Dyadic linear programming and extensions

Ahmad Abdi[*]   Gérard Cornuéjols[†]   Bertrand Guenin[‡]   Levent Tunçel[§]

April 10, 2024

Abstract

A rational number is *dyadic* if it has a finite binary representation $p/2^k$, where p is an integer and k is a nonnegative integer. Dyadic rationals are important for numerical computations because they have an exact representation in floating-point arithmetic on a computer. A vector is *dyadic* if all its entries are dyadic rationals. We study the problem of finding a dyadic optimal solution to a linear program, if one exists. We show how to solve dyadic linear programs in polynomial time. We give bounds on the size of the support of a solution as well as on the size of the denominators. We identify properties that make the solution of dyadic linear programs possible: closure under addition and negation, and density, and we extend the algorithmic framework beyond the dyadic case.

Keywords. Linear programming, integer programming, dyadic rational, floating-point arithmetic, polynomial algorithm, dense abelian subgroup.

1 Introduction

A rational number is *dyadic* if it is an integer multiple of $\frac{1}{2^k}$ for some nonnegative integer k. Dyadic numbers are important for numerical computations because they have a finite binary representation, and therefore they can be represented exactly on a computer in floating-point arithmetic. When real or rational numbers are approximated by dyadic numbers on a computer, approximation errors may propagate and accumulate throughout the computations. So it is natural to ask when linear programs have a dyadic optimal solution. More generally, the exact solution of linear programs with rational input data has led to interesting work; we just mention here the excellent dissertation of Espinoza [15]. In this paper we investigate a different direction.

A vector x is *dyadic* if all its entries are dyadic numbers. A *dyadic linear program* is an optimization problem of the form

$$\sup \left\{ w^\top x : Ax \leq b, x \text{ dyadic} \right\}$$

where A, b, w have integral entries.

Note that we do not restrict ourselves to fixed precision; we just require a finite number of bits in the binary representation. This is an important point as we will see that it makes the problem

---

[*]Department of Mathematics, London School of Economics. Corresponding author, email address: a.abdi1@lse.ac.uk

[†]Tepper School of Business, Carnegie Mellon University

[‡]Department of Combinatorics & Optimization, University of Waterloo

[§]Department of Combinatorics & Optimization, University of Waterloo

1

tractable. On the other hand, if the vector x in the dyadic linear program were restricted to be of the form $\frac{y}{2^k}$ for an integral vector y and a nonnegative integer k bounded above by a given value K, then the problem would be a classical integer linear program. Indeed the problem can then be written as $\frac{1}{2^K} \cdot \max \left\{ w^\top y : Ay \leq 2^K b, y \text{ integral} \right\}$.

Some natural questions about dyadic linear programs are: When is the problem feasible? Can we check feasibility in polynomial time? If the problem is infeasible, can we provide a certificate of infeasibility? When does a dyadic linear program have an optimal solution? Note that a dyadic linear program may be feasible and bounded, but not have an optimal solution (in dimension one, $\sup \{x : 3x \leq 1, x \text{ dyadic}\}$ is such an example). Can dyadic linear programs be solved in polynomial time? What is the size of the dyadic numbers in a solution when one exists? What is the support size of a solution? This paper addresses these questions. In particular, we show that dyadic linear programs can be solved in polynomial time.

The interest in dyadic linear programming stems not only from the computer science perspective mentioned above, but also from mathematics and from optimization. Take a mathematical point of view: Given a prime integer $p \geq 2$, we say that a rational number is *finitely p-adic* if it is of the form $\frac{r}{p^k}$ for some integer r and nonnegative integer k. This concept is closely related to the notion of the *p-adic numbers* introduced by Hensel, formally defined as the set of "finite-tailed" infinite series $\sum_{i=N}^{+\infty} a_i p^i$ where $N \in \mathbb{Z}$, and $a_i \in \mathbb{Z}$ and $0 \leq a_i < p$ for each $i \geq N$.[1] The study of p-adic numbers gives rise to beautiful and powerful mathematics; see the excellent book by Gouvêa for more [17]. It can be readily checked that the set of finitely p-adic numbers is the set of finite series of the form $\sum_{i=N}^{M} a_i p^i$, where $M, N \in \mathbb{Z}$, $M \geq N$, and $0 \leq a_i < p, a_i \in \mathbb{Z}$ for all $N \leq i \leq M$, justifying our terminology.[2] In this paper, we will only deal with finitely p-adic numbers; for simplicity we refer to them as *p-adic numbers* throughout the paper. Also we refer to "2-adic" as "dyadic". More generally, we say that a rational number is *[p]-adic* if it is of the form $\frac{r}{s}$ where r is an integer and s is a product of powers of primes between 2 and p. These numbers appear naturally in some of the theorems in this paper. For the optimization point of view, let us mention an intriguing conjecture of Seymour dating back to 1975; see Schrijver [28] 79.3e. Let A be a 0,1 matrix such that the set covering polyhedron $Ax \geq \mathbf{1}, x \geq 0$ has only integral vertices, where $\mathbf{1}$ denotes the vector of all 1s. Thus the linear program $\min \left\{ c^\top x : Ax \geq \mathbf{1}, x \geq 0 \right\}$ has an optimal 0,1 solution for any objective function $c \in \mathbb{Z}_+^n$. Seymour conjectured that the dual linear program $\max \left\{ \mathbf{1}^\top y : A^\top y \leq c, y \geq 0 \right\}$ always has a dyadic optimal solution y. This conjecture is still open but is known to hold in a few important special cases. For example, when A is the T-cut versus edge incidence matrix of a graph, an optimal dual solution y is $\frac{1}{2}$-integral (Lovász [22]). Seymour's conjecture was proved recently in a couple of other special cases [2], [5].

We will show in this paper that dyadic linear programming shares aspects of classical linear programming as well as certain aspects of integer programming. In particular, we will show that, just like linear programs, dyadic linear programs can be solved in polynomial time. However, when it comes to the support size of a solution, the situation is more akin to that in integer programming. Indeed, in classical linear programming, for a problem in standard equality form $x \geq 0, Ax = b$, if it has an optimal solution, there is a basic optimal solution with at most m nonzero entries where m is the row rank of the constraint matrix A. For integer programs, the support size may be superlinear in m, and a similar situation occurs for dyadic linear programs. Next, we present an outline of the paper.

---

[1]The p-adic numbers form a field extension of the rational numbers, albeit in a different way than the real numbers.

[2]The set of finitely p-adic numbers does not form a field. For instance, 3 is finitely 2-adic, but $1/3$ is not.

In Section 2, we present two key ideas that make the polynomial solution of dyadic linear programs possible. The first ingredient is the density of the dyadic numbers in the real line. This property enables us to convert the feasibility question for a dyadic linear program to that of the existence of a dyadic point in an affine space. Specifically, we show that, if $\mathbb{L}$ is a dense subset of the real line closed under addition and negation, and P is a nonempty convex set whose affine hull is rational, then P contains a point in $\mathbb{L}^n$ if and only if its affine hull $\mathrm{aff}(P)$ does. This equivalence begs the question: When does the affine space $\mathrm{aff}(P)$ contain a point in $\mathbb{L}^n$?

The second key ingredient is a theorem of the alternatives. This theorem allows us to answer the above question. Specifically, consider a matrix $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$. Then exactly one of the following holds: (a) $Ax = b$ has a solution in $\mathbb{L}^n$, or (b) there exists $u \in \mathbb{R}^m$ such that $A^\top u \in \mathbb{Z}^n$ and $b^\top u \notin \mathbb{L}$. This theorem of the alternative is reminiscent of the so-called "integer Farkas lemma" and it can be proved in a similar way, using the Hermite normal form of A. Because the Hermite normal form of an integral matrix can be found in polynomial time (Kannan and Bachem [21]), one can obtain a polynomial certificate for statements (a) or (b), whichever holds.

These two are the basic ingredients we need to check feasibility of dyadic linear programs in polynomial time.

In Section 3, we present an algorithm to solve dyadic linear programs. There are four possible outcomes for this optimization problem: (i) the problem is infeasible, (ii) the problem is unbounded, (iii) the problem has an optimal solution, (iv) the problem is feasible and bounded but has no optimal solution. We show how to decide in polynomial time which of these outcomes is the correct one and, in each case, we give a concise (polynomial size) certificate. The complexity of our algorithm is (up to a constant factor) the same as that of solving an ordinary linear program. Our results in this section are extended beyond the dyadic numbers to any subset $\mathbb{L} \subseteq \mathbb{R}$ that is closed under addition and negation, contains all the p-adic numbers for some prime p, and is equipped with a membership oracle.

In Section 4, we focus on the size of the denominators of a solution to a feasible dyadic linear program. In particular, we show that if $Ax \le b, x$ dyadic is feasible, where $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$, then there exists a $\frac{1}{2^k}$-integral solution, where $k \le \left\lceil \log_2 n + (2n+1) \log_2(\|A\|_\infty \sqrt{n+1}) \right\rceil$. Here $\|A\|_\infty$ denotes the largest absolute value of an entry in A. Our results in this section are presented more generally for p-adic linear programs.

In Section 5, we study the size of the support of a solution to a dyadic linear program. That is, we consider the smallest number of nonzero components in a dyadic solution. Surprisingly, the lower and upper bounds that we obtain on the smallest support size resemble results for integer programming and are very different from the value of the support size given by Carathéodory's theorem for classical linear programming. Specifically, let $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m$ and $w \in \mathbb{R}^n$. If $\min\{w^\top x : Ax = b, x \ge \mathbf{0}, x$ dyadic$\}$ has an optimal solution, then we show that it has one with support size at most $m(1 + 0.84 \ln m + 1.68 \ln \|A\|_\infty)$. We give lower bounds by constructing examples and show that they are extremal in some sense. Our results in this section are presented more generally for integer and $[p]$-adic linear programs.

Section 6 provides conclusions and possible directions for future research.

2 Foundational results

In this section, we identify two results that underpin much of the work in the paper, and are key to solving dyadic linear programs. The first result reduces *dyadic feasibility* of a rational polyhedron

to that of its affine hull, while the second result provides a *theorem of the alternatives* for dyadic feasibility of a linear system of equations. We then combine the two results to obtain a *certificate of dyadic infeasibility* of a rational polyhedron. The results in this section are presented not only for the dyadic numbers, but more generally for any subset $\mathbb{L}$ of $\mathbb{R}$ closed under addition and negation, where sometimes we require $\mathbb{L}$ to be dense in $\mathbb{R}$, and at other times $\mathbb{L} \neq \mathbb{R}$. Let us lay the groundwork.

2.1 Abelian subgroups, p-adic and $[p]$-adic numbers

Let $\mathbb{L} \subseteq \mathbb{R}$. We say that $\mathbb{L}$ is *closed under addition* if $x + y \in \mathbb{L}$ for all $x, y \in \mathbb{L}$, and that $\mathbb{L}$ is *closed under negation*, or equivalently *symmetric around the origin*, if $-x \in \mathbb{L}$ for all $x \in \mathbb{L}$. Clearly, if $\mathbb{L}$ is closed under addition and negation, then $ax \in \mathbb{L}$ for all $a \in \mathbb{Z}$ and $x \in \mathbb{L}$. In particular, if $\mathbb{L} \neq \emptyset$ then $0 \in \mathbb{L}$.

The condition that $\mathbb{L} \subseteq \mathbb{R}$ is closed under addition and negation is equivalent to requiring that $(\mathbb{L}, +)$ *forms an abelian subgroup of* $(\mathbb{R}, +)$. It can be readily checked that for any such nonempty set, either $\mathbb{L}$ is dense in $\mathbb{R}$, or $\mathbb{L}$ is of the form $\{ax : a \in \mathbb{Z}\}$ for some $x \in \mathbb{R}$. In the latter case, $\mathbb{L}$ is isomorphic to $\mathbb{Z}$, in which case checking if a rational polyhedron in $\mathbb{R}^n$ contains a point in $\mathbb{L}^n$ is equivalent to integer programming feasibility in dimension n.

The discussion above motivates us to focus on dense sets in $\mathbb{R}$ closed under addition and negation. We present a construction for such sets, but we first require a definition. A subset $\mathcal{S}$ of positive integers is *closed under multiplication* if $pq \in \mathcal{S}$ for all $p, q \in \mathcal{S}$. Given such a subset, note that $\mathcal{S}$ is finite if and only if $\mathcal{S} \subseteq \{1\}$.

Lemma 2.1. *Let $\mathcal{S}$ be an infinite set of positive integers that is closed under multiplication. Let $\mathbb{L}$ be the set of all numbers $\frac{r}{s}$ where $s \in \mathcal{S}$ and $r \in \mathbb{Z}$. Then $(\mathbb{L}, +)$ is a dense abelian subgroup of $(\mathbb{R}, +)$.*

Proof. Pick $x \in \mathbb{R}$ and $\epsilon > 0$. Since $\mathcal{S}$ is an infinite set of positive integers, there exists $s \in \mathcal{S}$ with $s \geq \frac{1}{\epsilon}$. Let $r = \lfloor sx \rfloor$, then $|x - \frac{r}{s}| < \epsilon$. Since $\frac{r}{s} \in \mathbb{L}$, it follows that $\mathbb{L}$ is a dense subset of $\mathbb{R}$. Since $\mathcal{S}$ is closed under multiplication, if $\frac{r}{s}, \frac{r'}{s'} \in \mathbb{L}$, then their sum $\frac{rs' + r's}{ss'} \in \mathbb{L}$, so $\mathbb{L}$ is closed under addition. Finally, if $\frac{r}{s} \in \mathbb{L}$ then $\frac{-r}{s} \in \mathbb{L}$, so $\mathbb{L}$ is closed under negation. $\square$

We can use this result to provide two important examples of dense abelian subgroups of $(\mathbb{R}, +)$.

Definition 2.2. *Let $p \geq 2$ be a prime number. We say that a rational number is p-adic if it is of the form $\frac{r}{s}$ where s is a power of p and $r \in \mathbb{Z}$. We say that a rational number is $[p]$-adic if it is of the form $\frac{r}{s}$ where s is a product of powers of primes between 2 and p, and $r \in \mathbb{Z}$.*

Observe that the set of p-adic numbers can be obtained from the construction in Lemma 2.1 by choosing $\mathcal{S} = \{p^n : n \geq 0, n \in \mathbb{Z}\}$, while the set of $[p]$-adic numbers is obtained by choosing $\mathcal{S}$ to consist of all positive integers with prime factors less than or equal to p. Thus, both sets yield dense abelian subgroups of $(\mathbb{R}, +)$, by Lemma 2.1. Observe further that when $p = 2$, the p-adic, $[p]$-adic, and dyadic numbers coincide. More generally, we have the following relation between p-adic and $[p]$-adic sets.

Theorem 2.3. *Let $p \geq 2$ be an integer. Then the following are equivalent for a subset $\mathbb{L} \subseteq \mathbb{R}$:*

(1) $\mathbb{L}$ is the set of $[p]$-adic numbers,

(2) $(\mathbb{L}, +)$ is the abelian subgroup of $(\mathbb{R}, +)$ generated by the q-adic numbers for primes $q \leq p$.

Proof. Denote by $\mathbb{L}_1$ the set $\mathbb{L}$ as defined by (1) and by $\mathbb{L}_2$ the set $\mathbb{L}$ as defined by (2). We need to show $\mathbb{L}_1 = \mathbb{L}_2$. Note that $\mathbb{L}_2 \subseteq \mathbb{L}_1$ since (i) every q-adic number for a prime $q \leq p$ is $[p]$-adic by definition, and since (ii) $\mathbb{L}_1$ is closed under addition and negation by Lemma 2.1. We need to show that every point in $\mathbb{L}_1$ is in $\mathbb{L}_2$. Since $\mathbb{L}_2$ is closed under addition and negation, it suffices to consider points of the form $\frac{1}{Q} \in \mathbb{L}_1$ where $Q \in \mathbb{Z}$, $Q \geq 1$. As $1 \in \mathbb{L}_2$ we may assume $Q \geq 2$. Then $Q = \prod_{i=1}^r q_i^{\alpha_i}$ where $q_1, \ldots, q_r \leq p$ are distinct primes and $\alpha_i \geq 1$, $\alpha_i \in \mathbb{Z}$ for all $i \in [r]$. For all $i \in [r]$ define, $Q_i := Q q_i^{-\alpha_i}$. Then $Q_1, \ldots, Q_r$ are relatively prime and so it follows from Bézout's lemma that there exist $\rho_1, \ldots, \rho_r \in \mathbb{Z}$ such that $\sum_{i=1}^r \rho_i Q_i = 1$. Observe that,

$$\sum_{i=1}^r \rho_i q_i^{-\alpha_i} = \frac{1}{Q} \sum_{i=1}^r \rho_i Q_i = \frac{1}{Q}.$$

Each of the terms on the left hand side of the previous expression is in $\mathbb{L}_2$. Since $\mathbb{L}_2$ is closed under addition, it follows that $\frac{1}{Q} \in \mathbb{L}_2$, as required. $\qquad\square$

2.2 Density and affine hulls

In [3, 4] we proved that a rational polyhedron contains a dyadic point if and only if its affine hull does. This is a special case of the following more general result.

Theorem 2.4. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$. Consider $P \subseteq \mathbb{R}^n$ where (i) the relative interior of P is non-empty, and (ii) the affine hull $\mathrm{aff}(P)$ of P is a translate of a rational subspace. Then $P \cap \mathbb{L}^n \neq \emptyset$ if and only if $\mathrm{aff}(P) \cap \mathbb{L}^n \neq \emptyset$.*

To prove this theorem, we need a technical lemma. To state it we need some notations. For a vector v and $1 \leq q \leq +\infty$, $\|v\|_q$ denotes the q-norm of v. Given $\epsilon > 0$ and a vector $\bar{x}$, we write $B_q(\bar{x}, \epsilon)$ for the closed q-norm ball $\{x : \|x - \bar{x}\|_q \leq \epsilon\}$ centered at $\bar{x}$ with radius ϵ.

Lemma 2.5. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$, and let $P \subseteq \mathbb{R}^n$. Suppose that $\mathrm{aff}(P) = z + \mathrm{span}\{d^1, \ldots, d^\ell\}$ for some $z \in \mathbb{R}^n$ and $d^1, \ldots, d^\ell \in \mathbb{Z}^n$, in particular, $\mathrm{aff}(P)$ is a translate of a rational subspace. Consider $z' \in \mathrm{aff}(P)$ and $\epsilon > 0$. Then the following statements hold for any $1 \leq q \leq +\infty$:*

(a) *There exists $\bar{\rho} \in \mathbb{L}^n$ such that $z + \bar{\rho} \in \mathrm{aff}(P) \cap B_q(z', \epsilon)$.*

(b) *If for some prime p, $\mathbb{L}$ contains all the p-adic numbers, we can find in (a) an explicit $\bar{\rho}$ that is p-adic. Namely, pick a nonnegative integer r for which*

$$p^r \geq \frac{\ell \max\{\|d^1\|_q, \ldots, \|d^\ell\|_q\}}{\epsilon}. \tag{1}$$

Pick $\alpha \in \mathbb{R}^\ell$ satisfying

$$z + \sum_{i=1}^\ell \alpha_i d^i = z'. \tag{2}$$

Then we can choose

$$\bar{\rho} := \sum_{i=1}^\ell \frac{\lfloor p^r \alpha_i \rfloor}{p^r} d^i. \tag{3}$$

Furthermore, for this choice of $\bar{\rho}$ we have $\|p^r \bar{\rho}\|_q \leq p^r (\|z' - z\|_q + \epsilon)$.

Proof. Given $\beta \in \mathbb{R}^\ell$ denote $\rho(\beta) := \sum_{i=1}^\ell \beta_i d^i$. Then, since $z' \in \mathrm{aff}(P)$, we have $z + \rho(\alpha) = z'$ for some $\alpha \in \mathbb{R}^\ell$. We need the claim below.

Claim. $z + \rho(\beta) \in B_q(z', \epsilon)$ *if*

$$|\beta_i - \alpha_i| \leq \frac{\epsilon}{\ell \max\{\|d^1\|_q, \dots, \|d^\ell\|_q\}} \qquad \textit{for } i = 1, \dots, \ell. \tag{4}$$

Proof of Claim. We need to show that $\|z + \rho(\beta) - z'\|_q \leq \epsilon$. We have,

$$\|z + \rho(\beta) - z'\|_q = \|\rho(\beta) - \rho(\alpha)\|_q = \left\| \sum_{i=1}^\ell (\beta_i - \alpha_i) d^i \right\|_q$$

$$\leq \sum_{i=1}^\ell \left\| (\beta_i - \alpha_i) d^i \right\|_q = \sum_{i=1}^\ell |\beta_i - \alpha_i| \, \|d^i\|_q \leq \epsilon,$$

where the first inequality arises from the triangle inequality and the second inequality from (4). $\diamond$

(a) Since $\mathbb{L}$ is dense in $\mathbb{R}$, we can pick $\beta_i \in \mathbb{L}, i \in [\ell]$ such that (4) holds. Let $\bar{\rho} := \rho(\beta)$. Since $\mathbb{L}$ is closed under addition and negation, and since $\beta_i \in \mathbb{L}$ and d^i is integral for each $i \in [\ell]$, we have $\bar{\rho} \in \mathbb{L}^n$. By the claim, $z + \bar{\rho} \in B_q(z', \epsilon)$. Moreover, since $\mathrm{aff}(P) = z + \mathrm{span}\{d^1, \dots, d^\ell\}$, we have $z + \bar{\rho} \in \mathrm{aff}(P)$. Thus, $z + \bar{\rho} \in \mathrm{aff}(P) \cap B_q(z', \epsilon)$, so (a) holds.

(b) Suppose now $\mathbb{L}$ contains all the p-adic numbers. Pick r so that (1) holds and for each $i = 1, \dots, \ell$ let $\beta_i := \frac{\lfloor p^r \alpha_i \rfloor}{p^r}$. Then $|\beta_i - \alpha_i| \leq \frac{1}{p^r}$. Equation (1) then implies that (4) holds. It follows from the claim that for $\bar{\rho} := \rho(\beta)$, we have $z + \bar{\rho} \in \mathrm{aff}(P) \cap B_q(z', \epsilon)$.

Moreover, as β_i is p-adic and d^i is integral for each $i \in [\ell]$, $\bar{\rho}$ is p-adic. By the triangle inequality, $\|\bar{\rho}\|_q \leq \|z' - z\|_q + \|\bar{\rho} + z - z'\|_q$. Multiplying both sides by p^r yields $\|p^r \bar{\rho}\|_q \leq p^r \|z' - z\|_q + p^r \|\bar{\rho} + z - z'\|_q$. As $\bar{\rho} + z \in B_q(z', \epsilon)$, we have $\|\bar{\rho} + z - z'\|_q \leq \epsilon$, so $\|p^r \bar{\rho}\|_q \leq p^r (\|z' - z\|_q + \epsilon)$. $\square$

Lemma 2.5 (b) is used in Section 3 for efficiently finding a dyadic point inside a rational polyhedron. As for part (a), we will use it below to prove Theorem 2.4.

Proof of Theorem 2.4. Since $P \subseteq \mathrm{aff}(P)$, $\mathrm{aff}(P) \cap \mathbb{L}^n = \emptyset$ implies $P \cap \mathbb{L}^n = \emptyset$. Assume now that $\mathrm{aff}(P) \cap \mathbb{L}^n \neq \emptyset$. Pick $z \in \mathrm{aff}(P) \cap \mathbb{L}^n$. Since $\mathrm{aff}(P)$ is a translate of a rational subspace by hypothesis (ii), we can express $\mathrm{aff}(P)$ as $z + \mathrm{span}\{d^1, \dots, d^\ell\}$ for some vectors $d^1, \dots, d^\ell \in \mathbb{Z}^n$. Take $1 \leq q \leq +\infty$. By hypothesis (i), there exists a q-norm ball of B of radius $\epsilon > 0$ centered at some $z' \in P$ for which $\mathrm{aff}(P) \cap B \subseteq P$. By Lemma 2.5(a) there exists $\bar{\rho} \in \mathbb{L}^n$ for which $z + \bar{\rho} \in \mathrm{aff}(P) \cap B$. Since $z, \bar{\rho} \in \mathbb{L}^n$ and $\mathbb{L}$ is closed under addition, $z + \bar{\rho} \in \mathbb{L}^n$. Putting it altogether, we get that $z + \bar{\rho} \in P \cap \mathbb{L}^n$, so $P \cap \mathbb{L}^n \neq \emptyset$, as required. $\square$

Let us present an important corollary of this result. Since every non-empty convex set has a non-empty relative interior, Theorem 2.4 implies the following.

Corollary 2.6. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$. Consider a nonempty convex set P, where $\mathrm{aff}(P)$ is a translate of a rational subspace. Then $P \cap \mathbb{L}^n \neq \emptyset$ if and only if $\mathrm{aff}(P) \cap \mathbb{L}^n \neq \emptyset$.*

When $\mathbb{L}$ is the set of the dyadic numbers, and P is a polyhedron, we retrieve the fact that a rational polyhedron contains a dyadic point if and only if its affine hull does.

2.3 Theorem of the alternatives and consequences

In light of Corollary 2.6 we are interested in characterizing when a rational affine space contains a point in $\mathbb{L}^n$. We addressed the case when $\mathbb{L}$ is the set of dyadic points in [4]. Density is irrelevant in this case however, and the following general theorem holds; its proof is a careful adaptation of the well-known result for the case of integers (e.g., see Theorem 1.17 in [10]). For the proof, we need a definition. A square matrix is *unimodular* if it has integral entries and its determinant is ± 1. Observe that if U is unimodular then so is U^{-1}, by Cramer's rule for instance.

Theorem 2.7. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$ where $\mathbb{L} \neq \mathbb{R}$. Consider a matrix $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$. Then exactly one of the following holds:*

(a) $Ax = b$ has a solution in $\mathbb{L}^n$,

(b) there exists $u \in \mathbb{R}^m$ such that $A^\top u \in \mathbb{Z}^n$ and $b^\top u \notin \mathbb{L}$.

Moreover, if (a) holds, then $Ax = b$ has a solution in $\mathbb{L}^n \cap \mathbb{Q}^n$.

Proof. Suppose (a) and (b) both hold. Then we have $\bar{x} \in \mathbb{L}^n$ with $A\bar{x} = b$ and therefore $u^\top A\bar{x} = u^\top b$. As $u^\top A$ is integral and since $\mathbb{L}$ is closed under addition and negation, $\mathbb{L} \ni u^\top A\bar{x} = u^\top b$, a contradiction. Assume now that (a) does not hold. We prove that (b) holds. If $Ax = b$ does not have a solution in $\mathbb{Q}^n$, then there exists $u \in \mathbb{Q}^m$ for which $u^\top A = \mathbf{0}^\top$ and $u^\top b = 1$. Since $\mathbb{L}$ is a proper subset of $\mathbb{R}$, there exists $p \in \mathbb{R} \setminus \mathbb{L}$. Then after updating $u := p \cdot u$, we have $u^\top A = \mathbf{0}^\top \in \mathbb{Z}^n$ and $u^\top b = p \notin \mathbb{L}$, and (b) holds. Thus let us assume that $Ax = b$ has a solution in $\mathbb{Q}^n$. We may further assume that the rows of A are linearly independent for otherwise we can eliminate redundant constraints, prove (b) for the smaller system and derive the result for the original system. We can now find a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ for which $AU = (B\ \mathbf{0})$ where B is a square non-singular matrix (for example one can choose U that converts A into Hermite normal form, see §A for more). We claim that $\bar{z} := B^{-1}b \notin \mathbb{L}^m$. For otherwise,

$$\bar{x} := U \begin{pmatrix} \bar{z} \\ \mathbf{0} \end{pmatrix}, \tag{5}$$

is a solution to $Ax = b$. Since $\mathbb{L}$ is closed under addition and negation and since U is integral, this would imply $\bar{x} \in \mathbb{L}^n$, a contradiction as (a) does not hold by assumption. Thus for some $i \in [m]$ we have $\bar{z}_i \notin \mathbb{L}$. Let $u = B^{-\top}e_i$. Then $u^\top b = e_i^\top B^{-1}b = \bar{z}_i \notin \mathbb{L}$. Moreover, $u^\top A = e_i^\top B^{-1}(B\ \mathbf{0})U^{-1} \in \mathbb{Z}^n$ since U^{-1} is integral as U is unimodular. Hence, (b) holds.

Thus, exactly one of (a) and (b) holds. For the final part of the theorem, suppose that (a) holds. Then $\bar{z} = B^{-1}b \in \mathbb{L}^m$, for otherwise the above argument shows that (b) holds, which is not the case. Furthermore, $\bar{z} \in \mathbb{Q}^m$, since $b \in \mathbb{Z}^m$, and B is integral so B^{-1} is rational. Subsequently, $\bar{x}$ as defined in (5) is a solution of $Ax = b$ in $\mathbb{L}^n \cap \mathbb{Q}^n$, as required. $\square$

Let us point out two things in Theorem 2.7. First, the only place in the proof where the condition $\mathbb{L} \neq \mathbb{R}$ is necessary is for finding the certificate u in (b) in case (a) does not hold. Secondly, a caveat of the result is that if (a) does not hold, then we cannot always find a certificate u in (b) that is rational. Consider for instance the case where $\mathbb{L}$ contains all rationals. Then we require $b^\top u \notin \mathbb{L} \supseteq \mathbb{Q}$ in (b), in particular, u is not rational. However, in this example, if (a) does not hold, then $Ax = b$ has no solution in $\mathbb{Q}^n$ either. By eliminating this possibility we can guarantee that the certificate u in (b) is rational.

Remark 2.8. *In Theorem 2.7, if $Ax = b$ has a solution in $\mathbb{Q}^n$ and has no solution in $\mathbb{L}^n$, then there exists a rational certificate u in (b).*

Proof. Indeed, suppose that $Ax = b$ has a solution in $\mathbb{Q}^n$. Then, proceeding as in the proof of Theorem 2.7, we can pick $u = B^{-\top}e_i$ for (b), which is rational. □

Given Corollary 2.6 and the second part of Theorem 2.7, we may ask the following question. Given a dense subset $\mathbb{L}$ of $\mathbb{R}$ closed under addition and negation, and given a rational polyhedron R which contains a point in $\mathbb{L}^n$, does R necessarily contain a point in $\mathbb{L}^n \cap \mathbb{Q}^n$? Alas, this need not be the case. Consider for instance $\mathbb{L} := \left\{\frac{a}{b}\sqrt{2} : a, b \in \mathbb{Z}, b \neq 0\right\}$, and let $R \subseteq \mathbb{R}^2$ be the convex hull of $(1, 1)$ and $(2, 2)$. Then $R \cap \mathbb{L}^2 \neq \emptyset$, but $\mathbb{L}^2 \cap \mathbb{Q}^2 = (0, 0)$ so $R \cap \mathbb{L}^2 \cap \mathbb{Q}^2 = \emptyset$. Note that in this example, $\mathbb{Q} \cap \mathbb{L}$ is not a dense subset of $\mathbb{R}$, and this is no accident as the next result shows.

Theorem 2.9. *Let* $(\mathbb{L}, +)$ *be an abelian subgroup of* $(\mathbb{R}, +)$ *and suppose that* $\mathbb{L} \cap \mathbb{Q}$ *is dense in* $\mathbb{R}$. *Then a rational polyhedron contains a point in* $\mathbb{L}^n$ *if and only if it contains a point in* $\mathbb{L}^n \cap \mathbb{Q}^n$.

Proof. The result is well-known when $\mathbb{L} = \mathbb{R}$. Otherwise, $\mathbb{L} \neq \mathbb{R}$. ($\Leftarrow$) is clear. For ($\Rightarrow$), suppose we have a rational polyhedron P with $P \cap \mathbb{L}^n \neq \emptyset$. Then $\mathrm{aff}(P) \cap \mathbb{L}^n \neq \emptyset$, so it follows from Theorem 2.7 that $\mathrm{aff}(P) \cap \mathbb{L}^n \cap \mathbb{Q}^n \neq \emptyset$. Since $\mathbb{L} \cap \mathbb{Q}$ is a dense subset of $\mathbb{R}$ that is closed under addition and negation, we may apply Corollary 2.6 to $\mathbb{L} \cap \mathbb{Q}$ and P to conclude that $P \cap \mathbb{L}^n \cap \mathbb{Q}^n \neq \emptyset$, as required. □

2.4 Certificate of $\mathbb{L}$-infeasibility of a rational polyhedron

Consider a dense abelian subgroup $(\mathbb{L}, +)$ of $(\mathbb{R}, +)$, and let P be a rational polyhedron. We wish to characterize when $P \cap \mathbb{L}^n \neq \emptyset$. By Corollary 2.6, it suffices to check if $\mathrm{aff}(P) \cap \mathbb{L}^n \neq \emptyset$. Furthermore, since P is a rational polyhedron, $\mathrm{aff}(P)$ is a rational affine space, so we can use Theorem 2.7 to characterize when $\mathrm{aff}(P) \cap \mathbb{L}^n \neq \emptyset$. In this subsection we combine these results to yield a *certificate of $\mathbb{L}$-infeasibility* of a rational polyhedron. We need the following technical lemma (which is also useful later in Section 3).

Lemma 2.10. *Let* $(\mathbb{L}, +)$ *be a dense abelian subgroup of* $(\mathbb{R}, +)$ *such that* $\mathbb{L} \neq \mathbb{R}$, *and consider a polyhedron* $P := \{x : Ax \leq b\}$ *where* $A \in \mathbb{Z}^{m \times n}$ *and* $b \in \mathbb{Z}^m$. *Suppose that*

$$\max\{c^\top x : Ax \leq b\}, \tag{P}$$

has an optimal solution of value τ, *and let* $F := P \cap \{x : c^\top x = \tau\}$ *be the optimal face. Then the following statements are equivalent:*

(a) $F \cap \mathbb{L}^n = \emptyset$.

(b) There exists $\bar{y}, \bar{u} \in \mathbb{Q}^m$ *that satisfy the following conditions,*

   (i) $\mathrm{support}(\bar{u}) \subseteq \mathrm{support}(\bar{y})$,
   (ii) $\bar{y}$ *is an optimal solution to the dual of (P),*
   (iii) $A^\top u \in \mathbb{Z}^n$ *and* $b^\top u \notin \mathbb{L}$.

Morever, for $\bar{y}$ *satisfying (ii), we have* $\mathrm{support}(\bar{y}) \subseteq \{i \in [m] : \mathrm{row}_i(A)x = b_i, \text{ for all } x \in F\}$.

8

Proof. Let $I^= := \{i \in [m] : \text{row}_i(A)x = b_i, \text{ for all } x \in F\}$ and denote, by $A^=x \le b^=$ the inequalities of $Ax \le b$ corresponding to $I^=$. Then, (see [10], Theorem 3.24), $F = P \cap \{x : A^=x = b^=\}$. Therefore, (see [10], Theorem 3.17), $\text{aff}(F) = \{x : A^=x = b^=\}$. Consider the dual of (P),

$$\min\{b^\top y : A^\top y = c, y \ge \mathbf{0}\}. \tag{D}$$

(a)$\Rightarrow$(b) By Corollary 2.6, $\text{aff}(F)$ has no point in $\mathbb{L}^n$. Hence, by Theorem 2.7, there exists $\bar{u}$ satisfying (iii) where $\text{support}(\bar{u}) \subseteq I^=$. Since $A^=x = b^=$ has a solution, it follows from Remark 2.8 that we can choose $\bar{u} \in \mathbb{Q}^{I^=}$. Let $\bar{x}$ and $\bar{y}$ be a strictly complementary pair of rational optimal solutions for (P) and (D). Then $\text{support}(\bar{y}) = I^=$. It follows that (i) holds.

(b)$\Rightarrow$(a) Let $i \notin I^=$. Then for some $\bar{x} \in F$ we have $\text{row}_i(A)\bar{x} < b_i$. By Complementary Slackness, $\bar{y}_i = 0$, i.e. $i \notin \text{support}(\bar{y})$. Hence, $\text{support}(\bar{y}) \subseteq I^=$, and the "moreover" statement holds. Furthermore, by (i) we have $\text{support}(\bar{u}) \subseteq I^=$. Therefore, by Theorem 2.7 and (iii), there is no point in $\mathbb{L}^n$ that also lies in $\{x : A^=x = b^=\} = \text{aff}(F)$. It follows that $F \cap \mathbb{L}^n = \emptyset$. $\qquad\square$

Theorem 2.11. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$ such that $\mathbb{L} \ne \mathbb{R}$. Consider a non-empty polyhedron $P := \{x : Ax \le b\}$ where $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$. Then the following are equivalent.*

(a) $P \cap \mathbb{L}^n = \emptyset$.

*(b) There exists a **certificate of $\mathbb{L}$-infeasibility** for P, that is, a pair of vectors $\bar{y}, \bar{u} \in \mathbb{Q}^m$ that satisfy the following conditions:*

    (i) $\text{support}(\bar{u}) \subseteq \text{support}(\bar{y})$,

    (ii) $\bar{y} \ge \mathbf{0}$, $A^\top \bar{y} = \mathbf{0}$, $b^\top \bar{y} = 0$,

    (iii) $A^\top u \in \mathbb{Z}^n$ and $b^\top u \notin \mathbb{L}$.

Moreover, for $\bar{y}$ satisfying (ii), we have $\text{support}(\bar{y}) \subseteq \{i \in [m] : \text{row}_i(A)x = b_i, \text{ for all } x \in P\}$.

Proof. Consider the linear program (P) defined as $\max\{0 : Ax \le b\}$ and let $F = P$. Every $\bar{x} \in P$ is an optimal solution to (P) of value 0. Therefore, condition (ii) says that $\bar{y}$ is an optimal solution to the dual of (P). The result now follows from Lemma 2.10. $\qquad\square$

3 Algorithms: feasibility and optimization

In this section, we present algorithms to check whether a rational polyhedron contains a point in $\mathbb{L}^n$ and to optimize a linear function over a rational polyhedron restricted to $\mathbb{L}^n$ where $\mathbb{L}$ satisfies the following three properties:

    (group) $(\mathbb{L}, +)$ is an abelian subgroup of $(\mathbb{R}, +)$,

    (density) $\mathbb{L}$ contains all p-adic numbers for some prime p, and

    (membership)   we have a membership oracle for $\mathbb{L}$.

Assuming the (group) property we also need to require $\mathbb{L}$ to be a dense subset of the reals for otherwise we are operating within the context of integer programming as discussed in Section 2.1. We want to be able to carry all computations over $\mathbb{Q}$, in particular, we insist that if a rational polyhedron contains a point in $\mathbb{L}^n$ then it contains one in $\mathbb{L}^n \cap \mathbb{Q}^n$. Because of Theorem 2.9 this can be achieved by choosing $\mathbb{L}$ with the property that $\mathbb{L} \cap \mathbb{Q}$ is dense. A natural choice is to include all p-adic numbers in $\mathbb{L}$, i.e. imposing the (density) condition above. Note, that we will assume that we are also given the prime value p explicitly. A *membership oracle* for $\mathbb{L}$ is a function that takes as input $x \in \mathbb{Q}$ and returns YES if $x \in \mathbb{L}$ and NO otherwise. We will present algorithms that run in oracle polynomial time for both feasibility and optimization over polyhedra restricted to $\mathbb{L}^n$. When $\mathbb{L}$ is the set of p-adic, or $[p]$-adic numbers, our three properties (group), (density), and (membership) hold, and we have trivial polynomial oracles. Thus, we will be able to solve the feasibility and optimization problems for p-adic and $[p]$-adic numbers in polynomial time. In particular, we can solve the problem for dyadic numbers.

Our algorithms will rely on the existence of a number of polynomial-time subroutines that we present next.

Algorithm A.
Takes as input a matrix $A \in \mathbb{Q}^{m \times n}$ and a vector $b \in \mathbb{Q}^m$. Returns one of the following: (i) $\bar{x} \in \mathbb{Q}^n$ satisfying $Ax = b$, or (ii) $u \in \mathbb{Q}^m$ such that $A^\top u = \mathbf{0}$ and $b^\top u \neq 0$ certifying $Ax = b$ has no solution.

Algorithm B.
Takes as input a matrix $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$. We are also given a membership oracle that describes an abelian subgroup $(\mathbb{L}, +)$ of $(\mathbb{R}, +)$. Returns one of the following: (i) $\bar{x} \in \mathbb{L}^n \cap \mathbb{Q}^n$ satisfying $Ax = b$, or (ii) $u \in \mathbb{Q}^m$ such that $A^\top u = \mathbf{0}$ and $b^\top u \neq 0$ certifying $Ax = b$ has no solution, or (iii) $u \in \mathbb{Q}^m$ such that $A^\top u$ is integral and $u^\top b \notin \mathbb{L}$ certifying $Ax = b$ has no solution in $\mathbb{L}^n$.

Algorithm C.
Takes as input a matrix $A \in \mathbb{Z}^{m \times n}$. Returns linearly independent vectors $d^1, \ldots, d^\ell \in \mathbb{Z}^n$ with the property that $\operatorname{span}\{d^1, \ldots, d^\ell\} = \{x : Ax = \mathbf{0}\}$.

Algorithm D.
Takes as input a matrix $A \in \mathbb{Q}^{m \times n}$ and vectors $b \in \mathbb{Q}^m$ and $c \in \mathbb{Q}^n$. Then solves the linear program

$$\max\{c^\top x : Ax \leq b\}. \tag{P}$$

Namely, it returns one of the following: (i) $u \in \mathbb{Q}^m$ such that $A^\top u \geq \mathbf{0}$ and $b^\top u < 0$ certifying that (P) is infeasible, or (ii) $x, r \in \mathbb{Q}^n$ such that $Ax \leq b$, $Ar \leq \mathbf{0}$ and $c^\top r > 0$ certifying that (P) is unbounded, or (iii) $x \in \mathbb{Q}^n$, $y \in \mathbb{Q}^m$ which form a pair of strictly complementary optimal solutions for (P) and its dual.

Algorithm B emulates the argument in the proof of Theorem 2.7. We first ensure that $Ax = b$ has a solution using Algorithm A, and then eliminate redundant constraints. We then find a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ for which $AU = (B\ \mathbf{0})$ where B is an m-by-m matrix and compute $\bar{z} = B^{-1}b$. We use the membership oracle to check whether each of $\bar{z}_i \in \mathbb{L}$. If this is the case then $U \begin{pmatrix} \bar{z} \\ \mathbf{0} \end{pmatrix} \in \mathbb{L}^n$ is a solution to $Ax = b$. Otherwise, for some $i \in [m]$, $\bar{z}_i \notin \mathbb{L}$ and we return $u = B^{-\top} e_i$. For Algorithm C, we eliminate linearly dependent rows of A and find a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ for which $AU = (B\ \mathbf{0})$ where B is an m-by-m matrix. Then the columns of U corresponding to the $\mathbf{0}$ columns of $(B\ \mathbf{0})$ are the required vectors d^i. For both algorithms, finding the matrix U can achieved by rewriting A in Hermite normal form which can be found in polynomial time [21]. This implies that

there is an implementation of Algorithm C that runs in polynomial time, and an implementation of Algorithm B that runs in *oracle* polynomial time.

3.1 $\mathbb{L}$-Feasibility Problem (LFP)

Consider a polyhedron $P := \{x : Ax \leq b\}$. The $\mathbb{L}$-*Feasibility Problem (LFP)* takes as input a matrix $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$ that define the polyhedron P. We consider $\mathbb{L} \subseteq \mathbb{R}$ satisfying the (group), (density) and (membership) properties (with p given explicitly). We then need to return (i) a point in $P \cap \mathbb{L}^n$, or (ii) a certificate that $P = \emptyset$, or (iii) a certificate of $\mathbb{L}$-infeasibility (as defined in Section 2.4). We will show that there exists an oracle polynomial time algorithm to solve LFP. Note that by Farkas' lemma, $P = \emptyset$ if and only if there exists $y \geq \mathbf{0}$ for which $A^\top y = \mathbf{0}$ and $b^\top y < 0$; such a y is a *certificate of real-infeasibility*, and is the output of (ii).

3.1.1 The LFP algorithm

Here is a description of our algorithm to solve LFP.

Step 1: *Find the implicit equalities of P. That is, identify the inequalities of $Ax \leq b$ that hold at equality for all feasible solutions.*

Consider the following primal-dual pair,

$$\max\{0 : Ax \leq b\}, \tag{P}$$
$$\min\{b^\top y : A^\top y = \mathbf{0}, y \geq \mathbf{0}\}. \tag{D}$$

Use Algorithm D to check whether $P = \emptyset$. If it is, return a certificate of real-infeasibility u and stop. Otherwise, Algorithm D finds a strictly complementary pair of optimal solutions $\bar{x} \in \mathbb{Q}^n$ and $\bar{y} \in \mathbb{Q}^m$ for (P) and (D) respectively. Since every $x \in P$ is an optimal solution to (P), strict complementarity implies that

Claim. $\text{support}(\bar{y}) = I^=$ *where* $I^= = \{i \in [m] : \text{row}_i(A)x = b_i \ \forall \ x \in P\}$.

Denote by $A^= x \leq b^=$ the constraints from $Ax \leq b$ indexed by $I^=$. Then $\text{aff}(P) = \{x : A^= x = b^=\}$.

Step 2: *Find an internal description of $\text{aff}(P)$ or certify $\mathbb{L}$-infeasibility.*

Let $I^< = [m] \setminus I^=$ and let $A^< x \leq b^<$ denote the constraints of $Ax \leq b$ indexed by $I^<$. Then use Algorithm B to either,

(i) find $z \in \text{aff}(P) \cap \mathbb{L}^n \cap \mathbb{Q}^n$, or

(ii) find $u^= \in \mathbb{Q}^m$ such that $A^{=\top} u^=$ is integral and $b^\top u^= \notin \mathbb{L}$.

If (ii) occurs, then extend $u^=$ to a vector indexing the rows of A by assigning zeros to all entries corresponding to $I^<$, and denote the resulting vector by $\bar{u}$. Then observe that $\bar{y}, \bar{u}$ is a certificate of $\mathbb{L}$-infeasibility, and we can stop. Otherwise we have z as described in (i). Use Algorithm C to find an integral basis $d^1, \ldots, d^\ell$ of $\{d : A^= d = \mathbf{0}\}$. It then follows that

$$\text{aff}(P) = z + \text{span}\{d^1, \ldots, d^\ell\}. \tag{6}$$

Step 3: *Find a Euclidean ball B such that $B \cap \text{aff}(P) \subseteq P$.*

11

For each $i \in [m]$ let $\gamma_i := \lceil \|\operatorname{row}_i(A)\|_2 \rceil$ (γ_i can be computed in polynomial time on a Turing machine, without evaluating the square-root to a high accuracy). Consider the following linear program with variables ζ and e:

$$
\begin{aligned}
\max \quad & e \\
\text{subject to} \quad & \\
& A^= \zeta = b^= \\
& \gamma_i e + \operatorname{row}_i(A)\zeta \le b_i \qquad\qquad (i \in I^<) \qquad\qquad (7)\\
& e \le 1.
\end{aligned}
$$

Since $e \le 1$, (7) is not unbounded. Moreover, (7) is feasible (pick $\zeta \in P$ and $e = 0$). Hence, we can use Algorithm D to find an optimal solution $\zeta = z' \in \mathbb{Q}^n$, $e = \epsilon \in \mathbb{Q}$ of (7). By definition of $I^<$ we have $\epsilon > 0$. Then $z' \in P$ and for every $i \in [m]$, $\frac{1}{\gamma_i}[b_i - \operatorname{row}_i(A)z']$ is a lower bound on the Euclidean distance from z' to the hyperplane $\{h : \operatorname{row}_i(A)h = b_i\}$ because $\gamma_i \ge \|\operatorname{row}_i(A)\|_2$. This implies that $B \subseteq \{x : A^< x \le b^<\}$ where B denotes the Euclidean ball of radius ϵ centered at z'. Then $B \cap \operatorname{aff}(P) \subseteq \{x : A^< x \le b^<\} \cap \{x : A^= x = b^=\} = P$.

Step 4: *Find a point in $P \cap \mathbb{L}^n$.*

Pick

$$
r := \left\lceil \log_p \left(\frac{\ell \max\{\|d^1\|_2, \ldots, \|d^\ell\|_2\}}{\epsilon} \right) \right\rceil. \qquad\qquad (8)
$$

Then we satisfy (1) (this is the place where we need to know the value of p explicitly). Use Algorithm A to find α satisfying $\sum_{i \in [\ell]} \alpha_i d^i = z' - z$ so that (2) holds. Choose $\bar\rho$ as in (3). It then follows from Lemma 2.5 that $\bar\rho$ is p-adic and that $z + \bar\rho \in \operatorname{aff}(P) \cap B \subseteq P$. Finally, as $z \in \mathbb{L}^n \cap \mathbb{Q}^n$, the (group) and (density) properties imply that $z + \bar\rho \in \mathbb{L}^n \cap \mathbb{Q}^n$, as required.

3.1.2 The alternate LFP algorithm

We sketch out a variant of our algorithm for solving the $\mathbb{L}$-feasibility problem for polyhedra that are in standard equality form, i.e. for $P := \{x \ge \mathbf{0} : Ax = b\}$. The implicit equalities will be of the form $Ax = b$ as well as $x_j = 0$ for a subset $J^= \subseteq [n]$ of the column indices. In particular, we have

$$
\operatorname{aff}(P) = \{x : Ax = b, x_j = 0 \ \forall j \in J^=\}.
$$

We consider the following primal-dual pair,

$$
\begin{aligned}
& \max\{0 : Ax = b, x \ge \mathbf{0}\}, && \text{(P')}\\
& \min\{b^\top y : A^\top y \ge \mathbf{0}\}. && \text{(D')}
\end{aligned}
$$

In *Step 1*, we proceed as in the previous version and use Algorithm D to find a strictly complementary pair of optimal solutions x' and y' for (P') and (D'). Then $J^= = \{j \in [n] : \operatorname{col}_j(A)^\top y' > 0\}$ and this allows us to identify $\operatorname{aff}(P)$. In *Step 2*, we use Algorithm C to find an integral basis $\{d^1, \ldots, d^\ell\}$ of $\{d : Ad = \mathbf{0}, d_j = 0 \ \forall j \in J^=\}$. The most notable change is for *Step 3*. Let $J^< = [n] \setminus J^=$ and denote by D the column submatrix of A indexed by columns $J^<$. Instead of (7) we solve, the linear program with variables e, ζ where

$$
\begin{aligned}
\max \quad & e \\
\text{subject to} \quad & \\
& D\zeta = b \\
& e \le \zeta_j \qquad\qquad (j \in J^<) \qquad\qquad (9)\\
& e \le 1.
\end{aligned}
$$

The above linear program is clearly feasible and bounded, hence we can use Algorithm D to find an optimal solution $\zeta = \bar{z}$ and $e = \epsilon$. Let $z' \in \mathbb{Q}^n$ be obtained from $\bar{z}$ by setting entries corresponding to $J^=$ to zero. Let $B = \{z : \|z' - z\|_\infty \leq \epsilon\}$, i.e. B is the ∞-norm ball of radius ϵ centered at z'. Then we have $B \subseteq \{x : x_j \geq \mathbf{0} \; \forall j \in J^<\}$ by construction. It follows that $B \cap \text{aff}(P) \subseteq \{x : x_j \geq 0 \; \forall j \in J^<\} \cap \{x : Ax = b, x_j = 0 \; \forall j \in J^=\} = P$. *Step 4* is the same as for the original algorithm, except that while the original algorithm used the 2-norm ball B in Lemma 2.5, this version of the algorithm uses the ∞-norm ball. In particular, we need to choose r according to,

$$r := \left\lceil \log_p \left(\frac{\ell \max\{\|d^1\|_\infty, \ldots, \|d^\ell\|_\infty\}}{\epsilon} \right) \right\rceil. \tag{10}$$

rather than according to (8).

3.1.3 Output size and running time analysis

We refer to the algorithm described in Section 3.1.1 as *the LFP algorithm*, and the algorithm described in Section 3.1.2 as the *alternate* LFP algorithm. Informally, the runtime of our LFP algorithm is dominated by the runtime of our linear program solver, which we call twice, once for checking feasibility of $Ax \leq b$ and once for solving (7). Note, that both linear programs have essentially the same size (with respect to many measures), moreover, they are both using the original data A, b. Thus, checking for $\mathbb{L}$-feasibility is about at most twice as time consuming as checking for real-feasibility. The same conclusion applies to the alternate LFP algorithm.

We will analyze the running time of the LFP algorithm and the output size of the alternate LFP algorithm (the analysis is somewhat cleaner for that version because of the use of ∞-norms). The *encoding size* of an integer α is defined as $\text{size}(\alpha) := \log_2(|\alpha| + 1)$.[3] The encoding size of a rational $\frac{r}{s}$ is defined as $\text{size}\left(\frac{r}{s}\right) := \text{size}(r) + \text{size}(s)$. Observe that for nonzero rationals $\frac{r}{s}, \frac{r'}{s'}$ we have $\text{size}\left(\frac{r}{s}\right) = \text{size}\left(\frac{s}{r}\right)$ and that $\text{size}\left(\frac{rr'}{ss'}\right) \leq \text{size}\left(\frac{r}{s}\right) + \text{size}\left(\frac{r'}{s'}\right)$. We consider p which appears in the (density) property of the set $\mathbb{L}$ to be an absolute constant. For each of Algorithms A-D we can view the input as an m'-by-n' matrix where the largest encoding size of any entry is given by σ. Then the runtime is bounded by a function f_a, f_b, f_c, f_d for each of algorithms A, B, C, D where f_a, f_b, f_c, f_d are functions of m', n', σ. In addition, for the output, the largest entry size is bounded by a function g_b, g_c, g_d for each of algorithms B, C, D where g_b, g_c, g_d are also functions of m', n', σ. There exist implementations for each algorithm where each of $f_a, f_b, f_c, f_d, g_b, g_c, g_d$ is a polynomial in m', n', σ. Note, for Algorithm B the runtime is in terms of the number of calls to the $\mathbb{L}$-oracle.

Let us now analyze the runtime.

Theorem 3.1. *Consider $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$ and let σ denote the largest size of any entry in A or b. Then the LFP algorithm has runtime*

$$O\big(f_a(n, n+1, \sigma') + f_b(m, n+1, \sigma) + f_c(m, n, \sigma) + f_d(m+n+1, n+2, \sigma)\big)$$

where

$$\sigma' = g_b(m, n+1, \sigma) + g_c(m, n, \sigma) + g_d(m+n+1, n+2, \sigma).$$

---

[3]Note that the number of bits required to represent α on a computer is $\lceil \text{size}(\alpha) \rceil + 1$, where we reserved an additional bit for the sign of α. Thus, $\text{size}(\alpha)$ is not the *true* encoding size, but it is easier to work with than $\lceil \text{size}(\alpha) \rceil + 1$, and differs from it by only a constant.

Proof. The runtime of the algorithm is longest when it finds a point in $P \cap \mathbb{L}^n$ so we assume that this is the case in the analysis. *Step 1.* The runtime is dominated by Algorithm D with A, b. It is in $O\big(f_d(m, n+1, \sigma)\big)$ since the data A, b can be represented as an m-by-$(n+1)$ matrix. The algorithm returns $\bar{x}$ and $\bar{y}$ which are used to find the implicit equalities $A^= x \leq b^=$ of $Ax \leq b$. *Step 2.* We run Algorithm B for the system $A^= x = b^=$. This takes $O\big(f_b(m, n+1, \sigma)\big)$ and we obtain $z \in \mathbb{L}^n \cap \mathbb{Q}^n$ with largest size of an entry in $O\big(g_b(m, n+1, \sigma)\big)$. We then use Algorithm C to get an integral basis $\{d^1, \ldots, d^\ell\}$ of $\{d : A^= d = \mathbf{0}\}$. Note that $\ell \leq n$. This takes $O\big(f_c(m, n, \sigma)\big)$ and for each $i \in [\ell]$ the largest size of an entry in d^i is $O\big(g_c(m, n, \sigma)\big)$. *Step 3.* The linear program (7) has $n+1$ variables and at most $m+n+1$ constraints. We run Algorithm D to solve it. This takes $O\big(f_d(m+n+1, n+2, \sigma)\big)$ and we return z' and ϵ with largest size of an entry in $O\big(g_d(m+n+1, n+2, \sigma)\big)$. *Step 4.* We solve the system $\sum_{i \in [\ell]} \alpha_i d^i = z' - z$ using Algorithm A. Note, that z, d^i, z' are outputs of Algorithms B, C and D respectively. As $\ell \leq n$, this takes $O\big(f_a(n, n+1, \sigma')\big)$ for σ' defined as in the statement. $\square$

We close this discussion by showing that functions g_b, g_c, g_d applied to the original data determine the size of the solution returned by the alternate LFP algorithm.

Theorem 3.2. *Consider $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$ and let σ denote the largest size of any of an entry in A or b. Assume that $P := \{x \geq \mathbf{0} : Ax = b\}$ contains a point in $\mathbb{L}^n$. Then the alternate LFP algorithm finds a point $\bar{x} \in P \cap \mathbb{L}^n \cap \mathbb{Q}^n$ with*

$$\text{size}(\|\bar{x}\|_\infty) \in O\big(g_b(m+n, n+1, \sigma) + g_c(m+n, n, \sigma) + g_d(m+n+1, n+1, \sigma) + \log(n)\big).$$

Proof. In Step 1, we find $J^=$ with $\text{aff}(P) = \{x : Ax = b, x_j = 0 \ \forall j \in J^=\}$. Thus $\text{aff}(P)$ is described by a system with at most $m+n$ constraints. In Step 2, we find $z \in \text{aff}(P)$ using Algorithm B. Hence,

$$\text{size}(\|z\|_\infty) \in O\big(g_b(m+n, n+1, \sigma)\big). \tag{11}$$

We then use Algorithm C to find an integer basis $d^1, \ldots, d^\ell$ of $\{d : Ad = \mathbf{0}, d_j = 0 \ \forall j \in J^=\}$. Thus,

$$\text{size}\big(\|d^i\|_\infty\big) \in O\big(g_c(m+n, n, \sigma)\big). \tag{12}$$

In Step 3, we solve (9) using Algorithm D. It follows that,

$$\text{size}(\epsilon), \text{size}\big(\|z'\|_\infty\big) \in O\big(g_d(m+n+1, n+1, \sigma)\big). \tag{13}$$

In Step 4 we pick r as in (10). Note, that $\ell \leq n$. Therefore,

$$\text{size}(p^r) \in O\big(\text{size}(\|d\|_\infty) + \text{size}(\epsilon) + \text{size}(n)\big).$$

By (12) and (13) in follows in turn that,

$$\text{size}(p^r) \in O\big(g_c(m+n, n, \sigma) + g_d(m+n+1, n+1, \sigma) + \log(n)\big). \tag{14}$$

In Step 4 we construct $\bar{\rho}$ as described in (3). Since $p = \infty$, Lemma 2.5(b) implies that for every $i \in [n]$

$$|p^r \bar{\rho}_i| \leq p^r(|z'_i - z_i| + 1). \tag{15}$$

Since $p^r \bar{\rho}_i \in \mathbb{Z}$ it follows from (15) that $\text{size}(p^r \bar{\rho}_i) \in O\big(\text{size}(p^r) + \text{size}(\|z\|_\infty) + \text{size}(\|z'\|_\infty)\big)$. This in turn implies,

$$\text{size}(\|\bar{x}\|_\infty) = \text{size}(\|z + \bar{\rho}\|_\infty) \in O\big(\text{size}(p^r) + \text{size}(\|z\|_\infty) + \text{size}\big(\|z'\|_\infty\big)\big).$$

The result now follows from (11), (13) and (14). $\square$

3.2 $\mathbb{L}$-Linear Programming

Suppose that $(\mathbb{L}, +)$ is a dense abelian subgroup of $(\mathbb{R}, +)$, and consider the following optimization problem,

$$\sup \left\{ c^\top x : Ax \leq b, \ x \in \mathbb{L}^n \right\}, \tag{16}$$

where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$ and $c \in \mathbb{Z}^n$. We say that (16) is an $\mathbb{L}$-*linear program*. Trivially, the status of this optimization problem has to fall within exactly one of the following outcomes:

(o1) it is infeasible,

(o2) it is unbounded,

(o3) it has an optimal solution,

(o4) it is feasible, bounded, but has no optimal solution.

Note that in contrast to linear programming, (o4) can occur, such as for $\sup\{x : 3x \leq 1, \ x \text{ dyadic}\}$.

3.2.1 Certificates

Here we certify each of the outcomes (o1)-(o4). We certified (o1) with a **certificate of $\mathbb{L}$-infeasibility** in Theorem 2.11. (o2) is similar to linear programming.

Theorem 3.3. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$ such that $\mathbb{Z} \subset \mathbb{L}$. Suppose that* (16) *is feasible. Then the following are equivalent:*

(a) (16) *is unbounded,*

(b) $\max\{c^\top x : Ax \leq b\}$ *is unbounded,*

(c) *there exists $r \in \mathbb{Z}^n$ with $Ar \leq \mathbf{0}$ and $c^\top r > 0$.*

A **certificate of unboundedness** *is a pair $(\bar{x}, r)$, where $\bar{x}$ is a feasible solution to* (16)*, and r is from (b).*

Proof. Denote by (P) the linear program $\max\{c^\top x : Ax \leq b\}$. Since (16) is feasible, so is (P). For the equivalence between (b) and (c), see Proposition 3.9 in [10]. Note, that for (c) the condition that r is rational is equivalent to the condition that r is integral because of scaling. We show that (a) and (b) are equivalent. First if (16) is unbounded, so is (P) since it is a relaxation of (16). Thus assume that (P) is unbounded. Then there exists r as described in (c). Let $\bar{x}$ be a feasible solution to (16) and for any λ define $x(\lambda) := \bar{x} + \lambda r$. Consider $\lambda \in \mathbb{Z}$ where $\lambda \geq 0$. Then $\lambda r \in \mathbb{Z}^n$. By the hypothesis $\mathbb{L} \supset \mathbb{Z}$, it follows that $\lambda r \in \mathbb{L}^n$. Since $\mathbb{L}$ is closed under addition and negation, $x(\lambda) \in \mathbb{L}^n$ and is therefore feasible for (16). For $\lambda \to \infty$ we have $c^\top x(\lambda) \to \infty$. Hence, (16) is unbounded. $\qquad\square$

We next distinguish between outcomes (o3) and (o4).

Theorem 3.4. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$. Suppose that* (16) *is feasible and bounded. Then the following are equivalent,*

(a) (16) *has no optimal solution,*

(b) there exist $\bar{x} \in \mathbb{R}^n$ and $\bar{y}, \bar{u} \in \mathbb{R}^m$ that satisfy the following conditions,

    (i) $\mathrm{support}(\bar{u}) \subseteq \mathrm{support}(\bar{y})$,

    (ii) $A\bar{x} \le b$, $A^\top \bar{y} = c$, $\bar{y} \ge \mathbf{0}$, $c^\top \bar{x} = b^\top \bar{y}$,

    (iii) $A^\top \bar{u}$ is integral and $b^\top \bar{u} \notin \mathbb{L}$.

A **certificate of unattainability** *is a triple $(\bar{x}, \bar{y}, \bar{u})$ satisfying (i)-(iii).*

Proof. Note that when $\mathbb{L} = \mathbb{R}$, then neither (a) nor (b) holds. Thus, we may assume $\mathbb{L} \ne \mathbb{R}$. Condition (ii) implies that $\bar{x}$ and $\bar{y}$ form a pair of primal dual solutions with the same value, hence, $\bar{y}$ is optimal for the dual of (P). Conversely, if $\bar{y}$ is optimal, then by strong duality there exists an optimal solution $\bar{x}$ of (P) with $c^\top \bar{x} = b^\top \bar{y}$. Thus condition (ii) simply says that $\bar{y}$ is optimal for the dual. The result now follows from Lemma 2.10. $\qquad\square$

We can be more specific about (o4). When (16) is feasible and bounded, then we say that a feasible solution $\bar{x} \in \mathbb{L}^n$ is an ϵ-*approximation* if $c^\top \bar{x} \ge \max\{c^\top x : Ax \le b\} - \epsilon$. The result below shows that for every $\epsilon > 0$ there exists an ϵ-approximation.

Theorem 3.5. *Let $(\mathbb{L}, +)$ be a dense abelian subgroup of $(\mathbb{R}, +)$ such that $\mathbb{Z} \subset \mathbb{L}$. If (16) is feasible and bounded, then,*

$$\sup \left\{ c^\top x : Ax \le b, \ x \in \mathbb{L}^n \right\} = \max\{c^\top x : Ax \le b\}.$$

Proof. Denote by (P) the linear program $\max\{c^\top x : Ax \le b\}$. Since (16) is feasible so is (P). Since (16) is bounded, so is (P) by Theorem 3.3. It follows that (P) has an optimal solution, say $\bar{x}$ and let $\tau := c^\top \bar{x}$. Pick $\epsilon > 0$ and define $Q_\epsilon := \{x : Ax \le b\} \cap \{x : c^\top x \ge \tau - \epsilon\}$. Because of $\bar{x}$, $c^\top x \ge \tau - \epsilon$ is not an implicit equality of Q_ϵ. Therefore, $\{x : Ax \le b\}$ and Q_ϵ have the same implicit equalities, say $A^= x \le b^=$. Hence, $\mathrm{aff}(\{x : Ax \le b\}) = \mathrm{aff}(Q_\epsilon) = \{x : A^= x = b^=\}$. Since (16) is feasible, there exists a solution to $A^= x = b^=$ in $\mathbb{L}^n$. Hence, by Corollary 2.6 there exists a point in $Q_\epsilon \cap \mathbb{L}^n$. In particular, $\sup\{c^\top x : Ax \le b, \ x \in \mathbb{L}^n\}$ has a feasible solution of value $\ge \tau - \epsilon$. Letting $\epsilon \to 0$ proves the result. $\qquad\square$

3.2.2 Outcomes for primal-dual pairs

Here we review the possible outcomes for a primal-dual pair of $\mathbb{L}$-linear programs. Namely, we consider the following pair of optimization problems,

$$\sup\{c^\top x : Ax \le b, \ x \in \mathbb{L}^n\}, \qquad\qquad\qquad \text{(P)}$$
$$\inf\{b^\top y : A^\top y = c, \ y \ge \mathbf{0}, y \in \mathbb{L}^m\} \qquad\qquad\qquad \text{(D)}$$

where $(\mathbb{L}, +)$ is a dense abelian subgroup of $(\mathbb{R}, +)$ such that $\mathbb{Z} \subset \mathbb{L}$. We observed that each of (P) and (D) has 4 possible outcomes (o1)-(o4). In the next table we indicate the possible pairs of outcomes for (P) and (D). The rows of the matrix indicate the possible outcomes for (P) and the columns of the matrix indicate the possible outcomes for (D). A check mark in the table indicates that the corresponding outcome is possible for *some* choice of $\mathbb{L}$, and a cross that the outcome is not possible for *any* choice

	(o1)	(o2)	(o3)	(o4)
(o1)	✓	✓	✓	✓
(o2)	✓	✗	✗	✗
(o3)	✓	✗	✓	✓
(o4)	✓	✗	✓	✓

Table 1: Possible outcomes for (P) and (D).

of $\mathbb{L}$. We illustrate some of these outcomes. Consider the following dyadic linear programs, which can easily be brought into (P)'s format:

$$\sup\{3x : 3x = 1, x \geq \mathbf{0}, x \text{ dyadic}\}, \tag{17}$$
$$\sup\{x : 3x = 1, x \geq \mathbf{0}, x \text{ dyadic}\}, \tag{18}$$
$$\sup\{x : 3x \leq 3, x \geq \mathbf{0}, x \text{ dyadic}\}, \tag{19}$$
$$\sup\{x : 3x \leq 1, x \geq \mathbf{0}, x \text{ dyadic}\}. \tag{20}$$

Then for (P) described as (17) and its dual (D) we have outcomes (o1) for (P) and (o3) for (D). Similarly, (18) corresponds to row (o1) and column (o4); (19) corresponds to row (o3) and column (o4); and (20) corresponds to row (o4) and column (o4). Note that (17)-(20) extend more generally to any dense abelian group $\mathbb{L}$ that does not contain $\mathbb{Q}$ (e.g., if $\frac{b}{a} \notin \mathbb{L}$ for $a, b \in \mathbb{Z}_{\geq 0}, a \neq 0$, then replace (20) by $\sup\{bx : ax \leq b, x \geq \mathbf{0}, x \in \mathbb{L}\}$). Table 1 is also applicable to pairs of primal-dual convex optimization problems in conic form (although the details of their duality theory are significantly more complicated than our setting, from this very specific and high level view, they coincide).

We close this discussion by including a table that indicates the possible pairs of outcomes for (P) and the LP relaxation of (D). The rows of the matrix indicate the possible outcomes for (P) and the columns of the matrix indicate the possible outcomes for the LP relaxation of (D).

	(o1)	(o2)	(o3)
(o1)	✓	✓	✓
(o2)	✓	✗	✗
(o3)	✗	✗	✓
(o4)	✗	✗	✓

Table 2: Possible outcomes for (P) and the LP relaxation of its dual (D).

3.2.3 Algorithm for solving $\mathbb{L}$-linear programs

We consider $\mathbb{L}$ satisfying the (group), (density) and (membership) properties (with p given explicitly). Observe that $\mathbb{L} \supset \mathbb{Z}$ and $\mathbb{L}$ satisfies the hypotheses of Theorem 3.3, Theorem 3.4, and Theorem 3.5, that characterize possible outcomes, and ϵ-approximation for $\mathbb{L}$-linear programs.

We are given $\epsilon > 0$, integral matrices and vectors A, b, c describing the $\mathbb{L}$-linear program (16). Then in oracle polynomial time we return one of the following, (i) a certificate of real-infeasibility, (ii) a certificate of $\mathbb{L}$-infeasibility, (iii) a certificate of unboundedness, (iv) an optimal solution, (v) a certificate of unattainability and an ϵ-approximation. Note, if we know that we have one of outcomes (o1), (o2), (o3) then it is not necessary to supply ϵ. A schematic representation of the algorithm is given in Figure 1.

First we apply the LFP algorithm to $P = \{x : Ax \leq b\}$. If it returns a certificate of real-infeasibility, or a certificate of $\mathbb{L}$-infeasibility, we stop. Otherwise, it returns a point $x^f \in P \cap \mathbb{L}^n$. We
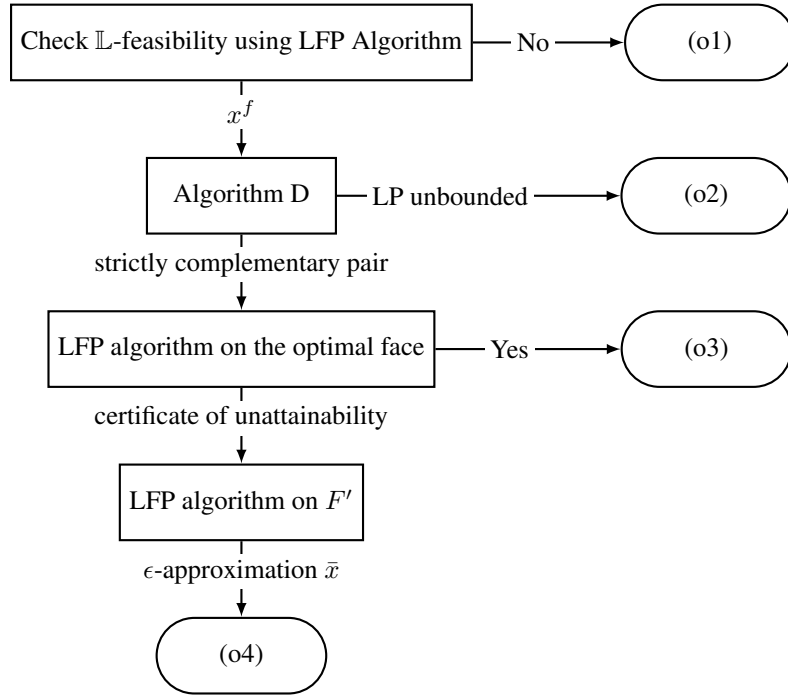
Figure 1: Schematic description of the $\mathbb{L}$-linear program solver

then consider the linear programming relaxation,

$$\max\{c^\top x : Ax \le b\}, \tag{P}$$

of (16) and use Algorithm D to solve it. Note that since (16) is feasible so is (P). If (P) is unbounded, then Algorithm D will return a rational vector r with $Ar \le \mathbf{0}$. After scaling we may assume that $r \in \mathbb{Z}^n$ and x^f, r is a certificate of unboundedness. Thus, we may assume that Algorithm D returns a strictly complementary pair $x^\star$ of (P) and $y^\star$ of its dual (D). Then define the face

$$F := P \cap \{x : c^\top x \ge c^\top x^\star\}.$$

Let $I^= := \text{support}(y^\star)$ and let $A^= x \le b^=$ be the inequalities from $Ax \le b$ indexed by $I^=$. Note that face F is obtained from P by setting some inequalities to equalities. Furthermore, by strict complementarity, $A^= x = b^=$ is the set of implicit equalities of F. It follows that,

Claim. $F = P \cap \{x : A^= x = b^=\}$ *and* $\text{aff}(F) = \{x : A^= x = b^=\}$.

We then apply the LFP algorithm to the system $Ax \le b, A^= x \ge b^=$ that defines F. If the algorithm returns a point $x^d \in F \cap \mathbb{L}^n$ then x^d is an optimal solution to (16) and we stop. Otherwise the LFP algorithm will return a certificate $\bar{y}, \bar{u}$ of $\mathbb{L}$-infeasibility for F. Theorem 2.11 implies that $\text{support}(\bar{y}) \subseteq I^=$. Then we have $\text{support}(\bar{u}) \subseteq \text{support}(\bar{y}) \subseteq I^= = \text{support}(y^\star)$. It follows that $x^\star, y^\star, \bar{u}$ is a certificate of unattainability.

At this juncture we look for an ϵ-approximation by running the LFP algorithm for the polyhedron,

$$F' = P \cap \{x : c^\top x \ge c^\top x^\star - \epsilon\}.$$

18

Note that since A, b, c are rational, so is $c^\top x^\star$, so F' is a rational polyhedron. By Theorem 3.5 F' contains a point in $\mathbb{L}^n$. We use the LFP algorithm once more to find such a point in F'.

3.2.4 Solving linear programs versus solving $\mathbb{L}$-linear programs

Solving the $\mathbb{L}$-linear program required at most two calls of the LFP procedure for outcomes (o1)-(o3) and three calls in case of outcome (o4). Thus the running time of our $\mathbb{L}$-linear program solver is at most three times that of LFP.

   We have shown that we can use a black-box algorithm that solves the $\mathbb{L}$-feasibility problem to solve $\mathbb{L}$-linear programs. Moreover, our LFP algorithm leverages a linear program solver to solve the $\mathbb{L}$-feasibility problem. Thus $\mathbb{L}$-linear programs can be solved using a black-box linear program solver. Here we show the converse, namely one may use a single call to a black-box algorithm for solving $\mathbb{L}$-linear programs, to solve linear feasibility problems over rationals, i.e., finding a rational point in a polyhedron (which in turn is sufficient for solving linear programs).

   Suppose we are given $A \in \mathbb{Z}^{m \times n}$ of full row rank and $b \in \mathbb{Z}^m$ and want to find $x \in \mathbb{Q}^n$ such that $Ax = b, x \geq \mathbf{0}$ or prove that no such x exists. We are given an $\mathbb{L}$-linear program solver that works for a specific set $\mathbb{L}$ where $\mathbb{L}$ satisfies our (group), (density), and (membership) conditions. Note that we do not get to choose $\mathbb{L}$, it could be for instance that $\mathbb{L}$ is the set of p-adic numbers for $p = 2^{82,589,933} - 1$ (which happens to be prime). We feed the $\mathbb{L}$-linear program solver the optimization problem:

$$\inf \left\{ t \; : \; Ax + bt = b, \; x \geq \mathbf{0}, \; t \geq 0, \; x \in \mathbb{L}^n, \; t \in \mathbb{L} \right\}, \tag{21}$$

and we pick $\epsilon := 2^{-2 \, \mathsf{size}(A,b)}$.

   Note that with $\bar{x} := \mathbf{0}$, $\bar{t} := 1$, $(\bar{x}, \bar{t}) \in \mathbb{L}^{n+1}$ makes a feasible solution for (21). Since (21) is not unbounded ($t \geq 0$ for all feasible solutions), the only possible outcomes are (o3) and (o4). In case of (o3), the $\mathbb{L}$-linear program solver returns a feasible solution $(\bar{x}, \bar{t})$ of (21) with the smallest possible $\bar{t}$. If $\bar{t} = 0$ then $\bar{x} \in \mathbb{Q}_{\geq 0}^n$ such that $A\bar{x} = b$. If $\bar{t} > 0$ then Theorem 3.5 proves that the LP relaxation of (21) has optimal value $\bar{t} > 0$, in particular $Ax = b, x \geq \mathbf{0}$ is infeasible. In the case of outcome (o4), the solver returns a certificate of unattainability and an ϵ-approximation $(\bar{x}, \bar{t})$. If $\bar{t} > \epsilon$ then again Theorem 3.5 proves that the LP relaxation of (21) has optimal value $\bar{t} > 0$, and $Ax = b, x \geq \mathbf{0}$ is infeasible. Otherwise, $\bar{t} \leq \epsilon$. Since $\bar{t} \leq 2^{-2 \, \mathsf{size}(A,b)}$, every extreme point of

$$\left\{ (x, t) \in \mathbb{R}^{n+1} \; : \; Ax + bt = b, \; x \geq \mathbf{0}, \; t \geq 0 \right\}$$

whose objective value is less than or equal to $\bar{t}$ must have $\bar{t} = 0$. Such an extreme point exists (and is guaranteed to be rational due to integrality of A and b), and can be found in strongly polynomial time (i.e., the number of elementary arithmetic operations is bounded above by a polynomial function of n only), starting with $(\bar{x}, \bar{t})$ (see, for instance, [24] and [31, Section 4.3]). The "x-part" of such an extreme point is a rational solution of $Ax = b, x \geq \mathbf{0}$.

   One of the complexity measures of our algorithms and analyses is based on the radius of the largest Euclidean ball contained in some polyhedra. Similar complexity measures have been used before in analyzing the complexity of algorithms based on the ellipsoid method as well as interior-point algorithms for linear programs in particular, and convex optimization problems in general. We will remark on the primal-dual version. Consider the primal-dual pair of LPs where A is m-by-n:

$$\min \left\{ c^\top x \; : \; Ax = b, \; x \geq \mathbf{0} \right\} \quad \text{and} \quad \max \left\{ b^\top y \; : \; A^\top y + s = c, \; s \geq \mathbf{0} \right\}.$$

Suppose that both are feasible. Let $[B, N]$ denote the strict complementarity partition of $[n]$ for this primal-dual pair. One then defines

$$r_P(A, b, c) := \min_{j \in B} \left\{ \max \left\{ x_j \ : \ A_B x_B = b, \ x_B \geq \mathbf{0} \right\} \right\},$$
$$r_D(A, b, c) := \min_{j \in N} \left\{ \max \left\{ s_j \ : \ A_B^\top y = c_B, \ A_N^\top y + s_N = c_N, \ s_N \geq \mathbf{0} \right\} \right\},$$
$$r(A, b, c) := \min \left\{ r_P(A, b, c), r_D(A, b, c) \right\}.$$

There are polynomial time algorithms for linear programs whose complexity are bounded above by a polynomial function of n and $\log(1/r(A, b, c))$ [25, 33] (assuming suitable feasible start, or one can apply the approach to a homogeneous self-dual reformulation, see [34, 19], the reformulation would change r though). Note that $r_P(A, b, c)$ is essentially the radius we used in our approach for problems in standard equality form. $r_D(A, b, c)$ would also correspond to the radius we used for problems in inequality form, provided the columns of A are scaled so that they are all approximately of unit norm. In this latter case, $r(A, b, c)$ would also be relevant for our analysis when we are interested in finding solutions for primal-dual pair of $\mathbb{L}$-linear programs.

4 Bounding the fractionality of dyadic solutions

Given a dyadic linear program $Ax \leq b, x$ dyadic that is feasible, for some $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$, can we find a solution whose denominators are "small"? In this section, we prove that if the program is feasible, then there exists a $\frac{1}{2^k}$-integral solution, where $k \leq \lceil \log_2 n + (2n + 1) \log_2(\|A\|_\infty \sqrt{n + 1}) \rceil$. In doing so, we take an integer linear programming perspective towards dyadic linear programs, in contrast to the linear programming approach taken in the previous sections. The results in this section are presented more generally for the p-adic numbers for any prime $p \geq 2$.

A hierarchy of integer linear programs. Let p be a prime, and $\mathbb{L} := \left\{ \frac{a}{p^\ell} : a, \ell \in \mathbb{Z}, \ell \geq 0 \right\}$ the set of p-adic numbers. Consider the $\mathbb{L}$-linear program:

$$\sup\{c^\top x : Ax \leq b, x \text{ is } p\text{-adic}\}, \tag{p-LP}$$

where $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m, c \in \mathbb{Z}^n$. For each integer $k \geq 0$, consider the following restriction of (p-LP):

$$\max\{c^\top x : Ax \leq b, x \text{ is } 1/p^k\text{-integral}\}, \tag{p-LP$_k$}$$

where we replaced sup by max because every element of the domain is isolated. In fact, (p-LP$_k$) is equivalent to the ILP $\max\{c^\top z \ : \ Az \leq p^k b, z \in \mathbb{Z}^n\}$, in the sense that if x is a feasible solution to (p-LP$_k$) of value α, then $p^k x$ is a feasible solution to the ILP of value $p^k \alpha$, and if z is a feasible solution to the ILP of value β, then $\frac{1}{p^k} z$ is a feasible solution to (p-LP$_k$) of value $\frac{1}{p^k} \beta$.

Denote by $\sup(p\text{-LP})$ the supremum value of (p-LP); if the $\mathbb{L}$-LP is infeasible then $\sup(p\text{-LP}) := -\infty$, and if it is unbounded then $\sup(p\text{-LP}) := +\infty$.[4] Similarly, we define $\text{opt}(p\text{-LP}_k)$ for each integer $k \geq 0$. Clearly we have the following chain of inequalities:

$$\text{opt}(p\text{-LP}_0) \leq \text{opt}(p\text{-LP}_1) \leq \text{opt}(p\text{-LP}_2) \leq \cdots \leq \sup(p\text{-LP}) \tag{22}$$

---

[4]Observe that when $\sup(p\text{-LP})$ is finite, then $\sup(p\text{-LP}) = \max\{c^\top x \ : \ Ax \leq b\}$ by Theorem 3.5. This equality, however, is not the focus in this section.

where any value in the chain may be finite or $\pm\infty$. In fact, we have the following theorem, thereby justifying our integer linear programming perspective.

Theorem 4.1. $\lim_{k\to\infty} \mathrm{opt}(p\text{-}LP_k) = \sup(p\text{-}LP)$. *In fact,* $\mathrm{opt}(p\text{-}LP_k) = \sup(p\text{-}LP)$ *for sufficiently large* k, *unless* $\sup(p\text{-}LP)$ *is finite and not attained by any feasible solution to* $(p\text{-}LP)$.

Proof. There are three cases:

1. If $\sup(p\text{-}LP) = -\infty$, then clearly, $\mathrm{opt}(p\text{-}LP_k) = \sup(p\text{-}LP)$ for all $k \geq 0$.

2. If $\sup(p\text{-}LP) = +\infty$, then the linear relaxation of $(p\text{-}LP)$ is also unbounded, so there is an extreme ray $r \in \mathbb{R}^n$ of the polyhedron $\{x : Ax \leq b\}$ such that $c^\top r > 0$. Given that A, b have integral entries, we may assume that r is integral. Let $\bar{x}$ be any feasible solution to $(p\text{-}LP)$. Then $\bar{x}$ is $1/p^N$-integral for some integer $N \geq 0$. It can be readily checked that $(\bar{x} + t \cdot r : t = 0, 1, 2, \ldots)$ is an infinite sequence of feasible solutions to $(p\text{-}LP_k)$ of arbitrarily large objective value, for any integer $k \geq N$. Subsequently, $\mathrm{opt}(p\text{-}LP_k) = +\infty$ for all $k \geq N$.

3. Otherwise, $\sup(p\text{-}LP)$ is finite. The inequalities in (22), together with the Monotone Convergent Theorem from Real Analysis, imply that $\lim_{k\to\infty} \mathrm{opt}(p\text{-}LP_k)$ exists. In fact, the sequence must converge to $\sup(p\text{-}LP)$ as we argue below.

   (a) If the optimal value of $(p\text{-}LP)$ is attained, say by $\bar{x}$ that is $1/p^N$-integral for some integer $N \geq 0$, then $\bar{x}$ is an optimal solution to $(p\text{-}LP_N)$, so $\mathrm{opt}(p\text{-}LP_N) = \sup(p\text{-}LP)$. Subsequently, it follows from (22) that $\mathrm{opt}(p\text{-}LP_k) = \sup(p\text{-}LP)$ for all $k \geq N$.

   (b) Otherwise, $\sup(p\text{-}LP)$ is finite but the optimal value is not attained by any feasible solution. In this case, by definition, there exists a sequence of feasible solutions $(\bar{x}^i : i \geq 1)$ to $(p\text{-}LP)$ such that $\lim_{i\to\infty} c^\top \bar{x}^i = \sup(p\text{-}LP)$. Observe that each $\bar{x}^i$ is feasible solution to $(p\text{-}LP_k)$ for some sufficiently large k. Subsequently,

   $$\sup(p\text{-}LP) = \lim_{i\to\infty} c^\top \bar{x}^i \leq \lim_{k\to\infty} \mathrm{opt}(p\text{-}LP_k) \leq \sup(p\text{-}LP)$$

   where the last inequality follows from (22). Equality must hold throughout, so we have $\lim_{k\to\infty} \mathrm{opt}(p\text{-}LP_k) = \sup(p\text{-}LP)$, as required.

   $\square$

Given the theorem above, a natural question is for how small of a k can we guarantee $\mathrm{opt}(p\text{-}LP_k) = \sup(p\text{-}LP)$? By switching to an equivalent model, for the sake of convenience, we may instead ask: given that $(p\text{-}LP)$ is feasible, what is the smallest integer k such that $(p\text{-}LP_k)$ is feasible? In what follows, we provide a polynomial upper bound on the size of the smallest k.[5] For more on $\gcd(A)$, see Appendix A.

Lemma 4.2. *Let A be an $m \times n$ integer matrix of full row rank, and let $(B\ \mathbf{0})$ be the Hermite normal form of A, where B is a square matrix. Then for all $b \in \mathbb{Z}^m$ and $k \in \mathbb{Z}_+$, the following statements are equivalent:*

---

[5]Note that this statement has no bearing on the time complexity of solving $(p\text{-}LP_k)$. Given a fixed integer $k \geq 0$ (possibly $k = 0$), $(p\text{-}LP_k)$ is NP-hard as its decision version is NP-complete (*Given A, b and $k \geq 0$, does $Ax \leq b$ have a $1/p^k$-integral solution?*) (see [7], Chapter 2).

i. $Ax = b$ has a $1/p^k$-integral solution,

ii. $B^{-1}b$ is $1/p^k$-integral.

Moreover, if $Ax = b$ has a $1/p^\kappa$-integral solution, and $\kappa \geq 0$ is the smallest such integer, then p^κ divides $\gcd(A)$.

Proof. Let U be a unimodular matrix such that $AU = (B\ \mathbf{0})$ is in Hermite normal form, where B is a square matrix. Let I, J be the sets of column labels of $B, \mathbf{0}$ in $(B\ \mathbf{0})$. Observe that $\{x : Ax = b\} = \{Uz : z_I = B^{-1}b, z_J$ free$\}$. Since U is unimodular, U^{-1} is integral, so Uz is $1/p^k$-integral if and only if $z = U^{-1}(Uz)$ is $1/p^k$-integral. This implies that $Ax = b$ has a $1/p^k$-integral solution if, and only if, $B^{-1}b$ is $1/p^k$-integral, so (i) and (ii) are equivalent.

Suppose now that $Ax = b$ has a $1/p^\kappa$-integral solution, and κ is the smallest such integer. If $\kappa = 0$, then $p^\kappa = 1$, so we are done. Otherwise, $\kappa \geq 1$. It follows from our choice of κ that $B^{-1}b$ is not $1/p^{\kappa-1}$-integral but it is $1/p^\kappa$-integral. On the other hand, by Cramer's rule, $B^{-1}b$ is $1/\det(B)$-integral, so $p^\kappa \mid \det(B)$. Since $\det(B) = \gcd(A)$, it follows that p^κ divides $\gcd(A)$, as required. $\square$

Given the system $Ax = b$ above, we can use the algorithm of Kannan and Bachem [21] to compute the Hermite normal form in strongly polynomial time. The state-of-the-art can be found in Storjohann's PhD thesis, giving an algorithm with running time complexity nm^ω, where $\omega \in (2, 2.376)$ is the matrix multiplication exponent, and the absolute value of each entry of B, U is bounded above by $m(\sqrt{m}\|A\|_\infty)^{2m}$ ([30], Chapter 6). Either of these leads to a strongly polynomial time algorithm for finding κ, or certifying that it does not exist.

Moving forward, for $A \in \mathbb{Z}^{m \times n}$, define

$$\xi_p(A, b) := \min\{k \in \mathbb{Z}_+ : Ax \leq b \text{ has a } 1/p^k\text{-integral solution}\} \qquad \forall\, b \in \mathbb{Z}^m$$
$$\xi_p(A) := \max\left\{\xi_p(A, b) : b \in \mathbb{Z}^m \text{ s.t. } Ax \leq b \text{ has a } p\text{-adic solution}\right\}.$$

Thus, for any $b \in \mathbb{Z}^m$ such that $Ax \leq b$ has a p-adic solution, there is a $1/p^k$-integral solution for $k = \xi_p(A)$. In what follows, we provide an upper bound on $\xi_p(A)$ that depends only polynomially on n and the encoding size of A.

Theorem 4.3. $\xi_p(A) \leq \left\lceil \log_p n + (2n+1)\log_p(\|A\|_\infty \sqrt{n+1}) \right\rceil$ *for all $A \in \mathbb{Z}^{m \times n}$.*

Proof. Let $P := \{x : Ax \leq b\}$. We need to prove that for some $k \leq \text{RHS}$, P contains a $1/p^k$-integral point. We shall apply Lemma 2.5.

Denote by $A^=x \leq b^=$ the subsystem comprised of all implicit equalities of $Ax \leq b$, and by $A^<x \leq b^<$ the subsystem for the other inequalities. Let $F := \{x : A^=x = b^=\}$, which is the affine hull of P.

Recall that $B_\infty(x, \epsilon) \subseteq \mathbb{R}^n$ is the ∞-norm closed ball of radius ϵ centered at x. Let $\tilde{\epsilon} := \max\left\{\epsilon : \exists\, x \in P \text{ s.t. } B_\infty(x, \epsilon) \cap F \subseteq P\right\}$, and let $\tilde{B}$ be an ∞-norm closed ball of radius $\tilde{\epsilon}$ such that $\tilde{B} \cap F \subseteq P$.

Finally, let $\kappa := \min\{k : F \text{ contains a } 1/p^k\text{-integral point}\}$. Let z be a $1/p^\kappa$-integral point in F. Let $\ell := \text{nullity}(A^=)$, and let $d^1, \ldots, d^\ell \in \mathbb{Z}^n$ be a basis for $\ker(A^=)$. Note that $F = z + \text{span}\{d^1, \ldots, d^\ell\}$.

Claim 1. *P contains a $1/p^k$-integral point for all $k \geq \max\left\{\kappa, \left\lceil \log_p\left(\frac{\ell \max\{\|d^1\|_\infty, \ldots, \|d^\ell\|_\infty\}}{\tilde{\epsilon}}\right) \right\rceil\right\}$.*

Proof of Claim. If $k \geq \log_p \left(\frac{\ell \max\{\|d^1\|_\infty, \ldots, \|d^\ell\|_\infty\}}{\tilde{\epsilon}} \right)$, there exists a $1/p^k$-integral $\bar{\rho} \in \mathbb{R}^n$ such that $z + \bar{\rho} \in P$, by Lemma 2.5. Moreover, if $k \geq \kappa$ and z is $1/p^\kappa$-integral, it follows that $z + \bar{\rho}$ is $1/p^k$-integral; $z + \bar{\rho}$ is the desired point (which in fact belongs to $\tilde{B}$). $\diamond$

It therefore suffices to upper bound κ, $\log_p(\max_i \|d^i\|_\infty)$ and $-\log_p(\tilde{\epsilon})$.

Claim 2. p^κ *divides* $\gcd(A^=)$. *In particular,* $\kappa \leq (n - \ell) \log_p(\|A^=\|_\infty \sqrt{n - \ell})$.

Proof of Claim. Note that $\text{rank}(A^=) = n - \ell$. Let $A'x = b'$ be a system of $n - \ell$ linearly independent constraints of $A^=x = b^=$. Observe that $\{x : A'x = b'\} = \{x : A^=x = b^=\}$. It follows from Lemma 4.2 that p^κ divides $\gcd(A')$ which in turn divides every subdeterminant of A' of order $n - \ell$. By repeating this argument for every choice of A', we obtain that p^κ divides every subdeterminant of $A^=$ of order $n - \ell$, so p^κ divides $\gcd(A^=)$. By Hadamard's inequality (see Appendix A for more), $\gcd(A^=) \leq (\|A^=\|_\infty \sqrt{n - \ell})^{n-\ell}$, so $\kappa \leq (n - \ell) \log_p(\|A^=\|_\infty \sqrt{n - \ell})$. $\diamond$

Claim 3. *We may choose* $d^1, \ldots, d^\ell$ *such that* $\log_p(\max_i \|d^i\|_\infty) \leq (n - \ell) \log_p(\|A^=\|_\infty \sqrt{n - \ell})$.

Proof of Claim. Let A' be a row submatrix of $A^=$ comprised of $n - \ell$ linearly independent rows. Observe that $A', A^=$ have the same kernel. Let A'' be a square nonsingular column submatrix of A'. Denote by I and J the sets of column labels of A' inside and outside A'', respectively. Note that $|J| = \ell$. For each $j \in J$, the jth column of A' can be expressed as a unique linear combination of the columns of A''. Subsequently one obtains ℓ vectors in $\ker(A')$, say $c^j \in \mathbb{R}^n, j \in J$, where each c^j has only one nonzero entry in J, namely in the jth position. To elaborate, c^j is the difference between the jth column of A', and the unique linear combination of the columns of A''. In particular, $c^j, j \in J$ are linearly independent and therefore form a basis of $\ker(A')$. By applying Cramer's rule, we see that for all $j \in J, i \in I$, we have $c_i^j = \pm \frac{\det(B)}{\det(A'')}$ where B is obtained from A'' by swapping out the ith column for the jth column of A'. The desired vectors $d^1, \ldots, d^\ell$ may be picked as $\det(A'') \cdot c^j, j \in J$. Note that $\max_i \|d^i\|_\infty$ is at most the absolute value of the maximum subdeterminant of A' of order $n - \ell$. Thus, by Hadamard's inequality, $\max_i \|d^i\|_\infty \leq (\|A'\|_\infty \sqrt{n - \ell})^{n-\ell}$, thereby proving the claim. $\diamond$

Claim 4. $\tilde{\epsilon} \geq \frac{1}{|M| \max_i(|A^<|\mathbf{1})_i}$ *where* M *is a minor of* $\left(\begin{smallmatrix} A^= & \mathbf{0} \\ A^< & \mathbf{1} \end{smallmatrix} \right)$, *and* $|A^<|$ *is obtained from* $A^<$ *by replacing every entry with its absolute value. In particular,* $-\log_p(\tilde{\epsilon}) \leq (n+1) \log_p(\|A\|_\infty \sqrt{n + 1}) + \log_p(n\|A^<\|_\infty)$.

Proof of Claim. Consider the LP $\max\{t : A^=x = b^=, A^<x + t\mathbf{1} \leq b^<\}$. Let $(\tilde{x}, \tilde{t})$ be a basic optimal solution to the LP. Our choice of $A^<x \leq b^<$ immediately implies that $\tilde{t} > 0$, and so because A, b have integral entries, it follows from Cramer's rule that $\tilde{t} \geq \frac{1}{|M|}$ where M is a minor of $\left(\begin{smallmatrix} A^= & \mathbf{0} \\ A^< & \mathbf{1} \end{smallmatrix} \right)$. Let $\epsilon := \frac{\tilde{t}}{\max_i(|A^<|\mathbf{1})_i}$. We claim that $B_\infty(\tilde{x}, \epsilon) \cap F \subseteq P$. To this end, pick a point $x \in F$ such that $\|x - \tilde{x}\|_\infty \leq \epsilon$. Then

$$A^<(x - \tilde{x}) \leq |A^<(x - \tilde{x})| \leq |A^<||x - \tilde{x}| \leq \epsilon|A^<|\mathbf{1} \leq \tilde{t}\mathbf{1} \leq b^< - A^<\tilde{x},$$

so $A^<x \leq b^<$, implying that $x \in P$. Thus, $B_\infty(\tilde{x}, \epsilon) \cap F \subseteq P$. By definition, we must have $\tilde{\epsilon} \geq \epsilon$, and since $\epsilon \geq \frac{1}{|M| \max_i(|A^<|\mathbf{1})_i}$, we get that $\tilde{\epsilon} \geq \frac{1}{|M| \max_i(|A^<|\mathbf{1})_i}$. The inequality $-\log_p(\tilde{\epsilon}) \leq (n+1) \log_p(\|A\|_\infty \sqrt{n + 1}) + \log_p(n\|A^<\|_\infty)$ follows by an application of Hadamard's inequality. $\diamond$

Observe that our upper bounds on κ and $\log_p(\max_i \|d^i\|_\infty)$ are matching, thus we may ignore κ when applying Claim 1. Putting the claims together, we see that for some integer $k \geq 0$ satisfying

$$k \leq \left\lceil \log_p \ell + \log_p(\max_i \|d^i\|_\infty) - \log_p(\tilde{\epsilon}) \right\rceil \leq \left\lceil \log_p n + (2n+1) \log_p(\|A\|_\infty \sqrt{n+1}) \right\rceil,$$

P contains a $1/p^k$-integral point, thereby proving the theorem. $\qquad\square$

Corollary 4.4. *Fix a matrix $A \in \mathbb{Z}^{m \times n}$. Suppose p is a sufficiently large prime number. Then the following statements hold:*

    a. For any $b \in \mathbb{Z}^m$, if $Ax = b$ has a p-adic solution, then it has an integral solution.

    b. For any $b \in \mathbb{Z}^m$, if $Ax \leq b$ has a p-adic solution, then it has a $1/p$-integral solution. That is, $\lim_{p \to \infty} \xi_p(A) \leq 1$.

Proof. **(a)** Suppose p is a prime number such that $p > \gcd(A)$, and that for some $b \in \mathbb{Z}^m$, $Ax = b$ has a p-adic solution. Let κ be the smallest integer $k \geq 0$ such that $Ax = b$ has a $1/p^\kappa$-integral solution. It then follows from Lemma 4.2 that $p^\kappa \mid \gcd(A)$. Since $p > \gcd(A)$, it follows that $\kappa = 0$. Thus, $Ax = b$ has an integral solution.

    (b) We know from Theorem 4.3 that $\xi_p(A) \leq \left\lceil \log_p n + (2n+1) \log_p(\|A\|_\infty \sqrt{n+1}) \right\rceil$. Given a fixed A, the RHS approaches 1 as p tends to ∞, implying in turn that $\lim_{p \to \infty} \xi_p(A) \leq 1$, as required. $\qquad\square$

Another consequence of Theorem 4.3 is the following, bringing this section to an end.

Corollary 4.5. *Let $A \in \mathbb{Z}^{m \times n}$. Given a feasible dyadic linear program $Ax \leq b, x$ dyadic, for some $b \in \mathbb{Z}^m$, there exists a $\frac{1}{2^k}$-integral solution where $k \leq \left\lceil \log_2 n + (2n+1) \log_2(\|A\|_\infty \sqrt{n+1}) \right\rceil$.* $\qquad\square$

5   Bounding the support size of dyadic solutions

Take $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$. Given a dyadic linear program of the form $Ax = b, x \geq \mathbf{0}$ and dyadic, that is feasible, does there exist a solution with a small number of nonzero entries? We have placed dyadic linear program as a problem on the spectrum between LP and ILP, so let us give a brief overview of the state-of-the-art for the two extremes.

    For the case of real solutions to $Ax = b, x \geq \mathbf{0}$, we have the upper bound of m on the support size of a solution, given by Carathéodory's famous theorem. In fact, the same guarantee holds for an optimal solution to the standard equality form LP $\min\{w^\top x : Ax = b, x \geq \mathbf{0}\}$, for any $w \in \mathbb{R}^n$ for which there is a finite optimum.

    For the case of integral solutions to $Ax = b, x \geq \mathbf{0}$, a "Carathéodory-type" upper bound of $2m \log_2(4m\|A\|_\infty)$ on the size of the support was first established in [14] by making an elegant use of the *Pigeonhole Principle*. This bound was later improved to $2m \log_2(2\sqrt{m}\|A\|_\infty)$ in [6] by the use of *Siegel's Lemma*, a tool from the Geometry of Numbers, which we shall later see and prove in this section. In fact, the latter also obtained the same guarantee for an optimal solution to $\min\{w^\top x : Ax = b, x \geq \mathbf{0}$ and integral$\}$, for any $w \in \mathbb{R}^n$ for which there is a finite optimum.

    A natural first step for studying both extremes, as well as dyadic linear program, is to obtain guarantees for the system of linear equations $Ax = b$, with the appropriate restriction on the domain

of x. Observe that the guarantees above carry over in a black-box fashion to this setting, by simply transforming $Ax = b$ to $[A \;\; -A]\left(\begin{smallmatrix} y \\ z \end{smallmatrix}\right) = b, \left(\begin{smallmatrix} y \\ z \end{smallmatrix}\right) \geq \mathbf{0}$ with the substitution formula $x = y - z$.

With this context in mind, let us now move on to the spectrum between LP and ILP. In the previous section, for the sake of transparency but also generality, we provided guarantees not just for dyadic linear programs but more generally p-adic linear programs, for any prime $p \geq 2$. In this section, for the same reasons, we will provide guarantees for a different extension of dyadic linear programs, as explained below.

For every integer $k \geq 1$, denote by p_k the kth prime number. Recall from Section 2 that a rational number is $[p_k]$-adic if it is of the form $\frac{a}{b}$ where $a \in \mathbb{Z}$ and b is a product of primes in $[p_k]$. Note that a rational number is $[2]$-adic if and only if it is dyadic. Let $p_0 := 1$. We also deal with $[p_0]$-adic numbers, which are precisely the integers.[6] The guarantees we provide in this section will apply more generally to optimal solutions to the following $[p_k]$-adic linear program, for any integer $k \geq 0$:

$$\min\{w^\top x : Ax = b, x \geq \mathbf{0} \text{ and } [p_k]\text{-adic}\}. \tag{23}$$

Observe that for $k = 0$ we recover integer linear programming, for $k = 1$ dyadic linear programming, and for $k = \infty$ linear programming. Our bounds are given exactly but indirectly in terms of 'proxy' functions (see §5.4 for clarification on this), and also loosely but directly as a function of p_k, m, and the maximum absolute value $\|A\|_\infty$ of an entry of A; none of the bounds however depend on n. Along the way, we shall also provide improved and tight guarantees for solutions to

$$Ax = b, x \; [p_k]\text{-adic.} \tag{24}$$

5.1 Examples where every solution has full support

Let us present instances of (23) and (24) where every solution has full support. The example below is inspired by [11].

Example 5.1. *Let $q_1, \ldots, q_n$ be distinct primes such that $q_i \geq p_{k+1}$ for all $i \in [n]$. Let $Q := q_1 q_2 \cdots q_n$ and $A := \left(\frac{Q}{q_1} \;\; \frac{Q}{q_2} \;\; \cdots \;\; \frac{Q}{q_n} \right) \in \mathbb{R}^{1 \times n}$. Then the system $Ax = 1, x \; [p_k]$-adic is feasible, and every solution has full support.*

One can extend this example to one with an arbitrary number m of rows, by replacing $Ax = 1$ by $(A \otimes I)y = \mathbf{1}$, where $\otimes$ denotes the Kronecker product, I the m-by-m identity matrix, and $\mathbf{1}$ the all-ones m-dimensional column vector.

Proof. We only prove the first statement, and leave the easy verification of the second statement to the reader. Since the entries of A have GCD 1, it follows from Bézout's Lemma that $Ax = 1$ has an integral, thus $[p_k]$-adic solution. This proves feasibility of the system $Ax = 1, x \; [p_k]$-adic. Now let $\bar{x}$ be a feasible solution. Suppose for a contradiction that $\bar{x}$ does not have full support, say $\bar{x}_n = 0$. For each $i \in [n-1]$, write $\bar{x}_i = \frac{a_i}{b_i}$ where $a_i, b_i \in \mathbb{Z}$ and b_i is a product of primes in $[p_k]$. Let B be the least common multiple of $b_i, i \in [n-1]$, which is also a product of primes in $[p_k]$. Then we have the identity

$$\sum_{i=1}^{n-1} A_{1i} \frac{a_i B}{b_i} = B.$$

---

[6]Note that the $[p_0]$-adic numbers are discrete as opposed to the $[p_k]$-adic numbers for $k \geq 1$ which form a dense set. However, discreteness will be irrelevant in this section.

By construction, the GCD of $A_{1i}, i \in [n-1]$ is q_n. Since each $\frac{a_i B}{b_i}, i \in [n-1]$ is an integer, it therefore follows from the identity above that $q_n \mid B$, a contradiction since q_n is a prime outside $[p_k]$ while B is a product of primes in $[p_k]$. □

This example can naively be extended to the inequality case.

Example 5.2. *Let A be the matrix from Example 5.1. Take a resigning A^s of A, obtained by negating some entries of A, such that $A^s x = 1, x \geq 0$ has an integral solution. It can be readily checked that $A^s x = 1, x \geq 0, x \ [p_k]$-adic, is feasible, and every solution has full support. Once again, this example can be extended to one with an arbitrary number m of rows: $(A^s \otimes I)y = 1, y \geq 0, y \ [p_k]$-adic.*

For $k = 0$, there is another interesting example, which also appears in [14].

Example 5.3. *Let $A := (1 \ 2 \ 2^2 \ \cdots \ 2^{n-1}) \in \mathbb{R}^{1 \times n}$. Consider the integer linear program*

$$\min \left\{ 1^\top x : Ax = 2^n - 1, x \geq 0 \text{ and integral} \right\}.$$

Then $x = 1$ is the unique optimal solution, which in particular has full support. As before, this example can readily be extended to one with an arbitrary number m of rows:

$$\min \left\{ 1^\top y : (A \otimes I)y = (2^n - 1) \cdot 1, y \geq 0 \text{ and integral} \right\}.$$

Proof. We only verify the first statement, and leave the proof of the second statement to the reader. Clearly, $x^\star = 1$ is a feasible solution to the integer linear program. Take another feasible solution $\bar{x}$. Let $i \in [n]$ be the largest index such that $\bar{x}_i > 1$. Since $\bar{x}$ is integral and nonnegative, and $A\bar{x} = 2^n - 1$, it follows that $i < n$. We now change $\bar{x}$ by updating $\bar{x}_i := \bar{x}_i - 2$ and $\bar{x}_{i+1} := \bar{x}_{i+1} + 1$; note that this change reduces $1^\top \bar{x}$ by 1. By repeatedly applying this operation, we obtain the solution $x^\star = 1$ to the integer linear program. This procedure proves in particular that $x^\star = 1$ is the unique optimal solution to the integer linear program. □

5.2 From full support solutions to large prime factors

In this section, we pave the way for obtaining an upper bound on the support size for (23), and an even better bound for (24). The gap between these two bounds is due to the following lemma.

Lemma 5.4. *Let $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m, w \in \mathbb{R}^n$, and take an integer $k \geq 0$. Then the following statements hold:*

1. *Suppose $Ax = b, x \ [p_k]$-adic, is feasible, and every solution has full support. Then for every integral solution $\bar{x}$ to $Ax = 0$, every nonzero entry has a prime factor greater than or equal to p_{k+1}.*

2. *Suppose $\min\{w^\top x : Ax = b, x \geq 0, x \ [p_k]$-adic$\}$ has an optimal solution, and every optimal solution has full support. Then for every nonzero integral solution $\bar{x}$ to $Ax = 0$, there exists some nonzero entry with a prime factor greater than or equal to p_{k+1}.*

Proof. **(1)** Let $\bar{x}$ be a nonzero integral vector such that $A\bar{x} = \mathbf{0}$. Suppose for a contradiction that for some index i, $\bar{x}_i \neq 0$ and every prime factor of $\bar{x}_i$ is at most p_k. Let x^1 be a $[p_k]$-adic solution to $Ax = b$. By the hypothesis, x^1 has full support, so $x_i^1 \neq 0$. Let $x^2 := x^1 - \frac{x_i^1}{\bar{x}_i}\bar{x}$, which is another solution to $Ax = b$. Since every prime factor of $\bar{x}_i$ belongs to $\{p_1, \ldots, p_k\}$, it follows that x^2 is another $[p_k]$-adic solution to $Ax = b$, one whose support excludes i, a contradiction to our hypothesis.

(2) is similar to (1), except that in order to ensure x^2 remains nonnegative given the nonnegativity of x^1, we would need the prime factors of every nonzero entry of $\bar{x}$ to be less than p_{k+1}. Let us elaborate. Let $\bar{x}$ be a nonzero integral vector such that $A\bar{x} = \mathbf{0}$.

First, we prove that $w^\top\bar{x} = 0$. Suppose otherwise. Let $x^\star$ be an optimal solution to $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \text{ is } [p_k]\text{-adic}\}$. By assumption, $x^\star$ has full support, implying in turn that for a sufficiently small and $[p_k]$-adic $\epsilon > 0$, both $x^\star \pm \epsilon\bar{x}$ are feasible solutions to the $[p_k]$-adic linear program. However, since $w^\top\bar{x} \neq 0$, one of $x^\star \pm \epsilon\bar{x}$ would have a strictly smaller objective value than $x^\star$, thereby contradicting the optimality of $x^\star$. Thus, $w^\top\bar{x} = 0$.

Secondly, we prove that some nonzero entry of $\bar{x}$ has a prime factor greater than or equal to p_{k+1}. Suppose otherwise. We shall use $\bar{x}$ to construct an optimal solution to $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \text{ is } [p_k]\text{-adic}\}$ without full support, thereby contradicting the hypothesis. To this end, let x^1 be an optimal solution to the $[p_k]$-adic linear program. By the hypothesis, x^1 has full support. Choose

$$i \in \arg\min_{j \in [n]} \left\{ \frac{x_j^1}{\bar{x}_j} : \bar{x}_j \neq 0 \right\}.$$

Let $x^2 := x^1 - \frac{x_i^1}{\bar{x}_i}\bar{x}$. Our choice of i ensures that x^2 is defined and nonnegative. Since every prime factor of $\bar{x}_i$ belongs to $\{p_1, \ldots, p_k\}$ by the contrary assumption, x^2 is $[p_k]$-adic. Thus, since $w^\top\bar{x} = 0$, it follows that x^2 is another optimal solution to $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \text{ is } [p_k]\text{-adic}\}$, one whose support excludes i, a contradiction to our hypothesis. $\square$

5.3 Large prime factors: examples and analysis

It may not be clear how to find examples that satisfies the conclusions of Lemma 5.4 parts (1) and (2). Let us present two examples, both of which we will prove to be extremal in a sense. Throughout the subsection we assume that $k \in \mathbb{Z}_{\geq 0}$.

Example 5.5. *Let $q_1, \ldots, q_n$ be distinct primes such that $q_i \geq p_{k+1}$ for all $i \in [n]$. Let $Q := q_1 q_2 \cdots q_n$ and $A := \left(\frac{Q}{q_1} \ \frac{Q}{q_2} \ \cdots \ \frac{Q}{q_n} \right) \in \mathbb{R}^{1 \times n}$. It can be readily checked that for any integral solution $\bar{x}$ to $A\bar{x} = \mathbf{0}$, and for each $i \in [n]$, we have $q_i \mid \bar{x}_i$, so if $\bar{x}_i \neq 0$ then $\bar{x}_i$ has a prime factor greater than or equal to p_{k+1}. Thus the 1-by-n matrix A satisfies the conclusion of Lemma 5.4 (1).*

First, notice that the example above comes from Example 5.1, indicating that its essence is captured by Lemma 5.4 (1). Secondly, note that in the example above, the entries of the row vector A are "large" with respect to the GCD of its entries. More precisely, the size of every entry divided by the GCD of the entries, is at least $p_{k+1}p_{k+2}\cdots p_{k+n-1}$. In Lemma 5.6 below, we prove this bound more generally for a full-row-rank matrix with m rows, where the notions of the "size of an entry" and the "GCD of the entries" have been replaced by "a nonzero order-m minor" and the "GCD of order-m minors". The argument is inspired by a similar one in [13].

27

Lemma 5.6. *Let A be an m-by-n integral matrix of full row rank, where for every integral solution $\bar{x}$ to $Ax = \mathbf{0}$, if $\bar{x}_i \neq 0$ then x_i has a prime factor greater than or equal to p_{k+1}. Then for every subset $I \subseteq [n]$ of size m such that $\det(A_{[m] \times I}) \neq 0$ we have*

$$\frac{|\det(A_{[m] \times I})|}{\gcd(A)} \geq \begin{cases} p_{k+1}^{n-m} & \text{if } n < 2m \\ p_{k+1}^{m} p_{k+2}^{m} \cdots p_{k+\lfloor \frac{n}{m} \rfloor -1}^{m} p_{k+\lfloor \frac{n}{m} \rfloor}^{n-m\lfloor \frac{n}{m} \rfloor} & \text{otherwise.} \end{cases}$$

Moreover, there is a subset $J \subseteq [n]$ of size m such that $\det(A_{[m] \times J}) \neq 0$, and

$$\frac{|\det(A_{[m] \times J})|}{\gcd(A)} \geq \begin{cases} p_{k+2}^{n-m} & \text{if } n < 2m \\ p_{k+2}^{m} p_{k+3}^{m} \cdots p_{k+\lfloor \frac{n}{m} \rfloor}^{m} p_{k+\lfloor \frac{n}{m} \rfloor +1}^{n-m\lfloor \frac{n}{m} \rfloor} & \text{otherwise.} \end{cases}$$

Proof. Let U be an $n \times n$ unimodular matrix such that $AU = (B \ \mathbf{0})$, where B is an $m \times m$ matrix. (For instance, U can be the unimodular matrix that brings A into Hermite normal form after some elementary unimodular column operations.) We know that $\gcd(A) = |\det(B)|$. Let $(U_1 \ U_2)$ be the partition of U into two column submatrices such that $AU_1 = B$ and $AU_2 = \mathbf{0}$. Observe that the $n - m$ columns of U_2 form a basis for $\ker(A)$. In fact, since U is a unimodular matrix, the columns of U_2 form a basis for the lattice $L := \ker(A) \cap \mathbb{Z}^n$, that is, $\{U_2 y : y \in \mathbb{R}^{n-m}\} \cap \mathbb{Z}^n = \{U_2 y : y \in \mathbb{Z}^{n-m}\}$. Given that $L = \overline{L}$, it follows that $\gcd(U_2) = [\overline{L} : L] = 1$ (see Appendix A for more).

Given a prime number p, we say that p *divides a row of* U_2 if it divides every entry of the row.

Claim 1. *Every row of U_2 is divisible by a prime greater than or equal to p_{k+1}.*

Proof of Claim. Let $g \in \mathbb{Z}_{\geq 1}$ be the GCD of the entries of a nonzero row of U_2, say row i. Then there exists a $y \in \mathbb{Z}^{n-m}$ such that $(U_2 y)_i = g$. Since $x := U_2 y \in L$, our key assumption implies that every nonzero entry of x, and in particular $x_i = g$, has a prime factor greater than or equal to p_{k+1}, as claimed. $\diamond$

Claim 2. *Every prime number p divides at most m rows of U_2.*

Proof of Claim. Suppose otherwise, that is, for some prime number p, there is a subset $J \subseteq [n]$ of row indices of U_2 such that each row of U_2 with an index in J is divisible by p, and $|J| \geq m + 1$. Every $(n-m)$-by-$(n-m)$ submatrix of U_2 contains a row index from J, therefore its determinant is divisible by p. This implies that $p \mid \gcd(U_2)$, which is a contradiction since $\gcd(U_2) = 1$. $\diamond$

Denote by I_1, I_2 the set of column labels of U_1, U_2, respectively. Then $|I_1| = m$ and $|I_2| = n - m$.

Claim 3. *For every subset $I \subseteq [n]$ of size m such that $\det(U_{\overline{I} \times I_2}) \neq 0$, we have*

$$|\det(U_{\overline{I} \times I_2})| \geq \begin{cases} p_{k+1}^{n-m} & \text{if } n < 2m \\ p_{k+1}^{m} p_{k+2}^{m} \cdots p_{k+\lfloor \frac{n}{m} \rfloor -1}^{m} p_{k+\lfloor \frac{n}{m} \rfloor}^{n-m\lfloor \frac{n}{m} \rfloor} & \text{otherwise.} \end{cases}$$

Moreover, there is a subset $J \subseteq [n]$ of size m such that $\det(U_{\overline{J} \times I_2}) \neq 0$, and

$$|\det(U_{\overline{J} \times I_2})| \geq \begin{cases} p_{k+2}^{n-m} & \text{if } n < 2m \\ p_{k+2}^{m} p_{k+3}^{m} \cdots p_{k+\lfloor \frac{n}{m} \rfloor}^{m} p_{k+\lfloor \frac{n}{m} \rfloor +1}^{n-m\lfloor \frac{n}{m} \rfloor} & \text{otherwise.} \end{cases}$$

Here, $\overline{I}, \overline{J}$ refer to the complements of I, J, respectively.

Proof of Claim. Take a subset $I \subseteq [n]$ of size m such that $\det(U_{\bar{I} \times I_2}) \neq 0$. By Claim 1, every row of $U_{\bar{I} \times I_2}$ is divisible by a prime in $P := \{p_{k+1}, p_{k+2}, \ldots\}$. On the other hand, by Claim 2, every prime in P divides at most $\min\{|\bar{I}|, m\} = \min\{n - m, m\}$ rows of $U_{\bar{I} \times I_2}$. These two facts immediately imply the first inequality. To get the second, stronger inequality, it suffices to choose $J := I$ such that it includes the indices of all the rows of U_2 divisible by p_{k+1} (of which there are at most m by Claim 2), and $\det(U_{\bar{J} \times I_2}) \neq 0$. This can be done by using the fact that $\gcd(U_2) = 1$, so there exists a minor of U_2 of order $n - m$ that is not divisible by p_{k+1}; this will be precisely $\det(U_{\bar{J} \times I_2})$. $\Diamond$

Claim 4. *For every subset $I \subseteq [n]$ of size m, we have $|\det(A_{[m] \times I})| = \gcd(A) \cdot |\det(U_{\bar{I} \times I_2})|$.*

Proof of Claim. It follows from $A = (B\ \mathbf{0})U^{-1}$ that $A_{[m] \times I} = (B\ \mathbf{0})(U^{-1})_{[n] \times I} = B \cdot (U^{-1})_{I_1 \times I}$. Subsequently,

$$|\det(A_{[m] \times I})| = |\det(B)| \cdot |\det((U^{-1})_{I_1 \times I})| = \gcd(A) \cdot |\det((U^{-1})_{I_1 \times I})|.$$

The right-hand side term can be rewritten in terms of the adjugate $\mathrm{adj}(U)$ of U. Observe that $\mathrm{adj}(U) = \det(U) \cdot U^{-1}$, so $U^{-1} = \pm\mathrm{adj}(U)$ because U is unimodular. Thus,

$$|\det((U^{-1})_{I_1 \times I})| = |\det(\mathrm{adj}(U)_{I_1 \times I})| = |\det(U_{\bar{I} \times I_2})| \cdot |\det(U)|^{m-1} = |\det(U_{\bar{I} \times I_2})|$$

where the second equality follows from Jacobi's Theorem on the adjugate matrix (see Appendix A for more), and the last equality from the unimodularity of U. Combining the two lines of equalities above yields the claim. $\Diamond$

The lemma readily follows from Claims 3 and 4. $\square$

Next, let us present an example that satisfies the conclusion of Lemma 5.4 (2).

Example 5.7. *Let $A := \begin{pmatrix} 1 & p_{k+1} & p_{k+1}^2 & \cdots & p_{k+1}^{n-1} \end{pmatrix} \in \mathbb{R}^{1 \times n}$. It can be readily checked that for any nonzero integral solution $\bar{x}$ to $Ax = \mathbf{0}$, the smallest index $i \in [n]$ such that $\bar{x}_i \neq 0$ satisfies $p_{k+1} \mid \bar{x}_i$. Thus the 1-by-n matrix A satisfies the conclusion of Lemma 5.4 (2).*

First, notice that this example is the same as the feasible region of Example 5.3 for $k = 0$, indicating that in this case the essence of the example is captured by Lemma 5.4 (2). Secondly, in the example above, the row vector A has small entries as well as large, however its 2-norm is "large" relative to the GCD of its entries. More precisely, the 2-norm of the row vector divided by the GCD of the entries, is equal to $\sqrt{\frac{p_{k+1}^{2n} - 1}{p_{k+1}^2 - 1}}$; the latter is sandwiched between p_{k+1}^{n-1} and $\sqrt{1 + \frac{1}{p_{k+1}^2 - 1}} \cdot p_{k+1}^{n-1}$. In Lemma 5.8 below, known as *Siegel's Lemma*, we prove the lower bound more generally for a full-row-rank matrix with m rows, where the "2-norm of the row vector" is replaced by "the m-dimensional volume of the parallelepiped generated by the rows of A", and as before, the "GCD of the entries" is replaced by the "GCD of order-m minors".

Lemma 5.8 (Siegel's Lemma, see [9]). *Consider a linear system $Ax = \mathbf{0}$, where $A \in \mathbb{Z}^{m \times n}$ has full row rank, and let $\ell \geq 1$. Suppose for every nonzero integral solution $\bar{x}$ to $Ax = \mathbf{0}$, $\|\bar{x}\|_\infty \geq \ell$. Then $\sqrt{\det(AA^\top)}/\gcd(A) \geq \ell^{n-m}$.*

Proof. Consider the lattice $L := \{A^\top y : y \in \mathbb{Z}^m\}$ and its orthogonal complement lattice $L^\perp := \{x \in \mathbb{Z}^n : Ax = \mathbf{0}\}$. By assumption, the convex set $Q := \{x : \|x\|_\infty < \ell\} \cap \{x : Ax = \mathbf{0}\}$, which is symmetric about the origin, contains no nonzero vector of the lattice $L^\perp$. We may therefore apply Minkowski's First Theorem to upper bound the $(n-m)$-dimensional volume of Q (see Appendix A for more). The theorem implies that $\mathrm{vol}_{n-m}(Q) \leq 2^{n-m} \det(L^\perp)$. On the one hand, $\frac{1}{2\ell} \cdot Q$ is an $(n-m)$-dimensional affine slice of the unit hypercube $\{x : \|x\|_\infty < \frac{1}{2}\}$ going through the origin, so by Vaaler [32], $\mathrm{vol}_{n-m}(\frac{1}{2\ell}Q) \geq 1$, implying in turn that $\mathrm{vol}_{n-m}(Q) \geq (2\ell)^{n-m}$. On the other hand, given that $\overline{L} := \{A^\top y : y \in \mathbb{R}^m\} \cap \mathbb{Z}^n \supseteq L$, we have

$$\det(L^\perp) = \det(\overline{L}) = \frac{\det(L)}{[\overline{L} : L]} = \frac{\det(L)}{\gcd(A^\top)} = \frac{\sqrt{\det(AA^\top)}}{\gcd(A)}$$

(see Appendix A for more). Putting everything together we obtain the desired inequality. □

5.4 Proxy and direct upper bounds on the support size

We obtain the following exact upper bound on the support size of solutions to $[p_k]$-adic linear systems and $[p_k]$-adic linear programs. Note that the upper bounds are provided indirectly by suitable proxy functions of the input size.

Theorem 5.9. *Let $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, and $w \in \mathbb{R}^n$. Then the following statements hold for every integer $k \geq 0$:*

1. *If $Ax = b, x$ $[p_k]$-adic, is feasible, then it has a solution with support size at most n', where for some full-row-rank m'-by-n' submatrix A' of A, we have*

$$\Delta_{m'}(A') \geq \begin{cases} p_{k+2}^{\frac{n'}{m'}-1} & \text{if } n' < 2m' \\ p_{k+2}p_{k+3}\cdots p_{k+\lfloor\frac{n'}{m'}\rfloor} p_{k+\lfloor\frac{n'}{m'}\rfloor+1}^{\frac{n'}{m'}-\lfloor\frac{n'}{m'}\rfloor} & \text{otherwise,} \end{cases}$$

where $\Delta_{m'}(A')$ is the m'^{th} root of the maximum absolute value of an order-m' minor of A'.

2. *If $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \ [p_k]\text{-adic}\}$ has an optimal solution, then it has an optimal solution with support size at most n', where for some full-row-rank m'-by-n' submatrix A' of A, we have*
$$\left(\frac{\sqrt{\det(A'A'^\top)}}{\gcd(A')}\right)^{\frac{1}{m'}} \geq p_{k+1}^{\frac{n'}{m'}-1}.$$

Proof. **(1)** Let $x^\star$ be a solution to $Ax = b, x$ $[p_k]$-adic, with minimum support size. After moving to a submatrix of A, and the corresponding subvector of b, if necessary, we may assume that $x^\star$ has full support, and $A' = A$ has full row rank; thus $m' = m \leq n = n'$. By Lemma 5.4 (1), for every integral solution $\bar{x}$ to $Ax = \mathbf{0}$, every nonzero entry of $\bar{x}$ has a prime factor greater than or equal to p_{k+1}. Thus, by Lemma 5.6, A has an m-by-m submatrix B such that

$$|\det(B)| \geq \begin{cases} p_{k+2}^{n-m} & \text{if } n < 2m \\ p_{k+2}^m p_{k+3}^m \cdots p_{k+\lfloor\frac{n}{m}\rfloor}^m p_{k+\lfloor\frac{n}{m}\rfloor+1}^{n-m\lfloor\frac{n}{m}\rfloor} & \text{otherwise.} \end{cases}$$

Taking the mth of both sides, and taking advantage of the inequality $\Delta_m(A) \geq |\det(B)|^{1/m}$ by definition, we obtain (1).

(2) Let $x^\star$ be an optimal solution to $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x\ [p_k]\text{-adic}\}$ with minimum support size. After moving to a submatrix of A, and the corresponding subvectors of w and b, if necessary, we may assume that $x^\star$ has full support, and $A' = A$ has full row rank; thus $m' = m \leq n = n'$. By Lemma 5.4 (2), for every nonzero integral solution $\bar{x}$ to $Ax = \mathbf{0}$, there exists a nonzero entry with a prime factor greater than or equal to p_{k+1}, so in particular $\|\bar{x}\|_\infty \geq p_{k+1}$. It therefore follows from Siegel's Lemma that

$$\frac{\sqrt{\det(AA^\top)}}{\gcd(A)} \geq p_{k+1}^{n-m},$$

proving (2). □

Observe that for fixed A, both bounds above guarantee that $\frac{n'}{m'} \to 1$ as $p_k \to \infty$, thereby matching Carathéodory's bounds for the support size of solutions to linear systems, and optimal solutions to linear programs.

We can use the theorem above, along with Hadamard's inequality, to provide loose but direct upper bounds on the support size of solutions.

Theorem 5.10. *Let $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, and $w \in \mathbb{R}^n$. Then the following statements hold for every integer $k \geq 0$:*

1. *If $Ax = b, x\ [p_k]$-adic, is feasible, then it has a solution with support size at most n', where for some $1 \leq m' \leq m$ and $r = \lfloor \frac{n'}{m'} \rfloor$, the following holds: if $r \geq 7$ and $\ln(\sqrt{m'}\|A\|_\infty) \geq e$, then*

$$r \leq 1 + \frac{2(1+e)}{e} \frac{\ln(\sqrt{m'}\|A\|_\infty)}{\ln\ln(\sqrt{m'}\|A\|_\infty)}.$$

2. *If $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x\ [p_k]\text{-adic}\}$ has an optimal solution, then it has an optimal solution with support size at most n', where for some $1 \leq m' \leq m$ and $r = \frac{n'}{m'}$, we have*

$$r \leq \begin{cases} 1 + \ln\left(m'\|A\|_\infty^2\right)/(2\ln p_{k+1} - 1) & \text{for all } k \geq 0, \\ \max\left\{\frac{4\|A\|_\infty^2}{m'}, 1 + \log_2\|A\|_\infty + \log_2(m'\|A\|_\infty) \cdot \frac{1+\log_2\|A\|_\infty}{1+2\log_2\|A\|_\infty}\right\} & \text{if } k = 0. \end{cases}$$

Proof. (1) For some full-row-rank m'-by-n' submatrix A' of A, the inequality of Theorem 5.9 (1) holds. We may assume that $A' = A$, $m' = m$ and $n' = n$. Let $r := \lfloor \frac{n}{m} \rfloor$. If $r < 7$ then there is nothing to prove. Otherwise, $r \geq 7$. Then by Theorem 5.9 (1) we have

$$\Delta_m(A) \geq \prod_{i=1}^{r-1}(p_{k+2} + i - 1) \geq \prod_{i=1+\lceil\frac{r-2}{2}\rceil}^{r-1}(p_{k+2} + i - 1) \geq \left(p_{k+2} + \left\lceil\frac{r-2}{2}\right\rceil\right)^{\lceil\frac{r-1}{2}\rceil}.$$

For the third inequality above, we used the equality $\lceil\frac{r-1}{2}\rceil + \lceil\frac{r-2}{2}\rceil = r - 1$. On the other hand, by Hadamard's inequality, $\sqrt{m}\|A\|_\infty \geq \Delta_m(A)$. Combining this inequality with the one above, and then taking the natural logarithm, we obtain

$$\left\lceil\frac{r-1}{2}\right\rceil \ln\left(p_{k+2} + \left\lceil\frac{r-2}{2}\right\rceil\right) \leq \ln(\sqrt{m}\|A\|_\infty).$$

31

Let $\lambda := \frac{r-1}{2}$ and $\mu := \ln(\sqrt{m}\|A\|_\infty)$. Then the inequality above implies that $\lambda \ln(\lambda) \leq \mu$. Note that since $r \geq 7 > 1 + 2e$, we have $\lambda > e$.

Claim 1. *For $\lambda, \mu \geq e$, we have $\lambda \leq \frac{1+e}{e} \cdot \frac{\mu}{\ln(\mu)}$.*

Proof of Claim. Let $\nu := \lambda \ln(\lambda)$. Then for $\lambda \geq e$,

$$\frac{\nu}{\ln(\nu)} = \frac{\lambda \ln(\lambda)}{\ln(\lambda) + \ln \ln(\lambda)} \geq \frac{\lambda \ln(\lambda)}{(1 + 1/e)\ln(\lambda)} = \frac{e}{1+e}\lambda$$

where the middle inequality holds because $\ln \ln(\lambda) \leq \frac{1}{e}\ln(\lambda)$ for all $\lambda \geq e$. Since the function $\frac{2t}{\ln(t)}$ is increasing on $t \in [e, \infty)$, and $\mu \geq \nu \geq e$, it follows that $\frac{1+e}{e} \cdot \frac{\mu}{\ln(\mu)} \geq \frac{1+e}{e} \cdot \frac{\nu}{\ln(\nu)}$, so the claim follows. $\diamond$

Claim 1 proves the inequality of (1).

(2) For some full-row-rank m'-by-n' submatrix A' of A, the inequality of Theorem 5.9 (2) holds. We may assume that $A' = A$, $m' = m$ and $n' = n$. Thus, we have that

$$\sqrt{\det(AA^\top)} \geq p_{k+1}^{n-m}.$$

Suppose $a^1, \ldots, a^m \in \mathbb{Z}^n$ are the rows of A, viewed as column vectors. By Hadamard's inequality,

$$\sqrt{\det(AA^\top)} \leq \sqrt{\prod_{i=1}^m \|Aa^i\|_2} \leq \sqrt{\prod_{i=1}^m (\sqrt{m}\sqrt{n}\|A\|_\infty^2)} \leq \left(\sqrt{n}\|A\|_\infty\right)^m.$$

Combining the inequalities above, and then taking logarithms base p_{k+1}, we obtain

$$n \leq m + m \log_{p_{k+1}}\left(\sqrt{n}\|A\|_\infty\right). \tag{25}$$

Let $f, g : \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 0}$ be the functions defined as $g(x) = x + x\log_{p_{k+1}}\|A\|_\infty$ and $f(x) := \log_{p_{k+1}} x$. Then (25) may be rewritten as $n \leq g(m) + \frac{m}{2}f(n)$. Observe that f is an increasing function.

Claim 2. *The following inequalities hold:*

a. $f(g(m) + \frac{m}{2}f(n)) \leq f(g(m)) + \frac{m}{2\ln(p_{k+1})g(m)}f(n)$,

b. *for $k = 0$, if $n \geq 4\|A\|_\infty^2$, then $f(g(m) + \frac{m}{2}f(n)) \leq f(g(m)) + \frac{m}{2g(m)}f(n)$.*

Proof of Claim. To see the inequalities, note that $\log_{p_{k+1}}(x + y) = \log_{p_{k+1}}(x) + \log_{p_{k+1}}\left(1 + \frac{y}{x}\right) \leq \log_{p_{k+1}}(x) + \frac{1}{\ln(p_{k+1})}\frac{y}{x}$ for all x, y over which the LHS and RHS are defined. Thus,

$$f\left(g(m) + \frac{m}{2}f(n)\right) = \log_{p_{k+1}}\left(g(m) + \frac{m}{2}f(n)\right) \leq \log_{p_{k+1}} g(m) + \frac{m \cdot f(n)}{2\ln(p_{k+1})g(m)}$$

thereby proving (a). When $k = 0$ (i.e. $p_{k+1} = 2$), we can replace $\log_{p_{k+1}}(1 + \frac{y}{x}) \leq \frac{1}{\ln(p_{k+1})}\frac{y}{x}$ by the improved inequality $\log_{p_{k+1}}(1 + \frac{y}{x}) \leq \frac{y}{x}$ as long as $\frac{y}{x} \geq 1$. Thus, after repeating the above argument with this improved inequality, we obtain (b). $\diamond$

Subsequently,

$$n \leq g(m) + \frac{m}{2}f(n) \leq g(m) + \frac{m}{2}f\left(g(m) + \frac{m}{2}f(n)\right) \quad \text{since } f \text{ is increasing}$$

$$\leq g(m) + \frac{m}{2}f(g(m)) + \frac{m}{2}\frac{m}{2\ln(p_{k+1})g(m)}f(n) \quad \text{by part (a) of Claim 2}$$

$$\vdots$$

$$\leq g(m) + \frac{m}{2}f(g(m))\sum_{t=0}^{\infty}\left(\frac{m}{2\ln(p_{k+1})g(m)}\right)^t$$

$$= g(m) + \frac{m}{2}f(g(m)) \cdot \frac{2\ln(p_{k+1})g(m)}{2\ln(p_{k+1})g(m) - m}.$$

Substituting for $g(m)$ and $f(g(m))$, and dividing both sides by m, we get the following inequality:

$$\frac{n}{m} \leq 1 + \log_{p_{k+1}}\|A\|_\infty + \frac{1}{2}\log_{p_{k+1}}(m + m\log_{p_{k+1}}\|A\|_\infty) \cdot \frac{1 + \log_{p_{k+1}}\|A\|_\infty}{1 + \log_{p_{k+1}}\|A\|_\infty - \frac{1}{2\ln(p_{k+1})}}$$

$$\leq 1 + \log_{p_{k+1}}\|A\|_\infty + \left(\log_{p_{k+1}}m + \frac{\log_{p_{k+1}}\|A\|_\infty}{\ln(p_{k+1})}\right) \cdot \frac{1 + \log_{p_{k+1}}\|A\|_\infty}{2 + 2\log_{p_{k+1}}\|A\|_\infty - \frac{1}{\ln(p_{k+1})}}$$

$$\leq 1 + \log_{p_{k+1}}\|A\|_\infty + \left(\log_{p_{k+1}}m + \frac{\log_{p_{k+1}}\|A\|_\infty}{\ln(p_{k+1})}\right) \cdot \frac{1}{2 - \frac{1}{\ln(p_{k+1})}}$$

$$= 1 + \frac{\ln m + 2\ln\|A\|_\infty}{2\ln p_{k+1} - 1}.$$

Assume now that $k = 0$. We need to prove another upper bound on $\frac{n}{m}$. If $n < 4\|A\|_\infty^2$, then $\frac{n}{m} < \frac{4\|A\|_\infty^2}{m}$, so we are done. Otherwise, $n \geq 4\|A\|_\infty^2$. We then use part (b) instead of part (a) of Claim 2 in the inequalities above, and obtain

$$n \leq g(m) + \frac{m}{2}f(g(m)) \cdot \frac{2g(m)}{2g(m) - m}.$$

Substituting for $g(m)$ and $f(g(m))$, and dividing both sides by m, we get the following inequality:

$$\frac{n}{m} \leq 1 + \log_2\|A\|_\infty + \frac{1}{2}\log_2(m + m\log_2\|A\|_\infty) \cdot \frac{1 + \log_2\|A\|_\infty}{1 + \log_2\|A\|_\infty - \frac{1}{2}}$$

$$\leq 1 + \log_2\|A\|_\infty + (\log_2 m + \log_2\|A\|_\infty) \cdot \frac{1 + \log_2\|A\|_\infty}{1 + 2\log_2\|A\|_\infty},$$

as required. $\qquad\square$

Let us mention a few notable cases. First, the upper bound of Theorem 5.10 (1) for $k = 0$ is interesting in its own right, and was recently obtained in [13] (their upper bound is given in terms

of big O notation, in contrast to our bound). Secondly, for $k = 0$, thanks to an improved asymptotic analysis, the upper bound of Theorem 5.10 (2) gives a minor improvement over the guarantee of $2m \log_2(2\sqrt{m}\|A\|_\infty)$ in [6]. Thirdly, for $k = 0$ and $\|A\|_\infty = 1$, the upper bound of Theorem 5.10 (2) simplifies to the following.

Corollary 5.11. *Let* $A \in \{0, \pm1\}^{m \times n}, b \in \mathbb{Z}^m$. *If* $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \in \mathbb{Z}^n\}$ *has an optimal solution, then it has one with support size at most* $m(1 + \log_2 m) \approx m(1 + 1.45 \ln m)$. $\square$

Finally, for dyadic linear programs, we obtain the following, bringing this subsection to an end.

Corollary 5.12. *Let* $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m$ *and* $w \in \mathbb{R}^n$. *If* $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \ dyadic\}$ *has an optimal solution, then it has one with support size at most* $m(1 + \ln(m\|A\|_\infty^2)/(2\ln 3 - 1)) \approx m(1 + 0.84 \ln m + 1.68 \ln \|A\|_\infty)$. $\square$

5.5 Examples revisited

Example 5.1 revisited. *Consider the example* $(A \otimes I)y = \mathbf{1}, y\ [p_k]$*-adic with* mn *variables and* m *equations. Let* $q_i := p_{k+i}$ *for* $i \in [n]$. *Observe that*

$$\Delta_m(A \otimes I) = \frac{Q}{q_1} = p_{k+2}p_{k+3}\cdots p_{k+n}.$$

Observe that the RHS is precisely the lower bound provided by Theorem 5.9 (1). This shows that (a) this example is extremal, and (b) the lower bound given on Δ_m *by Theorem 5.9 (1) cannot be improved in the case when the number of variables is a multiple of* m.

Example 5.2 revisited. *Consider the example* $\min\{0 : (A^s \otimes I)y = \mathbf{1}, y \geq \mathbf{0}, y\ [p_k]$*-adic$\}$ with* mn *variables and* m *equations. Let* $q_i := p_{k+i}$ *for* $i \in [n]$. *Let* $B := A^s \otimes I$ *and consider the inequality of Theorem 5.9 (2). The LHS is*

$$\left(\frac{\sqrt{\det(BB^\top)}}{\gcd(B)}\right)^{1/m} = \sqrt{\sum_{i=1}^n \left(\frac{Q}{q_i}\right)^2} \geq p_{k+1}\cdots p_{k+n-1}\sqrt{n}$$

while the RHS is p_{k+1}^{n-1}, *so there is a multiplicative gap of at least*

$$\frac{p_{k+2}}{p_{k+1}}\cdots\frac{p_{k+n-1}}{p_{k+1}}\sqrt{n}$$

between the LHS and RHS for this example.

Example 5.3 revisited. *For this example we have* $k = 0$. *Consider the integer linear program*

$$\min\left\{\mathbf{1}^\top y : (A \otimes I)y = (2^n - 1) \cdot \mathbf{1}, y \geq \mathbf{0} \ and \ integral\right\}.$$

Let $B := A \otimes I$ *and consider the inequality of Theorem 5.9 (2). The LHS is*

$$\left(\frac{\sqrt{\det(BB^\top)}}{\gcd(B)}\right)^{1/m} = \sqrt{\sum_{i=1}^n (2^{i-1})^2} = \sqrt{\frac{4^n - 1}{3}} = \sqrt{\frac{4}{3}\left(1 - \frac{1}{4^n}\right)} \cdot 2^{n-1} \in \left[2^{n-1}, \sqrt{\frac{4}{3}} \cdot 2^{n-1}\right)$$

while the RHS is 2^{n-1}, *so there is a constant multiplicative gap of at most* $\sqrt{4/3}$ *between the LHS and RHS for this example. This shows that (a) this example is extremal up to the constant factor, and (b) the lower bound given in Theorem 5.9 (2) cannot be improved beyond this constant factor, in the case when* $k = 0$.

6 Concluding remarks and future research

In this paper, we studied dyadic linear programming and its extension to $\mathbb{L}$-linear programming, where $(\mathbb{L}, +)$ is a dense abelian subgroup of $(\mathbb{R}, +)$. Two important extensions were p-adic and $[p]$-adic linear programs, for a prime p.

We laid the foundation for $\mathbb{L}$-linear programming by characterizing feasibility, stating optimality conditions, classifying all the possible outcomes and providing concise certificates in each case. A distinguishing feature was that unlike linear programs, an $\mathbb{L}$-linear program may have an optimal value that is converged to but never attained within the feasible region.

We proved that under mild assumptions on $\mathbb{L}$, namely that $\mathbb{L}$ comes with a membership oracle and contains all p-adic numbers for some explicitly given prime p, an $\mathbb{L}$-linear program can be solved in polynomial time. In fact, we established a constant factor equivalence between the running times of solving an $\mathbb{L}$-linear program and a linear program, with blackbox reductions going in either direction.

Going beyond the blackbox reductions, if we are given deeper access to an algorithm for solving LPs which is guaranteed to find strictly complementary solutions (when the instance has an optimal solution), we can modify such an algorithm in part by inserting our subroutines in suitable places so that the LP algorithm is run only once (with these inserted subroutines) to solve the corresponding $\mathbb{L}$-linear program. Such modifications can be particularly straightforward for the two-phase algorithms for LPs (as one can follow the analysis in Section 3 to see how to modify the LP algorithm).

Our blackbox approach can also be useful in solving $\mathbb{L}$-*convex programs*. For a special class of convex optimization problems at hand, if we are able to compute affine hulls (of the feasible region and the optimal face) and obtain rational representations for them (when possible) then, we can solve the $\mathbb{L}$-convex program using the approach in Section 3. We do not need the convex programming instance to satisfy strict complementarity, but we would require the convex optimization algorithm to compute rational vectors (when they exist) in the relative interiors of the corresponding sets. Limits of sequences of solutions generated by many interior-point algorithms for convex optimization lie in the relative interiors of the corresponding sets.

An irony of our polynomial algorithm, and even some of the foundational results, is that even though we set to solve an $\mathbb{L}$-linear program, the numbers encountered throughout may in fact fall outside $\mathbb{L}$. For instance, in the theorem of the alternatives, Theorem 2.7, the non-existence certificate u must inevitably be outside $\mathbb{L}$. That said, the algorithm does successfully characterize and solve the various outcomes of an $\mathbb{L}$-linear program, and provides the first step for finding a polynomial algorithm where all the numbers involved in the computations belong to $\mathbb{L}$.

Given $Ax \leq b, x$ p-adic, that is feasible, what is the smallest $k \in \mathbb{Z}_{\geq 0}$ such that there is a $1/p^k$-integral solution? While determining k is NP-hard, we provided upper bounds on k that are polynomial in n and the encoding size of A. A particular case of interest comes from combinatorial optimization. Given a graph $G = (V, E)$ and a nonempty set $T \subseteq V$ of even size, a *T-join* is an edge set whose odd-degree vertices coincides with T. It is known that the *fractional T-join packing* problem

$$\max \left\{ \mathbf{1}^\top y : \sum (y_J : J \ni e) \leq 1 \ \forall e \in E; y_J \geq 0 \ \forall \ T\text{-joins } J \right\}$$

has an optimal solution that is dyadic, i.e., $\frac{1}{2^k}$-integral for some integer $k \geq 0$ [5]. The proof provides no upper bound guarantee on k. That said, it has been conjectured by Seymour that $k \leq 2$ ([12], Conjecture 2.15, also see Schrijver [28] 79.3e). An upper bound of $k \leq c \log(|E|)$ for some universal constant c, also remains open. The conjecture of Seymour combined with our approach in the current

manuscript, suggests a study of classes of linear programs with integral data such that for every integral objective function vector, the primal has a $\frac{1}{2^{k_1}}$-integral optimal solution (whenever it has an optimal solution) and the dual has a $\frac{1}{2^{k_2}}$-integral optimal solution, for some fixed pair of nonnegative integers k_1 and k_2. Seymour's conjecture above corresponds to the special case $k_1 := 0$, $k_2 := 2$.

Given a $[p]$-adic linear program $\min\{w^\top x : Ax = b, x \geq \mathbf{0}, x \; [p]\text{-adic}\}$ that has an optimal solution, where A has m rows, we provided upper bound guarantees on the support size of an optimal solution, where the bound depended polynomially on m, p and the encoding size of A. A helpful twist in this case was extending the notion of $[p]$-adic numbers to include the case of $p = 1$, by declaring the $[1]$-adic numbers as the integers. As such, we obtained a spectrum of guarantees ranging from ILPs ($p = 1$) on the one end, passing through dyadic linear programs ($p = 2$), and reaching LPs ($p = \infty$) on the other and matching Carathéodory's bound. Along the way, we also provided tight upper bounds on the support size of a solution to a feasible $[p]$-adic linear system of the form $Ax = b, x \; [p]$-adic.

While our upper bound guarantees for $[p]$-adic linear programs are tight for the two ends of the spectrum, $p = 1$ (Example 5.3) and $p = \infty$, there remains a gap between our best lower bound (Example 5.2) and our upper bound for $2 \leq p < \infty$, as discussed in Section 5.5. We believe that due to the density of the feasible region for $p \geq 2$, the upper bounds in this case should look more like the upper bounds for $[p]$-adic linear systems.

In the special case of $\|A\|_\infty = 1$, the best lower bound on the support size of an optimal solution to a $[p]$-adic linear program that we can show is at most $O(m)$, while our upper bound is $O(m \ln m)$. Closing the gap in this case remains an intriguing open question. An important special case comes in the dyadic ($p = 2$) case from the fractional T-join packing problem mentioned above. By developing a column generation technique for solving dyadic linear programs, and by leveraging tools from matching theory, we achieve a matching upper bound of $O(m)$ (note $m = |E|$ in this case) [1].

We have used the size of the input, in particular $\ln \|A\|_\infty$ to state our results (for bounds on computational complexity as well as support size bounds etc.). However, for specially structured instances, there are better complexity measures, capturing more intrinsic properties of the instance. This typically yields tighter and more insightful bounds. Thus, it would be fruitful to pursue this direction in future research.

Let $a^1, \ldots, a^n \in \mathbb{Z}^m$. The set $\{a^1, \ldots, a^n\}$ is a *dyadic generating set for a cone (DGSC)* if every integral vector in the conic hull of the vectors can be expressed as a dyadic conic combination of the vectors. This notion was coined and studied in our first work on dyadic linear programming [4]. Given a DGSC $\{a^1, \ldots, a^n\}$ and an integral vector b in the conic hull, we know that b can be expressed as a dyadic conic combination of the vectors. What is the fewest number k of nonzero coefficients in such a representation? While Corollary 5.12 gives an upper bound of $O(m \ln(m \|A\|_\infty^2))$ on k, we conjecture that there is a $O(m)$ upper bound on k. The rationale behind this comes from the observation that a DGSC may be viewed as the dyadic analogue of *Hilbert bases* for integer linear programming [16] for which the analogous upper bound guarantee is $2m - 2$ [29].

Finally, we propose a weakening of a known conjecture. A matrix $A \in \{0, 1\}^{m \times n}$ is *ideal* if the set covering linear program $\min\{c^\top x : Ax \geq \mathbf{1}, x \geq \mathbf{0}\}$ has an integral optimal solution for all $c \in \mathbb{Z}_{\geq 0}^n$. Seymour conjectures that the dual linear program $\max\{\mathbf{1}^\top y : A^\top y \leq c, y \geq \mathbf{0}\}$ has a dyadic optimal solution for all $c \in \mathbb{Z}_{\geq 0}^n$ (see Schrijver [28] 79.3e). We propose the following weakening of this conjecture.

Conjecture 6.1. *Let $A \in \{0, 1\}^{m \times n}$ be an ideal matrix, and for some $c \in \mathbb{Z}_{\geq 0}^n$, let $\tau_c := \min\{c^\top x : Ax \geq \mathbf{1}, x \geq \mathbf{0}\}$. Let p be the largest prime in $[\tau_c]$. Then $\max\{\mathbf{1}^\top y : A^\top y \leq c, y \geq \mathbf{0}\}$ has a $[p]$-adic*

optimal solution.

This conjecture has been verified for the clutter of dijoins of a digraph ([20], Theorem 2.13).

Acknowledgements

References

[1] A. Abdi, G. Cornuéjols, B. Guenin, and L. Tunçel. Dyadic linear programming: implicit models and applications. In preparation.

[2] A. Abdi, G. Cornuéjols, B. Guenin, and L. Tunçel. Clean clutters and dyadic fractional packings. *SIAM Journal on Discrete Mathematics*, 36:1012–1037, 2022.

[3] A. Abdi, G. Cornuéjols, B. Guenin, and L. Tunçel. Total dual dyadicness and dyadic generating sets. In K. Aardal and L. Sanità, editors, *Integer Programming and Combinatorial Optimization*, pages 1–14, Cham, 2022. Springer International Publishing.

[4] A. Abdi, G. Cornuéjols, B. Guenin, and L. Tunçel. Total dual dyadicness and dyadic generating sets. *Mathematical Programming*, 2023.

[5] A. Abdi, G. Cornuéjols, and Z. Palion. On dyadic fractional packings of T-joins. *SIAM Journal on Discrete Mathematics*, 36:2445–2451, 2022.

[6] I. Aliev, J. A. De Loera, T. Oertel, and C. O'Neill. Sparse solutions of linear Diophantine equations. *SIAM J. Appl. Algebra Geometry*, 1(1):239–253, 2017.

[7] S. Arora and B. Barak. *Complexity Theory: A Modern Approach*. Cambridge University Press, 2009.

[8] E. F. Beckenbach and R. Bellman. *Inequalities*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge. Springer Berlin, Heidelberg, 1961.

[9] E. Bombieri and J. Vaaler. On Siegel's lemma. *Inventiones mathematicae*, 73(1):11–32, 1983.

[10] M. Conforti, G. Cornuéjols, and G. Zambelli. *Integer Programming*. Springer International Publishing, 2014.

[11] W. Cook, J. Fonlupt, and A. Schrijver. An integer analogue of Carathéodory's theorem. *Journal of Combinatorial Theory, Series B*, 40(1):63–70, 1986.

[12] G. Cornuéjols. *Combinatorial Optimization: Packing and Covering*. SIAM, 2001.

[13] Y. Dubey and S. Liu. A short proof of tight bounds on the smallest support size of integer solutions to linear equations. arXiv:2307.08826, July 2023.

[14] F. Eisenbrand and G. Shmonin. Carathéodory bounds for integer cones. *Operations Research Letters*, 34(5):564–568, 2006.

[15] D. Espinoza. *On Linear Programming, Integer Programming and Cutting Planes*. PhD thesis, School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, GA, 2006.

[16] F. Giles and W. Pulleyblank. Total dual integrality and integer polyhedra. *Linear Algebra and its Applications*, 25:191 – 196, 1979.

[17] F. Gouvêa. *p-adic Numbers - An Introduction*. Springer, 1997.

[18] J. Hadamard. Resolution d'une question relative aux determinants. *Bull. Sci. Math.*, 2:240–248, 1893.

[19] J. C. K. Ho and L. Tunçel. Reconciliation of various complexity and condition measures for linear programming problems and a generalization of Tardos' theorem. In *Foundations of computational mathematics (Hong Kong, 2000)*, pages 93–147. World Sci. Publ., River Edge, NJ, 2002.

[20] S. Hwang. The Edmonds-Giles conjecture and its relaxations. Master's thesis, University of Waterloo, 2022.

[21] R. Kannan and A. Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, 1979.

[22] L. Lovász. On two minimax theorems in graph theory. *Journal of Combinatorial Theory, Series B*, 21:96 – 103, 1976.

[23] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag Berlin Heidelberg, 2003.

[24] N. Megiddo. On finding primal- and dual-optimal bases. *ORSA J. Comput.*, 3(1):63–65, 1991.

[25] S. Mehrotra and Y. Ye. Finding an interior point in the optimal face of linear programs. *Math. Programming*, 62(3):497–515, 1993.

[26] V. V. Prasolov. *Problems and Theorems in Linear Algebra*, volume 134 of *Translations of Mathematical Monographs*. American Mathematical Society, 1994.

[27] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, April 1998.

[28] A. Schrijver. *Combinatorial Optimization. Polyhedra and Efficiency*, volume 24 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, 2003.

[29] A. Sebő. Hilbert bases, Carathéodory's theorem, and combinatorial optimization. In R. Kannan and W. Pulleyblank, editors, *Integer Programming and Combinatorial Optimization (IPCO 1990), Lecture Notes in Computer Science*, pages 431–456, 1990.

[30] A. Storjohann. *Algorithms for matrix canonical forms*. PhD thesis, ETH Zurich, 2000.

[31] L. Tunçel. *Polyhedral and semidefinite programming methods in combinatorial optimization*, volume 27 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI; Fields Institute for Research in Mathematical Sciences, Toronto, ON, 2010.

[32] J. D. Vaaler. A geometric inequality with applications to linear forms. *Pacific Journal of Mathematics*, 83(2):543 – 553, 1979.

[33] Y. Ye. *Interior point algorithms*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., New York, 1997. Theory and analysis, A Wiley-Interscience Publication.

[34] Y. Ye, M. J. Todd, and S. Mizuno. An $O(\sqrt{n}L)$-iteration homogeneous and self-dual linear programming algorithm. *Math. Oper. Res.*, 19(1):53–67, 1994.

A   Primer on lattices and determinants

Generally we follow [23, 8, 26] as reference texts on lattices, inequalities, and equalities in linear algebra, respectively. More specifically, we use the following specific results in the paper.

Hermite normal form. Let $A \in \mathbb{Z}^{m \times n}$ be a matrix of full row rank. Then A can be brought into *Hermite normal form* by means of *elementary unimodular column operations*. In particular, there exists an n-by-n unimodular matrix U such that $AU = (B\ \mathbf{0})$, where B is a non-singular m-by-m matrix, and $\mathbf{0}$ is an m-by-$(n-m)$ matrix with zero entries. See ([10], Section 1.5.2) or ([27], Chapter 4) for more details.

Matrix GCD. Denote by $\gcd(A)$ the greatest common divisor (GCD) of all order-m minors of A. This quantity can be found as follows. First, bring A into Hermite normal form after applying elementary unimodular column operations, say we obtain $(B\ \mathbf{0})$ where B is a square matrix. Then $\gcd(A) = \gcd(B) = |\det(B)|$, where the first equality can be readily checked by the reader, and the second one follows immediately from definition.

Lattice "closure" and index. Let L be an m-dimensional lattice contained in $\mathbb{Z}^n$, and let $\overline{L} := \mathrm{aff}(L) \cap \mathbb{Z}^n$. Clearly, $\overline{L}$ is a lattice containing L. Observe that within the affine hull of L, and confined to the integers, $\overline{L}$ is the maximal lattice containing L. It is known that $\overline{L}$ can be partitioned into a number of integral linear translations of L; this number is denoted as the *index* $[\overline{L} : L] \in \mathbb{Z}_{\geq 1}$. Thus, $L = \overline{L}$ if and only if $[\overline{L} : L] = 1$.

Lattice determinant and orthogonal complement. The *determinant of L*, denoted $\det(L)$, is the m-dimensional volume of its fundamental parallelepiped. The inverse of $\det(L)$ may be used to measure the "density" of L: the smaller the determinant, the larger the density. It is known that $\det(L) = [\overline{L} : L]\det(\overline{L})$ (see [23], Proposition 1.1.5 (4)). The *orthogonal complement* of L is the lattice $L^\perp := \{y \in \mathbb{Z}^n : y^\top x = 0\ \forall\, x \in L\}$. It can be readily checked that $L^\perp$ has index 1, that is, $L^\perp = \overline{L^\perp}$. It is known that $\det(L^\perp) = \det(\overline{L})$ (see [23], Proposition 1.9.8).

Lattice formulas. Let $C \in \mathbb{Z}^{n \times m}$ be a matrix with m linearly independent columns, and consider the lattice $L := \{Cy : y \in \mathbb{Z}^m\} \subseteq \mathbb{Z}^n$. Let us find $\det(L), \overline{L}, [\overline{L} : L]$ and $L^\perp$ in terms of C. First, the fundamental parallelepiped of L is $\{C\lambda : \mathbf{0} \leq \lambda < \mathbf{1}\}$, whose m-dimensional volume is $\det(L)$. Subsequently, it can be readily checked that $\det(L)^2$ is the Gram determinant of the columns of C, that is, $\det(L) = \sqrt{\det(C^\top C)}$. It can be readily seen that $\overline{L} = \{Cy : y \in \mathbb{R}^m\} \cap \mathbb{Z}^n$. By turning $C^\top$ into Hermite normal form after applying elementary unimodular column operations, it can be shown that $[\overline{L} : L] = \gcd(C)$ (see [23], Proposition 1.1.5 (4)). Finally, observe that $L^\perp = \{x \in \mathbb{Z}^n : C^\top x = \mathbf{0}\}$. By combining the equalities provided thus far, we see that $\det(L^\perp) = \sqrt{\det(C^\top C)}/\gcd(C)$.

Lattice-free sets. Observe that $P := \{C\lambda : -\mathbf{1} < \lambda < \mathbf{1}\}$ is *lattice-free*, that is, P contains no nonzero vector from the lattice L. The set P is the union of 2^m reflections of the fundamental parallelepiped of L, whose relative interiors are pairwise disjoint, so $\mathrm{vol}_m(P) = 2^m \det(L)$. Observe further that P is a convex set that is symmetric about the origin. An important result of Minkowski from the Geometry of Numbers states that among all such sets which are lattice-free, P reaches the maximum m-dimensional volume.

Minkowski's First Theorem (see [23], Theorem 2.7.1). *Let $L \subseteq \mathbb{Z}^n$ be an m-dimensional lattice. Let C be a convex set that is symmetric about the origin. If $C \cap L = \{\mathbf{0}\}$, then $\mathrm{vol}_m(C) \leq 2^m \det(L)$.*

Hadamard's inequality. Let $B \in \mathbb{Z}^{m \times m}$ be a matrix with columns $b^1, \ldots, b^m$. Observe that $|\det(B)|$ is the volume of the parallelepiped with sides $b^1, \ldots, b^m$, implying in turn the well-known *Hadamard inequality*, stating that $|\det(B)| \leq \prod_{i=1}^{m} \|b^i\|_2$ ([18], see [8], Chapter 2, §11). Subsequently, since $\|b^i\|_2 \leq \sqrt{m} \|b^i\|_\infty$ for each $i \in [m]$, it follows that $|\det(B)|^{1/m} \leq \sqrt{m} \|B\|_\infty$.

Minors of the adjugate matrix. Let U be an n-by-n matrix. The *adjugate of U*, denoted $\mathrm{adj}(U)$, is an n-by-n matrix such that $U \mathrm{adj}(U) = \det(U)I$. For all $i, j \in [n]$, $\mathrm{adj}(U)_{ji}$ is defined as a cofactor of U, namely, it is $(-1)^{i+j}$ times the determinant of the submatrix of U obtained after removing row i and column j. An extension of this identity attributed to Jacobi expresses every minor of $\mathrm{adj}(U)$ as a cofactor of the original matrix U.

Jacobi's Theorem (see [26], Theorem 2.5.2). *Let U be an n-by-n matrix, and $m \in [n-1]$. For row labels $I \subseteq [n]$ and column labels $J \subseteq [n]$ of U such that $|I| = |J| = m$, we have*

$$\det(\mathrm{adj}(U)_{J \times I}) = \mathrm{sgn}(\sigma) \det(U_{\bar{I} \times \bar{J}}) \det(U)^{m-1}.$$

where $\sigma : [n] \to [n]$ is the permutation defined as $\sigma(i_k) = j_k$ for all $k \in [n]$, for the following labelling of the rows and columns of U: the rows/columns of $U_{I \times J}$ are labelled $\{i_1, \ldots, i_m\}/\{j_1, \ldots, j_m\}$ from top to bottom/left to right, and the rows/columns of $U_{\bar{I} \times \bar{J}}$ are labelled $\{i_{m+1}, \ldots, i_n\}/\{j_{m+1}, \ldots, j_n\}$ from top to bottom/left to right.