitriou. On the complexity of integer programming. *Journal of the ACM (JACM)*, 28(4):765–768, 1981.
[21] Victor Reis and Thomas Rothvoss. The subspace flatness conjecture and faster integer programming. In *64th IEEE Symposium on Foundations of Computer Science (FOCS)*, 2023. to appear.
[22] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.
[23] Larry J Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3(1):1–22, 1976.
[24] Celia Wrathall. Complete sets and the polynomial-time hierarchy. *Theoretical Computer Science*, 3(1):23–33, 1976.