Total dual dyadicness and dyadic generating sets*

Ahmad Abdi
Department of Mathematics, LSE, London, UK
a.abdi1@lse.ac.uk

Gérard Cornuéjols
Tepper School of Business, Carnegie Mellon University, Pittsburgh, USA
gc0v@andrew.cmu.edu

Bertrand Guenin
Department of Combinatorics and Optimization, University of Waterloo, Canada
bguenin@uwaterloo.ca

Levent Tunçel
Department of Combinatorics and Optimization, University of Waterloo, Canada
ltuncel@uwaterloo.ca

January 23, 2023

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 matroids, T-joins, cycles, and perfect matchings of a graph.

*An extended abstract of this work appeared in IPCO 2022.

Corresponding author: Gerard Cornuejols, Carnegie Mellon University, gc0v@andrew.cmu.edu

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 [31] as well as the need for exact solvers [10, 29].

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 $w \in \mathbb{Z}^n$.

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

($\mathbf{0}$ and $\mathbf{1}$ denote respectively the all-zeros and all-ones column, or row, vectors of appropriate dimension.) 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 [13]. 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 optimal solution. For $p = 2$, we abbreviate 'totally dual dyadic' as 'TDD'. We emphasize that for any statement that includes p-adic numbers, or a definition that relies on p-adic numbers (such as totally dual p-adic systems) we assume that $p \geq 2$ and that p is a prime.

Given a nonempty face F of a polyhedron $Ax \leq b$, denote by $A_F x \leq b_F$ the subsystem of $Ax \leq b$ corresponding to the implicit equalities of F.

We prove the following characterization, which relies on two key notions defined afterwards.

Theorem 1.1 (proved in §4)**.** *Let $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m$ and $P := \{x : Ax \leq b\}$. 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 $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$. The set $\{a^1, \ldots, a^n\}$ 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, $\{a^1, \ldots, a^n\}$ 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.

Notice that an *integral* generating set for a cone (where the vectors are expressed as integer conic combinations) is just a *Hilbert basis* [16]. (We address differing definitions of Hilbert bases in §7.)

In a departure from Hilbert bases, where a satisfying characterization remains elusive, we have the following polyhedral characterization of a p-GSC:

Theorem 1.2 (proved in §3)**.** *Let $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$, $C := \mathrm{cone}\{a^1, \ldots, a^n\}$, and p a prime. Then $\{a^1, \ldots, a^n\}$ 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 1.1, enjoys a third equivalent condition, namely (3). This new condition, as well as the characterization of a p-GSC, Theorem 1.2, 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. In the following statement GCD stands for the Greatest Common Divisor.

Theorem 1.3 (proved in §3)**.** *The following statements are equivalent for a matrix $A \in \mathbb{Z}^{m \times n}$ of rank r and a 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 1.3 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 1.1 (see §4), and the problem of testing the p-GSC property belongs to co-NP by Theorem 1.2 (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 [12, 22].

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 1.4. *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$, and $P := \{x : Ax \leq b\}$. Then the following are equivalent:*

(1) $Ax \leq b$ is totally dual p-adic for all primes p,

(2) $Ax \leq b$ 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 $\mathrm{rank}(A_F)$ 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 1.1, so the GCD of the subdeterminants of A_F of order $\mathrm{rank}(A_F)$ is both a power of p and a power of q by Theorem 1.3, so the GCD of the subdeterminants of A_F of order $\mathrm{rank}(A_F)$ must be 1. **(3) ⇒ (1)** follows from Theorem 1.1 and Theorem 1.3. □

If $Ax \leq b$ is TDI, and therefore totally dual p-adic for any prime p, then statement (3) above must hold (this is folklore, and explored in [25]. In fact, if P is pointed, then for every vertex of P, we have a stronger property known as *local strong unimodularity* [15].) It was a widely known fact that the converse is not true. Theorem 1.4 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 [13, 16]. We shall strengthen this result:

Theorem 1.5 (proved in §5)**.** *If $Ax \leq b$ is totally dual p- and q-adic, for distinct primes p, q, then $\{x : Ax \leq b\}$ is an integral polyhedron.*

In the context of set packing systems, Fulkerson's theorem that every integral set packing system is TDI, can be seen as a (stronger) converse to Theorem 1.5 [14]. For set covering systems, there is a related conjecture originally due to Paul Seymour, which may be viewed as some sort of a converse of Theorem 1.5.

Conjecture 1.6 (The Dyadic Conjecture [24], §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. Similar settings to the one below have been studied previously; see for example [19, 5] (the last reference has more relevant citations).

Theorem 1.7. *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.*

Proof. Choose an integral w such that $\min\{b^\top y : A^\top y = w, y \geq \mathbf{0}\}$ has an optimal solution. Let $y^\star$ be a basic optimal solution. We claim that $y^\star$ is p-adic, thereby finishing the proof. Let $I := \{i \in [m] : y^\star_i > 0\}$. Then A_I, the row submatrix of A corresponding to the indices in I, has full row rank. In particular, $y^\star_I$ is the unique solution to $A_I^\top z = w$. By moving to a square row submatrix B of $A_I^\top$ of full rank, and the corresponding subvector w_B of w, we see that $y^\star_I$ is the unique solution to $Bz = w_B$. Since B is nonsingular, $\det(B) \in \{\pm p^k : k \in \mathbb{Z}_+\}$, so by Cramer's rule $y^\star_I$, and therefore $y^\star$, is p-adic. □

For example, 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 [32].

Moving to 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 $J \subseteq E$ with the property that the odd-degree vertices of the graph induced by the edges in 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 [9], Chapter 5). As a consequence of a recent result [3], we shall obtain the following.

Theorem 1.8 (proved in §6)**.** *Let $G = (V, E)$ be a graph, and $T \subseteq V$ a nonempty subset of even cardinality. Then the linear system $x(J) \geq 1 \; \forall \, T$-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 be non-dyadic, as we note in §6, thereby creating an interesting contrast between the proofs of Theorem 1.7 and Theorem 1.8. The system in Theorem 1.8 defines an integral set covering polyhedron (see [11], Chapter 2), so Theorem 1.8 verifies Conjecture 1.6 for such instances. In fact, it has been conjectured that the system in Theorem 1.8 is totally dual *quarter-integral* ([11], 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 [17] for an excellent survey on lattice and conic characterizations of these two sets. We shall prove the following:

Theorem 1.9 (proved in §6)**.** *Let $G = (V, E)$ be a graph. Then $\mathbf{C}(G)$ is a DGSC.*

If G is bridgeless, then the *Cycle Double Cover Conjecture* [30, 27] predicts that $\mathbf{1}$ can be written as a *half-integral* conic combination of the vectors in $\mathbf{C}(G)$. It is straightforward to verify that $\mathbf{1}$ can be written as a conic combination of the vectors in $\mathbf{C}(G)$. Theorem 1.9 then implies that this can be done *dyadically*. Bermond et al. [6] proved in fact, using graph techniques, that $\frac{1}{4}$ fractions suffice.

Theorem 1.10 (proved in §6)**.** *Let $G = (V, E)$ be a graph with $|V|$ even. Then $\mathbf{M}(G)$ is a DGSC.*

G is an *r-graph* if G is r-regular, has an even number of vertices, and every cut with an odd number of vertices on each shore, contains at least r edges. If G is an *r-graph*, then the *Generalized Berge-Fulkerson Conjecture* [26] predicts that $\mathbf{1}$ can be written as a *half-integral* conic combination of $\mathbf{M}(G)$. By leveraging Theorem 1.10 one can show that this can be done *dyadically*.

In §6, we see that the preceding three theorems do *not* extend to the p-adic setting for $p \geq 3$, further emphazing the importance of the dyadic setting.

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

Lemma 2.2 (Density Lemma)**.** *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$. 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. Suppose $\{x : Ax = b\}$ contains a p-adic point, say $\hat{x}$. Since A has integral entries, its kernel has an integral basis, say $d^1, \ldots, d^r$. 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 2.1, 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 first part of the lemma.

Consider now a nonempty rational polyhedron P. Then $P = \{x : Ax \leq b\}$ for some integer A and b. Its affine hull $\mathrm{aff}(P) = \{x : A'x = b'\}$ where $A'x \leq b'$ is a subsystem of $Ax \leq b$. Since $P \neq \emptyset$ there exists $\bar{x}$ in the relative interior of P. Hence, for some $\epsilon > 0$ there exists a ball B of radius ϵ centred at $\bar{x}$ for which $B \cap \mathrm{aff}(P) \subseteq P$. By density of $\mathrm{aff}(P)$ there exists a p-adic point in $B \cap \mathrm{aff}(P)$ as required. □

A natural follow-up question arises: When does a rational affine space 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 ([8], Section 1.5.2) or ([23], Chapter 4) for more details.

Lemma 2.3 (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 square 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

$$\{z : AUz = b\} = \left\{z : (B\ \mathbf{0}) \begin{pmatrix} z_I \\ z_J \end{pmatrix} = b\right\} = \{z : Bz_I = b, z_J \text{ free}\} = \left\{z : z_I = B^{-1}b, z_J \text{ free}\right\}.$$

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 in particular $y^\top A$, is integral. □

The reader may notice the similarity between Lemma 2.3 and its integer analogue, which characterizes when a linear system of equations admits an integral solution, commonly known as the *Integer Farkas Lemma* (see [8], Theorem 1.20). We refrain from calling Lemma 2.3 the "p-adic Farkas Lemma" as we reserve that title for Corollary 2.6 below.

Remark 2.4. *If t is a p- and q-adic rational, for distinct primes p, q, then t is integral.*

Corollary 2.5. *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 2.4. 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 the Farkas Lemma in Linear Programming.

Corollary 2.6 (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 $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ 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.

Lemma 3.1. *Let $A \in \mathbb{Z}^{m\times n}$, and let U be 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.

Proof. **(1)** It suffices to prove ($\Rightarrow$), since U^{-1} is also unimodular. Pick $b \in \mathbb{Z}^m$ such that $(UA)x = b$ has a solution $\bar{x}$; we need to show that the system has a p-adic solution. Note that $A\bar{x} = U^{-1}b \in \mathbb{Z}^m$, so by assumption, there exists a p-adic $x^\star$ such that $Ax^\star = U^{-1}b$. Left-multiplying by U, we get that $(UA)x^\star = b$, so $x^\star$ is the desired p-adic solution. **(2)** Once again, it suffices to prove ($\Rightarrow$). Pick $b \in \mathbb{Z}^m$ such that $(AU)z = b$ has a solution $\bar{z}$; we need to show that the system has a p-adic solution. Note that $Ax = b$ has a solution, namely $U\bar{z}$, so by assumption there exists a p-adic $x^\star$ such that $Ax^\star = b$. Let $z^\star = U^{-1}x^\star$, which is also p-adic. Then $(AU)z^\star = Ax^\star = b$, so $z^\star$ is the desired p-adic solution. □

In order to prove Theorem 1.3, 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 $\delta_1, \ldots, \delta_r \geq 1$ such that $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_r$ (see [23], Section 4.4). It can be readily checked that for each $i \in [r]$, $\prod_{j=1}^{i} \delta_j$ is the GCD of the subdeterminants of A of order i (see for instance, the survey paper [28], in particular, Theorem 2.4). The δ_i's are referred to as the *elementary divisors*. The Smith normal form of an integral matrix, and therefore its elementary divisors, can be computed in polynomial time [18].

Proof of Theorem 1.3. **(1) $\Leftrightarrow$ (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) $\Leftrightarrow$ (3) holds by applying the established equivalence (1) $\Leftrightarrow$ (3) to $A^\top$.

(1) $\Leftrightarrow$ (4): By Lemma 3.1, the condition (1) is preserved under elementary unimodular row/column operations; these operations clearly preserve (4) as well. Thus, it suffices to prove the equivalence between (1) 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 $\delta_1, \ldots, \delta_r \geq 1$ such that $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_r$. Suppose (1) holds. 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) $\Leftrightarrow$ (5) is rather immediate; the only additional remark is that every divisor of a power of p is also a power of p.

(6) $\Rightarrow$ (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) $\Rightarrow$ (6) Choose unimodular matrices U, W such that UAW is in Smith normal form with elementary divisors $\delta_1, \ldots, \delta_r$. Let B' be the $n \times m$ matrix with a leading diagonal matrix $D^{-1} = \mathrm{Diag}(\frac{1}{\delta_1}, \ldots, \frac{1}{\delta_r})$, and zeros everywhere else. Let $B := WB'U$, 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, $UABAW = UAW$ since U and W are invertible square matrices. To this end, we have

$$UABAW = UA(WB'U)AW = (UAW)B'(UAW)$$
$$= \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} D^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} = UAW,$$

where the penultimate equality holds due to the definition of B' and the Smith normal form of UAW.

□

In light of the previous theorem 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?*

Theorem 3.2. *Problem (A) belongs to* P.

Proof. Let A be an integral matrix. By Theorem 1.3, A forms a p-GSS if, and only if, each elementary divisor of A is a power of p. Since the elementary divisors of A can be found in polynomial time, the theorem follows. □

Recall that a set of vectors $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ 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 3.3. *If $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ 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 $a^1, \ldots, a^n$. 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. $\square$

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 $\{4, \ldots, p^k\}$ such that $m - 1$ is not a power of p. Consider the matrix

$$A := \left(J_n - I_n \;\middle|\; \begin{array}{c} J_m - I_m \\ \hline \mathbf{0} \end{array} \right)$$

where J_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 $|\det(J_n - I_n)| = n - 1 = p^k$, 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 1.3. 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.[1]

However, we do have the following sort of converse.

Remark 3.4. *If $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ is a p-GSS, then $\{\pm a^1, \ldots, \pm a^n\}$ is a p-GSC.*

Next we show that p-GSC are closed under taking faces.

Proposition 3.5. *Let $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ 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 $\{a^1, \ldots, a^n\}$. 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. $\square$

[1] Smaller counterexamples exist; for instance, the vectors $(0,1,1,1,1), (1,0,1,1,1), (1,1,0,1,1), (1,1,1,0,1)$, $(1,1,1,1,0), (3,0,1,1,1)$ form a DGSS but not a DGSC.

Proof of Theorem 1.2. ($\Rightarrow$) follows from Proposition 3.5 and Proposition 3.3. ($\Leftarrow$) 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 (Lemma 2.2), 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 $\mathring{y} > \mathbf{0}$ (meaning all entries are positive), 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 3.6. *Problem (B) belongs to co-NP.*

Proof. Suppose a set of integral vectors $\{a^1, \ldots, a^n\}$, whose conic hull is denoted C, is not a p-GSC. By Theorem 1.2, there exists a face $F = C \cap \{x : a^\top x \geq 0\}$ such that $S := F \cap \{a^1, \ldots, a^n\}$ does not form a p-GSS. The subset S, along with the face provided by its supporting hyperplane $a^\top x \geq 0$, can be provided as a certificate that $\{a^1, \ldots, a^n\}$ is not a p-GSC. Testing that S is not a p-GSS can be done in polynomial time by Theorem 3.2, so the result follows. □

4 Totally dual p-adic systems

Given integral A, b, recall that $Ax \leq b$ is totally dual p-adic if for every integral w for which $\min\{b^\top y : A^\top y = w, y \geq \mathbf{0}\}$ 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, $Ax \leq \mathbf{0}$ is totally dual p-adic.

Proof of Theorem 1.1. Consider the following pair of dual linear programs, for w later specified.

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

For every nonempty 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) $\Rightarrow$ **(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 $Ax \leq b$ is totally dual p-adic, (D) has a p-adic optimal solution, say $\bar{y} \geq \mathbf{0}$. 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)** $\Rightarrow$ **(3)** follows from Proposition 3.3. **(3)** $\Rightarrow$ **(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 $Q := \{y : A^\top y = w, y \geq \mathbf{0}, y_{\bar{F}} = \mathbf{0}\}$. 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 1.1 with $b = \mathbf{0}$, we obtain another proof of Theorem 1.2. Moving on, consider the following complexity problem:

(C) *Given a system $Ax \leq b$ where A, b are integral, is the system totally dual p-adic?*

Theorem 4.1. *Problem (C) belongs to co-NP.*

Proof. Suppose $Ax \leq b$ is not totally dual p-adic for some integral A, b. Let $P := \{x : Ax \leq b\}$. By Theorem 1.1, there exists a nonempty face $F := P \cap \{x : a^\top x \leq \beta\}$ of P such that the rows of A_F do not form a p-GSS. The rows A_F, along with the face provided by the supporting hyperplane $a^\top x \leq \beta$, can be given as a certificate that $Ax \leq b$ is not totally dual p-adic. Testing that the rows of A_F do not form a p-GSS can be done in polynomial time by Theorem 3.2, so the result follows. □

5 p-adic polyhedra

A nonempty rational polyhedron is *p-adic* if every nonempty face contains a p-adic point. In this section we provide a characterization of p-adic polyhedra.

Remark 5.1. *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 5.2. *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 a prime p:*

(1) P is a p-adic polyhedron,

(2) for every nonempty face F of P, $\mathrm{aff}(F)$ 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 optimal solution,

(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 [8], Theorem 4.1), namely the novelty of statements (2) and (3), which are ultimately due to Strict Complementarity and the Density Lemma.

Proof. **(1)** $\Rightarrow$ **(2)** follows immediately from definition. **(2)** $\Rightarrow$ **(1)** By the Density Lemma, every nonempty face contains a p-adic point, so P is a p-adic polyhedron. **(2)** $\Leftrightarrow$ **(3)** follows from the Theorem of the Alternative. **(1)** $\Rightarrow$ **(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)** $\Rightarrow$ **(5)** If x is a p-adic vector, and w an integral vector, then $w^\top x$ is a p-adic rational.

(5) $\Rightarrow$ **(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 5.1, we may assume that $z \geq \mathbf{0}$. Consider the following pair of dual linear programs:

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

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 5.3. *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 5.2 (5) $\Rightarrow$ (1) and LP duality. □

Proof of Theorem 1.5. By Corollary 5.3, $P := \{x : Ax \leq b\}$ is a p- and q-adic polyhedron, that is, every minimal nonempty face of P contains a p-adic point and a q-adic point. Each minimal nonempty face of P is an affine subspace, so by Corollary 2.5, it contains an integral point. Thus, every minimal nonempty face of P contains an integral point, so P is an integral polyhedron. □

6 T-joins, circuits, 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 of edges that induces a subgraph whose set of odd degree vertices is precisely T. It can be readily checked that every T-cut and T-join intersect (see [11], Chapter 2). The following result was recently proved:

Theorem 6.1 ([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 6.1 uses the Density Lemma, the Theorem of the Alternative, and a result of Lovász on the *matching lattice* [20].

Proof of Theorem 1.8. 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, in particular, $w \geq \mathbf{0}$. 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 6.1, 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 $\sum(\bar{y}_J : J \text{ a } T\text{-join of } G' \text{ containing } e) \leq 1 \; \forall e \in E(G')$. 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. □

Given the proof of Theorem 1.7, a natural attempt to prove Theorem 1.8 is to prove that every basic optimal solution of $\max\{\mathbf{1}^\top y : A^\top y \leq w, y \geq \mathbf{0}\}$ is dyadic. However, this is not necessarily true if $G = (V, E)$ is a *snark*, $T = V$, and $w = \mathbf{1}$. In fact, as was shown by Palion [21], for the majority of snarks on up to 40 vertices, an off-the-shelf LP solver finds a basic optimal solution that is not dyadic. For example, if G is the first *Blanuša* snark with HoG graph ID 2760 [7], which has 18 vertices, the linear program has a basic optimal solution that assigns $\frac{1}{3}$ to some seven perfect matchings, and $\frac{2}{3}$ to some other perfect matching.

Theorem 1.8 does not extend to the p-adic setting for any prime $p \geq 3$. To see this, consider the graph G with vertices $1, 2, 3, 4, 5$ and edges $13, 14, 15, 23, 24, 25$, let $T := \{1, 3, 4, 5\}$ and let $w := \mathbf{1}$. Note that the T-joins are $\{13, 14, 15\}$, $\{13, 24, 25\}$, $\{14, 23, 25\}$, and $\{15, 23, 24\}$. Then the linear program $\max\{\mathbf{1}^\top y : A^\top y \leq w, y \geq \mathbf{0}\}$ has a unique optimal solution, which assigns $\frac{1}{2}$ to each of the T-joins. In particular, there is no p-adic optimal solution for any $p \geq 3$.

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 $\{\chi_M : M \text{ a perfect matching of } G\}$, is a DGSC.

Proof of Theorem 1.10. 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 1.8, 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 1.1 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 1.3, and so they do not form a p-GSC by Proposition 3.3. Thus, Theorem 1.10 does not extend to the p-adic setting for $p \geq 3$.

Let $G = (V, E)$ be a graph. Recall that a cycle is a subset $C \subseteq E$ such that every vertex in V is incident with an even number of edges in C. In particular, $\emptyset$ is a cycle. Define $\mathbf{C}'(G) := \{\chi_C : C \text{ a cycle of } G\}$. We shall prove that this set is a DGSC. First, we need to prove the following:

Lemma 6.2. *Let $G = (V, E)$ be a graph. Consider edge variables $x, z \in \mathbb{R}^E$. Then the linear system $x(C) + z(E \setminus C) \geq 1 \; \forall$ cycles $C; x \geq \mathbf{0}; z \geq \mathbf{0}$ is TDD.*

Proof. Let H be the graph obtained from G by replacing every edge e by a pair of series edges $e, \hat{e}$. For a subset $S \subseteq E$ we write $\hat{S}$ for $\{\hat{e} : e \in S\}$. Observe that H has edge set $E \cup \hat{E}$. Pick $T \subseteq V(H)$ so that $\hat{E}$ is a T-join of H (i.e. T is the set of odd degree vertices of the subgraph of H induced by $\hat{E}$). Define a function $f : 2^E \to 2^{E \cup \hat{E}}$ where $f(C) := C \cup \widehat{E \setminus C}$. Then f induces a bijection between the cycles of G and the T-joins of H. To see this, observe that C is a cycle of G if and only if $C \cup \hat{C}$ is a cycle in H. Moreover, the symmetric difference $\hat{E} \triangle (C \cup \hat{C})$ is a T-join of H if and only if $C \cup \hat{C}$ is a cycle in H. As $\hat{E} \triangle (C \cup \hat{C}) = C \cup \widehat{E \setminus C}$ the claim about bijection follows. Subsequently, $y(J) \geq 1 \; \forall \, T$-joins J of $H; y \geq \mathbf{0}$ is just a relabeling of $x(C) + z(E \setminus C) \geq 1 \; \forall$ cycles C of $G; x \geq \mathbf{0}; z \geq \mathbf{0}$. Since the first system is TDD by Theorem 1.8, the second system is also TDD. □

Lemma 6.2 above takes advantage of the fact that the *cuboid* of the cycle space of a graph is isomorphic to the clutter of T-joins of another graph [2].

Lemma 6.3. *Let $G = (V, E)$ be a graph. Then $\mathbf{C}'(G)$ is a DGSC.*

Proof. Let M be the coefficient matrix of the linear system $x(C) + z(E \setminus C) \geq 1 \; \forall$ cycles C from Lemma 6.2. Note that M is a $0, 1$ matrix with exactly $|E|$ 1s per row. Let A be the column submatrix corresponding to the x variables; observe that $J - A$ is the column submatrix corresponding to the z variables, where J denotes the all-ones matrix. By Lemma 6.2, $Ax + (J - A)z \geq \mathbf{1}; x \geq \mathbf{0}; z \geq \mathbf{0}$ is TDD. Let P be the corresponding polyhedron, and F the minimal face containing the point $\frac{1}{|E|} \cdot \mathbf{1}$. The tight constraints of F are precisely $Ax + (J - A)z \geq \mathbf{1}$, so by Theorem 1.1 for $p = 2$, the rows of $(A \mid J - A)$ form a DGSC.

To finish the proof, we need to show that the rows of A, which are precisely the elements of $\mathbf{C}'(G)$, form a DGSC. To this end, let w be an integral vector in the conic hull of the rows of A. We need to show that w can be expressed as a dyadic conic combination of the rows of A. There exists a $\bar{y} \geq 0$ such that $\bar{y}^\top A = w^\top$. Since A has a zero row, we may assume that $\mathbf{1}^\top \bar{y}$ is an integer. Subsequently, $\bar{y}^\top (A \mid J - A) = (w^\top \mid (\mathbf{1}^\top \bar{y}) \cdot \mathbf{1}^\top - w^\top)$ is an integral vector, so because the rows of $(A \mid J - A)$ form a DGSC, there exists a dyadic $y' \geq \mathbf{0}$ such that $\bar{y}^\top (A \mid J - A) = y'^\top (A \mid J - A)$. In particular, $y'^\top A = w^\top$, so w is a dyadic conic combination of the rows of A, as needed. □

Recall that a circuit is a nonempty cycle that does not contain another nonempty cycle. Recall that $\mathbf{C}(G) = \{\chi_C : C \text{ a circuit of } G\}$.

Proof of Theorem 1.9. Observe that every nonempty cycle is the disjoint union of some circuits. Thus, since $\mathbf{C}'(G)$ is a DGSC by Lemma 6.3, we obtain immediately that $\mathbf{C}(G)$ is a DGSC. □

Let H be the graph on two vertices with three parallel edges. Then $\mathbf{1} \in \mathrm{cone}(\mathbf{C}(H))$. In fact, $\mathbf{1}$ can be written as a unique conic combination of the vectors in $\mathbf{C}(H)$, in which every vector is assigned a coefficient of $\frac{1}{2}$. Consequently, for any prime $p \geq 3$, the vectors in $\mathbf{C}(H)$ do not form a p-GSC, so Theorem 1.9 does not extend to the p-adic setting.

Finally, let us contrast Theorem 1.9 with another result. Our result implies that every integral vector in $\mathrm{cone}(\mathbf{C}(G))$ can be expressed as a dyadic conic combination of the vectors in $\mathbf{C}(G)$. A very interesting result of Alspach, Goddyn, and Zhang [4] states that a graph has the so-called *circuit cover*

property if, and only if, it has no Petersen minor. What this implies is that if G has no Petersen minor, then every integral vector in $\mathrm{cone}(\mathbf{C}(G))$ can be expressed as a half-integral linear combination of the vectors in $\mathbf{C}(G)$. Thus, in the absence of a Petersen minor, they can drastically improve from dyadic to half-integral coefficients, though at the expense of dropping their nonnegativity.

7 Differing definitions of Hilbert bases

We mentioned that the notion of a DGSC is the dyadic analogue of a Hilbert basis. To elaborate, a set $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ is an *integral generating set for a cone (IGSC)*, or a *Hilbert basis*, if every integral vector in the conic hull can be expressed as an integral conic combination of the vectors.

Our definition of Hilbert basis follows the convention implied in the original paper [16] and explicitly stated in [23], §22.3. However, some other sources including [17] and [24], §5.18, define it in a more relaxed way, as follows.

We call $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ a *relaxed IGSC* if every integral vector in the conic hull can either be expressed as an integral conic combination of the vectors, or cannot be expressed as an integral linear combination of the vectors at all. That is, the notion requires that every integral vector that belongs to the conic hull *and* the integer hull (i.e. the lattice generated by integral linear combinations of the vectors) can be expressed as an integral conic combination of the vectors.

While it is clear that every IGSC is also a relaxed IGSC, the converse is not necessarily true.

For example, the set $\{(1,1,0),(1,0,1),(0,1,1)\}$ of row vectors does not form an IGSC, because $(1,1,1)$ which is in the conic hull cannot be expressed an an integral conic combination of the vectors. Note, however, that $(1,1,1)$ does not belong to the integer lattice at all. Indeed, the set forms a relaxed IGSC. This can be proved by noticing, for instance, that the three vectors are linearly independent, so every vector in $\mathbb{R}^3$ can be expressed in a unique way as a linear combination of the vectors.

A second example comes from the Petersen graph. It was noted in [17] that the set $\mathbf{M}(P_{10})$ of incidence vectors of the perfect matchings of the Petersen graph forms a relaxed IGSC. However, as we noted in §6, $\mathbf{M}(P_{10})$ does not even form a p-GSC for any prime $p \geq 3$, let alone an IGSC. (Indeed, an IGSC is a p-GSC for any prime $p \geq 2$.)

We call $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ an *integral generating set for a subspace (IGSS)* if every integral vector in the linear hull can be expressed as an integral linear combination of the vectors. Observe that if $\{a^1, \ldots, a^n\}$ is an IGSS, then it is a relaxed IGSC if and only if it is an IGSC. In addition, by an argument similar to Proposition 3.3, it can be shown that an IGSC is necessarily an IGSS. Thus,

Theorem 7.1. *$\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ is an IGSC if, and only if, it is a relaxed IGSC and an IGSS.*

Let A be the matrix whose columns are $a^1, \ldots, a^n$. An argument similar to Theorem 1.3 tells us that $\{a^1, \ldots, a^n\}$ is an IGSS if, and only if, the elementary divisors of A are equal to 1. Thus, we understand the IGSS property well. The theorem above then pushes the study of the IGSC property to the relaxed IGSC property. The observations above seem to be a key reason for the indifference in the literature between the two notions of Hilbert bases. However, one has to take caution when it comes to examples. Arguably, IGSC examples are richer and more interesting than relaxed IGSC examples.

Finally, for every prime p, we call $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ a *relaxed p-GSC* if every integral vector in the conic hull can either be expressed as a p-adic conic combination of the vectors, or cannot be expressed as a p-adic linear combination of the vectors at all. We have a p-adic analogue of Theorem 7.1.

Theorem 7.2. *Let p be a prime. Then, $\{a^1, \ldots, a^n\} \subseteq \mathbb{Z}^m$ is a p-GSC if, and only if, it is a relaxed p-GSC and a p-GSS.*

Acknowledgement

We would like to thank the referees whose comments on an earlier draft improved the final presentation. Gérard Cornuéjols was supported by ONR grant N00014-22-1-2528. Bertrand Guenin was supported by Discovery Grants from NSERC and ONR grant N00014-18-1-2078. Levent Tunçel was supported by Discovery Grants from NSERC and ONR grant N00014-18-1-2078.

References

[1] A. Abdi, G. Cornuéjols, B. Guenin, and L. Tunçel. Clean clutters and dyadic fractional packings. *SIAM J. Discret. Math.*, 36(2):1012–1037, 2022.

[2] A. Abdi, G. Cornuéjols, N. Guričanová, and D. Lee. Cuboids, a class of clutters. *Journal of Combinatorial Theory, Series B*, 142:144–209, 2020.

[3] A. Abdi, G. Cornuéjols, and Z. Palion. On dyadic fractional packings of T-joins. *SIAM J. Discret. Math.*, 36(3):2445–2451, 2022.

[4] B. Alspach, L. Goddyn, and C. Zhang. Graphs with the circuit cover property. *Transactions of the American Mathematical Society*, 344(1):131–154, 1994.

[5] G. Appa and B. Kotnyek. Rational and integral k-regular matrices. *Discrete Math.*, 275:1–15, 2004.

[6] J. C. Bermond, B. Jackson, and F. Jaeger. Shortest coverings of graphs with cycles. *Journal of Combinatorial Theory, Series B*, 35(3):297–308, 1983.

[7] G. Brinkmann, K. Coolsaet, J. Goedgebeur, and H. Mélot. House of graphs: a database of interesting graphs. *Discrete Applied Maathematics*, 161(1-2):311–314, 2013.

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

[9] W. Cook, W. Cunningham, W. R. Pulleyblank, and A. Schrijver. *Combinatorial Optimization*. John Wiley and Sons, Inc., 1998.

[10] W. Cook, T. Koch, D. Steffy, and K. Wolter. An exact rational mixed-integer programming solver. In O. Günlük and G. Woeginger, editors, *Integer Programming and Combinatorial Optimization (IPCO 2011), Lecture Notes in Computer Science*, volume 6655, pages 104–116. Springer, Berlin, Heidelberg, 2011.

[11] G. Cornuéjols. *Combinatorial Optimization: Packing and Covering*, volume 74. SIAM, 2001.

[12] G. Ding, L. Feng, and W. Zang. The complexity of recognizing linear systems with certain integrality properties. *Math. Program.*, 114:321–334, 2008.

[13] J. Edmonds and R. Giles. A min-max relation for submodular functions on graphs. In *Studies in integer programming (Proc. Workshop, Bonn, 1975)*, pages 185–204. Ann. of Discrete Math., Vol. 1, 1977.

[14] D. Fulkerson. Blocking and anti-blocking pairs of polyhedra. *Math. Program.*, 1:168–194, 1971.

[15] B. Gerards and A. Sebő. Total dual integrality implies local strong unimodularity. *Math. Program.*, 38:69–73, 1987.

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

[17] L. Goddyn. Cones, lattices, and Hilbert bases of circuits and perfect matchings. In *Contemporary Mathematics*, volume 147, pages 419–439. Amer. Math. Soc., 1993.

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

[19] J. Lee. Subspaces with well-scaled frames. *Linear Algebra Appl.*, 114/115:21–56, 1989.

[20] L. Lovász. Matching structure and the matching lattice. *Journal of Combinatorial Theory, Series B*, 43(2):187 – 222, 1987.

[21] Z. Palion. On dyadic fractional packings of T-joins. Undergraduate thesis, London School of Economics and Political Science, April 2021.

[22] J. Pap. Recognizing conic TDI systems is hard. *Math. Program., Ser. A*, 128:43–48, 2011.

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

[24] A. Schrijver. *Combinatorial Optimization. Polyhedra and Efficiency.* Springer, Berlin, Heidelberg, 2003.

[25] 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.

[26] P. D. Seymour. On multi-colourings of cubic graphs, and conjectures of Fulkerson and Tutte. *Proceedings of the London Mathematical Society*, 38(3):423–460, 05 1979.

[27] P. D. Seymour. Matroids and multicommodity flows. *Europ. J. Combinatorics*, 2:257–290, 1981.

[28] R. P. Stanley. Smith normal form in combinatorics. *J. Combin. Theory Ser. A*, 144:476–495, 2016.

[29] D. E. Steffy. *Topics in Exact Precision Mathematical Programming*. PhD thesis, Georgia Institute of Technology, 2011.

[30] G. Szekeres. Polyhedral decomposition of cubic graphs. *Bull. Austral. Math. Soc.*, 8:367–387, 1973.

[31] H. Wei. *Numerical Stability in Linear Programming and Semidefinite Programming*. PhD thesis, University of Waterloo, 2006.

[32] G. Whittle. A characterization of the matroids representable over GF(3) and the rationals. *Journal of Combinatorial Theory, Series B*, 65:222–261, 1995.