Isolating a Vertex via Lattices: Polytopes with Totally Unimodular Faces

Rohit Gurjar*[1], Thomas Thierauf†[2], and Nisheeth K. Vishnoi[3]

[1]California Institute of Technology, USA
[2]Aalen University, Germany
[3]École Polytechnique Fédérale de Lausanne (EPFL), Switzerland

Abstract

We present a geometric approach towards derandomizing the Isolation Lemma by Mulmuley, Vazirani, and Vazirani. In particular, our approach produces a quasi-polynomial family of weights, where each weight is an integer and quasi-polynomially bounded, that can isolate a vertex in any 0/1 polytope for which each face lies in an affine space defined by a totally unimodular matrix. This includes the polytopes given by totally unimodular constraints and generalizes the recent derandomization of the Isolation Lemma for bipartite perfect matching and matroid intersection. We prove our result by associating a lattice to each face of the polytope and showing that if there is a totally unimodular kernel matrix for this lattice, then the number of vectors of length within 3/2 of the shortest vector in it is polynomially bounded. The proof of this latter geometric fact is combinatorial and follows from a polynomial bound on the number of circuits of size within 3/2 of the shortest circuit in a regular matroid. This is the technical core of the paper and relies on a variant of Seymour's decomposition theorem for regular matroids. It generalizes an influential result by Karger on the number of minimum cuts in a graph to regular matroids.

*The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 257575 and from the Israel Science Foundation (grant number 552/16).

†Supported by DFG grant TH 472/4.

Contents

1 Introduction

The Isolation Lemma by Mulmuley, Vazirani, and Vazirani [14] states that for any given family of subsets of a ground set E, if we assign random weights (bounded in magnitude by $\text{poly}(|E|)$) to the elements of E then, with high probability, the minimum weight set in the family is unique. Such a weight assignment is called an *isolating weight assignment*. The lemma was introduced in the context of randomized parallel algorithms for the matching problem. Since then it has found numerous other applications, in both algorithms and complexity: e.g., a reduction from CLIQUE to UNIQUE-CLIQUE [14], $\text{NL/poly} \subseteq \oplus\text{L/poly}$ [31], $\text{NL/poly} = \text{UL/poly}$ [19], an RNC-algorithm for linear matroid intersection [16], and an RP-algorithm for disjoint paths [4]. In all of these results, the Isolation Lemma is the only place where they need randomness. Thus, if the Isolation Lemma can be derandomized, i.e., if a polynomially bounded isolating weight assignment can be deterministically constructed, then the aforementioned results that rely on it can also be derandomized. In particular, it will give a deterministic parallel algorithm for matching.

A simple counting argument shows that a single weight assignment with polynomially bounded weights cannot be isolating for all possible families of subsets of E. We can relax the question and ask if we can construct a poly-size list of poly-bounded weight assignments such that for each family $\mathcal{B} \subseteq 2^E$, one of the weight assignments in the list is isolating. Unfortunately, even this can be shown to be impossible via arguments involving the polynomial identity testing (PIT) problem. The PIT problem asks if an implicitly given multivariate polynomial is identically zero. Derandomization of PIT is another important consequence of derandomizing the Isolation Lemma. Here, the Isolation Lemma is applied to the family of monomials present in the polynomial. In essence, if we have a small list of weight assignments that works for all families, then we will have a small hitting-set for all small degree polynomials, which is impossible (see [2]). Once we know that a deterministic isolation is not possible for all families, a natural question is to solve the isolation question for families $\mathcal{B}$, that have a succinct representation, for example, the family of perfect matchings of a graph.

For the general setting of families with succinct representations, no deterministic isolation is known, other than the trivial construction with exponentially large weights. In fact, derandomizing the isolation lemma in this setting will imply circuit lower bounds [2]. Efficient deterministic isolation is known only for very special kinds of families, for example, perfect matchings in some special classes of graphs [1, 6, 7, 10], s-t paths in directed graphs [5, 12, 30]. Recently, there has been significant progress on deterministic isolation for perfect matchings in bipartite graphs [8] and subsequently, in general graphs [27], and matroid intersection [11], which implied quasi-NC algorithms for these problems.

Motivated by these recent works, we give a generic approach towards derandomizing the Isolation Lemma. We show that the approach works for a large class of combinatorial polytopes and conjecture that it works for a significantly larger class. For a family of sets $\mathcal{B} \subseteq 2^E$, define the polytope $P(\mathcal{B}) \subseteq \mathbb{R}^E$ to be the convex hull of the indicator vectors of the sets in $\mathcal{B}$. Our main result shows that for $m := |E|$, there exists an $m^{O(\log m)}$-sized family of weight assignments on E with weights bounded by $m^{O(\log m)}$ that is isolating for any family $\mathcal{B}$ whose corresponding polytope $P(\mathcal{B})$ satisfies the following property: *the affine space spanned by any face of $P(\mathcal{B})$ is parallel to the null space of* **some** *totally unimodular (TU) matrix*; see Theorem 2.3. This is a black-box weight construction in the sense that it does not need the description of the family or the polytope.

A large variety of polytopes satisfy this property and, as a consequence, have been extensively studied in combinatorial optimization. The simplest such class is when the polytope $P(\mathcal{B})$ has a description $Ax \leq b$ with A being a TU matrix. Thus, a simple consequence of our main result is a resolution to the problem of derandomizing the isolation lemma for polytopes with TU constraints, as raised in a recent work [27]. This generalizes the isolation result for perfect matchings in a bipartite graph [8], since the perfect matching polytope of a bipartite graph can be described by the incidence matrix of the graph, which is TU. Other examples of families whose polytopes are defined by TU constraints are vertex covers of a bipartite graph, independent sets of a bipartite graph, and, edge covers of a bipartite graph. Note that these three problems are computationally equivalent to bipartite matching and thus, already have quasi-NC algorithms due to [8]. However, the isolation results for these families are not directly implied by isolation for bipartite matchings.

Our work also generalizes the isolation result for the family of common bases of two matroids [11]. In the matroid intersection problem, the constraints of the common base polytope are a rank bound on every subset of the ground set. These constraints, in general, do not form a TUM. However, for every face of the polytope there exist two laminar families of subsets that form a basis for the tight constraints of the face. The incidence matrix for the union of two laminar families is TU (see [22, Theorem 41.11]).

Since our condition on the polytope $P(\mathcal{B})$ does not require the constraint matrix defining the polytope itself (or any of its faces) to be TU, it is quite weak and is also well studied. Schrijver [21, Theorem 5.35] shows that this condition is sufficient to prove that the polytope is *box-totally dual integral*. The second volume of Schrijver's book [22] gives an excellent overview of polytopes that satisfy the condition required in Theorem 2.3 such as

- $R - S$ bibranching polytope [22, Section 54.6]
- directed cut cover polytope [22, Section 55.2]
- submodular flow polyhedron [22, Theorem 60.1]
- lattice polyhedron [22, Theorem 60.4]
- submodular base polytope [22, Section 44.3]
- many other polytopes defined via submodular and supermodular set functions [22, Sections 46.1, 48.1, 48.23, 46.13, 46.28, 46.29, 49.3, 49.12, 49.33, 49.39, 49.53].

We would like to point out that it is not clear if our isolation results in the above settings lead to any new derandomization of algorithms. Finding such algorithmic applications of our isolation result would be quite interesting.

To derandomize the Isolation Lemma, we abstract out ideas from the bipartite matching and matroid intersection isolation [8, 11], and give a geometric approach in terms of certain *lattices* associated to polytopes. For each face F of $P(\mathcal{B})$, we consider the lattice L_F of all integer vectors parallel to F. We show that, if for each face F of $P(\mathcal{B})$, the number of near-shortest vectors in L_F is polynomially bounded then we can construct an isolating weight assignment for $\mathcal{B}$ with quasi-polynomially bounded weights; see Theorem 2.4. Our main technical contribution is to give a polynomial bound on the number of near-shortest vectors in L_F (whose ℓ_1-norm is less than $3/2$ times the smallest ℓ_1-norm of any vector in L_F), when this lattice is the set of integral vectors in the null space of a TUM; see Theorem 2.5.

The above lattice result is in contrast to general lattices where the number of such near-shortest vectors could be exponential in the dimension.

Our result on lattices can be reformulated using the language of matroid theory: the number of near-shortest circuits in a regular matroid is polynomially bounded; see Theorem 2.6. In fact, we show how Theorem 2.5 can be deduced from Theorem 2.6. One crucial ingredient in the proof of Theorem 2.6 is Seymour's remarkable decomposition theorem for regular matroids [23]. Theorem 2.6 answers a question raised by Subramanian [26] and is a generalization of (and builds on) known results in the case of graphic and cographic matroids, that is, the number of near-minimum length cycles in a graph is polynomially bounded (see [26,28]) and the result of Karger [13] that states that the number of near-mincuts in a graph is polynomially bounded.

Thus, not only do our results make progress in derandomizing the isolation lemma for combinatorial polytopes, they make interesting connections between lattices (that are geometric objects) and combinatorial polytopes. Our structural results about the number of near-shortest vectors in lattices and near-shortest circuits in matroids should be of independent interest and raise the question: to what extent are they generalizable?

A natural conjecture would be that for any $(0,1)$-matrix, the lattice formed by its integral null vectors has a small number of near-shortest vectors. In turn, this would give us the isolation result for any polytope which is defined by a $(0,1)$-constraint matrix. Many combinatorial polytopes have this property. One such interesting example is the perfect matchings polytope for general graphs. The recent result of [27], which showed a quasi-NC algorithm for perfect matchings, does not actually go via a bound on the number of near-shortest vectors in the associated lattice. Obtaining a polynomial bound on this number would give a proof for their quasi-NC result in our unified framework and with improved parameters. Another possible generalization is for $(0,1)$-polytopes that have this property that the integers occurring in the description of each supporting hyperplane are bounded by a polynomial in the dimension of the polytope. Such polytopes generalize almost all combinatorial polytopes and yet seem to have enough structure – they have been recently studied in the context of optimization [24, 25].

2 Our Results

2.1 Isolating a vertex in a polytope

For a set E and a weight function $w\colon E \to \mathbb{Z}$, we define the extension of w to any set $S \subseteq E$ by

$$w(S) := \sum_{e \in S} w(e).$$

Let $\mathcal{B} \subseteq 2^E$ be a family of subsets of E. A weight function $w\colon E \to \mathbb{Z}$ is called *isolating for $\mathcal{B}$* if the minimum weight set in $\mathcal{B}$ is unique. In other words, the set $\arg\min_{S \in \mathcal{B}} w(S)$ is unique. The Isolation Lemma of Mulmuley, Vazirani, and Vazirani [14] asserts that a uniformly random weight function is isolating with a good probability for any $\mathcal{B}$.

Lemma 2.1 (Isolation Lemma)**.** *Let E be a set, $|E| = m$, and let $w\colon E \to \{1, 2, \ldots, 2m\}$ be a random weight function, where for each $e \in E$, the weight $w(e)$ is chosen uniformly and independently at random. Then for any family $\mathcal{B} \subseteq 2^E$, w is isolating with probability at least $1/2$.*

The task of derandomizing the Isolation Lemma requires the deterministic construction of an isolating weight function with weights polynomially bounded in $m = |E|$. Here, we view the isolation question for $\mathcal{B}$ as an isolation over a corresponding polytope $P(\mathcal{B})$, as follows. For a set $S \subseteq E$, its indicator vector $x^S := (x^S_e)_{e \in E}$ is defined as

$$x^S_e := \begin{cases} 1, & \text{if } e \in S, \\ 0, & \text{otherwise.} \end{cases}$$

For any family of sets $\mathcal{B} \subseteq 2^E$, the polytope $P(\mathcal{B}) \subseteq \mathbb{R}^m$ is defined as the convex hull of the indicator vectors of the sets in $\mathcal{B}$, i.e.,

$$P(\mathcal{B}) := \operatorname{conv}\left\{ x^S \mid S \in \mathcal{B} \right\}.$$

Note that $P(\mathcal{B})$ is contained in the m-dimensional unit hypercube.

The isolation question for a family $\mathcal{B}$ is equivalent to constructing a weight vector $w \in \mathbb{Z}^E$ such that $\langle w, x \rangle$ has a unique minimum over $P(\mathcal{B})$. The property we need for our isolation approach is in terms of total unimodularity of a matrix.

Definition 2.2 (Totally unimodular matrix)**.** *A matrix $A \in \mathbb{R}^{n \times m}$ is said to be* totally unimodular (TU)*, if every square submatrix has determinant 0 or ± 1.*

Our main theorem gives an efficient quasi-polynomial isolation for a family $\mathcal{B}$ when each face of the polytope $P(\mathcal{B})$ lies in the affine space defined by a TU matrix.

Theorem 2.3 (**Main Result**)**.** *Let E be a set with $|E| = m$. Consider a class $\mathcal{C}$ of families $\mathcal{B} \subseteq 2^E$ that have the following property: for any face F of the polytope $P(\mathcal{B})$, there exists a TU matrix $A_F \in \mathbb{R}^{n \times m}$ such that the affine space spanned by F is given by $A_F x = b_F$ for some $b_F \in \mathbb{R}^n$. We can construct a set W of $m^{O(\log m)}$ weight assignments on E with weights bounded by $m^{O(\log m)}$ such that for any family $\mathcal{B}$ in the class $\mathcal{C}$, one of the weight assignments in W is isolating.*

2.2 Short vectors in lattices associated to polytopes

Our starting point towards proving Theorem 2.3 is a reformulation of the isolation approach for bipartite perfect matching and matroid intersection [8, 11]. For a set E and a family $\mathcal{B} \subseteq 2^E$, we define a lattice corresponding to each face of the polytope $P(\mathcal{B})$. The isolation approach works when this lattice has a small number of near-shortest vectors. For any face F of $P(\mathcal{B})$, consider the lattice of all integral vectors parallel to F,

$$L_F := \left\{ v \in \mathbb{Z}^E \mid v = \alpha(x_1 - x_2) \text{ for some } x_1, x_2 \in F \text{ and } \alpha \in \mathbb{R} \right\}.$$

The length of the shortest nonzero vector of a lattice L is denoted by

$$\lambda(L) := \min \{ \|v\| \mid 0 \neq v \in L \},$$

where $\|\cdot\|$ denotes the ℓ_1-norm. We prove that if, for all faces F of $P(\mathcal{B})$ the number of near-shortest vectors in L_F is small, then we can efficiently isolate a vertex in $P(\mathcal{B})$.

Theorem 2.4 (**Isolation via Lattices**)**.** *Let E be a set with $|E| = m$ and let $\mathcal{B} \subseteq 2^E$ be a family such that there exists a constant $c > 1$, such that for any face F of polytope $P(\mathcal{B})$, we have*

$$|\{ v \in L_F \mid \|v\| < c\,\lambda(L_F) \}| \leq m^{O(1)}.$$

Then one can construct a set of $m^{O(\log m)}$ weight functions with weights bounded by $m^{O(\log m)}$ such that at least one of them is isolating for $\mathcal{B}$.

The main ingredient of the proof of Theorem 2.3 is to show that the hypothesis of Theorem 2.4 is true when the lattice L_F is the set of all integral vectors in the nullspace of a TU matrix. For any $n \times m$ matrix A we define a lattice:

$$L(A) := \{ v \in \mathbb{Z}^m \mid Av = 0 \}.$$

Theorem 2.5 (Near-shortest vectors in TU lattices)**.** *For an $n \times m$ TU matrix A, let $\lambda := \lambda(L(A))$. Then*

$$|\{\, v \in L(A) \mid \|v\| < 3/2\, \lambda \,\}| \;=\; O(m^5).$$

A similar statement can also be shown with any ℓ_p-norm for $p \geq 2$, but with an appropriate multiplicative constant. Theorem 2.5 together with Theorem 2.4 implies Theorem 2.3.

Proof of Theorem 2.3. Let F be a face of the polytope $P(\mathcal{B})$ and let A_F be the TU matrix associated with F. Thus $A_F x = b_F$ defines the affine span of F. In other words, the set of vectors parallel to F is precisely the solution set of $A_F x = 0$ and the lattice L_F is given by $L(A_F)$. Theorem 2.5 implies the hypothesis of Theorem 2.4 for any $L_F = L(A_F)$, when the matrix A_F is TU. □

2.3 Near-shortest circuits in regular matroids

The proof of Theorem 2.5 is combinatorial and uses the language and results from matroid theory. We refer the reader to Section 6 for preliminaries on matroids; here we just recall a few basic definitions. A matroid is said to be *represented by a matrix A*, if its ground set is the column set of A and its independent sets are the sets of linearly independent columns of A. A matroid represented by a TU matrix is said to be a *regular matroid.* A *circuit* of a matroid is a minimal dependent set. The following is one of our main results which gives a bound on the number of near-shortest circuits in a regular matroid, which, in turn, implies Theorem 2.5. Instead of the circuit size, we consider the weight of a circuit and present a more general result.

Theorem 2.6 (Near-shortest circuits in regular matroids)**.** *Let $M = (E, \mathcal{I})$ be a regular matroid with $m = |E| \geq 2$ and let $w \colon E \to \mathbb{N}$ be a weight function. Suppose M does not have any circuit C with $w(C) < r$ for some number r. Then*

$$|\{\, C \mid C \text{ circuit in } M \text{ and } w(C) < 3r/2 \,\}| \;\leq\; 240\, m^5.$$

Remark 2.7. *An extension of this result would be to give a polynomial bound on the number of circuits of weight at most αr for any constant α. Our current proof technique does not extend to this setting.*

3 Isolation via the Polytope Lattices: Proof of Theorem 2.4

This section is dedicated to a proof of Theorem 2.4. That is, we give a construction of an isolating weight assignment for a family $\mathcal{B} \subseteq 2^E$ assuming that for each face F of the corresponding polytope $P(\mathcal{B})$, the lattice L_F has small number of near-shortest vectors. First, let us see how the isolation question for a family $\mathcal{B}$ translates in the polytope setting. For any weight function $w \colon E \to \mathbb{Z}$, we view w as a vector in $\mathbb{Z}^E$ and consider the function $\langle w, x \rangle$ over the points in $P(\mathcal{B})$. Note that $\langle w, x^B \rangle = w(B)$, for any $B \subseteq E$. Thus, a weight function $w \colon E \to \mathbb{Z}$ is isolating for a family $\mathcal{B}$ if and only if $\langle w, x \rangle$ has a unique minimum over the polytope $P(\mathcal{B})$.

Observe that for any $w \colon E \to \mathbb{Z}$, the points that minimize $\langle w, x \rangle$ in $P(\mathcal{B})$ will form a face of the polytope $P(\mathcal{B})$. The idea is to build the isolating weight function in rounds. In every round, we slightly modify the current weight function to get a smaller minimizing face. Our goal is to significantly reduce the dimension of the minimizing face in every round. We stop when we reach a zero-dimensional face, i.e., we have a unique minimum weight point in $P(\mathcal{B})$.

The following claim asserts that if we modify the current weight function on a small scale, then the new minimizing face will be a subset of the current minimizing face. In the following, we will denote the size of the set E by m.

Claim 3.1. *Let $w\colon E \to \mathbb{Z}$ be a weight function and F be the face of $P(\mathcal{B})$ that minimizes w. Let $w'\colon E \to \{0, 1, \dots, N-1\}$ be another weight function and let F' be the face that minimizes the combined weight function $mN\, w + w'$. Then $F' \subseteq F$.*

Proof. Consider any vertex $x \in F'$. We show that $x \in F$. By definition of F', for any vertex $y \in P(\mathcal{B})$ we have

$$\langle mN\, w + w', x\rangle \leq \langle mN\, w + w', y\rangle.$$

In other words,

$$\langle mN\, w + w', x - y\rangle \leq 0. \tag{1}$$

Since x and y are vertices of $\mathcal{P}(\mathcal{B})$, we have $x, y \in \{0,1\}^m$. Thus, $|\langle w', x-y\rangle| < mN$. On the other hand, if $|\langle mN\, w, x-y\rangle|$ is nonzero then it is at least mN and thus dominates $|\langle w', x-y\rangle|$. Hence, for (1) to hold, it must be that

$$\langle mN\, w, x-y\rangle \leq 0.$$

It follows that $\langle w, x\rangle \leq \langle w, y\rangle$, and therefore $x \in F$. □

Thus, in each round, we will add a new weight function to the current function using a smaller scale and try to get a sub-face with significantly smaller dimension. Henceforth, N will be a sufficiently large number bounded by $\mathrm{poly}(m)$. The following claim gives a way to go to a smaller face.

Claim 3.2. *Let F be the face of $P(\mathcal{B})$ minimizing $\langle w, x\rangle$ and let $v \in L_F$. Then $\langle w, v\rangle = 0$.*

Proof. Since $v \in L_F$, we have $v = \alpha(x_1 - x_2)$, for some $x_1, x_2 \in F$ and $\alpha \in \mathbb{R}$. As $x_1, x_2 \in F$, we have $\langle w, x_1\rangle = \langle w, x_2\rangle$. The claim follows. □

Now, let F_0 be the face that minimizes the current weight function w_0. Let v be in L_{F_0}. Choose a new weight function $w' \in \{0, 1, \dots, N-1\}^E$ such that $\langle w', v\rangle \neq 0$. Let $w_1 := mN\, w_0 + w'$ and let F_1 be the face that minimizes w_1. Clearly, $\langle w_1, v\rangle \neq 0$ and thus, by Claim 3.2, $v \notin L_{F_1}$. This implies that F_1 is strictly contained in F_0. To ensure that F_1 is *significantly* smaller than F_0, we choose many vectors in L_{F_0}, say $v_1, v_2, \dots, v_k$, and construct a weight vector w' such that for all $i \in [k]$, we have $\langle w', v_i\rangle \neq 0$. The following well-known lemma actually constructs a list of weight vectors such that one of them has the desired property (see [9, Lemma 2]).

Lemma 3.3. *Given m, k, t, let $q = mk \log t$. In time $\mathrm{poly}(q)$ one can construct a set of weight vectors $w_1, w_2, \dots, w_q \in \{0, 1, 2, \dots, q\}^m$ such that for any set of nonzero vectors $v_1, v_2, \dots, v_k$ in $\{-(t-1), \dots, 0, 1, \dots, t-1\}^m$ there exists a $j \in [q]$ such that for all $i \in [k]$ we have $\langle w_j, v_i\rangle \neq 0$.*

Proof. First define $w := (1, t, t^2, \dots, t^{m-1})$. Clearly, $\langle w, v_i\rangle \neq 0$ for each i, because each coordinate of v_i is less than t in absolute value. To get a weight vector with small coordinates, we go modulo small numbers. We consider the following weight vectors w_j for $1 \leq j \leq q$:

$$w_j := w \bmod j.$$

We claim that this set of weight vectors has the desired property. We know that

$$W = \prod_{i=1}^{k} \langle w, v_i\rangle \neq 0.$$

Note that the product W is bounded by t^{mk}. On the other hand, it is known that $\mathrm{lcm}(2, 3, \dots, q) > 2^q = t^{mk}$ for all $q \geq 7$ [15]. Thus, there must exist a $2 \leq j \leq q$ such that j does not divide W. In other words, for all $i \in [k]$

$$\langle w, v_i\rangle \not\equiv 0 \pmod{j}$$

which is the desired property. □

There are two things to note about this lemma: (i) It is black-box in the sense that we do not need to know the set of vectors $\{v_1, v_2, \dots, v_k\}$. (ii) We do not know a priori which function will work in the given set of functions. So, one has to try all possibilities.

The lemma tells us that we can ensure that $\langle w', v \rangle \neq 0$ for polynomially many vectors v whose coordinates are polynomially bounded. Below, we formally present the weight construction.

To prove Theorem 2.4, let c be the constant in the assumption of the theorem. Let $N = m^{O(1)}$ be a sufficiently large number and $p = \lfloor \log_c(m+1) \rfloor$. Let $w_0 \colon E \to \mathbb{Z}$ be a weight function such that $\langle w_0, v \rangle \neq 0$ for all nonzero $v \in \mathbb{Z}^E$ with $\|v\| < c$. For $i = 1, 2, \dots, p$, define

F_{i-1}: the face of $P(\mathcal{B})$ minimizing w_{i-1}

w'_i: a weight vector in $\{0, 1, \dots, N-1\}^E$ such that $\langle w'_i, v \rangle \neq 0$ for all nonzero $v \in L_{F_{i-1}}$ with $\|v\| < c^{i+1}$.

w_i: $mNw_{i-1} + w'_i$.

Observe that $F_i \subseteq F_{i-1}$, for each i by Claim 3.1. Hence, also for the associated lattices we have $L_{F_i} \subseteq L_{F_{i-1}}$. As we show in the next claim, the choice of w'_i together with Claim 3.2 ensures that there are no vectors in L_{F_i} with norm less than c^{i+1}.

Claim 3.4. *For $i = 0, 1, 2, \dots, p$, we have $\lambda(L_{F_i}) \geq c^{i+1}$.*

Proof. Consider a nonzero vector $v \in L_{F_i}$. By Claim 3.2, we have

$$\langle w_i, v \rangle = mN \langle w_{i-1}, v \rangle + \langle w'_i, v \rangle = 0. \tag{2}$$

Since v is in L_{F_i}, it is also in $L_{F_{i-1}}$ and again by Claim 3.2, we have $\langle w_{i-1}, v \rangle = 0$. Together with (2) we conclude that $\langle w'_i, v \rangle = 0$. By the definition of w'_i, this implies that $\|v\| \geq c^{i+1}$. □

Finally we argue that w_p is isolating.

Claim 3.5. *The face F_p is a point.*

Proof. Let $y_1, y_2 \in F_p$ be vertices and thus belong to $\{0,1\}^m$. Then $y_1 - y_2 \in L_{F_p}$ and $\|y_1 - y_2\| \leq m < c^{p+1}$. By Claim 3.4, we have that $y_1 - y_2$ must be zero, i.e., $y_1 = y_2$. □

The following claim, which gives bounds on the number of weight vectors we need to try and the weights involved, finishes the proof of Theorem 2.4.

Claim 3.6. *The number of possible choices for w_p such that one of them is isolating for $\mathcal{B}$ is $m^{O(\log m)}$. The weights in each such weight vector are bounded by $m^{O(\log m)}$.*

Proof. To bound the weights of w_p, we bound w'_i for each i. By Claim 3.4, we have $\lambda(L_{F_{i-1}}) \geq c^i$, for each $1 \leq i \leq p$. The hypothesis of Theorem 2.4 implies

$$\left| \left\{ v \in L_{F_{i-1}} \mid \|v\| < c^{i+1} \right\} \right| \leq m^{O(1)}.$$

Recall that we have to ensure $\langle w'_i, v \rangle \neq 0$ for all nonzero vectors v in the above set. We apply Lemma 3.3 with $k = m^{O(1)}$. For parameter t, note that as $\|v\| < c^{i+1} \leq c^{p+1} \leq c(m+1)$, each coordinate of v is less than $c(m+1)$ and therefore $t \leq c(m+1)$. Thus, we get w'_i with weights bounded by $m^{O(1)}$. Therefore the weights in w_p are bounded by $m^{O(p)} = m^{O(\log m)}$.

Recall that Lemma 3.3 actually gives a set of $m^{O(1)}$ weight vectors for possible choices of w'_i and one of them has the desired property. Thus, we try all possible combinations for each w'_i. This gives us a set of $m^{O(\log m)}$ possible choices for w_p such that one of them is isolating for $\mathcal{B}$. □

4 Number of Short Vectors in Lattices: Proof of Theorem 2.5

In this section, we show that Theorem 2.5 follows from Theorem 2.6. We define a circuit of a matrix and show that to prove Theorem 2.5, it is sufficient to upper bound the number of near-shortest circuits of a TU matrix. We argue that this, in turn, is implied by a bound on the number of near-shortest circuits of a regular matroid. Just as a circuit of a matroid is a minimal dependent set, a circuit of matrix is a minimal linear dependency among its columns. Recall that for an $n \times m$ matrix A, the lattice $L(A)$ is defined as the set of integer vectors in its kernel,

$$L(A) := \{ v \in \mathbb{Z}^m \mid Av = 0 \} .$$

Definition 4.1 (Circuit)**.** *For an $n \times m$ matrix A, a vector $u \in L(A)$ is a* circuit of A *if*

- *there is no nonzero $v \in L(A)$ with $\operatorname{supp}(v) \subsetneq \operatorname{supp}(u)$, and*
- $\gcd(u_1, u_2, \ldots, u_m) = 1$.

Note that if u is a circuit of A, then so is $-u$. The following property of the circuits of a TU matrix is well known (see [17, Lemma 3.18]).

Fact 4.2. *Let A be a TU matrix. Then every circuit of A has its coordinates in $\{-1, 0, 1\}$.*

Now, we define a notion of conformality among two vectors.

Definition 4.3 (Conformal [17])**.** *Let $u, v \in \mathbb{R}^m$. We say that u is* conformal to v*, denoted by $u \sqsubseteq v$, if $u_i v_i \geq 0$ and $|u_i| \leq |v_i|$, for each $1 \leq i \leq m$.*

Observation 4.4. *For vectors u and v with $u \sqsubseteq v$, we have $\|v - u\| = \|v\| - \|u\|$.*

The following lemma follows from [17, Lemma 3.19].

Lemma 4.5. *Let A be a TU matrix. Then for any nonzero vector $v \in L(A)$, there is a circuit u of A that is conformal to v.*

We use the lemma to argue that any small enough vector in $L(A)$ must be a circuit.

Lemma 4.6. *Let A be a TU matrix and let $\lambda := \lambda(L(A))$. Then any nonzero vector $v \in L(A)$ with $\|v\| < 2\lambda$ is a circuit of A.*

Proof. Suppose $v \in L(A)$ is not a circuit of A. We show that $\|v\| \geq 2\lambda$. By Lemma 4.5, there is a circuit u of A with $u \sqsubseteq v$. Since v is not a circuit, $v - u \neq 0$. Since both u and $v - u$ are nonzero vectors in $L(A)$, we have $\|u\|, \|v - u\| \geq \lambda$. By Observation 4.4, we have $\|v\| = \|v - u\| + \|u\|$ and thus, we get that $\|v\| \geq 2\lambda$. □

Recall that a matroid represented by a TU matrix is a regular matroid (see Theorem 6.3). The following lemma shows that the two definitions of circuits, 1) for TU matrices and 2) for regular matroids, coincide.

Lemma 4.7. *Let $M = (E, \mathcal{I})$ be a regular matroid, represented by a TU matrix A. Then there is a one to one correspondence between the circuits of M and the circuits of A (up to change of sign).*

Proof. If $u \in \mathbb{R}^E$ is a circuit of A, then the columns in A corresponding to the set $\operatorname{supp}(u)$ are minimally dependent. Thus, the set $\operatorname{supp}(u)$ is a circuit of matroid M.

In the other direction, a circuit $C \subseteq E$ of matroid M is a minimal dependent set. Thus, the set of columns of A corresponding to C is minimally linear dependent. Hence, there are precisely two circuits $u, -u \in L(A)$ with their support being C. □

To prove Theorem 2.5, let A be TU matrix. By Lemma 4.6, it suffices to bound the number of near-shortest circuits of A. By Lemma 4.7, the circuits of A and the circuits of the regular matroid M represented by A, coincide. Moreover, the size of a circuit of M is same as the ℓ_1-norm of the corresponding circuit of A, as a circuit of A has its coordinates in $\{-1, 0, 1\}$ by Fact 4.2. Now Theorem 2.5 follows from Theorem 2.6 when we define the weight of each element being 1.

5 Proof Overview of Theorem 2.6

Theorem 2.6 states that for a regular matroid, the number of near-shortest circuits – circuits whose size is at most 3/2 of the shortest circuit size – is polynomially bounded. The starting point of the proof of this theorem is a remarkable result of Seymour [23] which showed that every regular matroid can be decomposed into a set of much simpler matroids. Each of these building blocks for regular matroids either belongs to the classes of graphic and cographic matroids – the simplest and well-known examples of regular matroids, or is a special 10-element matroid R_{10} (see Section 6 for the definitions). One important consequence of Seymour's result is a polynomial time algorithm, the only one known, for testing the total unimodularity of a matrix; see [20] (recall that a TU matrix represents a regular matroid). Our strategy is to leverage Seymour's decomposition theorem in order to bound the number of circuits in a regular matroid.

Seymour's Theorem and a simple inductive approach

Seymour's decomposition involves a sequence of binary operations on matroids, each of which is either a 1-sum, a 2-sum or a 3-sum. Formally, it states that for every regular matroid M, we can build a decomposition tree – which is a binary rooted tree – in which the root node is the matroid M, every node is a k-sum of its two children for $k = 1, 2$, or 3, and at the bottom we have graphic, cographic and the R_{10} matroids as the leaf nodes. Note that the tree, in general, is not necessarily balanced and can have large depth (linear in the ground set size).

This suggests that to bound the number of near-shortest circuits in a regular matroid, perhaps one can use the tree structure of its decomposition, starting from the leaf nodes and arguing, inductively, all the way up to the root. It is known that the number of near-shortest circuits in graphic and cographic matroids is polynomially bounded. This follows from the polynomial bounds on the number of near-shortest cycles of a graph [26] and on the number of near min-cuts in a graph [13] (Theorem 6.8). The challenge is to show how to combine the information at an internal node.

The k-sum M of two matroids M_1 and M_2 is defined in a way such that each circuit of M can be built from a combination of two circuits, one from M_1 and another from M_2. Thus, if we have upper bounds for the number of circuits in M_1 and M_2, their product will give a naive upper bound for number of circuits in M. Since there can be many k-sum operations involved, the naive product bound can quickly explode. Hence, to keep a polynomial bound we need to take a closer look at the k-sum operations.

k-sum operations

1-sum. A 1-sum M of two matroids M_1 and M_2 is simply their direct sum. That is, the ground set of M is the disjoint union of the ground sets of M_1 and M_2, and any circuit of M is either a circuit of M_1 or a circuit of M_2.

The 2-sum and 3-sum are a bit more intricate. It is known that the set of circuits of a matroid completely characterizes the matroid. The 2-sum and 3-sum operations are defined by describing the set of circuits of the matroid obtained by the sum. To get an intuition for the 2-sum operation, we first describe it on two graphic matroids. A graphic matroid is defined with respect to a graph, where a circuit is a simple cycle in the graph.

2-sum on graphs. For two graphs G_1 and G_2, their 2-sum $G = G_1 \oplus_2 G_2$ is any graph obtained by identifying an edge (u_1, v_1) in G_1 with an edge (u_2, v_2) in G_2, that is, identifying u_1 with u_2 and v_1 with v_2 and then, deleting the edge $(u_1, v_1) = (u_2, v_2)$. It would be instructive to see how a cycle in G, i.e., a circuit of the associated graphic matroid, looks like. A cycle in G is either a cycle in G_1 or in G_2 that avoids the edge $(u_1, v_1) = (u_2, v_2)$, or it is a union of a path $u_1 \rightsquigarrow v_1$ in G_1 and a path $v_2 \rightsquigarrow u_2$ in G_2. This last possibility is equivalent to taking a symmetric difference $C_1 \triangle C_2$ of two cycles C_1 in G_1 and C_2 in G_2 such that C_1 passes through (u_1, v_1) and C_2 passes through (u_2, v_2).

2-sum on matroids. The 2-sum $M_1 \oplus_2 M_2$ of two matroids M_1 and M_2 is defined analogously. The grounds sets of M_1 and M_2, say E_1 and E_2 respectively, have an element in common, say e (this can be achieved by identifying an element from E_1 with an element from E_2). The sum $M_1 \oplus_2 M_2$ is defined on the ground set $E = E_1 \Delta E_2$, the symmetric difference of the two given ground sets. Any circuit of the sum $M_1 \oplus_2 M_2$ is either a circuit in M_1 or in M_2 that avoids the common element e, or it is the symmetric difference $C_1 \triangle C_2$ of two circuits C_1 and C_2 of M_1 and M_2, respectively, such that both C_1 and C_2 contain the common element e.

3-sum on matroids. A 3-sum is defined similarly. A matroid M is a 3-sum of two matroids M_1 and M_2 if their ground sets E_1 and E_2 have a set S of three elements in common such that S is a circuit in both the matroids and the ground set of M is the symmetric difference $E_1 \triangle E_2$. Moreover, a circuit of M is either a circuit in M_1 or in M_2 that avoids the common elements S, or it is the symmetric difference $C_1 \triangle C_2$ of two circuits C_1 and C_2 of M_1 and M_2, respectively, such that both C_1 and C_2 contain a common element e from S and no other element from S.

The inductive bound on the number of circuits

Our proof is by a strong induction on the ground set size.

Base case: For a graphic or cographic matroid with a ground set of size m, if its shortest circuit has size r then the number of its circuits of size less than αr is at most $m^{4\alpha}$. For the R_{10} matroid, we present a constant upper bound on the number of circuits.

Induction hypothesis: For any regular matroid with a ground set of size $m < m_0$, if its shortest circuit has size r, then the number of its circuits of size less than αr is bounded by $m^{c\alpha}$ for some sufficiently large constant c.

Induction step: We prove the induction hypothesis for a regular matroid M with a ground set of size m_0. Let the minimum size of a circuit in M be r. We want to show a bound of $m_0^{c\alpha}$ on the number of circuits in M of size less than αr. The main strategy here is as follows: by Seymour's Theorem, we can write M as a k-sum of two smaller regular matroids M_1 and M_2, with ground sets of size $m_1 < m_0$ and $m_2 < m_0$ respectively. As the circuits of M can be written as a symmetric differences of circuits of M_1 and M_2, we derive an upper bound on the number circuits of M from the corresponding bounds for M_1 and M_2, which we get from the induction hypothesis.

The 1-sum case. In this case, any circuit of M is either a circuit of M_1 or a circuit of M_2. Hence, the number of circuits in M of size less than αr is simply the sum of the number of circuits in M_1 and M_2 of size less than αr. Using the induction hypothesis, this sum is bounded by $m_1^{c\alpha} + m_2^{c\alpha}$, which is less than $m_0^{c\alpha}$ since $m_0 = m_1 + m_2$.

The 2-sum and 3-sum cases. Let the set of common elements in the ground sets of M_1 and M_2 be S. Note that $m_0 = m_1 + m_2 - |S|$. Recall from the definition of a k-sum that any circuit C of M is of the form $C_1 \triangle C_2$, where C_1 and C_2 are circuits in M_1 and M_2 respectively, such that either **(i)** one of them, say C_1, has no element from S and the other one C_2 is empty or **(ii)** they both contain exactly one common element from S. We will refer to C_1 and C_2 as projections of C. Note that $|C_1|, |C_2| \leq |C|$. In particular, if circuit C is of size less than αr, then so are its projections C_1 and C_2.

An obstacle. The first step would be to bound the number of circuits C_1 of M_1 and C_2 of M_2 using the induction hypothesis. However, we do not have a lower bound on the minimum size of a circuit in M_1 or M_2, which is required to use the induction hypothesis. What we do know is that any circuit in M_1 or M_2 that does not involve elements from S is also a circuit of M, and thus, must have size at least r. However, a circuit that involves elements from S could be arbitrarily small. We give different solutions for this obstacle in case **(i)** and case **(ii)** mentioned above.

Case (i): deleting elements in S. Let us first consider the circuits C_1 of M_1 that do not involve elements from S. These circuits can be viewed as circuits of a new regular matroid $M_1 \setminus S$ obtained by deleting the elements in S from M_1. Since we know that the minimum size of a circuit in $M_1 \setminus S$ is r, we can apply the induction hypothesis to get a bound of $(m_1 - |S|)^{c\alpha}$ for the number of circuits C_1 of $M_1 \setminus S$ of size less than αr. Summing this with a corresponding bound for $M_2 \setminus S$ gives us a bound less than $m_0^{c\alpha}$ for the number of circuits of M in case **(i)**.

Case (ii): stronger induction hypothesis. The case when circuits C_1 and C_2 contain an element from S turns out to be much harder. For this case, we actually need to strengthen our induction hypothesis. Let us assume that for a regular matroid of ground set size $m < m_0$, if the minimum size of a circuit that avoids a given element $\widetilde{e}$ is r, then the number of circuits containing $\widetilde{e}$ and of size less than αr is bounded by $m^{c\alpha}$. This statement will also be proved by induction, but we will come to its proof later.

Since we know that any circuit in M_1 (or M_2) that avoids elements from S has size at least r, we can use the above stronger inductive hypothesis to get a bound of $m_1^{c\alpha}$ on the number of circuits C_1 in M_1 containing a given element from S and of size less than αr. Similarly, we get an analogous bound of $m_2^{c\alpha}$ for circuits C_2 of M_2. Since C can be a symmetric difference of any C_1 and C_2, the product of these two bounds, that is, $(m_1 m_2)^{c\alpha}$ bounds the number of circuits C of M of size less than αr. Unfortunately, this product can be much larger than $m_0^{c\alpha}$. Note that this product bound on the number of circuits C is not really tight since C_1 and C_2 both cannot have their sizes close to αr simultaneously. This is because $C = C_1 \triangle C_2$ and thus, $|C| = |C_1| + |C_2| - 1$. Hence, a better approach is to consider different cases based on the sizes of C_1 and C_2.

Number of circuits C when one of its projections is small. We first consider the case when the size of C_1 is very small, i.e., close to zero. In this case, the size of C_2 will be close to αr and we have to take the bound of $m_2^{c\alpha}$ on the number of such circuits C_2. Now, if number of circuits C_1 with small size is N then we get a bound of $N m_2^{c\alpha}$ on the number of circuits C of M of this case. Note that $N m_2^{c\alpha}$ is dominated by $m_0^{c\alpha}$ only when $N \leq 1$, as m_2 can be comparable to m. While $N \leq 1$ does not always hold, we show something weaker which is true.

Uniqueness of C_1. We can show that for any element s in the set of common elements S, there is at most one circuit C_1 of size less than $r/2$ that contains s and no other element from S. To see this, assume that there are two such circuits C_1 and C_1'. It is known that the symmetric difference of two circuits of a matroid is a disjoint union of some circuits of the matroid. Thus, $C_1 \triangle C_1'$ will be a disjoint union of circuits of M_1. Since $C_1 \triangle C_1'$ does not contain any element from S, it is also a disjoint union of circuits of M. This would lead us to a contradiction because the size of $C_1 \triangle C_1'$ is less than r and M does not have circuits of size less than r. This proves the uniqueness of C_1. Our problem is still not solved since the set S can have three elements in case of a 3-sum, and thus, there can be three possibilities for C_1 (i.e., N=3).

Assigning weights to the elements. To get around this problem, we use a new idea of considering matroids elements with weights. For each element s in S, consider the unique circuit C_1 of size at most $r/2$ that contains s. In the matroid M_2, we assign a weight of $|C_1| - 1$ to the element s. The elements outside S get weight 1. The weight of element $s \in S$ signifies that if a circuit C_2 of M_2 contains s then it has to be summed up with the unique circuit C_1 containing s, which adds a weight of $|C_1| - 1$. Essentially, the circuits of the weighted matroid M_2 that have weight γ will have a one-to-one correspondence with circuits $C = C_1 \triangle C_2$ of M that have size γ and have $|C_1| < r/2$. Hence, we can assume there are no circuits in the weighted matroid M_2 of weight less than r. Thus, we can apply the induction hypothesis on M_2, but we need to further strengthen the hypothesis to a weighted version. By this new induction hypothesis, we will get a bound of $m_2^{c\alpha}$ on the number of circuits of M_2 with weight less that αr. As mentioned above, this will bound the number of circuits $C = C_1 \triangle C_2$ of M with size less than αr and $|C_1| < r/2$. Note that the bound $m_2^{c\alpha}$ is smaller than the desired bound $m_0^{c\alpha}$.

Number of circuits C when none of its projections is small. It is relatively easier to handle the other case when C_1 has size at least $r/2$ (and less than αr). In this case, C_2 has size less than $(\alpha - 1/2)r$. The bounds we get by the induction hypothesis for the number of circuits C_1 and C_2 are $m_1^{c\alpha}$ and $m_2^{c(\alpha-1/2)}$ respectively. Their product $m_1^{c\alpha} m_2^{c(\alpha-1/2)}$ bounds the number of circuits C in this case. However, this product is not bounded by $m_0^{c\alpha}$.

Stronger version of Seymour's Theorem. To get a better bound we need another key idea. Instead of Seymour's Theorem, we work with a stronger variant given by Truemper [29]. It states that any regular matroid can be written as a k-sum of two smaller regular matroids M_1 and M_2 for $k = 1, 2$ or 3 such that one of them, say M_1, is a graphic, cographic or R_{10} matroid. The advantage of this stronger statement is that we can take a relatively smaller bound on the number of circuits of M_1, which gives us more room for the inductive argument. Formally, we know from above that when M_1 is a graphic or cographic matroid, the number of its circuits of size less than αr is at most $m_1^{4\alpha}$. One can choose the constant c in our induction hypothesis to be sufficiently large so that the product $m_1^{4\alpha} m_2^{c(\alpha-1/2)}$ is bounded by $m_0^{c\alpha}$.

A stronger induction hypothesis

To summarize, we work with an inductive hypothesis as follows: If a regular matroid (with weights) has no circuits of weight less than r that avoid a given set R of elements then the number of circuits of weight less than αr that contain the set R is bounded by $m^{c\alpha}$. As the base case, Lemma 7.1 shows this statement for the graphic and cographic case.

When we rerun the whole inductive argument with weights and with a fixed set R, we run into another issue. It turns out that in the case when the size of C_1 is very small, our arguments above do not go through if C_1 has some elements from R. To avoid such a situation we use yet another strengthened version of Seymour's Theorem. It says that any regular matroid with a given element $\widetilde{e}$ can be written as a k-sum of two smaller regular matroids M_1 and M_2, such that M_1 is a graphic, cographic or R_{10} matroid and M_2 is a regular matroid containing $\widetilde{e}$ (Theorem 6.19). When our

R is a single element set, say $\{\widetilde{e}\}$, we use this theorem to ensure that M_1, and thus C_1, has no elements from R. This rectifies the problem when R has size 1. However, as we go deeper inside the induction, the set R can grow in size. Essentially, whenever α decreases by $1/2$ in the induction, the size of R grows by 1. Thus, we take α to be $3/2$, which means that to reach $\alpha = 1$ we need only one step of decrement, and thus, the size of R at most becomes 1. This is the reason our main theorem only deals with circuits of size less than $3/2$ times the smallest size.

In order to generalize this result for an arbitrary constant α, a different method is required. This will be the subject of a follow-up work.

Organization of the rest of the paper. The remainder of the paper is dedicated to the formal proof of Theorem 2.6. We first give some matroid preliminaries and Seymour's decomposition theorem for regular matroids in Section 6. Finally, in Section 7, we prove Theorem 2.6.

6 Matroids

In Section 6.1, we recall some basic definitions and well-known facts about matroids (see, for example, [18, 22]). In Section 6.2, we describe Seymour's decomposition theorem for regular matroids.

6.1 Matroids preliminaries

We start with some basic definitions.

Definition 6.1 (Matroid)**.** *A pair $M = (E, \mathcal{I})$ is a* matroid *if E is a finite set and $\mathcal{I}$ is a nonempty collection of subsets of E satisfying*

1. *if $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$,*
2. *if $I, J \in \mathcal{I}$ and $|I| < |J|$, then $I \cup \{z\} \in \mathcal{I}$, for some $z \in J \setminus I$.*

A subset I of E is said to be independent*, if I belongs to $\mathcal{I}$ and* dependent *otherwise. An inclusionwise maximal independent subset of E is a* base *of M. An inclusionwise minimal dependent set is a* circuit *of M.*

We define some special classes of matroids.

Definition 6.2 (Linear, binary, and regular matroid)**.** *A matroid $M = (E, \mathcal{I})$ with $m = |E|$ is* linear *or* representable *over some field $\mathbb{F}$, if there is a matrix $A \in \mathbb{F}^{n \times m}$, for some n, such that the collection of subsets of the columns of A that are linearly independent over $\mathbb{F}$ is identical to $\mathcal{I}$.*

A matroid M is binary*, if M is representable over* GF(2)*. A matroid M is* regular*, if M is representable over every field.*

It is well known that regular matroids can be characterized in terms of TU matrices.

Theorem 6.3 (See [18, 22])**.** *A matroid M is regular if, and only if, M can be represented by a TU matrix over $\mathbb{R}$.*

Two special classes of regular matroids are graphic matroids and their duals, cographic matroids.

Definition 6.4 (Graphic and cographic matroid)**.** *A matroid $M = (E, \mathcal{I})$ is said to be a* graphic*, if there is an undirected graph $G = (V, E)$ whose edges correspond to the ground set E of M, such that $I \in \mathcal{I}$ if and only if I forms a forest in G. By $M(G)$ we denote the graphic matroid corresponding to G.*

The dual *of M is the matroid $M^* = (E, \mathcal{I}^*)$ over the same ground set such that a set $I \subseteq E$ is independent in M^* if and only if $E \setminus I$ contains a base set of M. A* cographic matroid *is the dual of a graphic matroid.*

For $G = (V, E)$, we can represent $M(G)$ by the vertex-edge incidence matrix $A_G \in \{0,1\}^{V \times E}$ (over $GF(2)$),

$$A_G(v, e) = \begin{cases} 1 & \text{if } e \text{ is incident on } v, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 6.5 (Graph cut and cut-set)**.** *For a graph $G = (V, E)$, a* cut *is a partition (V_1, V_2) of V into two disjoint subsets. Any cut (V_1, V_2) uniquely determines a* cut-set*, the set of edges that have one endpoint in V_1 and the other in V_2. The* size of a cut *is the number of edges in the corresponding cut-set. A* minimum cut *is one of minimum size.*

Fact 6.6. *Let $G = (V, E)$ be a graph.*

1. *The circuits of the graphic matroid $M(G)$ are exactly the simple cycles of G.*
2. *The circuits of the cographic matroid $M^*(G)$ are exactly the inclusionwise minimal cut-sets of G.*

The symmetric difference of two cycles in a graph is a disjoint union of cycles. The analogous statement is true for binary matroids.

Fact 6.7. *Let M be binary. If C_1 and C_2 are circuits of M, then the symmetric difference $C_1 \triangle C_2$ is a disjoint union of circuits.*

To prove Theorem 2.6, we have to bound the number of short circuits in regular matroids. In Lemma 7.1, we start by providing such a bound for graphic and cographic matroids. The lemma is a variant of the following theorem that bounds the number of near-shortest cycles [26] and the number of near-minimum cuts [13] in a graph.

Theorem 6.8. *Let $G = (V, E)$ be a graph with $m \geq 1$ edges and $\alpha \geq 2$.*

1. *If G has no cycles of length at most r, then the number of cycles in G of length at most $\alpha r/2$ is bounded by $(2m)^\alpha$* [26].
2. *If G has no cuts of size at most r, then the number of cuts in G of size at most $\alpha r/2$ is bounded by m^α* [13].

We define two operations on matroids.

Definition 6.9 (Deletion, contraction, minor)**.** *Let $M = (E, \mathcal{I})$ be a matroid and $e \in E$. The* matroid obtained from M by deleting e *is denoted by $M \setminus e$. Its independent sets are given by the collection $\{\, I \in \mathcal{I} \mid e \notin I \,\}$.*

The matroid obtained by contracting e *is denoted by M/e. Its independent sets are given by the collection $\{\, I \subseteq E \setminus \{e\} \mid I \cup \{e\} \in \mathcal{I} \,\}$.*

A matroid obtained after a series of deletion and contraction operations on M is called a minor *of M.*

Fact 6.10. *Let $M = (E, \mathcal{I})$ be a matroid and $e \in E$.*

1. *The circuits of $M \setminus e$ are those circuits of M that do not contain e.*
2. *The classes of regular matroids, graphic matroids, and cographic matroids are minor closed.*

For a characterization of regular matroids, we will need a specific matroid R_{10}, first introduced by [3]. It is a matroid, with 10 elements in the ground set, represented over $GF(2)$ by the following matrix.

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Fact 6.11 ([23]). *Any matroid obtained by deleting some elements from R_{10} is a graphic matroid.*

6.2 Seymour's Theorem and its variants

The main ingredient for the proof of Theorem 2.6 is a theorem of Seymour [23, Theorem 14.3] that shows that every regular matroid can be constructed from piecing together three kinds of matroids – graphic matroids, cographic matroids, and the matroid R_{10}. This piecing together is done via matroid operations called 1-sum, 2-sum and 3-sum. These operations are defined for binary matroids.

Definition 6.12 (Sum of two matroids [23], see also [18]). *Let $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ be two binary matroids, and let $S = E_1 \cap E_2$. The* sum of M_1 and M_2 *is a matroid denoted by $M_1 \triangle M_2$. It is defined over the ground set $E_1 \triangle E_2$ such that the circuits of $M_1 \triangle M_2$ are minimal non-empty subsets of $E_1 \triangle E_2$ that are of the form $C_1 \triangle C_2$, where C_i is a (possibly empty) disjoint union of circuits of M_i, for $i = 1, 2$.*

From the characterization of the circuits of a matroid [18, Theorem 1.1.4], it can be verified that the sum $M_1 \triangle M_2$ is indeed a matroid.

We are only interested in three special sums:

Definition 6.13 ($1, 2, 3$-sums). *Let $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ be two binary matroids and $E_1 \cap E_2 = S$. Let $m_1 = |E_1|$, $m_2 = |E_2|$, and $s = |S|$. Let furthermore $m_1, m_2 < |E_1 \triangle E_2| = m_1 + m_2 - 2s$. The sum $M_1 \triangle M_2$ is called a*

- 1-*sum, if $s = 0$,*
- 2-*sum, if $s = 1$ and S is not a circuit of M_1, M_2, M_1^* or M_2^*,*
- 3-*sum, if $s = 3$ and S is a circuit of M_1 and M_2 that does not contain a circuit of M_1^* or M_2^*.*

Note that the condition $m_1, m_2 < m_1 + m_2 - 2s$ implies that

$$m_1, m_2 \geq 2s + 1 \tag{3}$$

From the definition of $M_1 \triangle M_2$ the following fact follows easily.

Fact 6.14. *Let C_i be a disjoint union of circuits of M_i, for $i = 1, 2$. If $C_1 \triangle C_2$ is a subset of $E_1 \triangle E_2$ then it is a disjoint union of circuits of $M_1 \triangle M_2$.*

In particular, it follows that for $i = 1, 2$, any circuit C_i of M_i with $C_i \subseteq E_i \backslash S$ is a circuit of $M_1 \triangle M_2$. Further, for 1-sums, circuits are easy to characterize.

Fact 6.15 (Circuits in a 1-sum)**.** *If M is a 1-sum of M_1 and M_2 then any circuit of M is either a circuit of M_1 or a circuit of M_2.*

Thus, if one is interested in the number of circuits, one can assume that the given matroid is not a 1-sum of two smaller matroids.

Definition 6.16 (Connected matroid)**.** *A matroid M is* connected *if it cannot be written as a 1-sum of two smaller matroids.*

A characterization of circuits in a 2-sum or 3-sum is not as easy. Seymour [23, Lemma 2.7] provides a unique representation of the circuits for these cases.

Lemma 6.17 (Circuits in a 2- or 3-sum, [23])**.** *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the sets of circuits of M_1 and M_2, respectively. Let M be a 2- or 3-sum of M_1 and M_2. For $S = E_1 \cap E_2$, we have $|S| = 1$ or $|S| = 3$, respectively. Then for any circuit C of M, one of the following holds:*

1. *$C \in \mathcal{C}_1$ and $S \cap C = \emptyset$, or*

2. *$C \in \mathcal{C}_2$ and $S \cap C = \emptyset$, or*

3. *there exist unique $e \in S$, $C_1 \in \mathcal{C}_1$ and $C_2 \in \mathcal{C}_2$ such that*

$$S \cap C_1 = S \cap C_2 = \{e\} \text{ and } C = C_1 \triangle C_2.$$

Seymour proved the following decomposition theorem for regular matroids.

Theorem 6.18 (Seymour's Theorem, [23])**.** *Every regular matroid can be obtained by means of 1-sums, 2-sums and 3-sums, starting from matroids that are graphic, cographic or R_{10}.*

However, to prove Theorem 2.6, we need a refined version of Seymour's Theorem that was proved by Truemper [29]. Seymour's Theorem decomposes a regular matroid into a sum of two smaller regular matroids. Truemper showed that one of the two smaller regular matroids can be chosen to be graphic, cographic, or the R_{10} matroid. The theorem we write here slightly differs from the one by Truemper [29, Lemma 11.3.18]. A proof of Theorem 6.19 is presented in Appendix A.

Theorem 6.19 (Truemper's decomposition for regular matroids, [29])**.** *Let M be a connected regular matroid, that is not graphic or cographic and is not isomorphic to R_{10}. Let $\widetilde{e}$ be a fixed element of the ground set of M. Then M is a 2-sum or 3-sum of M_1 and M_2, where M_1 is a graphic or cographic matroid, or a matroid isomorphic to R_{10} and M_2 is a regular matroid that contains $\widetilde{e}$.*

7 A Bound on the Number of near-shortest Circuits in Regular Matroids: Proof of Theorem 2.6

In this section, we prove our main technical tool: in a regular matroid, the number of circuits that have size close to a shortest circuit is polynomially bounded (Theorem 2.6). The proof argues along the decomposition provided by Theorem 6.19. First, we need to show a bound on the number of circuits for the two base cases – graphic and cographic matroids.

7.1 Base Case: Graphic and cographic matroids

We actually prove a lemma for graphic and cographic matroids that does more – it gives an upper bound on the number of circuits that contain a fixed element of the ground set. For a weight function $w\colon E \to \mathbb{N}$ on the ground set, the weight of any subset $C \subseteq E$ is defined as $w(C) := \sum_{e \in C} w(e)$.

Lemma 7.1. *Let $M = (E, \mathcal{I})$ be a graphic or cographic matroid, where $|E| = m \geq 2$, and $w\colon E \to \mathbb{N}$ be a weight function. Let $R \subseteq E$ with $|R| \leq 1$ (possibly empty) and r be a positive integer.*

If there is no circuit C in M such that $w(C) < r$ and $C \cap R = \emptyset$, then, for any integer $\alpha \geq 2$, the number of circuits C such that $R \subseteq C$ and $w(C) < \alpha r/2$ is at most $(2(m - |R|))^\alpha$.

Proof. **Part 1:** M **graphic**. (See [26, 28] for a similar argument as in this case.) Let $G = (V, E)$ be the graph corresponding to the graphic matroid M. By the assumption of the lemma, any cycle C in G such that $C \cap R = \emptyset$ has weight $w(C) \geq r$. Consider a cycle C in G with $R \subseteq C$ and $w(C) < \alpha r/2$. Let the edge sequence of the cycle C be $(e_1, e_2, e_3, \ldots, e_q)$ such that if R is nonempty then $R = \{e_1\}$. We choose α edges of the cycle C as follows: Let $i_1 = 1$ and for $j = 2, 3, \ldots, \alpha$, define i_j to be the least index greater than i_{j-1} (if one exists) such that

$$\sum_{a=i_{j-1}+1}^{i_j} w(e_a) \geq r/2. \tag{4}$$

If such an index does not exists then define $i_j = q$. Removing the edges $e_{i_1}, e_{i_2}, \ldots, e_{i_\alpha}$ from C gives us α paths: for $j = 1, 2, \ldots, \alpha - 1$

$$p_j := (e_{i_j+1}, e_{i_j+2}, \ldots, e_{i_{j+1}-1}),$$

and

$$p_\alpha := (e_{i_\alpha+1}, e_{i_\alpha+2}, \ldots, e_q).$$

Note that some of these paths might be empty. By the choice of i_j we know that $w(p_j) < r/2$ for $j = 1, 2, \ldots, \alpha - 1$. Combining (4) with the fact that $w(C) < \alpha r/2$, we obtain that $w(p_\alpha) < r/2$. We associate the ordered tuple of oriented edges $(e_{i_1}, e_{i_2}, \ldots, e_{i_\alpha})$ with the cycle C.

Claim 7.2. *For two distinct cycles C, C' in G, such that both contain R and $w(C), w(C') < \alpha r/2$, the two associated tuples (defined as above) are different.*

Proof. For the sake of contradiction, assume that the associated tuples are same for both the cycles. Thus, C and C' pass through $(e_{i_1}, e_{i_2}, \ldots, e_{i_\alpha})$ with the same orientation of these edges. Further, there are α paths connecting them, say $p_1, p_2, \ldots, p_\alpha$ from C and $p'_1, p'_2, \ldots, p'_\alpha$ from C'. Since C and C' are distinct, for at least one j, it must be that $p_j \neq p'_j$. However, since the starting points and the end points of p_j and p'_j are same, $p_j \cup p'_j$ contains a cycle C''. Moreover, since $w(p_j), w(p'_j) < r/2$, we can deduce that $w(C'') < r$. Finally, since neither of p_j and p'_j contain e_1, we get $C'' \cap R = \emptyset$. This is a contradiction. □

Since, each cycle C with $w(C) < \alpha r/2$ and $R \subseteq C$ is associated with a different tuple, the number of such tuples upper bounds the number of such cycles. We bound the number of tuples depending on whether R is empty or not.

- When R is empty, the number of tuples of α oriented edges is at most $(2m)^\alpha$.
- When $R = \{e_1\}$, the number of choices for the rest of the $\alpha - 1$ edges and their orientation is a most $(2(m-1))^{\alpha-1}$.

Part 2: M **cographic**. Let $G = (V, E)$ be the graph corresponding to the cographic matroid M and let $n = |V|$. Recall from Fact 6.6 that circuits in cographic matroids are inclusionwise minimal cut-sets in G. By the assumption of the lemma, any cut-set C in G with $R \cap C = \emptyset$ has weight $w(C) \geq r$. Note that this implies that G is connected, and therefore $m \geq n - 1$. We want to give a bound on the number of cut-sets $C \subseteq E$ such that $w(C) < \alpha r/2$ and $R \subseteq C$.

We argue similar to the probabilistic construction of a minimum cut of Karger [13]. The basic idea is to contract randomly chosen edges. *Contraction of an edge* $e = (u, v)$ means that all edges between u and v are deleted and then u is identified with v. Note that we get a multi-graph that way: if there were two edges (u, w) and (v, w) before the contraction, they become two parallel edges after identifying u and v. The contracted graph is denoted by G/e. The intuition behind contraction is, that randomly chosen edges are likely to avoid the edges of a minimum cut.

The following algorithm implements the idea. It does $k \leq n$ contractions in the first phase and then chooses a random cut within the remaining nodes of the contracted graph in the second phase that contains the edges of R. Note that any cut-set of the contracted graph is also a cut-set of the original graph.

```
Small Cut ($G = (V, E), R, \alpha$)
Contraction
Repeat $k = n - \alpha - |R|$ times
    randomly choose $e \in E \setminus R$ with probability $w(e)/w(E \setminus R)$
    $G \leftarrow G/e$
    $R \leftarrow R \cup \{$new parallel edges to the edges in $R\}$
Selection
Among all possible cut-sets $C$ in the obtained graph $G$ with $R \subseteq C$,
choose one uniformly at random and return it.
```

Let $C \subseteq E$ be a cut-set with $w(C) < \alpha r/2$ and $R \subseteq C$. We want to give a lower bound on the probability that Small Cut outputs C.

Let $G_0 = G$ and $G_i = (V_i, E_i)$ be the graph after the i-th contraction, for $i = 1, 2, \ldots, k$. Note that G_i has $n_i = n - i$ nodes since each contraction decreases the number of nodes by 1. Let R_i denote the set R after the i-th contraction. That is, if $R = \{e_1\}$, then R_i contains all edges parallel to e_1 in G_i. In case that $R = \emptyset$, also $R_i = \emptyset$. Note that in either case $R_i \subseteq C$, if no edge of C has been contracted till iteration i.

Conditioned on the event that no edge in C has been contracted in iterations 1 to i, the probability that an edge from C is contracted in the $(i + 1)$-th iteration is at most

$$w(C \setminus R_i)/w(E_i \setminus R_i).$$

We know that $w(C \setminus R_i) \leq w(C) < \alpha r/2$. For a lower bound on $w(E_i \setminus R_i)$, consider the graph G'_i obtained from G_i by contracting the edges in R_i. The number of nodes in G'_i will be $n'_i = n - i - |R|$ and its set of edges will be $E_i \setminus R_i$. For any node v in G'_i, consider the set $\delta(v)$ of edges incident on v in G'_i. The set $\delta(v)$ forms a cut-set in G'_i and also in G. Note that $\delta(v) \cap R = \emptyset$, as the edge in R has been contracted in G'_i. Thus, we can deduce that $w(\delta(v)) \geq r$. By summing this up for all nodes in G'_i, we obtain

$$w(E_i \setminus R_i) \geq r\, n'_i/2.$$

Hence,

$$w(E_i \setminus R_i) \geq r\,(n - i - |R|)/2.$$

Therefore the probability that an edge from C is contracted in the $(i+1)$-th iteration is

$$\leq \frac{w(C \setminus R_i)}{w(E_i \setminus R_i)} \leq \frac{\alpha\, r/2}{r\,(n-i-|R|)/2} = \frac{\alpha}{n-i-|R|}.$$

This bound becomes greater than 1, when $i > n - \alpha - |R|$. This is the reason why we stop the contraction process after $k = n - \alpha - |R|$ iterations.

The probability that no edge from C is contracted in any of the rounds is

$$\begin{aligned} &\geq \prod_{i=0}^{k-1}\left(1 - \frac{\alpha}{n-i-|R|}\right) \\ &= \prod_{i=0}^{k-1}\left(1 - \frac{\alpha}{k+\alpha-i}\right) \\ &= \prod_{i=0}^{k-1}\frac{k-i}{k+\alpha-i} \\ &= \frac{1}{\binom{k+\alpha}{k}} \\ &= \frac{1}{\binom{n-|R|}{\alpha}}. \end{aligned}$$

After $n - \alpha - |R|$ contractions we are left with $\alpha + |R|$ nodes. We claim that the number of possible cut-sets on these nodes that contain R is $2^{\alpha-1}$. In case when $R = \emptyset$, then the number of partitions of α nodes into two sets is clearly $2^{\alpha-1}$. When $R = \{e_1\}$, then the number of partitions of $\alpha+1$ nodes, such that the endpoints of e_1 are in different parts, is again $2^{\alpha-1}$. We choose one of these cuts randomly. Thus, the probability that C survives the *contraction* process and is also chosen in the *selection* phase is at least

$$\frac{1}{2^{\alpha-1}\binom{n-|R|}{\alpha}} \geq \frac{1}{(n-|R|)^{\alpha}}.$$

Note that in the end we get exactly one cut-set. Thus, the number of cut-sets C of weight $< \alpha r/2$ and $R \subseteq C$ must be at most $(n-|R|)^{\alpha}$, which is bounded by $(2(m-|R|))^{\alpha}$ because $m \geq n-1$. □

7.2 General regular matroids

In this section, we prove our main result about regular matroids.

Theorem (Theorem 2.6)**.** *Let $M = (E, \mathcal{I})$ be a regular matroid with $m = |E| \geq 2$ and $w\colon E \to \mathbb{N}$ be a weight function. Suppose M does not have any circuit C such that $w(C) < r$, for some number r. Then*

$$|\{\, C \mid C \text{ circuit in } M \text{ and } w(C) < 3r/2 \,\}| \leq 240\, m^5.$$

Proof. The proof is by an induction on m, the size of the ground set. For the base case, let $m \leq 10$. There are at most 2^m circuits in M. This number is bounded by $240\, m^5$, for any $2 \leq m \leq 10$.

For the inductive step, let $M = (E, \mathcal{I})$ be a regular matroid with $|E| = m > 10$ and assume that the theorem holds for all smaller regular matroids. Note that M cannot be R_{10} since $m > 10$. We can also assume that matroid M is neither graphic nor cographic, otherwise the bound follows from Lemma 7.1. By Theorem 6.18, matroid M can be written as a 1-, 2-, or 3-sum of two regular matroids $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$. We define

$$\begin{aligned} S &:= E_1 \cap E_2, \\ s &:= |S|, \\ m_i &:= |E_i|, \text{ for } i = 1, 2, \\ \mathcal{C}_i &:= \{\, C \mid C \text{ is a circuit of } M_i \,\}. \end{aligned}$$

In case that M is the 1-sum of M_1 and M_2, we have $S = \emptyset$, and therefore $m = m_1 + m_2$. By Fact 6.15, the set of circuits of M is the union of the sets of circuits of M_1 and M_2. From the induction hypothesis, we have that M_i has at most $240\, m_i^5$ circuits of weight less than $3r/2$, for $i = 1, 2$. For the number of such circuits in M we get the bound of

$$240\, m_1^5 + 240\, m_2^5 \leq 240\, m^5.$$

This proves the theorem in case of a 1-sum. Hence, in the following it remains to consider the case that M cannot be written as a 1-sum. In other words, we may assume that M is connected (Definition 6.16).

Now we can apply Theorem 6.19 and assume that M is a 2- or 3-sum of M_1 and M_2, where M_1 is a graphic, cographic or the R_{10} matroid, and M_2 is a regular matroid.

We define for $i = 1, 2$ and $e \in S$

$$\begin{aligned} \mathcal{C}_{i,e} &:= \{\, C \mid C \in \mathcal{C}_i \text{ and } C \cap S = \{e\} \,\}, \\ M_i' &:= M_i \setminus S, \\ \mathcal{C}_i' &:= \left\{\, C \mid C \text{ is a circuit of } M_i' \,\right\}. \end{aligned}$$

By Facts 6.10 and 6.11, matroid M_1' is graphic or cographic, and M_2' is regular. Recall from Lemma 6.17 that any circuit C of M can be uniquely written as $C_1 \triangle C_2$ such that one of the following holds:

- $C_1 = \emptyset$ and $C_2 \in \mathcal{C}_2'$.
- $C_2 = \emptyset$ and $C_1 \in \mathcal{C}_1'$.
- $C_1 \in \mathcal{C}_{1,e}$, and $C_2 \in \mathcal{C}_{2,e}$, for some $e \in S$.

Thus, we will view each circuit C of M as $C_1 \triangle C_2$ and consider cases based on how the weight of C is distributed among C_1 and C_2. Recall that the weight function w is defined on $E = E_1 \triangle E_2$. We extend w to a function on $E_1 \cup E_2$ by defining

$$w(e) = 0, \text{ for } e \in S.$$

Now, for the desired upper bound, we will divide the set of circuits of M of weight less than $3r/2$ into three cases.

Case 1. $C_1 \in \mathcal{C}_1'$.

Case 2. $w(C_1) < r/2$. This includes the case that $C_1 = \emptyset$.

Case 3. $w(C_1) \geq r/2$ and $C_2 \neq \emptyset$.

In the following, we will derive an upper bound for the number of circuits in each of the three cases. Then the sum of these bounds will be an upper bound on the number of circuits in M. We will show that the sum is less than $240\, m^5$.

Case 1: $C_1 \in \mathcal{C}_1'$

We have $C_2 = \emptyset$ and $C = C_1 \in \mathcal{C}_1'$. That is, we need to bound the number of circuits of M_1'. Recall that any circuit of M_1' is also a circuit of M. Hence, we know there is no circuit C_1 in M_1' with $w(C_1) < r$. Since M_1' is graphic or cographic, from Lemma 7.1, the number of circuits C_1 of M_1' with $w(C_1) < 3r/2$ is at most $(2(m_1 - s))^3$. Recall from (3) that $m_1 \geq 2s+1$. For any $m_1 \geq 2s+2$, one can verify that

$$(2(m_1 - s))^3 \leq 240\,(m_1 - 2s)^5 =: T_0.$$

On the other hand, when $m_1 = 2s+1$, the number of circuits can be at most $2^{m_1 - s} \leq 2^4$, which is again bounded by T_0.

Case 2: $w(C_1) < r/2$

The main point why we distinguish case 2 is that here C_1 is uniquely determined.

Claim 7.3. *For any $e \in S$, there is at most one circuit $C_1 \in \mathcal{C}_{1,e}$ with $w(C_1) < r/2$.*

Proof. For the sake of contradiction, assume that there are two circuits $C_1, C_1' \in \mathcal{C}_{1,e}$, with $w(C_1), w(C_1') < r/2$. By Fact 6.7, we know that $C_1 \triangle C_1'$ is a disjoint union of circuits in M_1. Note that $C_1 \cap S = C_1' \cap S = \{e\}$, and hence $(C_1 \triangle C_1') \cap S = \emptyset$. Thus, $C_1 \triangle C_1'$ is in fact a disjoint union of circuits in M. Let $\widetilde{C}$ be a subset of $C_1 \triangle C_1'$ that is a circuit. For the weight of $\widetilde{C}$ we have

$$w(\widetilde{C}) \leq w(C_1 \triangle C_1') \leq w(C_1) + w(C_1') < r/2 + r/2 = r.$$

This is a contradiction because M has no circuit of weight less than r. □

Thus, as we will see, it suffices to bound the number of circuits C_2 in M_2. Let C_e^* be the unique choice of a circuit provided by Claim 7.3 (if one exists) for element $e \in S$. For the ease of notation, we assume in the following that there is a C_e^* for every $e \in S$. Otherwise we would delete any element $e \in S$ from M_2 for which no C_e^* exists, and then would consider the resulting smaller matroid. It might actually be that we thereby delete all of S from M_2.

We define a weight function w' on E_2 as follows:

$$w'(e) := \begin{cases} w(C_e^*), & \text{if } e \in S, \\ w(e), & \text{otherwise.} \end{cases}$$

We now have that any circuit C of Case 2 can be written as $C_e^* \triangle C_2$, for some $e \in S$, or $C = C_2$ when $C_1 = \emptyset$. Because C_e^* is unique, the mapping $C \mapsto C_2$ is injective for circuits C of Case 2. Moreover, we have $w(C) = w'(C_2)$. This follows from the definition in case that $C = C_2$. In the other case, we have

$$w(C) = w(C_e^* \triangle C_2) = w(C_e^*) + w(C_2) = w'(C_2). \tag{5}$$

For the equalities, recall that $w(e) = 0$ for $e \in S$.

We conclude that the number of circuits C_2 in M_2 with $w'(C_2) < 3r/2$ is an upper bound on the number of Case 2 circuits C of M with $w(C) < 3r/2$. Now, to get an upper bound on the number of circuits in M_2, we want to apply induction hypothesis. We need the following claim.

Claim 7.4. *There is no circuit C_2 in M_2 with $w'(C_2) < r$.*

Proof. For the sake of contradiction let C_2 be such a circuit. We show that there exists a circuit C' in M with $w(C') < r$. This would contradict the assumption of the lemma.

Case(i): $C_2 \cap S = \emptyset$. Then $C_2 \in \mathcal{C}_2'$ itself yields the contradiction because it is a circuit of M and $w(C_2) = w'(C_2) < r$.

Case(ii): $C_2 \cap S = \{e\}$. By Fact 6.14, the set $C_2 \triangle C_e^*$ is a disjoint union of circuits of M. Let $C' \subseteq C_2 \triangle C_e^*$ be a circuit of M. Then, because $w(e) = 0$, we have

$$w(C') \leq w(C_e^* \triangle C_2) = w(C_e^*) + w(C_2) = w'(C_2) < r.$$

Case(iii): $C_2 \cap S = \{e_1, e_2\}$. By Fact 6.14, similar as in case (ii), there is a set $C' \subseteq C_2 \triangle C_{e_1}^* \triangle C_{e_2}^*$ that is a circuit of M. Then, because $w(e_1) = w(e_2) = 0$, we have

$$w(C') \leq w(C_2 \triangle C_{e_1}^* \triangle C_{e_2}^*) \leq w(C_2) + w(C_{e_1}^*) + w(C_{e_2}^*) = w'(C_2) < r.$$

Case(iv): $C_2 \cap S = \{e_1, e_2, e_3\}$. Since S is a circuit, it must be the case that $C_2 = S$. Since $C_{e_1}^*, C_{e_2}^*, C_{e_3}^*$ and S constitute all the circuits of M_1, the set $C_{e_1}^* \triangle C_{e_2}^* \triangle C_{e_3}^* \triangle S$ contains a circuit C' of M_1. Since $\{e_i\} = C_{e_i}^* \cap S$, for $i = 1, 2, 3$, we know that $S \cap C' = \emptyset$. Thus, $C' \in \mathcal{C}_1'$ is a circuit of M. Since $w(e_1) = w(e_2) = w(e_3) = 0$, we obtain that

$$w(C') \leq w(C_{e_1}^*) + w(C_{e_2}^*) + w(C_{e_3}^*) = w'(S) = w'(C_2) < r.$$

This proves the claim. □

By Claim 7.4, we can apply the induction hypothesis for M_2 with the weight function w'. We get that the number of circuits C_2 in M_2 with $w'(C_2) < 3r/2$ is bounded by

$$T_1 := 240\, m_2^5.$$

As mentioned above, this is an upper bound on the number of circuits C in M with $w(C) < 3r/2$ in Case 2.

Case 3: $w(C_1) \geq r/2$

Since $w(C) = w(C_1) + w(C_2) < 3r/2$, we have $w(C_2) < r$ in this case. We also assume that $C_2 \neq \emptyset$. Hence, there is an $e \in S$ such that $C_1 \in \mathcal{C}_{1,e}$ and $C_2 \in \mathcal{C}_{2,e}$.

Let T_2 be an upper bound on the number of circuits $C_1 \in \mathcal{C}_{1,e}$ with $w(C_1) < 3r/2$, for each $e \in S$. Let T_3 be an upper bound on the number of circuits $C_2 \in \mathcal{C}_{2,e}$ with $w(C_2) < r$, for each $e \in S$. Because there are s choices for the element $e \in S$, the number of circuits $C = C_1 \triangle C_2$ with $w(C) < 3r/2$ in Case 3 will be at most

$$s\, T_2\, T_3. \tag{6}$$

To get an upper bound on the number of circuits in $\mathcal{C}_{1,e}$ and $\mathcal{C}_{2,e}$, consider two matroids $M_{1,e}$ and $M_{2,e}$. These are obtained from M_1 and M_2, respectively, by deleting the elements in $S \setminus \{e\}$. The ground set cardinalities of these two matroids are $m_1 - s + 1$ and $m_2 - s + 1$.

We know that for $i = 1, 2$, any circuit C_i of $M_{i,e}$ with $e \notin C_i$ is in $\mathcal{C}_i'$ and hence, is a circuit of M. Therefore, there is no circuit C_i of $M_{i,e}$ with $e \notin C_i$ and $w(C_i) < r$. Using this fact, we want to bound the number of circuits C_i of $M_{i,e}$ with $e \in C_i$. We start with $M_{1,e}$.

Claim 7.5. *An upper bound on the number of circuits C_1 in $M_{1,e}$ with $e \in C_1$ and $w(C_1) < 3r/2$ is*

$$T_2 := \min\{8(m_1 - s)^3, 2^{m_1 - s}\} \tag{7}$$

Proof. Recall that the decomposition of M was such that M_1 is graphic, cographic or the R_{10} matroid.

Case(i). When M_1 is graphic or cographic, the matroid $M_{1,e}$ falls into the same class by Fact 6.10. Recall that the ground set of $M_{1,e}$ has cardinality $m_1 - s + 1$. In this case, we apply Lemma 7.1 to $M_{1,e}$ with $R = \{e\}$ and $\alpha = 3$ and get a bound of $8(m_1 - s)^3$. The number of circuits containing e is also trivially bounded by the number of all subsets that contain e, which is 2^{m_1-s}. Thus, we get Equation (7).

Case(ii). When M_1 is the R_{10} matroid, then the cardinality of $M_{1,e}$, that is $m_1 - s + 1$, is at most 10. In this case again, we use the trivial upper bound of 2^{m_1-s}. One can verify that when $m_1 - s + 1 \leq 10$ then $2^{m_1-s} \leq 8(m_1 - s)^3$. Thus, we get Equation (7). □

Next, we want to bound the number of circuits C_2 in $M_{2,e}$ with $e \in C_2$ and $w(C_2) < r$. This is done in Lemma 7.7 below, where we get a bound of $T_3 := 48(m_2 - s)^2$.

To finish Case 3, we now have

$$\begin{aligned} T_2 &= \min\{8(m_1 - s)^3, 2^{m_1-s}\}, \\ T_3 &= 48(m_2 - s)^2. \end{aligned}$$

By Equation (6), the number of circuits in Case 3 is bounded by $s\,T_2\,T_3$.

Claim 7.6. *For $s = 1, 3$ and $m_1 \geq 2s + 1$,*

$$s\,T_2\,T_3 \leq 2400\,(m_1 - 2s)^3\,(m_2 - s)^2.$$

Proof. We consider $s\,T_2$. For $m_1 - 2s \geq 12$, we have

$$s \cdot 8(m_1 - s)^3 \leq 50(m_1 - 2s)^3.$$

On the other hand, when $m_1 - 2s \leq 11$,

$$s \cdot 2^{m_1-s} \leq 50(m_1 - 2s)^3.$$

This proves the claim. □

Summing up Cases 1, 2 and 3

Finally we add the bounds on the number of circuits of Case 1, 2 and 3. The total upper bound we get is

$$\begin{aligned} T_0 + T_1 + s\,T_2\,T_3 &\leq 240\,(m_1 - 2s)^5 + 240\,m_2^5 + 240\binom{5}{2}(m_1 - 2s)^3(m_2 - s)^2 \\ &\leq 240\,(m_2 + m_1 - 2s)^5 \\ &\leq 240\,m^5 \end{aligned}$$

This completes the proof of Theorem 2.6, except for the bound on T_3 that we show in Lemma 7.7. □

Now we move on to prove Lemma 7.7, which completes the proof of Theorem 2.6. The lemma is similar to Theorem 2.6, but differs in two aspects: (i) we want to count circuits up to a smaller weight bound, that is, r, and (ii) we have a weaker assumption that there is no circuit of weight less than r that does not contain a fixed element e.

Lemma 7.7. *Let $M = (E, \mathcal{I})$ be a connected, regular matroid with ground set size $m \geq 2$ and $w\colon E \to \mathbb{N}$ be a weight function on E. Let r be a positive integer and let $\widetilde{e} \in E$ be any fixed element of the ground set. Assume that there is no circuit C in M such that $\widetilde{e} \notin C$ and $w(C) < r$. Then, the number of circuits C in M such that $\widetilde{e} \in C$ and $w(C) < r$ is bounded by $48(m-1)^2$.*

Proof. We closely follow the proof of Theorem 2.6. We proceed again by an induction on m, the size of the ground set E.

For the base case, let $m \leq 10$. There are at most 2^{m-1} circuits that contain $\widetilde{e}$. This number is bounded by $48(m-1)^2$, for any $2 \leq m \leq 10$.

For the inductive step, let $M = (E, \mathcal{I})$ be a regular matroid with $|E| = m > 10$ and assume that the theorem holds for all smaller regular matroids. Since $m > 10$, matroid M cannot be R_{10}. If M is graphic or cographic, then the bound of the lemma follows from Lemma 7.1. Thus, we may assume that M is neither graphic nor cographic.

By Theorem 6.18, matroid M can be written as a 1-, 2-, or 3-sum of two regular matroids $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$. We use the same notation as Theorem 2.6,

$$\begin{aligned} S &= E_1 \cap E_2, \\ s &= |S|, \\ m_i &= |E_i|, \text{ for } i = 1, 2, \\ \mathcal{C}_i &= \{\, C \mid C \text{ is a circuit of } M_i \,\}. \end{aligned}$$

The case that M is a 1-sum of M_1 and M_2 is again trivial. Hence, we may assume that M is connected. By Theorem 6.19, M is a 2-sum or a 3-sum of M_1 and M_2, where M_1 is a graphic, cographic or the R_{10} matroid, and M_2 is a regular matroid containing $\widetilde{e}$. For $i = 1, 2$ and $e \in S$, define

$$\mathcal{C}_{i,e} \;:=\; \{\, C \mid C \in \mathcal{C}_i \text{ and } C \cap S = \{e\} \,\}.$$

Also the weight function w is extended on S by $w(e) = 0$, for any $e \in S$.

We again view each circuit C of M as $C_1 \triangle C_2$ and consider cases based on how the weight of C is distributed among C_1 and C_2. Note that $\widetilde{e}$ is in M_2 and we are only interested in circuits C that contain $\widetilde{e}$. Hence, we have $\widetilde{e} \in C_2$. Therefore we do not have the case where $C_2 = \emptyset$. We consider the following two cases.

Case (i). $w(C_1) < r/2$.

Case (ii). $w(C_1) \geq r/2$.

We will give an upper bound for the number of circuits in each of the two cases.

Case (i): $w(C_1) < r/2$

Since $\widetilde{e} \notin C_1$, we can literally follow the proof for Case 2 from Theorem 2.6 for this case. We have again Claim 7.3, that C_1 is uniquely determined as $C_1 = C_e^*$, for $e \in S$, or $C_1 = \emptyset$. Therefore the mapping $C \mapsto C_2$ is injective. The only point to notice now is that the mapping maintains that $\widetilde{e} \in C$ if and only if $\widetilde{e} \in C_2$. With the same definition of w', we also have $w(C) = w'(C_2)$. Therefore it suffices to get an upper bound on the number of circuits C_2 in M_2 with $w'(C_2) < r$ and $\widetilde{e} \in C_2$.

To apply the induction hypothesis, we need the following variant of Claim 7.4. It has a similar proof.

Claim 7.8. *There is no circuit C_2 in M_2 such that $w'(C_2) < r$ and $\widetilde{e} \notin C_2$.*

By the induction hypothesis applied to M_2, the number of circuits C_2 in M_2 with $w'(C_2) < r$ and $\widetilde{e} \in C_2$ is bounded by

$$T_0 := 48(m_2 - 1)^2.$$

Case (ii): $w(C_1) \geq r/2$

Since $w(C) = w(C_1) + w(C_2) < r$, we have $w(C_2) < r/2$ in this case. This is the major difference to Case 3 from Theorem 2.6 where the weight of C_2 was only bounded by r. Hence, now we have again a uniqueness property similar as in Claim 7.3, but for C_2 this time. A difference comes with $\widetilde{e}$. But the proof remains the same.

Claim 7.9. *For any $e \in S$, there is at most one circuit $C_2 \in \mathcal{C}_{2,e}$ with $w(C_2) < r/2$ and $\widetilde{e} \in C_2$.*

We conclude that any circuit C in case (ii) can be written as $C = C_1 \triangle C_e^*$, for a $e \in S$ and the unique circuit $C_e^* \in \mathcal{C}_{2,e}$. Therefore the mapping $C \mapsto C_1$ is injective for the circuits C of case (ii). Thus, it suffices to count circuits $C_1 \in \mathcal{C}_{1,e}$ with $w(C_1) < r$, for every $e \in S$.

Let $e \in S$ and consider the matroid $M_{1,e}$ obtained from M_1 by deleting the elements in $S \setminus \{e\}$. It has $m_1 - s + 1$ elements. Since M_1 is a graphic, cographic or R_{10}, the matroid $M_{1,e}$ is graphic or cographic by Facts 6.10 and 6.11. The circuits in $\mathcal{C}_{1,e}$ are also circuits of $M_{1,e}$.

Any circuit C_1 of $M_{1,e}$ with $e \notin C_1$ is also a circuit of M. Thus, there is no circuit C_1 of $M_{1,e}$ with $e \notin C_1$ and $w(C_1) < r$. Therefore we can apply Lemma 7.1 to $M_{1,e}$ with $R = \{e\}$. We conclude that the number of circuits $C_1 \in \mathcal{C}_{1,e}$ with $w(C_1) < r$ is at most

$$T_1 := 4(m_1 - s)^2.$$

Since there are s choices for $e \in S$, we obtain a bound of $s\,T_1$.

There is also a trivial bound of $s\,2^{m_1 - s}$ on the number of such circuits. We take the minimum of the two bounds. Recall from the definition of 2-sum and 3-sum that $m_1 \geq 2s + 1$.

Claim 7.10. *For $s = 1$ or 3 and $m_1 \geq 2s + 1$,*

$$\min\{s\,2^{m_1 - s}, 4s\,(m_1 - s)^2\} \leq 48(m_1 - 2s)^2.$$

Proof. One can verify that when $m_1 - 2s \leq 4$ then

$$s\,2^{m_1 - s} \leq 48(m_1 - 2s)^2.$$

On the other hand, when $m_1 - 2s \geq 5$ then

$$4s\,(m_1 - s)^2 \leq 48(m_1 - 2s)^2.$$

This proves the claim. □

Hence, we get a bound of $48(m_1 - 2s)^2$ on the number circuits in case (ii). Now we add the number of circuits of case (i) and (ii) and get a total upper bound of

$$\begin{aligned} 48(m_2 - 1)^2 + 48(m_1 - 2s)^2 &\leq 48(m_2 - 1 + m_1 - 2s)^2 \\ &\leq 48(m - 1)^2. \end{aligned}$$

This gives us the desired bound and completes the proof of Lemma 7.7. □

References

[1] Manindra Agrawal, Thanh Minh Hoang, and Thomas Thierauf. The polynomially bounded perfect matching problem is in NC^2. In *24th International Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 4393 of *Lecture Notes in Computer Science*, pages 489–499. Springer Berlin Heidelberg, 2007.

[2] Vikraman Arvind and Partha Mukhopadhyay. Derandomizing the isolation lemma and lower bounds for circuit size. In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques, 11th International Workshop, APPROX, and 12th International Workshop, RANDOM*, pages 276–289, 2008.

[3] Robert E Bixby. Kuratowski's and Wagner's theorems for matroids. *Journal of Combinatorial Theory, Series B*, 22(1):31 – 53, 1977.

[4] Andreas Björklund and Thore Husfeldt. Shortest two disjoint paths in polynomial time. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, pages 211–222, 2014.

[5] C. Bourke, R. Tewari, and N. V. Vinodchandran. Directed planar reachability is in unambiguous log-space. *ACM Trans. Comput. Theory*, 1:4:1–4:17, February 2009.

[6] Elias Dahlhaus and Marek Karpinski. Matching and multidimensional matching in chordal and strongly chordal graphs. *Discrete Applied Mathematics*, 84(13):79 – 91, 1998.

[7] Samir Datta, Raghav Kulkarni, and Sambuddha Roy. Deterministically isolating a perfect matching in bipartite planar graphs. *Theory of Computing Systems*, 47:737–757, 2010.

[8] Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite perfect matching is in quasi-NC. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 754–763, 2016.

[9] Michael L. Fredman, János Komlós, and Endre Szemerédi. Storing a sparse table with O(1) worst case access time. *J. ACM*, 31(3):538–544, June 1984.

[10] Dima Grigoriev and Marek Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in NC (extended abstract). In *28th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 166–172, 1987.

[11] Rohit Gurjar and Thomas Thierauf. Linear matroid intersection is in quasi-NC. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 821–830, New York, NY, USA, 2017. ACM.

[12] Vivek Anand T. Kallampally and Raghunath Tewari. Trading determinism for time in space bounded computations. In *41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016, August 22-26, 2016 - Kraków, Poland*, pages 10:1–10:13, 2016.

[13] David R. Karger. Global min-cuts in RNC, and other ramifications of a simple min-cut algorithm. In *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '93, pages 21–30, Philadelphia, PA, USA, 1993. Society for Industrial and Applied Mathematics.

[14] Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987.

[15] Mohan Nair. On Chebyshev-type inequalities for primes. *The American Mathematical Monthly*, 89(2):126–129, 1982.

[16] H. Narayanan, Huzur Saran, and Vijay V. Vazirani. Randomized parallel algorithms for matroid union and intersection, with applications to arboresences and edge-disjoint spanning trees. *SIAM J. Comput.*, 23(2):387–397, 1994.

[17] S. Onn. *Nonlinear Discrete Optimization: An Algorithmic Theory*. Zurich lectures in advanced mathematics. European Mathematical Society Publishing House, 2010.

[18] James G. Oxley. *Matroid Theory (Oxford Graduate Texts in Mathematics)*. Oxford University Press, Inc., New York, NY, USA, 2006.

[19] Klaus Reinhardt and Eric Allender. Making nondeterminism unambiguous. *SIAM Journal on Computing*, 29(4):1118–1131, 2000.

[20] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Inc., New York, NY, USA, 1986.

[21] Alexander Schrijver. *Combinatorial optimization: polyhedra and efficiency. Vol. A. , Paths, flows, matchings*. Algorithms and combinatorics. Springer-Verlag, Berlin, Heidelberg, New York, 2003.

[22] Alexander Schrijver. *Combinatorial optimization: polyhedra and efficiency. Vol. B. , Matroids, trees, stable sets*. Algorithms and combinatorics. Springer-Verlag, Berlin, Heidelberg, New York, N.Y., et al., 2003.

[23] Paul D. Seymour. Decomposition of regular matroids. *J. Comb. Theory, Ser. B*, 28(3):305–359, 1980.

[24] Mohit Singh and Nisheeth K. Vishnoi. Entropy, optimization and counting. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 50–59. ACM, 2014.

[25] Damian Straszak and Nisheeth K. Vishnoi. Computing Maximum Entropy Distributions Everywhere. *ArXiv e-prints*, November 2017.

[26] Ashok Subramanian. A polynomial bound on the number of light cycles in an undirected graph. *Information Processing Letters*, 53(4):173 – 176, 1995.

[27] Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In *58th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2017, 15-17 October, 2017, Berkeley, California, USA*, 2017.

[28] C. P. Teo and K. M. Koh. The number of shortest cycles and the chromatic uniqueness of a graph. *Journal of Graph Theory*, 16(1):7–15, 1992.

[29] Klaus Truemper. *Matroid Decomposition*. Leibniz, Plano, Texas (USA), 1998.

[30] Dieter van Melkebeek and Gautam Prakriya. Derandomizing isolation in space-bounded settings. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 5:1–5:32, 2017.

[31] Avi Wigderson. NL/poly $\subseteq \oplus$ L/poly. In *Proceedings of the Ninth Annual Structure in Complexity Theory Conference, Amsterdam, The Netherlands, June 28 - July 1, 1994*, pages 59–62, 1994.

A Proof of Theorem 6.19

We show some properties of the sum operation on matroids. First note that the k-sum operations are commutative because their definition is based on symmetric set differences which is commutative. Further, it is known that the k-sum operations are also associative in some cases. We give a proof here for completeness. The 2-sum operation is denoted by $\oplus_2$.

Lemma A.1 (Associativity). *Let $M = M_1 \oplus_2 M_2$ with e being the common element in M_1 and M_2. Let $M_2 = M_3 \triangle M_4$ be a k-sum for $k = 2$ or 3 with the common set S. Further, let $e \in M_3$. Then*

$$M = M_1 \oplus_2 (M_3 \triangle M_4) = (M_1 \oplus_2 M_3) \triangle M_4, \tag{8}$$

where $M_1 \oplus_2 M_3$ is defined via the common element e and $(M_1 \oplus_2 M_3) \triangle M_4$ is defined via the common set S.

Proof. We show that the matroids in Equation (8) have the same circuits. This implies the equality. Let E_i denote the ground set of M_i, for $i = 1, 2, 3, 4$.

Let C be a circuit of $M = M_1 \oplus_2 M_2$. We consider the nontrivial case in Lemma 6.17: we have $C = C_1 \triangle C_2$ and $e \in C_1 \cap C_2$, where C_1 and C_2 are circuits in M_1 and $M_2 = M_3 \triangle M_4$, respectively. Similarly, we have $C_2 = C_3 \triangle C_4$, for circuits C_3 and C_4 of M_3 and M_4, respectively. By our assumption, we have $e \in C_3$. It follows that $C_1 \triangle C_3 \subseteq E_1 \triangle E_3$ is a circuit of $M_1 \oplus_2 M_3$. Since C_4 is a circuit of M_4, we get from Fact 6.14 that $(C_1 \triangle C_3) \triangle C_4$ is a disjoint union of circuits in $(M_1 \oplus_2 M_3) \triangle M_4$.

For the reverse direction, consider a circuit C of $(M_1 \oplus_2 M_3) \triangle M_4$. Similarly as above by Lemma 6.17, we can write $C = C' \triangle C_4$, where C' and C_4 are circuits of $M_1 \oplus_2 M_3$ and M_4, respectively, with $S \cap C' = S \cap C_4$. Further, $C' = C_1 \triangle C_3$, where C_1 and C_3 are circuits in M_1 and M_3, respectively. Since S is disjoint from E_1, it must be that $S \cap C' = S \cap C_3$. Thus, $C_3 \triangle C_4 \subseteq E_3 \triangle E_4$ is a union of disjoint circuits in $M_3 \triangle M_4$. Since, C_1 is a circuit in M_1, it follows that $C_1 \triangle (C_3 \triangle C_4)$ is a disjoint union of circuits in $M_1 \oplus_2 (M_3 \triangle M_4)$.

Thus, we have shown that a circuit of one matroid in Equation (8) is a disjoint union of circuits in the other matroid and vice-versa. Consequently, by the minimality of circuits, it follows that their sets of circuits must be the same. □

Truemper proves the statement of Theorem 6.19 for 3-connected matroids.

Definition A.2 (3-connected matroid [29]). *A matroid $M = (E, \mathcal{I})$ is said to be 3-connected if for $\ell = 1, 2$, and for any partition $E = E_1 \cup E_2$ with $|E_1|, |E_2| \geq \ell$ we have*

$$\operatorname{rank}(E_1) + \operatorname{rank}(E_2) \geq \operatorname{rank}(E) + \ell.$$

Lemma A.3 (Decomposition of a matroid [29]). *If a binary matroid is not 3-connected then it can be written as a 2-sum or 1-sum of two smaller binary matroids.*

Theorem A.4 (Truemper's decomposition for 3-connected matroids, [29]). *Let M be a 3-connected, regular matroid, that is not graphic or cographic and is not isomorphic to R_{10}. Let $\widetilde{e}$ be a fixed element of the ground set of M. Then M is a 3-sum of M_1 and M_2, where M_1 is a graphic or a cographic matroid and M_2 is a regular matroid that contains $\widetilde{e}$.*

Theorem 6.19 can be seen as the extension of Theorem A.4 to connected regular matroids.

Proof of Theorem 6.19. The proof is by induction on the ground set size of M. If M is 3-connected then the statement is true by Theorem A.4. If M is not 3-connected, then we invoke Lemma A.3. Since M is connected, it can be written as 2-sum of two matroids $M = M_1 \oplus_2 M_2$. From the definition of a 2-sum, it follows that M_1 and M_2 are minors of M (see [23, Lemma 2.6]), and thus are regular matroids by Fact 6.10. Without loss of generality, let the fixed element $\widetilde{e}$ be in M_2. If M_1 is graphic, cographic or R_{10} then we are done.

Suppose, M_1 is neither of these. Let e' be the element common in the ground sets of M_1 and M_2. By induction, M_1 is a 2-sum or a 3-sum $M_1 = M_{11} \triangle M_{12}$, where M_{12} is a regular matroid that contains e' and M_{11} is a graphic or cographic matroid, or a matroid isomorphic to R_{10}. Since M_{12} and M_2 share e', we can take the 2-sum of these two matroids using e'. By Lemma A.1, the matroid M is the same as $M_{11} \triangle (M_{12} \oplus_2 M_2)$. The matroid $M_{12} \oplus_2 M_2$ contains $\widetilde{e}$ and is regular because both M_{12} and M_2 are regular (see [29, Theorem 11.3.14]). Thus, the two matroids M_{11} and $M_{12} \oplus_2 M_2$ satisfy the desired properties. □