Total dual dyadicness and dyadic generating sets

Ahmad Abdi[1], Gérard Cornuéjols[2], Bertrand Guenin[3], and Levent Tunçel[3]

[1] Department of Mathematics, LSE, London, UK
a.abdi1@lse.ac.uk
[2] Tepper School of Business, Carnegie Mellon University, Pittsburgh, USA
gc0v@andrew.cmu.edu
[3] Department of Combinatorics and Optimization, University of Waterloo
bguenin@uwaterloo.ca,ltuncel@uwaterloo.ca

Abstract. A vector is *dyadic* if each of its entries is a dyadic rational number, i.e. of the form $\frac{a}{2^k}$ for some integers a, k with $k \geq 0$. A linear system $Ax \leq b$ with integral data is *totally dual dyadic* if whenever $\min\{b^\top y : A^\top y = w, y \geq \mathbf{0}\}$ for w integral, has an optimal solution, it has a dyadic optimal solution. In this paper, we study total dual dyadicness, and give a co-NP characterization of it in terms of *dyadic generating sets for cones and subspaces*, the former being the dyadic analogue of *Hilbert bases*, and the latter a polynomial-time recognizable relaxation of the former. Along the way, we see some surprising turn of events when compared to total dual integrality, primarily led by the *density* of the dyadic rationals. Our study ultimately leads to a better understanding of total dual integrality and polyhedral integrality. We see examples from dyadic matrices, T-joins, cycles, and perfect matchings of a graph.

1 Introduction

A *dyadic rational* is a number of the form $\frac{a}{2^k}$ for some integers a, k where $k \geq 0$. The dyadic rationals are precisely the rational numbers with a finite binary representation, and are therefore relevant for (binary) floating-point arithmetic in numerical computations. Modern computers represent the rational numbers by fixed-size floating points, inevitably leading to error terms, which are compounded if serial arithmetic operations are performed such as in the case of mixed-integer linear, semidefinite, and more generally convex optimization. This has led to an effort to mitigate floating-point errors [27] as well as the need for exact solvers [6,25].

We address a different, though natural theoretical question: *When does a linear program admit an optimal solution whose entries are dyadic rationals?* A vector is *dyadic* if every entry is a dyadic rational. Consider the following primal dual pair of linear programs for $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and $w \in \mathbb{Z}^n$.

$$(P) \quad \max\{w^\top x : Ax \leq b\} \qquad (D) \quad \min\{b^\top y : A^\top y = w, y \geq \mathbf{0}\}.$$

When does (D) admit a dyadic optimal solution for all $w \in \mathbb{Z}^n$? How about (P)? Keeping close to the integral case, these questions lead to the notions of *totally* *dual dyadic* systems and *dyadic polyhedra*. In this paper, we reassure the reader that dyadic polyhedra enjoy a similar characterization as *integral polyhedra*, but in studying totally dual dyadic systems, we see an intriguing and somewhat surprising turn of events when compared to *totally dual integral (TDI)* systems [10]. As such, we shall keep the focus of the paper on total dual dyadicness and its various characterizations. The characterizations lead to *dyadic generating sets* for cones and subspaces, where the first notion is polyhedral and can be thought of as a dyadic analogue of *Hilbert bases*, while the second notion is lattice-theoretic and new. We shall see some intriguing examples of totally dual dyadic systems and dyadic generating sets from Integer Programming, Combinatorial Optimization, and Graph Theory. Our study eventually leads to a better understanding of TDI systems and integral polyhedra.

Our characterizations extend easily to the *p-adic rationals* for any prime number $p \geq 3$. For this reason, we shall prove our characterizations in the general setting. Interestingly, however, most of our examples do *not* extend to the p-adic setting for $p \geq 3$.

1.1 Totally dual p-adic systems and p-adic generating sets

Let $p \geq 2$ be a prime number. A *p-adic rational* is a number of the form $\frac{a}{p^k}$ for some integers a, k where $k \geq 0$. A vector is *p-adic* if every entry is a p-adic rational. Consider a linear system $Ax \leq b$ where $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$. We say that $Ax \leq b$ is *totally dual p-adic* if for all $w \in \mathbb{Z}^n$ for which $\min\{b^\top y : A^\top y = w, y \geq \mathbf{0}\}$ has an optimum, it has a p-adic optimum. For $p = 2$, we abbreviate 'totally dual dyadic' as 'TDD'. We prove the following characterization, which relies on two key notions defined afterwards.

Theorem 1 (proved in §4). *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and $P := \{x : Ax \leq b\}$. Given a nonempty face F, denote by $A_F x \leq b_F$ the subsystem of $Ax \leq b$ corresponding to the implicit equalities of F. Then the following statements are equivalent for every prime p: (1) $Ax \leq b$ is totally dual p-adic, (2) for every nonempty face F of P, the rows of A_F form a p-adic generating set for a cone, (3) for every nonempty face F of P, the rows of A_F form a p-adic generating set for a subspace.*

In fact, in (2), it suffices to consider only the minimal nonempty faces.

Let $\{a^1, \dots, a^n\} \subseteq \mathbb{Z}^m$. The set $\{a^1, \dots, a^n\}$ is a *p-adic generating set for a cone (p-GSC)* if every integral vector in the conic hull of the vectors can be expressed as a p-adic conic combination of the vectors (meaning that the coefficients used are p-adic). In contrast, $\{a^1, \dots, a^n\}$ is a *p-adic generating set for a subspace (p-GSS)* if every integral vector in the linear hull of the vectors can be expressed as a p-adic linear combination of the vectors. For $p = 2$, we use the acronyms DGSC and DGSS instead of 2-GSC and 2-GSS, respectively.

The careful reader may notice that an *integral* generating set for a cone is just a *Hilbert basis* [13] (following [21], §22.3). In contrast with Hilbert bases where a satisfying characterization remains elusive, we have the following polyhedral characterization of a p-GSC:

Theorem 2 (proved in §3). *Let $\{a^1, \dots, a^n\} \subseteq \mathbb{Z}^m$, $C := \operatorname{cone}\{a^1, \dots, a^n\}$, and p a prime. Then $\{a^1, \dots, a^n\}$ is a p-GSC if, and only if, for every nonempty face F of C, $\{a^i : a^i \in F\}$ is a p-GSS.*

The careful reader may notice that in contrast to total dual integrality, the characterization of totally dual p-adic systems, Theorem 1, enjoys a third equivalent condition, namely (3). This new condition, as well as the characterization of a p-GSC, Theorem 2, is made possible due to a distinguishing feature of the p-adic rationals: *density*. The p-adic rationals, as opposed to the integers, form a dense subset of $\mathbb{R}$. We shall elaborate on this in §2.

Going further, we have the following lattice-theoretic characterization of a p-GSS. We recall that the *elementary divisors* (a.k.a. *invariant factors*) of an integral matrix are the nonzero entries of the *Smith normal form* of the matrix; see §3 for more.

Theorem 3 (proved in §3). *The following statements are equivalent for a matrix $A \in \mathbb{Z}^{m\times n}$ of rank r and every prime p: (1) the columns of A form a p-GSS, (2) the rows of A form a p-GSS, (3) whenever $y^\top A$ and Ax are integral, then $y^\top Ax$ is a p-adic rational, (4) every elementary divisor of A is a power of p, (5) the GCD of the subdeterminants of A of order r is a power of p, (6) there exists a matrix B with p-adic entries such that $ABA = A$.*

Theorem 3 is used in §3 to prove that testing the p-GSS property can be done in polynomial time. Subsequently, the problem of testing total dual p-adicness belongs to co-NP by Theorem 1 (see §4), and the problem of testing the p-GSC property belongs to co-NP by Theorem 2 (see §3). Whether the two problems belong to NP, or P, remains unsolved. It should be pointed out that testing total dual *integrality*, as well as testing the Hilbert basis property, is co-NP-complete [9,19].

1.2 Connection to integral polyhedra and TDI systems

Our characterizations stated so far, as well as our characterization of *p-adic polyhedra* explained in §5, have the following intriguing consequence:

Theorem 4. *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$, and $P := \{x : Ax \le b\}$. Then the following are equivalent: (1) $Ax \le b$ is totally dual p-adic for all primes p, (2) $Ax \le b$ is totally dual p- and q-adic, for distinct primes p, q, (3) for every nonempty face F of P, the GCD of the subdeterminants of A_F of order $\operatorname{rank}(A_F)$ is 1.*

Proof. **(1) ⇒ (2)** is immediate. **(2) ⇒ (3)** For every nonempty face F of P, the rows of A_F form both a p- and a q-GSS by Theorem 1, so the GCD of the subdeterminants of A_F of order $\operatorname{rank}(A_F)$ is both a power of p and a power of q by Theorem 3, so the GCD of the subdeterminants of A_F of order $\operatorname{rank}(A_F)$ must be 1. **(3) ⇒ (1)** follows from Theorem 1 and Theorem 3 □

If $Ax \leq b$ is TDI, then statement (3) above must hold (this is folklore, and explored in [22]. In fact, if P is pointed, then for every vertex of P, we have a stronger property known as *local strong unimodularity* [12].) It was a widely known fact that the converse is not true. Theorem 4 clarifies this further by equating (3) with (1) and (2). Going a step further, it is known that if $Ax \leq b$ is TDI, then $\{x : Ax \leq b\}$ is an integral polyhedron [10,13]. We shall strengthen this result in the pointed case:

Theorem 5 (proved in §5). *Suppose $P := \{x : Ax \leq b\}$ is a pointed polyhedron. If $Ax \leq b$ is totally dual p- and q-adic, for distinct primes p, q, then P is an integral polyhedron.*

Fulkerson's theorem that every integral set packing system is TDI, can be seen as a (stronger) converse to Theorem 5 [11]. As for set covering systems, there is a conjecture of Paul Seymour that predicts a (stronger) converse to Theorem 5.

Conjecture 6 (The Dyadic Conjecture [20], §79.3e). Let A be a matrix with $0, 1$ entries. If $Ax \geq \mathbf{1}, x \geq \mathbf{0}$ defines an integral polyhedron, then it is TDD.

The authors recently proved the first nontrivial step of the Dyadic Conjecture: If $Ax \geq 1, x \geq \mathbf{0}$ defines an integral polyhedron, then for every nonnegative integral w such that $\min\{w^\top x : Ax \geq \mathbf{1}, x \geq \mathbf{0}\}$ has optimal value two, the dual has a dyadic optimal solution [1].

1.3 Examples

Our first example comes from Integer Programming, and more precisely, from matrices with restricted subdeterminants.

Theorem 7. *Let $A \in \mathbb{Z}^{m\times n}$ be a matrix whose subdeterminants belong to $\{0\} \cup \{\pm p^k : k \in \mathbb{Z}_+\}$ for some prime p, and let $b \in \mathbb{Z}^m$. Then $Ax \leq b$ is totally dual p-adic.* □

Similar, if not identical, settings have been studied previously; see for example [16,4] (the last reference has more relevant citations); see the full version for more details and the proof [2]. The node-edge incidence matrix of a graph is known to satisfy the hypothesis for $p = 2$ (folklore), and therefore leads to a TDD system. More generally, matrices whose subdeterminants belong to $\{0\} \cup \{\pm 2^k : k \in \mathbb{Z}_+\}$ have been studied from a matroid theoretic perspective; matroids representable over the rationals by such matrices are known as *dyadic matroids* and their study was initiated by Whittle [28].

Moving on, from Combinatorial Optimization, we get examples only in the dyadic setting. Let $G = (V, E)$ be a graph, and T a nonempty subset of even cardinality. A *T-join* is a subset $J \subseteq E$ such that the odd-degree vertices of $G[J]$ is precisely T. T-joins were studied due to their connection to the *minimum weight perfect matching problem*, but also to the *Chinese postman set problem* (see [7], Chapter 5). As a consequence of a recent result [3], we obtain the following.

Theorem 8 (proved in §6). *Let $G = (V, E)$ be a graph, and $T \subseteq V$ a nonempty subset of even cardinality. Then $x(J) \geq 1 \ \forall \ T$-joins $J; x \geq \mathbf{0}$ is TDD.*

The basic solutions to the dual of $\min\{\mathbf{1}^\top x : x(J) \geq 1 \ \forall \ T\text{-joins } J; x \geq \mathbf{0}\}$ may actually be non-dyadic, with many examples coming from snarks G on at least 18 vertices with $T = V(G)$ and $w = \mathbf{1}$ [18], thereby creating an interesting contrast between the proofs of Theorem 7 and Theorem 8. Also, Theorem 8 does not extend to the p-adic setting for any prime $p \geq 3$. To see this, let G be the graph with vertices $1,2,3,4,5$ and edges $\{1,3\},\{1,4\},\{1,5\},\{3,2\},\{4,2\},\{5,2\}$, let $T := \{1,2,3,4\}$, and let $w := \mathbf{1}$. Then the dual has a unique optimum, namely $y^\star = \frac{1}{2} \cdot \mathbf{1}$, which is not p-adic for any $p \geq 3$.

The system in Theorem 8 defines an integral set covering polyhedron (see [8], Chapter 2), so Theorem 8 verifies Conjecture 6 for such instances. In fact, it has been conjectured that the system in Theorem 8 is totally dual *quarter-integral* ([8], Conjecture 2.15).

Moving on, let $G = (V, E)$ be a graph. A *cycle* is a subset $C \subseteq E$ such that every vertex in V is incident with an even number of edges in C. A *circuit* is a nonempty cycle that does not contain another nonempty cycle. A *perfect matching* is a subset $M \subseteq E$ such that every vertex in V is incident with exactly one edge in M. Define $\mathbf{C}(G) := \{\chi_C : C \text{ a circuit of } G\}$ and $\mathbf{M}(G) := \{\chi_M : M \text{ a perfect matching of } G\}$. See [14] for an excellent survey on lattice and conic characterizations of these two sets.

Theorem 9 (proved in §6). *Let $G = (V, E)$ be a graph such that $|V|$ is even. Then $\mathbf{M}(G)$ is a DGSC.*

This theorem does not extend to the p-adic setting for $p \geq 3$ either; this is justified in §6. If G is an *r-graph*, then the *Generalized Berge-Fulkerson Conjecture* [23] predicts that the all-ones vector can be written as a *half-integral* conic combination of $\mathbf{M}(G)$; Theorem 9 proves this can be done *dyadically*.

Theorem 10. *Let $G = (V, E)$ be a graph. Then $\mathbf{C}(G)$ is a DGSC.* □

If G is bridgeless, then the *Cycle Double Cover Conjecture* [26,24] predicts that the all-ones vector can be written as a *half-integral* conic combination of the vectors in $\mathbf{C}(G)$; Theorem 10 implies this can be done *dyadically*. The theorem is proved in the full version [2], and uses Theorem 1 and interestingly the notion of *cuboids* [1]. There, we also note that the theorem does not extend to the p-adic setting for $p \geq 3$.

2 Density Lemma and the Theorem of the Alternative

Many of our results are made possible by an important feature of the p-adic rationals distinguishing them from the integers, namely *density*.

Remark 11. The p-adic rationals form a dense subset of $\mathbb{R}$.

Lemma 12 (Density Lemma). *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and p a prime. If $\{x : Ax = b\}$ contains a p-adic point, then the p-adic points in the set form a dense subset. In particular, a nonempty rational polyhedron contains a p-adic point if, and only if, its affine hull contains a p-adic point.*

Proof. It suffices to prove the first statement. Suppose $\{x : Ax = b\}$ contains a p-adic point, say $\hat{x}$. Since A has integral entries, its kernel has an integral basis, say $d^1, \cdots, d^r$. Observe that $\{x : Ax = b\}$ is the set of vectors of the form $\hat{x} + \sum_{i=1}^r \lambda_i d^i$ where $\lambda \in \mathbb{R}^r$. Consider the set $S := \left\{\hat{x} + \sum_{i=1}^r \lambda_i d^i : \lambda_i \text{ is } p\text{-adic for each } i\right\}$. By Remark 11, it can be readily checked that S is a dense subset of $\{x : Ax = b\}$. Since $\hat{x}$ is p-adic, and the d^i's are integral, the points in S are p-adic, thereby proving the lemma. □

A natural follow-up question arises: When does a rational subspace contain a p-adic point? Addressing this question requires a familiar notion in Integer Programming. Every integral matrix of full row rank can be brought into *Hermite normal form* by means of *elementary unimodular column operations.* In particular, if A is an integral $m \times n$ matrix of full row rank, there exists an $n \times n$ *unimodular* matrix U such that $AU = (B\ \mathbf{0})$, where B is a non-singular $m \times m$ matrix, and $\mathbf{0}$ is an $m \times (n-m)$ matrix with zero entries. By a square unimodular matrix, we mean a square integral matrix whose determinant is ± 1; note that the inverse of such a matrix is also unimodular. See ([5], Section 1.5.2) or ([21], Chapter 4) for more details.

Lemma 13 (Theorem of the Alternative). *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$, and p a prime. Then either $Ax = b$ has a p-adic solution, or there exists a $y \in \mathbb{R}^m$ such that $y^\top A$ is integral and $y^\top b$ is non-p-adic, but not both.*

Proof. Suppose $A\hat{x} = b$ for a p-adic point $\hat{x}$, and $y^\top A$ is integral. Then $y^\top b = y^\top (A\hat{x}) = (y^\top A)\hat{x}$ is an integral linear combination of p-adic rationals, and is therefore a p-adic rational. Thus, both statements cannot hold simultaneously. Suppose $Ax = b$ has no p-adic solution. If $Ax = b$ has no solution at all, then there exists a vector y such that $y^\top A = \mathbf{0}$ and $y^\top b \neq 0$; by scaling y appropriately, we can ensure that $y^\top b$ is non-p-adic, as desired. Otherwise, $Ax = b$ has a solution. We may assume that A has full row rank. Then there exists a square unimodular matrix U such that $AU = (B\ \mathbf{0})$, where B is a non-singular matrix. Observe that $\{x : Ax = b\} = \{Uz : AUz = b\}$. Thus, as $Ax = b$ has no p-adic solution x, and U has integral entries, we may conclude that the system $AUz = b$ has no p-adic solution z either. Let us expand the latter system. Let I, J be the sets of column labels of $B, \mathbf{0}$ in $AU = (B\ \mathbf{0})$, respectively. Then $\{z : AUz = b\} = \left\{z : (B\ \mathbf{0})\binom{z_I}{z_J} = b\right\} = \{z : Bz_I = b, z_J \text{ free}\} = \left\{z : z_I = B^{-1}b, z_J \text{ free}\right\}$. In particular, since $AUz = b$ has no p-adic solution, the vector $B^{-1}b$ is non-p-adic. Thus, there exists a row $y^\top$ of B^{-1} for which $y^\top b$ is non-p-adic. We claim that $y^\top A$ is integral, thereby showing y is the desired vector. To this end, observe that $B^{-1}AU = B^{-1}(B\ \mathbf{0}) = (I\ \mathbf{0})$, implying in turn that $B^{-1}A = (I\ \mathbf{0})U^{-1}$. As the inverse of a square unimodular matrix, U^{-1} is also unimodular and therefore has integral entries, implying in turn that $B^{-1}A$, and so $y^\top A$, is integral. □

Remark 14. If t is a p- and q-adic rational, for distinct primes p, q, then t is integral.

Corollary 15. *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$. If $Ax = b$ has p- and q-adic solutions, for distinct primes p and q, then the system has an integral solution.*

Proof. By the Theorem of the Alternative, whenever $y^\top A$ is integral, $y^\top b$ is both p- and q-adic, implying in turn that $y^\top b$ is integral by Remark 14. Thus, by the Integer Farkas Lemma, $Ax = b$ has an integral solution. □

Finally, the Density Lemma and the Theorem of the Alternative have the following p-adic analogue of Farkas Lemma in Linear Programming.

Corollary 16 (p-Adic Farkas Lemma). *Let P be a nonempty rational polyhedron whose affine hull is $\{x : Ax = b\}$, where A, b are integral. Then for every prime p, P contains a p-adic point if, and only if, there does not exist y such that $y^\top A$ is integral and $y^\top b$ is non-p-adic.*

3 p-Adic generating sets for subspaces and cones

Recall that a set of vectors $\{a^1, \dots, a^n\} \subseteq \mathbb{Z}^m$ forms a p-GSS if every integral vector in the linear hull of the vectors can be expressed as a p-adic linear combination of the vectors. Observe that every p-adic vector in the linear hull of a p-GSS can also be expressed as a p-adic linear combination of the vectors. We prove the following lemma in the full version [2].

Lemma 17. *Let $A \in \mathbb{Z}^{m\times n}$, and U a unimodular matrix of appropriate dimensions. Then (1) the columns of A form a p-GSS if, and only if, the columns of UA do, and (2) the columns of A form a p-GSS if, and only if, the columns of AU do.* □

In order to prove Theorem 3, we need a definition. Let A be an integral matrix of rank r. It is well-known that by applying elementary row *and* column operations, we can bring A into *Smith normal form*, that is, into a matrix with a leading $r \times r$ minor D and zeros everywhere else, where D is a diagonal matrix with diagonal entries $\delta_1, \dots, \delta_r \geq 1$ such that $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_r$ (see [21], Section 4.4). It can be readily checked that for each $i \in [r]$, δ_i is the GCD of the subdeterminants of A of order i. The δ_i's are referred to as the *elementary divisors*, or *invariant factors*, of A.

Proof of Theorem 3. **(1) ⇔ (3)** Suppose (1) holds. Choose x, y such that $y^\top A$ and Ax are integral. Let $b := Ax \in \mathbb{Z}^m$. By (1), there exists a p-adic $\bar{x}$ such that $b = A\bar{x}$. Thus, $y^\top Ax = y^\top A\bar{x} = (y^\top A)\bar{x}$, which is p-adic because $y^\top A$ is integral and $\bar{x}$ p-adic, as required. Suppose conversely that (3) holds. Pick $b \in \mathbb{Z}^m$ such that $A\bar{x} = b$ for some $\bar{x}$. We need to prove that $Ax = b$ has a p-adic solution. If $y^\top A$ is integral, then $y^\top b = y^\top A\bar{x}$, which is p-adic by (3). Thus, by the Theorem of the Alternative, $Ax = b$ has a p-adic solution, as required.

(2) ⇔ (3) holds by applying the established equivalence (1) ⇔ (3) to $A^\top$.

(1)-(3) ⇔ (4): By Lemma 17, the equivalent conditions (1)-(3) are preserved under elementary unimodular row/column operations; these operations clearly preserve (4) as well. Thus, it suffices to prove the equivalence between (1)-(3) and (4) for integral matrices in Smith normal form. That is, we may assume that A has a leading $r\times r$ minor D and zeros everywhere else, where D is a diagonal matrix with diagonal entries $\delta_1,\dots,\delta_r \geq 1$ such that $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_r$. Suppose (1)-(3) hold. We need to show that each δ_i is a power of p. Consider the feasible system $Ax = e_i$; every solution x to this system satisfies $x_j = 0, j \in [r] - \{i\}$ and $x_i = \frac{1}{\delta_i}$. Since the columns of A form a p-GSS, $\frac{1}{\delta_i}$ must be p-adic, so δ_i is a power of p, as required. Suppose conversely that (4) holds. We need to show that whenever $Ax = b, b \in \mathbb{Z}^m$ has a solution, then it has a p-adic solution. Clearly, it suffices to prove this for $b = e_i, i \in [r]$, which holds because each $\delta_i, i \in [r]$ is a power of p.

(4) ⇔ (5) is rather immediate; the only additional remark is that every divisor of a power of p is also a power of p.

(6) ⇒ (3) If $y^\top A$ and Ax are integral, then $y^\top Ax = y^\top(ABA)x = (y^\top A)B(Ax)$, which is p-adic since $y^\top A, Ax$ are integral and B has p-adic entries, as required.

(4) ⇒ (6) Choose unimodular matrices U_r, U_c such that U_rAU_c is in Smith normal form with elementary divisors $\delta_1,\dots,\delta_r$. Let B' be the $n\times m$ matrix with a leading diagonal matrix $D^{-1} = \mathrm{Diag}(\frac{1}{\delta_1},\dots,\frac{1}{\delta_r})$, and zeros everywhere else. Let $B := U_cB'U_r$, which is a matrix with p-adic entries since each δ_i is a power of p. We claim that $ABA = A$, thereby proving (6). This equality holds if, and only if, $U_rABAU_c = U_rAU_c$. To this end, we have $U_rABAU_c = U_rA(U_cB'U_r)AU_c = (U_rAU_c)B'(U_rAU_c) = U_rAU_c$, where the last equality holds due the definition of B' and the Smith normal form of U_rAU_c. □

In light of the previous proposition we may say that an integral *matrix* forms a p-GSS if its rows, respectively its columns, form a p-GSS. Consider the following complexity problem: (A) *Given an integral matrix, does it form a p-GSS?* The Smith normal form of an integral matrix, and therefore its elementary divisors, can be computed in polynomial time [15]. Thus, Theorem 3 has the following consequence.

Corollary 18. (A) *belongs to* P*.*

Recall that a set of vectors $\{a^1,\dots,a^n\} \subseteq \mathbb{Z}^m$ forms a p-GSC if every integral vector in the conic hull of the vectors can be expressed as a p-adic conic combination of the vectors. Observe that every p-adic vector in the conic hull of a p-GSC can also be expressed as a p-adic conic combination of the vectors.

Proposition 19. *If* $\{a^1,\dots,a^n\} \subseteq \mathbb{Z}^m$ *is a p-GSC, then it is a p-GSS.*

Proof. Let $A \in \mathbb{Z}^{m\times n}$ be the matrix whose columns are $a^1,\dots,a^n$. Take $b \in \mathbb{Z}^m$ such that $A\bar{x} = b$ for some $\bar{x}$. We need to show that the system $Ax = b$ has a p-adic solution. To this end, let $\bar{x}' := \bar{x} - \lfloor \bar{x} \rfloor \geq \mathbf{0}$ and $b' := A\bar{x}' = b - A\lfloor \bar{x} \rfloor \in \mathbb{Z}^m$. Thus, $Ax = b', x \geq \mathbf{0}$ has a solution, namely $\bar{x}'$, so it has a p-adic solution, say $\bar{z}'$, as the columns of A form a p-GSC. Let $\bar{z} := \bar{z}' + \lfloor \bar{x} \rfloor$, which is also p-adic. Then $A\bar{z} = A\bar{z}' + A\lfloor \bar{x} \rfloor = b' + A\lfloor \bar{x} \rfloor = b$, so $\bar{z}$ is a p-adic solution to $Ax = b$, as required. □

The converse of this result, however, does not hold. For example, let $k \geq 3$ be an integer, $n := p^k + 1$, and m an integer in $\{4, \dots, p^k\}$ such that $m-1$ is not a power of p. Consider the matrix

$$A := \left(E_n - I_n \left| \begin{array}{c} E_m - I_m \\ \hline \mathbf{0} \end{array} \right. \right)$$

where E_d, I_d denote the all-ones square and identity matrices of dimension d, respectively. We claim that the columns of A form a p-GSS but not a p-GSC. To see the former, note that A has rank n, and since $\det(E_n - I_n) = n - 1 = p^k$, the GCD of the subdeterminants of A of order n is a power of p, so the columns of A form a p-GSS by Theorem 3. To see the latter, consider the vector $b \in \{0,1\}^n$ whose first m entries are equal to 1, and whose last $n-m$ entries are equal to 0. Then $Ay = b, y \geq \mathbf{0}$ has a unique solution, namely $\bar{y}$ defined as $\bar{y}_i = 0$ for $1 \leq i \leq n$, and $\bar{y}_i = \frac{1}{m-1}$ for $n+1 \leq i \leq n+m$. In particular, as $m-1$ is not a power of p, b is an integral vector in the conic hull of the columns of A, but it cannot be expressed as a p-adic conic combination of the columns. Thus, the columns of A do not form a p-GSC.

However, we do have the following sort of converse.

Remark 20. If $\{a^1, \dots, a^n\} \subseteq \mathbb{Z}^m$ is a p-GSS, then $\{\pm a^1, \dots, \pm a^n\}$ is a p-GSC.

Proposition 21. *Let $\{a^1, \dots, a^n\} \subseteq \mathbb{Z}^m$ be a p-adic generating set for a cone, and F a nonempty face of the cone. Then $\{a^i : a^i \in F\}$ is a p-adic generating set for the cone F.*

Proof. Let b be an integral vector in the face F. Since $b \in C$, we can write b as a p-adic conic combination of the vectors in $\{a^1, \dots, a^n\}$. However, since b is contained in the face F, the conic combination can only assign nonzero coefficients to the vectors in F, implying in turn that b is a p-adic conic combination of the vectors in $\{a^i : a^i \in F\}$. As this holds for every b, $\{a^i : a^i \in F\}$ forms a p-GSC. □

Proof of Theorem 2. ($\Rightarrow$) follows from Proposition 21 and Proposition 19. ($\Leftarrow$) Let b be an integral vector in C, and F the minimal face of C containing b. Let B be the matrix whose columns are the vectors $\{a^i : a^i \in F\}$. We need to show that $Q := \{y : By = b, y \geq \mathbf{0}\}$, which is nonempty, contains a p-adic point. By the Density Lemma, it suffices to show that $\mathrm{aff}(Q)$, the affine hull of Q, contains a p-adic point. Our minimal choice of F implies that Q contains a point $\mathring{y}$ such that $\mathring{y} > \mathbf{0}$, implying in turn that $\mathrm{aff}(Q) = \{y : By = b\}$. As the columns of B form a p-GSS, and b is integral, it follows that $\mathrm{aff}(Q)$ contains a p-adic point, as required. □

Consider the following complexity problem: (B) *Given a set of vectors, does it form a p-GSC?* Theorem 2 and Corollary 18 have the following consequence.

Corollary 22. (B) *belongs to co-NP.*

4 Totally dual p-adic systems

Given integral A, b, recall that $Ax \le b$ is totally dual p-adic if for every integral w for which $\min\{b^\top y : A^\top y = w, y \ge \mathbf{0}\}$ has an optimal solution, it has a p-adic optimum. It can be readily checked that the rows of A form a p-GSS if, and only if, $Ax = \mathbf{0}$ is totally dual p-adic; and the rows of A form a p-GSC if, and only if, $Ax \le \mathbf{0}$ is totally dual p-adic.

Proof of Theorem 1. Consider the following pair of dual linear programs, for w later specified.

$$(P) \quad \max\{w^\top x : Ax \le b\} \qquad (D) \quad \min\{b^\top y : A^\top y = w, y \ge \mathbf{0}\}$$

For every face F of P, denote by $A_{\bar{F}}$ the row submatrix of A corresponding to the rows not in A_F. For every vector y, denote by $y_F, y_{\bar{F}}$ the variables corresponding to the rows in $A_F, A_{\bar{F}}$, respectively.

(1) ⇒ (2) Consider a nonempty face F of P. We need to show that the rows of A_F form a p-GSC. Let w be an integral vector in the conic hull of the rows of A_F. It suffices to express w as a p-adic conic combination of the rows of A_F. To this end, observe that every point in F is an optimal solution to (P). As $Ax \le b$ is TDD, (D) has a p-adic optimal solution, say $\bar{y} \ge \mathbf{0}$. As Complementary Slackness holds for all pairs $(\bar{x}, \bar{y}), \bar{x} \in F$, it follows that $\bar{y}_{\bar{F}} = \mathbf{0}$. Subsequently, we have $w = A^\top \bar{y} = A_F^\top \bar{y}_F$, thereby achieving our objective. **(2) ⇒ (3)** follows from Proposition 19. **(3) ⇒ (1)** Choose an integral w for which (D) has an optimal solution; we need to show now that it has a p-adic optimal solution. Denote by F the face of the optimal solutions to the primal linear program (P). By Complementary Slackness, the set of optimal solutions to the dual (D) is $Q := \{y : A^\top y = w, y \ge \mathbf{0}, y_{\bar{F}} = \mathbf{0}\}$. We need to show that Q contains a p-adic point. In fact, by the Density Lemma, it suffices to find a p-adic point in $\mathrm{aff}(Q)$, the affine hull of Q. By Strict Complementarity, Q contains a point $\mathring{y}$ such that $\mathring{y}_F > \mathbf{0}$, implying in turn that $\mathrm{aff}(Q) = \{y : A_F^\top y_F = w, y_{\bar{F}} = \mathbf{0}\}$. Since the rows of A_F form a p-GSS, and w is integral, we get that $\mathrm{aff}(Q)$ contains a p-adic point, as required. □

The careful reader may notice that by applying polarity to Theorem 1 with $b = \mathbf{0}$, we obtain another proof of Theorem 2. Moving on, consider the following complexity problem: (C) *Given a system $Ax \le b$ where A, b are integral, is the system totally dual p-adic?* Theorem 1 (3) and Corollary 18 have the following consequence.

Corollary 23. (C) *belongs to co-NP.*

5 p-Adic polyhedra

A nonempty rational polyhedron is *p-adic* if every nonempty face contains a p-adic point. We have the following characterization of p-adic polyhedra.

Remark 24. Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m, y \in \mathbb{R}^m$ and $y' := y - \lfloor y \rfloor \geq \mathbf{0}$. Then $A^\top y \in \mathbb{Z}^n$ if and only if $A^\top y' \in \mathbb{Z}^n$, y is p-adic if and only if y' is p-adic, and $b^\top y$ is p-adic if and only if $b^\top y'$ is p-adic.

Theorem 25. *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and $P := \{x : Ax \leq b\}$. Then the following are equivalent for every prime p: (1) P is a p-adic polyhedron, (2) for every nonempty face F of P, $\operatorname{aff}(F)$ contains a p-adic point, (3) for every nonempty face F of P, and z, if $A_F^\top z$ is integral then $b_F^\top z$ is p-adic, (4) for all $w \in \mathbb{R}^n$ for which $\max\{w^\top x : x \in P\}$ has an optimum, it has a p-adic optimum, (5) for all $w \in \mathbb{Z}^n$ for which $\max\{w^\top x : x \in P\}$ has an optimum, it has a p-adic optimal value.* □

There is an intriguing contrast between this characterization and that of integral polyhedra (see [5], Theorem 4.1), namely the novelty of statement (3), which is ultimately due to Strict Complementarity and the Density Lemma.

Proof. **(1) ⇒ (2)** follows immediately from definition. **(2) ⇒ (1)** By the Density Lemma, every nonempty face contains a p-adic point, so P is a p-adic polyhedron. **(2) ⇔ (3)** follows from the Theorem of the Alternative. **(1) ⇒ (4)** Suppose $\max\{w^\top x : x \in P\}$ has an optimum. Let F be the set of optimal solutions. As F is in fact a face of P, and P is p-adic, it follows that F contains a p-adic point. **(4) ⇒ (5)** If x is a p-adic vector, and w an integral vector, then $w^\top x$ is a p-adic rational.

(5) ⇒ (3) We prove the contrapositive. Suppose (3) does not hold, that is, there exist a nonempty face F and z such that $w := A_F^\top z \in \mathbb{Z}^n$ and $b_F^\top z$ is not p-adic. By Remark 24, we may assume that $z \geq \mathbf{0}$. Consider the following pair of dual linear programs:

$$(P) \quad \max\{w^\top x : Ax \leq b\} \qquad (D) \quad \min\{b^\top y : A^\top y = w, y \geq \mathbf{0}\}$$

Denote by $A_{\bar{F}}$ the row submatrix of A corresponding to rows not in A_F. Denote by $y_F, y_{\bar{F}}$ the variables of (D) corresponding to rows A_F and $A_{\bar{F}}$ of A, respectively. Define $\bar{y} \geq \mathbf{0}$ where $\bar{y}_F = z$ and $\bar{y}_{\bar{F}} = \mathbf{0}$. Then $A^\top \bar{y} = A_F^\top z = w$, so $\bar{y}$ is feasible for (D). Moreover, Complementary Slackness holds for every pair $(x, \bar{y}), x \in F$. Subsequently, $\bar{y}$ is an optimal solution to (D), and $b^\top \bar{y} = b_F^\top z$ is the common optimal value of the two linear programs. Since w is integral and $b_F^\top z$ is not p-adic, (5) does not hold, as required. □

Corollary 26. *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$, and p a prime. If $Ax \leq b$ is totally dual p-adic, then $\{x : Ax \leq b\}$ is a p-adic polyhedron.*

Proof. This follows immediately from Theorem 25 (5) ⇒ (1). □

Proof of Theorem 5. By Corollary 26, P is a p- and q-adic polyhedron. Since P is pointed, the minimal nonempty faces are vertices, so every vertex of P must be both p- and q-adic and therefore integral by Remark 14. Thus, P is an integral polyhedron. □

6 *T*-joins and perfect matchings

Let $G=(V,E)$ be a graph, and T a nonempty subset of even cardinality. A T*-cut* is a cut of the form $\delta(U)$ where $|U\cap T|$ is odd. Recall that a T-join is a subset $J\subseteq E$ such that the odd-degree vertices of $G[J]$ is precisely T. It can be readily checked that every T-cut and T-join intersect (see [8], Chapter 2). The following result was recently proved:

Theorem 27 ([3]). *Let $G=(V,E)$ be a graph, and T a nonempty subset of even cardinality. Let τ be the minimum cardinality of a T-cut. Then there exists a dyadic assignment $y_J\geq \mathbf{0}$ to every T-join J such that $\mathbf{1}^\top y=\tau$ and $\sum(y_J : J$ a T-join containing $e)\leq 1\ \forall e\in E$.*

The proof of Theorem 27 uses the Density Lemma, the Theorem of the Alternative, and a result of Lovász on the *matching lattice* [17].

Proof of Theorem 8. Let A be the matrix whose columns are labeled by E, and whose rows are the incidence vectors of the T-joins. We need to show that $\min\{w^\top x : Ax\geq \mathbf{1}, x\geq \mathbf{0}\}$ yields a TDD system. Choose an integral w such that the dual $\max\{\mathbf{1}^\top y : A^\top y\leq w, y\geq \mathbf{0}\}$ has an optimal solution, that is, $w\geq \mathbf{0}$. Let G' be obtained from G after replacing every edge e with w_e parallel edges (if $w_e=0$, then e is deleted). Let τ_w be the minimum cardinality of a T-cut of G', which is also the minimum weight of a T-cut of G. By Theorem 27, there exists a dyadic assignment $\bar{y}_J\geq 0$ to every T-join of G' such that $\mathbf{1}^\top\bar{y}=\tau_w$ and $\sum(\bar{y}_J : J$ a T-join of G' containing $e)\leq 1\ \forall e\in E(G')$. This naturally gives a dyadic assignment $y^\star_J\geq 0$ to every T-join of G such that $\mathbf{1}^\top y^\star=\tau_w$ and $A^\top y^\star\leq w$. Now let $\delta(U)$ be a minimum weight T-cut of G. Then $\chi_{\delta(U)}$ is a feasible solution to the primal which has value τ_w. As a result, $\chi_{\delta(U)}$ is optimal for the primal, and $y^\star$ is optimal for the dual. Thus, the dual has a dyadic optimal solution, as required. □

Moving on, let $G=(V,E)$ be a graph such that $|V|$ is even. Let us prove that $\mathbf{M}(G)$, which is equal to the set $\{\chi_M : M$ a perfect matching of $G\}$, is a DGSC.

Proof of Theorem 9. We may assume that G contains a perfect matching. Let $T:=V$. Note that every T-join has cardinality at least $\frac{|V|}{2}$, with equality holding precisely for the perfect matchings. By Theorem 8, the linear system $x(J)\geq 1\ \forall\ T$-joins $J; x\geq \mathbf{0}$ is TDD. Let P be the corresponding polyhedron, and F the minimal face containing the point $\frac{2}{|V|}\cdot\mathbf{1}$. The tight constraints of F are precisely $x(M)\geq 1$ for perfect matchings M, so by Theorem 1 for $p=2$, the rows of the corresponding coefficient matrix form a DGSC, implying in turn that $\mathbf{M}(G)$ is a DGSC. □

Let P_{10} be the Petersen graph. Then P_{10} has six perfect matchings. Let M be the matrix whose columns are labeled by $E(P_{10})$, and whose rows are the incidence vectors of the perfect matchings. It can be checked that the elementary divisors of M are $(1,1,1,1,1,2)$. Thus, for any prime $p\geq 3$, the rows of M which are the vectors in $\mathbf{M}(P_{10})$ do not form a p-GSS by Theorem 3, and so they do not form a p-GSC by Proposition 19. Thus, Theorem 9 does not extend to the p-adic setting for $p\geq 3$.

References

1. Abdi, A., Cornuéjols, G., Guenin, B., Tunçel, L.: Clean clutters and dyadic fractional packings. SIAM J. Discret. Math. Accepted
2. Abdi, A., Cornuéjols, G., Guenin, B., Tunçel, L.: Total dual dyadicness and dyadic generating sets (November 2021), full version
3. Abdi, A., Cornuéjols, G., Palion, Z.: On dyadic fractional packings of T-joins (2021), submitted
4. Appa, G., Kotnyek, B.: Rational and integral k-regular matrices. Discrete Math. **275**, 1–15 (2004)
5. Conforti, M., Cornuéjols, G., Zambelli, G.: Integer Programming. Springer International Publishing (2014)
6. Cook, W., Koch, T., Steffy, D., Wolter, K.: An exact rational mixed-integer programming solver. In: Günlük, O., Woeginger, G. (eds.) Integer Programming and Combinatorial Optimization (IPCO 2011), Lecture Notes in Computer Science. vol. 6655, pp. 104–116. Springer, Berlin, Heidelberg (2011)
7. Cook, W., Cunningham, W., Pulleyblank, W.R., Schrijver, A.: Combinatorial Optimization. John Wiley and Sons, Inc. (1998)
8. Cornuéjols, G.: Combinatorial Optimization: Packing and Covering, vol. 74. SIAM (2001)
9. Ding, G., Feng, L., Zang, W.: The complexity of recognizing linear systems with certain integrality properties. Math. Program. **114**, 321–334 (2008)
10. Edmonds, J., Giles, R.: A min-max relation for submodular functions on graphs. In: Studies in integer programming (Proc. Workshop, Bonn, 1975). pp. 185–204. Ann. of Discrete Math., Vol. 1 (1977)
11. Fulkerson, D.: Blocking and anti-blocking pairs of polyhedra. Math. Program. **1**, 168–194 (1971)
12. Gerards, B., Sebő, A.: Total dual integrality implies local strong unimodularity. Math. Program. **38**, 69–73 (1987)
13. Giles, F., Pulleyblank, W.: Total dual integrality and integer polyhedra. Linear Algebra and its Applications **25**, 191 – 196 (1979). https://doi.org/https://doi.org/10.1016/0024-3795(79)90018-1
14. Goddyn, L.: Cones, lattices, and hilbert bases of circuits and perfect matchings. In: Contemporary Mathematics. vol. 147, pp. 419–439. Amer. Math. Soc. (1993)
15. Kannan, R., Bachem, A.: Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. SIAM J. Comput. **8**, 499–507 (1979)
16. Lee, J.: Subspaces with well-scaled frames. Linear Algebra Appl. **114/115**, 21–56 (1989)
17. Lovász, L.: Matching structure and the matching lattice. Journal of Combinatorial Theory, Series B **43**(2), 187 – 222 (1987). https://doi.org/https://doi.org/10.1016/0095-8956(87)90021-9
18. Palion, Z.: On dyadic fractional packings of T-joins (April 2021), undergraduate thesis, London School of Economics and Political Science
19. Pap, J.: Recognizing conic TDI systems is hard. Math. Program., Ser. A **128**, 43–48 (2011)
20. Schrijver, A.: Combinatorial Optimization. Polyhedra and Efficiency. Springer, Berlin, Heidelberg (2003)
21. Schrijver, A.: Theory of Linear and Integer Programming. Wiley (April 1998)
22. Sebő, A.: Hilbert bases, Carathéodory's theorem, and combinatorial optimization. In: Kannan, R., Pulleyblank, W. (eds.) Integer Programming and Combinatorial Optimization (IPCO 1990), Lecture Notes in Computer Science. pp. 431–456 (1990)

23. Seymour, P.D.: On multi-colourings of cubic graphs, and conjectures of Fulkerson and Tutte. Proceedings of the London Mathematical Society **38**(3), 423–460 (05 1979). https://doi.org/https://doi.org/10.1112/plms/s3-38.3.423
24. Seymour, P.D.: Matroids and multicommodity flows. Europ. J. Combinatorics **2**, 257–290 (1981)
25. Steffy, D.E.: Topics in Exact Precision Mathematical Programming. Ph.D. thesis, Georgia Institute of Technology (2011)
26. Szekeres, G.: Polyhedral decomposition of cubic graphs. Bull. Austral. Math. Soc. **8**, 367–387 (1973)
27. Wei, H.: Numerical Stability in Linear Programming and Semidefinite Programming. Ph.D. thesis, University of Waterloo (2006)
28. Whittle, G.: A characterization of the matroids representable over GF(3) and the rationals. Journal of Combinatorial Theory, Series B **65**, 222–261 (1995)