Problems on Group-Labeled Matroid Bases

Florian Hörsch
Algorithms and Complexity Group, CISPA, Saarbrücken, Germany

András Imolay
MTA-ELTE Matroid Optimization Research Group, Department of Operations Research, ELTE Eötvös Loránd University, Budapest, Hungary

Ryuhei Mizutani
Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Japan

Taihei Oki
Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Japan

Tamás Schwarcz
MTA-ELTE Matroid Optimization Research Group, Department of Operations Research, ELTE Eötvös Loránd University, Budapest, Hungary

Abstract

Consider a matroid equipped with a labeling of its ground set to an abelian group. We define the label of a subset of the ground set as the sum of the labels of its elements. We study a collection of problems on finding bases and common bases of matroids with restrictions on their labels. For zero bases and zero common bases, the results are mostly negative. While finding a non-zero basis of a matroid is not difficult, it turns out that the complexity of finding a non-zero common basis depends on the group. Namely, we show that the problem is hard for a fixed group if it contains an element of order two, otherwise it is polynomially solvable.

As a generalization of both zero and non-zero constraints, we further study F-avoiding constraints where we seek a basis or common basis whose label is not in a given set F of forbidden labels. Using algebraic techniques, we give a randomized algorithm for finding an F-avoiding common basis of two matroids represented over the same field for finite groups given as operation tables. The study of F-avoiding bases with groups given as oracles leads to a conjecture stating that whenever an F-avoiding basis exists, an F-avoiding basis can be obtained from an arbitrary basis by exchanging at most $|F|$ elements. We prove the conjecture for the special cases when $|F| \leq 2$ or the group is ordered. By relying on structural observations on matroids representable over fixed, finite fields, we verify a relaxed version of the conjecture for these matroids. As a consequence, we obtain a polynomial-time algorithm in these special cases for finding an F-avoiding basis when $|F|$ is fixed.

2012 ACM Subject Classification Mathematics of computing → Matroids and greedoids

Keywords and phrases matroids, matroid intersection, congruency constraint, exact-weight constraint, additive combinatorics, algebraic algorithm, strongly base orderability

Digital Object Identifier 10.4230/LIPIcs.ICALP.2024.86

Category Track A: Algorithms, Complexity and Games

Related Version *Full Version*: `https://arxiv.org/abs/2402.16259`

Funding This research has been implemented with the support provided by the Lendület Programme of the Hungarian Academy of Sciences – grant number LP2021-1/2021.
András Imolay: Supported by the Rényi Doctoral Fellowship of the Rényi Institute.
Ryuhei Mizutani: Supported by Grant-in-Aid for JSPS Fellows Grant Number JP23KJ0379 and JST SPRING Grant Number JPMJSP2108.
Taihei Oki: Supported by JSPS KAKENHI Grant Number JP22K17853 and JST ERATO Grant Number JPMJER1903.

51st International Colloquium on Automata, Languages, and Programming (ICALP 2024).
Editors: Karl Bringmann, Martin Grohe, Gabriele Puppis, and Ola Svensson;
Article No. 86; pp. 86:1–86:20
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Tamás Schwarcz: Supported by the ÚNKP-23-3 New National Excellence Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund.

Acknowledgements The authors are grateful to the organizers of the 14th Emléktábla Workshop, where the collaboration of the authors started. The authors thank Naonori Kakimura, Kevin Long, and Tomohiko Yokoyama for several discussions during the workshop, and Kristóf Bérczi, András Frank, and András Sebő for pointing out the connections to lattices and dual lattices.

1 Introduction

Several combinatorial optimization problems involve additional constraints, such as parity, congruency, and exact-weight constraints [35, 41, 42, 43, 44]. These constraints are subsumed by *group-label constraints* defined as follows: the ground set E is equipped with a labeling $\psi\colon E \to \Gamma$ to an abelian group Γ and a solution $X \subseteq E$ must ensure that the sum of the labels of its entries is not in a prescribed forbidden set $F \subseteq \Gamma$, i.e., $\psi(X) \coloneqq \sum_{e \in X} \psi(e) \notin F$. We call such a solution *F-avoiding*.

Particularly important special cases of group-label constraints include the *non-zero* ($F = \{0\}$) and *zero* ($F = \Gamma \setminus \{0\}$) constraints, where F-avoiding sets are referred to as *non-zero* and *zero*, respectively. The non-zero constraint has been extensively studied for path problems on graphs as it generalizes constraints on parity and topology. This line of research includes packing non-zero A-paths [12] as well as finding a shortest odd s–t path [46, Section 29.11e], a shortest non-zero s–t path [25], and an F-avoiding s–t path with $|F| \leq 2$ [28]. For these problems, some literature allows Γ to be non-abelian since the order of operations can be naturally defined for paths. Problems related to non-zero perfect bipartite matchings in $\mathbb{Z}_2$ have also been dealt with, see [1, 18, 26]. The zero constraint, or, slightly more generally, the group-label constraint with $|\Gamma \setminus F| = 1$, can encode the congruency and exact-weight constraints by setting Γ to be a cyclic group $\mathbb{Z}_m$ and the integers $\mathbb{Z}$, respectively. Examples of problems whose congruency-constrained versions have been studied include submodular function minimization [42], minimum cut [43], and integer linear programming with totally unimodular coefficients [41]. For the last problem, Nägele, Santiago, and Zenklusen [41] gave a randomized strongly polynomial-time algorithm to test the existence of an F-avoiding feasible solution, where the group is $\mathbb{Z}_m$ with prime m and $|F| \leq 2$, implying the congruency constraint if $m = 3$.

The exact-weight constraint was first considered for the matching problem by Papadimitriou and Yannakakis [44]. Mulmuley, Vazirani, and Vazirani [40] gave a randomized polynomial-time algorithm for solving the problem using an algebraic technique. Derandomizing this algorithm is a major open problem and there is a collection of partial results for it, see e.g. [6, 18, 22, 49, 52]. Other exact problems include arborescences, matchings, cycles [2], and independent sets or bases in a matroid [11, 16, 45].

In this work, we explore group-label constraints for matroid bases and matroid intersection. Throughout the paper, we assume that any group Γ is abelian without mentioning it. In the problems Non-Zero Basis and Zero Basis, we are given a matroid M on a ground set E and a group labeling $\psi\colon E \to \Gamma$, and we are to find a non-zero or zero basis, respectively, or to correctly report that no such basis exists. In F-avoiding Basis, along with the matroid M and labeling ψ, we are also given a forbidden label set $F \subseteq \Gamma$, and we need to find an F-avoiding basis, that is, a basis B with $\psi(B) \notin F$. In Non-Zero Common Basis, Zero Common Basis, and F-avoiding Common Basis, instead of a single matroid, we are given two matroids M_1 and M_2 on a common ground set E and seek a non-zero, zero, and F-avoiding common basis, respectively. We also tackle the weighted variants of these problems, referred to as Weighted Non-Zero Basis for example, where we are to find a feasible solution minimizing a given weight function $w\colon E \to \mathbb{R}$.

We note that the target label 0 in the non-zero and zero problems can be changed to an arbitrary group element $g \in \Gamma$ by appending a coloop to the ground set with label $-g$. Regarding the input of the group, we consider the following three types: (i) operation and zero-test oracle, (ii) operation table of a finite group, and (iii) a fixed finite group. Unless otherwise stated, we assume that a group is given as the oracles and the matroids are given as independence oracles. In this case, by a polynomial-time algorithm, we mean an algorithm making polynomially many elementary steps, group operations, and independence oracle calls. If the group is finite and is given by its operation table, then the running time of a polynomial-time algorithm can depend polynomially on the group size.

Our research follows the recent initiative by Liu and Xu [35], who addressed Zero Basis[1]. They conjectured that, given the existence of a zero basis, for any non-zero basis B, there is a zero basis B^* such that $|B^* \setminus B| \leq D(\Gamma) - 1$, where $D(\Gamma)$ denotes the Davenport constant of Γ (see Section 6.3 for definition), which is upper-bounded by $|\Gamma|$. Liu and Xu proved the conjecture for cyclic groups $\Gamma = \mathbb{Z}_m$ with the order m being a prime power or the product of two primes, with the aid of an additive combinatorics result by Schrijver and Seymour [47], deriving an FPT algorithm parameterized by $|\Gamma| = m$ for Zero Basis. In Theorem 6.6, we give a counterexample to this conjecture for groups with $\mathbb{Z}_2^d$ with $d \geq 4$.

The non-zero constraint is closely related to *lattices* studied by Lovász [37]. The *lattice* generated by vectors $\{v_1, \ldots, v_n\} \subseteq \mathbb{R}^n$ is the set $\{\sum_{i=1}^n \lambda_i v_i \mid \lambda_1, \ldots, \lambda_n \in \mathbb{Z}\}$. For a set family $\mathcal{F} \subseteq 2^E$, let $\mathrm{lat}(\mathcal{F})$ denote the lattice generated by the characteristic vectors of $\mathcal{F}$. Every lattice has a *lattice basis* $A = \{a_1, \ldots, a_n\} \subseteq \mathbb{Z}^E$, which is a set of linearly independent vectors generating it. Since $\mathcal{F}$ and its lattice basis A generate the same lattice, $\mathcal{F}$ has a non-zero member if and only if A has a non-zero member, i.e., $\psi(a_i) \coloneqq \sum_{e \in E} a_i(e)\psi(e) \neq 0$ for some i. This implies that if a basis of $\mathrm{lat}(\mathcal{F})$ can be computed in polynomial time, then the existence of a non-zero member of $\mathcal{F}$ can be decided in polynomial time. Such set families $\mathcal{F}$ include matroid bases [45], common bases of a matroid and a partition matroid having two classes [45], and perfect matchings [37, 38].

Below, we summarize our results for each problem.

Non-Zero Basis. The tractability of Non-Zero Basis can be derived from the above lattice argument together with a characterization of base lattices [45]. We observe that for any zero basis B, there exists a non-zero basis B^* such that $|B^* \setminus B| \leq 1$, provided that at least one non-zero basis exists. A weighted variant of this statement is shown in the same way. This result generalizes an algorithm for Weighted Zero Basis with $\Gamma = \mathbb{Z}_2$ by Liu and Xu [35].

Non-Zero Common Basis. We show in Theorems 3.7 and 6.1 that Non-Zero Common Basis is polynomially solvable if and only if Γ does not contain $\mathbb{Z}_2$ as a subgroup. Our hardness proof for $\Gamma = \mathbb{Z}_2$ is based on an information-theoretic argument using sparse paving matroids, which is independent of the $\mathsf{P} \neq \mathsf{NP}$ conjecture. The polynomial-time algorithm for $\Gamma \not\geq \mathbb{Z}_2$ is a modification of the negatively directed cycle elimination algorithm for weighted matroid intersection [9]. In Theorem 3.9, we also give a 2-approximation algorithm for Weighted Non-Zero Common Basis if $\Gamma \not\geq \mathbb{Z}_2$ and the weight function is nonnegative. Finally, in Theorems 3.11 and 3.12, we solve Weighted

[1] Called *Group-Constrained Matroid Base* (GCMB) in [35].

Non-Zero Common Basis for an arbitrary group when both matroids are partition matroids or one of the matroids is a partition matroid defined by a partition having two classes.

- **F-avoiding Basis and Common Basis.** If the group is fixed and finite, (Weighted) F-avoiding Basis reduces to polynomially many instances of (weighted) matroid intersection [35]. On the other hand, it follows from the results of [16] that F-avoiding Basis requires exponentially many independence oracle queries if F is part of the input and the group is finite and is given as an operation table, while the same hardness of F-avoiding Common Basis follows from our Theorem 6.1 even if the group is fixed and finite. Regarding positive results for F-avoiding problems, our contribution is twofold. First, using similar ideas as in [11, 51], in Theorem 4.2 we give a randomized algebraic algorithm for F-avoiding Common Basis in case where the matroids are represented over the same field and the group is finite and is given as an operation table. We observe in Theorem 4.3 that the algorithm can be derandomized in certain cases, including F-avoiding Basis for graphic matroids. Second, we turn to the study of F-avoiding Basis for cases where $|F|$ is fixed and the group is given by an oracle. Motivated by the work of Liu and Xu [35], we propose Conjecture 5.1 stating that if at least one F-avoiding basis exists, then each basis can be turned into an F-avoiding basis by exchanging at most $|F|$ elements. The validity of the conjecture follows from the results of [35] for groups of prime order. We show that the conjecture also holds if Γ is an ordered group (Theorem 5.6) or if $|F| \leq 2$ (Theorem 5.18). By introducing a novel relaxation of strong base orderability, in Theorem 5.11 we show that a relaxation of the conjecture holds for $\mathrm{GF}(q)$-representable matroids for every fixed prime power q. In Theorem 5.17, we prove a somewhat stronger version of this result for graphic matroids. In each of these special cases, we obtain the polynomial solvability of F-avoiding Basis for fixed F.
- **Zero Basis and Zero Common Basis.** The zero constraint for $\Gamma = \mathbb{Z}$ corresponds to the exact-weight constraint, implying that many problems are NP-hard, in particular, Zero Basis is NP-hard even for uniform matroids (Theorem 6.2). It follows from the results of [16] that Zero Basis requires exponentially many independence oracle queries for a finite group given by operation table. We show the same hardness of Zero Common Basis for any fixed nontrivial group (Theorem 6.4). On the other hand, we obtain positive results from the aforementioned results on F-avoiding problems. In particular, Zero Basis is polynomially solvable if the group is fixed and finite [35], Theorem 4.2 implies a randomized polynomial-time algorithm for Zero Common Basis for matroids represented over the same field if Γ is finite and is given as an operation table, and using the results of [35], Theorem 5.11 implies an FPT algorithm for Zero Basis when parameterized by $|\Gamma|$ if the matroids are representable over a fixed, finite field.

Other work related to group-labeled matroids

Bérczi and Schwarcz [5] showed the hardness of partitioning into common bases, see also [4, 24] for later results. A natural relaxation of that problem gives rise to problems related to Non-Zero Common Basis for the group $\mathbb{R}/\mathbb{Z}$. This relation is explained in the full version.

It is straightforward to verify that the family of non-zero subsets of a set satisfies the axiom of *delta-matroids*, which are a generalization of matroids introduced by Bouchet [8]. From this viewpoint, Non-Zero Basis offers a tractable special case of the intersection of a matroid and a delta-matroid. We note that the intersection of a matroid and a delta-matroid is intractable in general, as it encompasses matroid parity. Kim, Lee, and Oum [29] defined a delta-matroid, called a Γ-*graphic delta-matroid*, from a graph equipped with a labeling of vertices to an abelian group Γ. In the definition, they employ a constraint similar to but different from non-zero. Exploring the relationship between Γ-graphic delta-matroids and our findings is left for future work.

Organization

The rest of this paper is organized as follows. Section 2 provides preliminaries on groups and matroids. Section 3 deals with non-zero problems. Section 4 provides an algebraic algorithm for F-avoiding Common Basis for represented matroids. Section 5 studies F-avoiding Basis if $|F|$ is fixed. Section 6 includes our hardness results for each of the problems. Finally, Section 7 concludes this paper enumerating open problems.

2 Preliminaries

Let $\mathbb{N}$, $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}_{\geq 0}$, and $\mathbb{R}$ denote the set of positive integers, nonnegative integers, integers, rationals, nonnegative reals, and reals, respectively. We let $[n] \coloneqq \{1, \dots, n\}$ for $n \in \mathbb{Z}_{\geq 0}$. For a set S, we simply write $S \setminus \{x\}$ as $S - x$ for $x \in S$ and $S \cup \{y\}$ as $S + y$ for $y \notin S$. For a set E and $r \in \mathbb{Z}_{\geq 0}$, we let $\binom{E}{r} \coloneqq \{\, S \subseteq E \mid |S| = r \,\}$.

In this paper, all groups are implicitly assumed to be abelian. We use the additive notation for the operations of groups except in Section 4. For $m \in \mathbb{N}$, let $\mathbb{Z}_m = \{0, \dots, m-1\}$ denote the cyclic group of order m. For groups Γ_1 and Γ_2, we mean by $\Gamma_1 \leq \Gamma_2$ that Γ_1 is a subgroup of Γ_2. A group Γ is said to be *ordered* if Γ is equipped with a total order $\leq$ compatible with the operation of Γ in the sense that $a \leq b$ implies $a + c \leq b + c$ for all $a, b, c \in \Gamma$. A *labeling* is a function $\psi\colon E \to \Gamma$ from a set E to a group Γ, and we let $\psi(S) \coloneqq \sum_{x \in S} \psi(x)$ for $S \subseteq E$. Let $\mathrm{GF}(q)$ denote the finite field of q elements for a prime power q.

We follow [14] for basic terminologies on graphs such as paths and cycles. The vertex and edge sets of a graph G are denoted by $V(G)$ and $E(G)$, respectively. Similarly, $V(D)$ denotes the vertex set of a directed graph D, and $A(D)$ denotes its arc set. Given a weight function $w\colon A(D) \to \mathbb{R}$ and a subgraph C of D, the *weight* of C is defined as $w(C) \coloneqq w(A(C))$. A weight function w is said to be *conservative* if D does not contain a directed cycle of negative weight.

We refer the reader to [20, 46] for basics on matroid optimization. A *matroid* M consists of a finite ground set $E(M)$ and a nonempty set family $\mathcal{B}(M) \subseteq 2^{E(M)}$ such that for any $B_1, B_2 \in \mathcal{B}(M)$ and $x \in B_1 \setminus B_2$, there exists $y \in B_2 \setminus B_1$ such that $B_1 - x + y \in \mathcal{B}(M)$. Elements in $\mathcal{B}(M)$ are called *bases*. The next basis exchange property was proved by Brualdi [10], see also [46, Theorem 39.12].

▶ **Lemma 2.1** (Brualdi [10]). *If B and B' are bases of a matroid M, then there exists a bijection $\phi\colon B \setminus B' \to B' \setminus B$ such that $B - e + \phi(e)$ is a basis for each $e \in B \setminus B'$.*

Following [20], we define a *partition matroid* as a direct sum of uniform matroids and a *unitary partition matroid* as a direct sum of rank-1 uniform matroids. We note that several authors refer to the latter object as partition matroids. Given a matrix A over some field, we denote by $M(A)$ the matroid defined on the column indices of A where a set is a basis of $M(A)$ if the corresponding columns form a basis of the vector space spanned by the columns of A. Given a connected graph G, its *cycle matroid* $M(G)$ is the matroid whose ground set is $E(G)$ and whose bases are the edge sets of the spanning trees of G. If $M = M(A)$ for a matrix A over a field $\mathbb{F}$ or a graph A, we say that M is $\mathbb{F}$-*representable* or *graphic*, respectively.

3 Non-Zero Basis and Common Basis

3.1 Non-Zero Basis

In this section, we consider (Weighted) Non-Zero Basis. The following theorem can be derived from the description of the lattices of matroid bases by Rieder [45]. In what follows we give a direct proof of the result.

▶ **Theorem 3.1.** *Let M be a matroid and $\psi\colon E(M) \to \Gamma$ a group labeling. The following are equivalent:*

(i) *all bases of M have the same label,*
(ii) *M has a basis B such that $\psi(B') = \psi(B)$ holds for each basis B' with $|B \setminus B'| \leq 1$, and*
(iii) *ψ is constant on each component of M.*

Proof. It is clear that (i) implies (ii) and (iii) implies (i). In what follows, we show that (ii) implies (iii). Let B be a basis such that $\psi(B') = \psi(B)$ holds for each basis B' with $|B \setminus B'| \leq 1$. Let G_B denote the bipartite graph with bipartition $(B, E(M) \setminus B)$ and edge set $\{\, xy \mid x \in B, y \in E(M) \setminus B, B - x + y \in \mathcal{B}(M) \,\}$. By the assumption on B, it follows that $\psi(x) = \psi(y)$ for each edge xy of G_B. Then, ψ is constant on each connected component of the graph G_B, and thus (iii) follows by using that the connected components of the graph G_B coincide with the components of the matroid M [32]. ◀

Note that Theorem 3.1(iii) provides a characterization for "NO" instances of Non-Zero Basis, while Theorem 3.1(ii) provides a simple algorithm for this problem. Liu and Xu [35] gave the following simple and constructive algorithm for Weighted Zero Basis with $\Gamma = \mathbb{Z}_2$, for which the zero and non-zero constraints are equivalent, without decomposing the matroid into components. First, find a minimum weight basis $B \in \mathcal{B}(M)$, and if $\psi(B) \neq 0$, then we are done. Otherwise, consider all the bases of the form $B - x + y$ with $x \in B$ and $y \in E(M) \setminus B$. Among these bases, if there is none with a non-zero label, then there does not exist a non-zero basis, otherwise, choose a non-zero basis of minimum weight among the considered ones. Actually, this algorithm works correctly for Weighted Non-Zero Basis for any group, and the proof of [35, Proposition 1] can be modified to show its correctness. In what follows, we give a different proof of this fact.

▶ **Lemma 3.2.** *Let M be a matroid, $\psi\colon E(M) \to \Gamma$ a group labeling, and $w\colon E(M) \to \mathbb{R}$ a weight function. Then, for any minimum-weight basis B, there exists a minimum-weight non-zero basis B^* such that $|B \setminus B^*| \leq 1$, provided that at least one non-zero basis exists.*

Proof. Let B' be a minimum-weight non-zero basis with $|B \setminus B'|$ being minimal. If $B = B'$ then we are done, otherwise $\psi(B) = 0$. According to the symmetric exchange axiom, we can choose $x \in B \setminus B'$ and $y \in B' \setminus B$ such that $B - x + y$ and $B' + x - y$ are both bases. As $0 \neq \psi(B) + \psi(B') = \psi(B - x + y) + \psi(B' + x - y)$, one of $B - x + y$ and $B' + x - y$ must be non-zero. Suppose $\psi(B - x + y) \neq 0$. Since $w(B) + w(B') = w(B - x + y) + w(B' + x - y)$ and $w(B)$ has the minimum weight, we have $w(B - x + y) \leq w(B')$, which implies $w(B - x + y) = w(B')$ by $\psi(B - x + y) \neq 0$. Thus, we can take $B^* = B - x + y$. If $\psi(B' + x - y) \neq 0$, then it can be shown in the same way that $B' + x - y$ is a minimum-weight non-zero basis, contradicting the assumption that B' is a minimum-weight non-zero basis closest to B. ◀

We obtain the following from Lemma 3.2.

▶ **Theorem 3.3.** Weighted Non-Zero Basis *can be solved in polynomial time.*

3.2 Non-Zero Common Basis

3.2.1 Polynomial-time Algorithm with $\mathbb{Z}_2 \not\leq \Gamma$

In this section, we show the polynomial solvability of Non-Zero Common Basis when $\mathbb{Z}_2 \not\leq \Gamma$, that is, Γ does not contain any element of order two. Later, we will show in Theorem 6.1 that the problem is hard if $\mathbb{Z}_2 \leq \Gamma$. Our algorithm is a modification of the weighted matroid intersection algorithm given by Krogdahl [30, 31, 32] and independently by Brezovec, Cornuéjols, and Glover [9].

We will use the following result on directed graphs. While several works concentrated on finding non-zero paths and cycles in group-labeled graphs [25], their setting does not seem to include group-labeled digraphs. Therefore, we give a proof of the next result in the full version. While this result may be of independent interest, it will later be applied as a subroutine.

▶ **Theorem 3.4.** *Let D be a digraph, $\psi\colon A(D) \to \Gamma$ a group labeling, and $w\colon A(D) \to \mathbb{R}$ a conservative weight function. Then, there is a polynomial-time algorithm that returns a non-zero directed cycle in D which is shortest with respect to w or correctly reports that D contains no non-zero directed cycle.*

We note that the problem of finding an odd directed path is NP-hard even in the unweighted case [33]. In contrast to Theorem 3.4, the key distinction here lies between walks and paths: while a walk can include a directed cycle to change a group label, a path cannot. Consequently, a Dijkstra-style algorithm for finding an odd directed path must track not only the last vertex but also all intermediate vertices, leading to an exponential increase in running time.

Let M_1 and M_2 be matroids on a common ground set E and $\psi\colon E \to \Gamma$ a group labeling. Given a common basis B, we define the digraph $D_{M_1,M_2}(B)$ on the vertex set E and the labeling ψ' on its arcs as follows. For each $x \in B$ and $y \in E \setminus B$ such that $B - x + y \in \mathcal{B}(M_1)$, we add an arc xy to $D_{M_1,M_2}(B)$ with label $\psi'(xy) \coloneqq \psi(y)$. Similarly, for each $x \in B$ and $y \in E \setminus B$ such that $B - x + y \in \mathcal{B}(M_2)$, we add an arc yx and with label $\psi'(yx) \coloneqq -\psi(x)$.

▶ **Lemma 3.5.** *Let M_1 and M_2 be matroids on a common ground set E and $\psi\colon E \to \Gamma$ a group labeling. Let B and B' be common bases of M_1 and M_2 such that $\psi(B) = 0$ and $\psi(B') \neq 0$. Then, $D_{M_1,M_2}(B)$ contains a non-zero directed cycle C with $V(C) \subseteq B \triangle B'$.*

Proof. By Lemma 2.1, $D_{M_1,M_2}(B)$ contains a collection P_1 of $|B \setminus B'|$ pairwise vertex-disjoint arcs from $B \setminus B'$ to $B' \setminus B$ and a collection P_2 of $|B \setminus B'|$ pairwise vertex-disjoint arcs from $B' \setminus B$ to $B \setminus B'$. The union of P_1 and P_2 has label $\psi(B' \setminus B) - \psi(B \setminus B') = \psi(B') - \psi(B) = \psi(B') \neq 0$ and consists of pairwise vertex-disjoint directed cycles in $D_{M_1,M_2}(B)$, hence it contains a non-zero directed cycle. ◀

The following result and proof are analogous to that of [9, Theorem 2]. In that result, a weight function is given instead of a labeling, and the constraint "non-zero" is replaced by "negative". In our setting, the proof only works if we assume $\mathbb{Z}_2 \not\leq \Gamma$, as we need to guarantee that if we decompose an arc set having label $2\psi'(C)$ for some non-zero directed cycle C, then at least one member of the decomposition has non-zero label. We give the proof in the full version.

▶ **Lemma 3.6.** *Let Γ be a group such that $\mathbb{Z}_2 \not\leq \Gamma$. Let M_1 and M_2 be matroids on a common ground set E, $\psi\colon E \to \Gamma$ a group labeling, and B a common basis. If C is a non-zero directed cycle of $D_{M_1,M_2}(B)$ whose vertex set is inclusion-wise minimal among non-zero directed cycles, then $B \triangle V(C)$ is a common basis.*

Combining Lemmas 3.5 and 3.6, we obtain the main result of the section.

▶ **Theorem 3.7.** *Let Γ be a group such that $\mathbb{Z}_2 \not\leq \Gamma$. Let M_1 and M_2 be matroids on a common ground set E, $\psi\colon E \to \Gamma$ a group labeling, and B_0 a zero common basis. Then, M_1 and M_2 have a non-zero common basis if and only if $D_{M_1,M_2}(B_0)$ contains a non-zero directed cycle. Moreover,* Non-Zero Common Basis *is polynomially solvable.*

Proof. If there exists a non-zero common basis B^*, then $D_{M_1,M_2}(B_0)$ contains a non-zero directed cycle by Lemma 3.5. Conversely, if $D_{M_1,M_2}(B_0)$ contains a non-zero directed cycle, then let C be a minimum length non-zero directed cycle. Then, Lemma 3.6 implies that $B^* := B \triangle V(C)$ is a common basis, and we have $\psi(B^*) = \psi(B_0) + \psi'(C) = \psi'(C) \neq 0$.

This provides the following algorithm for Non-Zero Common Basis. First, we find a common basis B_0. If no common basis exists or B_0 is non-zero, we are done. Otherwise, we find a minimum length non-zero directed cycle C in $D_{M_1,M_2}(B_0)$ using Theorem 3.4. If no non-zero directed cycle exists then we report that there is no non-zero common basis, otherwise we output $B_0 \triangle V(C)$. ◀

We turn to the study of Weighted Non-Zero Common Basis. Given two matroids M_1 and M_2 on a common ground set E, a common basis B, and a weight function $w\colon E \to \mathbb{R}$, we define the weight function w' on the arcs of $D_{M_1,M_2}(B)$ as follows. For each arc xy such that $x \in B$, $y \in E \setminus B$ and $B - x + y \in \mathcal{B}(M_1)$ we define $w'(xy) := w(y)$, and for each arc yx such that $x \in B$, $y \in E \setminus B$ and $B - x + y \in \mathcal{B}(M_2)$ we define $w'(yx) := -w(x)$. Then, B is a minimum-weight common basis if and only if w' is conservative [31, 21, 9], see also [46, Theorem 41.5]. We observe the following relationship between the weight of a shortest non-zero directed cycle in $D_{M_1,M_2}(B)$ and the weights of non-zero common bases of M_1 and M_2. Its simple proof can be found in the full version.

▶ **Lemma 3.8.** *Let M_1 and M_2 be matroids on a common ground set E, $\psi\colon E \to \Gamma$ a group labeling, and $w\colon E \to \mathbb{R}$ a weight function. Let B_0 be a minimum-weight common basis and assume that $\psi(B_0) = 0$. Let C be a shortest non-zero directed cycle in $D_{M_1,M_2}(B_0)$ with respect to w'. Then, $w(B_0 \triangle V(C)) \leq w(B^*)$ holds for each non-zero common basis B^*.*

We note that Lemma 3.8 generalizes Lemma 3.2, as in the special case $M_1 = M_2$ each arc of $D_{M_1,M_2}(B_0)$ is bidirectional, thus a shortest non-zero directed cycle consists of two vertices.

In Lemma 3.8, the weight of C is measured by w' (which takes negative values on some arcs), so $V(C)$ is not necessarily inclusion-wise minimal among the vertex sets of non-zero directed cycles. Thus, it does not yield an algorithm for Weighted Non-Zero Common Basis. In fact, the complexity of the problem remains open for a group Γ with $\mathbb{Z}_2 \not\leq \Gamma$. Nevertheless, we use Lemma 3.8 to give a 2-approximation if the weight function w is nonnegative. The proof of the result is given in the full version.

▶ **Theorem 3.9.** *Let Γ be a group with $\mathbb{Z}_2 \not\leq \Gamma$. Let M_1 and M_2 be matroids on a common ground set E, $\psi\colon E \to \Gamma$ a group labeling, and $w\colon E \to \mathbb{R}_{\geq 0}$ a weight function. Then, there exists a polynomial-time algorithm that computes a non-zero common basis B that satisfies $w(B) \leq 2w(B^*)$ for every non-zero common basis B^* or correctly outputs that there exists no non-zero common basis.*

3.2.2 Certificate for All Common Bases Being Zero

Given a strongly connected digraph having labels on its arcs, the fact that all directed cycles have label zero can be certified by a certain labeling of its vertices. Using this result and assuming a property of the matroid pair ensuring strong connectivity, we get a characterization for all directed cycles of $D_{M_1,M_2}(B)$ having label zero, which is analogous to the weight-splitting theorem of Frank [19]. By Theorem 3.7, this provides the following certificate for the "NO" instances of Non-Zero Common Basis if $\mathbb{Z}_2 \not\leq \Gamma$. We give details in the full paper.

▶ **Theorem 3.10.** *Let M_1 and M_2 be matroids on a common ground set E and the same rank r. Assume that $r_{M_1}(X) + r_{M_2}(E \setminus X) > r$ holds for every $\emptyset \neq X \subsetneq E$. Let B be a common basis of M_1 and M_2, and $\psi\colon E \to \Gamma$ a group labeling. Then, $D_{M_1,M_2}(B)$ contains no non-zero directed cycle if and only if there exist labelings $\psi_1, \psi_2\colon E \to \Gamma$ such that $\psi = \psi_1 + \psi_2$ and ψ_i is constant on each connected component of M_i for $i = 1, 2$.*

3.2.3 Partition matroids

When both matroids are partition matroids, we can drop the assumption $\mathbb{Z}_2 \not\leq \Gamma$ from Theorem 3.7 and extend it to the weighted setting. The proof of the next result is given in the full version.

▶ **Theorem 3.11.** Weighted Non-Zero Common Basis *is polynomially solvable if M_1 and M_2 are partition matroids.*

Given a graph G and a function $b\colon V(G) \to \mathbb{Z}_{\geq 0}$, a *perfect b-matching* is an edge set $F \subseteq E(G)$ such that $d_F(v) = b(v)$ for each $v \in V$. If G is bipartite, then its perfect b-matchings form the family of common bases of two partition matroids. Therefore, Theorem 3.11 can be formulated as having a polynomial-time algorithm for finding a minimum weight non-zero perfect b-matching in a bipartite graph with weights and labels on its edges. For perfect matchings and the group $\mathbb{Z}_2$, the idea of essentially the same algorithm as ours was briefly mentioned in [26], where the authors noted that it can also be derived from results of [1]. A formal description of the algorithm and a proof of its correctness were given in [18] for a special weight function.

Next, we consider the special case of Weighted Non-Zero Common Basis when we only assume that one of the matroids is a partition matroid. Without further assumptions, this problem is not easier than the general one: a construction similar to that of Harvey, Király and Lau [23] shows that the general problem can be reduced to the special case when one of the matroids is a unitary partition matroid and all partition classes have size two. In what follows, we will consider the case when the partition matroid is defined by a partition having two classes. In this special case, the polynomial solvability of Non-Zero Common Basis follows from the corresponding lattice basis characterization of Rieder [45]. We extend this result by solving the weighted version of the problem.

▶ **Theorem 3.12.** Weighted Non-Zero Common Basis *is polynomially solvable if M_2 is a partition matroid defined by a partition having two classes.*

The proof of the theorem is given in the full version. The proof of both Theorem 3.11 and Theorem 3.12 relies on Lemma 3.8 by observing that the special property of the matroid pair guarantees that $B_0 \triangle V(C)$ is a common basis whenever B_0 is a minimum-weight common basis having label zero and C is a shortest non-zero directed cycle in $D_{M_1,M_2}(B)$.

4 Algebraic Algorithm for F-avoiding Basis and Common Basis

We present a randomized polynomial-time algorithm for F-avoiding Common Basis for representable matroids given as matrices over a field $\mathbb{F}$ and a finite group Γ given as an operation table. Our algorithm is a generalization of the exact-weight matroid intersection algorithm for representable matroids by Camerini, Galtiati, and Maffioli [11]. A similar algebraic algorithm has also been considered by Webb [51, Section 3.7].

Before describing the algorithm, we introduce needed algebraic notions and results. We assume that the arithmetic operations and the zero test over $\mathbb{F}$ can be performed in constant time. In this section, we use the multiplicative notation for the operation of Γ, and let e denote the group unit (zero) of Γ instead of 0. The *group ring* $K[\Gamma]$ of Γ over a field K is the set of formal K-coefficient linear combinations of the elements in Γ, i.e., $K[\Gamma] \coloneqq \{ \sum_{g\in\Gamma} a_g g \mid a_g \in K \ (g \in \Gamma) \}$. The addition and multiplication of $f = \sum_{g\in\Gamma} a_g g \in K[\Gamma]$ and $h = \sum_{g\in\Gamma} b_g g \in K[\Gamma]$ are naturally defined as $f + h = \sum_{g\in\Gamma}(a_g + b_g)g$ and $fh = \sum_{g,g'\in\Gamma} a_g b_{g'} gg'$. With these operations, $K[\Gamma]$ forms a commutative ring, containing K as a subring under the natural identification $K \ni a \mapsto ae \in K[\Gamma]$. Note that the operations of $K[\Gamma]$ and the zero test can be performed in polynomially many operations of K and Γ.

For finite sets R and C, we mean by an $R \times C$ *matrix* a matrix of size $|R| \times |C|$ whose rows and columns are identified with R and C, respectively. We simply write $[r] \times C$ as $r \times C$ for $r \in \mathbb{Z}_{\geq 0}$. Given a ground set E and a labeling $\psi\colon E \to \Gamma$, we define an $E \times E$ diagonal matrix D_ψ as follows: for every $j \in E$, we set the (j, j) diagonal entry of D_ψ as $x_j\psi(j)$, where x_j is an indeterminate (variable) whose actual value comes from $\mathbb{F}$. Then, D_ψ is regarded as a matrix over the group ring $\mathbb{F}(\{x_e\}_{e\in E})[\Gamma]$, where $\mathbb{F}(\{x_e\}_{e\in E})$ denotes the rational function field over $\mathbb{F}$ in $|E|$ indeterminates $\{x_e\}_{e\in E}$.

The following is a modification of a claim of Tomizawa and Iri [50], who first used the Cauchy–Binet formula in the context of linear matroid intersection.

▶ **Lemma 4.1.** *Let $\mathbb{F}$ be a field, M_1 and M_2 $\mathbb{F}$-representable matroids with the common ground set E and the same rank r, A_k an $r \times E$ matrix representing M_k for $k = 1, 2$, and $\psi\colon E \to \Gamma$ a labeling. Let $\Xi = A_1 D_\psi A_2^\top$. Then, the coefficient of $g \in \Gamma$ in $\det(\Xi)$ is a non-zero polynomial in $\{x_j\}_{j\in E}$ if and only if a common basis with label g exists.*

Proof. By the Cauchy–Binet formula, we can expand $\det(\Xi)$ as

$$\det(\Xi) = \sum_{B\in\binom{E}{r}} \det(A_1[B]) \det(A_2[B]) \prod_{j\in B} x_j \cdot \psi(B), \tag{1}$$

where $A_k[B]$ denotes the submatrix of A_k obtained by extracting the columns in B for $k = 1, 2$. Observe that $\det(A_1[B]) \det(A_2[B])$ is non-zero if and only if B is a common basis of M_1 and M_2, and the terms coming from different common bases do not cancel out thanks to the factor $\prod_{j\in B} x_j$, proving the claim. ◀

Lemma 4.1 together with the Schwartz–Zippel lemma [36, 48, 53], division-free determinant algorithm [27], search-to-decision reduction, and the field extension for small fields give rise to a randomized algebraic algorithm for F-avoiding Common Basis. The proof of the result is given in the full version.

▶ **Theorem 4.2.** *Let $\mathbb{F}$ be a field and M_1 and M_2 $\mathbb{F}$-representable matroids with the common ground set E. There is a randomized algorithm that, given matrices A_1 and A_2 over $\mathbb{F}$ representing M_1 and M_2, respectively, the operation table of a finite abelian group Γ, a group labeling $\psi\colon E \to \Gamma$, and a forbidden label set $F \subseteq \Gamma$, solves F-avoiding Common Basis in expected polynomial time.*

A *Pfaffian pair* is a pair of $r \times n$ matrices A_1, A_2 such that $\det(A_1[B]) \det(A_2[B])$ is a non-zero constant for any common basis B [51]. This property implies that if $\mathbb{F} = \mathbb{Q}$ and matroids are given as a Pfaffian pair, then no cancel-out occurs in the summands of $\det(\Xi)$ in the equation (1) even if we substitute 1 for all x_i. Therefore, we can derandomize the algorithm given in Theorem 4.2. Examples of common bases of matroid pairs representable by Pfaffian pairs include spanning trees, regular matroid bases, arborescences, perfect matchings in Pfaffian-orientable bipartite graphs, and node-disjoint S–T paths in planar graphs [39].

▶ **Theorem 4.3.** *F-*AVOIDING COMMON BASIS *is polynomially solvable for $\mathbb{Q}$-representable matroids if matroids are given as a Pfaffian pair and a group is given as the operation table.*

We can also generalize Theorem 4.2 to a randomized pseudo-polynomial-time algorithm for the weighted problem as follows. See the full version for the proof.

▶ **Theorem 4.4.** *Let $\mathbb{F}$ be a field and M_1 and M_2 $\mathbb{F}$-representable matroids on a common ground set E. There is a randomized algorithm that, given matrices A_1 and A_2 over $\mathbb{F}$ representing M_1 and M_2, respectively, the operation table of a finite abelian group Γ, a group labeling $\psi\colon E \to \Gamma$, a forbidden label set $F \subseteq \Gamma$, and a weight function $w\colon E \to \mathbb{Z}$, solves* WEIGHTED F-AVOIDING COMMON BASIS *in pseudo-polynomial time in expectation. The algorithm can be derandomized if $\mathbb{F} = \mathbb{Q}$ and (A_1, A_2) is a Pfaffian pair.*

5 F-avoiding Basis with Fixed $|F|$

As we will see in Theorem 6.3, ZERO BASIS is hard for groups given by operation tables. This implies the hardness of F-AVOIDING BASIS if the set F of forbidden labels is part of the input. In this section, we study the problem when F has a fixed size. Note that in contrast to the setting of Section 4, we assume that Γ is given as an operation oracle (and it is not necessarily finite).

Related to the notion of k-closeness recently introduced by Liu and Xu [35], we propose the following conjecture.

▶ **Conjecture 5.1.** *Let M be a matroid, $\psi\colon E(M) \to \Gamma$ a labeling, and $F \subseteq \Gamma$ a finite collection of forbidden labels. Then, for any basis B, there exists an F-avoiding basis B^* with $|B \setminus B^*| \leq |F|$, provided that at least one F-avoiding basis exists.*

Note that Lemma 3.2 (applied with a constant weight function) implies that Conjecture 5.1 holds for $|F| = 1$. A tightness example for Conjecture 5.1 can be found in the full version. We can relax Conjecture 5.1 as follows.

▶ **Conjecture 5.2.** *There exists a function $f\colon \mathbb{N} \to \mathbb{N}$ with the following property: If M is a matroid, $\psi\colon E(M) \to \Gamma$ is a group labeling, and $F \subseteq \Gamma$ is a finite collection of forbidden labels, then, for any basis B, there exists an F-avoiding basis B^* with $|B \setminus B^*| \leq f(|F|)$, provided that at least one F-avoiding basis exists.*

Conjectures 5.1 and 5.2 have algorithmic implications due to the following simple observation.

▶ **Lemma 5.3.** *Let α be a fixed positive integer. Further, let M be a matroid, $\psi\colon E(M) \to \Gamma$ a group labeling, and $F \subseteq \Gamma$ a finite collection of forbidden labels, such that, for any basis B, there exists an F-avoiding basis B^* with $|B \setminus B^*| \leq \alpha$, provided that at least one F-avoiding basis exists. Then, an F-avoiding basis of M can be found in polynomial time, if one exists.*

Proof. We first compute an arbitrary basis B of M. Then, for every $X \subseteq B$ and every $Y \subseteq E(M) \setminus B$ with $|X| = |Y| \leq \alpha$, we test whether $(B \setminus X) \cup Y$ is an F-avoiding basis of M. As there are at most $1 + n^{\alpha}$ choices for each of X and Y, the desired running time follows. If we find an F-avoiding basis during this procedure, we return it. Otherwise, no F-avoiding basis exists by assumption. ◀

The following is an immediate consequence of Lemma 5.3.

▶ **Corollary 5.4.** *If Conjecture 5.2 holds, then* F-AVOIDING BASIS *is solvable in polynomial time if $|F|$ is fixed.*

Liu and Xu [35] defined a finite group Γ to be *k-close* for an integer $k \geq 1$, if for any matroid M, group labeling $\psi\colon E(M) \to \Gamma$, element $g \in \Gamma$ and basis B, there exists a basis B^* with $|B \setminus B^*| \leq k$ and $\psi(B^*) = g$, provided that M has at least one basis with label g. Observe that Conjecture 5.1 would imply $(|\Gamma| - 1)$-closeness, and Conjecture 5.2 would imply $f(|\Gamma| - 1)$-closeness of each finite group Γ for some function $f\colon \mathbb{N} \to \mathbb{N}$. This would imply an FPT algorithm for Zero Basis when parameterized with $|\Gamma|$ due to the following result, which is a consequence of [35, Theorem 1].

▶ **Theorem 5.5** (see Liu–Xu [35]). *Assume that for each finite group Γ, there exists an integer k such that Γ is k-close. Then,* Zero Basis *is in FPT for finite groups when parameterized by $|\Gamma|$.*

Liu and Xu [35] observed that if all subgroups of Γ satisfy a conjecture by Schrijver and Seymour [47], then Γ is $(|\Gamma| - 1)$-close. By the results of DeVos, Goddyn, and Mohar [13], this implies that any cyclic group Γ is $(|\Gamma| - 1)$-close whose order is a prime power or the product of two primes. The proof of [35, Theorem 4] does not seem to generalize to our setting. Thus, it is not clear whether the conjecture of Schrijver and Seymour implies Conjecture 5.1. If Γ has prime order, then Liu and Xu [35, Theorem 3] gave a simpler proof of $(|\Gamma| - 1)$-closeness. That proof also generalizes to show that Conjecture 5.1 holds for such groups.

Using the results of Lemos [34], we can also prove that Conjecture 5.1 holds for *ordered groups*, which is a group Γ equipped with a total order $\leq$ on Γ such that $a \leq b$ implies $a + c \leq b + c$ for all $a, b, c \in \Gamma$. The result is restated in the following theorem, whose proof can be found in the full version.

▶ **Theorem 5.6.** *Let M be a matroid, $\psi\colon E(M) \to \Gamma$ a labeling to an ordered group Γ, $F \subseteq \Gamma$ a finite collection of forbidden labels, B a basis of M, and suppose that M has an F-avoiding basis. Then, there exists an F-avoiding basis B^* of M with $|B^* \setminus B| \leq |F|$.*

5.1 Strongly Base Orderable Matroids and Relaxations

In this section, we introduce a relaxed notion of strong base-orderability, called (α, k)-weak base orderability, where α and k are positive integers. In Section 5.1.1, we define this notion and show its relation to strong base-orderability and group-restricted bases. In Section 5.1.2 and Section 5.1.3, we conclude results for matroids representable over fixed finite fields and graphic matroids, respectively.

5.1.1 (α, k)-Weakly Base Orderable Matroids

A matroid is called *strongly base orderable* if for any two bases B_1, B_2, there exists a bijection $\varphi\colon B_1 \setminus B_2 \to B_2 \setminus B_1$ such that $(B_1 \setminus Z) \cup \varphi(Z)$ is a basis for each $Z \subseteq B_1 \setminus B_2$. For some positive integer k, we say that the ordered basis pair (B_1, B_2) has the *k-exchange property* if there exist pairwise disjoint nonempty subsets $X_1, \ldots, X_k \subseteq B_1 \setminus B_2$ and $Y_1, \ldots, Y_k \subseteq B_2 \setminus B_1$ such that $\left(B_1 \setminus \bigcup_{i \in Z} X_i\right) \cup \bigcup_{i \in Z} Y_i$ is a basis for each $Z \subseteq [k]$. For positive integers α and k, we define a matroid M to be *weakly (α, k)-base orderable* if the ordered pair (B_1, B_2) has the k-exchange property for any two bases B_1, B_2 of M with $|B_1 \setminus B_2| \geq \alpha$. We note that (α, k)-weak base orderability is a relaxation of *k-base orderability* defined by Bonin and Savitsky [7], and our definition of the k-exchange property differs from their definition of k-exchange-ordering. Observe that strongly base orderable matroids are precisely the matroids that are (k, k)-weakly base orderable for each $k \geq 1$.

For a matroid M and two disjoint bases B_1, B_2 of M with $B_1 \cup B_2 = E(M)$, we say that (B_1, B_2) is a *basis partition* of M. For a basis B of a matroid M, we say that a minor M' of M is a *B-minor* if it is obtained by contracting some elements of B and deleting some elements of $E(M) \setminus B$. We use the following simple observation later, whose proof can be found in the full version.

▶ **Lemma 5.7.** *Let B_1 and B_2 be two bases of a matroid M. Further, let M' be a B_1-minor of M such that (B_1', B_2') is a basis partition of M' and has the k-exchange property for some $k \in \mathbb{N}$, where $B_i' \coloneqq B_i \cap E(M')$ for $i = 1, 2$. Then (B_1, B_2) has the k-exchange property in M.*

The following result is our main motivation to consider weak base orderability. It establishes a connection between weak base orderability and Conjecture 5.2.

▶ **Theorem 5.8.** *Let M be a matroid, $\psi\colon E(M) \to \Gamma$ a group labeling, and $F \subseteq \Gamma$ a finite collection of forbidden labels. If M is $(\alpha, |F|+1)$-weakly base orderable, then for each basis B, there exists an F-avoiding basis B^* with $|B \setminus B^*| \leq \alpha - 1$, provided that at least one F-avoiding basis exists.*

For the proof, we need the following result, which is most likely routine; see the full version for the proof.

▶ **Proposition 5.9.** *Let S be a finite set, $\psi\colon S \to \Gamma$ a group labeling, and $0 \notin F \subseteq \Gamma$ satisfying $|F| \leq |S| - 1$. Then, there exists some nonempty $S' \subseteq S$ with $\psi(S') \notin F$.*

Proof of Theorem 5.8. Let $k \coloneqq |F|$ and let B be a basis and B' an F-avoiding basis minimizing $|B' \setminus B|$. If $|B' \setminus B| \leq \alpha - 1$, there is nothing to prove. We may hence suppose that $|B' \setminus B| \geq \alpha$. Then, as M is $(\alpha, k+1)$-weakly base orderable, there exist pairwise disjoint nonempty subsets $X_1, \ldots, X_{k+1} \subseteq B' \setminus B$ and $Y_1, \ldots, Y_{k+1} \subseteq B \setminus B'$ such that $\left(B' \setminus \bigcup_{i \in Z} X_i\right) \cup \bigcup_{i \in Z} Y_i$ is a basis for each $Z \subseteq [k+1]$. We define $\psi'\colon [k+1] \to \Gamma$ by $\psi'(i) = \psi(Y_i) - \psi(X_i)$ for all $i \in [k+1]$. Observe that $0 \notin F' \coloneqq \{\, f - \psi(B') \mid f \in F \,\}$, as B' is an F-avoiding basis. It hence follows from Proposition 5.9 that there exists some nonempty $Z \subseteq [k+1]$ with $\psi'(Z) \notin F'$. Let $B'' \coloneqq \left(B' \setminus \bigcup_{i \in Z} X_i\right) \cup \bigcup_{i \in Z} Y_i$. By the definition of $X_1, \ldots, X_{k+1}$ and $Y_1, \ldots, Y_{k+1}$, we obtain that B'' is a basis of M. Further, we have $\psi(B'') = \psi(B') + \psi'(Z) \notin F$. Finally, we have $|B'' \setminus B| < |B' \setminus B|$ since Z is nonempty. This contradicts the choice of B'. ◀

As strongly base orderable matroids are (k, k)-weakly base orderable for any $k \geq 1$, we also get the following.

▶ **Corollary 5.10.** *Strongly base orderable matroids satisfy Conjecture 5.1.*

A connection of the results obtained in this section with certain orderings of elements of matroids introduced by Baumgart [3] can be found in the full version.

5.1.2 Matroids Representable over Finite Fields

In this section, we prove that the concept of weakly base orderability allows us to deal with a large class of matroids, namely all those which are representable over a fixed finite field. More precisely, we prove the following result.

▶ **Theorem 5.11.** *There is a function $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for every prime power q, every $\mathrm{GF}(q)$-representable matroid is weakly $(f(q,k), k)$-orderable for any positive integer k.*

On a high level, the proof works in the following way. First, relying on results of [15] on the existence of certain submatrices of large matrices over finite fields, we show that every GF(q)-representable matroid has a certain substructure. We then show that this substructure has the desired property. From this, we can conclude the theorem.

In order to find this substructure, we deal with the matrices representing the matroids in consideration. We first need some notation for these matrices. For two matrices A and A', we say that A contains A' as a *permuted submatrix* if A' can be obtained from A by deleting and permuting rows and columns. For a square matrix, we refer by its *size* to its number of rows. Let q be a prime power. We say that a triple (α, β, γ) of elements of GF(q) is *feasible* if $\alpha \neq \beta$ and at least one of $\beta \neq 0$ and $\gamma \neq 0$ hold. For a triple (α, β, γ) and a positive integer t, the (α, β, γ)-*diagonal matrix* of size t is the $t \times t$ matrix $A = (A_{ij})$ such that for $i, j \in [t]$, we have $A_{ij} = \alpha$ if $i < j$, $A_{ii} = \beta$ if $i = j$, and $A_{ij} = \gamma$ if $i > j$. We now collect some properties of (α, β, γ)-diagonal matrices. We first need the following result showing that (α, β, γ)-diagonal matrices can always be found in sufficiently large matrices over a fixed finite field. The following result can easily be concluded from a slightly weaker result due to Ding, Oporowski, Oxley, and Vertigan [15]. Its detailed proof can be found in the full version.

▶ **Proposition 5.12.** *There is a computable function $f_1 \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the following property: Let q be a prime power, t a positive integer, and A a matrix over* GF(q) *having at least $f_1(q, t)$ columns no two of which are identical. Then, A contains a permuted square submatrix A' of size t which is (α, β, γ)-diagonal for a feasible triple (α, β, γ).*

We are now ready to give the following result showing that every sufficiently large matroid that is representable over a fixed finite field has a certain substructure. The approach is to choose a matrix representing the matroid and find a particular submatrix in this matrix using Proposition 5.12. After, we show that a minor represented by this matrix can be obtained by applying certain deletions and contractions. The detailed proof can be found in the full version.

▶ **Lemma 5.13.** *There is a computable function $f_1 \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the following properties: Let q be a prime power, k a positive integer, M a* GF(q)*-representable matroid of rank at least $f_1(q, k)$ and (B_1, B_2) a basis partition of M. Then, there exists a B_1-minor M' of M that can be represented by a matrix of the form $[I_k\ A]$, where I_k is the identity matrix of size k and A is an (α, β, γ)-diagonal matrix for a feasible triple (α, β, γ), and the columns of I_k correspond to the elements of B'_1 and those of A correspond to the elements of B'_2, where $B'_i \coloneqq B_i \cap E(M')$ for $i = 1, 2$.*

We will prove Theorem 5.11 by showing that matroids representable by a very specific class of matrices satisfy its conclusion. For this, we need a statement showing that certain matrices are nonsingular, which we derive from an explicit formula for the determinants of (α, β, γ)-triangular matrices due to Efimov [17]. The detailed proof can be found in the full version.

▶ **Proposition 5.14.** *Let q be a prime power, (α, β, γ) a feasible triple, t a multiple of $q(q-1)$, and A the (α, β, γ)-diagonal matrix of size t. Then, A is nonsingular.*

We are now ready to conclude the result for the specific class of matroids.

▶ **Lemma 5.15.** *There is a computable function $f_2 \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the following properties: Let q be a prime power, k a positive integer, and M a matroid that can be represented by $[I\ A]$ over* GF(q)*, where I is an identity matrix of size $f_2(q, k)$ and A is an (α, β, γ)-diagonal* *matrix of the same size for a feasible triple* (α, β, γ)*. Next, let* B_1 *and* B_2 *be the subsets of* $E(M)$ *corresponding to* I *and* A*, respectively. Then,* (B_1, B_2) *is a basis partition of* M *and has the* k*-exchange property.*

Proof. Let f_2 be the function defined by $f_2(q, k) \coloneqq q(q-1)k$ for all positive integers q and k. By Proposition 5.14, we have that A is nonsingular and hence (B_1, B_2) is a basis partition of M. For $i \in [k]$, let X_i be the subset of B_1 and Y_i be the subset of B_2 that corresponds to the columns of indices $q(q-1)(i-1)+1$ to $q(q-1)i$ of I and A, respectively. For $Z \subseteq [k]$, let $B_Z \coloneqq \left(B_1 \setminus \bigcup_{i \in Z} X_i\right) \cup \bigcup_{i \in Z} Y_i$. It suffices to prove that B_Z is a basis of M for every $Z \subseteq [k]$. To this end, consider some fixed $Z \subseteq [k]$. Observe that the matrix obtained from restricting $[I\ A]$ to the columns corresponding to B_Z can be transformed into a matrix of the form $A^* = \begin{bmatrix} I' & A_1 \\ O & A' \end{bmatrix}$ by exchanging rows and columns. Here, I' is the identity matrix of size $q(q-1)(k-|Z|)$, O is a zero matrix, A' is an (α, β, γ)-diagonal matrix of size $q(q-1)|Z|$, and A_1 is an arbitrary matrix. As the size of A' is divisible by $q(q-1)$, we obtain by Proposition 5.14 that A' is nonsingular. It follows that A^* is nonsingular, and hence B_Z is independent. As $|B_Z| = |B_1|$ by construction, we obtain that B_Z is a basis of M. This finishes the proof. ◀

Finally, we combine Lemmas 5.7, 5.13, and 5.15 to conclude Theorem 5.11.

Proof of Theorem 5.11. We prove the statement for the function $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(q, k) \coloneqq f_1(q, f_2(q, k))$ for each $k \in \mathbb{N}$ and prime power q. Let B_1 and B_2 be bases of a $\mathrm{GF}(q)$-representable matroid M with $|B_1 \setminus B_2| \geq f(q, k)$. We need to prove that (B_1, B_2) has the k-exchange property. Let $M' \coloneqq M \,/\, (B_1 \cap B_2) \setminus (E(M) \setminus (B_1 \cup B_2))$. Further, for $i = 1, 2$, let $B_i' \coloneqq B_i \cap E(M')$ and observe that (B_1', B_2') is a basis partition of M'. It follows from Lemma 5.13 that there exists a B_1'-minor M'' of M' that can be represented by a matrix of the form $[I\ A]$, where I is the identity matrix of size $f_2(q, k)$, A is an (α, β, γ)-diagonal matrix of size $f_2(q, k)$ for a feasible triple (α, β, γ) and the columns of I and A correspond to the elements of B_1'' and B_2'', respectively, where $B_i'' \coloneqq B_i' \cap E(M'')$ for $i = 1, 2$. We now obtain from Lemma 5.15 that (B_1'', B_2'') is a basis partition of M'' and has the k-exchange property in M''. As M'' is a B_1-minor of M, we now obtain from Lemma 5.7 that (B_1, B_2) has the k-exchange property in M. ◀

Combining Theorems 5.8 and 5.11, Lemma 5.3, and Theorem 5.5, we get the following.

▶ **Corollary 5.16.** *Let* q *be a prime power,* M *a* $\mathrm{GF}(q)$*-representable matroid,* $\psi\colon E \to \Gamma$ *a group labeling and* $F \subseteq \Gamma$ *a finite set of forbidden labels. When* $|F|$ *is fixed,* F-Avoiding Basis *is solvable in polynomial time. Moreover, if* $|\Gamma|$ *is finite, then* Zero Basis *is in FPT when parameterized by* $|\Gamma|$*.*

We note that Corollary 5.16 is not implied by Theorem 4.2. The former applies to arbitrary groups, while the latter is limited to finite groups given by an operation table. Furthermore, Corollary 5.16 gives a deterministic polynomial-time algorithm, in contrast to the randomized algorithm in Theorem 4.2.

5.1.3 Graphic matroids

As a strengthening of the k-exchange property, we say that the basis pair (B_1, B_2) of a matroid has the *elementary* k*-exchange property* if there exist k-element subsets $X \subseteq B_1 \setminus B_2$ and $Y \subseteq B_2 \setminus B_1$ and a bijection $\varphi\colon X \to Y$ such that $(B_1 \setminus Z) \cup \varphi(Z)$ is a basis for each $Z \subseteq X$. Note that this is equivalent to requiring $|X_i| = |Y_i| = 1$ for each $i \in [k]$ in the definition of the k-exchange property. We define a matroid M to be *elementarily* (α, k)*-weakly base orderable* if (B_1, B_2) has the elementary k-exchange property for any pair of basis B_1 and B_2 with $|B_1 \setminus B_2| \geq \alpha$.

It turns out that all regular matroids are elementarily $(f(k), k)$-weakly base orderable for some large function $f\colon \mathbb{N} \to \mathbb{N}$, while the same is not true for binary matroids. The proofs of these results can be found in the full version. As graphic matroids are regular, they are elementarily $(f(k), k)$-weakly base orderable for some large function $f\colon \mathbb{N} \to \mathbb{N}$. We give a proof in the full version, independent from the proof of Theorem 5.11, which shows that for graphic matroids, there exists such a function f satisfying $f(k) = O(k^3)$.

▶ **Theorem 5.17.** *Graphic matroids are elementarily* $(3k^3, k)$*-weakly base orderable for any* $k \geq 1$.

5.2 Two forbidden labels

The objective of this section is to prove the following restatement of the case $|F| = 2$ of Conjecture 5.1. Its proof can be found in the full version. Vaguely speaking, we first reduce the problem to matroids on six elements and then combine some earlier results with a particular treatment for the cycle matroid of K_4.

▶ **Theorem 5.18.** *Let* M *be a matroid,* $\psi\colon E(M) \to \Gamma$ *a group labeling, and let* F *be a 2-element subset of* Γ*. For any basis* B*, there exists an* F*-avoiding basis* B^* *such that* $|B \setminus B^*| \leq 2$*, provided that there exists at least one* F*-avoiding basis.*

6 Hardness and Negative Results

In this section, we give the algorithmic hardness results and counterexamples contained in this work. Sections 6.1 and 6.2 contain algorithmic intractability results and Section 6.3 contains a counterexample to a conjecture of Liu and Xu [35]. All proofs can be found in the full version.

6.1 Hardness of Non-zero Common Basis with $\mathbb{Z}_2 \leq \Gamma$

We here show that Non-Zero Common Basis is intractable for any group Γ such that $\mathbb{Z}_2 \leq \Gamma$. This implies that the condition on Γ in Theorem 3.7 is crucial indeed.

▶ **Theorem 6.1.** Non-Zero Common Basis *requires an exponential number of independence queries for any fixed group* Γ *such that* $\mathbb{Z}_2 \leq \Gamma$*.*

Our proof of Theorem 6.1 provides a new and simpler proof of the result of Bérczi and Schwarcz [5] showing that the problem of partitioning the ground set into common bases is hard. In addition to this new proof, we also describe the relation of a relaxation of that problem to a problem on non-zero common bases via dual lattices in the full version.

6.2 Hardness of Zero Basis

In this section, we show two hardness results for Zero Basis. The first one shows that the problem is hard even for uniform matroids by using the hardness of the well-known Subset Sum problem.

▶ **Theorem 6.2.** Zero Basis *is* NP-hard *for a uniform matroid and* $\Gamma = \mathbb{Z}$*.*

It can be derived from [16, Theorem 1.3] that Zero Basis is also hard for finite groups given as operation tables.

▶ **Theorem 6.3** (see Doron-Arad–Kulik–Shachnai [16, Theorem 1.3]). Zero Basis *requires an exponential number of independence queries for a finite group* Γ *given as an operation table.*

Recall that (Weighted) Zero Basis is solvable if Γ is a fixed, finite group [35]. In contrast, Theorem 6.1 implies that Non-Zero Common Basis is hard for any fixed group Γ such that $\mathbb{Z}_2 \leq \Gamma$. By modifying that proof, the hardness of Zero Common Basis follows even when the assumption $\mathbb{Z}_2 \leq \Gamma$ is dropped.

▶ **Theorem 6.4.** Zero Common Basis *requires an exponential number of independence queries for any nontrivial fixed group* Γ*.*

6.3 Counterexample to a Conjecture of Liu and Xu

Liu and Xu [35] proposed a conjecture which is even stronger than the implications from Conjectures 5.1 and 5.2. In order to state their conjecture, we need the following definition. For a finite abelian group Γ its *Davenport constant* $D(\Gamma)$ is defined as the minimum value such that every sequence of elements from Γ of length $D(\Gamma)$ contains a nonempty subsequence with sum 0. Liu and Xu proposed the following conjecture.

▶ **Conjecture 6.5** (Liu–Xu [35]). *Let* Γ *be a finite abelian group. Then,* Γ *is* $(D(\Gamma) - 1)$*-close.*

We provide a counterexample for Conjecture 6.5. More precisely, we prove the following result.

▶ **Theorem 6.6.** *Let* $\Gamma = \mathbb{Z}_2^d$ *for some* $d \geq 4$*. Then,* Γ *is not* $(D(\Gamma) - 1)$*-close.*

7 Conclusion

In this work, we have treated several problem settings on finding bases of group-labeled matroids whose labels satisfy certain conditions. Many questions remain open. In Section 3.2, we deal with Weighted Non-Zero Common Basis for groups Γ with $\mathbb{Z}_2 \not\leq \Gamma$ and give an approximation algorithm and exact algorithms for some special cases. However, the general complexity of Weighted Non-Zero Basis for $\mathbb{Z}_2 \not\leq \Gamma$ remains open. In Section 4, randomized algebraic algorithms turn out to be a powerful tool for finding bases and common bases of certain labels. It would be interesting to see whether more of the problems that can be solved by these randomized algorithms can also be solved deterministically. For example, one could consider Non-Zero Common Basis for arbitrary groups when one of the matroids is graphic, and the other one is a partition matroid. Finally, while Conjectures 5.1 and 5.2 remain wide open, the following stronger conjecture can be formulated analogously to the notion of strongly k-closeness introduced by Liu and Xu [35]. Note that the conjecture holds for $|F| = 1$ by Lemma 3.2, and it can also be shown that it holds for strongly base orderable matroids.

▶ **Conjecture 7.1.** *Let* M *be a matroid on a ground set* E*,* $\psi\colon E \to \Gamma$ *a group labeling,* $F \subseteq \Gamma$ *a finite subset, and* $w\colon E \to \mathbb{R}$ *a weight function. Suppose that* M *has an* F*-avoiding basis. Then, for any minimum weight basis* B*, there exists a minimum weight* F*-avoiding basis* B^* *such that* $|B \setminus B^*| \leq |F|$*.*

References

1 Stephan Artmann, Robert Weismantel, and Rico Zenklusen. A strongly polynomial algorithm for bimodular integer linear programming. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2017)*. ACM, 2017. doi:10.1145/3055399.3055473.

2 Francisco Barahona and William R. Pulleyblank. Exact arborescences, matchings and cycles. *Discrete Applied Mathematics*, 16(2):91–99, 1987. doi:10.1016/0166-218x(87)90067-9.

3 Matthias Baumgart. *Ranking and ordering problems of spanning trees.* PhD thesis, Technische Universität München, München, 2009.

4 Kristóf Bérczi, Gergely Csáji, and Tamás Király. On the complexity of packing rainbow spanning trees. *Discrete Mathematics*, 346(4):113297, 2023. doi:10.1016/j.disc.2022.113297.

5 Kristóf Bérczi and Tamás Schwarcz. Complexity of packing common bases in matroids. *Mathematical Programming*, 188(1):1–18, 2021. doi:10.1007/s10107-020-01497-y.

6 Nayantara Bhatnagar, Dana Randall, Vijay V. Vazirani, and Eric Vigoda. Random bichromatic matchings. *Algorithmica*, 50(4):418–445, 2007. doi:10.1007/s00453-007-9096-4.

7 Joseph E. Bonin and Thomas J. Savitsky. An infinite family of excluded minors for strong base-orderability. *Linear Algebra and its Applications*, 488:396–429, 2016. doi:10.1016/j.laa.2015.09.055.

8 André Bouchet. Greedy algorithm and symmetric matroids. *Mathematical Programming*, 38(2):147–159, 1987. doi:10.1007/BF02604639.

9 Carl Brezovec, Gérard Cornuéjols, and Fred Glover. Two algorithms for weighted matroid intersection. *Mathematical Programming*, 36(1):39–53, 1986. doi:10.1007/bf02591988.

10 Richard A. Brualdi. Comments on bases in dependence structures. *Bulletin of the Australian Mathematical Society*, 1(2):161–167, 1969. doi:10.1017/s000497270004140x.

11 Paolo M. Camerini, Giulia Galbiati, and Francesco Maffioli. Random pseudo-polynomial algorithms for exact matroid problems. *Journal of Algorithms*, 13(2):258–273, 1992. doi:10.1016/0196-6774(92)90018-8.

12 Maria Chudnovsky, Jim Geelen, Bert Gerards, Luis Goddyn, Michael Lohman, and Paul Seymour. Packing non-zero A-paths in group-labelled graphs. *Combinatorica*, 26(5):521–532, 2006. doi:10.1007/s00493-006-0030-1.

13 Matt DeVos, Luis Goddyn, and Bojan Mohar. A generalization of Kneser's Addition Theorem. *Advances in Mathematics*, 220(5):1531–1548, 2009. doi:10.1016/j.aim.2008.11.003.

14 Reinhard Diestel. *Graph Theory*, volume 173 of *Graduate Texts in Mathematics*. Springer, Berlin, fifth edition, 2017.

15 Guoli Ding, Bogdan Oporowski, James Oxley, and Dirk Vertigan. Unavoidable minors of large 3-connected binary matroids. *Journal of Combinatorial Theory, Series B*, 66(2):334–360, 1996. doi:10.1006/jctb.1996.0026.

16 Ilan Doron-Arad, Ariel Kulik, and Hadas Shachnai. Lower bounds for matroid optimization problems with a linear constraint. In *51th International Colloquium on Automata, Languages, and Programming (ICALP 2024)*, 2024. To appear. arXiv:2307.07773.

17 Dmitry Efimov. Determinant of three-layer Toeplitz matrices. *Journal of Integer Sequences*, 24(2):3, 2021.

18 Nicolas El Maalouly, Raphael Steiner, and Lasse Wulf. Exact matching: Correct parity and FPT parameterized by independence number. In *34th International Symposium on Algorithms and Computation (ISAAC 2023)*, pages 28:1–28:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. doi:10.4230/LIPICS.ISAAC.2023.28.

19 András Frank. A weighted matroid intersection algorithm. *Journal of Algorithms*, 2(4):328–336, 1981. doi:10.1016/0196-6774(81)90032-8.

20 András Frank. *Connections in Combinatorial Optimization*, volume 38 of *Oxford Lecture Series in Mathematics and its Applications*. Oxford University Press, Oxford, 2011.

21 Satoru Fujishige. A primal approach to the independent assignment problem. *Journal of the Operations Research Society of Japan*, 20(1):1–15, 1977. doi:10.15807/jorsj.20.1.

22 Anna Galluccio and Martin Loebl. On the theory of Pfaffian orientations. I. Perfect matchings and permanents. *The Electronic Journal of Combinatorics*, 6(1), 1998. doi:10.37236/1438.

23 Nicholas J. A. Harvey, Tamás Király, and Lap Chi Lau. On disjoint common bases in two matroids. *SIAM Journal on Discrete Mathematics*, 25(4):1792–1803, 2011. doi:10.1137/100815232.

24 Florian Hörsch, Tomáš Kaiser, and Matthias Kriesell. Rainbow bases in matroids. *arXiv preprint*, 2022. arXiv:2206.10322.

25 Yoichi Iwata and Yutaro Yamaguchi. Finding a shortest non-zero path in group-labeled graphs. *Combinatorica*, 42(S2):1253–1282, 2022. doi:10.1007/s00493-021-4736-x.

26 Xinrui Jia, Ola Svensson, and Weiqiang Yuan. The exact bipartite matching polytope has exponential extension complexity. In *Proceedings of the 34th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2023)*, pages 1635–1654. SIAM, 2023. doi:10.1137/1.9781611977554.ch61.

27 Erich Kaltofen and Gilles Villard. On the complexity of computing determinants. *Computational Complexity*, 13(3-4):91–130, 2005. doi:10.1007/s00037-004-0185-3.

28 Yasushi Kawase, Yusuke Kobayashi, and Yutaro Yamaguchi. Finding a path with two labels forbidden in group-labeled graphs. *Journal of Combinatorial Theory, Series B*, 143:65–122, 2020. doi:10.1016/j.jctb.2019.12.001.

29 Donggyu Kim, Duksang Lee, and Sang-il Oum. Γ-graphic delta-matroids and their applications. *Combinatorica*, 43(5):963–983, 2023. doi:10.1007/s00493-023-00043-6.

30 Stein Krogdahl. A combinatorial base for some optimal matroid intersection algorithms. Technical Report STAN-CS-74-468, Computer Science Department, Stanford University, Stanford, CA, 1974.

31 Stein Krogdahl. A combinatorial proof for a weighted matroid intersection algorithm. Technical Report Computer Science Report 17, Institute of Mathematical and Physical Sciences, University of Tromso, Tromso, 1976.

32 Stein Krogdahl. The dependence graph for bases in matroids. *Discrete Mathematics*, 19(1):47–59, 1977. doi:10.1016/0012-365X(77)90118-2.

33 Andrea S. Lapaugh and Christos H. Papadimitriou. The even-path problem for graphs and digraphs. *Networks*, 14(4):507–513, 1984. doi:10.1002/net.3230140403.

34 Manoel Lemos. Weight distribution of the bases of a matroid. *Graphs and Combinatorics*, 22(1):69–82, 2006. doi:10.1007/s00373-005-0648-6.

35 Siyue Liu and Chao Xu. On the congruency-constrained matroid base. In *Proceedings of the 25th Conference on Integer Programming and Combinatorial Optimization (IPCO '24)*, 2024. To appear. arXiv:2311.11737.

36 László Lovász. On determinants, matchings, and random algorithms. In Lothar Budach, editor, *Fundamentals of Computation Theory, FCT '79, Proceedings of the Conference on Algebraic, Arthmetic, and Categorial Methods in Computation Theory*, pages 565–574. Akademie-Verlag, Berlin, 1979.

37 László Lovász. Some algorithmic problems on lattices. In László Lovász and Endre Szemerédi, editors, *Theory of algorithms*, volume 44 of *Colloquia Mathematica Societatis János Bolyai*, pages 323–337. North-Holland, Amsterdam, 1985.

38 László Lovász. Matching structure and the matching lattice. *Journal of Combinatorial Theory, Series B*, 43(2):187–222, 1987. doi:10.1016/0095-8956(87)90021-9.

39 Kazuki Matoya and Taihei Oki. Pfaffian pairs and parities: counting on linear matroid intersection and parity problems. *SIAM Journal on Discrete Mathematics*, 36(3):2121–2158, 2022. doi:10.1137/21M1421751.

40 Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987. doi:10.1007/bf02579206.

41 Martin Nägele, Richard Santiago, and Rico Zenklusen. Congruency-constrained TU problems beyond the bimodular case. *Mathematics of Operations Research*, 2023. doi:10.1287/moor.2023.1381.

42 Martin Nägele, Benny Sudakov, and Rico Zenklusen. Submodular minimization under congruency constraints. *Combinatorica*, 39(6):1351–1386, 2019. doi:10.1007/s00493-019-3900-1.

43 Martin Nägele and Rico Zenklusen. A new contraction technique with applications to congruency-constrained cuts. *Mathematical Programming*, 183(1):455–481, 2020. doi:10.1007/s10107-020-01498-x.

44 Christos H. Papadimitriou and Mihalis Yannakakis. The complexity of restricted spanning tree problems. *Journal of the ACM*, 29(2):285–309, 1982. doi:10.1145/322307.322309.

45 Jörg Rieder. The lattices of matroid bases and exact matroid bases. *Archiv der Mathematik*, 56(6):616–623, 1991. doi:10.1007/bf01246778.

46 Alexander Schrijver. *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, Berlin, 2003.

47 Alexander Schrijver and Paul D. Seymour. Spanning trees of different weights. In William J. Cook and Paul D. Seymour, editors, *Polyhedral Combinatorics*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, pages 281–288. DIMACS/AMS, 1990. doi:10.1090/DIMACS/001/21.

48 Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980. doi:10.1145/322217.322225.

49 Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In *Proceedings of the 58th Annual Symposium on Foundations of Computer Science (FOCS 2017)*. IEEE, 2017. doi:10.1109/focs.2017.70.

50 Nobuaki Tomizawa and Masao Iri. An algorithm for determining the rank of a triple matrix product AXB with application to the problem of discerning the existence of the unique solution in a network (in Japanese). *Electronics and Communications in Japan*, 57(11):50–57, 1974.

51 Kerri P. Webb. *Counting Bases*. PhD thesis, University of Waterloo, Waterloo, ON, 2004.

52 Raphael Yuster. Almost exact matchings. *Algorithmica*, 63(1–2):39–50, 2012. doi:10.1007/s00453-011-9519-0.

53 Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W Ng, editor, *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, Berlin, 1979. doi:10.1007/3-540-09519-5_73.