Isolating a Vertex via Lattices: Polytopes with Totally Unimodular Faces

Rohit Gurjar[1]
California Institute of Technology, USA

Thomas Thierauf[2]
Aalen University, Germany

Nisheeth K. Vishnoi
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.

2012 ACM Subject Classification Mathematics of computing → Combinatorial optimization, Mathematics of computing → Matroids and greedoids, Theory of computation → Pseudorandomness and derandomization

Keywords and phrases Derandomization, Isolation Lemma, Total unimodularity, Near-shortest vectors in Lattices, Regular matroids

Digital Object Identifier 10.4230/LIPIcs.ICALP.2018.74

Related Version A full version of the paper is available at [11], `https://arxiv.org/abs/1708.02222`.

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 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

[1] 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).
[2] Supported by DFG grant TH 472/4.

45th International Colloquium on Automata, Languages, and Programming (ICALP 2018).
Editors: Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella;
Article No. 74; pp. 74:1–74:14

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

then it has found numerous other applications, in both algorithms and complexity: e.g., a reduction from CLIQUE to UNIQUE-CLIQUE [14], NL/poly $\subseteq \oplus$L/poly [29], NL/poly = UL/poly [17], an RNC-algorithm for linear matroid intersection [15], and an RP-algorithm for disjoint paths [3]. 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, 5, 6, 9], s-t paths in directed graphs [4, 12, 28]. Recently, there has been significant progress on deterministic isolation for perfect matchings in bipartite graphs [7] and subsequently, in general graphs [25], and matroid intersection [10], 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 [25]. This generalizes the isolation result for perfect matchings in a bipartite graph [7], 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 [7]. 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 [10]. 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 [20, 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 [19, 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 [20] gives an excellent overview of polytopes that satisfy the condition required in Theorem 2.3 such as

- $R - S$ bibranching polytope [20, Section 54.6]
- directed cut cover polytope [20, Section 55.2]
- submodular flow polyhedron [20, Theorem 60.1]
- lattice polyhedron [20, Theorem 60.4]
- submodular base polytope [20, Section 44.3]
- many other polytopes defined via submodular and supermodular set functions [20, 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 [7, 10], 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 [21]. Theorem 2.6 answers a question raised by Subramanian [24] 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 [24, 26]) 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 [25], 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 [22, 23].

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 $x^S_e = 1$ if $e \in S$ and $x^S_e = 0$ otherwise. 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 [7, 10]. 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,

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

Let $\lambda(L) := \min\{ \|v\| \mid 0 \neq v \in L \}$ denote the length of the shortest nonzero vector of a lattice 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 recall a few basic definitions from matroid theory. 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. 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 $P(\mathcal{B})$.

In the following, we will denote the size of the set E by m. 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. See the full version [11] for a proof.

▶ **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 $w'\colon E \to \{0, 1, \ldots, N-1\}$ be another weight function and let F' be the face that minimizes the combined weight function $mN\, w + w'$. Then $F' \subseteq F$.*

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 $w' \in \{0, 1, \ldots, N-1\}^E$ 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 $v_1, v_2, \ldots, v_k$, 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 [8, 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 $w_1, w_2, \ldots, w_q \in \{0, 1, 2, \ldots, q\}^m$ such that for any set of nonzero vectors $v_1, v_2, \ldots, v_k$ in $\{-(t-1), \ldots, 0, 1, \ldots, t-1\}^m$ there exists a $j \in [q]$ such that for all $i \in [k]$ we have $\langle w_j, v_i \rangle \neq 0$. (see the full version [11] for a proof).*

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 $\{v_1, v_2, \ldots, v_k\}$. (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 $i = 1, 2, \ldots, p$, define

- F_{i-1}: the face of $P(\mathcal{B})$ minimizing w_{i-1}
- w'_i: a weight vector in $\{0, 1, \ldots, N-1\}^E$ 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 $i = 0, 1, 2, \ldots, p$, 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

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

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 (1) 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., $y_1 = y_2$. ◀

We get a bound of $m^{O(\log m)}$ on both the number of weight vectors we need to try and the weights involved, which finishes the proof of Theorem 2.4 (see the full version [11]).

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 $\text{supp}(v) \subsetneq \text{supp}(u)$, 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 [16, 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 [16]). 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 [16, 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. The following lemma shows that the two definitions of circuits, 1) for TU matrices and 2) for regular matroids, coincide. See the full version [11] for a proof.

▶ **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).*

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

Here we give a proof overview of Theorem 2.6; see the full version [11] for a complete proof. Theorem 2.6 states that for a regular matroid, the number of near-shortest circuits – circuits whose size is a constant multiple of the shortest circuit size – is polynomially bounded. The starting point of the proof of this theorem is a remarkable result of Seymour [21] 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 the full version [11] 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 [18] (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 [24] and on the number of near min-cuts in a graph [13]. 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 [27]. 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, we first show 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 $\widetilde{e}$. 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.

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. doi:10.1007/978-3-540-70918-3_42.
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. doi:10.1007/978-3-540-85363-3_23.
3. 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. doi:10.1007/978-3-662-43948-7_18.
4. 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. doi:10.1145/1490270.1490274.
5. Elias Dahlhaus and Marek Karpinski. Matching and multidimensional matching in chordal and strongly chordal graphs. *Discrete Applied Mathematics*, 84(1–3):79–91, 1998. doi:10.1016/S0166-218X(98)00006-7.
6. Samir Datta, Raghav Kulkarni, and Sambuddha Roy. Deterministically isolating a perfect matching in bipartite planar graphs. *Theory of Computing Systems*, 47:737–757, 2010. doi:10.1007/s00224-009-9204-8.
7. 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. doi:10.1145/2897518.2897564.
8. 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, 1984. doi:10.1145/828.1884.
9. 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. doi:10.1109/SFCS.1987.56.
10. 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. doi:10.1145/3055399.3055440.
11. Rohit Gurjar, Thomas Thierauf, and Nisheeth K. Vishnoi. Isolating a vertex via lattices: Polytopes with totally unimodular faces. *ArXiv e-prints*, abs/1708.02222, August 2017. arXiv:1708.02222.
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. doi:10.4230/LIPIcs.MFCS.2016.10.
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. URL: http://dl.acm.org/citation.cfm?id=313559.313605.
14. Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987. doi:10.1007/BF02579206.

15 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. doi:10.1137/S0097539791195245.

16 S. Onn. *Nonlinear Discrete Optimization: An Algorithmic Theory.* Zurich lectures in advanced mathematics. European Mathematical Society Publishing House, 2010. URL: https://books.google.co.il/books?id=wzAGMQAACAAJ.

17 Klaus Reinhardt and Eric Allender. Making nondeterminism unambiguous. *SIAM Journal on Computing*, 29(4):1118–1131, 2000. doi:10.1137/S0097539798339041.

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

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

20 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.

21 Paul D. Seymour. Decomposition of regular matroids. *J. Comb. Theory, Ser. B*, 28(3):305–359, 1980. doi:10.1016/0095-8956(80)90075-1.

22 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.

23 Damian Straszak and Nisheeth K. Vishnoi. Computing Maximum Entropy Distributions Everywhere. *ArXiv e-prints*, 2017. arXiv:1711.02036.

24 Ashok Subramanian. A polynomial bound on the number of light cycles in an undirected graph. *Information Processing Letters*, 53(4):173–176, 1995. doi:10.1016/0020-0190(94)00202-A.

25 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.

26 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.

27 Klaus Truemper. *Matroid Decomposition.* Leibniz, Plano, Texas (USA), 1998.

28 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. doi:10.4230/LIPIcs.CCC.2017.5.

29 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. doi:10.1109/SCT.1994.315817.