Electronic Colloquium on Computational Complexity, Report No. 182 (2016)

Linear Matroid Intersection is in quasi-NC*

Rohit Gurjar[1] and Thomas Thierauf[2]

[1]Tel Aviv University
[2]Aalen University

November 14, 2016

Abstract

Given two matroids on the same ground set, the matroid intersection problem asks to find a common independent set of maximum size. We show that the linear matroid intersection problem is in quasi-NC^2. That is, it has uniform circuits of quasi-polynomial size $n^{O(\log n)}$, and $O(\log^2 n)$ depth. This generalizes the similar result for the bipartite perfect matching problem. We do this by an almost complete derandomization of the Isolation lemma for matroid intersection.

Our result also implies a blackbox singularity test for symbolic matrices of the form $A_0 + A_1 z_1 + A_2 z_2 + \cdots + A_m z_m$, where the matrices $A_1, A_2, \ldots, A_m$ are of rank 1.

1 Introduction

Matroids are combinatorial structures that generalize the notion of *linear independence* in Linear Algebra. A matroid M is a pair $M = (E, \mathcal{I})$, where E is the finite ground set and $\mathcal{I} \subseteq \mathcal{P}(E)$ is a family of subsets of E that are said to be the *independent sets*. There are two axioms the independent sets must satisfy: (1) closure under subsets and (2) the *augmentation property*. (See the Preliminary Section for exact definitions.)

Matroids are motivated by Linear Algebra. For an $n \times m$ matrix V over some field, let $v_1, v_2, \ldots, v_m$ be the column vectors of V, in this order. We define the ground set $E = \{1, 2, \ldots, m\}$ as the set of indices of the columns of V. A set $I \subseteq E$ is defined to be independent, if the collection of vectors v_i, for $i \in I$, is linearly independent. Then $M = (E, \mathcal{I})$ is a matroid: Any subset of of an independent set is again independent. The augmentation property is equivalent to the Steinitz Exchange Lemma for two bases of the vector space spanned by the column vectors of V. A matroid is called *linear*, if it can be represented by a matrix in the above sense.

Although we will formulate most of our results in terms of general matroids, our main result is for *linear* matroids. Hence, for a reader who is unfamiliar with matroid theory, it suffices to think of a matroid simply as a matrix as described above.

The augmentation property implies that all inclusion-wise maximal independent sets have the same size. A maximal independent set is called a *base* of the matroid. The *matroid problem* consists in computing a base of a given matroid. It can be solved efficiently by a simple *greedy algorithm*, provided that we can efficiently test whether a set is independent. There is also a parallel (NC)

*Supported by DFG grant TH 472/4. Email: `rohitgurjar0@gmail.com`, `thomas.thierauf@uni-ulm.de`

ISSN 1433-8092

algorithm: for each i, include the i-th element in the base if it is independent of the first $i-1$ elements.

In the *matroid intersection problem*, we are given two matroids M_1, M_2 over the same ground set. One has to find the largest set which is independent in both matroids. In the Linear Algebra example, we are given two matrices U and V of the same dimensions. We want to compute the largest set I of indices, such that the columns of U and the columns of V indexed by I are both independent sets. As another example, the bipartite matching problem can be expressed as a matroid intersection problem.

The matroid intersection problem can be solved in polynomial time by an algorithm due to Edmonds [Edm68, Edm79]. Edmonds' algorithm is a generalization of the famous augmenting path algorithm for bipartite matching. In the case of linear matroids, its parallel complexity is also similar to the matching problem. Narayanan, Saran, and Vazirani [NSV94] presented a randomized NC-algorithm based on the *Isolation Lemma*. Applied to matroid intersection, the Isolation Lemma states that randomly chosen weights for the elements of the ground sets isolate a common base, i.e., there is a unique minimum weight basis set, with high probability.

In order to obtain *deterministic* parallel algorithms, the derandomization of the Isolation Lemma is a major open problem. Recently, the authors together with Fenner [FGT16] (almost) achieved this in the case of bipartite perfect matching and presented a quasi-NC-algorithm for this problem. In the current paper, we generalize the matching algorithm to a quasi-NC-algorithm for linear matroid intersection. Our main result is:

Linear Matroid Intersection is in quasi-NC.

This puts a rich class of problems in quasi-NC.

Our technique is to deterministically construct a weight assignment that isolates a base in the matroid intersection. Hence this can again be seen as a derandomization of the Isolation Lemma in this setting. Following the approach of the matching result [FGT16], we look at the isolation question in the corresponding polytope. However, since the matroid intersection polytope has a more complicated description than the bipartite matching polytope, we need more ideas. As before, our weights have $O(\log^2 n)$ bits, and so we get circuits of quasi-polynomial size $n^{O(\log n)}$. Hence, we get linear matroid intersection in quasi-NC^2. It remains open whether the problem is in NC. We would like to point out that our isolating weight assignment actually works for general matroid intersection and even for polymatroid intersection. However, we get the quasi-NC-bound only in the case of linear matroids, because only there we have a connection to the determinant. Derandomizing the Isolation Lemma in this setting also gives a blackbox polynomial identity testing algorithm for an interesting class of polynomials.

1.1 Polynomial Identity Testing (PIT)

The polynomial identity problem asks whether a given multivariate polynomial is the zero-polynomial. The polynomial is given as an arithmetic computational model such that evaluating the polynomial at a point is easy. Various arithmetic models have been considered for the problem, for example, arithmetic circuits, arithmetic branching programs, and determinant of a symbolic matrix. Arithmetic circuits are the most powerful model among these. There is an easy randomized polynomial identity test: just evaluate the polynomial at a random point. It is known that a nonzero polynomial will have a nonzero evaluation with a good probability [DL78, Sch80, Zip79]. However, no nontrivial deterministic tests are known. Deterministic PIT is known to have connections with arithmetic circuit lower bounds [KI03, Agr05].

It is known that the determinant of a matrix, where the entries are linear polynomials, captures small degree arithmetic circuits, with only a quasi-polynomial blow-up [Val79, VSBR83]. Efficient polynomial identity tests are known only for very restricted input models. One such case which has received a lot of attention is $\det(\sum_i z_i A_i)$, where the A_i's are rank-1 matrices. Polynomial identity testing for this case exactly corresponds to the linear matroid intersection question, and thus has a polynomial time algorithm [Edm79, Lov89]. However, no blackbox PIT algorithm was known for this case. In a blackbox algorithm, one cannot see the input, but has to output a set of points such that if the polynomial is nonzero, then it evaluates to nonzero at one of the points. Such a set of points is called a *hitting-set*. With our derandomization of the Isolation Lemma we get a hitting-set for $\det(\sum_i z_i A_i)$, when A_i's are of rank-1.

A generalization of this case has also been considered, which we get by adding an arbitrary constant matrix A_0, i.e., $\det(A_0+\sum_i z_i A_i)$. PIT for this case is also known as the matrix completion problem and has a polynomial time algorithm [Mur93, Gee99, IKS10]. Using reductions from Anderson, Shpilka and Volk [ASV16] and Murota [Mur93], our hitting-set can also be shown to work for this case. This also generalizes the previously known quasi-polynomial hitting-set for read-once formulas [SV09].

> *There is a quasi-polynomial time hitting-set for polynomials of form* $\det(A_0 + \sum_i z_i A_i)$, *where* A_i *is a matrix of rank* 1 *for each* $1 \leq i \leq m$.

2 Preliminaries

For a set E, we denote by $\mathcal{P}(E)$ the power set of E. For an integer m, we define $[m] = \{1, 2, \ldots, m\}$.

2.1 Complexity classes

Barrington [Bar92] generalized the class NC^k to define the class quasi-NC^k as the class of problems which have uniform circuits of quasi-polynomial size $2^{\log^{O(1)} n}$ and poly-logarithmic depth $O(\log^k n)$. The class quasi-NC is the union of classes quasi-NC^k, over all $k \geq 0$. Here, *uniformity* means quasi-polynomial time uniformity.

2.2 Matroids

Matroid theory originated in the middle of the 1930s. There is a huge literature on matroids by now. For an introduction, see for example the excellent textbooks of Oxley [Oxl06] or Schrijver [Sch03]. Below we give some basic definitions and facts about matroids.

A *matroid* M is a pair $M = (E, \mathcal{I})$, where E is the finite ground set and $\mathcal{I} \subseteq \mathcal{P}(E)$ is a nonempty family of subsets of E that satisfies the following two axioms.

1. *Closure under subsets.* For every $I \in \mathcal{I}$ and $J \subseteq I$ we have $J \in \mathcal{I}$.

2. *Augmentation property.* For every $I, J \in \mathcal{I}$ where $|I| < |J|$, there is an $j \in J$ such that $I \cup \{j\} \in \mathcal{I}$.

We denote $m = |E|$ throughout the paper. The sets in $\mathcal{I}$ are called the *independent sets of* M. An inclusion-wise maximal set $B \in \mathcal{I}$ is called a *base*. Note that by the augmentation property, all base sets have the same size. Let $\mathcal{B} \subseteq \mathcal{I}$ denote the collection of base sets.

As an example, we already mentioned *linear matroids* in the Introduction which come from linear independence in Linear Algebra. Another well known example are *graphic matroids*. Given an undirected graph $G = (V, E)$, we take E as the ground set and the forests in G as the independent sets. It is not hard to see that forests fulfill the matroid axioms.

Matroid rank. Also motivated by Linear Algebra, there is a *rank-function* of a matroid that is defined for every subset $A \subseteq E$ as the size of the largest independent set that is contained in A,

$$\text{rank}(A) = \max\{\, |I| \mid I \in \mathcal{I} \text{ and } I \subseteq A \,\}.$$

The size of every maximal independent set is rank(E). This number is called the *rank of* M. The *matroid problem* is to compute a maximal independent set.

An important property of the rank-function is its submodularity. In general, a function f defined on $\mathcal{P}(E)$ is called *submodular*, if for any sets $S, T \subseteq E$, we have

$$r(S) + r(T) \geq r(S \cup T) + r(S \cap T).$$

Lemma 2.1 (See [Sch03])**.** *The rank-function of a matroid is submodular.*

Proof. Let $S, T \subseteq E$. Let $I, J \in \mathcal{I}$ be maximal such that $I \subseteq S \cap T$ and $I \subseteq J \subseteq S \cup T$. Hence rank$(S \cap T) = |I|$ and rank$(S \cup T) = |J|$.

Define $S' = J \cap S$ and $T' = J \cap T$. Note that $S', T' \in \mathcal{I}$ and $S' \cap T' = I$. Hence, we get

$$r(S) + r(T) \geq |S'| + |T'| = |S' \cup T'| + |S' \cap T'| \geq |J| + |I| = r(S \cup T) + r(S \cap T).$$

$\square$

Dual Matroid. There is a concept of *duality* in matroid theory that generalizes the notion of orthogonality in vector spaces. Let $M = (E, \mathcal{I})$ be a matroid with base sets $\mathcal{B}$. Define $\mathcal{B}^*$ as the complements of the base sets, $\mathcal{B}^* = \{\, \overline{B} \mid B \in \mathcal{B} \,\}$. Then $\mathcal{B}^*$ are the base sets of a matroid M^*, the *dual of* M. In terms of independent sets, we can write $M^* = (E, \mathcal{I}^*)$, where

$$\mathcal{I}^* = \{\, I \mid \exists B \in \mathcal{B} \;\; B \cap I = \emptyset \,\}.$$

It is known that the dual of a linear matroid is again linear. Moreover, given the matrix representing a linear matroid, the matrix representing the dual matroid can be computed in NC^2 [NSV94].

Matroid intersection. Our main focus is the *matroid intersection problem*. Given two matroids $M_1 = (E, \mathcal{I}_1)$ and $M_2 = (E, \mathcal{I}_2)$ over the same ground set, compute a maximum size set in $\mathcal{I}_1 \cap \mathcal{I}_2$, the common independent sets. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the collections of base sets of M_1 and M_2, respectively. In another variant of the problem, one has to decide whether the matroids have a common base, i.e., whether $\mathcal{B}_1 \cap \mathcal{B}_2$ is nonempty, and in this case, to construct such a base $B \in \mathcal{B}_1 \cap \mathcal{B}_2$. The two variants are equivalent for linear matroids. The reduction from former to the latter is implicit in Narayanan et al. [NSV94, Theorem 4.2]. Note that in general $(E, \mathcal{I}_1 \cap \mathcal{I}_2)$ is not a matroid anymore.

Matroid intersection captures many interesting combinatorial problems.

- We already mentioned the common linear independent columns of two matrices.
- A well known example is *bipartite maximum matching*. Let $G = (L \cup R, E)$ be a bipartite graph. We define two matroids M_L and M_R over the ground set E. In matroid M_L, a set $I \subseteq E$ is independent if no two edges have a common end point in L. Matroid M_R is defined similarly with respect to vertex set R. Then any common independent set of M_L and M_R is a matching in the graph G.
- Another example are *rainbow spanning trees*. Given a graph with colored edges, the problem asks if there is a spanning tree with all its edges having distinct colors. To capture this by matroid intersection, define the first matroid to be the graphic matroid of G, and the second matroid so that its independent sets are sets of edges with all distinct edge colors.

2.3 Matroid Polytope

With every matroid, there is an associated *matroid polytope*. This polytope is crucial for our arguments. We summarize the properties we will use later on.

For a set $I \subseteq E$, its characteristic vector $x^I \in \mathbb{R}^E$ is defined as

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

For any collection of sets $\mathcal{A} \subseteq \mathcal{P}(E)$, the polytope $P(\mathcal{A})$ is defined as the convex hull of the characteristic vectors of the sets in $\mathcal{A}$,

$$P(\mathcal{A}) = \operatorname{conv}\{x^I \mid I \in \mathcal{A}\}.$$

For a matroid $M = (E, \mathcal{I})$, its *matroid polytope* is defined as $P(\mathcal{I}) \subseteq \mathbb{R}^E$, i.e., the convex hull of the characteristic vectors of the independent sets. The points $\{x^I \mid I \in \mathcal{I}\}$ are the corners of the matroid polytope $P(\mathcal{I})$.

Edmonds [Edm70] gave a simple description of this polytope which uses the rank function of the matroid (see also [Sch03]). For convenience, we define for any $x \in \mathbb{R}^E$ and $S \subseteq E$,

$$x(S) = \sum_{e \in S} x_e.$$

Lemma 2.2 ([Edm70])**.** *For a matroid $(E, \mathcal{I})$ with rank function r, a point $x \in \mathbb{R}^E$ is in $P(\mathcal{I})$ iff*

$$\begin{aligned} x_e &\geq 0 \quad \forall\, e \in E & (1) \\ x(S) &\leq r(S) \quad \forall\, S \subseteq E. & (2) \end{aligned}$$

It is easy to see that any 0-1 corner of the polytope given by (1) and (2) corresponds to an independent set in $\mathcal{I}$. The nontrivial part is to show that the described polytope does not have a non-integral corner. Let $\mathcal{B}$ be the family of base sets of the matroid $(E, \mathcal{I})$. The matroid base polytope, defined as $P(\mathcal{B})$, is clearly a face of the matroid polytope $P(\mathcal{I})$. Adding the following equation to (1) and (2) will give a description of $P(\mathcal{B})$,

$$x(E) = n. \tag{3}$$

Matroid Intersection Polytope. The intersection of two matroids also has an easy polytope description: Edmonds [Edm70] showed a surprising result that one can describe the matroid intersection polytope $P(\mathcal{I}_1 \cap \mathcal{I}_2)$ just by putting together the constraints of the two matroid polytopes $P(\mathcal{I}_1)$ and $P(\mathcal{I}_2)$ (see also [Sch03]).

Theorem 2.3 ([Edm70])**.** *For two matroids $(E, \mathcal{I}_1)$ and $(E, \mathcal{I}_2)$,*

$$P(\mathcal{I}_1 \cap \mathcal{I}_2) = P(\mathcal{I}_1) \cap P(\mathcal{I}_2).$$

That is, a point $x \in \mathbb{R}^E$ is in the polytope $P(\mathcal{I}_1 \cap \mathcal{I}_2)$ iff

$$\begin{aligned} x_e &\geq 0 \quad \forall\, e \in E, & (4) \\ x(S) &\leq r_1(S) \quad \forall\, S \subseteq E, & (5) \\ x(S) &\leq r_2(S) \quad \forall\, S \subseteq E, & (6) \end{aligned}$$

where r_1 and r_2 are the rank functions of the two matroids, respectively.

Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the families of base sets of the matroids $(E, \mathcal{I}_1)$ and $(E, \mathcal{I}_2)$, respectively. To obtain the base polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ one just needs to add the constraint $x(E) = n$ to the above inequalities.

2.4 An RNC-algorithm for linear matroid intersection

Narayanan, Saran, and Vazirani [NSV94] showed that the matroid intersection problem is in RNC. Their technique was to reduce the problem to a polynomial identity test (PIT), namely whether the determinant of a symbolic matrix is nonzero. We give some details on the argument, because we will use the same algorithm, except that we *deterministically* compute the points where to evaluate the determinant. Let the linear matroids M_1 and M_2 be given by two matrices U and V. W.l.o.g. we can assume that both matrices are $n \times m$ and have full rank. We want to find out whether M_1 and M_2 have a common base.

Lemma 2.4. *Let Z be an $m \times m$ diagonal matrix with variables on the diagonal, $Z_{e,e} = z_e$, for $e = 1, 2, \ldots, m$. Define the $n \times n$ symbolic matrix $D = UZV^{\mathsf{T}}$. Then M_1 and M_2 have a common base $\iff \det(D) \not\equiv 0$.*

Proof. By the Binet-Cauchy formula, we can write

$$\det(D) = \sum_{\substack{B \subseteq [m] \\ |B| = n}} \left(\prod_{e \in B} z_e \right) \det(U_B) \det(V_B),$$

where U_B and V_B are submatrices of U and V, respectively, with columns indexed by B. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the collections of bases for M_1 and M_2, respectively. Clearly, $\det(U_B)\det(V_B) \neq 0$ if and only if $B \in \mathcal{B}_1 \cap \mathcal{B}_2$. Hence, the monomials of $\det(D)$ are coming precisely from the common bases,

$$\det(D) = \sum_{B \in \mathcal{B}_1 \cap \mathcal{B}_2} \left(\prod_{e \in B} z_e \right) \det(U_B) \det(V_B). \tag{7}$$

This proves the lemma. □

Let $w \colon E \to \mathbb{Z}$ be a weight function. The *weight of a set* $B \subseteq E$ is defined as $w(B) = \sum_{e \in B} w(e)$. Replace each variable z_e in equation (7) by $z^{w(e)}$, for a new variable z. Then $\det(D)$ becomes a univariate polynomial $\det(D)(z)$. The monomial $\prod_{e \in B} z_e$ in equation (7) becomes $z^{w(B)}$ in $\det(D)(z)$.

Definition 2.5. A weight function w is *isolating* for a family of sets $\mathcal{A} \subseteq \mathcal{P}(E)$, if there is a unique minimum weight set in $\mathcal{A}$.

Let w be an isolating weight assignment for $\mathcal{B}_1 \cap \mathcal{B}_2$. If $\mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$, then the minimum degree term in $\det(D)(z)$ is unique. Thus, $\det(D)(z) \neq 0 \iff \mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$.

The RNC-algorithm now simply uses random weights. The Isolation Lemma [MVV87] states that a random weight function w with polynomially bounded weights is isolating for any family $\mathcal{A}$ with high probability. Moreover, a determinant with small degree univariate entries can be computed in NC [BCP84].

Theorem 2.6 ([NSV94])**.** *Linear Matroid Intersection is in* RNC*.*

One can also compute the common base set B^* that is isolated. For each $e \in E$, in parallel, delete e and re-compute $\det(D)(z)$. If the minimum term disappears then $e \in B^*$.

3 Linear Matroid Intersection in quasi-NC

In this section, we show how to derandomize the algorithm from Theorem 2.6.

Theorem 3.1. *Linear Matroid Intersection is in* quasi-NC*.*

In the RNC-algorithm described in Section 2.4, random weights were used to isolate a base in the intersection of two matroids. We will construct an isolating weight assignment *deterministically*.

We build the isolating weight assignment in rounds. In every round, we slightly modify the current weight assignment to get a smaller set of *minimum* weight common bases. Our goal is to reduce their number in every round significantly. We stop when we have a unique minimum weight common base.

We define an extension of weight function $w : E \to \mathbb{Z}$ to $\mathbb{R}^E$. For $x \in \mathbb{R}^E$,

$$w(x) = w \cdot x = \sum_{e \in E} w(e)\, x_e.$$

Note that $w(x^B) = x(B)$, for any $B \subseteq E$. We consider the minimum weight points in the polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. As $w(x)$ is a linear function, these points will form a face of the polytope. The corners of this face will come precisely from the minimum weight common bases. Therefore we want to understand the properties of such faces. We start considering the faces of a single matroid in Section 3.1, and then consider the intersection of two matroids in Section 3.2.

3.1 Faces in the Matroid Polytope

Let $(E, \mathcal{I})$ be a matroid with the family of base sets $\mathcal{B}$ and rank function r. From the description of the polytope $P(\mathcal{B})$ in Lemma 2.2, we know that any of its faces can be described by equations of the type $x_e = 0$ or $x(S) = r(S)$. The collection of sets S for which the second equation holds has some structure.

Lemma 3.2 ([Edm70])**.** *For any point $x \in P(\mathcal{B})$ and any sets $S, T \subseteq E$,*

$$x(S) = r(S) \text{ and } x(T) = r(T) \implies x(S \cap T) = r(S \cap T) \text{ and } x(S \cup T) = r(S \cup T).$$

Proof. From the lemma hypothesis,

$$\begin{aligned} r(S) + r(T) = x(S) + x(T) &= x(S \cup T) + x(S \cap T) \\ &\leq r(S \cup T) + r(S \cap T) \qquad (x \text{ satisfies (2)}) \\ &\leq r(S) + r(T). \qquad (\text{submodularity, Lemma 2.1}) \end{aligned}$$

Thus, all the inequalities are in fact equalities. Hence, the claim follows. □

Lemma 3.2 allows us to partition the ground set E into a family of disjoint sets $\mathcal{S}$ that serve as a basis to write every set T that satisfies $x(T) = r(T)$ as a union of sets from $\mathcal{S}$.

Lemma 3.3. *Let $(E, \mathcal{I})$ be a matroid with family of base sets $\mathcal{B}$ and rank function r. Let F be a face of the matroid base polytope $P(\mathcal{B})$. Then there exists a family of disjoint sets $\mathcal{S}$ that form a partition of E, such that for any $S \in \mathcal{S}$ there exists a number $n_S \geq 0$ such that for any $x \in F$,*

$$x(S) = n_S.$$

Moreover,

(i) if F satisfies $x(T) = r(T)$, for some $T \subseteq E$, then T is a disjoint union of sets from $\mathcal{S}$,

(ii) if F satisfies $x_e = 0$ for some $e \in E$, then there is a $S \in \mathcal{S}$ such that $S = \{e\}$ and $n_S = 0$.

Proof. We consider the equations of type $x(T) = r(T)$ in F,

$$\mathcal{T} = \{\, T \subseteq E \mid x(T) = r(T) \;\; \forall x \in F \,\}.$$

Let $\mathcal{T} = \{T_1, T_2, \ldots, T_p\}$. Consider the family of sets

$$\mathcal{S} = \{\, R_1 \cap R_2 \cap \cdots \cap R_p \mid R_i \in \{T_i, \overline{T}_i\} \;\text{ for } i = 1, 2, \ldots, p \,\}.$$

Clearly, the sets in $\mathcal{S}$ form a partition of E. We will show that for any $S \in \mathcal{S}$, there exists a number n_S such that $x(S) = n_S$, for all $x \in F$.

W.l.o.g. let $S = T_1 \cap \cdots \cap T_j \cap \overline{T}_{j+1} \cap \cdots \cap \overline{T}_p$. Let us denote $S' = T_1 \cap \cdots \cap T_j$ (for $j = 0$, let $S' = E$), and $S'' = T_{j+1} \cup \cdots \cup T_p$ (for $j = p$, let $S'' = \emptyset$). Then we have $S = S' - (S' \cap S'')$. As $x(T_i) = r(T_i)$, for each $1 \le i \le p$, we get from Lemma 3.2

$$x(S') = r(S') \;\text{ and }\; x(S'') = r(S'').$$

Again by Lemma 3.2, we have $x(S' \cap S'') = r(S' \cap S'')$. Now,

$$x(S) = x(S') - x(S' \cap S'') = r(S') - r(S' \cap S'').$$

Hence, for $n_S = r(S') - r(S' \cap S'')$, we have $x(S) = n_S$.

Claim (i) follows directly from the definition of $\mathcal{S}$. For claim (ii), consider an element $e \in E$ such that $x_e = 0$ for all $x \in F$. For any $x \in F$, we have $x(E - \{e\}) = x(E) - x_e = n = r(E - \{e\})$. Thus, $E - \{e\} \in \mathcal{T}$. We claim that $\{e\} \in \mathcal{S}$. To see this, define R_i to be T_i or $\overline{T}_i$, whichever contains e. Then clearly, $R_1 \cap R_2 \cap \cdots \cap R_p = \{e\}$. $\square$

3.2 Faces in the Matroid Intersection Polytope

Let $(E, \mathcal{I}_1)$ and $(E, \mathcal{I}_2)$ be two matroids with family of base sets $\mathcal{B}_1$ and $\mathcal{B}_2$ and rank functions r_1 and r_2, respectively. By Theorem 2.3, the faces of polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ can be described by replacing some of the inequalities (4), (5), and (6) by equalities. This basically means that any face F of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ can be written as $F = F_1 \cap F_2$, for some faces F_1, F_2 of $P(\mathcal{B}_1)$ and $P(\mathcal{B}_2)$, respectively. Using this fact, we get the following extension of Lemma 3.3 that will be crucial for our weight assignment design.

Lemma 3.4. *Let $(E, \mathcal{I}_1)$ and $(E, \mathcal{I}_2)$ be two matroids with families of base sets $\mathcal{B}_1$ and $\mathcal{B}_2$ and rank functions r_1 and r_2, respectively. Let F be a face of the matroid intersection base polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. Then there exist two families of disjoint sets $\mathcal{S}$ and $\mathcal{T}$, each forming a partition of E, such that for any $S \in \mathcal{S}$ and $T \in \mathcal{T}$ there exist numbers $n_S, m_T \ge 0$ such that for any $x \in F$,*

$$x(S) = n_S \;\; \textit{and} \;\; x(T) = m_T.$$

Moreover,

(i) if F satisfies $x(R) = r_1(R)$ or $x(R) = r_2(R)$, for some $R \subseteq E$, then R is a disjoint union of sets from $\mathcal{S}$, respectively $\mathcal{T}$,

(ii) if F satisfies $x_e = 0$ for some $e \in E$, then there is a $S \in \mathcal{S}$ and a $T \in \mathcal{T}$ such that $S = T = \{e\}$ and $n_S = m_T = 0$.

Proof. We define sets for each type of equality of face F,

$$\begin{aligned} S_0 &= \{\, e \in E \mid x_e = 0 \ \ \forall x \in F \,\}, \\ \mathcal{T}_1 &= \{\, T \subseteq E \mid x(T) = r_1(T) \ \ \forall x \in F \,\}, \\ \mathcal{T}_2 &= \{\, T \subseteq E \mid x(T) = r_2(T) \ \ \forall x \in F \,\}. \end{aligned}$$

Now, define faces F_1 and F_2 of polytopes $P(\mathcal{B}_1)$ and $P(\mathcal{B}_2)$ respectively, as

$$\begin{aligned} F_1 &= \{\, x \in P(\mathcal{B}_1) \mid x(S_0) = 0 \text{ and } x(T) = r_1(T) \ \ \forall\, T \in \mathcal{T}_1 \,\}, \\ F_2 &= \{\, x \in P(\mathcal{B}_2) \mid x(S_0) = 0 \text{ and } x(T) = r_2(T) \ \ \forall\, T \in \mathcal{T}_2 \,\}. \end{aligned}$$

By Theorem 2.3, we have $F = F_1 \cap F_2$. Applying Lemma 3.3 to F_1 and F_2 proves the lemma. ☐

3.3 Cycles in Matroid Intersection

As mentioned earlier, we will construct the weight assignment in rounds. In each round, we want the dimension of the face of minimum weight common bases to become smaller. To measure this decrement, we define a *cycle* with respect to a face.

Definition 3.5 (Cycle)**.** Let F be a face of the polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ with the partitions $\mathcal{S}$ and $\mathcal{T}$ as in Lemma 3.4. A sequence $C = (e_1, e_2, \ldots, e_{2r})$ of distinct elements of E is called a *cycle* with respect to face F, if consecutive pairs are alternately in a set from $\mathcal{S}$ and a set from $\mathcal{T}$. That is, for $i = 1, 2, \ldots, r$,

$$\begin{aligned} &e_{2i-1}, e_{2i} \in S, \quad \text{for some } S \in \mathcal{S}, \\ &e_{2i}, e_{2i+1} \in T, \quad \text{for some } T \in \mathcal{T}, \end{aligned}$$

where $e_{2r+1} = e_1$.

Note that if the face F satisfies equation $x_e = 0$ for some element $e \in E$, then e cannot appear in any cycle defined with respect to F. This is because $\{e\}$ appears as a singleton set in both the partitions constructed for F.

Let $\mathcal{C}_F$ denote the family of all cycles with respect to face F. Consider a face $F' \subseteq F$. All equations that hold for F also hold for F'. Therefore the partitions of E that we get from F' will be refinements of those from F. Hence, when we go to a sub-face, cycles are only destroyed; no new cycles are created.

Lemma 3.6. *Let F, F' be two faces of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ such that $F' \subseteq F$. Then $\mathcal{C}_{F'} \subseteq \mathcal{C}_F$.*

Next we show that there are cycles for any face of dimension ≥ 1. We argue that the exchange cycle for any two bases in the face F fits Definition 3.5.

Lemma 3.7. *If face F of polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ contains at least two corners then $\mathcal{C}_F \neq \emptyset$.*

Proof. Consider any two corners of face F that correspond to the common bases B_1, B_2, i.e., $x^{B_1}, x^{B_2} \in F$. We show that $B_1 \triangle B_2$ consists of a set of disjoint cycles.

Let $\mathcal{S}$ and $\mathcal{T}$ be the two partitions of E as in Lemma 3.4. Then we have $|B_1 \cap S| = |B_2 \cap S| = n_S$, for every $S \in \mathcal{S}$, and $|B_1 \cap T| = |B_2 \cap T| = m_T$, for every $T \in \mathcal{T}$.

As $B_1 \neq B_2$, there is an element $e_1 \in B_1 - B_2$. Let $e_1 \in S_1 \cap T_1$, for some $S_1 \in \mathcal{S}$ and $T_1 \in \mathcal{T}$. As $|B_1 \cap S_1| = |B_2 \cap S_1|$, there must be another element $e_2 \in S_1$ such that $e_2 \in B_2 - B_1$. Now, let

$e_2 \in T_2$. By a similar argument, there must be another element $e_3 \in T_2$ such that $e_3 \in B_1 - B_2$. We keep finding such elements, alternatively from $B_1 - B_2$ and $B_2 - B_1$, until we get back to an element already seen. This would give us the desired cycle. □

Lemma 3.7 implies that if $\mathcal{C}_F = \emptyset$, then F has only one corner, in other words, F is just a point. Thus, the strategy is to successively eliminate cycles to reach smaller and smaller faces, until we reach a face F where $\mathcal{C}_F = \emptyset$. For this purpose, we define the *circulation* of a cycle.

Definition 3.8. For a weight assignment $w\colon E \to \mathbb{Z}$, the *circulation* $c_w(C)$ of a cycle $C = (e_1, e_2, \dots, e_k)$ is defined as the alternating sum

$$c_w(C) = |w(e_1) - w(e_2) + w(e_3) - \cdots - w(e_k)|.$$

Let B_1, B_2 be two common bases with $w(B_1) = w(B_2)$ such that $C = B_1 \triangle B_2$ is a cycle. Then we have $c_w(C) = |w(B_1) - w(B_2)| = 0$. Our next lemma generalizes this observation to *all* cycles in a minimum weight face F.

Lemma 3.9. *Let F be a face of the polytope $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. Let $w\colon E \to \mathbb{Z}$ be a weight function such that $w \cdot x$ is constant on F. Then $c_w(C) = 0$, for any $C \in \mathcal{C}_F$.*

Proof. Let $C = (e_1, e_2, \dots, e_{2r}) \in \mathcal{C}_F$. We split C into two sets, $C_1 = \{e_1, e_3, \dots, e_{2r-1}\}$ and $C_2 = \{e_2, e_4, \dots, e_{2r}\}$. Now, define the *circulation vector* $\delta_C \in \mathbb{R}^E$ for cycle C as

$$\delta_C = x^{C_1} - x^{C_2}.$$

δ_C is just has alternating $+1$s and -1s corresponding to the cycle elements. Note that $c_w(C) = |w \cdot \delta_C|$. We will show that $w \cdot \delta_C = 0$.

Let $\{a_1, a_2, \dots, a_p\}$ be the set of corners of F. Consider their average $a = (a_1 + a_2 + \cdots + a_p)/p$. Clearly, $a \in F$. Now we move from point a along the vector δ_C and go to a new point $b = a + \epsilon\, \delta_C$, for some small $\epsilon \in \mathbb{R}$. We claim that $b \in F$. If this is true then $w \cdot \delta_C = (1/\epsilon)(w \cdot b - w \cdot a) = 0$, which proves the lemma.

It remains to argue that $b \in F$. Consider an inequality which is not tight for F. Then, it will not be tight for a too, because a is the centroid of F. One can choose ϵ to be small enough so that the inequality remains non-tight for b. So, we only need to care about the equalities for F,

$$\begin{aligned} S_0 &= \{\, e \in E \mid x_e = 0 \ \ \forall x \in F \,\}, \\ \mathcal{T}_1 &= \{\, T \subseteq E \mid x(T) = r_1(T) \ \ \forall x \in F \,\}, \\ \mathcal{T}_2 &= \{\, T \subseteq E \mid x(T) = r_2(T) \ \ \forall x \in F \,\}. \end{aligned}$$

We will show that b satisfies all these constraints. Consider an element $e \in S_0$. By definition of a, we have $a_e = 0$. We already remarked above, that e cannot be a part of a cycle. Therefore, we have $b_e = a_e$, and hence $b_e = 0$.

Let $\mathcal{S}$ and $\mathcal{T}$ be the two partitions of E as in Lemma 3.4. From the definition of a cycle we know that $|C_1 \cap S| = |C_2 \cap S|$ for any $S \in \mathcal{S}$. Thus,

$$\delta_C(S) = 0, \quad \text{for all } S \in \mathcal{S}.$$

Let $R \in \mathcal{T}_1$. By Lemma 3.4, R is the disjoint union of sets from $\mathcal{S}$, Hence, we conclude that $\delta_C(R) = 0$. Therefore

$$b(R) = a(R) = r_1(R).$$

This shows the second constraint. Similarly, one can show the third constraint. □

Let C be a cycle, say in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$, and let w be a weight function such that $c_w(C) \neq 0$. Let F be the face we get by minimizing w over $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. It follows from Lemma 3.9 that $C \notin \mathcal{C}_F$. This means that if w ensures nonzero circulation for *all* cycles in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$, then all cycles will be eliminated, i.e., $\mathcal{C}_F = \emptyset$ and F will be a corner. Thus, w would be isolating. However, we cannot achieve nonzero circulation for all cycles at once, as there are exponentially many possible cycles.

We get around this problem by constructing the weight function in rounds. In each round, we double the length of the eliminated cycles and reach a face of smaller dimension. Thus, in $\log m$ rounds, we eliminate all cycles and reach a corner. The following lemma shows that the number of cycles we handle in each round remains small. A similar lemma for the number of cycles in a graph was proved by Fenner et al. [FGT16].

Lemma 3.10. *Let F be a face of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. If $\mathcal{C}_F$ has no cycles of length $\leq r$, for some even number $r \geq 2$, then $\mathcal{C}_F$ has $\leq m^4$ cycles of length $\leq 2r$.*

Proof. Let $\mathcal{S}$ and $\mathcal{T}$ be the two partitions of E as in Lemma 3.4. Let $C = (e_0, e_1, \ldots, e_{s-1})$ be a cycle of length $s \leq 2r$. We choose four elements from the cycle C which divide it into four almost equal parts: Let $(a, b, c, d) = (0, \lceil s/4 \rceil, \lceil 2s/4 \rceil, \lceil 3s/4 \rceil)$. We associate the tuple (e_a, e_b, e_c, e_d) with cycle C. Since we could choose cycle C with any of its element as a starting point, the ordered tuple associated with C is not uniquely defined. However, we claim that the tuple uniquely describes C.

Claim 1. *Cycle C is the only cycle in $\mathcal{C}_F$ of length $\leq 2r$ that is associated with (e_a, e_b, e_c, e_d).*

Proof. Suppose $C' = (f_0, f_1, \ldots, f_{t-1})$ is another such cycle of length $t \leq 2r$. We will show that there exists a cycle of length $\leq r$, which will be a contradiction.

Let $(a', b', c', d') = (0, \lceil t/4 \rceil, \lceil 2t/4 \rceil, \lceil 3t/4 \rceil)$. From the assumption, $e_0 = f_0$, $e_b = f_{b'}$, $e_c = f_{c'}$ and $e_d = f_{d'}$. Without loss of generality, let C and C' differ in their first segment. Let $0 < p < b, b'$ be the first index such that $e_p \neq f_p$. Let $p < q \leq b$ be the first index such that $e_q = f_h$ for some $p < h \leq b'$. As $e_{p-1} = f_{p-1}$, e_p and f_p both belong to some common $S \in \mathcal{S}$ or $T \in \mathcal{T}$.

We consider two cases:

(i) q and h have the same parity: because $e_q = f_h$, e_{q-1} and f_{h-1} belong to some common S or T. Hence, $(e_p, e_{p+1}, \ldots, e_{q-1}, f_{h-1}, f_{h-2} \ldots, f_p)$ forms a valid cycle.

(ii) q and h have a different parity: then $(e_p, e_{p+1}, \ldots, e_{q-1}, f_h, f_{h-1} \ldots, f_p)$ forms a valid cycle since e_{q-1} and f_h both belong to some common S or T.

The cycles we get in both cases have length $\leq q - p + h - p + 1 \leq b - 1 + b' \leq r$. □

There are at most m^4 ways to choose the tuple (e_a, e_b, e_c, e_d). By Claim 1, this gives a bound on the number of cycles of length $\leq 2r$. □

There are standard techniques to give nonzero weights to a small number of sets (see, for example [FKS84]).

Lemma 3.11. *For any number s, one can construct a set of $O(m^2 s)$ integer weight functions on the set E with weights bounded by $O(m^2 s)$ in time $\mathsf{poly}(ms)$ such that for any set of s cycles, one of the weight function will give nonzero circulation to each of the s cycles.*

For a proof see [FGT16, Lemma 2.3]. We apply Lemma 3.11 to a set of $s = m^4$ cycles. Then, in each round, we get a set of $O(m^6)$ weight functions, each bounded by $O(m^6)$.

3.4 Isolating weight construction

We define the weight function for two matroids $(E, \mathcal{I}_1)$ and $(E, \mathcal{I}_2)$ with family of base sets $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively. Let $m = |E|$ and $t = \lceil \log m \rceil$. We will define a sequence of weight functions and faces of $P(\mathcal{B}_1 \cap \mathcal{B}_2)$. Let $F_0 = P(\mathcal{B}_1 \cap \mathcal{B}_2)$. For $i = 0, 1, \ldots, t-1$, define

w_i: a weight assignment such that $c_{w_i}(C) \neq 0$, for any cycle $C \in \mathcal{C}_{F_i}$ of length $\leq 2^{i+1}$,

F_{i+1}: the set of points in F_i minimizing the weight function w_i.

We combine the weight functions $w_0, w_1, \ldots, w_{t-1}$ with decreasing precedence. Let N be number that is larger than any of these weights, i.e., $N = O(m^6)$. For $i = 0, 1, \ldots, t-1$, define

$$W_i = w_0 N^i + w_1 N^{i-1} + \cdots + w_i N^0.$$

Our final weight assignment will be W_{t-1}.

Claim 2. *F_{i+1} is the set of minimum points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ with respect to W_i, for $i = 0, 1, \ldots t-1$.*

Proof. We prove this by induction. The claim is clearly true for $i = 0$. Now, assume that F_i is the set of points in $P(\mathcal{B}_1 \cap \mathcal{B}_2)$ that minimizes W_{i-1}. Then F_i is also the set of points that minimizes $N\,W_{i-1}$. As $N\,W_{i-1}$ always dominates w_i, the set of points that minimizes $W_i = N\,W_{i-1} + w_i$ will be a subset of F_i. This subset is exactly those points in F_i where w_i is minimized, that is F_{i+1}. $\square$

Claim 3. *$\mathcal{C}_{F_i}$ has no cycles of length 2^i, for $i = 1, 2, \ldots t$.*

Proof. By the definition of w_{i-1}, $c_{w_{i-1}}(C) \neq 0$ for any cycle $C \in \mathcal{C}_{F_{i-1}}$ of length $\leq 2^i$. As w_{i-1} is constant over the face F_i, we have $c_{w_{i-1}}(C) = 0$, for all cycles $C \in \mathcal{C}_{F_i}$, by Lemma 3.9. Recall Lemma 3.6 that $\mathcal{C}_{F_i} \subseteq \mathcal{C}_{F_{i-1}}$. Thus, $\mathcal{C}_{F_i}$ has no cycles of length 2^i. $\square$

Lemma 3.12. *Weight function W_{t-1} is isolating.*

Proof. By Claim 2, the face minimized by W_{t-1} is F_t. By Claim 3, $\mathcal{C}_{F_t}$ has no cycles of length $\leq 2^t = m$. That is, $\mathcal{C}_{F_t} = \emptyset$. By Lemma 3.7, F_t has only one corner, i.e., W_{t-1} is isolating. $\square$

Each w_i has weights bounded by $O(m^6)$ by Lemma 3.11. Thus, W_{t-1} will have weights bounded by $O(m^{6\log m})$. By Lemma 3.11, we get $O(m^6)$ possible weight functions for each w_i, and therefore $O(m^{6\log m})$ combinations for W_{t-1}. We need to try all of them in parallel.

Lemma 3.13. *For a given number m, we can construct $O(m^{6\log m})$ weight functions on $[m]$ with weights bounded by $O(m^{6\log m})$ such that for any matroid intersection on the ground set $[m]$, one of the weight functions isolates a common base.*

As mentioned in Section 2, by plugging-in a isolating weight assignment in the determinant polynomial we can decide whether there exists a common base. As our weights are quasi-polynomially bounded, the determinant entries will have quasi-polynomial bits. Thus, the determinant can be computed in quasi-NC^2 [Ber84, BCP84]. This proves Theorem 3.1.

4 Applications

We already mentioned the connection of our isolating weight construction to *Polynomial Identity Testing* in Section 2.4. In this section, we extend the class of polynomials even further where our technique applies. Then we show that this extended class of polynomials can be used to solve the *matroid union problem* in quasi-NC.

4.1 Polynomial Identity Testing (PIT)

By Lemma 2.4, the weight assignment constructed in Lemma 3.13 yields a quasi-polynomial time blackbox identity test, i.e., a hitting-set, for polynomials of the form $D = UZV^{\mathsf{T}}$, where U, V are $n \times m$ matrices and Z is a $m \times m$ diagonal matrix with $Z_{i,i} = z_i$, for $i = 1, 2, \ldots, m$.

Let u_i and v_i be the i-th columns of U and V, respectively. Then we can rewrite D as $D = \sum_{i=1}^{m} z_i u_i v_i^{\mathsf{T}}$. Note that $u_i v_i^{\mathsf{T}}$ is a rank-1 matrix, for $i = 1, 2, \ldots, m$. Thus we get the following corollary.

Corollary 4.1. *In quasi-polynomial time one can compute a hitting-set for polynomials of the form* $\det(\sum_{i=1}^{m} z_i A_i)$*, where A_i is a matrix of rank 1, for $i = 1, 2, \ldots, m$.*

We can further generalize the class of polynomials we can handle and add an arbitrary constant matrix A_0, i.e., with no rank restriction.

Theorem 4.2. *There is an $m^{O(\log m)}$-time hitting-set for polynomials of form* $\det(A_0 + \sum_{i=1}^{m} z_i A_i)$*, where A_i is a matrix of rank 1, for $i = 1, 2, \ldots, m$.*

Let U and V be the matrices from above such that $A_0 + \sum_{i=1}^{m} z_i A_i = A_0 + UZV^{\mathsf{T}}$. Observe that the entries of this matrix are linear forms in the variables $z_1, z_2, \ldots, z_m$. The following lemma constructs a matrix M such that $\det(A_0 + UZV^{\mathsf{T}}) = \det(M)$ and the entries of M are either constant or a single variable z_i. Moreover, every variable z_i occurs only once in M. This *rank-one to read-once* reduction is due to Matthew Anderson, Amir Shpilka and Ben Lee Volk [ASV16].

Lemma 4.3 ([ASV16])**.**

$$\det(A_0 + UZV^{\mathsf{T}}) = \det \begin{pmatrix} I & Z & 0 \\ 0 & I & V^{\mathsf{T}} \\ U & 0 & A_0 \end{pmatrix}. \tag{8}$$

Proof. Let A, B, C, D be matrices where A and D are square matrices and A is invertible. Then we have

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & I \end{pmatrix} \begin{pmatrix} I & A^{-1}B \\ 0 & D - CA^{-1}B \end{pmatrix}$$

and hence,

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A) \det(D - CA^{-1}B). \tag{9}$$

We split the matrix on the right hand side of (8) into

$$A = \begin{pmatrix} I & Z \\ 0 & I \end{pmatrix}, \quad B = \begin{pmatrix} 0 \\ V^{\mathsf{T}} \end{pmatrix}, \quad C = \begin{pmatrix} U & 0 \end{pmatrix}, \quad D = A_0$$

and apply Equation (9). We have $\det(A) = 1$. Note that $A^{-1} = \begin{pmatrix} I & -Z \\ 0 & I \end{pmatrix}$, and therefore we get $D - CA^{-1}B = A_0 + UZV^{\mathsf{T}}$. This proves the lemma. $\square$

Murota [Mur93] has shown that PIT for read-once matrices reduces to the matroid intersection problem. We present the reduction in a way that is suitable for blackbox identity testing. Let $Q(\boldsymbol{z}) = \det\left(A_0 + UZV^{\mathsf{T}}\right)$. By Lemma 4.3, polynomial $Q(\boldsymbol{z})$ is multilinear.

The first step is to *homogenize* $Q(\boldsymbol{z})$. Consider the polynomial

$$Q'(z_1, z_2, \ldots, z_{2m}) = z_{m+1} z_{m+2} \cdots z_{2m} \cdot Q(z_1/z_{m+1}, z_2/z_{m+2}, \ldots, z_m/z_{2m}),$$

where $z_{m+1}, z_{m+2}, \ldots, z_{2m}$ are new variables. Observe that Q' is homogeneous, every monomial in Q' has degree m. Note also that $Q' \neq 0$ if and only if $Q \neq 0$. Moreover, if Q' is nonzero at a point $(\alpha_1, \alpha_2, \ldots, \alpha_{2m})$, where $\alpha_{m+1}, \ldots, \alpha_{2m} \neq 0$, then Q is nonzero at the point $(\alpha_1/\alpha_{m+1}, \alpha_2/\alpha_{m+2}, \ldots, \alpha_m/\alpha_{2m})$. Thus, it suffices to find a hitting-set for Q'.

Let Z' be the $m \times m$ diagonal matrix with $Z'_{i,i} = z_{m+i}$. Then we can write

$$Q'(\boldsymbol{z}) = \det \begin{pmatrix} Z' & Z & 0 \\ 0 & I & V^{\mathsf{T}} \\ U & 0 & A_0 \end{pmatrix},$$

Compared with the representation of Q in (8), the matrix here has Z' in the left upper corner instead of I. That is, there are only variable entries in the first m rows, and zeros, but no other constants. We will take advantage of this representation.

Define matrices

$$Y = \begin{pmatrix} 0 & I & V^{\mathsf{T}} \\ U & 0 & A_0 \end{pmatrix} \quad \text{and} \quad L = \begin{pmatrix} Z' & Z & 0 \\ & Y & \end{pmatrix}.$$

Hence $Q'(\boldsymbol{z}) = \det(L)$. Let Y_i be the i-th column of Y, for $1 \leq i \leq 3m$. Since variables z_i and z_{m+i} are in the same row of L, exactly one of them will appear in any monomial of $Q'(\boldsymbol{z})$, for each $1 \leq i \leq m$. For any such monomial $\prod_{i \in S} z_i$ with $S \subseteq [2m]$, its coefficient is nonzero if and only if the columns $\{Y_i\}_{i \in [3m]-S}$ are linearly independent. With these observations, we can show that the monomials of $Q'(\boldsymbol{z})$ exactly correspond to the common bases of two matroids: Let $E = [3m]$.

- The first matroid $M_1 = (E, \mathcal{I}_1)$ is defined by the $m \times 3m$ matrix $\begin{pmatrix} I & I & 0 \end{pmatrix}$. The matrix has two ones in every row, at position i and $i+m$. Therefore any base set of matroid M_1 has exactly one of the two elements $i, m+i$, for each $1 \leq i \leq m$, and no elements $> 2m$. Let the collection of all its base sets be $\mathcal{B}_1$.

- Let matroid $M_2 = (E, \mathcal{I}_2)$ be defined by the $2m \times 3m$ matrix Y. Our second matroid is its *dual matroid* $M_2^* = (E, \mathcal{I}_2^*)$. Let the collection of all base sets of M_2^* be $\mathcal{B}_2^*$.

Now the monomials in $Q'(\boldsymbol{z})$ exactly correspond to the sets in $\mathcal{B}_1 \cap \mathcal{B}_2^*$. Thus, we can construct an isolating weight assignment for the monomials of $Q'(\boldsymbol{z})$, which gives us a hitting-set. As we have to try quasi-polynomially many weight assignments, our hitting-set size is quasi-polynomial. This proves Theorem 4.2.

4.2 Matroid Union

Given two matroids $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ the matroid union $M_1 \vee M_2$ is defined as $(E_1 \cup E_2, \mathcal{I}_1 \vee \mathcal{I}_2)$, where

$$\mathcal{I}_1 \vee \mathcal{I}_2 = \{\, I_1 \cup I_2 \mid I_1 \in \mathcal{I}_1 \text{ and } I_2 \in \mathcal{I}_2 \,\}.$$

$M_1 \vee M_2$ is again a matroid (see [Sch03]). The *matroid union problem* is to compute a base of $M_1 \vee M_2$, i.e., to compute independent sets $I_1 \in \mathcal{I}_1$ and $I_2 \cup \mathcal{I}_2$ which maximize $|I_1 \cup I_2|$. It is not directly obvious how to test if a set is independent in $M_1 \vee M_2$. The problem is essentially equivalent to matroid intersection, and thus has a polynomial-time algorithm [Edm68, Sch03].

In case of linear matroids, Narayanan, Saran, and Vazirani [NSV94] gave a randomized NC-algorithm computing a linear representation for the union. It turns out that we can derandomize their algorithm with our isolation technique. They find the linear representation as follows: Suppose the two matroids M_1 and M_2 are given by matrices U_1 and U_2. Without loss of generality, one can assume that both matroids have the same ground set, i.e., U and V have a one-to-one correspondence between their columns. If not then one can add extra zero columns to the matrices. Let us say U and V have dimensions $n_1 \times m$ and $n_2 \times m$, respectively. Narayanan et al. [NSV94] construct an $(n_1 + n_2) \times m$ matrix V as follows:

$$V(i,j) = \begin{cases} U_1(i,j) & \text{if } i \leq n_1, \\ U_2(i,j) z_j & \text{otherwise,} \end{cases}$$

where $z_1, z_2, \ldots, z_m$ are variables. They showed that a set is independent in $M_1 \vee M_2$ if and only if the corresponding columns in V are linearly independent (over the field $\mathbb{F}(z_1, z_2, \ldots, z_m)$). To get a matrix over the base field, they plug-in random values for z_i's. This works because a random substitution preserves the nonzeroness of minors with high probability [DL78, Sch80, Zip79].

Note that any minor of V is a polynomial of the form for which we have given a hitting-set in Theorem 4.2. Thus, any nonzero minor of V will have a nonzero evaluation at some point of the hitting-set. We consider a substitution from the hitting-set which maximizes the rank of V, and compute the set of columns I forming a maximum independent set. As our hitting-set size is quasi-polynomial, the set I can be computed quasi-NC.

The next step is to compute two sets $I_1 \in \mathcal{I}_1$ and $I_2 \in \mathcal{I}_2$ such that $I = I_1 \cup I_2$. This is called the *partition problem*. Narayanan et al. [NSV94, Section 5] give a NC-reduction of this problem to the linear matroid intersection problem. As we can solve the latter in quasi-NC (Theorem 3.1), we can find I_1 and I_2 in quasi-NC.

Theorem 4.4. *Linear Matroid Union is in* quasi-NC*.*

5 Discussion

One of main open questions is to do isolation with polynomially bounded weights, or to come up with a different NC-algorithm for linear matroid intersection. It would be interesting to find out for what polytopes our isolation technique works. For general matroids, the parallel complexity of matroid intersection is not clear. Can we find an NC algorithm (randomized or deterministic) for the general case.

A generalization of matroids are *polymatroids*. These are polytopes similar to the matroid polytope, where instead of the rank function one can use any submodular function that is nonnegative and nondecreasing. The key in our argument is the structure of the faces of the matroid polytope. It is based on Lemma 3.2. Note that for the proof of this lemma, it essentially suffices to have the submodularity of the rank function. One can verify that the whole argument generalizes to polymatroid intersection. That is, our weight function isolates a corner in a polymatroid intersection polytope.

Another generalization of matroid intersection is matroid matching, which also captures perfect matchings in general graphs (not necessarily bipartite). The isolation question is open even for perfect matchings in planar graphs.

6 Acknowledgments

We would like to thank Ben Lee Volk, Ankit Gupta and Stephen Fenner for helpful discussions. We are thankful to Matthew Anderson, Amir Shpilka and Ben Lee Volk for letting us use their reduction (Lemma 4.3).

References

[Agr05] Manindra Agrawal. Proving lower bounds via pseudo-random generators. In *FSTTCS*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105, 2005.

[ASV16] Matthew Anderson, Amir Shpilka, and Ben Lee Volk. Personal communication, 2016.

[Bar92] David A. Mix Barrington. Quasipolynomial size circuit classes. In *Proceedings of the Seventh Annual Structure in Complexity Theory Conference*, pages 86–93, 1992.

[BCP84] Allan Borodin, Stephen Cook, and Nicholas Pippenger. Parallel computation for well-endowed rings and space-bounded probabilistic machines. *Information and Control*, 58(1-3):113–136, July 1984.

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147 – 150, 1984.

[DL78] Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193 – 195, 1978.

[Edm68] Jack Edmonds. Matroid partition. *Mathematics of the Decision Sciences*, 11:335–345, 1968.

[Edm70] Jack Edmonds. Submodular functions, matroids, and certain polyhedra. In *Combinatorial Structures and Their Applications, Gordon and Breach, New York*, pages 69–87, 1970.

[Edm79] Jack Edmonds. Matroid intersection. In E.L. Johnson P.L. Hammer and B.H. Korte, editors, *Discrete Optimization I (Proceedings of the Advanced Research Institute on Discrete Optimization and Systems Applications of the Systems Science Panel of NATO and of the Discrete Optimization Symposium)*, volume 4, pages 39 – 49. Elsevier, 1979.

[FGT16] 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*, pages 754–763, 2016.

[FKS84] Michael L. Fredman, János Komlós, and Endre Szemerédi. Storing a sparse table with 0(1) worst case access time. *J. ACM*, 31(3):538–544, June 1984.

[Gee99] James F. Geelen. Maximum rank matrix completion. *Linear Algebra and its Applications*, 288:211 – 217, 1999.

[IKS10] Gbor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM Journal of computing*, 39(8):2010, 2010.

[KI03] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *STOC*, pages 355–364, 2003.

[Lov89] László Lovász. Singular spaces of matrices and their application in combinatorics. *Boletim da Sociedade Brasileira de Matemática - Bulletin/Brazilian Mathematical Society*, 20(1):87–99, 1989.

[Mur93] Kazuo Murota. Mixed matrices: Irreducibility and decomposition. In Richard A. Brualdi, Shmuel Friedland, and Victor Klee, editors, *Combinatorial and Graph-Theoretical Problems in Linear Algebra*, pages 39–71. Springer New York, New York, NY, 1993.

[MVV87] Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987.

[NSV94] 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.

[Oxl06] James G. Oxley. *Matroid Theory (Oxford Graduate Texts in Mathematics).* Oxford University Press, Inc., New York, NY, USA, 2006.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.

[Sch03] Alexander Schrijver. *Combinatorial optimization : polyhedra and efficiency. Vol. B. , Matroids, trees, stable sets. chapters 39-69.* Algorithms and combinatorics. Springer-Verlag, Berlin, Heidelberg, New York, N.Y., et al., 2003.

[SV09] Amir Shpilka and Ilya Volkovich. Improved polynomial identity testing for read-once formulas. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 12th International Workshop, APPROX 2009, and 13th International Workshop, RANDOM 2009, Berkeley, CA, USA, August 21-23, 2009. Proceedings*, pages 700–713, 2009.

[Val79] L. G. Valiant. Completeness classes in algebra. In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 249–261, New York, NY, USA, 1979. ACM.

[VSBR83] L. G. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff. Fast parallel computation of polynomials using few processors. *SIAM journal of computing*, 12(4):641–644, November 1983.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation (EUROSAM)*, pages 216–226. Springer-Verlag, 1979.

ECCC ISSN 1433-8092
http://eccc.hpi-web.de