

# Advances on Strictly $\Delta$ -Modular IPs\*

Martin Nägele<sup>†</sup>    Christian Nöbel<sup>‡</sup>    Richard Santiago<sup>‡</sup>    Rico Zenklusen<sup>‡</sup>

## Abstract

There has been significant work recently on integer programs (IPs)  $\min\{c^\top x : Ax \leq b, x \in \mathbb{Z}^n\}$  with a constraint matrix  $A$  with bounded subdeterminants. This is motivated by a well-known conjecture claiming that, for any constant  $\Delta \in \mathbb{Z}_{>0}$ ,  $\Delta$ -modular IPs are efficiently solvable, which are IPs where the constraint matrix  $A \in \mathbb{Z}^{m \times n}$  has full column rank and all  $n \times n$  minors of  $A$  are within  $\{-\Delta, \dots, \Delta\}$ . Previous progress on this question, in particular for  $\Delta = 2$ , relies on algorithms that solve an important special case, namely *strictly  $\Delta$ -modular IPs*, which further restrict the  $n \times n$  minors of  $A$  to be within  $\{-\Delta, 0, \Delta\}$ . Even for  $\Delta = 2$ , such problems include well-known combinatorial optimization problems like the minimum odd/even cut problem. The conjecture remains open even for strictly  $\Delta$ -modular IPs. Prior advances were restricted to prime  $\Delta$ , which allows for employing strong number-theoretic results.

In this work, we make first progress beyond the prime case by presenting techniques not relying on such strong number-theoretic prime results. In particular, our approach implies that there is a randomized algorithm to check feasibility of strictly  $\Delta$ -modular IPs in strongly polynomial time if  $\Delta \leq 4$ .

---

\*Funded through the Swiss National Science Foundation grants 200021\_184622 and P500PT\_206742, the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 817750), and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXZ-2047/1 – 390685813.

<sup>†</sup>Research Institute for Discrete Mathematics and Hausdorff Center for Mathematics, University of Bonn, Bonn, Germany. Email: [mnaegele@uni-bonn.de](mailto:mnaegele@uni-bonn.de).

<sup>‡</sup>Department of Mathematics, ETH Zurich, Zurich, Switzerland. Email: {[cnoebel](mailto:cnoebel), [rtorres](mailto:rtorres), [ricoz](mailto:ricoz)}@ethz.ch.

# 1 Introduction

Integer Programs (IPs)  $\min\{c^\top x: Ax \leq b, x \in \mathbb{Z}^n\}$  are a central NP-hard problem class in Combinatorial Optimization. There is substantial prior work and interest in identifying special classes of polynomial-time solvable IPs while remaining as general as possible. One of the best-known such classes are IPs with a constraint matrix that is *totally unimodular* (TU), i.e., the determinant of any of its square submatrices is within  $\{-1, 0, 1\}$ . A long-standing open conjecture in the field is whether this result can be generalized to  $\Delta$ -modular constraint matrices for constant  $\Delta$ . Here, we say that a matrix  $A \in \mathbb{Z}^{k \times n}$  is  $\Delta$ -*modular* if it has full column rank and all  $n \times n$  submatrices have determinants in  $\{-\Delta, \dots, \Delta\}$ .<sup>1</sup> For brevity, we call an IP with  $\Delta$ -modular constraint matrix a  $\Delta$ -*modular IP*. We recap the above-mentioned conjecture below. Unfortunately, we do not know its precise origin; it may be considered folklore in the field.

**Conjecture 1.** *For constant  $\Delta \in \mathbb{Z}_{\geq 0}$ ,  $\Delta$ -modular IPs can be solved in polynomial time.*

First progress on [Conjecture 1](#) was made by Artmann, Weismantel, and Zenklusen [AWZ17], who showed that it holds for  $\Delta = 2$  (the bimodular case). Fiorini, Joret, Weltge, and Yuditsky [FJWY22] show that the conjecture is true for an arbitrary constant  $\Delta$  under the extra condition that the constraint matrix has at most two non-zero entries per row or column. Through a non-trivial extension of the techniques in [AWZ17], it was shown by Nägele, Santiago, and Zenklusen [NSZ22] that there is a randomized algorithm to check feasibility of an IP with a strictly 3-modular constraint matrix in polynomial time. Here, a matrix  $A \in \mathbb{Z}^{k \times n}$  is called *strictly  $\Delta$ -modular* if it has full column rank and all its  $n \times n$  submatrices have determinants in  $\{-\Delta, 0, \Delta\}$ .

As a key ingredient, all these prior approaches solve certain combinatorial optimization problems with congruency constraints. This is not surprising, as even strictly  $\Delta$ -modular IPs include the following class of *MCCTU problems*:<sup>2</sup>

**Multi-Congruency-Constrained TU Problem (MCCTU):** Let  $T \in \mathbb{Z}^{k \times n}$  be TU,  $b \in \mathbb{Z}^k$ ,  $c \in \mathbb{R}^k$ ,  $m \in \mathbb{Z}_{>0}^q$ ,  $\gamma_i \in \mathbb{Z}^n$  for  $i \in [q]$ ,  $r \in \mathbb{Z}^q$ . Solve

$$\min\{c^\top x: Tx \leq b, \gamma_i^\top x \equiv r_i \pmod{m_i} \forall i \in [q], x \in \mathbb{Z}^n\} .$$

Unless mentioned otherwise, we assume that in the context of [MCCTU](#) problems,  $q$  and  $m_i$  are constant. Even [MCCTU](#) with just a single congruency constraint, i.e.,  $q = 1$ , already contains the classical and well-studied odd and even cut problems, and, more generally, the problem of finding a minimum cut whose number of vertices is  $r \pmod{m}$ . (See [PR82; BC87; GLS84; GR95; NSZ19; NZ20] for related work.) It can also capture the minimum  $T$ -join problem, congruency-constrained flow problems, and many other problems linked to TU matrices.

Combinatorial optimization problems with congruency constraints are highly non-trivial and many open questions remain. As they are already captured by strictly  $\Delta$ -modular IPs, this motivates the following weakening of [Conjecture 1](#).

**Conjecture 2.** *Strictly  $\Delta$ -modular IPs can be solved in polynomial time for constant  $\Delta \in \mathbb{Z}_{\geq 0}$ .*

Even resolving this weaker conjecture would settle several open problems, including congruency-constrained min cuts (in both directed and undirected graphs), or the problem of efficiently and deterministically finding a perfect matching in a red/blue edge-colored bipartite graph such that the number

<sup>1</sup>A weaker variant of the conjecture claims efficient solvability of IPs with *totally  $\Delta$ -modular* constraint matrices, where all subdeterminants are bounded by  $\Delta$  in absolute value. The conjecture involving  $\Delta$ -modular matrices implies the weaker variant. Indeed, an IP  $\min\{c^\top x: Ax \leq b, x \in \mathbb{Z}^n\}$  with a totally  $\Delta$ -modular constraint matrix can be reformulated as  $\min\{c^\top(x^+ - x^-): A(x^+ - x^-) \leq b, x^+, x^- \in \mathbb{Z}_{\geq 0}^n\}$ . It is not hard to see that the constraint matrix of the new LP remains totally  $\Delta$ -modular; moreover, it has full column rank because of the non-negativity constraints.

<sup>2</sup>To capture an [MCCTU](#) problem as a strictly  $\Delta$ -modular IP, replace each congruency constraint  $\gamma_i^\top x \equiv r_i \pmod{m_i}$  by an equality constraint  $\gamma_i^\top x + m_i y_i = r$  with  $y_i \in \mathbb{Z}$ . The corresponding constraint matrix is strictly  $\Delta$ -modular for  $\Delta = \prod_{i=1}^q m_i$ .

of red matching edges is  $r \pmod{m}$ . (This is a simplified version of the famous red-blue matching problem, where the task is to find a perfect matching with a specified number of red edges; for both versions, randomized algorithms are known.) Interestingly, for the bimodular case ( $\Delta = 2$ ), a result by Veselov and Chirkov [VC09] implies that [Conjecture 1](#) and [Conjecture 2](#) are equivalent (see [AWZ17]).

Our goal is to shed further light on [Conjecture 2](#) and overcome some important hurdles of prior approaches. In a first step, we note that a positive resolution of [Conjecture 2](#) does not only imply efficient solvability of MCCTU problems, but also vice versa, and this reduction works in strongly polynomial time.

**Lemma 3.** *Let  $\Delta > 0$ . Every strictly  $\Delta$ -modular IP can, in strongly polynomial time, be reduced to an MCCTU problem with moduli  $m_i$  such that  $\Delta = \prod_{i=1}^q m_i$ .*

Without the strongly polynomial time condition, this also follows from very recent work of Gribanov, Shumilov, Malyshev, and Pardalos [GSMP22, Lemma 4].

Further, we are interested in making progress regarding the feasibility version of [Conjecture 2](#), i.e., efficiently deciding whether a strictly  $\Delta$ -modular IP is feasible. Prior approaches settle this question for  $\Delta = 2$  [AWZ17] and—using a randomized algorithm—for  $\Delta = 3$  [NSZ22]. A main hurdle to extend these is that they crucially rely on  $\Delta$  being prime, for example through the use of the Cauchy-Davenport Theorem. Our main contribution here is to address this. In particular, we can check feasibility for  $\Delta = 4$  with a randomized algorithm, which is the first result in this context for non-prime  $\Delta$ . More importantly, our techniques will hopefully prove useful for future advances on this challenging question.

**Theorem 4.** *There exists a strongly polynomial-time randomized algorithm to find a feasible solution of a strictly 4-modular IP, or detect that it is infeasible.*

We remark that the randomization appearing in the above theorem comes from the fact that one building block of our result is a reduction to a problem class that includes the aforementioned congruency-constrained red/blue-perfect matching problem, for which only randomized approaches are known.

## 1.1 Group-constrained problems and proof strategy for [Theorem 4](#)

To show [Theorem 4](#), we exploit its close connection to MCCTU. Capturing the congruency constraints of an MCCTU problem through an abelian group constraint, we attain the following *group-constrained TU feasibility problem*.

**Group-Constrained TU Feasibility (GCTUF):** Let  $T \in \mathbb{R}^{k \times n}$  be a TU matrix, let  $b \in \mathbb{Z}^k$ , let  $(G, +)$  be a finite abelian group, and let  $\gamma \in G^n$  and  $r \in G$ . The task is to show infeasibility or find a solution of the system

$$Tx \leq b, \gamma^\top x = r, x \in \mathbb{Z}^n .$$

Here, the scalar product  $\gamma^\top x$  denotes the linear combination of the group elements  $\gamma_1, \dots, \gamma_n$  with multiplicities  $x_1, \dots, x_n$  in  $G$ . Group constraints generalize congruency constraints, which are obtained in the special case where  $G$  is cyclic. More generally, by the fundamental theorem of finite abelian groups, a finite abelian group  $G$  is, up to isomorphism, a direct product of cyclic groups. Hence, a group constraint can be interpreted as a set of congruency constraints and vice versa. Thus, [GCTUF](#) and [MCCTU](#) feasibility are two views on the same problem. We stick to [GCTUF](#) mostly for convenience of notation. Moreover, the [GCTUF](#) setting also allows for an elegant use of group-related results later on. One may assume that the group is given through its multiplication table (the *Cayley table*). In fact, the precise group representation is not of great importance to us. Concretely, for constant  $\Delta$ , strictly  $\Delta$ -modular IP feasibility problems reduce to [GCTUF](#) problems with a constant size group. Many of our polynomial-time algorithmic results can even be extended to settings where the group size is not part of the input, and access to group operations is provided through an oracle.

By a slight extension of [Lemma 3](#) (see [Section 2](#)) and the aforementioned equivalent viewpoint of multiple congruency constraints and a group constraint, in order to prove [Theorem 4](#), it is enough for us to show the equivalent statement below.

**Theorem 5.** *There exists a strongly polynomial time randomized algorithm for [GCTUF](#) problems with a group of cardinality at most 4.*

On a high level, we follow a well-known strategy for TU-related problems by employing Seymour’s decomposition [[Sey80](#)] to decompose the problem into problems on simpler, more structured TU matrices. (See, e.g., [[DK14](#); [AWZ17](#); [AF21](#); [NSZ22](#)].) Roughly speaking, Seymour’s decomposition states that a TU matrix is either very structured—in which case we call it a *base block*—or can be decomposed into smaller TU matrices through a small set of well-defined operations. (See the discussion following [Theorem 15](#) for more details.) The use of Seymour’s decomposition typically comes with two main challenges, namely (i) solving the base block cases, and (ii) propagating solutions of the base block cases back through the decomposition efficiently to solve the original problem. First, we show that this propagation can be done efficiently for our problem.

**Theorem 6.** *Let  $G$  be an abelian group of size at most 4. Given an oracle for solving base block [GCTUF](#) problems with group  $G$ , we can solve [GCTUF](#) problems with group  $G$  in strongly polynomial time with strongly polynomially many calls to the oracle.*

In fact, our approach underlying [Theorems 5](#) and [6](#) operates in a hierarchy of [GCTUF](#) problems with increasingly relaxed group constraints of the form  $\gamma^\top x \in R$  for subsets  $R \subseteq G$  of increasing size, and allows for proving the above results for such relaxed [GCTUF](#) problems for arbitrary constant-size groups  $G$  as long as  $|G| - |R| \leq 3$ . (See [Section 4](#) for more details.) In principle, this is along the lines of the approach to congruency-constrained TU problems in [[NSZ22](#)], but incorporates the new viewpoint of group constraints, and additionally improves over earlier results in two ways: First, our approach applies to arbitrary finite abelian groups, while previous setups heavily relied on the group cardinality being a prime. Secondly, in the setting with relaxed group constraints, we extend the admissible range of  $|G| - |R|$  by one, thus proceeding further in the hierarchy of [GCTUF](#) problems, and newly covering [GCTUF](#) problems with groups of cardinality 4.

Besides being a key part of our approach, [Theorem 6](#) underlines that base block [GCTUF](#) problems are not merely special cases, but play a key role in progress on general [GCTUF](#) problems. There are only two non-trivial types of such base block [GCTUF](#) problems, namely when the constraint matrix is a so-called *network matrix* or a transpose thereof. Both cases cover combinatorial problems that are interesting on their own, and their complexity status remains open to date. If the constraint matrix is a network matrix, [GCTUF](#) can be cast as a circulation problem with a group constraint. By reducing to and exploiting results of Camerini, Galbiati, and Maffioli [[CGM92](#)] on exact perfect matching problems, a randomized algorithm for the congruency-constrained case has been presented in [[NSZ22](#)]. We observe that these results extend to the group-constrained setting. The other base block case, where the constraint matrix is the transpose of a network matrix, can be cast as a group-constrained directed minimum cut problem by leveraging a result in [[NSZ22](#)]. Prior work combined this reduction with results on congruency-constrained submodular minimization [[NSZ19](#)] to solve the optimization version of the problem for congruency-constraints of prime power modulus. We show that the feasibility question on this base block can be solved efficiently on any finite abelian group of constant order, thus circumventing the prime power restriction that is intrinsic in prior approaches.

**Theorem 7.** *Let  $G$  be a finite abelian group. There is a strongly polynomial time algorithm for solving [GCTUF](#) problems with group  $G$  where the constraint matrix is the transpose of a network matrix.*

## 1.2 Further related work

The parameter  $\Delta$  has been studied from various viewpoints. While efficient recognition of (totally)  $\Delta$ -modular matrices is open for any  $\Delta \geq 2$ , approaches to approximate the largest subdeterminant in

absolute value were studied [DEFM15; Nik15]. Also, focusing on more restricted subdeterminant patterns proved useful [VC09; AEGOVW16; GSW21]. Aiming at generalizing a bound of Heller [Hel57] for  $\Delta = 1$ , bounds on the maximum number of rows of a  $\Delta$ -modular matrix were obtained [GWZ18; LPSX22; AS22]. Also, the influence of the parameter  $\Delta$  on structure and properties of IPs and polyhedra is multi-faceted (see, e.g., [BDEHN14; EV17; GV16; GZ21; Gri21; LPSX20; PSW22; Tar86] and references therein).

### 1.3 Structure of the paper

We prove the strongly polynomial time reduction from Lemma 3 in Section 2. In Section 3, we prove Theorem 7. Section 4 illustrates our approach and new contributions towards Theorem 6 on a more technical level, and explains the main new ingredients of our proof. Throughout Section 4, we build on several results from [NSZ22] that are proved there for congruency-constrained TU problems, i.e., the case of a cyclic group constraint. In Appendix B, we show how these proofs can be adapted to the group setting.

## 2 Reducing to group-constrained problems

We prove the following slightly strengthened version of Lemma 3.

**Lemma 8.** *Let  $\Delta > 0$ . Given a strictly  $\Delta$ -modular IP of the form  $\min\{c^\top x : Ax \leq b, x \in \mathbb{Z}^n\}$ , one can, in strongly polynomial time, determine an MCCTU problem*

$$\min\{\bar{c}^\top y : Ty \leq b, \gamma_i^\top y \equiv r_i \pmod{m_i} \forall i \in [q], y \in \mathbb{Z}^n\}$$

together with a non-singular  $n \times n$  submatrix  $H$  of  $A$  such that the following holds:

- (i)  $\Delta = \prod_{i \in [q]} m_i$ .
- (ii)  $\bar{c}^\top = c^\top H^{-1}$ .
- (iii) *The map  $x \mapsto Hx$  is a bijection between feasible solutions of the strictly  $\Delta$ -modular IP and the MCCTU problem.*

We remark that the one-to-one correspondence of feasible solutions given in Item (iii) of Lemma 8 is (besides Item (i)) precisely what we need to deduce our main result, Theorem 4, from Theorem 5. Moreover, Items (ii) and (iii) of Lemma 8 together imply that  $x \mapsto Hx$  is not only a bijection between feasible solutions, but also a bijection between optimal solutions of the two involved problems, so Lemma 3 is indeed also implied by Lemma 8.

*Proof of Lemma 8.* We show how to transform the given strictly  $\Delta$ -modular problem into an MCCTU problem. Let  $H$  be an  $n \times n$  submatrix of  $A$  with  $|\det(H)| = \Delta$ . After a variable transformation to  $y = Hx$ , we can equivalently rewrite the original integer program in the form

$$\min\{\bar{c}^\top y : Ty \leq b, H^{-1}y \in \mathbb{Z}^n\} ,$$

where  $\bar{c}^\top = c^\top H^{-1}$ , and  $T = AH^{-1}$ . By definition, the map  $x \mapsto Hx$  is a bijection between feasible solutions of the original IP and the above problem. Note that  $T$  is unimodular and contains an identity submatrix; hence  $T$  is totally unimodular. To complete the proof, it thus suffices to show that the constraint  $H^{-1}y \in \mathbb{Z}^n$  can be transformed to multiple congruency constraints with moduli whose product equals  $\Delta$ .

To this end, we first write  $H^{-1} = H_I + H_F$  with an integer matrix  $H_I \in \mathbb{Z}^{n \times n}$  and a fractional matrix  $H_F \in [0, 1)^{n \times n}$ , i.e., matrices whose entries are given by

$$(H_I)_{i,j} := \lfloor (H^{-1})_{i,j} \rfloor \quad \text{and} \quad (H_F)_{i,j} := (H^{-1})_{i,j} - (H_I)_{i,j} ,$$

where, for  $x \in \mathbb{R}$ ,  $\lfloor x \rfloor$  is the integer part of  $x$ , i.e., the unique number  $n \in \mathbb{Z}$  with  $n \leq x < n+1$ . Using this decomposition, we obtain

$$H^{-1}y \in \mathbb{Z}^n \iff H_I y + H_F y \in \mathbb{Z}^n \iff H_F y \in \mathbb{Z}^n .$$

Because  $\det(H) = \Delta$ , we have  $\Delta H^{-1} \in \mathbb{Z}^{n \times n}$  by Cramer's rule, and thus also  $\tilde{H}_F := \Delta H_F \in \mathbb{Z}^{n \times n}$ . Furthermore, the entries of  $\tilde{H}_F$  are bounded by the constant  $\Delta$  in absolute value. Consequently, using a weakly polynomial time algorithm for computing the Smith normal form of an integer matrix [KB79], we can in strongly polynomial time determine the Smith normal form of  $\tilde{H}_F$ , i.e., we can in strongly polynomial time find unimodular matrices  $S, U \in \mathbb{Z}^{n \times n}$  and integers  $\tilde{m}_i \in \mathbb{Z}$  such that  $D = \text{diag}(\tilde{m}_1, \dots, \tilde{m}_n) = S^{-1} \tilde{H}_F U^{-1}$ . Using this decomposition, we get

$$H_F y \in \mathbb{Z}^n \iff SDU y \in \Delta \mathbb{Z}^n \iff DU y \in \Delta \mathbb{Z}^n .$$

Here, the last equivalence exploits unimodularity of  $S$ . Letting  $\gamma_i^\top$  denote the  $i^{\text{th}}$  row of  $U$ , we can further rewrite

$$DU y \in \Delta \mathbb{Z}^n \iff \forall i \in [n]: \tilde{m}_i \gamma_i^\top y \in \Delta \mathbb{Z}^n \iff \forall i \in [n]: \gamma_i^\top y \equiv 0 \pmod{m_i} ,$$

where we use  $m_i := \Delta / \gcd(\Delta, \tilde{m}_i)$ .<sup>3</sup> It is thus left to show  $\Delta = \prod_{i=1}^n m_i$ . To this end, consider the composed map

$$\Phi: \mathbb{Z}^n \xrightarrow{U} \mathbb{Z}^n \xrightarrow{\pi} \prod_{i=1}^n \mathbb{Z} / m_i \mathbb{Z} ,$$

where, for  $z \in \mathbb{Z}^n$ , the first map is defined by  $z \mapsto Uz$ , and the second is the component-wise projection given by  $\pi(z) := (\pi_1(z_1), \dots, \pi_n(z_n))$ , where  $\pi_i$  denotes the natural projection from  $\mathbb{Z}$  to  $\mathbb{Z}/m_i\mathbb{Z}$ . As  $U$  is unimodular, the first map is an isomorphism of groups. Furthermore,  $\pi$  is a surjective group homomorphism. By the isomorphism theorem, we thus get an isomorphism

$$\prod_{i=1}^n \mathbb{Z} / m_i \mathbb{Z} = \text{im } \Phi \cong \mathbb{Z}^n / \ker \Phi .$$

Note that the cardinality of the left-hand side group is  $\prod_{i=1}^n m_i$ . Therefore, we may finish the proof by showing that  $|\mathbb{Z}^n / \ker \Phi| = \Delta$ . To this end, observe that  $\ker \Phi$  is the set of  $y \in \mathbb{Z}^n$  fulfilling the congruency constraints, i.e.,  $\gamma_i^\top y \equiv 0 \pmod{m_i}$  for all  $i \in [n]$ . By the above discussion, this is precisely the set  $\{y \in \mathbb{Z}^n: H^{-1}y \in \mathbb{Z}^n\} = H\mathbb{Z}^n$ . Consequently,  $|\mathbb{Z}^n / \ker \Phi| = |\mathbb{Z}^n / H\mathbb{Z}^n| = |\det(H)| = \Delta$ , as desired.  $\square$

### 3 GCTUF with transposed network constraint matrices

In the setting with a congruency constraint instead of a group constraint, [NSZ22] shows that every base block problem with a constraint matrix that is a transposed network matrix can be reduced to a node-weighted minimization problem over a lattice with a congruency constraint,<sup>4</sup> i.e., a problem of the form

$$\min\{w(S): S \in \mathcal{L}, \gamma(S) \equiv r \pmod{m}\} , \tag{1}$$

where  $\mathcal{L} \subseteq 2^N$  is a lattice on some finite ground set  $N$ ,  $\gamma: N \rightarrow \mathbb{Z}$ ,  $r \in \mathbb{Z}$ ,  $m \in \mathbb{Z}_{>0}$ ,  $w: N \rightarrow \mathbb{R}$ , and we use  $\gamma(S) := \sum_{v \in S} \gamma(v)$  as well as  $w(S) := \sum_{v \in S} w(v)$ .<sup>5</sup> Being a special case of congruency-constrained submodular minimization, it is known that such problems, and thus the corresponding

<sup>3</sup>Note we might have  $\tilde{m}_i = 0$  for some  $i \in [n]$ . In this case,  $\gcd(\Delta, \tilde{m}_i) = \Delta$  and hence  $m_i = 1$ , so the corresponding congruency constraint is always satisfied.

<sup>4</sup>In fact, the proof in [NSZ22] claims a reduction to a submodular minimization problem, but shows the stronger one presented here.

<sup>5</sup>We recall that a *lattice*  $\mathcal{L} \subseteq 2^N$  is a set family such that for any  $A, B \in \mathcal{L}$ , we have  $A \cap B, A \cup B \in \mathcal{L}$ . We assume such a lattice to be given by a compact encoding in a directed acyclic graph  $H$  on the vertex set  $N$  such that  $X \subseteq N$  is an element of the lattice if and only if  $\delta_H^-(X) = \emptyset$  (cf. [GLS93, Section 10.3]). Here, as usual, in a digraph  $G = (V, A)$  and for  $X \subseteq V$ , we denote by  $\delta^+(X)$  and  $\delta^-(X)$  the arcs in  $A$  leaving and entering  $X$ , respectively. Moreover, we write  $\delta^\pm(v) := \delta^\pm(\{v\})$  for  $v \in V$ .

congruency-constrained TU problems with a transposed network constraint matrix, can be solved in strongly polynomial time for constant prime power moduli  $m$ , while the case of general constant composite moduli remains open [NSZ19]. The progress on GCTUF, particularly the reduction to base block feasibility problems through Theorem 6 and its generalization (Theorem 16 in Section 4), motivates studying these reductions and results in the feasibility setting and with a group constraint instead of a congruency constraint, giving rise to the following problem.

**Group-Constrained Lattice Feasibility (GCLF):** Let  $N$  be a finite set,  $\mathcal{L} \subseteq 2^N$  a lattice,  $(G, +)$  a finite abelian group,  $\gamma: N \rightarrow G$ ,  $r \in G$ . The task is to find  $X \in \mathcal{L}$  with  $\gamma(X) = r$ , or decide infeasibility.

We observe that the reduction in [NSZ22] from congruency-constrained TU problems with transposed network constraint matrices to problems of the form given in (1) extends to the group-constrained case. In particular, we obtain the following result in the feasibility setting. (See Appendix B.2 for some details.)

**Proposition 9.** *Let  $G$  be a finite abelian group. Any GCTUF problem with group  $G$  and a constraint matrix that is a transposed network matrix can in strongly polynomial time be reduced to a GCLF problem with group  $G$ .*

Thus, it remains to study GCLF problems. Interestingly, for the pure feasibility question, we can circumvent the barriers present in the optimization setting, and obtain the following result through a concise argument.

**Theorem 10.** *Let  $G$  be a finite abelian group. GCLF problems with group  $G$  can be solved in strongly polynomial time.*

Clearly, Proposition 9 and Theorem 10 together imply Theorem 7. The main observation towards a proof of Theorem 10 is the following elementary lemma.

**Lemma 11.** *Let  $G$  be a finite abelian group, and let  $\gamma_1, \dots, \gamma_\ell \in G$ . If  $\ell \geq |G|$ , then there is a non-empty subset  $I \subseteq [\ell]$  such that  $\sum_{i \in I} \gamma_i = 0$ .*

*Proof.* Either  $s_i := \sum_{j \leq i} \gamma_j = 0$  for some  $i \in [\ell]$ , or there exist  $i < j$  with  $s_i = s_j$ ; hence  $I = [i]$  or  $I = \{i + 1, \dots, j\}$ , respectively, has the desired properties.  $\square$

To prove Theorem 10, we work with a representation of the lattice  $\mathcal{L}$  through an acyclic digraph  $H$  (see Footnote 5). We exploit that every  $X \in \mathcal{L}$  is uniquely defined by the subset  $C_X := \{x \in X : \delta^+(x) \subseteq \delta^+(X)\}$ .

*Proof of Theorem 10.* We claim that if the given GCLF problem is feasible, there is a feasible  $X$  with  $|C_X| < |G|$ . If so, we obtain an efficient procedure for GCLF with group  $G$  through enumerating all such  $C_X$  and checking if  $\gamma(X) = r$ . To prove the claim, assume for contradiction that it is wrong, and let  $X \in \mathcal{L}$  be minimal with  $\gamma(X) = r$ . Then  $|C_X| \geq |G|$ , and applying Lemma 11 to  $C_X$  gives a non-empty subset  $Y \subseteq C_X$  with  $\gamma(Y) = 0$ . Thus,  $X \setminus Y$  is a strictly smaller lattice element with  $\gamma(X \setminus Y) = \gamma(X) - \gamma(Y) = \gamma(X) = r$ , a contradiction.  $\square$

## 4 Approaching GCTUF problems and a proof of Theorem 6

In order to tackle GCTUF problems, following ideas from [NSZ22], we introduce a hierarchy of slightly relaxed GCTUF problems by weakening the group constraint.

**R-Group-Constrained TU Feasibility (R-GCTUF):** Let  $T \in \{-1, 0, 1\}^{k \times n}$  be TU,  $b \in \mathbb{Z}^k$ , let  $(G, +)$  be a finite abelian group,  $\gamma \in G^n$  and  $R \subseteq G$ . The task is to show infeasibility or find a solution of

$$Tx \leq b, \gamma^\top x \in R, x \in \mathbb{Z}^n .$$

Here, we typically call  $R$  the set of target elements. The above setup allows us to measure progress between GCTUF (the case of  $|R| = 1$ ) and an unconstrained IP with TU constraint matrix (captured by setting  $R = G$ ). In particular, the difficulty of an R-GCTUF problem increases as the size of  $R$ , i.e., the number of target elements, decreases. The main parameter capturing this hardness is the *depth*  $d := |G| - |R|$  of the problem. We show the following generalization of [Theorem 5](#).

**Theorem 12.** *Let  $G$  be a finite abelian group. There is a strongly polynomial randomized algorithm solving R-GCTUF problems with group  $G$  and  $|G| - |R| \leq 3$ .*

Our approach exploits Seymour's decomposition theorem for TU matrices. To state this result, we first introduce the additional notions of a 3-sum of matrices, and pivoting operations.

**Definition 13 (3-sum).** *Let  $A \in \mathbb{Z}^{k_A \times n_A}$ ,  $B \in \mathbb{Z}^{k_B \times n_B}$ ,  $e \in \mathbb{Z}^{k_A}$ ,  $f \in \mathbb{Z}^{n_B}$ ,  $g \in \mathbb{Z}^{k_B}$ ,  $h \in \mathbb{Z}^{n_A}$ . The 3-sum of  $\begin{pmatrix} A & e & e \\ h^\top & 0 & 1 \end{pmatrix}$  and  $\begin{pmatrix} 0 & 1 & f^\top \\ g & g & B \end{pmatrix}$  is  $\begin{pmatrix} A & e & e \\ h^\top & 0 & 1 \end{pmatrix} \oplus_3 \begin{pmatrix} 0 & 1 & f^\top \\ g & g & B \end{pmatrix} := \begin{pmatrix} A & ef^\top \\ gh^\top & B \end{pmatrix}$ .*

**Definition 14 (Pivoting).** *Let  $C \in \mathbb{Z}^{k \times n}$ ,  $p \in \mathbb{Z}^n$ ,  $q \in \mathbb{Z}^k$ , and  $\varepsilon \in \{-1, 1\}$ . The matrix obtained from pivoting on  $\varepsilon$  in  $T := \begin{pmatrix} \varepsilon & p^\top \\ q & C \end{pmatrix}$ , i.e., pivoting on the element  $T_{11}$  of  $T$ , is  $\text{pivot}_{11}(T) := \begin{pmatrix} -\varepsilon & \varepsilon p^\top \\ \varepsilon q & C - \varepsilon q p^\top \end{pmatrix}$ . More generally,  $\text{pivot}_{i,j}(T)$  for indices  $i$  and  $j$  such that  $T_{ij} \in \{-1, 1\}$  is obtained from  $T$  by first permuting rows and columns such that the element  $T_{ij}$  is permuted to the first row and first column, then performing the above pivoting operation on the permuted matrix, and finally reversing the row and column permutations.*

With this notation at hand, we can state Seymour's TU decomposition theorem as follows.

**Theorem 15 (Seymour's TU decomposition).** *Let  $T \in \mathbb{Z}^{k \times n}$  be a totally unimodular matrix. Then, one of the following cases holds.*

- (i)  $T$  or  $T^\top$  is a network matrix.
- (ii)  $T$  is, possibly after iteratively applying the operations of
  - deleting a row or column with at most one non-zero entry,
  - deleting a row or column that appears twice or whose negation also appears in the matrix,
  - and
  - changing the sign of a row or column,

equal to one of

$$\begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ -1 & 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} .$$

- (iii)  $T$  can, possibly after row and column permutations and pivoting once, be decomposed into a 3-sum of totally unimodular matrices with  $n_A, n_B \geq 2$ .

Additionally, we can in time  $\text{poly}(n)$  decide which of the cases holds and determine the involved matrices.

We remark that typically, a 3-sum of the form  $\begin{pmatrix} A & ef^\top \\ gh^\top & B \end{pmatrix}$  would be called a 1- or 2-sum if both or one of the off-diagonal blocks  $ef^\top$  and  $gh^\top$  were zero, respectively. However, as we treat those special cases in the same way as 3-sums, there is no need for us to further distinguish between them. Generally, we refer to matrices covered by [Items \(i\) and \(ii\) of Theorem 15](#) as *base block* matrices. By porting results on congruency-constrained base block problems of [\[NSZ22\]](#) to the group-constrained setting and combining them with our new [Theorem 7](#), it follows that GCTUF problems can be solved in strongly polynomial time if the constraint matrix is a base block matrix. The potential pivoting step in



Item (iii) of Theorem 15 can also be handled by extending a result from [NSZ22] to the group setting. For the sake of completeness, we comment on how to extend the arguments from [NSZ22] for base block constraint matrices or pivot steps in Appendices B and C, respectively. Showing how to deal with  $R$ -GCTUF problems with constraint matrices that are 3-sums will lead to the following generalization of Theorem 6 which, in combination with the aforementioned results on base block problems, immediately implies Theorem 12. We devote the rest of this section to a discussion of its proof.

**Theorem 16.** *Let  $G$  be a finite abelian group and  $\ell \in \mathbb{Z}_{\geq 1}$  with  $\ell \geq |G| - 3$ . Given an oracle for solving base block  $R$ -GCTUF problems with group  $G$  and any  $R \subseteq G$  with  $|R| \geq \ell$ , we can solve  $R$ -GCTUF problems with group  $G$  and  $R \subseteq G$  with  $|R| \geq \ell$  in strongly polynomial time with strongly polynomially many calls to the oracle.*

#### 4.1 Reducing to a simpler problem when the target elements form a union of cosets

If  $R$ , the set of target elements, is a union of cosets of the same non-trivial proper subgroup  $H$  of  $G$  (i.e., it is of the form  $R = \bigcup_{i=1}^k (g_i + H)$  for some  $g_1, \dots, g_k \in G$ , or equivalently,  $R = R + H$ ), we can directly reduce to a simpler problem. We formalize this in the following lemma.

**Lemma 17.** *Assume we are given an  $R$ -GCTUF problem*

$$Tx \leq b, \gamma^\top x \in R, x \in \mathbb{Z}^n$$

*such that  $R = R + H$  for a non-trivial proper subgroup  $H$  of  $G$ . Then, the set of feasible solutions of the given  $R$ -GCTUF problem is invariant under replacing  $G$  by the quotient group  $\hat{G} = G/H$ ,  $R$  by  $\hat{R} = R/H$ , and  $\gamma$  by its image  $\hat{\gamma} \in \hat{G}^n$  under the quotient map.*

*Proof.* Let  $P$  denote the original  $R$ -GCTUF problem, and let  $\hat{P}$  denote the modified one. The inequality system  $Tx \leq b$  is the same in  $P$  and  $\hat{P}$ , hence it is enough to show that  $\gamma^\top x \in R$  if and only if  $\hat{\gamma}^\top x \in \hat{R}$ .

To this end, first note that for  $x \in \mathbb{Z}^n$ ,  $\gamma^\top x \in R$  immediately implies  $\hat{\gamma}^\top x \in \hat{R}$  by definition. For the other direction, assume  $x \in \mathbb{Z}^n$  satisfies  $\hat{\gamma}^\top x \in \hat{R}$ . Then, by definition of  $\hat{\gamma}$  and  $\hat{R}$ , we know that there is an element  $h \in H$  such that  $\gamma^\top x + h \in R$ . Then  $\gamma^\top x \in R - h = R$ , as desired.  $\square$

The depth of the new problem given by Lemma 17 in the corresponding hierarchy is  $\hat{d} = |G/H| - |R/H| = \frac{|G|-|R|}{|H|} < |G| - |R|$ , so we indeed end up with a simpler problem in that respect. Since the existence of such a subgroup  $H$  can be checked efficiently (given that  $G$  has constant size), we can always and in constant time determine upfront whether the  $R$ -GCTUF problem at hand is reducible using Lemma 17, and if so, reduce it to a simpler  $R$ -GCTUF problem. Thus, for the rest of this section, we assume  $R$  is not a union of cosets. This assumption allows us to apply a special case of the Cauchy-Davenport theorem that holds despite the fact that the group order may not be prime. We refer to Lemma 19 for details.

#### 4.2 Decomposing the problem

We now focus on an  $R$ -GCTUF problem with a constraint matrix  $T$  that can be decomposed into a 3-sum of the form  $T = \begin{pmatrix} A & ef^\top \\ gh^\top & B \end{pmatrix}$ . The decomposition allows for splitting  $x$ ,  $b$ , and  $\gamma$  into two parts accordingly, giving the equivalent formulation

$$\begin{pmatrix} A & ef^\top \\ gh^\top & B \end{pmatrix} \cdot \begin{pmatrix} x_A \\ x_B \end{pmatrix} \leq \begin{pmatrix} b_A \\ b_B \end{pmatrix}, \quad \gamma_A^\top x_A + \gamma_B^\top x_B \in R, \quad \begin{matrix} x_A \in \mathbb{Z}^{n_A} \\ x_B \in \mathbb{Z}^{n_B} \end{matrix}. \quad (2)$$

In the inequality system, the variables  $x_A$  and  $x_B$  interact only through the rank-one blocks  $ef^\top$  and  $gh^\top$ . Fixing values of  $\alpha := f^\top x_B$  and  $\beta := h^\top x_A$  allows for rephrasing (2) through the following two

almost independent problems

$$\begin{aligned} Ax_A &\leq b_A - \alpha e & Bx_B &\leq b_B - \beta g \\ h^\top x_A &= \beta & \text{and} & & f^\top x_B &= \alpha \\ x_A &\in \mathbb{Z}^{n_A} & & & x_B &\in \mathbb{Z}^{n_B} \end{aligned} \quad , \quad (3)$$

where we seek to find solutions  $x_A$  and  $x_B$  such that their corresponding group elements  $r_A := \gamma_A^\top x_A$  and  $r_B := \gamma_B^\top x_B$ , respectively, satisfy  $r_A + r_B \in R$ . Hence, this desired relation between the target elements  $r_A$  and  $r_B$  is the only dependence between the two problems once  $\alpha$  and  $\beta$  are fixed. We assume without loss of generality that  $A$  has no fewer columns than  $B$ , and refer to the problem on the left as the *A-problem*, and the problem on the right as the *B-problem*. We denote by  $\Pi$  the set of all  $(\alpha, \beta) \in \mathbb{Z}^2$  such that both the *A*- and *B*-problem are feasible. (Note that both problems are described through a TU constraint matrix; hence, feasibility can be checked efficiently.) Also, for  $(\alpha, \beta) \in \Pi$ , let  $\pi_A(\alpha, \beta) \subseteq G$  be all group elements  $r_A \in G$  for which there is a solution  $x_A$  to the *A*-problem with  $\gamma_A^\top x_A = r_A$ , and define  $\pi_B$  analogously. We refer to  $\pi_A$  and  $\pi_B$  as *patterns*. Hence, (2) is feasible if and only if there is a pair  $(\alpha, \beta) \in \Pi$  such that, for some  $r_A \in \pi_A(\alpha, \beta)$  and  $r_B \in \pi_B(\alpha, \beta)$ , we have  $r_A + r_B \in R$ . Thus, patterns contain all information needed to decide feasibility.

Using techniques from [NSZ22], we can restrict our search for feasible solutions to a constant-size subset  $\widehat{\Pi} \subseteq \Pi$ . More precisely, one can show the following (we give more details in [Appendix A.1](#)).

**Lemma 18.** *One can in strongly polynomial time find  $\ell_i, u_i \in \mathbb{Z}$  for  $i \in \{0, 1, 2\}$ , with  $u_i - \ell_i \leq d$  such that*

$$\widehat{\Pi} := \{(\alpha, \beta) \in \mathbb{Z}^2 : \ell_0 \leq \alpha + \beta \leq u_0, \ell_1 \leq \alpha \leq u_1, \ell_2 \leq \beta \leq u_2\} \quad (4)$$

*satisfies  $\widehat{\Pi} \subseteq \Pi$ , and if (2) is feasible, then there is a pair  $(\alpha, \beta)$  in  $\widehat{\Pi}$  for which there is a solution  $x_A$  to the *A*-problem and a solution  $x_B$  to the *B*-problem with  $\gamma_A^\top x_A + \gamma_B^\top x_B \in R$ .*

Therefore, the challenges lie less in the size of  $\Pi$ , but rather in how to obtain information on the sets  $\pi_A(\alpha, \beta)$  and  $\pi_B(\alpha, \beta)$  for pairs  $(\alpha, \beta) \in \Pi$ . Opposed to previous techniques, which almost solely focused on  $\pi_B$ , we investigate both  $\pi_A$  and  $\pi_B$  and their interplay—see [Section 4.3](#).

As  $B$  has at most half the columns of the constraint matrix  $T$  of the original *R-GCTUF* problem (2), we can afford (runtime-wise) to recursively call our algorithm multiple times on the *B*-problem for different targets  $R_B$  of the same depth  $d = |G| - |R|$  as the original problem, i.e., with  $|R_B| = |R|$ . (We refrain from using larger depths, as *GCTUF* become harder with increasing depth.) This allows us to compute a set  $\bar{\pi}_B(\alpha, \beta) \subseteq \pi_B(\alpha, \beta)$  of size  $|\bar{\pi}_B(\alpha, \beta)| = \min\{d + 1, \pi_B(\alpha, \beta)\}$ . Indeed, we can start with  $\bar{\pi}_B(\alpha, \beta) = \emptyset$  and, as long as  $|\bar{\pi}_B(\alpha, \beta)| < \min\{d + 1, \pi_B(\alpha, \beta)\}$ , we solve an *R<sub>B</sub>-GCTUF* *B*-problem (i.e., we look for a *B*-problem solution  $x_B$  with  $\gamma_B^\top x_B \in R_B$ ) with  $R_B = G \setminus \bar{\pi}_B(\alpha, \beta)$  being a set of size at least  $|G| - d$ . If  $R_B \cap \pi_B(\alpha, \beta) \neq \emptyset$ , then we find an element in  $R_B \cap \pi_B(\alpha, \beta)$  that can be added to  $\bar{\pi}_B(\alpha, \beta)$  and we repeat; otherwise,  $R_B \cap \pi_B(\alpha, \beta) = \emptyset$  and we know that we computed  $\bar{\pi}_B(\alpha, \beta) = \pi_B(\alpha, \beta)$ .

To the contrary, note that the *A*-problem may be almost as big as the original *GCTUF* problem (possibly with just two fewer columns). Hence, here we cannot afford (runtime-wise) a similar computation as for the *B*-problem. However, we can afford to solve multiple *R<sub>A</sub>-GCTUF* *A*-problems of smaller depth, i.e.,  $|R_A| > |R|$ , because the runtime decreases significantly with decreasing depth. By using the same approach as in the *B*-problem, but with sets  $R_A$  of size  $|R_A| \geq |R| + 1$ , we obtain a set  $\bar{\pi}_A(\alpha, \beta) \subseteq \pi_A(\alpha, \beta)$  of size  $|\bar{\pi}_A(\alpha, \beta)| = \min\{d, \pi_A(\alpha, \beta)\}$ .

Let us next take a closer look at patterns. Fix some  $(\alpha, \beta) \in \Pi$  and let  $\pi_A(\alpha, \beta) = \{r_A^1, \dots, r_A^{\ell_A}\}$  for some  $\ell_A \geq 1$  and pairwise different  $r_A^i \in G$ , and let  $x_A^1, \dots, x_A^{\ell_A}$  be corresponding solutions of the *A*-problem with  $\gamma_A^\top x_A^i = r_A^i$ . Define  $\ell_B, r_B^i$ , and  $x_B^i$  analogously. Observe that if  $\ell_A \leq d$  and  $\ell_B \leq d + 1$ , we have  $\bar{\pi}_X(\alpha, \beta) = \pi_X(\alpha, \beta)$  for both  $X \in \{A, B\}$ . Hence, we can compute all feasible group elements and check explicitly whether  $r_A^i + r_B^j \in R$  for some  $i \in [\ell_A]$  and  $j \in [\ell_B]$ , i.e., whether a solution exists. If  $\ell_B \geq d + 1$ , we can (independently of  $\ell_A$ ) even show that there always exists a

feasible solution, and we can also find one: Indeed, we can compute  $d + 1$  solutions  $x^i := (x_A^1, x_B^i)$  with pairwise different sums  $r_A^1 + r_B^i \in G$ , at least one of which must satisfy  $r_A^1 + r_B^i \in R$ . If  $\ell_A \geq d$  and  $\ell_B \geq 2$ , we can argue similarly: We show that among any  $d$  elements of  $\bar{\pi}_A(\alpha, \beta)$ , and any two elements of  $\bar{\pi}_B(\alpha, \beta)$  (which we can compute), there is a pair  $r_A^i, r_B^j$  with  $r_A^i + r_B^j \in R$ . Note that while for groups of prime order this can be shown via the Cauchy-Davenport theorem, the above result does not hold in general. We show, however, that as long as  $R$  is not a union of cosets in  $G$ , we can recover the implication (cf. Section 4.1 for why this assumption is legit).

**Lemma 19.** *Let  $G$  be a finite abelian group, and let  $R \subseteq G$  be such that  $R \neq R + H$  for any non-trivial subgroup  $H$  of  $G$ . Then, for any subsets  $X, Y \subseteq G$  with  $|X| = |G| - |R|$  and  $|Y| \geq 2$ , we have  $(X + Y) \cap R \neq \emptyset$ .*

*Proof.* Let  $b_1, b_2 \in Y$  with  $b_1 \neq b_2$ , and set  $h = b_1 - b_2$ . Assume  $(X + Y) \cap R = \emptyset$ . Then  $|X| = |G| - |R|$  implies  $|X + Y| = |X|$ . Thus,  $X + b_1 = X + b_2$  and hence  $X = X + h$ . Iterating gives  $X = X + \langle h \rangle$ , where  $\langle h \rangle$  denotes the subgroup generated by  $h$ . As  $R = G \setminus (X + b_1)$ , we get  $R = R + \langle h \rangle$ , a contradiction.  $\square$

The following observation summarizes the above discussion.

**Observation 20.** *Let  $(\alpha, \beta) \in \widehat{\Pi}$ . If  $|\bar{\pi}_A(\alpha, \beta)| \leq d - 1$  or  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ , we can immediately determine whether a feasible solution to the original  $R$ -GCTUF problem exists for such  $(\alpha, \beta)$ , and if so, obtain one by combining solutions computed for the  $A$ - and  $B$ -subproblem when determining  $\bar{\pi}_A$  and  $\bar{\pi}_B$ .*

Thus, the only case in which we cannot immediately check whether a feasible solution exists for some  $(\alpha, \beta)$ , is when  $\ell_B = 1$  and  $\ell_A \geq d + 1$  (which imply  $|\bar{\pi}_A(\alpha, \beta)| = d$  and  $|\bar{\pi}_B(\alpha, \beta)| = 1$ ). This is the only case where we may have  $(\pi_A(\alpha, \beta) + \pi_B(\alpha, \beta)) \cap R \neq \emptyset$  but  $(\bar{\pi}_A(\alpha, \beta) + \bar{\pi}_B(\alpha, \beta)) \cap R = \emptyset$ , in which case we say that  $(\alpha, \beta)$  contains a *hidden solution*.

### 4.3 New insights towards overcoming previous barriers for $d = 3$

We now describe how our new techniques allow for overcoming barriers restricting previous approaches to depth  $d = 2$ . Recall that we focus on a constant size subset  $\widehat{\Pi}$  as defined in (4). We call sets of this form, for any choice of  $\ell_i$  and  $u_i$ , *pattern shapes*, and denote by

$$\mathcal{D} := \left\{ \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} \quad (5)$$

the possible edge directions of  $\text{conv}(\widehat{\Pi})$ . Focusing on  $\widehat{\Pi}$  allows for efficiently computing  $\bar{\pi}_X(\alpha, \beta)$  for  $X \in \{A, B\}$  and all  $(\alpha, \beta) \in \widehat{\Pi}$  to the extent discussed earlier. In order to proceed, we use a structural result from [NSZ22], called averaging, that allows us to relate solutions—and thus elements of  $\pi_X$ —across different  $(\alpha, \beta)$ . Despite being true in more generality, the exposition here requires the following special case only.

**Proposition 21** ([NSZ22, special case of Lemma 5.3]). *Consider an  $R$ -GCTUF problem as described in (2). Let  $X \in \{A, B\}$ ,  $v \in \mathcal{D}$ , and  $(\alpha, \beta) \in \widehat{\Pi}$  with  $(\alpha, \beta) + 2v \in \widehat{\Pi}$ . Given a solution  $x_1$  of the  $X$ -problem for  $(\alpha, \beta)$  and, similarly,  $x_2$  for  $(\alpha, \beta) + 2v$ , there are solutions  $x_3, x_4$  for the  $X$ -problem for  $(\alpha, \beta) + v$  such that  $x_1 + x_2 = x_3 + x_4$ .*

We remark that the proof of the above result for congruency-constrained problems given in [NSZ22] only exploits that congruency-constraints are linear constraints; therefore, the result carries over to group-constraints seamlessly.

In previous approaches for depth  $d = 2$ , it was enough to only compute a single element from  $\pi_A$  (e.g., by solving the  $A$ -problem after dropping the group constraint). Concretely, consider patterns of the shape as given in Figure 1. For  $d = 2$ , Proposition 21 can be used to show that, if there is a hidden feasible solution for  $(\alpha, \beta) = (0, 0)$  or  $(\alpha, \beta) = (2, 0)$ , then there must also be a feasible solution for



**Figure 1:** Possible patterns  $\pi_A$  and  $\pi_B$  for a problem with group  $G = \mathbb{Z}/4\mathbb{Z}$ . Every square corresponds to a pair  $(\alpha, \beta) \in \widehat{\Pi}$ , and the numbers in the box indicate elements of  $\pi_A(\alpha, \beta)$  and  $\pi_B(\alpha, \beta)$ , respectively. For  $R = \{3\}$ , there is a feasible solution with  $(\alpha, \beta) = (0, 0)$ , but this cannot be detected without studying  $\pi_A$ .

$(\alpha, \beta) = (1, 0)$ . The example in [Figure 1](#) shows that this is no longer true if the depth  $d$  exceeds 2, as only  $(\alpha, \beta) = (0, 0)$  admits a feasible solution.

This problem can be circumvented by analyzing the  $A$ -pattern  $\bar{\pi}_A$ . As argued in [Section 4.2](#), if a pair  $(\alpha, \beta)$  has a hidden solution, then  $|\pi_A(\alpha, \beta)| \geq d + 1$  (and hence  $|\bar{\pi}_A(\alpha, \beta)| = d$ ), hence we assume that there exists at least one such pair. The following result uses averaging (i.e., [Proposition 21](#)) to show that pairs  $(\alpha', \beta')$  adjacent to such a pair  $(\alpha, \beta)$  containing a hidden solution also have large  $\bar{\pi}_A(\alpha', \beta')$ .

**Lemma 22.** *Let  $d \in \{1, 2, 3\}$ ,  $v \in \mathcal{D}$ , and  $(\alpha, \beta) \in \widehat{\Pi}$  such that  $|\pi_A(\alpha, \beta)| \geq d + 1$  and  $(\alpha, \beta) + 2v \in \widehat{\Pi}$ . Then  $|\bar{\pi}_A((\alpha, \beta) + v)| = d$ .*

*Proof.* It is enough to show that  $|\pi_A((\alpha, \beta) + v)| \geq d$ . To this end, for each of the at least  $d + 1$  elements  $r \in \pi_A(\alpha, \beta)$ , let  $x_1^r$  be a corresponding solution of the  $A$ -problem, and let  $x_2$  denote any fixed solution for the  $A$ -problem on the pair  $(\alpha, \beta) + 2v$ . [Proposition 21](#) applied to  $x_1^r$  and  $x_2$  gives solutions  $x_3^r$  and  $x_4^r$  corresponding to elements  $\gamma_A^\top x_3^r, \gamma_A^\top x_4^r \in \pi_A((\alpha, \beta) + v)$  with  $\gamma_A^\top x_3^r + \gamma_A^\top x_4^r$  taking at least  $d + 1$  different values. Assume for the sake of deriving a contradiction that  $|\pi_A((\alpha, \beta) + v)| \leq d - 1$ . Then, since the number of different sums of pairs of elements in  $\pi_A((\alpha, \beta) + v)$  is bounded by  $\binom{d-1}{2} + d - 1 = (d-1)d/2 < d + 1$  for  $d \in \{1, 2, 3\}$ , this contradicts the above construction.  $\square$

**Remark 23.** *For depth  $d = 4$ , one can find  $GCTUF$  problems with  $G = \mathbb{Z}/5\mathbb{Z}$  and patterns that fail to satisfy [Lemma 22](#); we present one such example in [Figure 2](#). Moreover, we remark that [Lemma 22](#) is the only place in our proofs where we use the assumption that  $d = |G| - |R| \leq 3$ .*



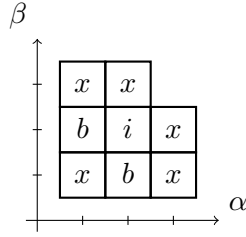
**Figure 2:** Possible patterns  $\pi_A$  and  $\pi_B$  for a problem with group  $G = \mathbb{Z}/5\mathbb{Z}$ . Every square corresponds to a pair  $(\alpha, \beta) \in \widehat{\Pi}$ , and the numbers in the box indicate the elements of  $\pi_A(\alpha, \beta)$  and  $\pi_B(\alpha, \beta)$ , respectively. For  $d = 4$ , [Lemma 22](#) fails to hold for  $(\alpha, \beta) = (0, 0)$  and  $v = (1, 0)$ .

To proceed, we observe that if, on top of the assumption in [Lemma 22](#),  $|\pi_B((\alpha, \beta) + v)| \geq 2$  holds, then [Lemma 19](#) guarantees  $(\bar{\pi}_A((\alpha, \beta) + v) + \bar{\pi}_B((\alpha, \beta) + v)) \cap R \neq \emptyset$ , i.e., existence of a feasible solution. Thus, from now on, we analyze both the  $A$ - and  $B$ -patterns in detail, in particular through averaging, to find a pattern constellation as mentioned above, or identify additional properties that allow for direct progress.

#### 4.4 Analyzing pattern structure

Before getting to an exhaustive analysis of patterns based on the insights laid out earlier, we introduce notions that will allow us to distinguish patterns from a structural point of view (also see [Figure 3](#)).

**Definition 24.** Let  $\mathcal{D}$  be the possible edge directions of a pattern shape as defined in (5). We call  $(\alpha, \beta) \in \widehat{\Pi}$  an interior pair if  $(\alpha, \beta) + v \in \widehat{\Pi}$  for all  $v \in \mathcal{D}$ , a border pair if  $(\alpha, \beta) \pm v \in \widehat{\Pi}$  for exactly two  $v \in \mathcal{D}$ , and a vertex pair if it is not an interior or border pair.



**Figure 3:** A pattern shape with interior, border, and vertex pairs (marked  $i$ ,  $b$ , and  $x$ , respectively).

Note that for a border pair  $(\alpha, \beta)$ , due to symmetry, the two directions  $v \in \mathcal{D}$  satisfying  $(\alpha, \beta) \pm v \in \widehat{\Pi}$  will always be antiparallel, i.e.,  $v$  and  $-v$  for some  $v \in \mathcal{D}$ . Next, we summarize results of [NSZ22] that we reuse here. We remark that these results were proved in a congruency-constrained setting, but translate to problems with group constraints straightforwardly. For the sake of completeness, we comment on how to adapt the proofs in Appendix A.2.

**Theorem 25** ([NSZ22]). Consider an  $R$ -GCTUF problem as described in (2).

- (i) If there is some  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ , then for each  $(\alpha', \beta') \in \widehat{\Pi}$ , there exists  $v \in \mathcal{D} \cup \{0\}$  such that  $|\bar{\pi}_B((\alpha', \beta') + v)| \geq 2$ . If in addition,  $\widehat{\Pi}$  contains an interior pair, then for each  $(\alpha', \beta') \in \widehat{\Pi}$ ,  $v$  can be chosen such that we additionally have  $(\alpha', \beta') + 2v \in \widehat{\Pi}$ .
- (ii) If  $|\bar{\pi}_B(\alpha, \beta)| = 1$  for all  $(\alpha, \beta) \in \widehat{\Pi}$ , or  $\widehat{\Pi}$  only contains vertex pairs and there are no solutions for  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ , then the problem can be reduced to a single  $R$ -GCTUF problem with the same group  $G$  and at the same depth  $d$ , and strictly fewer variables.

The two statements in the above theorem serve a complimentary purpose: While Item (ii) allows for direct progress (by reducing the number of variables), particularly in the case where no  $(\alpha, \beta) \in \widehat{\Pi}$  satisfies  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ , Item (i) shows that whenever such  $(\alpha, \beta)$  are present, then they are, in a certain sense, well spread over the pattern. We will exploit the latter in combination with Lemma 22.

To formally analyze patterns, based on Observation 20, we may assume that we face an  $R$ -GCTUF problem for which  $\widehat{\Pi}$  contains at least one  $(\alpha, \beta)$  such that  $|\bar{\pi}_A(\alpha, \beta)| \geq d + 1$  and  $|\bar{\pi}_B(\alpha, \beta)| = 1$ . Starting from there, we distinguish four different types of pattern structure as follows: (I)  $|\bar{\pi}_B(\alpha, \beta)| = 1$  for all  $(\alpha, \beta) \in \widehat{\Pi}$ , or this is not the case and (II)  $\widehat{\Pi}$  has an interior pair, or (III)  $\widehat{\Pi}$  has no interior but border pairs, or (IV)  $\widehat{\Pi}$  has only vertex pairs. The remainder of this section is devoted to presenting how to achieve progress in each of these four cases.

### Pattern structure of type I

Pattern structure of type I is covered by Theorem 25 (ii), which allows to reduce the problem to a new GCTUF problem with same group  $G$  and same depth  $d$ , and at least one variable less, thus allowing to make progress in that respect.

### Pattern structure of type II

For pattern structure of type II, we argue that if the  $R$ -GCTUF problem is feasible, then  $(\bar{\pi}_A + \bar{\pi}_B) \cap R \neq \emptyset$ . More precisely, we show that there must exist  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\bar{\pi}_A(\alpha, \beta)| = d$  and  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ . This then implies the desired result by Lemma 19. Concretely, assume that there exist  $(\alpha', \beta') \in \widehat{\Pi}$  containing a hidden solution. Then, since  $\widehat{\Pi}$  contains an interior pair, and there exists  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ , by Theorem 25 (i) there exists  $v \in \mathcal{D}$  such that  $(\alpha', \beta') + 2v \in \widehat{\Pi}$  and  $|\bar{\pi}_B((\alpha', \beta') + v)| \geq 2$ . As Lemma 22 implies that  $|\bar{\pi}_A((\alpha', \beta') + v)| = d$ , it follows by Lemma 19 that  $(\bar{\pi}_A((\alpha', \beta') + v) + \bar{\pi}_B((\alpha', \beta') + v)) \cap R \neq \emptyset$ ; thus we can find a solution at  $(\alpha', \beta') + v$ .

### Pattern structure of type III

In this case, we show that if  $\bar{\pi}_A + \bar{\pi}_B$  does not hit the target set  $R$ , i.e., we fail to find a solution by combining solutions of the  $A$ - and  $B$ -problem that we computed recursively, then we can reduce to a smaller pattern shape  $\Pi'$ , and recurse. Through such a reduction, we will after constantly many steps reach pattern structures of type I or type IV, and therefore achieve progress through the techniques presented for the corresponding type.

To start with, we show the following structural auxiliary result. We remark that this result can be seen as an implication of [NSZ22, Lemma 5.12], but we provide a more direct proof here.

**Lemma 26.** *Assume that  $\widehat{\Pi}$  does not contain interior pairs. Then  $\widehat{\Pi}$  contains at most four vertex pairs.*

*Proof.* Through shifting, we may assume that  $\ell_1 = \ell_2 = 0$ , and thus also  $\ell_3 \geq 0$  (if  $\ell_3 < 0$ , we may set it to zero without changing  $\widehat{\Pi}$ ). Similarly, we may assume  $u_3 \leq u_1 + u_2$ . Note that if  $u_1 - \ell_1 \leq 1$  there are at most four vertex pairs: At most two pairs  $(\alpha, \beta)$  may satisfy  $\alpha = \ell_1$ , and at most two further pairs may have  $\alpha = u_1$ . Similarly, we are done if  $u_2 - \ell_2 \leq 1$ , or  $u_3 - \ell_3 \leq 1$ . Thus, we assume  $u_i - \ell_i \geq 2$  for  $i \in \{1, 2, 3\}$ . Consider the pair

$$(\alpha, \beta) = \begin{cases} (1, \ell_3) & \text{if } \ell_3 < u_2 \\ (\ell_3 - u_2 + 2, u_2 - 1) & \text{if } \ell_3 \geq u_2 \end{cases}.$$

By definition,  $0 < \alpha, \beta < u_2$ , and  $\ell_3 < \ell_3 + 1 = \alpha + \beta < u_3$ . Because  $(\alpha, \beta)$  can not be an interior pair, we must either have  $\alpha \geq u_1$ , or  $\beta \leq 0$ . Because  $u_1 \geq 2 + \ell_1 = 2$ , we can only have  $\alpha \geq u_1$  in the case  $\ell_3 \geq u_2$ , which implies  $\ell_3 + 2 \geq u_1 + u_2$ . As also,  $\ell_3 + 2 \leq u_3 \leq u_1 + u_2$ , these inequalities must be tight, implying that there are precisely the three vertex pairs  $(u_1, u_2)$ ,  $(u_1 - 2, u_2)$ , and  $(u_1, u_2 - 2)$ . Similarly, because  $u_2 - 1 \geq 1 + \ell_2 \geq 1$ , we can only have  $\beta \leq 0$  in the case  $\ell_3 < u_2$ , which implies  $\ell_3 = 0$ . Consequently, we must also have  $u_2 = 2$ ; otherwise  $(1, 1)$  is an interior pair. This implies that there are precisely the three vertex pairs  $(0, 0)$ ,  $(2, 0)$ ,  $(0, 2)$ , and completes the proof.  $\square$

With the above at hand, we can achieve the desired progress for pattern structure of type III.

**Lemma 27.** *Consider an  $R$ -GCTUF instance of the form given in (2), and let the corresponding pattern shape  $\widehat{\Pi}$  be of type III. Then either  $(\bar{\pi}_A(\alpha, \beta) + \bar{\pi}_B(\alpha, \beta)) \cap R \neq \emptyset$  for some  $(\alpha, \beta) \in \widehat{\Pi}$ , or we can in strongly polynomial time find a pattern shape  $\Pi' \subsetneq \widehat{\Pi}$  such that the  $R$ -GCTUF instance is feasible on  $\widehat{\Pi}$  if and only if it is feasible on  $\Pi'$ .*

*Proof.* First assume there is a border pair  $(\alpha, \beta)$  with  $|\pi_B(\alpha, \beta)| \geq 2$ . Consider the unique constraint in the inequality description of  $\widehat{\Pi}$  that is tight at  $(\alpha, \beta)$ , and assume  $(\alpha', \beta') \in \widehat{\Pi} \setminus \{(\alpha, \beta)\}$  is another pair satisfying the same constraint with equality, and such that there is a hidden solution at  $(\alpha', \beta')$ . Let  $v \in \mathcal{D}$  be the direction pointing from  $(\alpha', \beta')$  to  $(\alpha, \beta)$ . By applying Proposition 21 repeatedly, we get  $|\bar{\pi}_B((\alpha', \beta') + v)| \geq 2$ . Moreover, as  $(\alpha, \beta)$  is a border pair, we have that  $(\alpha, \beta) + v$  lies in  $\widehat{\Pi}$ , and hence so does  $(\alpha', \beta') + 2v$ . It then follows from Lemma 22 that  $|\bar{\pi}_A((\alpha', \beta') + v)| = d$ , and hence  $(\bar{\pi}_A((\alpha', \beta') + v) + \bar{\pi}_B((\alpha', \beta') + v)) \cap R \neq \emptyset$  by Lemma 19. Thus, if we do not find a solution right away by combining elements from  $\bar{\pi}_A(\alpha, \beta)$  and  $\bar{\pi}_B(\alpha, \beta)$ , then there cannot be a hidden solution anywhere on the tight constraint. Thus, strengthening the tight constraint by one unit leads to the desired pattern shape  $\Pi' \subsetneq \widehat{\Pi}$ .

It is left to study the case where no border pair  $(\alpha, \beta) \in \widehat{\Pi}$  satisfies  $|\pi_B(\alpha, \beta)| \geq 2$ . Since  $\widehat{\Pi}$  has no interior pairs, there must exist a vertex pair  $(\alpha', \beta') \in \widehat{\Pi}$  with  $|\bar{\pi}_B(\alpha', \beta')| \geq 2$  (otherwise  $\widehat{\Pi}$  would be of type I). We now distinguish two cases:

*Case 1:* There are at least three vertex pairs with  $|\bar{\pi}_B(\alpha, \beta)| = 1$ . Combining the above discussion with Lemma 26, it follows that there is exactly one  $(\alpha', \beta') \in \widehat{\Pi}$  with  $|\pi_B(\alpha', \beta')| \geq 2$ . Then by Theorem 25 (i), for each of the other at least four pairs  $(\alpha, \beta) \in \widehat{\Pi}$  there exists  $v \in \mathcal{D}$  such that  $(\alpha, \beta) + v = (\alpha', \beta')$ , since  $(\alpha, \beta) + v$  must satisfy  $|\pi_B((\alpha, \beta) + v)| \geq 2$  and  $(\alpha', \beta')$  is the only such

pair. But  $(\alpha', \beta')$  is a vertex pair, and hence it can have at most three such adjacent pairs, a contradiction (also see Figure 4a).

*Case 2:* There are at most two vertex pairs with  $|\bar{\pi}_B(\alpha, \beta)| = 1$ . Consider a border pair  $(\alpha', \beta')$  and  $v \in \mathcal{D}$  such that  $(\alpha', \beta') \pm v \in \widehat{\Pi}$ . The tight constraint of  $(\alpha', \beta')$  contains two vertex pairs. Both of them must satisfy  $|\bar{\pi}_B(\alpha, \beta)| = 1$ , for otherwise, Proposition 21 would imply  $|\bar{\pi}_B(\alpha', \beta')| \geq 2$ , contradicting our assumption. Additionally, since we assumed to have at most two vertex pairs with  $|\bar{\pi}_B(\alpha, \beta)| = 1$ , it follows that any vertex pair  $(\alpha, \beta)$  outside this tight constraint must satisfy  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ . But then, from an argument analogous to the one in the first case above, it follows that there can not be a border pair  $(\alpha, \beta) \in \widehat{\Pi}$  that does not satisfy the tight constraint with equality, as otherwise we would get  $|\bar{\pi}_B(\alpha, \beta)| \geq 2$ . Consequently, all pairs  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\bar{\pi}_B(\alpha, \beta)| = 1$  (those are the only ones where there might be a hidden solution) satisfy the constraint that is tight at  $(\alpha', \beta')$  with equality. Thus, we can let  $\Pi'$  be the pattern shape defined by all  $(\alpha, \beta)$  that satisfy the tight constraint with equality (see Figure 4b for an example).  $\square$



(a) The pair marked in red is not adjacent to any  $(\alpha, \beta)$  with  $\pi_B(\alpha, \beta) \geq 2$ , hence this pattern cannot occur.

(b) Hidden solutions may only occur for the pairs marked in red.

**Figure 4:** The two cases arising in the proof of Lemma 27. Every square corresponds to a pair  $(\alpha, \beta) \in \widehat{\Pi}$ , and the numbers inside indicate the value of  $|\bar{\pi}_B(\alpha, \beta)|$ .

### Pattern structure of type IV

For type IV pattern structure, we first observe that, by Observation 20, if there are any solutions for pairs  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\pi_B(\alpha, \beta)| \geq 2$ , we can also find one efficiently by combining solutions computed for the  $A$ - and  $B$ -subproblem when determining  $\bar{\pi}_A$  and  $\bar{\pi}_B$ . The other case, i.e., when no solutions exist for such  $(\alpha, \beta)$ , is covered by Theorem 25 (ii). Again, that statement allows to reduce the problem to a new GCTUF problem with the same group  $G$  and at the same depth  $d$ , but at least one variable less. Therefore, it allows us to make progress with respect to the number of variables.

### Summary

The above discussion can be summarized in the following theorem. Recall that the depth of an  $R$ -GCTUF problem is defined as  $d := |G| - |R|$ .

**Theorem 28.** *Let  $G$  be a finite abelian group. Consider an  $R$ -GCTUF problem  $\mathcal{P}$  with  $n$  variables, group  $G$ , set of target residues  $R$ , depth  $d \leq 3$ , and a constraint matrix  $T$  that is a 3-sum of two matrices with  $n_A$  and  $n_B$  many columns, respectively, such that  $n = n_A + n_B$  and  $n_A, n_B \geq 2$ . Let  $p := \min\{n_A, n_B\}$ . Assume furthermore that there is no non-trivial subgroup  $H$  of  $G$  with  $R = R + H$ . Then, after solving at most  $(d + 1)^3$  many  $R$ -GCTUF problems with  $p$  variables, group  $G$  and depth at most  $d$ , as well as at most  $d(d + 1)^2$   $R$ -GCTUF problems with  $n - p$  variables, group  $G$  and depth at most  $d - 1$ , one can either*

- find a solution of  $\mathcal{P}$  in strongly polynomial time, or

- determine a single *R-GCTUF* problem  $\mathcal{P}'$  with at most  $n - p + 1$  variables, group  $G$  and depth  $d$ , such that  $\mathcal{P}$  is feasible if and only if  $\mathcal{P}'$  is feasible. Additionally, a solution of  $\mathcal{P}'$  can be transformed into a solution of  $\mathcal{P}$  in strongly polynomial time.

Furthermore, all involved *R-GCTUF* problems can be constructed in strongly polynomial time.

#### 4.5 Proof of Theorem 16

Consider an *R-GCTUF* problem with group  $G$ ,  $n$  variables, and depth  $d = |G| - |R| \leq 3$ . If  $d = 0$ , then the problem is an unconstrained TU problem, and thus it is enough to find a vertex solution of the linear relaxation. This can be done in strongly polynomial time using the algorithm of Tardos [Tar86]. If  $d > 0$ , we apply Theorem 15 to the constraint matrix  $T$ . If  $T$  is covered by one of Items (i) and (ii), then it is a base block matrix itself, so a single call to the oracle suffices. Else,  $T$  is covered by Item (iii) of Theorem 15, and we may assume that  $T$  decomposes into a 3-sum of two matrices with at least two columns each (see Appendix C for the case where a pivot step is necessary). In particular, note that in this case, we have  $n \geq 4$ . Using Lemma 17 or Theorem 28, we now reduce the problem to one or more smaller problems, until we eventually obtain base block problems, which we solve by an oracle call.

We bound the number of oracle calls triggered by our procedure. Let  $f(n, d)$  be the smallest upper bound on the number of oracle calls when starting from an instance with  $n$  variables and depth  $d$ . We claim that

$$f(n, d) \leq (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} .$$

To prove this bound, we use induction on  $n + d$ . First observe that, by the above discussion,  $f(n, 0) = 0$  for any  $n \geq 1$ , and  $f(n, d) = 1$  for  $n \leq 3$  and  $d > 0$  (in the latter case, we cannot attain Item (iii) of Theorem 15). Now consider an *R-GCTUF* problem with  $n$  variables and depth  $d$ . If  $R = R + H$  for a non-trivial subgroup  $H$  of  $G$ , Lemma 17 allows for a reduction to a single *R-GCTUF* problem at smaller depth. Thus, we end up with at most  $f(n, d')$  many base block problems for some  $d' < d$ . In this case, the induction hypothesis implies the claimed bound on  $f(n, d)$  because it is monotone in  $d$ . In the other case, we apply Theorem 28. Thus, there is a  $p \in \{2, \dots, \lfloor n/2 \rfloor\}$  such that the number of base block problems we have to solve is bounded by

$$\begin{aligned} & (d + 1)^3 f(p, d) + d(d + 1)^2 f(n - p, d - 1) + f(n - p + 1, d) \\ & \leq (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} \underbrace{\left( \left( \frac{p}{n} \right)^2 + \frac{n - p}{n^2} + \left( \frac{n - p + 1}{n} \right)^2 \right)}_{\leq 1} \leq (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} , \end{aligned}$$

proving the claimed bound on  $f(n, d)$ . Here, we use that

$$\begin{aligned} (d + 1)^3 f(p, d) & \leq (d + 1)^{3d+3} p^{d+3 \log_2(d+1)+2} \\ & = (d + 1)^3 \underbrace{\left( \frac{p}{n} \right)^{d+3 \log_2(d+1)}}_{\leq 1} (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} \left( \frac{p}{n} \right)^2 \\ & \leq (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} \left( \frac{p}{n} \right)^2 , \end{aligned}$$

as  $p/n \leq 1/2$  and hence  $(p/n)^{d+3 \log_2(d+1)} \leq (d + 1)^{-3}$ , together with

$$\begin{aligned} d(d + 1)^2 f(n - p, d - 1) & \leq d(d + 1)^2 d^{3d-3} (n - p)^{d-1+3 \log_2 d+2} \\ & \leq \underbrace{\frac{d(d + 1)^2}{(d + 1)^3} \left( \frac{n - p}{n} \right)^{d+3 \log_2(d+1)}}_{\leq 1} (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} \left( \frac{n - p}{n^2} \right) \\ & \leq (d + 1)^{3d} n^{d+3 \log_2(d+1)+2} \left( \frac{n - p}{n^2} \right) . \quad \square \end{aligned}$$



## References

- [AEGOVW16] S. Artmann, F. Eisenbrand, C. Glanzer, T. Oertel, S. Vempala, and R. Weismantel. “A note on non-degenerate integer programs with small sub-determinants”. In: *Operations Research Letters* 44.5 (2016), pp. 635–639. DOI: [10.1016/j.orl.2016.07.004](https://doi.org/10.1016/j.orl.2016.07.004) (cit. on p. 4).
- [AF21] M. Aprile and S. Fiorini. “Regular Matroids Have Polynomial Extension Complexity”. In: *Mathematics of Operations Research* 47.1 (2021), pp. 540–559. DOI: [10.1287/moor.2021.1137](https://doi.org/10.1287/moor.2021.1137) (cit. on p. 3).
- [AS22] G. Averkov and M. Schymura. “On the Maximal Number of Columns of a  $\Delta$ -modular Matrix”. In: *Proceedings of the 23rd International Conference on Integer Programming and Combinatorial Optimization (IPCO '22)*. Eindhoven, 2022, pp. 29–42. DOI: [10.1007/978-3-031-06901-7\\_3](https://doi.org/10.1007/978-3-031-06901-7_3) (cit. on p. 4).
- [AWZ17] S. Artmann, R. Weismantel, and R. Zenklusen. “A Strongly Polynomial Algorithm for Bimodular Integer Linear Programming”. In: *Proceedings of the 49th Annual ACM Symposium on Theory of Computing (STOC '17)*. Montreal, 2017, pp. 1206–1219. DOI: [10.1145/3055399.3055473](https://doi.org/10.1145/3055399.3055473) (cit. on pp. 1–3).
- [BC87] F. Barahona and M. Conforti. “A construction for binary matroids”. In: *Discrete Mathematics* 66.3 (1987), pp. 213–218. ISSN: 0012-365X. DOI: [10.1016/0012-365X\(87\)90097-5](https://doi.org/10.1016/0012-365X(87)90097-5) (cit. on p. 1).
- [BDEHN14] N. Bonifas, M. Di Summa, F. Eisenbrand, N. Haehnle, and M. Niemeier. “On Sub-determinants and the Diameter of Polyhedra”. In: *Discrete Computational Geometry* 52.1 (2014), pp. 102–115. DOI: [10.1007/s00454-014-9601-x](https://doi.org/10.1007/s00454-014-9601-x) (cit. on p. 4).
- [CGM92] P. M. Camerini, G. Galbiati, and F. Maffioli. “Random Pseudo-Polynomial Algorithms for Exact Matroid Problems”. In: *Journal of Algorithms* 13 (1992), pp. 258–273. DOI: [10.1016/0196-6774\(92\)90018-8](https://doi.org/10.1016/0196-6774(92)90018-8) (cit. on pp. 3, 21).
- [DEFM15] M. Di Summa, F. Eisenbrand, Y. Faenza, and C. Moldenhauer. “On Largest Volume Simplices and Sub-determinants”. In: *Proceedings of the 26th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '15)*. San Diego, 2015, pp. 315–323. DOI: [10.1137/1.9781611973730.23](https://doi.org/10.1137/1.9781611973730.23) (cit. on p. 4).
- [DK14] M. Dinitz and G. Kortsarz. “Matroid Secretary for Regular and Decomposable Matroids”. In: *SIAM Journal on Computing* 43.5 (2014), pp. 1807–1830. DOI: [10.1137/13094030X](https://doi.org/10.1137/13094030X) (cit. on p. 3).
- [EV17] F. Eisenbrand and S. Vempala. “Geometric random edge”. In: *Mathematical Programming* 164.1 (2017), pp. 325–339. DOI: [10.1007/s10107-016-1089-0](https://doi.org/10.1007/s10107-016-1089-0) (cit. on p. 4).
- [FJWY22] S. Fiorini, G. Joret, S. Weltge, and Y. Yuditsky. “Integer programs with bounded sub-determinants and two nonzeros per row”. In: *Proceedings of the 62nd Annual Symposium on Foundations of Computer Science (FOCS '22)*. 2022, pp. 13–24. DOI: [10.1109/FOCS52979.2021.00011](https://doi.org/10.1109/FOCS52979.2021.00011) (cit. on p. 1).
- [GLS84] M. Grötschel, L. Lovász, and A. Schrijver. “Corrigendum to our paper ‘The ellipsoid method and its consequences in combinatorial optimization’”. In: *Combinatorica* 4.4 (1984), pp. 291–295. ISSN: 1439-6912. DOI: [10.1007/BF02579139](https://doi.org/10.1007/BF02579139) (cit. on p. 1).
- [GLS93] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*. Vol. 2. Algorithms and combinatorics. Springer, 1993. DOI: [10.1007/978-3-642-78240-4](https://doi.org/10.1007/978-3-642-78240-4) (cit. on p. 5).
- [GR95] M. X. Goemans and V. S. Ramakrishnan. “Minimizing Submodular Functions over Families of Sets”. In: *Combinatorica* 15.4 (1995), pp. 499–513. DOI: [10.1007/BF01192523](https://doi.org/10.1007/BF01192523) (cit. on p. 1).

- [Gri21] D. V. Griбанov. “An FPTAS for the  $\Delta$ -Modular Multidimensional Knapsack Problem”. In: *Proceedings of the International Conference on Mathematical Optimization Theory and Operations Research (MOTOR)*. 2021, pp. 79–95. DOI: [10.1007/978-3-030-77876-7\\_6](https://doi.org/10.1007/978-3-030-77876-7_6) (cit. on p. 4).
- [GSMP22] D. Griбанov, I. Shumilov, D. Malyshev, and P. Pardalos. “On  $\Delta$ -modular integer linear problems in the canonical form and equivalent problems”. In: *Journal on Global Optimization* (2022). DOI: [10.1007/s10898-022-01165-9](https://doi.org/10.1007/s10898-022-01165-9) (cit. on p. 2).
- [GSW21] C. Glanzer, I. Stallknecht, and R. Weismantel. “On the Recognition of  $\{a, b, c\}$ -Modular Matrices”. In: *Proceedings of the 22nd International Conference on Integer Programming and Combinatorial Optimization (IPCO '21)*. Atlanta, 2021, pp. 238–251. DOI: [10.1007/978-3-030-73879-2\\_17](https://doi.org/10.1007/978-3-030-73879-2_17) (cit. on p. 4).
- [GV16] D. V. Griбанov and S. I. Veselov. “On integer programming with bounded determinants”. In: *Optimization Letters* 10.6 (2016), pp. 1169–1177. DOI: [10.1007/s11590-015-0943-y](https://doi.org/10.1007/s11590-015-0943-y) (cit. on p. 4).
- [GWZ18] C. Glanzer, R. Weismantel, and R. Zenklusen. “On the Number of Distinct Rows of a Matrix with Bounded Subdeterminants”. In: *SIAM Journal on Discrete Mathematics* 32.3 (2018), pp. 1706–1720. DOI: [10.1137/17M1125728](https://doi.org/10.1137/17M1125728) (cit. on p. 4).
- [GZ21] D. V. Griбанov and N. Y. Zolotykh. “On lattice point counting in  $\Delta$ -modular polyhedra”. In: *Optimization Letters* 16 (2021), pp. 1991–2018. DOI: [10.1007/s11590-021-01744-x](https://doi.org/10.1007/s11590-021-01744-x) (cit. on p. 4).
- [Hel57] I. Heller. “On linear systems with integral valued solutions”. In: *Pacific Journal of Mathematics* 7.3 (1957), pp. 1351–1364. DOI: [10.2140/pjm.1957.7.1351](https://doi.org/10.2140/pjm.1957.7.1351) (cit. on p. 4).
- [KB79] R. Kannan and A. Bachem. “Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix”. In: *SIAM J. Comput.* 8 (Nov. 1979), pp. 499–507. DOI: [10.1137/0208040](https://doi.org/10.1137/0208040) (cit. on p. 5).
- [LPSX20] J. Lee, J. Paat, I. Stallknecht, and L. Xu. “Improving Proximity Bounds Using Sparsity”. In: *Proceedings of the 6th International Symposium on Combinatorial Optimization (ISCO '20)*. Montreal, 2020, pp. 115–127. DOI: [10.1007/978-3-030-53262-8\\_10](https://doi.org/10.1007/978-3-030-53262-8_10) (cit. on p. 4).
- [LPSX22] J. Lee, J. Paat, I. Stallknecht, and L. Xu. “Polynomial Upper Bounds on the Number of Differing Columns of  $\Delta$ -Modular Integer Programs”. In: *Mathematics of Operations Research* (2022). DOI: [10.1287/moor.2022.1339](https://doi.org/10.1287/moor.2022.1339) (cit. on p. 4).
- [Nik15] A. Nikolov. “Randomized Rounding for the Largest Simplex Problem”. In: *Proceedings of the 47th Annual ACM Symposium on Theory of Computing (STOC '15)*. Portland, 2015, pp. 861–870. DOI: [10.1145/2746539.2746628](https://doi.org/10.1145/2746539.2746628) (cit. on p. 4).
- [NSZ19] M. Nägele, B. Sudakov, and R. Zenklusen. “Submodular Minimization Under Congruency Constraints”. In: *Combinatorica* 39.6 (2019), pp. 1351–1386. DOI: [10.1007/s00493-019-3900-1](https://doi.org/10.1007/s00493-019-3900-1) (cit. on pp. 1, 3, 6).
- [NSZ22] M. Nägele, R. Santiago, and R. Zenklusen. “Congruency-Constrained TU Problems Beyond the Bimodular Case”. In: *Proceedings of the 33rd Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '22)*. 2022, pp. 2743–2790. DOI: [10.1137/1.9781611977073.108](https://doi.org/10.1137/1.9781611977073.108) (cit. on pp. 1–10, 12, 13, 18–23).
- [NZ20] M. Nägele and R. Zenklusen. “A new contraction technique with applications to congruency-constrained cuts”. In: *Mathematical Programming* 183 (2020), pp. 455–481. DOI: [10.1007/s10107-020-01498-x](https://doi.org/10.1007/s10107-020-01498-x) (cit. on p. 1).
- [PR82] M. W. Padberg and M. R. Rao. “Odd Minimum Cut-Sets and  $b$ -Matchings”. In: *Mathematics of Operations Research* 7.1 (1982), pp. 67–80. DOI: [10.1287/moor.7.1.67](https://doi.org/10.1287/moor.7.1.67) (cit. on p. 1).

- [PSW22] J. Paat, M. Schlöter, and R. Weismantel. “The integrality number of an integer program”. In: *Mathematical Programming* 192 (2022), pp. 271–291. DOI: 10.1007/s10107-021-01651-0 (cit. on p. 4).
- [Sey80] P. D. Seymour. “Decomposition of regular matroids”. In: *Journal of Combinatorial Theory, Series B* 28.3 (1980), pp. 305–359. DOI: 10.1016/0095-8956(80)90075-1 (cit. on p. 3).
- [Tar86] É. Tardos. “A Strongly Polynomial Algorithm to Solve Combinatorial Linear Programs”. In: *Operations Research* 34.2 (1986), pp. 250–256. DOI: 10.1287/opre.34.2.250 (cit. on pp. 4, 15).
- [VC09] S. I. Veselov and A. J. Chirkov. “Integer program with bimodular matrix”. In: *Discrete Optimization* 6.2 (2009), pp. 220–222. DOI: 10.1016/j.disopt.2008.12.002 (cit. on pp. 2, 4).

## A Adapted proofs of structural results

This section is devoted to the proofs of [Lemma 18](#) and [Theorem 25](#). More precisely, given that these statements were proved in a congruency-constrained setting in [\[NSZ22\]](#), we mainly recall proof ideas and comment on how to adapt them to the group constraint setting that we work with.

### A.1 Proof of [Lemma 18](#)

[Lemma 18](#) is the group-constrained analogue of [\[NSZ22, Lemmas 2.5 and 5.1\]](#). To obtain the result, [\[NSZ22\]](#) exploits a decomposition theorem for solutions of totally unimodular systems [\[NSZ22, Lemma 2.1\]](#) combined with the following fact for the special case of  $G = \mathbb{Z}/m\mathbb{Z}$  [\[NSZ22, Lemma 2.2\]](#), which is indeed the only property of  $\mathbb{Z}/m\mathbb{Z}$  used throughout the proof.

**Lemma 29.** *Let  $G$  be a finite abelian group,  $R \subseteq G$ , and  $r_1, \dots, r_\ell \in G$  with  $\sum_{i \in [\ell]} r_i \in R$ . If there is no interval  $I = \{i_1, \dots, i_2\}$  with  $i_1, i_2 \in [\ell]$  and  $i_1 < i_2$  such that  $\sum_{i \in [\ell] \setminus I} r_i \in R$ , then  $\ell \leq |G| - |R|$ .*

Consequently, through [Lemma 29](#), the proofs of [\[NSZ22, Lemmas 2.5 and 5.1\]](#) immediately extend to the group constraint setting, and thereby imply [Lemma 18](#). We also remark that [Lemma 29](#) is in fact just a slightly generalized and more constructive version of [Lemma 11](#). Moreover, the original proof for  $G = \mathbb{Z}/m\mathbb{Z}$  directly generalizes. We repeat it here for completeness.

*Proof of [Lemma 29](#).* Assume for the sake of deriving a contradiction that there is no interval  $I \subseteq [\ell]$  with  $\sum_{i \in [\ell] \setminus I} r_i \in R$ , but  $\ell \geq |G| - |R| + 1$ . Consider the  $\ell$  group elements  $s_0 = 0, s_1 = r_1, \dots, s_{\ell-1} = r_1 + \dots + r_{\ell-1}$ . Observe that  $s_j \notin R$  for all  $j \in [\ell - 1]$ ; for otherwise, there is an interval  $I = \{j + 1, \dots, \ell\}$  for some  $j \in [\ell - 1]$  such that  $\sum_{i \in [\ell] \setminus I} r_i = s_j \in R$ , contradicting the assumption. Thus,  $s_j \in G \setminus R$  for all  $j \in [\ell - 1]$ . Hence, because  $\ell \geq |G| - |R| + 1$ , we have by the pigeonhole principle that there exist  $j_1, j_2 \in [\ell - 1]$  with  $j_1 < j_2$  such that  $s_{j_1} = s_{j_2}$ . Thus,  $I = \{j_1 + 1, \dots, j_2\}$  is an interval with  $\sum_{i \in [\ell] \setminus I} r_i = \sum_{i \in [\ell]} r_i - (s_{j_2} - s_{j_1}) = \sum_{i \in [\ell] \setminus I} r_i \in R$ , again contradicting the assumption and hence completing the proof.  $\square$

### A.2 Proof of [Theorem 25](#)

The statements in [Theorem 25](#) are closely linked to a [GCTUF](#) problem in the form presented in (2). In the following, we say that a solution  $x = (x_A, x_B)$  of a problem in that form is a solution for  $(\alpha, \beta)$  if  $\alpha = f^\top x_B$  and  $\beta = h^\top x_A$ .

### Item (i) of Theorem 25

In the congruency-constrained setting, the first part of Theorem 25 (i) was proved in [NSZ22, Lemma 5.9], while the second part is implicit in [NSZ22, Proof of Lemma 5.8]. The argument uses a generalized version of Proposition 21, which states that given distinct pairs  $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \widehat{\Pi}$ , there are  $(\alpha_3, \beta_3), (\alpha_4, \beta_4) \in \widehat{\Pi}$  such that for any solutions  $x_1$  for  $(\alpha_1, \beta_1)$  and  $x_2$  for  $(\alpha_2, \beta_2)$ , there exist solutions  $x_3$  for  $(\alpha_3, \beta_3)$  and  $x_4$  for  $(\alpha_4, \beta_4)$  such that  $x_1 + x_2 = x_3 + x_4$  (in fact,  $(\alpha_3, \beta_3)$  and  $(\alpha_4, \beta_4)$  are equal to  $\frac{1}{2}((\alpha_1, \beta_1) + (\alpha_2, \beta_2))$  up to rounding, see [NSZ22, Lemma 5.3]).

Towards a proof of Theorem 25 (i), we may assume that  $(\alpha', \beta') \neq (\alpha, \beta) + v$  for all  $v \in \mathcal{D} \cup \{0\}$ , and apply the above with  $(\alpha_1, \beta_1) = (\alpha', \beta')$  and  $(\alpha_2, \beta_2) = (\alpha, \beta)$ . This gives that  $(\alpha_3, \beta_3)$  and  $(\alpha_4, \beta_4)$  are both different from  $(\alpha_1, \beta_1)$  and  $(\alpha_2, \beta_2)$ , but “closer” to  $(\alpha', \beta')$  than  $(\alpha, \beta)$  was. The result will follow by iteratively applying this argument after showing that  $|\pi_B(\alpha_3, \beta_3)| \geq 2$  or  $|\pi_B(\alpha_4, \beta_4)| \geq 2$ . In the congruency-constrained case, the latter is concluded from the assumption that  $|\pi_B(\alpha, \beta)| \geq 2$ , i.e., that there are two feasible residues at  $(\alpha, \beta)$ . Indeed, if we had  $|\pi_B(\alpha_3, \beta_3)| = |\pi_B(\alpha_4, \beta_4)| = 1$ , then  $\gamma^\top(x_3 + x_4)$ —and hence also  $\gamma^\top(x_1 + x_2)$ —would have to yield the same residue for all solutions  $x_1$  for  $(\alpha_1, \beta_1)$  and  $x_2$  for  $(\alpha_2, \beta_2)$ . This reasoning holds analogously for any finite abelian group other than the cyclic groups  $\mathbb{Z}/m\mathbb{Z}$ , by well-definedness of addition to be precise. Because no other properties of congruency-constraints are exploited, the proofs of [NSZ22] directly translate to a proof of Theorem 25 (i).

### Item (ii) of Theorem 25

Theorem 25 (ii) gives two sufficient conditions that allow for reduction to a problem with fewer variables. The conditions are precisely that the pattern structure is of type I, or that it is of type IV and that there are no solutions for pairs  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\pi(\alpha, \beta)| \geq 2$ .

For pattern structure of type I, [NSZ22, Corollary 5.1] shows that—in the congruency-constrained setting—there exist  $r_0, r_1, r_2 \in \mathbb{Z}/m\mathbb{Z}$  such that  $\pi_B(\alpha, \beta) = \{r_0 + r_1\alpha + r_2\beta\}$  for all  $(\alpha, \beta) \in \widehat{\Pi}$ , and  $\pi_B$  is called *linear* in this case. Again, the proof is based on an averaging argument (i.e., Proposition 21) that seamlessly carries over to the more general group-constrained setting with a finite abelian group  $G$  by simply replacing calculations in  $\mathbb{Z}/m\mathbb{Z}$  by calculations in  $G$ . The same applies to showing that in case of a linear pattern, a GCTUF problem can be reduced to an equivalent problem with the same group  $G$ , at the same depth  $d$ , and strictly fewer variables [NSZ22, Theorems 2.4 and 2.5].

For pattern structure of type IV, Lemma 26 gives that  $\widehat{\Pi}$  consists of at most four pairs, and all of them are vertex pairs. This pattern family is very restricted, and is in fact a subset of the patterns covered by an analysis of certain small patterns in [NSZ22, Proof of Lemma 5.11]. Concretely, for the type IV pattern structure that we consider here, it was concluded (using another averaging argument, i.e., Proposition 21) that one can choose for every  $(\alpha, \beta) \in \widehat{\Pi}$  a singleton-subset  $\tilde{\pi}_B(\alpha, \beta) \subseteq \pi_B(\alpha, \beta)$  such that  $\tilde{\pi}_B$  is linear in the sense introduced above. Now recall that we also assume here that there are no solutions for pairs  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\pi(\alpha, \beta)| \geq 2$ , i.e., solutions can only occur for  $(\alpha, \beta) \in \widehat{\Pi}$  with  $|\pi_B(\alpha, \beta)| = 1$ . For those  $(\alpha, \beta)$ , we have  $\pi_B(\alpha, \beta) = \tilde{\pi}_B(\alpha, \beta)$ , so it is enough to look for solutions compatible with  $\tilde{\pi}_B$ . But then, linearity of  $\tilde{\pi}_B$  allows for the same reduction to an equivalent problem with fewer variables as discussed above (the congruency-constrained version is given in [NSZ22, Theorems 5.2 and 2.5]). Again, in all involved proofs of [NSZ22], all calculations in  $\mathbb{Z}/m\mathbb{Z}$  can directly be replaced by calculations in any fixed finite abelian group  $G$  without affecting correctness of the proofs, hence the results carry over as desired.  $\square$

## B Adapted proofs of base block results

In this section, we discuss how to extend the proofs of [NSZ22, Section 4] for congruency-constrained TU problems with a base block constraint matrix, i.e., matrices covered by Items (i) and (ii) of Theorem 15. The congruency constraints that were used previously may equivalently be formulated as constraints in a cyclic group  $\mathbb{Z}/m\mathbb{Z}$ , and it turns out that all arguments extend to general finite abelian

groups, i.e., the setting that we need for our purposes. In this appendix, we recall the proofs of [NSZ22] and comment on the mostly straightforward modifications for the sake of completeness.

To this end, let us first define *group-constrained TU problems* (GCTU problems) to be the optimization variant of GCTUF problems, i.e., where additionally to the GCTUF setup, we are given an objective  $c \in \mathbb{R}^n$  that we want to minimize over all feasible solutions of the GCTUF problem. Note that we can always assume to start with a GCTU problem whose relaxation (i.e., the problem obtained after dropping the group constraint) is feasible, which we can check in strongly polynomial time; for otherwise, the GCTU problem is clearly infeasible. Hence, we assume feasibility of the relaxation throughout this section. To start with, let us recall the definition of a *network matrix*.

**Definition 30.** *A matrix  $T$  is a network matrix if the rows of  $T$  can be indexed by the edges of a directed spanning tree  $(V, U)$ , and the columns can be indexed by the edges of a directed graph  $(V, A)$  on the same vertex set, such that for every arc  $a = (v, w) \in A$  and every arc  $u \in U$ ,*

$$T_{u,a} = \begin{cases} 1 & \text{if the unique } v\text{-}w \text{ path in } U \text{ passes through } u \text{ forwardly,} \\ 0 & \text{if the unique } v\text{-}w \text{ path in } U \text{ does not pass through } u, \\ -1 & \text{if the unique } v\text{-}w \text{ path in } U \text{ passes through } u \text{ backwardly.} \end{cases}$$

In the subsequent three sections, we distinguish the three different cases of base block matrices, namely whether the constraint matrix  $T$  of the GCTU problem that we consider is a network matrix, the transpose of a network matrix, or a matrix stemming from the constant-size matrices given in Item (ii) of Theorem 15.

## B.1 Network matrix base block GCTU problems

In this section, we discuss the extension from congruency constraints to group constraints in the case where the constraint matrix is a network matrix. Concretely, this will provide the following result.

**Theorem 31.** *Let  $G$  be a finite abelian group. There is a strongly polynomial time randomized algorithm for GCTU problems with group  $G$ , unary encoded objectives, and constraint matrices that are network matrices.*

In this case, one can exploit the graph structure that comes with network matrices to interpret GCTU problems with network constraint matrices as minimum-cost group-constrained circulation problems in certain directed graphs. To get started, let us recall that a circulation  $f$  in a directed graph  $H = (V, A)$  with capacities  $u: A \rightarrow \mathbb{Z}_{\geq 0}$  is a mapping  $f: A \rightarrow \mathbb{Z}_{\geq 0}$  such that  $f(a) \leq u(a)$  for every arc  $a \in A$ , and  $f(\delta^+(v)) = f(\delta^-(v))$  for every vertex  $v \in V$ . Given arc lengths  $\ell: A \rightarrow \mathbb{Z}$ , the length of a circulation  $f$  is  $\ell(f) := \sum_{a \in A} \ell(a)f(a)$ . Note that here, arc lengths are allowed to be negative. A group-constrained circulation problem is formally defined as follows.

**Group-Constrained Circulation (GCC):** Let  $H = (V, A)$  be a directed graph with capacities  $u: A \rightarrow \mathbb{Z}_{\geq 0}$ , arc lengths  $\ell: A \rightarrow \mathbb{Z}$ , and let  $G$  be a finite abelian group,  $\eta: A \rightarrow G$  and  $r \in G$ . Find a minimum-length circulation  $f: A \rightarrow \mathbb{Z}_{\geq 0}$  in the given network such that  $\sum_{a \in A} \eta(a)f(a) = r$ .

In [NSZ22, Lemma 4.2], a reduction from GCTU problems with a network matrix as constraint matrix to GCC is presented for the case of a cyclic group  $G = \mathbb{Z}/m\mathbb{Z}$ . In this reduction, the only property of  $\mathbb{Z}/m\mathbb{Z}$  that is exploited is [NSZ22, Lemma 2.2]. Thus, replacing this statement by its group-constrained analogue Lemma 29 proved earlier immediately gives the following.

**Lemma 32.** *GCTU problems with group  $G$ , objective vector  $c$ , and constraint matrices that are network matrices can be reduced in strongly polynomial time to GCC problems with group  $G$ , capacities  $u$  within  $\{0, \dots, |G| - 1\}$ , and arc lengths  $\ell$  with  $\|\ell\|_{\infty} \leq \|c\|_{\infty}$ .*

Now, one can finish the proof of [Theorem 31](#) by exploiting a connection to the so-called *exact length circulation problem*, where the goal is to find a circulation whose length is equal to a given value. The reduction follows the one given in [[NSZ22](#), Lemma 4.3], but needs to be slightly adapted in order to capture group constraints.

**Exact Length Circulation (XLC):** Let  $H = (V, A)$  be a digraph with capacities  $u: A \rightarrow \mathbb{Z}_{>0}$  and arc lengths  $\ell: A \rightarrow \mathbb{Z}$ . Given  $L \in \mathbb{Z}$ , find a circulation  $f$  in the given network such that  $\ell(f) = L$ .

Exact length circulation problems can be solved using a randomized pseudopolynomial algorithm, as shown by Camerini, Galbiati, and Maffioli [[CGM92](#)]. They reduce the problem to an exact cost perfect matching problem, which can then be reduced to computing the coefficients of a well-defined polynomial. The following theorem summarizes the result of Camerini, Galbiati, and Maffioli [[CGM92](#)] for **XLC**.

**Theorem 33** ([\[CGM92\]](#)). *There is a randomized algorithm for XLC problems in a directed graph  $H = (V, A)$  with capacities  $u: A \rightarrow \mathbb{Z}_{\geq 0}$  in time  $\text{poly}(|V|, \max_{a \in A} u(a), \max_{a \in A} |\ell(a)|)$ .*

Thus, it remains to extend the connection between **GCC** and **XLC** problems from the congruency-constrained to the group-constrained setting. To this end, we recall the reduction for a single congruency constraint modulo  $m$ : Taking an integer representative in  $\{0, \dots, m-1\}$  for each residue modulo  $m$ , we may construct new arc lengths that capture the residue representative  $r(a)$  and original arc lengths  $\ell(a)$  independently (e.g., by using  $\tilde{\ell}(a) = c \cdot \ell(a) + r(a)$  for a large enough constant  $c$ ). Guessing both the length and the residue class of an optimal solution of the **GCC** problem is then equivalent to guessing a target  $L$  with respect to the new lengths, hence the reduction can be achieved by binary search.

For group constraints, we recall that we may equivalently interpret a group constraint as multiple congruency constraints, which can then be integrated into new arc lengths  $\tilde{\ell}$  at different orders of magnitude. Formally, this leads to the following lemma, which is an analogue of [[NSZ22](#), Lemma 4.3].

**Lemma 34.** *A GCC problem in a graph  $H = (V, A)$  with group  $G$ , arc lengths  $\ell: A \rightarrow \mathbb{Z}$ , and capacities  $u: A \rightarrow \{0, 1, \dots, |H| - 1\}$  can be polynomially reduced to  $\text{poly}(|G|, |V|, |A|, \max_{a \in A} |\ell(a)|)$  many **XLC** problems in  $G$  with the same capacities.*

*Proof.* First, we may decompose  $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$  for some  $k \in \mathbb{Z}_{\geq 1}$ . For every  $i \in [k]$ , let  $\varphi_i: G \rightarrow \mathbb{Z}/m_i\mathbb{Z} \rightarrow \mathbb{Z}$  denote the corresponding natural projection maps composed with the natural mapping of a residue in  $\mathbb{Z}/m_i\mathbb{Z}$  to a representative in  $\{0, \dots, m_i - 1\}$ . Set  $m := |G|$ .

Define  $\tilde{\ell}: A \rightarrow \mathbb{Z}$  for every arc  $a \in A$  as

$$\tilde{\ell}(a) = \ell(a) \cdot m^{2k}|A|^k + \sum_{i=1}^k m^{2i-2}|A|^{i-1}\varphi_i(\eta(a)) .$$

We thus have  $\tilde{\ell}(f) = \ell(f) \cdot m^{2k}|A|^k + \sum_{i=1}^k m^{2i-2}|A|^{i-1}\varphi_i(\eta(f))$ . Observe that  $\sum_{a \in A} \varphi_i(\eta(a))f(a) < m^2|A|$  for every  $1 \leq i \leq k$ , hence from  $\tilde{\ell}(f)$ , one can retrieve  $\ell(f)$  as well as  $\sum_{a \in A} \varphi_i(\eta(a))f(a)$  for every  $i \in [k]$ . Consequently, finding a circulation of length  $L$  with  $\sum_{a \in A} \eta(a)f(a) = r$  is equivalent to solving **XLC** problems in  $H$  with respect to lengths  $\tilde{\ell}$  and with target length  $\tilde{L} = L \cdot m^{2k}|A|^k + \sum_{i=1}^k m^{2i-2}|A|^{i-1}(d_i m_i + \varphi_i(r))$  for all tuples  $(d_1, \dots, d_k) \in \{0, \dots, m|A| - 1\}^k$ . We can find the smallest  $L$  for which there is a **GCC** solution of length  $L$  by binary search in  $O(k \log(m|A|) \cdot \max_{a \in A} |\ell(a)|)$  iterations, because  $|\ell(f)| = |\sum_{a \in A} \ell(a)f(a)| \leq m|A| \cdot \max_{a \in A} |\ell(a)|$ . Altogether, this gives the desired result.  $\square$

Combining [Lemmas 32](#) and [34](#) and [Theorem 33](#) readily implies [Theorem 31](#).

## B.2 Transposed network matrix base block GCTU problems

For GCTU problems with a constraint matrix that is the transpose of a network matrix, we recall from Section 3 that we aim for a reduction to a lattice problem of the form given in (1). For the sake of completeness, let us restate that problem in the optimization setting here.

**Group-Constrained Lattice Optimization (GCLO):** Let  $N$  be a finite set,  $\mathcal{L} \subseteq 2^N$  a lattice,  $(G, +)$  a finite abelian group,  $\gamma: N \rightarrow G$ ,  $r \in G$ , and  $w: N \rightarrow \mathbb{Z}$ . The task is to find  $X \in \mathcal{L}$  with  $\gamma(X) := \sum_{x \in X} \gamma(x) = r$  minimizing  $\sum_{x \in X} w(x)$ , or decide infeasibility.

In [NSZ22, Section 4.2], the following result was shown implicitly for the case of a cyclic group  $G$ . It turns out, though, that no properties of cyclic groups beyond them being finite abelian groups are used in the proofs, hence by substituting all occurrences of congruency constraints, i.e., constraints in a cyclic group  $\mathbb{Z}/m\mathbb{Z}$ , with group constraints, the original proofs also imply the theorem for a general finite abelian group.

**Theorem 35.** *Given a finite abelian group  $G$ , consider a GCTU problem on  $n$  variables and a constraint matrix that is the transpose of a network matrix. One can in strongly polynomial time determine a GCLO problem over a ground set  $N$  with  $|N| = n|G|$  such that from an optimal solution of the GCLO problem, we can in strongly polynomial time compute an optimal solution of the GCTU problem.*

In particular, Theorem 35 implies the reduction claimed in Proposition 9 by observing that we can in strongly polynomial time determine  $w: N \rightarrow \mathbb{R}$  such that  $f(A) = \sum_{x \in A} w(x)$ .

## B.3 Matrices stemming from particular constant-size matrices

To complete the discussion of base block GCTU problems, we now cover GCTU problems with constraint matrices covered by Item (ii) of Theorem 15. In other words, these are matrices  $T$  that can be obtained from the two matrices

$$\begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ -1 & 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad (6)$$

by repeatedly appending unit vector rows or columns, appending a copy of a row or column, and inverting the sign of a row or column.

To tackle problems with such constraint matrices, [NSZ22, Section 4.3] more generally considers constraint matrices  $T$  that are obtained from a *core* matrix  $C$  through the above operations. (Concretely, in the case relevant here,  $C$  will be one of the two matrices in (6).) It is shown that if  $C$  has  $\ell$  columns, then there are integral vectors  $s_1, \dots, s_\ell$  such that once the values  $s_i^\top x$  are known for all  $i \in [\ell]$ , the inequality system  $Tx \leq b$  can be reduced to an equivalent system  $T'x \leq b'$  on the same variables  $x$ , where  $T'$  is a network matrix and the transpose of a network matrix at the same time, and  $b'$  is integral. By exploiting a proximity statement for congruency-constrained TU problems, [NSZ22] observe that it suffices to consider values  $s_i^\top x \in \{-m + 1, \dots, m - 1\}$ , where  $m$  is the modulus of the congruency-constraint, and they conclude that there are only  $(2m - 1)^\ell$  possible combinations of values for  $s_i^\top x$  to be enumerated, which can be done in polynomial time for constant  $\ell$ . To extend this reasoning from congruency constraints (i.e., constraints in a cyclic group  $G = \mathbb{Z}/m\mathbb{Z}$ ) to constraints in general finite abelian groups, we observe that the aforementioned proximity statement relies on a decomposition theorem for solutions of totally unimodular systems [NSZ22, Lemma 2.1] and the property of cyclic groups that we generalized in Lemma 29. Thereby, it is again a matter of replacing modular arithmetic by calculations in a general finite abelian group  $G$  to obtain the following result.

**Lemma 36.** *Let  $G$  be a finite abelian group and consider a  $GCTU$  problem with group  $G$  and a constraint matrix  $T$  that can be obtained from a matrix  $C$  with  $\ell$  columns by repeatedly appending unit vector rows or columns, appending a copy of a row or column, and inverting the sign of a row or column. Then, the  $GCTU$  problem can be reduced to  $(2|G| - 1)^\ell$  many  $GCTU$  problems with group  $G$  and constraint matrices of size linear in the size of  $T$  that are network matrices and transposes of network matrices at the same time.*

For feasibility problems, we may thus exploit [Theorem 7](#) to obtain the following direct corollary.

**Corollary 37.** *Let  $G$  be a finite abelian group. There is a strongly polynomial time algorithm for solving  $GCTUF$  problems with group  $G$  and a constraint matrix covered by [Item \(ii\)](#) of [Theorem 15](#).*

## C Pivoting steps

By [Theorem 15](#) (concretely, [Item \(iii\)](#)), we may face pivoting operations when applying Seymour's decomposition. For congruency-constrained TU problems, [[NSZ22](#), [Theorem 2.7](#)] shows that such operations can be dealt with in the following sense: After the addition of a single variable upper bound to a given congruency-constrained TU problem, there is a unimodular variable transformation that transforms the problem into an equivalent congruency-constrained TU problem such that (up to one extra constraint that is an upper bound on a variable), the new constraint matrix is the desired pivoted form of the original constraint matrix.

The transformation argument sketched above only exploits that congruency constraints are constraints on a linear combination of the variables, and thus immediately extends to group constraints. Adding an upper bound constraint on a variable can be done without changing the problem due to a proximity result for congruency-constrained TU problems [[NSZ22](#), [Lemma 3.2](#)]. The latter is again based on a decomposition theorem for solutions of TU systems [[NSZ22](#), [Lemma 2.1](#)] and the property of cyclic groups that we generalized in [Lemma 29](#), and thus translates to group constraints.