Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 100 (2026)

Bipartite Matching is in NC

Abhranil Chatterjee* Sumanta Ghosh† Rohit Gurjar‡ Roshan Raj§
Thomas Thierauf ¶

July 15, 2026

Abstract

We show that the bipartite matching problem is in NC. We extend the result to weighted bipartite matching and weighted linear matroid intersection. This in turn helps to show that the search versions of bipartite matching and linear matroid intersection are in NC as well. Additionally, we show that the computation of the noncommutative rank of a symbolic matrix is in NC. The techniques are based on a polynomial method, inspired from a construction of subspace design by Guruswami and Kopparty (Combinatorica 2016).

1 Introduction

Bipartite matching lies at the heart of two important questions in complexity theory: parallelization and derandomization. The problem has long been known to have deterministic polynomial-time algorithms [Kuh55, FF56, HK73]. The classical augmenting path paradigm underlying these algorithms appears inherently sequential; the best known parallel algorithm based on augmenting paths runs in $O(n^{2/3})$ time using polynomially many parallel processors [GPV88]. Consequently, bipartite matching became one of the first and most extensively studied problems in parallel complexity.

A different approach came from the algebraic formulation of the matching problem due to Edmonds [Edm67] and Tutte [Tut47]. Combining this formulation with the polynomial identity lemma [Sch80, Zip79, DL78, Ore22], Lovász [Lov79] gave a randomized algorithm for bipartite matching. The algorithm simply substitutes a random number (from a small range) for every edge in the bi-adjacency matrix and computes the rank of the resulting matrix. As rank computation was known to admit NC-algorithms [Ber84, Csa76], this placed the bipartite matching problem in the complexity class RNC (randomized NC). This was one of the earliest applications of the polynomial identity lemma in algorithms and complexity theory.

The above algorithm solves the decision version, but not the search version. That is, it can decide if the graph has a perfect matching, but does not construct a perfect matching. Note that the standard search-to-decision reduction is sequential, and so far no NC-reduction from search to

*Indian Institute of Technology Kharagpur. Email: abhranilc@cse.iitkgp.ac.in
†Indian Statistical Institute, Kolkata. Email: besusumanta@gmail.com
‡Indian Institute of Technology Bombay. Email: rgurjar@iitb.ac.in.
§The Ohio State University. Email: raj.144@sou.edu.
¶Ulm University and Aalen University. Email: thomas.thierauf@uni-ulm.de.

ISSN 1433-8092

decision is known. Interestingly, Lovász's algorithm also extends to the weighted version: given a bipartite graph with edge weights, it can output the weight of the maximum (or minimum) weight perfect matching (but does not construct the matching). Karp, Upfal, Wigderson [KUW86] and Mulmuley, Vazirani, Vazirani [MVV87] used this fact and solved the search problem via an RNC reduction from search to finding the minimum weight of any perfect matching. Mulmuley, Vazirani, Vazirani [MVV87] invented the famous Isolation Lemma for this, which since then, has found numerous applications in algorithms and complexity. The Isolation Lemma states that if edges are assigned weights randomly from a small range, then the minimum weight perfect matching is unique. This uniqueness was crucial for constructing a perfect matching.

Together, these algorithms [Lov79, KUW86, MVV87] established bipartite matching as a textbook problem for studying both parallel computation and randomness in algorithms. A natural question arises: does there exist an efficient deterministic parallel (NC) algorithm, which has been open since then. We expect a positive answer because some widely believed complexity theoretic conjectures are known to imply derandomization [NW94, DSY08, GKSS22], that is, problems with efficient randomized algorithms should also have efficient deterministic algorithms. Polynomial identity testing and Isolation Lemma have since become central problems in the study of derandomization. In particular, as a special case of these derandomization questions, bipartite matching has attracted a lot of attention. Another reason for this interest in bipartite matching is that many important problems including DFS tree construction, maxflow, subtree isomorphism NC-reduce to it (see [KR98, Chapter 14, 15]).

Deterministic NC-algorithms have been found for matching in many special cases including the case of planar graphs [DKR10, GK87, AHT07, DK98, TV12, AV20, San18, BEG24]. In the last decade, a major progress was made for bipartite matching where it was shown to be in quasi-NC (polylog time on quasi-polynomially many processors) [FGT19, FGT21], which was later extended to non-bipartite matching as well [ST17]. In this work, we resolve the question completely by showing that bipartite matching (decision as well as search version) is in NC. Our result also extends to the weighted version.

Theorem 1.1. *The problem of finding a maximum weight perfect matching in a bipartite graph with polynomially bounded edge weights is in* NC.

Our first step is an algorithm for deciding whether a given bipartite graph has a perfect matching. This can be viewed as a derandomization of Lovász's algorithm. We first augment the bi-adjacency matrix with a few additional columns which are made up of $n-1$ identity matrices. Next, we replace each nonzero entry with a Vandermonde matrix with appropriate parameters, and each zero entry with a zero matrix. We call the obtained matrix as the *matching matrix*, and we prove that it has full row rank if and only if the graph has a perfect matching.

We generalize the algorithm to the weighted case as well. For any edge e in the graph with weight $w(e)$, we multiply the corresponding Vandermonde matrix with $t^{w(e)}$, where t is an indeterminate. Then we multiply the weighted matching matrix with its transpose and compute its determinant, which is a polynomial in t. We show that the maximum weight of any perfect matching in the graph can be obtained from the degree of this polynomial. More precisely, we show that the degree is close to a multiple of the maximum weight. We show this using LP duality for bipartite matching. As mentioned earlier, rank and determinant computation is in NC^2 [Ber84, Csa76], even over the polynomial ring.

Note that this does not immediately imply an NC-algorithm for finding a perfect matching. Interestingly, the algorithm of Fenner, Gurjar, and Thierauf [FGT21] can be viewed as an NC-reduction from (weighted) search to computing the maximum/minimum weight of any perfect matching (see Section 2.5 for more details, also see [GG17, AV20]). Thus, we also get an NC-algorithm for finding a maximum weight perfect matching. Note that other versions of the matching problem, such as maximum-cardinality matching and maximum-weight matching, NC-reduce to maximum-weight perfect matching (see, for example, [GKMT17]).

1.1 Linear matroid intersection.

The linear matroid intersection problem is a generalization of bipartite matching. A linear matroid is represented by a matrix and for an $n \times m$ matrix, a subset with n column indices is called a base if the corresponding set of columns is linearly independent. The linear matroid intersection problem asks whether two given linear matroids have a common base. It captures several combinatorial problems such as, edge-disjoint spanning trees, r-arborescence, rainbow spanning trees. Linear matroid union and partitioning also reduce to it (see [Sch03b]). Linear matroid intersection is known to be RNC [NSV94] and quasi-NC [GT20], but not in NC. We extend the ideas of our bipartite matching algorithm and show that the linear matroid intersection is in NC.

Theorem 1.2. *Given two linear matroids by $n \times m$ matrices and a weight function with polynomially bounded weights on $[m]$, the problem of finding a maximum weight common base is in* NC.

Like in the bipartite matching case, we construct a matrix similar to the matching matrix and argue that it has full rank if and only if the input matroids have a common base. Similarly, for the weighted case, we construct a matrix with univariate entries such that the degree of the determinant of the product of this matrix with its transpose is "very close" to the maximum weight of a common base. Then we use the result of [GGR24] that finds a maximum weight common base in NC given a weighted decision oracle for linear matroid intersection.

1.2 Non-commutative rank

In the context of bipartite matching, Edmonds introduced the following problem: let $x_1, x_2, \dots, x_m$ be variables. Given a set of $n \times n$ matrices $A_1, A_2, \dots, A_m$ over a field $\mathbb{F}$, compute the rank of $\sum_i A_i x_i$ (over the rational function field $\mathbb{F}(x)$). Equivalently, find the maximum rank of a matrix in the linear span of $A_1, A_2, \dots, A_m$ (assuming $\mathbb{F}$ is large enough). This problem has a randomized polynomial-time algorithm using the polynomial identity lemma [Sch80, DL78, Ore22, Zip79], but no deterministic polynomial-time algorithm is known so far. Valiant [Val79] has shown that Edmonds' problem captures the polynomial identity testing problem for algebraic formulas.

We can reduce bipartite matching to Edmonds' problem as follows. Given a bipartite graph $G = (V, E)$, for every edge $e = (i, j) \in E$ construct an $n \times n$ matrix A_e such that $A_e(i, j) = 1$ and all its other entries are zero. Define $\mathcal{A}_G = \sum_{e \in E} A_e x_e$. It turns out that $\text{rank}(\mathcal{A}_G)$ is same as the size of the maximum matching [Edm67]. This means that when $\mathcal{A}_G$ is not full rank, then there is an easily verifiable certificate for that – the *Hall block* i.e., a set of s rows whose nonzero entries are contained in a set of at most $s - 1$ columns. The general Edmonds' problem has an easily verifiable certificate for full rank – some numbers $\alpha_1, \dots, \alpha_m$ with $\sum_j A_j \alpha_j$ being full rank. But, no such efficiently verifiable short certificate is known for rank not being full.

Non-commutative Edmonds' problem is an analogue of Edmonds' problem, which admits efficiently verifiable certificates for both 'yes' and 'no' instances. The problem has received a lot of attention in the last decade. It asks for computing the *non-commutative rank* of a symbolic matrix.

There are several equivalent formulations of non-commutative rank (see [GGdOW20, IQS18] and references therein). We first describe the formulation based on *shrunk subspace*, which provides a certificate for the no instance, similar to a Hall block in a bipartite graph.

Definition 1.3. *Given a set of $n \times n$ matrices $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ over a field $\mathbb{F}$, a subspace $U \leq \mathbb{F}^n$ is called a c-*shrunk subspace *of $\mathcal{A}$, for some $c \in \mathbb{N}$, if there exists a subspace $W \leq \mathbb{F}^n$ of dimension* $\dim(U) - c$ *such that for every $1 \leq i \leq m$,*

$$A_i(U) \leq W.$$

The non-commutative rank (nc-rank) *of $\sum_i A_i x_i$ is defined to be $n-c$, where c is the largest number for which $\mathcal{A}$ has a c-shrunk subspace.*

In particular, if $\sum_i A_i x_i$ does not have full nc-rank then there is a c-shrunk subspace with $c \geq 1$. The second formulation is based on a certificate for the 'yes' instance – a matrix substitution for every variable. For this definition, the underlying field is assumed to be large enough.

Definition 1.4. *Given a set of $n \times n$ matrices $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ over a field $\mathbb{F}$, the* nc-rank *of $\sum_i A_i x_i$ is the largest number r such that there exist $d \times d$ matrices $T_1, T_2, \ldots, T_m$, for some $d > 0$, so that $\sum_i A_i \otimes T_i$ has rank rd.*[1]

For an equivalence between the two definitions, see [IQS17, IQS18]. In our bipartite matching algorithm, in the augmented bi-adjacency matrix, we substitute a matrix for each edge. In that sense, the algorithm is actually deciding whether the symbolic matrix $\mathcal{A}_G$ defined above has full *nc-rank*. It just so happens that for a bipartite graph G, the symbolic matrix $\mathcal{A}_G$ satisfies

$$\operatorname{rank}(\mathcal{A}_G) = \text{nc-rank}(\mathcal{A}_G).$$

This can be shown by using a Hall block to construct a shrunk subspace for $\mathcal{A}_G$.

The correspondence between bipartite matching and non-commutative rank extends beyond certificates for 'yes' and 'no' instances. In the last decade, several polynomial-time algorithms have been found for computing non-commutative rank, most of which can be viewed as analogues of some bipartite matching algorithms.

- The first algorithm of Garg, Gurvits, Oliveira, Wigderson [GGdOW16] was based on the matrix scaling algorithm [Sin64, LSW98] that approximates the permanent of a non-negative matrix, and in particular, can decide the existence of a perfect matching.
- The Wong-sequence based algorithm of Ivanyos, Qiao, and Subrahmanyam [IQS18] can be viewed as an analogue of the augmenting path algorithm for bipartite matching [Kuh55, FF56].
- The algorithm of Hamada and Hirai [HH21] is an analogue of submodular minimization, which captures bipartite matching.
- Arvind, Chatterjee, and Mukhopadhyay [ACM24] gave another algorithm based on PIT for non-commutative ABPs and some other ideas in [IQS18].

[1] The maximum rank obtained by evaluating on $d \times d$ matrices is always a multiple of d [IQS17].

Despite the existence of multiple polynomial-time algorithms, no NC-algorithm is known for computing nc-rank. Quasi-NC algorithms have only been developed for specific cases, such as when all matrix coefficients $\{A_i\}_i$ are rank-one [GT20], or when they are all skew-symmetric with a rank of at most two [GOR24]. The crucial ingredient of our bipartite matching algorithm is the concept of a Hall block. Its correspondence with shrunk subspace allows us to lift our ideas to non-commutative rank.

Recall that our algorithm for bipartite matching substitutes a Vandermonde matrix for each edge variable. This is possible because each edge variable appears in exactly one entry in the matrix $\sum_e A_e x_e$. When matrices $\{A_i\}$ are arbitrary, each entry can involve multiple variables, and this interaction of Vandermonde matrices seems difficult to handle. Our first step is to use Hirai's reduction [Hir19] for the non-commutative rank problem, reducing it to a special case with block structure. More precisely, the reduction is to the nc-rank of an $mn \times mn$ symbolic matrix of the form

$$(A_{i,j} x_{i,j})_{i,j} \ ,$$

where each $A_{i,j}$ is an $n \times n$ matrix. By appropriately generalizing the ideas from bipartite matching, we get an NC-algorithm for deciding whether a given symbolic matrix of the above form has full nc-rank.

Theorem 1.5. *Given matrices $A_1, A_2, \ldots, A_m \in \mathbb{F}^{n \times n}$, the problem of deciding whether $\sum_i A_i x_i$ has full nc-rank is in NC.*

There is a well-known NC-reduction from computing the nc-rank to deciding if nc-rank is full (see [GGdOW20, Appendix A.3]).

1.3 Origins of the main ideas

The proofs for the decision problems use the corresponding combinatorial characterizations (Hall's theorem, Edmonds' theorem, Fortin-Reutenauer theorem) and the folded Wronskian criterion of linear independence of polynomials. The origin of this technique lies in some powerful ideas from coding theory, namely that of folded Reed-Solomon codes and subspace designs. Folded Reed-Solomon (FRS) codes are a variants of Reed-Solomon codes which are known for achieving list decoding capacity [GR08, PV05]. In the context of list-decoding, a pseudorandom object called *subspace design* was introduced in [GX13] and explicit constructions were given in [GK16]. One of their constructions was based on FRS codes.

Three seemingly different problems concerning explicit constructions of combinatorially optimal codes have been studied recently.

- Codes meeting Generalized Singleton Bound (GSB) [ST23]. GSB is a combinatorial bound on the best list size one can get from any code with a given rate and error bound. In recent breakthrough work [CZ25], it was shown that FRS codes or the so called subspace designable codes come arbitrarily close to GSB (also see [Sri25]).
- MR tensor codes [GHK+17]. These are codes which have the same correctable erasure patterns as the tensor product of two generic linear codes. [GHK+17] gave a combinatorial characterization of the correctable erasure patterns in a special case called $(m, n, 1, b)$-MR.
- $GZP(\ell)$ codes [BGM23] (motivated by GM-MDS conjecture [DSY14]). These are codes whose generator matrix has all maximal minors nonzero, and it can achieve any pattern of zeros

via row transformations, as long as the pattern of zeros do not enforce a maximal minor to be zero. Such patterns of zeros are naturally characterized by a generalization of Hall's Theorem [DSY14].

In a beautiful work, [BGM23] showed that the combinatorial characterizations in the three codes are equivalent, and so are the questions of their construction. Though [CZ25] showed that FRS codes come arbitrarily close to meeting GSB, it appears that they cannot meet GSB exactly for any folding parameter or equivalently, cannot be used to construct $(m, n, 1, b)$-MR Tensor codes. Nevertheless, the near-optimality of FRS codes turned out to be sufficient for algorithmic purposes. Building on [CZ25, LMS25], [BCDZ26] used FRS codes/subspace designs to develop an algorithm for testing correctable erasure patterns for $(m, n, 1, b)$-MR tensor codes. The algorithm is algebraic and can be easily seen to be in NC.

Our starting point was the algorithm of [BCDZ26]. Via the equivalence with $GZP(\ell)$ codes and the associated generalized Hall Theorem [BGM23], we obtained a reduction from bipartite matching to testing correctable erasure patterns for $(m, n, 1, b)$-MR tensor codes. The algorithm in [BCDZ26] is also supposed to work for all MR tensor codes, but assuming a matroid-theoretic conjecture. We observed that, even without the conjecture, it can be interpreted as an algorithm for computing the nc-rank of a special class of symbolic matrices. This class contains the matrices that can be obtained from taking subsets of columns from $(a_{i,j})_{i,j} \otimes (x_{i,j})_{i,j}$ for some $a_{i,j} \in \mathbb{F}$ and variables $\{x_{i,j}\}$. Our next main insight was that both linear matroid intersection and noncommutative rank for arbitrary symbolic matrices reduce to this special class.

The proofs presented in this paper are directly based on a polynomial method inspired from Guruswami-Kopparty's [GK16] construction of subspace designs. One of the crucial ingredients is the following interesting fact [GK16]: polynomials which have many disjoint high-multiplicity (or high folded-multiplicity) zeroes are linearly independent.

Organization of the paper. Section 2 introduces necessary preliminaries. Section 3 gives NC-algorithms for deciding existence of a perfect matching and for computing the maximum weight of a perfect matching in a bipartite graph. Section 4 does the same for the analogous questions in linear matroid intersection. Section 5 gives an NC-algorithm for deciding whether nc-rank of a given symbolic matrix is full. Appendix A gives an alternative NC algorithm for deciding existence of a perfect matching with slightly better parameters (presented using subspace designs). Note that the NC bound for linear matroid intersection immediately implies the same for bipartite matching. Similarly, the algorithm for nc-rank also works for decision versions of bipartite matching and linear matroid intersection. However, we present all the algorithms independently for the benefit of readers interested in only some of these problems.

2 Preliminaries

For a number $n \in \mathbb{N}$, we denote $[n] = \{1, 2, \ldots, n\}$. Parallel complexity classes are NC^k, for $k \in \mathbb{N}$, that consist of all problems computable by uniform polynomial-size boolean circuits of depth $O(\log^k n)$. Class NC is defined as $\mathsf{NC} = \cup_{k \in \mathbb{N}} \mathsf{NC}^k$.

Let $G = (V, E)$ be a graph. All graphs considered in this paper are *undirected*. For $v \in V$, the neighbors of v in G are denoted by $N(v)$,

$$N(v) = \{\, w \in V \mid (v, w) \in E \,\}.$$

For a set $S \subseteq V$, we denote the neighbors of S by $N(S)$,

$$N(S) = \bigcup_{v \in V} N(v).$$

If G is *bipartite*, we have a partition $V = L \cup R$. We say that G is *balanced* if L and R have the same size, $n = |L| = |R|$. The *bi-adjacency matrix* of G is the $n \times n$ matrix $A = (a_{i,j})$ where

$$a_{i,j} = \begin{cases} 1, & \text{if } (i,j) \in E, \\ 0, & \text{otherwise.} \end{cases}$$

By I_n we denote the $n \times n$ identity matrix.

In a graph $G = (V, E)$, a *matching* $M \subseteq E$ is a subset of edges with no two edges sharing an endpoint. A matching which covers every vertex is called a *perfect matching*. Let

$$\mathrm{PM} = \{\, G \mid G \text{ has a perfect matching} \,\}.$$

Clearly only balanced bipartite graphs can have perfect matchings. If $G = (L \cup R, E)$ is an unbalanced bipartite graph, say with $|L| < |R|$, we say that matching M is *left-saturating*, if M covers all nodes in L.

For any weight assignment $w \colon E \to \mathbb{N}$ on the edges of a graph, the *weight of a matching* M is defined to be the sum of weights of all the edges in M, i.e., $w(M) = \sum_{e \in M} w(e)$.

2.1 Hall's Theorem

Hall's Theorem gives a characterization for the existence of a perfect matching in bipartite graphs.

Theorem 2.1 (Philip Hall, 1935)**.** *Let $G = (L \cup R, E)$ be a balanced bipartite graph.*

$$G \in \mathrm{PM} \iff \forall\, S \subseteq L \quad |N(S)| \geq |S|.$$

For a balanced bipartite graph $G = (L \cup R, E)$ with $|L| = |R| = n$, a set $S \subseteq L$ is called a *Hall block*, if $|N(S)| < |S|$. A Hall block is a witness that G has no perfect matching. In the bi-adjacency matrix A of G, the submatrix A_S of A that consists of the rows indexed by Hall block S, there are exactly $|N(S)|$ nonzero columns. Hence, for $|S| = s$, there are $t = n - |N(S)| > n - s$ zero columns in A_S.

Corollary 2.2. *Bipartite graph $G = (L \cup R, E)$ has a Hall block if and only of the bi-adjacency matrix A of G has a $s \times t$ zero submatrix, where $s + t > n$.*

2.2 Linear matroids

Let U be a $n \times m$ matrix over some field, where $n \leq m$. Let u_j be the j-th column vector of U. Then we can write

$$U = (u_1\ u_2\ \cdots\ u_m).$$

The *matroid* $\mathcal{M}(U) = (E, \mathcal{I})$ associated with U has ground set $E = [m]$ and *independent sets* $\mathcal{I} \subseteq \mathcal{P}(E)$, where a set $I \subseteq E$ is *independent*, if the vectors $\{\, u_i \mid i \in I \,\}$ are linearly independent. An inclusion-wise maximal set $B \in \mathcal{I}$ is called a *base*.

Because $\mathcal{M}(U)$ is defined via matrix U, we call it a *linear matroid.* For any set $S \subseteq E$, the *rank* $r(S)$ of S is defined as

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

The *rank* of matroid $\mathcal{M}(U)$ is $r(E)$, which is the size $|B|$ of a base B of $\mathcal{M}(U)$. It is the same as the rank of matrix U in Linear Algebra.

Let $\mathcal{B}$ be the set of base sets of $\mathcal{M}(U)$. 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 $\mathcal{M}(U)^*$, the *dual of* $\mathcal{M}(U)$. It is known that the dual of a linear matroid is again a linear matroid. Let U have full rank. By rearranging its columns and finding a base, we can bring U in form $U = (I_n \; A)$. Then $\overline{U} = (A^T \; I_{m-n})$ is an $(m-n) \times m$ matrix representing the dual matroid $\mathcal{M}(U)^*$. The representation can be computed in NC^2.

Let r be the rank of $\mathcal{M}(U)$. For the rank function r^* of the dual $\mathcal{M}(U)^*$, it is known that for any $T \subseteq E$, we have

$$r^*(T) = r(E \setminus T) - r + |T|.$$

Let U_1 and U_2 be $n \times m$ matrices with $n \leq m$. The *linear matroid intersection* problem (LMI) is to decide, whether the two matroids $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$ have a common base. Let $\mathcal{B}_1, \mathcal{B}_2$ be the set of bases of $\mathcal{M}(U_1), \mathcal{M}(U_2)$, respectively, then

$$\mathrm{LMI} = \{\, (U_1, U_2) \mid \mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset \,\}.$$

The following theorem by Edmonds generalizes Hall's Theorem and gives a certificate when there does not exist a common base.

Theorem 2.3 ([Edm70])**.** *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two matroids on a common ground set E with rank functions r_1 and r_2 and $r_1(E) = r_2(E) = r$. Matroids $\mathcal{M}_1, \mathcal{M}_2$ do not have a common base if and only if there exists a subset $S \subseteq E$ such that*

$$r_1(S) + r_2(E \setminus S) < r.$$

Equivalently,

$$r_1(S) + r_2^*(S) < |S|,$$

where r_2^* is the rank function of the dual of $\mathcal{M}_2$.

2.3 Folded Vandermonde matrix

We will use a special Vandermonde matrix over field $\mathbb{F}$ that we call *folded* Vandermonde matrix. It is a rectangular $D \times r$ matrix with two parameters $\alpha, \gamma \in \mathbb{F}$. The *$\gamma$-folded Vandermonde matrix $V(\alpha)$* is defined as

$$V(\alpha) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \alpha\gamma & \cdots & \alpha\gamma^{r-1} \\ \alpha^2 & (\alpha\gamma)^2 & \cdots & (\alpha\gamma^{r-1})^2 \\ \vdots & \vdots & & \vdots \\ \alpha^{D-1} & (\alpha\gamma)^{D-1} & \cdots & (\alpha\gamma^{r-1})^{D-1} \end{pmatrix}$$

When $\alpha \neq 0$ and γ has order $\geq r$, the elements in the second row are pairwise different and $V(\alpha)$ has full rank.

2.4 Folded Wronskian matrix

Let $p_1(x), p_2(x), \ldots, p_s(x) \in \mathbb{F}[x]$ be polynomials of degree $\leq d$ and $|\mathbb{F}| > d$. A tool to determine whether these polynomials are linearly independent is the classical Wronskian matrix, an $s \times s$ matrix that has the derivatives $p_i^{(j-1)}(x)$ as entries. It is known that the Wronskian has full rank, its determinant in non-zero, if and only if $p_1(x), p_2(x), \ldots, p_s(x)$ are linearly independent.

We will instead use a *folded* Wronskian matrix that was introduced by Guruswami and Kopparty [GK16]. For some parameter $\gamma \in \mathbb{F}$ and polynomials $p_1(x), p_2(x), \ldots, p_s(x) \in \mathbb{F}[x]$, the *$\gamma$-folded Wronskian matrix* $W_\gamma(p_1, p_2, \ldots, p_s)$ is defined as

$$W_\gamma(p_1, p_2, \ldots, p_s) = \begin{pmatrix} p_1(x) & p_2(x) & \cdots & p_s(x) \\ p_1(\gamma x) & p_2(\gamma x) & \cdots & p_s(\gamma x) \\ p_1(\gamma^2 x) & p_2(\gamma^2 x) & \cdots & p_s(\gamma^2 x) \\ \vdots & \vdots & & \vdots \\ p_1(\gamma^{s-1} x) & p_2(\gamma^{s-1} x) & \cdots & p_s(\gamma^{s-1} x) \end{pmatrix}$$

Also the folded Wronskian matrix gives a criterion to decide linear independence of polynomials.

Lemma 2.4 (Folded Wronskian Lemma [GK16])**.** *Let $p_1(x), p_2(x), \ldots, p_s(x)$ be polynomials of degree at most d. Let $\gamma \in \mathbb{F}$ have order more than d. Then $p_1(x), p_2(x), \ldots, p_s(x)$ are linearly independent if and only if* $\det(W_\gamma(p_1, p_2, \ldots, p_s))(x)$ *is a nonzero polynomial.*

Proof. If $p_1(x), p_2(x), \ldots, p_s(x)$ are linearly dependent then the same linear dependence holds among the columns of $W_\gamma(p_1, p_2, \ldots, p_s)$, and thus, its determinant is zero.

Now, suppose $p_1(x), p_2(x), \ldots, p_s(x)$ are linearly independent. Then $d + 1 \geq s$. Let P be an $(d+1) \times s$ matrix whose i-th column has the coefficients of $p_i(x)$. Let V be the γ-folded Vandermonde matrix $V(1)$ with dimensions $(d + 1) \times s$. Observe that

$$W_\gamma(p_1, p_2, \ldots, p_s) = V^T \ \operatorname{diag}(1, x, \ldots, x^d)\ P,$$

where $\operatorname{diag}(1, x, \ldots, x^d)$ is the diagonal matrix with entries $1, x, \ldots, x^d$ on the diagonal. Using the Cauchy-Binet formula, we can write

$$\det(W_\gamma(p_1, p_2, \ldots, p_s))(x) = \sum_{\substack{S \subseteq [d+1] \\ |S| = s}} \det(V_S) \det(P_S) x^{w(S)}, \tag{2.1}$$

where V_S and P_S are the submatrices of V and P, respectively, obtained by taking rows corresponding to set S and $w(S) = \sum_{i \in S}(i - 1)$. Observe that $\det(V_S)$ is nonzero for every S. Hence, the minimum degree term in (2.1) will come from all those sets S^* for which

$$w(S^*) = \min\{\, w(S) \mid S \subseteq [d + 1],\ |S| = s,\ \det(P_S) \neq 0\,\}.$$

There will be a unique such S^*, because in a matroid with distinct weights on elements, the minimum weight base is unique (see e.g., [Sch03b]). Thus, the determinant is nonzero. □

Using the Folded Wronskian Lemma, we can get an interesting fact about roots of a linear space of polynomials.

Definition 2.5 (r-folded root). *An element $\alpha \in \mathbb{F}$ is an* r-folded root *of polynomial $p(x)$ with respect to an element $\gamma \in \mathbb{F}$, if $p(\alpha\gamma^\ell) = 0$ for each $0 \le \ell \le r-1$.*

For a linear space of polynomials $\mathcal{P} \subseteq \mathbb{F}[x]$, an element $\alpha \in \mathbb{F}$ is an r-folded root *of $\mathcal{P}$ with respect to γ, if α is an r-folded root of some polynomial $p(x) \in \mathcal{P}$ with respect to γ.*

Furthermore, let $Z_r(\mathcal{P}, \alpha)$ denote the number of linearly independent polynomials in $\mathcal{P}$ for which α is an r-folded root.

The choice of γ in the definition of an r-folded root will always be clear from the context. Our proofs mainly rely on the following bound on the number of r-folded roots of a space of polynomials.

Lemma 2.6 ([GK16]). *Let $T \subseteq \mathbb{F}$ and $\alpha, \gamma \in \mathbb{F}$ be such that the set*

$$\{\, \alpha\gamma^\ell \mid \alpha \in T,\ 0 \le \ell \le r-1 \,\}$$

has $|T|r$ distinct elements and γ has order more than D. Let $\mathcal{P} \subseteq \mathbb{F}[x]^{\le D}$ be a linear space of polynomials of degree at most D and of dimension s and let $r \ge s$.

1. *The number of r-folded roots of $\mathcal{P}$ in T with respect to γ is at most $sD/(r-s+1)$.*
2. *More generally,*
$$\sum_{\alpha \in T} Z_r(\mathcal{P}, \alpha) \le \frac{sD}{r-s+1}. \tag{2.2}$$

Proof. Let $p_1(x), p_2(x), \ldots, p_s(x) \in \mathbb{F}[x]$ be a basis for $\mathcal{P}$. By Lemma 2.4, the Wronskian determinant $\mathcal{D}_s(x) = \det(W_\gamma(p_1, p_2, \ldots, p_s))(x)$ is nonzero.

1. Let $\alpha \in T$ be an r-folded root of some $p_0(x) \in \mathcal{P}$. Since $p_0(x)$ is linearly dependent on $p_1(x), p_2(x), \ldots, p_s(x)$, we can do a column transformation on $W_\gamma(p_1, p_2, \ldots, p_s)$ so that one of its columns becomes
$$(p_0(x), p_0(\gamma x), \ldots, p_0(\gamma^{s-1}x)).$$
Note that the determinant will only change by a nonzero constant factor. Hence, it still has the same roots. Now, observe that setting x as any element in $\{\alpha, \alpha\gamma, \ldots, \alpha\gamma^{r-s}\}$ makes the p_0-column completely zero. This means that each element in $\{\alpha\gamma^\ell\}_{\ell=0}^{r-s}$ is a root of $\mathcal{D}_s(x)$. That is, each r-folded root of $\mathcal{P}$ gives $r-s+1$ distinct roots of $\mathcal{D}_s(x)$. The degree of $\mathcal{D}_s(x)$ is at most sD. Since the degree is an upper bound on the number of roots, we get the desired bound on the number of r-folded roots.

2. For the more general bound let $\alpha \in T$ and let $q = Z_r(\mathcal{P}, \alpha)$. Then α is an r-folded root of some linearly independent polynomials $g_1(x), g_2(x), \ldots, g_q(x) \in \mathcal{P}$. Since $g_1(x), g_2(x), \ldots, g_q(x)$ are linearly dependent on $p_1(x), p_2(x), \ldots, p_s(x)$, we can do a column transformation on $W_\gamma(p_1, p_2, \ldots, p_s)$ so that q of its columns become
$$(g_1(x), g_1(\gamma x), \ldots, g_1(\gamma^{s-1}x)),\ \ldots,\ (g_q(x), g_q(\gamma x), \ldots, g_q(\gamma^{s-1}x)).$$
Again, the determinant will only change by a nonzero constant factor. Now, observe that setting x as any element in
$$\{\alpha, \alpha\gamma, \ldots, \alpha\gamma^{r-s}\}$$

makes all the columns corresponding to $g_1, g_2, \ldots, g_q$ completely zero. This means that each element in $\{\alpha\gamma^\ell\}_{\ell=0}^{r-s}$ is a root of $\mathcal{D}_s(x)$ with multiplicity q. So, we conclude that the polynomial $\mathcal{D}_x(s)$ has at least

$$(r-s+1)\sum_{\alpha\in T} Z_r(\mathcal{P},\alpha)$$

roots (counting with multiplicity). The degree of $\mathcal{D}_s(x)$ is at most sD. Hence, we get (2.2). $\square$

Remark. *The first part of Lemma 2.6 suffices for the* NC*-algorithm for bipartite matching presented in Section 3. We require the more general statement for the* NC*-algorithm for linear matroid intersection in Section 4 and to compute the non-commutative rank in* NC *in Section 5.*

2.5 An NC reduction from search to weighted decision

As mentioned in the introduction, the algorithm of Fenner, Gurjar, and Thierauf [FGT21] can be viewed as an NC reduction from search to computing the minimum weight of a perfect matching. We explain the idea briefly.

Their algorithm goes in $\log n$ rounds. In the i-th round, they assign weights on the current graph G_{i-1} and and define G_i to be the union of minimum weight perfect matchings in G_{i-1}. The final weights in their scheme become quasi-polynomial because they do not have a way to compute these graphs in each round and thus, they just combine the weight functions from $\log n$ rounds on different scales. Given an oracle to compute the minimum weight of a perfect matching, we can use it to compute the union of minimum weight perfect matchings as follows. Let w^* be the minimum weight of a perfect matching. In parallel, for each edge e, subtract its weight by 1 and compute the minimum weight of a perfect matching. If the weight is w^*-1, then e is a part of a minimum weight perfect matching. In each round, they try polynomially many different weight functions. In the i-th round, there is at least one weight function which ensures that the obtained graph G_i has no cycles of length at most 2^{i+1}. This weight function can be identified by computing the length of the shortest cycle in each possible graph G_i. This, in turn, reduces to the shortest path problem, which is in NC (see, e.g., [DNS81]). As they prove, $G_{\log n-1}$ is a perfect matching. This idea works as is with an oracle for computing maximum weight of a perfect matching as well.

3 Bipartite perfect matching in NC

We give an NC-algorithm to decide whether a given bipartite graph has a perfect matching in Section 3.1. In Section 3.2, we generalize the NC-algorithm to weighted graphs and compute the weight of a maximum weight perfect matching. As explained in Section 2.5, thereby we also solve the construction problem and can compute a maximum weight perfect matching in NC.

3.1 Bipartite perfect matching decision

Let $G(L\cup R, E)$ be a balanced bipartite graph with $n=|L|=|R|$ and let A be its bi-adjacency matrix. We will construct a *matching matrix* $M(G)$ such that $M(G)$ has full rank if and only if G has a perfect matching.

First, we extend A to $\widehat{A}$ by attaching $n(n-1)$ columns to it. We define the extension matrix A_0 as

$$A_0 = \begin{pmatrix} 11\cdots 1 & & & \\ & 11\cdots 1 & & 0 \\ 0 & & \ddots & \\ & & & 11\cdots 1 \end{pmatrix}$$

Matrix A_0 has n rows. The 1-block in each row has length $n-1$. Hence, A_0 has $n(n-1)$ columns. All other entries are 0. Combining A and A_0, we define the $n \times n^2$ extension matrix $\widehat{A} = (A \;\; A_0)$.

We construct the matching matrix $M(G)$ from $\widehat{A}$ by replacing the 1's in $\widehat{A}$ by folded $D \times r$ Vandermonde matrices, for parameters D, r specified below. Let $\gamma \in \mathbb{F}$ be an element of order at least nr. We choose $\alpha_1, \alpha_2, \ldots, \alpha_{n^2} \in \mathbb{F}$, i.e. one value for every column of $\widehat{A}$, such that the set

$$\{\, \alpha_j \gamma^\ell \mid 1 \le j \le n^2,\; 0 \le \ell \le r-1 \,\}$$

has $n^2 r$ distinct elements. Hence, $\mathbb{F}$ should be a field of size at least $n^2 r$.

Now define $M(G)$ by replacing every 1 in column j of $\widehat{A}$ by the $D \times r$ γ-folded Vandermonde matrix $V(\alpha_j)$, for $j = 1, 2, \ldots, n^2$, and each 0 by a $D \times r$ zero-matrix. Hence, $M(G)$ is a $nD \times n^2 r$ matrix. Similar as $\widehat{A}$, we can view $M(G)$ as being composed of two parts, $M(G) = (M_0 \;\; M_1)$, where M_0 are the first nr columns of $M(G)$ coming from bi-adjacency matrix A, and M_1 are the remaining $n(n-1)r$ columns coming from the extension matrix A_0.

Matrix $M(G)$ would be square if we would choose D as nr. However, we need $M(G)$ to be rectangular with slightly less rows. Hence, we have a further parameter δ and we let

$$D = n(r - \delta).$$

We will see below that our arguments work when we choose the parameters such that

$$\delta \ge n \quad \text{and} \quad r > n^2 \delta.$$

Hence $\delta = n$ and $r = n^3 + 1$ is a valid choice.

Example. *For $n = 3$ consider the 3×3 bi-adjacency matrix A of a bipartite graph G,*

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

The extension matrix $\widehat{A}$ is

$$\widehat{A} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Then we get the matching matrix $M(G)$,

$$M(G) = \begin{pmatrix} V(\alpha_1) & V(\alpha_2) & 0 & V(\alpha_4) & V(\alpha_5) & 0 & 0 & 0 & 0 \\ V(\alpha_1) & 0 & V(\alpha_3) & 0 & 0 & V(\alpha_6) & V(\alpha_7) & 0 & 0 \\ 0 & V(\alpha_2) & V(\alpha_3) & 0 & 0 & 0 & 0 & V(\alpha_8) & V(\alpha_9) \end{pmatrix}$$

We show that the rank of $M(G)$ determines the existence of a perfect matching in G.

Theorem 3.1. *Let $G = (L \cup R, E)$ be a balanced bipartite graph. Then*

$$G \in \mathrm{PM} \iff M(G) \text{ has full rank.}$$

Proof. For one direction, we show that if G does not have a perfect matching then $M(G)$ does not have full row rank.

By Theorem 2.1, there is a Hall block $S \subseteq L$ with $|N(S)| < |S|$. Consider the row blocks in $M(G)$ corresponding to S. The total number of rows in these blocks will be

$$D|S| = n(r-\delta)|S| = nr|S| - n\delta|S| \geq nr|S| - n^2\delta.$$

We count the number of columns that have any nonzero entry in these rows. Recall that $M(G) = (M_0\, M_1)$ as explained above. Within M_0 we have $r|N(S)|$ nonzero columns and $(n-1)r|S|$ within M_1. In total, number of nonzero columns in $M(G)$ in these rows is

$$r|N(S)| + (n-1)r|S| \leq r(|S|-1) + (n-1)r|S| = nr|S| - r.$$

As $r > n^2\delta$, we get that number of columns with nonzero entries is strictly less than number of rows. Thus, this set of rows cannot have full row rank.

For the other direction, we prove the contrapositive. Suppose $M(G) = (M_0\, M_1)$ does not have full row rank. Then there is a vector $p \in \mathbb{F}^{nD}$ representing a linear dependency among the rows of $M(G)$, i.e.

$$p^T M(G) = 0. \tag{3.1}$$

Let us split p into blocks as $p = (p_1, p_2, \ldots, p_n)$, where $p_i \in \mathbb{F}^D$. Some of the p_i's might be zero vectors. Without loss of generality, let $p_1, p_2, \ldots, p_s$ be nonzero, for some $s \leq n$, and the rest of the vectors be zero. We view each p_i as the coefficient vector of a polynomial $p_i(x)$ of degree $\deg(p_i) = D-1$. Equation (3.1) gives us roots of the p_i's:

- From the M_1-part of $M(G)$, we get $p_i^T V(\alpha_j) = 0$, for $j = n+(i-1)(n-1)+1, \ldots, n+i(n-1)$, for each $i \in [s]$. Hence, polynomial $p_i(x)$ has the following $n-1$ elements as r-folded roots

$$\{\, \alpha_j \mid n+(i-1)(n-1)+1 \leq j \leq n+i(n-1) \,\}. \tag{3.2}$$

- From the M_0-part of $M(G)$, we get

$$\sum_{i \in [s] : (i,j) \in E} p_i^T V(\alpha_j) = 0, \tag{3.3}$$

for each $j \in [n]$. Define polynomial $q_j(x)$ as

$$q_j(x) = \sum_{i \in [s] : (i,j) \in E} p_i(x)\,. \tag{3.4}$$

From (3.3) we get that $q_j(\alpha_j) = 0$. In fact,

$$\alpha_j \text{ is an } r\text{-folded root of } q_j(x), \tag{3.5}$$

for each $j \in [n]$.

Note that for $j \notin N([s])$, the sum in (3.4) is empty, and hence q_j is zero. For $j \in N([s])$, there are summands in (3.4), still they might cancel each other. We show next that this is not the case: the polynomials $p_1(x), p_2(x), \ldots, p_s(x)$ are linearly independent, and hence, polynomials q_j are nonzero for $j \in N([s])$.

Claim 3.2. *$p_1(x), p_2(x), \ldots, p_s(x)$ are linearly independent.*

Proof. Let $\mathcal{P} = \operatorname{span}\{p_1(x), p_2(x), \ldots, p_s(x)\}$ have dimension $\ell \leq s$. From Lemma 2.6, the number of r-folded roots of $\mathcal{P}$ in $\{\alpha_j\}_j$ is at most

$$\frac{\ell(D-1)}{r-\ell+1} < \frac{\ell n(r-\delta)}{r-\ell+1} < \ell n.$$

The last inequality is because $\delta \geq n$, and thus, $r-\delta < r-\ell+1$. On the other hand, the total number of r-folded roots of $p_1(x), p_2(x), \ldots, p_s(x)$ given in (3.2) is $s(n-1)$. Thus, we have $\ell n > s(n-1)$. Hence, we get

$$\ell > \frac{s(n-1)}{n} \geq s - \frac{s}{n} \geq s-1.$$

This implies $\ell \geq s$, which proves Claim 3.2. □

Now, we know that $\mathcal{P} = \operatorname{span}\{p_1(x), p_2(x), \ldots, p_s(x)\}$ has dimension s. Let us count the r-folded roots of $\mathcal{P}$.

- The total number of r-folded roots of $p_1(x), p_2(x), \ldots, p_s(x)$ given in (3.2) is $s(n-1)$.
- From (3.5), we have an r-folded root of $\mathcal{P}$ for every $j \in [n]$ for which the polynomial $q_j(x)$ is nonzero. Since $p_1(x), p_2(x), \ldots, p_s(x)$ are linearly independent, the number of such polynomials q_j is precisely
  $$|\{\, j \mid (i,j) \in E \text{ for some } i \in [s] \,\}| = |N([s])|.$$
  Hence, we get $|N[s]|$ many r-folded roots of $\mathcal{P}$.

In total, the number of r-folded roots of $\mathcal{P}$ is at least $s(n-1) + |N[s]|$. On the other hand, from Lemma 2.6, we have that the number of r-folded roots of $\mathcal{P}$ in $\{\, \alpha_j \mid j \in [n^2] \,\}$ is at most

$$\frac{s(D-1)}{r-s+1} < sn\left(\frac{r-\delta}{r-s+1}\right) < sn.$$

The last inequality is because $\delta \geq n \geq s$. Comparing the lower and upper bounds, we have

$$s(n-1) + |N[s]| < sn \implies |N[s]| < s.$$

Thus, from Hall's Theorem (Theorem 2.1), G does not have perfect matching. □

Given bipartite graph G, the matching matrix $M(G)$ can be efficiently constructed in parallel. Also the rank of a matrix can be computed in NC. Therefore we get the main result of this section.

Corollary 3.3. *Bipartite perfect matching (decision) is in NC^2.*

3.2 Weighted bipartite perfect matching

Let $G(L \cup R, E)$ be a balanced bipartite graph with $n = |L| = |R|$ and $w : E \to \mathbb{N}$ be a weight function on the edges. We give an NC-algorithm that computes the weight of the maximum weight perfect matching (if one exists).

We generalize the matching matrix $M(G)$ from Section 3.1 to a *weighted matching matrix* $M(G, w)$. We take again the bi-adjacency matrix A of G and its $n \times n^2$ extension matrix $\widehat{A} = (A\, A_0)$. As in Section 3.1, we choose $\gamma \in \mathbb{F}$ and $\alpha_1, \alpha_2, \ldots, \alpha_{n^2} \in \mathbb{F}$ and parameters r, δ and let again

$$D = n(r - \delta).$$

We replace the 1's in $\widehat{A}$ by folded $D \times r$ Vandermonde matrices, where we additionally put the weights in the A-part of $\widehat{A}$. That is, in columns $j = 1, 2, \ldots, n$ of $\widehat{A}$, we replace a 1 in position (i, j) by $t^{w_{i,j}} V(\alpha_j)$, where t is an indeterminate. Formally, for $1 \le i \le n$ and $1 \le j \le n^2$,

$$\text{the } (i,j)\text{-th block of } M(G,w) = \begin{cases} t^{w(i,j)} V(\alpha_j) & \text{if } j \le n \text{ and } (i,j) \in E \\ V(\alpha_j) & \text{if } (n-1)i + 1 < j \le (n-1)(i+1) + 1 \\ 0 & \text{otherwise,} \end{cases}$$

Example. *In the example from Section 3.1, matrix $M(G, w)$ looks as follows,*

$$\begin{pmatrix} t^{w_{1,1}} V(\alpha_1) & t^{w_{1,2}} V(\alpha_2) & 0 & V(\alpha_4) & V(\alpha_5) & 0 & 0 & 0 & 0 \\ t^{w_{2,1}} V(\alpha_1) & 0 & t^{w_{2,3}} V(\alpha_3) & 0 & 0 & V(\alpha_6) & V(\alpha_7) & 0 & 0 \\ 0 & t^{w_{3,2}} V(\alpha_2) & t^{w_{3,3}} V(\alpha_3) & 0 & 0 & 0 & 0 & V(\alpha_8) & V(\alpha_9) \end{pmatrix}$$

Hence, $M(G, w)$ is a $nD \times n^2 r$ matrix.

Let us choose parameters δ and r such that

$$\delta \ge n \quad \text{and} \quad r > 4n^3 \delta W,$$

where W is the maximum weight of any edge. Hence $\delta = n$ and $r = 4n^4 W + 1$ is a valid choice.

With $M(G)$ or $M(G, w)$ we can again associate a bipartite graph $G^{r,\delta}$ that we call the *blow-up graph* of G. It is defined via its $nD \times n^2 r$ bi-adjacency matrix $A^{r,\delta}$, where

$$(A^{r,\delta})_{i,j} = \begin{cases} 1, & \text{if } M(G)_{i,j} \ne 0, \\ 0, & \text{otherwise.} \end{cases}$$

The definition given below gives an alternative construction of $G^{r,\delta}$ that starts from G and makes copies of nodes and edges.

Definition 3.4 (Blow-up graph $G^{r,\delta}$)**.** *Let $G(L \cup R, E)$ be a balanced bipartite graph with $n = |L| = |R|$. The* blow-up graph $G^{r,\delta}$ *of G is the following bipartite graph:*

- *For each $u_i \in L$ make D copies $u_{i,1}, \ldots, u_{i,D}$.*
- *For each $v_j \in R$ make r copies $v_{j,1}, \ldots, v_{j,r}$.*
- *For each $(u_i, v_j) \in E$, put an edge $(u_{i,p}, v_{j,q})$, for every $p \in D$ and $q \in [r]$.*

- *Add $n(n-1)r$ additional vertices on the right $\{ a_{i,q} \mid 1 \le i \le n,\ 1 \le q \le (n-1)r \}$.*
- *Put edge $(u_{i,p}, a_{i,q})$, for every $p \in [D]$ and $q \in [(n-1)r]$.*

Let $\widehat{w}$ be the induced weight function on the edges of $G^{r,\delta}$, that for any edge (u_i, v_j) in G, gives all the edges $(u_{i,p}, v_{i,q})$ the same weight $w(u_i, v_j)$. For the edges $(u_{i,p}, a_{i,q})$ connected to additional vertices, we give them weight zero.

To determine the maximum weight of a perfect matching in G, we will consider the degree of $\det(M(G,w)M(G,w)^T)$ (as a polynomial in t). Define

$$\mathcal{D}_w(t) = \det(M(G,w)M(G,w)^T).$$

Let w^* be the weight of a maximum weight perfect matching M^* in G. By lifting M^* to the blow-up graph $G^{r,\delta}$, one can get a left-saturating matching $\widehat{M}^*$ with weight $\widehat{w}(\widehat{M}^*) = rw^*$. One may hope that $\widehat{M}^*$ is a maximum weight left-saturating matching in $G^{r,\delta}$ and $\deg(\mathcal{D}_w) = 2rw^*$. Unfortunately this does *not* hold in general.

- There are examples where $G^{r,\delta}$ has left-saturating matchings that have weight larger than rw^*.
- In $\mathcal{D}_w$, the terms that come from the large weight left-saturating matchings might cancel each other and hence, $\deg(\mathcal{D}_w)$ might actually be much smaller than $2rw^*$.

We will show upper and lower bounds on $\deg(\mathcal{D}_w)$. These bounds turn out to be good enough to finally determine w^*.

To analyze the degree $\deg(\mathcal{D}_w)$, we will use the LP dual solution. Let us first write the primal and dual LP for bipartite (left-saturating) matching, where the right side has possibly more vertices than the left side.

Primal LP
(Maximum weight left-saturating matching)

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} w(u,v)\ x_{uv} & \\ \text{s.t.} \quad & \sum_{v:(u,v)\in E} x_{uv} = 1 & \forall u \in L \\ & \sum_{u:(u,v)\in E} x_{uv} \le 1 & \forall v \in R \\ & x_{uv} \ge 0 & \forall (u,v) \in E \end{aligned}$$

Dual LP
(Node Potentials)

$$\begin{aligned} \min \quad & \sum_{u\in L} y_u + \sum_{v \in R} z_v & \\ \text{s.t.} \quad & y_u + z_v \ge w(u,v) & \forall (u,v) \in E \\ & y_u \in \mathbb{R} & \forall u \in L \\ & z_v \ge 0 & \forall v \in R \end{aligned}$$

Note that the dual constraint $z_v \ge 0$ can be skipped in the case of a balanced bipartite graph.

Lemma 3.5. *Let w^* be the weight of a maximum matching in a balanced bipartite graph. Then there exists an optimal dual solution (y,z) with objective value w^* such that $y \le 0$ and $z \ge 0$. Moreover, the absolute values of all the dual values is bounded by $2nW$, where W is the maximum weight of any edge.*

Proof. It is known that optimal dual values can be computed as shortest distances in a directed graph based on a maximum weight perfect matching, where edge distances are the given weights or their negative ([Iri60], also see [San09], [Sch03a, Chapter 17]). This means that the dual values are in the range $(-nW, nW)$. To ensure $y \leq 0$ and $z \geq 0$, we can simply add an appropriately large number to all the z values and subtract the same number from all the y values. The solution remains optimal and in the range $(-2nW, 2nW)$. □

The following well known characterization of maximum weight perfect matchings comes from LP duality and it will be useful for us. For a given bipartite graph G with a weight function w and a feasible dual solution (y, z), an edge (u, v) is said to be *tight* if $y_u + z_v = w(u, v)$.

Lemma 3.6. *Suppose we are given a balanced bipartite graph G with weight function w and a feasible dual solution (y, z). If there is a perfect matching that consists only of tight edges then it is a maximum weight perfect matching in G, its weight is same as the sum of all the dual values, and the dual solution is optimal. Moreover, any maximum weight perfect matching in G consists only of tight edges.*

Now, we come to bounding the degree of $\mathcal{D}_w(t)$.

Lemma 3.7. *Let w^* be the weight of the maximum weight perfect matching and W be the maximum weight of any edge in G. Then*

$$|\deg(\mathcal{D}_w(t)) - 2rw^*| \leq 4n^3\delta W. \tag{3.6}$$

Proof. Let $\widehat{R}$ be the set of right side vertices of $G^{r,\delta}$. Recall that $M(G, w)$ is a $nD \times n^2r$ matrix. We index the columns of $M(G, w)$ by $\widehat{R}$ in the natural way. For a subset $S \subseteq \widehat{R}$ of cardinality nD, let $M(G, w)[S]$ be the square submatrix formed by taking columns indexed by S in $M(G, w)$. By the Cauchy-Binet formula, we know that

$$\mathcal{D}_w(t) = \sum_{\substack{S \subseteq [n^2 r] \\ |S| = nD}} \det(M(G, w)[S])^2. \tag{3.7}$$

Observe that $\det(M(G, w)[S])$ is a sum over all perfect matchings in $G^{r,\delta}[S]$, the graph obtained from $G^{r,\delta}$ by deleting all right side vertices outside S. Hence, the degree of $\det(M(G, w)[S])$ is upper bounded by the maximum weight of a perfect matching in $G^{r,\delta}[S]$, which is also a left-saturating matching in $G^{r,\delta}$. So, we conclude that the degree of $\mathcal{D}_w(t)$ can be at most twice the maximum weight of any left saturating matching.

Claim 3.8. *The maximum weight of any left-saturating matching in $G^{r,\delta}$ is bounded by*

$$rw^* + 2n^3\delta W.$$

Proof. Consider an optimal dual solution (y, z) for G, w, where $y \leq 0$, $z \geq 0$, and all values are in the range $(-2nW, 2nW)$ by Lemma 3.5. We construct a dual solution for $G^{r,\delta}$ as follows: for any left (right) side vertex u (v) in G, all its copies get the same dual value y_u (z_v). For any additional vertex $a_{j,q}$ on the right side, its dual value is assigned as $-y_j$ (this makes the edge $(u_{j,p}, a_{j,q})$ tight). Let us denote this dual solution as $(\widehat{y}, \widehat{z})$. Observe that $(\widehat{y}, \widehat{z})$ is a *feasible* dual solution for $G^{r,\delta}, \widehat{w}$.

Any feasible dual solution gives an upper bound on the maximum weight of any left-saturating matching. The upper bound is

$$\begin{aligned} D\sum_{u\in L} y_u + r\sum_{v\in R} z_v - (n-1)r\sum_{u\in L} y_u &= r(\sum_{u\in L} y_u + \sum_{v\in R} z_v) - n\delta\sum_{u\in L} y_u \\ &\leq rw^* + 2n^3\delta W. \end{aligned}$$

This proves Claim 3.8. ☐

As discussed above, this gives an upper bound on $\deg(\mathcal{D}_w(t))$,

$$\deg(\mathcal{D}_w(t)) \leq 2rw^* + 4n^3\delta W. \tag{3.8}$$

Next, we prove a lower bound on $\deg(\mathcal{D}_w(t))$. Clearly, there is a left-saturating matching of weight rw^* in $G^{r,\delta}$. However it is not clear if the corresponding term t^{2rw^*} will appear with a nonzero coefficient in $\mathcal{D}_w(t)$. What we need to show is that a term with large enough power of t will have a nonzero coefficient. We will reduce this task to the unweighted case using LP duality.

Let H be the subgraph of G that consists of the tight edges according to the dual solution (y, z). Similarly let H' be the subgraph of $G^{r,\delta}$ that consists of the tight edges according to the lifted dual solution $(\widehat{y}, \widehat{z})$, as defined in the proof of Claim 3.8. Recall that by construction of $(\widehat{y}, \widehat{z})$, all edges $(u_{j,p}, a_{j,q})$ are tight. Hence, we have $H' = H^{r,\delta}$.

By Lemma 3.6, graph H contains all perfect matchings of G of weight w^*. Hence, the matching matrix $M(H)$ must have full row rank by Theorem 3.1. Note that our choice of parameters δ and r also fullfills the conditions from Section 3.1. Let S be a subset of nD columns such that $\det(M(H)[S])$ is nonzero. Clearly, $H^{r,\delta}[S]$ must have a perfect matching. Since $H^{r,\delta}[S]$ consists of the tight edges of $G^{r,\delta}[S]$, by Lemma 3.6, we have the following for the dual values.

Observation 3.9. *The restriction of $(\widehat{y}, \widehat{z})$ on the vertices of $G^{r,\delta}[S]$ is an optimal dual solution for it. Moreover, the sum of the dual values gives the maximum weight of a perfect matching in $G^{r,\delta}[S]$.*

Let $\widehat{w}_S$ be the maximum weight of any perfect matching in $G^{r,\delta}[S]$,

$$\widehat{w}_S = \max\{\, \widehat{w}(T) \mid T \text{ is a perfect matching in } G^{r,\delta}[S]\,\}.$$

Claim 3.10. *The coefficient of the term $t^{\widehat{w}_S}$ in $\det(M(G, w)[S])$ is $\det(M(H)[S])$, which is nonzero. Thus, $\deg(\det(M(G, w)[S])) = \widehat{w}_S$.*

Proof. Recall that $H^{r,\delta}[S]$ precisely consists of the tight edges of $G^{r,\delta}[S]$. Hence, from Lemma 3.6, the set of maximum weight perfect matchings in $G^{r,\delta}[S]$ is the same as the set of perfect matchings in $H^{r,\delta}[S]$. Since the determinant of a square matrix is a sum over perfect matchings, we get the first part the claim. For the second part, observe that the degree cannot be larger than the maximum weight of a perfect matching. ☐

The next step is to show a lower bound on $\widehat{w}_S$. Then we will argue that $\deg(\mathcal{D}_w(t)) \geq 2\widehat{w}_S$.

Consider again a maximum weight perfect matching M^* in G with weight w^*. It can be lifted to a left-saturating matching $\widehat{M}^*$ in $G^{r,\delta}$ of weight rw^* such that it covers the following nD nodes on the right side of $G^{r,\delta}$:

$$S' = \{\, v_{j,q} \mid 1 \leq j \leq n, 1 \leq q \leq r \,\} \cup \{\, a_{j,q} \mid 1 \leq j \leq n, 1 \leq q \leq D - r \,\}.$$

The sum of the dual values for $G^{r,\delta}[S']$ is

$$D\sum_{u\in L} y_u + r\sum_{v\in R} z_v - (D-r)\sum_{u\in L} y_u = r(\sum_{u\in L} y_u + \sum_{v\in R} z_v) = rw^*.$$

Recall that $G^{r,\delta}$ has n^2r vertices on the right side and $|S| = |S'| = nD = n^2r - n^2\delta$. Therefore S can be obtained from S' by dropping at most $n^2\delta$ vertices from $\{v_{j,q}\}$ and adding at most $n^2\delta$ vertices from $\{a_{j,q}\}$. Hence, the sum of the dual values for $G^{r,\delta}[S]$ and $G^{r,\delta}[S']$ differ by at most $n^2\delta \cdot 2nW = 2n^3\delta W$. By Observation 3.9, $\widehat{w}_S$ is equal to the sum of dual values in $G^{r,\delta}[S]$.

Hence, we get the lower bound

$$\widehat{w}_S \geq rw^* - 2n^3\delta W. \tag{3.9}$$

To get a lower bound for $\deg(\mathcal{D}_w(t))$, observe that for any subset S^* which maximizes the degree of $\det(M(G,w)[S^*])$, we have $\deg(\det(M(G,w)[S^*])) \geq \deg(\det(M(G,w)[S])) = \widehat{w}_S$ (using Claim 3.10). Also note that the highest degree term in $(\det(M(G,w)[S^*]))^2$ has a positive coefficient[2]. Thus, the highest degree terms for all optimal subsets S^* cannot cancel each other in

$$\det(\mathcal{D}_w(t)) = \sum_{\substack{S\subseteq[n^2r] \\ |S|=nD}} \det(M(G,w)[S])^2.$$

Hence, we conclude that $\deg(\mathcal{D}_w(t)) \geq 2\widehat{w}_S$. By (3.9), we get that

$$\deg(\mathcal{D}_w(t)) \geq 2rw^* - 4n^3\delta W. \tag{3.10}$$

Now (3.6) follows from (3.8) and (3.10). $\square$

Lemma 3.7 shows the way how to compute the weight of the maximum weight perfect matching w^* in G. Since we chose $r > 4n^3\delta W$, by (3.6) we get

$$\left| \frac{\deg(\mathcal{D}_w(t))}{2r} - w^* \right| < \frac{1}{2}\,.$$

Therefore, we have

$$w^* = \text{ closest integer to } \frac{\deg(D_w(t))}{2r}.$$

As explained in Section 2.5, when we can compute the maximum weight of a perfect matching, we can also construct a maximum weight perfect matching. The algorithm described in Section 2.5 goes in $O(\log n)$ rounds, and in each round, it makes multiple parallel calls to the subroutine computing maximum weight. Hence, we get the main result of this section.

Theorem 3.11. *A maximum weight perfect matching in a weighted bipartite graph can be computed in* NC^3.

Clearly, this works as well in the unweighted case.

Corollary 3.12. *A perfect matching in a bipartite graph can be computed in* NC^3.

[2] assuming the underlying field is rationals

4 Linear matroid intersection in NC

We consider the decision version and its weighted generalization for linear matroid intersection, similar as in Section 3.2 for perfect matching. We give an NC-algorithm to decide the existence of a common base for two linear matroids in Section 4.1. In Section 4.2, we generalize our algorithm for the decision problem to find the maximum weight of a common base with respect to a weight function on the common ground set, if there exists a common base. Ghosh, Gurjar, and Raj [GGR24, Theorem 2 and Remark 3] showed that this suffices to solve the search problem, computing a maximum weight common base in NC.

Theorem 4.1 ([GGR24])**.** *Given an NC^2-algorithm for finding the maximum weight of a common base of two linear matroids, there exists an NC^3-algorithm for finding a maximum weight common base of two linear matroids with polynomially bounded weights.* [3].

4.1 Linear matroid intersection decision

In this section, we give an NC-algorithm to decide whether there exists a common base for two linear matroids. For a matrix U, let $\mathcal{M}(U)$ represent the matroid represented by U. Let U_1 and U_2 be $n \times m$ matrices over a field $\mathbb{F}$ with $n \leq m$. Let $\overline{U_2}$ be an $(m-n) \times m$ matrix representing the dual of the matroid $\mathcal{M}(U_2)$. For $j \in [m]$, let u_j and v_j denote the jth column vector of U_1 and $\overline{U_2}$ respectively, that is,

$$\begin{aligned} U_1 &= (u_1 \ u_2 \ \cdots \ u_m), \\ \overline{U_2} &= (v_1 \ v_2 \ \cdots \ v_m). \end{aligned}$$

Similar to Section 3.1, we choose parameters

$$\delta \geq m, \ r > m^2\delta \text{ and } D = m(r-\delta).$$

Let $\gamma \in \mathbb{F}$ be an element of order at least mr. We choose $\alpha_1, \alpha_2, \dots, \alpha_{3m-2} \in \mathbb{F}$, such that the set

$$\{\, \alpha_j \gamma^\ell \mid j \in [3m-2],\ 0 \leq \ell \leq r-1 \,\}$$

has $(3m-2)r$ distinct elements. Let A be the following $m \times m^2$ matrix

$$A = \begin{pmatrix} U_1 & I_n & \cdots & I_n & 0 & \cdots & 0 \\ \overline{U_2} & 0 & \cdots & 0 & I_{m-n} & \cdots & I_{m-n} \end{pmatrix},$$

where we put $m-1$ identity matrices I_n in the first n rows and $m-1$ identity matrices I_{m-n} in the last $(m-n)$ rows. We divide the columns of A into $3m-2$ parts, where the first m parts are the m single columns of the U_1-$\overline{U_2}$-matrix. Then each of the $2(m-1)$ identity matrices I_n or I_{m-n} forms one part. We also divide the rows into two parts, where the first part contains the initial n rows and the other part contains the remaining $(m-n)$ rows.

Let $M(U_1, \overline{U_2})$ denote the $mD \times m^2 r$ matrix obtained by tensoring the j-th part of the set of columns of A with the $D \times r$ γ-folded Vandermonde matrix $V(\alpha_j)$, for $j \in [3m-2]$. Formally, for

[3] Their search algorithm makes multiple calls to the algorithm for finding the maximum weight and for all these calls, the input linear matroids can be obtained in NC from the original input linear matroids.

$i \in [2]$, $j \in [3m-2]$, the

$$(i,j)\text{-th block of } M(U_1, \overline{U_2}) = \begin{cases} U_1[j] \otimes V(\alpha_j), & \text{for } i = 1,\ j \in [m], \\ \overline{U_2}[j] \otimes V(\alpha_j), & \text{for } i = 2,\ j \in [m], \\ I_n \otimes V(\alpha_j) & \text{for } i = 1,\ j \in [2m-1] - [m], \\ I_{m-n} \otimes V(\alpha_j) & \text{for } i = 2,\ j \in [3m-2] - [2m-1], \\ 0, & \text{otherwise.} \end{cases}$$

We show that the rank of $M(U_1, \overline{U_2})$ determines whether matroids $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$ have a common base.

Theorem 4.2. *Let U_1, U_2 be $m \times n$ matrices with $n \leq m$. Then*

$$(U_1, U_2) \in \text{LMI} \iff M(U_1, \overline{U_2}) \textit{ has full rank.}$$

Proof. For one direction, we show that if the matroids $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$ do not have a common base then $M(U_1, \overline{U_2})$ does not have full row rank.

Let r_1 and r_2 be the rank functions of $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$. Let r_2^* be the rank function of $\mathcal{M}(\overline{U_2})$, the dual of $\mathcal{M}(U_2)$. By Edmonds' Theorem (Theorem 2.3), there exist $S \subseteq [m]$ such that

$$r_1(S) + r_2^*(S) < |S|. \tag{4.1}$$

Let B_1 be an $n \times n$ invertible matrix that maps $\operatorname{span}(U_1[S])$ to the subspace spanned by the first $r_1(S)$ standard basis vectors of $\mathbb{F}^n$. Similarly, let B_2 be an $(m-n) \times (m-n)$ invertible matrix that maps $\operatorname{span}(\overline{U_2}[S])$ to the subspace spanned by the first $r_2^*(S)$ standard basis vectors of $\mathbb{F}^{m-n}$. Then we have zero submatrices,

$$B_1\, U_1[[n] - [r_1(S)], S] = 0, \tag{4.2}$$

$$B_2\, \overline{U_2}[[m-n] - [r_2^*(S)], S] = 0. \tag{4.3}$$

Let B be the following $mD \times mD$ invertible matrix

$$B = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix} \otimes I_D.$$

Let C be the following $m^2 r \times m^2 r$ invertible block diagonal matrix

$$C = \begin{pmatrix} I_m & & & & & & \\ & B_1^{-1} & & & & \text{\Large 0} & \\ & & \ddots & & & & \\ & & & B_1^{-1} & & & \\ & \text{\Large 0} & & & B_2^{-1} & & \\ & & & & & \ddots & \\ & & & & & & B_2^{-1} \end{pmatrix} \otimes I_r$$

with $(m-1)$ blocks of B_1^{-1} and B_2^{-1}, respectively. Consider the $mD \times rm^2$ product matrix P,

$$P = B\, M(U_1, \overline{U_2})\, C.$$

Using the mixed product property for tensors, we get that for $i \in [2]$, $j \in [3m-2]$, the

$$(i,j)\text{-th block of } P = \begin{cases} B_1 U_1[j] \otimes V(\alpha_j), & \text{for } i = 1,\ j \in [m], \\ B_2 \overline{U_2}[j] \otimes V(\alpha_j), & \text{for } i = 2,\ j \in [m], \\ I_n \otimes V(\alpha_j) & \text{for } i = 1,\ j \in [2m-1] - [m], \\ I_{m-n} \otimes V(\alpha_j) & \text{for } i = 2,\ j \in [3m-2] - [2m-1], \\ 0, & \text{otherwise.} \end{cases}$$

Consider the set R of row indices of P,

$$R = \{r_1(S)D + 1, \ldots, nD\} \;\cup\; \{(n + r_2^*(S))D + 1, \ldots, mD\}.$$

These are $|R| = \rho D$ rows in total, for

$$\rho = m - (r_1(S) + r_2^*(S)).$$

We count the non-zero columns in R. From (4.2) and (4.3) we conclude that among the first mr columns of matrix P, there are at least $r|S|$ zero-columns in rows R. Hence, the number of non-zero columns in R is at most

$$(m - |S|)\, r.$$

In the remaining $m(m-1)r$ columns there are exactly $\rho(m-1)r$ non-zero columns in R. Hence, the number of non-zero columns in R is at most

$$\begin{aligned} (m - |S|)\, r + \rho(m-1)\, r &= mr\rho - r\,(|S| - r_1(S) - r_2^*(S)) \\ &\le mr\rho - r && \text{by (4.1)} \\ &< mr\rho - m^2\delta && \text{by our choice } r > m^2\delta \\ &\le mr\rho - m\delta\rho && \text{as } \rho \le m \\ &= \rho D && \text{by our choice } D = m(r-\delta). \end{aligned}$$

Since $|R| = \rho D$, this implies that P, and hence $M(U_1, \overline{U_2})$, does not have full row rank.

To prove the other direction, we show that if $M(U_1, \overline{U_2})$ does not have full row rank, then $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$ do not have a common base. Let $M(U_1, \overline{U_2}) = (M_0\ M_1)$, where M_0 consists of the first mr columns and M_1 consists of the remaining $m(m-1)r$ columns. Since $M(U_1, \overline{U_2})$ does not have full row rank, there is a non-zero vector $p \in \mathbb{F}^{mD}$ representing a linear dependency among the rows of $M(U_1, \overline{U_2})$, i.e. $p^T\, M(U_1, \overline{U_2}) = 0$. Let us split p into m blocks as

$$p = (p_{1,1}, \ldots, p_{1,n}, p_{2,1} \ldots, p_{2,m-n}),$$

where each $p_{i,k} \in \mathbb{F}^D$. Let

$$\begin{aligned} \mathcal{P}_1 &= \operatorname{span}\{p_{1,1}, \ldots, p_{1,n}\}, \\ \mathcal{P}_2 &= \operatorname{span}\{p_{2,1}, \ldots, p_{2,m-n}\}, \\ \mathcal{P} &= \operatorname{span}\{p_{1,1}, \ldots, p_{1,n}, p_{2,1} \ldots, p_{2,m-n}\} \end{aligned}$$

with dimensions $s_1 = \dim \mathcal{P}_1$, $s_2 = \dim \mathcal{P}_2$, and $s = \dim \mathcal{P}$.

Let us view each $p_{i,k}$ as the coefficient vector of a polynomial $p_{i,k}(x)$ of degree $D-1$. The equation $p^T\,(M_0\ M_1) = 0$ gives us roots of the $p_{i,k}$'s:

- From $p^T\,M_1 = 0$, we get for each $1 \le j < m$ and $1 \le k \le n$,

  $$p_{1,k}^T V(\alpha_{m+j}) = 0.$$

  That is, polynomial $p_{1,k}(x)$ has α_{m+j} as an r-folded root. Similarly, for each $1 \le j < m$ and $1 \le k \le m-n$, polynomial $p_{2,k}(x)$ has α_{2m+j-1} as an r-folded root.

  Recall from Definition 2.5 that $Z_r(\mathcal{P}, \alpha)$ denotes the number of linearly independent polynomials in $\mathcal{P}$ for which α is an r-folded root. We conclude that for each $1 \le j < m$, we have

  $$Z_r(\mathcal{P}, \alpha_{m+j}) \ge s_1 \text{ and } Z_r(\mathcal{P}, \alpha_{2m+j-1}) \ge s_2,$$

  and hence,

  $$\sum_{j=m+1}^{3m-2} Z_r(\mathcal{P}, \alpha_j) \ge (m-1)(s_1+s_2). \tag{4.4}$$

- Considering $p^T M_0$, define vectors q_j, for $j \in [m]$, as

  $$q_j = \sum_{k=1}^{n} p_{1,k} U_1[k,j] + \sum_{k=1}^{m-n} p_{2,k} \overline{U_2}[k,j].$$

  From $p^T M_0 = 0$, we get

  $$q_j V(\alpha_j) = 0, \tag{4.5}$$

  for each $j \in [m]$. We view q_i as the coefficient vector of polynomial $q_j(x)$. By (4.5), we have that α_j is an r-folded root of polynomial q_j. Hence, for $j \in [m]$,

  $$Z_r(\mathcal{P}, \alpha_j) = \begin{cases} 1, & \text{if } q_j(x) \ne 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4.6}$$

  Define

  $$S = \{\, j \in [m] \mid q_j = 0 \,\}.$$

  Then we have $\sum_{j=1}^{m} Z_r(\mathcal{P}, \alpha_j) = m - |S|$.

Our goal now is to show that set S is a blocking set for $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$ to have a common base according to Theorem 2.3.

Together with (4.4), we get

$$\sum_{j=1}^{3m-2} Z_r(\mathcal{P}, \alpha_j) \ge (m-1)(s_1+s_2) + m - |S|. \tag{4.7}$$

As an upper bound on the Z_r-sum, we can apply Lemma 2.6:

$$\sum_{j=1}^{3m-2} Z_r(\mathcal{P}, \alpha_j) \le \frac{s(D-1)}{r-s+1} < sm \left(\frac{r-\delta}{r-s+1}\right) < sm. \tag{4.8}$$

The last inequality is because $\delta \geq m \geq s$. Combining (4.7) and (4.8), we get

$$(m-1)(s_1+s_2)+m-|S|<sm. \tag{4.9}$$

Hence, we get a lower bound for $|S|$,

$$(m-1)(s_1+s_2)-sm+m<|S|. \tag{4.10}$$

In Section 3.1, we showed in Claim 3.2 that the corresponding p-polynomials were linearly independent. Here, we show a weaker statement that $\mathcal{P}$ is a direct sum of spaces $\mathcal{P}_1$ and $\mathcal{P}_2$, i.e. $\mathcal{P}=\mathcal{P}_1\oplus\mathcal{P}_2$. That is, $\mathcal{P}=\mathcal{P}_1\cup\mathcal{P}_2$ and $\mathcal{P}_1\cap\mathcal{P}_2=\{0\}$. Equivalently one can say that the dimensions are additive.

Claim 4.3. *$s=s_1+s_2$.*

Proof. From (4.9) we get $sm>(m-1)(s_1+s_2)$. We can write

$$s>\frac{(s_1+s_2)(m-1)}{m}=(s_1+s_2)-\frac{s_1+s_2}{m}\geq s_1+s_2-1.$$

Therefore $s\geq s_1+s_2$. Since we also have $s\leq s_1+s_2$ by definition, this proves the claim. $\square$

Plugging $s=s_1+s_2$ in (4.10), we get

$$m-(s_1+s_2)<|S|. \tag{4.11}$$

In the definition of set S, we have the condition $q_j=0$. Since $\mathcal{P}=\mathcal{P}_1\oplus\mathcal{P}_2$, we have $q_j=0$ iff the two sums in the definition of q_j each are zero. These sums we can write as matrix products. Define $D\times n$ matrix P_1 and $D\times(m-n)$ matrix P_2 with column vectors $p_{i,j}$,

$$P_1=\begin{pmatrix}p_{1,1} & \dots & p_{1,n}\end{pmatrix},$$
$$P_2=\begin{pmatrix}p_{2,1} & \cdots & p_{2,m-n}\end{pmatrix}.$$

Then, for each $j\in[m]$,

$$q_j=0 \iff P_1U_1[j]=P_2\overline{U_2}[j]=0.$$

Since P_1 has dimension s_1, the null-space of P_1 has dimension $n-s_1$. Since $P_1U_1[S]=0$, we have

$$r_1(S)=\dim(\mathrm{span}(U_1[S]))\leq n-s_1.$$

Similarly $r_2^*(S)\leq m-n-s_2$. Putting this in (4.11), we get

$$r_1(S)+r_2^*(S)<|S|,$$

which implies that $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$ do not have a common base from Theorem 2.3. $\square$

4.2 Weighted linear matroid intersection

First we discuss some notations and known results in matroid theory. For an $n \times m$ matrix U and a subset $S \subseteq [m]$, let $U[S]$ denote the sub-matrix of U with columns indexed by S. When $S = \{j\}$, we use $U[j]$ instead of $U[\{j\}]$. For a weight function $w : [m] \to \mathbb{Z}$ and $c \in \mathbb{Z}$, let

$$U^{w,>c} = \mathrm{span}(\{U[j] \mid w(j) > c\}).$$

Similarly we define $U^{w,\geq c}$, $U^{w,<c}$ and $U^{w,\leq c}$.

Lemma 4.4. *Let M_1 be an $n \times m$ matrix and $w : [m] \to \mathbb{Z}$ with ℓ distinct weights $c_1 > \cdots > c_\ell$. Let $E_0 = \emptyset$ and*

$$E_i = \{j \in [m] \mid w(j) \geq c_i\} \text{ for each } i \in [\ell].$$

Let X_i be a subspace of $\mathbb{F}^n$ such that $\mathrm{span}(M_1[E_i])$ is a direct sum of X_i and $\mathrm{span}(M_1[E_{i-1}])$ for each $i \in [\ell]$. Let M_2 be another matrix such that for each $i \in [\ell]$ and $j \in E_i \setminus E_{i-1}$, its jth column is X_i-component of $M_1[j]$. Then, for any subset B of $[m]$ of size n, $\det(M_1[B]) = \det(M_2[B])$ if B is a maximum weight base for M_1, otherwise zero.

Proof. To show this, we will use the following claim that directly follows from the greedy algorithm for finding a maximum weight base of a matroid [Sch03b].

Claim 4.5. *Let $\mathcal{M}$ be a matroid on ground set $[m]$ and $w : [m] \to \mathbb{Z}$ be a weight function. Then, a subset B is a maximum weight base of $\mathcal{M}$ if and only if for each $i \in [\ell]$, $|B \cap E_i| = \mathrm{rank}(E_i)$.*

Let $B \subseteq [m]$ be a maximum weight base. Let j be some element in B with weight c_{i+1}. From above claim, $\mathrm{span}(M_1[E_i]) = \mathrm{span}(M_1[E_i \cap B])$. Since $M_1[j] - M_2[j] \in \mathrm{span}(M_1[E_i])$, we can convert $M_1[j]$ to $M_2[j]$ by adding appropriate multiples of columns in $M_1[B \cap E_i]$ to it. Note that these column operations do not change the $\mathrm{span}(M_1[E_{i+1}])$. By applying this transformation sequentially along the nested subsets $(E_1 \cap B) \subseteq \cdots \subseteq (E_\ell \cap B)$, we can systematically convert $M_1[B]$ into $M_2[B]$. Hence, $\det(M_1[B]) = \det(M_2[B])$.

Let B be a set of size n that is not a maximum weight base. Then, from Claim 4.5, there exists some $i \in [\ell]$ such that $|B \cap (E_i \setminus E_{i-1})| > \mathrm{rank}(M_1[E_i]) - \mathrm{rank}(M_1[E_{i-1}])$. However, from construction of M_2,

$$\mathrm{rank}(M_2[E_i \setminus E_{i-1}]) = \mathrm{rank}(M_1[E_i]) - \mathrm{rank}(M_1[E_{i-1}]).$$

This implies that columns in $B \cap (E_i \setminus E_{i-1})$ are dependent in M_2 and hence $\det(M_2[B]) = 0$. $\square$

Analogously, we can show the following lemma.

Lemma 4.6. *Let M_1 be an $n \times m$ matrix and $w : [m] \to \mathbb{Z}$ with ℓ distinct weights $c_1 < \cdots < c_\ell$. Let $E_0 = \emptyset$ and*

$$E_i = \{j \in [m] \mid w(j) \leq c_i\} \text{ for each } i \in [\ell].$$

Let X_i be a subspace of $\mathbb{F}^n$ such that $\mathrm{span}(M_1[E_i])$ is a direct sum of X_i and $\mathrm{span}(M_1[E_{i-1}])$ for each $i \in [\ell]$. Let M_2 be another matrix such that for each $i \in [\ell]$ and $j \in E_i \setminus E_{i-1}$, its jth column is X_i-component of $M_1[j]$. Then, for any subset B of $[m]$ of size n, $\det(M_1[B]) = \det(M_2[B])$ if B is a minimum weight base for M_1, otherwise zero.

In our algorithm, we will be working rectangular matrices whose entries are univariate polynomials. The following lemma follows from [DW92, Proposition 2.9] and it states that the set of minors with the maximum degree forms a matroid. See [Mur96, Example 3.2, Lemma 3.1] for more details.

Lemma 4.7. *Let t be a variable and M be an $n \times m$ matrix over $\mathbb{F}[t]$ with $n \leq m$. Let $\omega : \binom{[m]}{n} \to \mathbb{Z}$ be a function such that for a subset S of $[m]$ of size n,*

$$\omega(S) = \begin{cases} \deg(\det(M[S])) & \text{if } \det(M[S]) \neq 0 \\ -\infty & \text{otherwise.} \end{cases}$$

Then, the family of sets that maximize ω forms a matroid on $[m]$.

Now, we discuss some results related to *optimal weight splitting* for matroid intersection which generalizes the idea of optimal dual solution for bipartite matching. For a ground set E, a set family $\mathcal{F}$ on E and a weight function $w : E \to \mathbb{Z}$, let

$$w^{\max}(\mathcal{F}) = \max_{S \in \mathcal{F}} w(S) \text{ and } w^{\min}(\mathcal{F}) = \min_{S \in \mathcal{F}} w(S).$$

Definition 4.8. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two matroids defined on a common ground set E. Let $w, w_1, w_2 : E \to \mathbb{Z}$ be weight functions on E. Then, w_1 and w_2 is said be a* split *of w if $w_1 + w_2 = w$.*
Moreover, it is called an optimal split *for $\mathcal{M}_1$ and $\mathcal{M}_2$ if*

$$w^{\max}(\mathcal{M}_1 \cap \mathcal{M}_2) = {w_1}^{\max}(\mathcal{M}_1) + {w_2}^{\max}(\mathcal{M}_2).$$

Note that for any split w_1, w_2 of w

$$w^{\max}(\mathcal{M}_1 \cap \mathcal{M}_2) \leq {w_1}^{\max}(\mathcal{M}_1) + {w_2}^{\max}(\mathcal{M}_2).$$

The following lemma gives a characterization of when an split is an optimal split [Fra81, Fra08].

Lemma 4.9. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two matroids defined on a common ground set E. Let $w, w_1, w_2 : E \to \mathbb{Z}$ be weight functions on E. Then, w_1, w_2 is an optimal split of w for $\mathcal{M}_1$ and $\mathcal{M}_2$ if and only if there exists a common base B that maximizes both w_1 for $\mathcal{M}_1$ and w_2 for $\mathcal{M}_2$.*

An optimal weight split always exists and can be computed in polynomial time [Fra81]. Furthermore, if the weights of w are integers, then the algorithm of [Fra81] computes an optimal weight split w_1, w_2 such that the weights are integers. The following lemma gives an optimal split such that the weight functions of the split are bounded with respect to the original weight function [Har07]. As in Lemma 3.5, these weights are defined by the vertex-weighted shortest distances in a directed graph on the vertex set E, where each vertex $e \in E$ has a weight of $\pm w(e)$.

Lemma 4.10. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two matroids defined on a common ground set E of size m. Let $w : E \to \mathbb{N}$ be a weight function on E such that the maximum weight is bounded by W. Then, there exists an optimal split w_1, w_2 of w for $\mathcal{M}_1$ and $\mathcal{M}_2$ such that*

$$-2mW \leq w_1(e) < 0 \text{ and } 0 < w_2(e) \leq 2mW \text{ for each } e \in E.$$

Now we discuss the algorithm for computing the maximum weight of the common base of two linear matroids represented by $n \times m$ matrices U_1 and U_2 with respect to a weight function $w : [m] \to \mathbb{N}$. Let

$$U_1 = (u_1 \; u_2 \; \cdots \; u_m),$$
$$\overline{U_2} = (v_1 \; v_2 \; \cdots \; v_m).$$

Let t be a variable and A^w be the following $m \times m^2$ matrix

$$\begin{pmatrix} t^{w(1)}u_1 & \cdots & t^{w(m)}u_m & I_n & \cdots & I_n & 0 & \cdots & 0 \\ v_1 & \cdots & v_m & 0 & \cdots & 0 & I_{m-n} & \cdots & I_{m-n} \end{pmatrix},$$

where we put $m-1$ identity matrices I_n in the first n rows and $m-1$ identity matrices I_{m-n} in the last $(m-n)$ rows. Like in Subsection 4.1, we divide the columns of A^w into $3m-2$ parts, where the first m parts are the initial m columns. Then each of the $2(m-1)$ identity matrices I_n or I_{m-n} forms one part. Let $M(U_1, \overline{U_2}, w)$ denote the $mD \times m^2 r$ matrix obtained by tensoring the columns in the jth part of A^w with $V(\alpha_j)$ for each $j \in [3m-2]$. Formally, for $i \in [2]$, $j \in [3m-2]$, the

$$(i,j)\text{-th block of } M(U_1, \overline{U_2}, w) = \begin{cases} (t^{w(j)} U_1[j]) \otimes V(\alpha_j), & \text{for } i = 1,\ j \in [m], \\ \overline{U_2}[j] \otimes V(\alpha_j), & \text{for } i = 2,\ j \in [m], \\ I_n \otimes V(\alpha_j) & \text{for } i = 1,\ j \in [2m-1] - [m], \\ I_{m-n} \otimes V(\alpha_j) & \text{for } i = 2,\ j \in [3m-2] - [2m-1], \\ 0, & \text{otherwise,} \end{cases}$$

For a weight function w on $[m]$, let $\widehat{w}$ denote the induced weight function on $[m^2 r]$ defined as follows. For $j \in [m^2]$ and $q \in [r]$,

$$\widehat{w}((j-1)r + q) = \begin{cases} w(j) & \text{if } j \in [m] \\ 0 & \text{otherwise.} \end{cases}$$

Note that if w_1, w_2 is an split of w, then $\widehat{w_1}, \widehat{w_2}$ is an split of $\widehat{w}$. Let us choose parameters δ and r such that

$$\delta \geq m \;\text{ and }\; r > 12m^3\delta W,$$

where W is the maximum weight of any element with respect to w.

Let z be another variable and $f : [m^2 r] \to \mathbb{N}$ be a weight function with each element having distinct weights and Z be an $m^2 r \times m^2 r$ diagonal matrix whose ith diagonal entry is $z^{f(i)}$. To determine the maximum weight of a common base of U_1 and U_2, we will consider the degree of $\det(M(U_1, \overline{U_2}, w) Z M(U_1, \overline{U_2}, w)^T)$ (as a polynomial in t). Define

$$\mathcal{D}_w(t,z) = \det(M(U_1, \overline{U_2}, w) Z M(U_1, \overline{U_2}, w)^T).$$

In the following two lemmas, we give a bound on $\deg_t(\mathcal{D}_w(t,z))$. Let w_1, w_2 be an optimal split of w for $\mathcal{M}(U_1), \mathcal{M}(U_2)$ from Lemma 4.9. Then,

$$-2mW \leq w_1(j) < 0 \text{ and } 0 < w_2(j) \leq 2mW \text{ for each } j \in [m]. \tag{4.12}$$

Lemma 4.11. *Let $w^* = w^{\max}(\mathcal{M}(U_1) \cap \mathcal{M}(U_2))$ and W be the maximum weight of any element in $[m]$. Then,*

$$\deg_t(\mathcal{D}_w(t,z)) \leq 2rw^* + 8m^3\delta W. \tag{4.13}$$

Proof. For a matrix A with mD rows, let A^{top} and A^{bot} represent the submatrices of A with the first nD rows and the remaining $(m-n)D$ rows, respectively. By the Cauchy-Binet formula, we know that

$$\mathcal{D}_w(t,z) = \sum_{\substack{S \subseteq [m^2 r] \\ |S| = mD}} z^{f(S)} (M(U_1, \overline{U_2}, w)[S])^2. \tag{4.14}$$

For a subset S of $[m^2r]$ of size mD, by Laplace Theorem,

$$\det(M(U_1, \overline{U_2}, w))[S] = \sum_{\substack{T \subset S \\ |T| = nD}} \pm t^{\widehat{w}(T)} \det(M(U_1, \overline{U_2})^{\text{top}}[T]) \cdot \det(M(U_1, \overline{U_2})^{\text{bot}}[S \setminus T]).$$

Hence,

$$\begin{aligned}
\deg_t(\det(M(U_1, \overline{U_2}, w)[S])) &\leq \max_{\substack{T \in \mathcal{M}(M(U_1, \overline{U_2})^{\text{top}}) \\ S \setminus T \in \mathcal{M}(M(U_1, \overline{U_2})^{\text{bot}})}} \widehat{w}(T) \\
&= \max_{\substack{T \in \mathcal{M}(M(U_1, \overline{U_2})^{\text{top}}) \\ S \setminus T \in \mathcal{M}(M(U_1, \overline{U_2})^{\text{bot}})}} \widehat{w_1}(T) - \widehat{w_2}(S \setminus T) + \widehat{w_2}(S) \\
&\leq \widehat{w_1}^{\max}(\mathcal{M}(M(U_1, \overline{U_2})^{\text{top}})) - \widehat{w_2}^{\min}(\mathcal{M}(M(U_1, \overline{U_2})^{\text{bot}})) + rw_2([m]).
\end{aligned}$$

Above, the second equality follows from the fact that $\widehat{w_1}, \widehat{w_2}$ is a split of $\widehat{w}$. The last inequality follows from the fact that elements in $[mr]$ and $[m^2r] \setminus [mr]$ has positive and zero weights, respectively, in $\widehat{w_2}$; and $\widehat{w_2}(S) \leq \widehat{w_2}([mr]) = rw_2([m])$. Now, we discuss how the following claim which directly implies the upper bound on $\deg_t(\mathcal{D}_w(t,z))$. From (4.14) and above discussion,

$$\begin{aligned}
\deg_t(\mathcal{D}_w(t,z)) &\leq 2\left(\widehat{w_1}^{\max}(\mathcal{M}(M(U_1, \overline{U_2})^{\text{top}})) - \widehat{w_2}^{\min}(\mathcal{M}(M(U_1, \overline{U_2})^{\text{bot}})) + rw_2([m])\right) \\
&\leq 2\left(r({w_1}^{\max}(\mathcal{M}(U_1)) - {w_2}^{\min}(\mathcal{M}(\overline{U_2})) + w_2([m])) + 4m^3\delta W\right) \\
&= 2(r({w_1}^{\max}(\mathcal{M}(U_1)) + {w_2}^{\max}(\mathcal{M}(U_2))) + 4m^3\delta W) \\
&= 2rw^* + 8m^3\delta W.
\end{aligned} \tag{4.15}$$

The second inequality above follows from Claim 4.12. The second last equality follows from the fact that $\mathcal{M}(\overline{U_2})$ is dual of $\mathcal{M}(U_2)$, and for any matroid $\mathcal{M}$ and its dual $\mathcal{M}^*$ defined on ground set $[m]$ with a weight function w, the following holds.

$$w^{\min}(\mathcal{M}^*) = w([m]) - w^{\max}(\mathcal{M}).$$

The last equality follows from the fact that w_1, w_2 is an optimal split of w for $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$.

Claim 4.12.

$$\begin{aligned}
\widehat{w_1}^{\max}(\mathcal{M}(M(U_1, \overline{U_2})^{\text{top}})) &\leq r({w_1}^{\max}(\mathcal{M}(U_1))), \\
\widehat{w_2}^{\min}(\mathcal{M}(M(U_1, \overline{U_2})^{\text{bot}})) &\geq r({w_2}^{\min}(\mathcal{M}(\overline{U_2}))) - 4m^3\delta W.
\end{aligned}$$

Proof. First, we compute $\widehat{w_1}^{\max}(\mathcal{M}(M(U_1,\overline{U_2})^{\text{top}}))$. Let $S_1 \subset [m]$ and $\widehat{S_1} \subset [m^2r]$ be the maximum weight base of $\mathcal{M}(U_1)$ and $\mathcal{M}(M(U_1,\overline{U_2})^{\text{top}})$ chosen by the greedy algorithm with respect to w_1 and $\widehat{w_1}$, respectively. The weights of the elements in $[mr]$ and $[m^2r] \setminus [mr]$ are negative and zero in $\widehat{w_1}$, respectively. Also, the set of non-zero columns of $M(U_1,\overline{U_2})^{\text{top}}$ in $[m^2r] \setminus [mr]$ are independent. Hence, $\widehat{S_1}$ contains all the elements from the set $[m^2r] \setminus [mr]$ corresponding to the non-zero columns of $M(U_1,\overline{U_2})^{\text{top}}$.

Now, we show the following claim that establishes a relation between S_1 and $\widehat{S_1}$.

Claim 4.13. *Let $j \in [m] \setminus S_1$. Then*

$$\widehat{S_1} \cap \{(j-1)r + q \mid q \in [r]\} = \emptyset. \tag{4.16}$$

Proof. Let $M = M(U_1,\overline{U_2})^{\text{top}}$. Then, the above claim is equivalent to showing that for each $j \in [m]$,

$$u_j \in U^{w_1,>w_1(j)} \implies \left(\text{span}(u_j \otimes V(\alpha_j)) \leq M^{\widehat{w_1},>w_1(j)}\right).$$

For this, we will show that for each $k \in [m], v \in \mathbb{F}^D$, we have

$$u_k \otimes v \in \text{span}(u_k \otimes V(\alpha_k)) + M^{\widehat{w_1},=0}.$$

Let V^{top} be the $D \times (m-1)r$ matrix defined as

$$V^{\text{top}} = \begin{pmatrix} V(\alpha_{m+1}) & V(\alpha_{m+2}) & \cdots & V(\alpha_{2m-1}) \end{pmatrix}.$$

Note that

$$M^{\widehat{w_1},=0} = \text{span}(M[[m^2r] \setminus [mr]]) = \text{span}(I_n \otimes V^{\text{top}}).$$

Hence, for any $a \in \text{span}(V^{\text{top}})$, $u_k \otimes a \in M^{\widehat{w_1},=0}$. Let us consider the $D \times mr$ matrix $(V(\alpha_j) \;\; V^{\text{top}})$. It is a Vandermonde matrix with mr columns which is greater than D. Hence, this matrix spans $\mathbb{F}^D$, which in turn implies that there exists $a \in \text{span}(V^{\text{top}})$ and $b \in \text{span}(V(\alpha_j))$ such that $v = a + b$. Therefore,

$$u_k \otimes v \in \text{span}(u_k \otimes V(\alpha_k)) + M^{\widehat{w_1},=0}. \tag{4.17}$$

Let $u \in U^{w_1,>w_1(j)}$ and $v \in \mathbb{F}^D$. Then, there exists scalars λ_ks such that

$$u = \sum_{w_1(k)>w_1(j)} \lambda_k u_k \text{ and } u \otimes v = \sum \lambda_k (u_k \otimes v).$$

For any k with $w_1(k) > w_1(j)$, from (4.17), we have

$$u_k \otimes v \in \text{span}(u_k \otimes V(\alpha_k)) + M^{\widehat{w_1},=0} \leq M^{\widehat{w_1},>w_1(j)}.$$

Hence, $u \otimes v \in M^{\widehat{w_1},>w_1(j)}$. Since $u_j \in U^{w_1,>w_1(j)}$ and $\text{span}(V(\alpha_j)) \leq \mathbb{F}^D$, we have

$$\text{span}(u_j \otimes V(\alpha_j)) \leq M^{\widehat{w_1},>w_1(j)},$$

which in turn proves the Claim 4.13. ∎

Thus,

$$\begin{aligned}
\widehat{w_1}(\widehat{S_1}) &= \sum_{j\in[m]} w_1(j)\cdot|\widehat{S_1}\cap\{(j-1)r+q \mid q\in[r]\}| && [\text{Definition of } \widehat{S_1}]\\
&= \sum_{j\in S_1} w_1(j)\cdot|\widehat{S_1}\cap\{(j-1)r+q \mid q\in[r]\}| && [\text{From Claim 4.13}]\\
&\le r\sum_{j\in S_1} w_1(j) = r{w_1}^{\max}(\mathcal{M}(U_1)).
\end{aligned}$$

Now, we compute $\widehat{w_2}^{\min}(\mathcal{M}(M(U_1,\overline{U_2})^{\mathrm{bot}}))$. Let $S_2\subset[m]$ and $\widehat{S_2}\subset[m^2r]$ be the minimum weight base of $\mathcal{M}(\overline{U_2})$ and $\mathcal{M}(M(U_1,\overline{U_2})^{\mathrm{bot}})$ chosen by the greedy algorithm with respect to w_2 and $\widehat{w_2}$, respectively. The weights of the elements in $[mr]$ and $[m^2r]\setminus[mr]$ are positive and zero in $\widehat{w_2}$, respectively. Also, the set of non-zero columns of $M(U_1,\overline{U_2})^{\mathrm{bot}}$ in $[m^2r]\setminus[mr]$ are independent. Hence, $\widehat{S_2}$ contains all the elements from the set $[m^2r]\setminus[mr]$ corresponding to the non-zero columns of $M(U_1,\overline{U_2})^{\mathrm{bot}}$. Let

$$S_2' = (\widehat{S_2}\cap([m^2r]\setminus[mr]))\cup\{(j-1)r+q \mid j\in S_2, q\in[r-m\delta]\}.$$

Clearly, $|S_2'|=(m-n)D$ and $\widehat{w_2}(S_2')=(r-m\delta)w_2(S_2)$. Let

$$\overline{S_2}=\{(j-1)r+q \mid j\in S_2, q\in[r]\}.$$

Using arguments similar to show Claim 4.13, we can show that if some $j\in[m]$ does not belong to S_2, then

$$\widehat{S_2}\cap\{(j-1)r+q \mid q\in[r]\}=\emptyset. \tag{4.18}$$

Hence, $S_2'\setminus\widehat{S_2},\widehat{S_2}\setminus S_2'\subseteq\overline{S_2}$ which is of size $(m-n)r$. Also,

$$|S_2'\cap\overline{S_2}|=|\widehat{S_2}\cap\overline{S_2}|=(m-n)(D-(m-1)r)=(m-n)(r-m\delta).$$

Therefore, $\widehat{S_2}$ can be obtained from S_2' by dropping at most $(m-n)m\delta$ elements from $\overline{S_2}$ and adding at most $(m-n)m\delta$ elements from $\overline{S_2}$. Hence, from construction of $\widehat{w_2}$ and (4.12), we get that $\widehat{w_2}(\widehat{S_2})$ and $\widehat{w_2}(S_2')$ differ by at most $(m-n)m\delta\cdot 2mW$. Hence,

$$\begin{aligned}
\widehat{w_2}(\widehat{S_2}) &\ge \widehat{w_2}(S_2') - 2m^2(m-n)\delta W\\
&= (r-m\delta)w_2(S_2) - 2(m-n)m^2\delta W\\
&\ge rw_2(S_2) - 4(m-n)m^2\delta W \ge r{w_2}^{\min}(\mathcal{M}(\overline{U_2})) - 4m^3\delta W,
\end{aligned}$$

where the second last inequality follows from that fact that $w_2(S_2)\le 2(m-n)mW$. This proves Claim 4.12. □

As discussed earlier (in Eq. 4.15), Claim 4.12 implies Lemma 4.11. This completes the proof of Lemma 4.11. □

Now, we discuss a lower bound on $\deg_t(\mathcal{D}_w(t,z))$.

Lemma 4.14. *Let $w^*=w^{\max}(\mathcal{M}(U_1)\cap\mathcal{M}(U_2))$ and W be the maximum weight of any element in $[m]$. Then,*

$$\deg_t(\mathcal{D}_w(t,z)) \ge 2rw^* - 12m^3\delta W. \tag{4.19}$$

Proof. For this, we will first show that there exists a subset $S \subset [m^2 r]$ of size mD such that the t-degree of $\det(M(U_1, \overline{U_2}, w)[S])$ is at least $rw^* - 6m^3\delta W$. Let

$$M_1 = M(U_1, \overline{U_2}).$$

We start by constructing another matrix M_2 with full row rank based on matrices U and V and optimal split w_1, w_2 of weight function w. Let us assume that w_1 has ℓ_1 distinct weights $c_1^1 > \cdots > c_{\ell_1}^1$. Let $E_0^1 = \emptyset$ and

$$E_i^1 = \{j \in [m] \mid w_1(j) \geq c_i^1\} \text{ for each } i \in [\ell_1].$$

Let X_i^1 be a subspace of $\mathbb{F}^n$ such that $\mathrm{span}(U_1[E_i^1])$ is direct sum of X_i^1 and $\mathrm{span}(U_1[E_{i-1}^1])$ for each $i \in [\ell_1]$. Let H_1 be the $n \times m$ matrix such that for each $i \in [\ell_1]$ and $j \in E_i^1 \setminus E_{i-1}^1$, its jth column is the X_i^1-component of $U_1[j]$. Similarly, we define H_2 for $\overline{U_2}$. Let us assume that w_2 has ℓ_2 distinct weights $c_1^2 < \cdots < c_{\ell_2}^2$. Let $E_0^2 = \emptyset$ and

$$E_i^2 = \{j \in [m] \mid w_2(j) \leq c_i^2\} \text{ for each } i \in [\ell_2].$$

Let X_i^2 be a subspace of $\mathbb{F}^n$ such that $\mathrm{span}(\overline{U_2}[E_i^2])$ is direct sum of X_i^2 and $\mathrm{span}(\overline{U_2}[E_{i-1}^2])$ for each $i \in [\ell_2]$. Let $\overline{H_2}$ be the $n \times m$ matrix such that for each $i \in [\ell_2]$ and $j \in E_i^2 \setminus E_{i-1}^2$, its jth column is the X_i^2-component of $\overline{U_2}[j]$.

Since w_1, w_2 is an optimal split of w for $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$, from Lemma 4.9, there exists a common base B that maximizes w_1 for $\mathcal{M}(U_1)$ and w_2 for $\mathcal{M}(U_2)$ simultaneously. This implies that $[m] \setminus B$ minimizes w_2 for $\mathcal{M}(\overline{U_2})$. From Lemma 4.6, $[m] \setminus B$ is a base of $\mathcal{M}(\overline{H_2})$. In other words, B is a base of dual of $\mathcal{M}(\overline{H_2})$. Since B is a common base of $\mathcal{M}(H_1)$ and dual of $\mathcal{M}(\overline{H_2})$, from Theorem 4.2, $M(H_1, \overline{H_2})$ has full row rank. Let

$$M_2 = M(H_1, \overline{H_2}).$$

Note that $[m^2 r] \setminus [mr]$ columns of M_2 are independent. Hence, there exists a set $S \subset [m^2 r]$ of size mD such that $([m^2 r] \setminus [mr]) \subset S$ and $M_2[S]$ has full rank. Now, we compute the degree of $\det(M(U_1, \overline{U_2}, w)[S])$. Recall $M_1 = M(U_1, \overline{U_2})$. Let

$$\widehat{w^*} = \widehat{w_1}^{\max}(\mathcal{M}(M_1^{\mathrm{top}})) - \widehat{w_2}^{\min}(\mathcal{M}(M_1^{\mathrm{bot}})) + \widehat{w_2}(S).$$

Let $\mathcal{B}^{\mathrm{top}}$ and $\mathcal{B}^{\mathrm{bot}}$ represent the set of maximum and minimum weight bases of $\mathcal{M}(M_1^{\mathrm{top}})$ and $\mathcal{M}(M_1^{\mathrm{bot}})$ with respect to $\widehat{w_1}$ and $\widehat{w_2}$, respectively. By Laplace Theorem,

$$\det(M(U_1, \overline{U_2}, w)[S]) = \sum_{T \subset S, |T| = nD} \sigma(T) t^{\widehat{w}(T)} \det(M_1^{\mathrm{top}}[T]) \cdot \det(M_1^{\mathrm{bot}}[S \setminus T]),$$

where σ is some sign function on subsets of S. Hence,

$$\begin{aligned}
\deg(\det(M(U_1, \overline{U_2}, w)[S])) &\leq \max_{\substack{T \in \mathcal{M}(M_1^{\mathrm{top}}) \\ S \setminus T \in \mathcal{M}(M_1^{\mathrm{bot}})}} \widehat{w}(T) \\
&= \max_{\substack{T \in \mathcal{M}(M_1^{\mathrm{top}}) \\ S \setminus T \in \mathcal{M}(M_1^{\mathrm{bot}})}} \widehat{w_1}(T) - \widehat{w_2}(S \setminus T) + \widehat{w_2}(S) \qquad \leq \widehat{w^*}.
\end{aligned}$$

Thus, $\deg(\det(M(U_1,\overline{U_2},w)[S])) \le \widehat{w^*}$ and the coefficient of $t^{\widehat{w^*}}$ in $\det(M(U_1,\overline{U_2},w))$ is exactly equal to

$$\sum_{\substack{T\subset S, T\in\mathcal{B}^{\mathrm{top}}\\ S\setminus T\in\mathcal{B}^{\mathrm{bot}}}} \sigma(T)\det({M_1}^{\mathrm{top}}[T])\det({M_1}^{\mathrm{bot}}[S\setminus T]). \tag{4.20}$$

We will show that this is exactly equal to $\det(M_2[S])$ which is non-zero. Let

$$S_1 = [(m+(m-1)n)r]\setminus[mr] \text{ and } S_2 = [m^2r]\setminus[(m+(m-1)n)r]$$

be two sets forming a partition of $[m^2r]\setminus[mr]$. Let T be any subset of $[m^2r]$ in $\mathcal{B}^{\mathrm{top}}$. Since elements in $[m^2r]\setminus[mr]$ have the highest weight with respect to $\widehat{w_1}$ and the columns in S_1 are exactly the non-zero columns in $[m^2r]\setminus[mr]$ which are also independent, we have

$$T\cap([m^2r]\setminus[mr]) = S_1.$$

Similarly, we can argue that for any subset T of $[m^2r]$ in $\mathcal{B}^{\mathrm{bot}}$, we have

$$T\cap([m^2r]\setminus[mr]) = S_2.$$

By Laplace Theorem,

$$\begin{aligned}\det(M_2[S]) &= \sum_{|T|=nD,\ T\subset S} \sigma(T)\det(M_2^{\mathrm{top}}[T])\det(M_2^{\mathrm{bot}}[S\setminus T])\\ &= \sum_{\substack{|T|=nD,\ T\subset S,\\ S_1\subset T,\ S_2\subset S\setminus T}} \sigma(T)\det(M_2^{\mathrm{top}}[T])\det(M_2^{\mathrm{bot}}[S\setminus T]), \end{aligned} \tag{4.21}$$

where the last equality follows from the fact that for a subset T of S with either $S_1\not\subset T$ or $S_2\not\subset(S\setminus T)$,

$$\det(M_2^{\mathrm{top}}[T])\det(M_2^{\mathrm{bot}}[S\setminus T]) = 0$$

as in this case, either $M_2^{\mathrm{top}}[T]$ or $M_2^{\mathrm{bot}}[S\setminus T]$ has a zero column.

Now we show the following claim, which, combined with the above discussion directly implies that the coefficient of $t^{\widehat{w^*}}$ in $\det(M(U_1,\overline{U_2},w)[S])$ (Eq. 4.20) and $\det(M_2[S])$ (Eq. 4.21) are the same.

Claim 4.15. *Let T be a subset of $[m^2r]$.*

1. *If T has size nD and $S_1\subset T$, then*

$$\det(M_2^{\mathrm{top}}[T]) = \det(M_1^{\mathrm{top}}[T]) \textit{ if } T\in\mathcal{B}^{\mathrm{top}},\ \textit{otherwise } 0.$$

2. *If T has size $(m-n)D$ and $S_2\subset T$, then*

$$\det(M_2^{\mathrm{bot}}[T]) = \det(M_1^{\mathrm{bot}}[T]) \textit{ if } T\in\mathcal{B}^{\mathrm{bot}},\ \textit{otherwise } 0.$$

Proof. We just show the first part of the claim here. The second part can be shown similarly.

We start by constructing another $nD \times [m^2r]$ matrix M such that for a subset T of $[m^2r]$ of size nD, $\det(M[T]) = \det(M_1[T])$ if $T \in \mathcal{B}^{\mathrm{top}}$, otherwise zero. Let

$$\widehat{E}_{-1} = \emptyset, \widehat{E_0} = [m^2r] \setminus [mr] \text{ and } \widehat{E}_i = \widehat{E}_0 \cup \{(j-1)r + q \mid j \in E_i^1, q \in [r]\}\ \forall i \in [\ell_1].$$

Note that for each $i \in [\ell_1]$ and the $(i+1)$th largest weight of $\widehat{w_1}$, which is c_i^1, we have

$$\widehat{E}_i = \{j \in [m^2r] \mid \widehat{w_1}(j) \geq c_i^1\}. \tag{4.22}$$

Let V^{top} be an $D \times (m-1)r$ matrix defined as

$$V^{\mathrm{top}} = \begin{pmatrix} V(\alpha_{m+1}) & V(\alpha_{m+2}) & \cdots & V(\alpha_{2m-1}) \end{pmatrix}.$$

Let Y, Z be subspaces of $\mathbb{F}^D$ such that $Y = \mathrm{span}(V^{\mathrm{top}})$ and $\mathbb{F}^D = Y \oplus Z$. Let $\widehat{X}_0 = \mathrm{span}(I_n \otimes V^{\mathrm{top}})$. For $i \in [\ell_1]$, let

$$\widehat{X}_i = \mathrm{span}\left(\{a \otimes b \mid a \in \mathrm{span}(H_1[E_i^1 \setminus E_{i-1}^1]), b \in Z\}\right).$$

Next, we show that for each $0 \leq i \leq \ell_1$, $\mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_i])$ is a direct sum of $\widehat{X}_i$ and $\mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_{i-1}])$. It is trivially true for $i = 0$. First, we show that $\widehat{X}_i$ and $M_1^{\mathrm{top}}[\widehat{E}_{i-1}]$ completely spans $M_1^{\mathrm{top}}[\widehat{E}_i]$. It is equivalent to showing that for each $j \in E_i^1 \setminus E_{i-1}^1$, $q \in [r]$, we have $u_j \otimes V(\alpha_j)[q] \in \widehat{X}_i + \mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_{i-1}])$. From construction of H_1, we have $u_j = H_1[j] + u$ for some $u \in \mathrm{span}(U_1[E_{i-1}^1])$. Also, $V(\alpha_j) = a + b$ for some $a \in Y$ and $b \in Z$. Hence,

$$u_j \otimes V(\alpha_j)[q] = u_j \otimes a + H_1[j] \otimes b + u \otimes b.$$

Clearly $u_j \otimes a \in \widehat{X}_0$, $H_1[j] \otimes b \in \widehat{X}_i$. For any $k \in [m]$, consider $D \times mr$ matrix $(V(\alpha_k)\ \ V^{\mathrm{top}})$. It is a Vandermonde matrix with mr columns which is greater than D. Hence, this matrix spans $\mathbb{F}^D$ which in turn implies that

$$u_k \otimes b \in \mathrm{span}(u_k \otimes V^{\mathrm{top}}) + \mathrm{span}(u_k \otimes V(\alpha_k)).$$

Since $u \in \mathrm{span}(U_1[E_{i-1}^1])$, we get $u \otimes b \in \mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_{i-1}])$. Note that the above discussion also shows that if $\widehat{X}_i \cap \mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_{i-1}]) = \{0\}$, then

$$\widehat{X}_i\text{-component of } M_1^{\mathrm{top}}[(j-1)r + q] = H_1[j] \otimes b = H_1[j] \otimes Z\text{-component of } V(\alpha_j)[q]. \tag{4.23}$$

It also implies the following observation.

Observation 4.16. *For each $i \in [\ell_1]$, $\mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_i]) = \sum_{k=0}^{i} \widehat{X}_i$*

Next, we show that $\widehat{X}_i \cap \mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_{i-1}]) = \{0\}$ for each $i \in [\ell_1]$, which implies (4.23) as discussed above. Suppose, this is not true. Using Observation 4.16, this implies that

$$\exists\ \widehat{a} \neq 0 \in \widehat{X}_i,\ \widehat{b} \in \sum_{k=1}^{i-1} \widehat{X}_k \text{ and } \widehat{c} \in \widehat{X}_0 \text{ such that } \widehat{a} = \widehat{b} + \widehat{c}.$$

Since

$$\sum_{k=1}^{i-1} \widehat{X}_k = \mathrm{span}(\{a \otimes b) \mid a \in \mathrm{span}(H_1[E_{i-1}^1]), b \in Z\}) \ \&\ \mathrm{span}(H_1[E_i^1 \setminus E_{i-1}^1]) \cap \mathrm{span}(H_1[E_{i-1}^1]) = \{0\},$$

we have

$$\widehat{a} - \widehat{b} = p \otimes q \neq 0 \text{ where } p \in \mathbb{F}^n, q \in Z.$$

Since $\widehat{c} = p' \otimes q'$ for some $p' \in \mathbb{F}^n, q' \in Y$ and $Y \cap Z = \{0\}$, we get that $\widehat{a} - \widehat{b} = \widehat{c}$ is a contradiction. This completes the proof of

$$\mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_i]) = \widehat{X}_i \oplus \mathrm{span}(M_1^{\mathrm{top}}[\widehat{E}_{i-1}]) \ \forall\ 0 \leq i \leq \ell_1. \tag{4.24}$$

Let M be the $nD \times m^2 r$ matrix such that for each $0 \leq i \leq \ell_1,\ j \in \widehat{E}_i \setminus \widehat{E}_{i-1}$, its jth column is the $\widehat{X}_i$-component of $M_1^{\mathrm{top}}[j]$ for each $j \in [m^2 r]$. From (4.24, 4.22) and Lemma 4.4, we get that for a subset T of $[m^2 r]$ of size nD,

$$\det(M[T]) = \det(M_1^{\mathrm{top}}[T]) \text{ if } T \in \mathcal{B}^{\mathrm{top}}, \text{ otherwise } 0. \tag{4.25}$$

Let T be any subset of size nD such that $S_1 \subset T$. From construction of M, note that the columns in $[m^2 r] \setminus [mr]$ are same for M, M_1^{top} and M_2^{top}. Next, we show that the columns in $[mr]$ of $M_2^{\mathrm{top}} - M$ belongs to $\widehat{X}_0 = \mathrm{span}(M[S_1])$. Let $i \in [\ell_1]$, $j \in E_i^1 \setminus E_{i-1}^1$ and $q \in r$. Then,

$$\begin{aligned}
(M_2^{\mathrm{top}} - M)[(j-1)r + q] &= H_1[j] \otimes V(\alpha_j)[q] - \widehat{X}_i\text{-component of } M_1^{\mathrm{top}}[(j-1)r + q] \\
&= H_1[j] \otimes V(\alpha_j)[q] - H_1[j] \otimes Z\text{-component of } V(\alpha_j)[q] \\
&= H_1[j] \otimes Y\text{-component of } V(\alpha_j)[q],
\end{aligned}$$

where the second equality follows from (4.23). Hence, $(M_2^{\mathrm{top}} - M)[(j-1)r + q] \in \mathrm{span}(M[S_1])$. This implies that any column of M in $[mr]$ can be converted to the corresponding column of M_2^{top} by adding appropriate multiples of columns in $M[S_1]$ to it. Since these column operations preserve determinant, we have

$$\det(M[T]) = \det(M_2^{\mathrm{top}}[T]) \text{ if } S_1 \subset T. \tag{4.26}$$

Thus, the first part of the Claim 4.15 directly follows from (4.25) and (4.26). The second part follows by a similar line of argument. $\square$

Hence, $\deg_t(\det(M(U_1, \overline{U_2}, w)[S])) = \widehat{w^*}$. Next, we give a lower bound on $\widehat{w^*}$. Using arguments similar to prove Claim 4.12, we can show the following claim.

Claim 4.17.

$$\begin{aligned}
&\widehat{w_1}^{\max}(\mathcal{M}(M(U_1, \overline{U_2})^{\mathrm{top}})) \geq r{w_1}^{\max}(\mathcal{M}(U_1)) - 4m^3\delta W, \\
&\widehat{w_2}^{\min}(\mathcal{M}(M(U_1, \overline{U_2})^{\mathrm{bot}})) \leq r{w_2}^{\min}(\mathcal{M}(\overline{U_2}))).
\end{aligned}$$

For each $e \in [m^2 r]$, we have $\widehat{w_2}(e) \leq 2mW$ and since $m^2 r - |S| = m^2\delta$, we get that

$$\widehat{w_2}(S) = \widehat{w_2}([m^2 r]) - \widehat{w_2}([m^2 r] - S) \geq r w_2([m]) - 2m^3\delta W.$$

Hence,

$$\begin{aligned}
2\widehat{w^*} &= 2(\widehat{w_1}^{\max}(\mathcal{M}(M_1^{\mathrm{top}})) - \widehat{w_2}^{\min}(\mathcal{M}(M_1^{\mathrm{bot}})) + \widehat{w_2}(S)) \\
&\geq 2(r{w_1}^{\max}(\mathcal{M}(U_1)) - 4m^3\delta W - r{w_2}^{\min}(\mathcal{M}(\overline{U_2})) + r w_2([m]) - 2m^3\delta W)) \\
&= 2r({w_1}^{\max}(\mathcal{M}(U_1)) - {w_2}^{\min}(\mathcal{M}(\overline{U_2})) + w_2([m])) - 12m^3\delta W \\
&= 2rw^* - 12m^3\delta W,
\end{aligned} \tag{4.27}$$

where the last equality follows from the fact that w_1, w_2 is an optimal split of w for $\mathcal{M}(U_1)$ and $\mathcal{M}(U_2)$, and $\mathcal{M}(\overline{U_2})$ is dual matroid of $\mathcal{M}(U_2)$.

Now, we relate $\deg_t(\mathcal{D}_w(t,z))$ with $\widehat{w^*}$. Let

$$d = \max_{B \in \binom{[m^2r]}{mD}} \deg_t(\det(M(U_1, \overline{U_2}, w)[B])) \;\&\; \mathcal{F} = \left\{ B \in \binom{[m^2r]}{mD} \,\middle|\, \deg_t(\det(M(U_1, \overline{U_2}, w)[B])) = d \right\}.$$

Here we Next, we argue that $\deg_t(\mathcal{D}_w(t,z)) = 2d$. From Lemma 4.7, $\mathcal{F}$ is the set of bases of some matroid on $[m^2r]$. Consider weight function f on $\mathcal{F}$. Since weights in f are all distinct, there exists a unique maximum weight set B^* in $\mathcal{F}$. This in turn implies that B^* is the only subset of $[m^2r]$ of size mD which contributes to the monomial $t^{2d} z^{f(B^*)}$ in

$$\mathcal{D}_w(t,z) = \sum_{\substack{S \subseteq [m^2r] \\ |S| = mD}} z^{f(S)} (M(U_1, \overline{U_2}, w)[S])^2.$$

Hence, this term does not get cancelled out in $\mathcal{D}_w(t,z)$, and combining this with (4.27), we get

$$\deg_t(\mathcal{D}_w(t,z)) = 2d \geq 2\widehat{w^*} \geq 2rw^* - 12m^3\delta W.$$

$\square$

Next, we use these bounds to get an algorithm for finding the maximum weight of a common base. Since we chose $r > 12m^3\delta W$, by Lemmas 4.11 and 4.14, we get

$$\left| \frac{\deg(\mathcal{D}_w(t,z))}{2r} - w^* \right| < \frac{1}{2}.$$

Therefore, we have

$$w^* = \text{ closest integer to } \frac{\deg_t(\mathcal{D}_w(t,z))}{2r}.$$

This gives us an NC^2 algorithm to compute the maximum weight of a common base of two linear matroids. Hence, from Theorem 4.1, we get the main result of this section.

Theorem 4.18. *A maximum weight common base of two linear matroids with polynomially bounded weights can be computed in* NC^3.

Clearly, this works as well in the unweighted case.

Corollary 4.19. *A common base of two linear matroids can be computed in* NC^3.

5 Non-commutative rank in NC

In this section, we prove Theorem 1.5. That is, given $n \times n$ matrices $A_1, \ldots, A_m$, we design an NC-algorithm to decide whether the symbolic matrix $\sum_{i=1}^m A_i x_i$ has full nc-rank. First, we will use a reduction from [Hir19, Appendix A.1] that reduces nc-rank computation for the general case to a symbolic matrix in a special block form.

Lemma 5.1 ([Hir19, Appendix A.1]). *For any given $n \times n$ matrices $A_1, A_2, \ldots, A_m$, the matrix $\sum_{i=1}^m A_i x_i$ has full non-commutative rank if and only if the following symbolic matrix does*

$$\begin{pmatrix} A_1\, x_{1,1} & I_n\, x_{1,2} & 0 & \cdots & 0 \\ A_2\, x_{2,1} & I_n\, x_{2,2} & I_n\, x_{2,3} & \cdots & 0 \\ A_3\, x_{3,1} & 0 & I_n\, x_{3,3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{m-1}\, x_{m-1,1} & 0 & \cdots & I_n\, x_{m-1,m-1} & I_n\, x_{m-1,m} \\ A_m\, x_{m,1} & 0 & \cdots & 0 & I_n\, x_{m,m} \end{pmatrix},$$

where I_n is the $n \times n$ identity matrix.

Thus, it suffices to test the non-commutative rank of an $mn \times mn$ symbolic matrix of the form

$$\mathcal{A} = (A_{i,j} x_{i,j})_{1 \le i,j \le m},$$

for $n \times n$ matrices $A_{i,j}$. That is, $\mathcal{A}$ has $m \times m$ blocks, where each block has size $n \times n$. Following the construction from bipartite matching, our goal is to construct an *nc-rank-certificate* matrix $N(\mathcal{A})$ such that it has full row rank if and only if $\mathcal{A}$ has full non-commutative rank.

First, we add additional columns to extend $\mathcal{A}$ to an $mn \times (nm)^2$ symbolic matrix $\widehat{\mathcal{A}}$. Define the $mn \times mn(mn-1)$ extension matrix $\mathcal{A}_0$ as

$$\mathcal{A}_0 = \begin{pmatrix} I_n\, z_{1,1} \cdots I_n\, z_{1,mn-1} & & & \\ & I_n\, z_{2,1} \cdots I_n\, z_{2,mn-1} & & \text{\Large 0} \\ \text{\Large 0} & & \ddots & \\ & & & I_n\, z_{m,1} \cdots I_n\, z_{m,mn-1} \end{pmatrix},$$

where $z'_{i,j}s$ are variables. Now the $mn \times (mn)^2$ extension $\widehat{\mathcal{A}}$ of $\mathcal{A}$ is defined as

$$\widehat{\mathcal{A}} = \begin{pmatrix} \mathcal{A} \; \mathcal{A}_0 \end{pmatrix}.$$

That is, $\widehat{\mathcal{A}}$ has $m \times nm^2$ blocks, where each block has size $n \times n$.

We construct the *nc-rank-certificate* matrix $N(\mathcal{A})$ from $\widehat{\mathcal{A}}$ by evaluating $\widehat{\mathcal{A}}$ on $D \times r$ folded Vandermonde matrices, for parameters D, r specified below.

Let $\gamma \in \mathbb{F}$ be an element of order $\ge nmr$. We choose $\alpha_1, \alpha_2, \ldots, \alpha_{nm^2} \in \mathbb{F}$, i.e. one value for every block-column of $\widehat{\mathcal{A}}$, such that the set

$$\{\, \alpha_j \gamma^\ell \mid 1 \le j \le nm^2,\ 0 \le \ell \le r-1 \,\}$$

has $nm^2 r$ distinct elements. Hence, $\mathbb{F}$ should be a field of size $\ge nm^2 r$.

Now define $N(\mathcal{A})$ as an evaluation of $\widehat{\mathcal{A}}$ where we substitute each variable in block-column j of $\widehat{\mathcal{A}}$ by the $D \times r$ γ-folded Vandermonde matrix $V(\alpha_j)$, for $j = 1, 2, \ldots, nm^2$, and each 0 by a $D \times r$ zero-matrix. More precisely, the nc-rank-certificate matrix $N(\mathcal{A})$ has $m \times nm^2$ blocks of size $nD \times nr$ such that For $1 \le i \le m$ and $1 \le j \le nm^2$,

$$\text{the } (i,j)\text{-th block of } N(\mathcal{A}) = \begin{cases} A_{i,j} \otimes V(\alpha_j) & \text{if } j \le m \\ I_{n\times n} \otimes V(\alpha_j) & \text{if } (nm-1)(i-1)+m < j \le (nm-1)i+m \\ 0 & \text{otherwise.} \end{cases}$$

Matrix $N(\mathcal{A})$ would be square if we would choose $D = nmr$. However, we need $N(\mathcal{A})$ to be rectangular with slightly fewer rows. Hence, we have a further parameter δ and we let

$$D = nm(r - \delta). \tag{5.1}$$

We will see below that our arguments work when we choose the parameters such that

$$\delta \geq mn \quad \text{and} \quad r > m^2 n^2 \delta. \tag{5.2}$$

Hence $\delta = mn$ and $r = m^3 n^3 + 1$ is a valid choice.

We show that the row rank of $N(\mathcal{A})$ determines whether $\mathcal{A}$ has full non-commutative rank. For this, we will need the following generalization of Hall's Theorem that gives a certificate for a symbolic matrix not having full non-commutative rank (see [GGdOW20, Theorem 1.4]).

Theorem 5.2 ([GGdOW20], [FR04])**.** *Given $n \times n$ matrices $A_1, \dots, A_m$ over $\mathbb{F}$, consider the symbolic matrix $\mathcal{A} = \sum_i A_i x_i$. $\mathcal{A}$ is not of full non-commutative rank if and only if there exist non-singular matrices B, C over $\mathbb{F}$ such that the symbolic matrix $B\mathcal{A}C$ has a $s \times t$ block of zeros, where $s + t > n$.*

Now, we prove the main theorem of this section.

Theorem 5.3. *Given $n \times n$ matrices $A_{i,j}$, for $i, j \in [m]$, define the $mn \times mn$ symbolic matrix $\mathcal{A}$ by*

$$\mathcal{A} = (A_{i,j} x_{i,j})_{i,j}.$$

Then

$$\mathcal{A} \text{ has full nc-rank} \iff N(\mathcal{A}) \text{ has full rank.}$$

Proof. For one direction, we show that if $\mathcal{A}$ does not have full non-commutative rank then $N(\mathcal{A})$ does not have full row rank. From the characterization of nc-rank (Theorem 5.2), there are two $mn \times mn$ non-singular matrices B and C over $\mathbb{F}$ such that $B\mathcal{A}C$ has an all zero submatrix of size $a \times b$ where $a + b \geq mn + 1$. Since B is non-singular, there must exist a partition, $S_1, S_2, \dots, S_m$ of $[mn]$ with each part of size n such that for each $i \in [m]$, the $n \times n$ sub-matrix with rows from S_i and columns from $(i-1)n + 1$ to in is non-singular. Let $\tilde{B}$ be the $mn \times mn$ non-singular block-diagonal matrix with these m submatrices as blocks. As $\mathcal{A}$ has the block structure with one variable appearing in exactly one block, we can substitute B with $\tilde{B}$ such that $\tilde{B}\mathcal{A}C$ has a zero submatrix of size $a \times b$ where $a + b \geq mn + 1$. Similarly, we can substitute C with a block diagonal matrix. Hence, we can assume, without loss of generality, that B and C are block diagonal with $n \times n$ matrices as blocks, say $B_1, B_2, \dots, B_m$ and $C_1, C_2, \dots, C_m$. Let us define

$$B' = B \otimes I_D$$

and

$$C' = \begin{pmatrix} C & 0 & 0 & \cdots & 0 \\ 0 & I_{mn-1} \otimes B_1^{-1} & 0 & \cdots & 0 \\ 0 & 0 & I_{mn-1} \otimes B_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & I_{mn-1} \otimes B_m^{-1} \end{pmatrix} \otimes I_r.$$

Clearly, B', C' are non-singular. Consider $B'N(\mathcal{A})C'$. It will have a block of zeros of size $aD \times br$ in the first mnr columns. Among the last $(mn-1)mnr$ columns, these aD rows will have at most $a(mn-1)r$ nonzero columns. Thus, we get a zero block of size

$$(amn(r-\delta)) \times (br + (mn-1)mnr - a(mn-1)r).$$

Adding the two dimensions,

$$\begin{aligned} a(mn(r-\delta)) + br + (mn-1)mnr - a(mn-1)r &= m^2n^2r - mnr + ar + br + a - amn\delta \\ &\geq m^2n^2r + r - amn\delta. \end{aligned}$$

The last inequality is because $a + b \geq mn + 1$. As $a < mn$ and $r > m^2n^2\delta$, we get a block of zeros whose sum of dimensions is larger than the number of columns, i.e., m^2n^2r. Thus the matrix $N(\mathcal{A})$ cannot have full row rank.

To prove the other direction, we show that if $\mathcal{A}$ is of full non-commutative rank then the nc-rank-certificate matrix $N(\mathcal{A})$ has full row rank.

For the sake of contradiction, assume that $N(\mathcal{A}) = (N_0 \ \ N_1)$ does not have full row rank where N_0 contains the first mnr columns (i.e. the evaluation of the symbolic matrix $\mathcal{A}$) and N_1 contains the remaining columns. Then there is a vector $p \in \mathbb{F}^{nmD}$ representing a linear dependency among the rows of $N(\mathcal{A})$, i.e.

$$p^T N(\mathcal{A}) = 0 \qquad \text{i.e.} \quad p^T(N_0 \ \ N_1) = 0. \tag{5.3}$$

Let us split p into blocks as

$$p = (p_{1,1}, \ldots, p_{1,n}, p_{2,1}, \ldots, p_{2,n}, \ldots, p_{m,1}, \ldots, p_{m,n}),$$

where each $p_{i,k} \in \mathbb{F}^D$. Some of the $p_{i,j}$'s may have dependency. For $1 \leq i \leq m$, Let d_i be the dimension of the span$\{p_{i,1}, \ldots, p_{i,n}\}$. Define $\Delta := \sum_{i=1}^m d_i$.

Let us view each $p_{i,k}$ as the coefficient vector of a polynomial $p_{i,k}(x)$ of degree $D-1$. Let $\mathcal{P} = \text{span}\{p_{i,k}(x)\}_{i,k}$. Equation (5.3) gives us roots of the $p_{i,k}$'s:

- As $p^T \cdot N_1 = 0$, we get for each $1 \leq i \leq m$, $m + (i-1)(nm-1) + 1 \leq j \leq m + i(nm-1)$ and $1 \leq k \leq n$,

  $$p_{i,k}^T V(\alpha_j) = 0,$$

  i.e., polynomial $p_{i,k}(x)$ has α_j as an r-folded root. That means, for each $1 \leq i \leq m$ and $m + (i-1)(nm-1) + 1 \leq j \leq m + i(nm-1)$, we have

  $$Z_r(\mathcal{P}, \alpha_j) \geq d_i.$$

  From this, we get

  $$\sum_{j=m+1}^{nm^2} Z_r(\mathcal{P}, \alpha_j) \geq (nm-1)\sum_{i=1}^{m} d_i = (nm-1)\Delta. \tag{5.4}$$

- Moreover, $p^T N_0 = 0$, which implies $\sum_{i,k} p_{i,k} A_{i,j}(k,\ell) V(\alpha_j) = 0$, for each $1 \leq j \leq m$ and $1 \leq \ell \leq n$. Therefore, for each $1 \leq j \leq m$ and $1 \leq \ell \leq n$, the polynomial $\sum_{i,k} A_{i,j}(k,\ell) p_{i,k}(x)$ has α_j as an r-folded root. That means, for each $1 \leq j \leq m$

  $$Z_r(\mathcal{P}, \alpha_j) \geq \dim \left\{ \sum_{i,k} A_{i,j}(k,\ell) p_{i,k}(x) : 1 \leq \ell \leq n \right\}. \tag{5.5}$$

Now we prove that $\text{span}\{p_{1,k}\}_k + \cdots + \text{span}\{p_{m,k}\}_k$ is a direct sum. Let $\mathcal{P} = \text{span}\{p_{i,k}(x)\}_{i,k}$ have dimension q. We need to prove $q = \Delta$. First, observe that from Lemma 2.6, we have

$$\sum_{j=1}^{nm^2} Z_r(\mathcal{P}, \alpha_j) \leq \frac{q(D-1)}{r-q+1} < qmn \left(\frac{r-\delta}{r-q+1}\right) < qmn. \tag{5.6}$$

The last inequality is because $\delta \geq mn \geq q$.

Claim 5.4.

$$\dim(\mathcal{P}) = \Delta.$$

Proof. Combining (5.6) with (5.4), we get $qnm > (nm-1)\Delta$. We can write

$$q > \Delta(nm-1)/nm = \Delta - \Delta/nm \geq \Delta - 1.$$

This means $q \geq \Delta$, which proves the claim. □

Now, we know that $\mathcal{P}$ has dimension $q = \Delta$. Let us lower bound the sum $\sum_{j=1}^{m} Z_r(\mathcal{P}, \alpha_j)$. From (5.5), we get $\sum_{j=1}^{m} Z_r(\mathcal{P}, \alpha_j) \geq L$, where

$$L = \sum_{j=1}^{m} \dim \left\{ \sum_{i,k} A_{i,j}(k,\ell) p_{i,k}(x) : 1 \leq \ell \leq n \right\}.$$

This is the same as

$$\sum_{j=1}^{m} \text{rank} \left(\sum_{i=1}^{m} P_i A_{i,j} \right), \tag{5.7}$$

where P_i is the matrix with coefficient vectors of $p_{i,1}, p_{i,2}, \ldots, p_{i,n}$ as columns.

Now, we prove a lower bound on this number. Let U be a block-diagonal matrix with $P_1, P_2, \ldots, P_m$ as the blocks on the diagonal. Note that $\text{rank}(U) = \Delta$. Let A_j be an $mn \times n$ matrix whose i-th block is $A_{i,j}$.

Claim 5.5. $\text{rank}(\sum_{i=1}^{m} P_i A_{i,j}) = \text{rank}(UA_j)$.

Proof. Clearly any vector in $\ker(UA_j)$ is also in $\ker(\sum_{i=1}^{m} P_i A_{i,j})$. We now argue the other way. Let $\sum_{i=1}^{m} P_i A_{i,j}\, x = 0$, for some $x \in \mathbb{F}^n$. This gives us $p_1 + p_2 + \cdots + p_m = 0$ for some $p_i \in \text{colspan}(P_i)$. But, using Claim 5.4, it must be that $p_1 = p_2 = \cdots = p_m = 0$. Thus, we get that x is in the kernel of $P_i A_{i,j}$ for each $1 \leq i \leq m$. □

Now, observe that the quantity in (5.7) is equal to $\sum_{j=1}^{m} \text{rank}(UA_j)$. Let us define $\widetilde{A}_{i,j}$ as an $m \times m$ block matrix with (i,j) block as $A_{i,j}$ and other blocks as 0. $\sum_{j=1}^{m} \text{rank}(UA_j)$ is nothing but the dimension of the image of $\text{rowspan}(U)$ under the matrices $\{\widetilde{A}_{i,j}^T\}_{i,j}$.

If $\mathcal{A}$ has full nc-rank, then clearly $\mathcal{A}^T$ (the transpose of $\mathcal{A}$) also has full nc-rank. From shrunk-subspace criterion (Definition 1.3), if $\mathcal{A}^T$ has full nc-rank, then the dimension of any subspace would not shrink under the matrices $\{\widetilde{A}_{i,j}^T\}_{i,j}$. In particular, the dimension of the image of $\text{colspan}(U^T)$

under the matrices $\{\widetilde{A}_{i,j}^T\}_{i,j}$ must be at least $\mathrm{rank}(U) = \Delta$, and $\sum_{j=1}^m \mathrm{rank}(UA_j) = L \geq \Delta$. Thus, we get

$$\sum_{j=1}^{m} Z_r(\mathcal{P}, \alpha_j) \geq L \geq \Delta. \tag{5.8}$$

.

Combining (5.4) and (5.8), we have

$$\sum_{j=1}^{nm^2} Z_r(\mathcal{P}, \alpha_j) \geq nm\Delta.$$

This together with (5.6) gives a contradiction, as $q = \Delta$. □

Given a symbolic matrix $\sum_{i=1}^m A_i x_i$, we can construct the nc-rank-certificate matrix $N(\mathcal{A})$ from the description of the corresponding block-symbolic matrix $\mathcal{A} = (A_{i,j}x_{i,j})_{i,j}$ (as described in Lemma 5.1) in NC. Also the rank of a matrix can be computed in NC. Therefore, we get the main result of this section.

Corollary 5.6. *Deciding if a symbolic matrix $\sum_{i=1}^m A_i x_i$ is of full nc-rank is in NC^2.*

Acknowledgments

We thank Amit Kumar Sinhababu for pointing us to Algorithm 1 in [BCDZ26]. We thank Mrinal Kumar for helpful discussions on coding theory and helping with improving the presentation. We thank Youming Qiao for pointing out a mistake in the proof of Theorem 5.3.

S.G. thanks the funding support from ANRF (ANRF/ARGM/2025/000718/MTR). T.T. is supported by DFG grant TH 472/5-2.

Acknowledgment of the use of AI (specifically, Google's Gemini Pro 3.1 model): Our initial NC-algorithm (Appendix A) for the decision version of bipartite matching was derived from a reduction from bipartite matching to a specific submodular minimization problem on a lattice of vector spaces. We provided this reduction to the model encoded in the language of linear matroid intersection (LMI) and asked it to extend it to LMI. The model successfully produced such an extension. Inspired by this extension, we designed an alternative algorithm for bipartite matching decision (Section 3.1), which we subsequently generalized to broader settings (Sections 3.2, 4, 5).

References

[ACM24] Vikraman Arvind, Abhranil Chatterjee, and Partha Mukhopadhyay. Trading determinism for noncommutativity in Edmonds' problem. In *65th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 539–559. IEEE, 2024.

[AHT07] 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, 2007.

[AV20] Nima Anari and Vijay V. Vazirani. Planar graph perfect matching is in NC. *Journal of the ACM*, 67(4), 2020.

[BCDZ26] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. From random to explicit via subspace designs with applications to local properties and matroids. In *58th ACM Symposium on Theory of Computing (STOC)*, pages 619–630. ACM, 2026.

[BEG24] Sujoy Bhore, Sarfaraz Equbal, and Rohit Gurjar. Parallel Complexity of Geometric Bipartite Matching. In *44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, volume 323 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 12:1–12:15. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024.

[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.

[BGM23] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic Reed-Solomon codes achieve list-decoding capacity. In *55th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1488–1501. ACM, 2023.

[Csa76] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976.

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized singleton bounds. In *57th ACM Symposium on Theory of Computing (STOC)*, pages 1–12. ACM, 2025.

[DK98] Elias Dahlhaus and Marek Karpinski. Matching and multidimensional matching in chordal and strongly chordal graphs. *Discrete Applied Mathematics*, 84(1–3):79 – 91, 1998.

[DKR10] Samir Datta, Raghav Kulkarni, and Sambuddha Roy. Deterministically isolating a perfect matching in bipartite planar graphs. *Theory of Computing Systems*, 47:737–757, 2010.

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

[DNS81] Eliezer Dekel, David Nassimi, and Sartaj Sahni. Parallel matrix and graph algorithms. *SIAM Journal on Computing*, 10(4):657–675, 1981.

[DSY08] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. In *14th ACM Symposium on Theory of Computing (STOC)*, page 741–748. ACM, 2008.

[DSY14] Son Hoang Dau, Wentu Song, and Chau Yuen. On the existence of MDS codes over small fields with constrained generator matrices. In *IEEE International Symposium on Information Theory*, pages 1787–1791, 2014.

[DW92] Andreas W.M Dress and Walter Wenzel. Valuated matroids. *Advances in Mathematics*, 93(2):214–250, 1992.

[Edm67] Jack Edmonds. Systems of distinct representatives and linear algebra. *Journal of Research of the National Bureau of Standards Section B Mathematics and Mathematical Physics*, page 241, 1967.

[Edm70] Jack Edmonds. Submodular functions, matroids, and certain polyhedra. In Richard Guy, Haim Hanani, Norbert Sauer, and Johanan Schönheim, editors, *Combinatorial Structures and Their Applications*, pages 69–87, New York, 1970. Gordon and Breach.

[FF56] JR L. R. Ford and Delbert Ray Fulkerson. Maximal flow through a network. *Canadian Journal of Mathematics*, 8:399 – 404, 1956.

[FGT19] Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. A deterministic parallel algorithm for bipartite perfect matching. *Commun. ACM*, 62(3):109–115, 2019.

[FGT21] Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite perfect matching is in quasi-NC. *SIAM Journal on Computing*, 50(3), 2021.

[FR04] Marc Fortin and Christophe Reutenauer. Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank. *Séminaire Lotharingien de Combinatoire [electronic only]*, 52, 01 2004.

[Fra81] András Frank. A weighted matroid intersection algorithm. *Journal of Algorithms*, 2(4):328–336, 1981.

[Fra08] András Frank. A quick proof for the matroid intersection weight-splitting theorem. *EGRES Quick-Proofs*, 3, 2008.

[GG17] Shafi Goldwasser and Ofer Grossman. Bipartite perfect matching in pseudo-deterministic NC. In *44th International Colloquium on Automata, Languages, and Programming (ICALP)*, volume 80 of *LIPIcs*, pages 87:1–87:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[GGdOW16] Ankit Garg, Leonid Gurvits, Rafael Mendes de Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 109–117. IEEE Computer Society, 2016.

[GGdOW20] Ankit Garg, Leonid Gurvits, Rafael Mendes de Oliveira, and Avi Wigderson. Operator scaling: Theory and applications. *Foundations of Computational Mathematics*, 20(2):223–290, 2020.

[GGR24] Sumanta Ghosh, Rohit Gurjar, and Roshan Raj. A deterministic parallel reduction from weighted matroid intersection search to decision. *Algorithmica*, 86(4):1057–1079, 2024.

[GHK+17] Parikshit Gopalan, Guangda Hu, Swastik Kopparty, Shubhangi Saraf, Carol Wang, and Sergey Yekhanin. Maximally recoverable codes for grid-like topologies. In *28th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2092–2108. SIAM, 2017.

[GK87] 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.

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016.

[GKMT17] Rohit Gurjar, Arpita Korwar, Jochen Messner, and Thomas Thierauf. Exact perfect matching in complete graphs. *ACM Transations on Compututation Theory*, 9(2):8:1–8:20, 2017.

[GKSS22] Zeyu Guo, Mrinal Kumar, Ramprasad Saptharishi, and Noam Solomon. Derandomization from algebraic hardness. *SIAM Journal on Computing*, 51(2):315–335, 2022.

[GOR24] Rohit Gurjar, Taihei Oki, and Roshan Raj. Fractional linear matroid matching is in quasi-nc. In Timothy M. Chan, Johannes Fischer, John Iacono, and Grzegorz Herman, editors, *32nd Annual European Symposium on Algorithms, ESA 2024, Royal Holloway, London, United Kingdom, September 2-4, 2024*, volume 308 of *LIPIcs*, pages 63:1–63:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[GPV88] A. V. Goldberg, S. A. Plotkin, and P. M. Vaidya. Sublinear-time parallel algorithms for matching and related problems. In *29th Symposium on Foundations of Computer Science (FOCS)*, page 174–185. IEEE, 1988.

[GR08] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions of Information Theory*, 54(1):135–150, 2008.

[GT20] Rohit Gurjar and Thomas Thierauf. Linear matroid intersection is in quasi-NC. *computational complexity*, 29(2):9, 2020.

[GX13] Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the singleton bound. In *45th Symposium on Theory of Computing Conference (STOC)*, pages 843–852. ACM, 2013.

[Har07] Nicholas J. A. Harvey. An algebraic algorithm for weighted linear matroid intersection. In *Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07, page 444–453, USA, 2007. Society for Industrial and Applied Mathematics.

[HH21] Masaki Hamada and Hiroshi Hirai. Computing the nc-rank via discrete convex optimization on cat(0) spaces. *SIAM Journal on Applied Algebra and Geometry*, 5(3):455–478, 2021.

[Hir19] Hiroshi Hirai. Computing the degree of determinants via discrete convex optimization on euclidean buildings. *SIAM Journal on Applied Algebra and Geometry*, 3(3):523–557, 2019.

[HK73] John E. Hopcroft and Richard M. Karp. An $n^{5/2}$ algorithm for maximum matchings in bipartite graphs. *SIAM Journal on Computing*, 2(4):225–231, 1973.

[IQS17] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative Edmonds' problem and matrix semi-invariants. *computational complexity*, 26(3):717–763, 2017.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *computational complexity*, 27(4):561–593, 2018.

[Iri60] Masao Iri. A new method for solving transportation-network problems. *Journal of the Operations Research Society of Japan*, 3:27–87, 1960.

[KR98] Marek Karpinski and Wojciech Rytter. *Fast parallel algorithms for graph matching problems*. Oxford University Press, Inc., USA, 1998.

[Kuh55] H. W. Kuhn. The hungarian method for the assignment problem. *Naval Research Logistics Quarterly*, 2(1-2):83–97, 1955.

[KUW86] Richard M. Karp, Eli Upfal, and Avi Wigderson. Constructing a perfect matching is in random NC. *Combinatorica*, 6(1):35–48, 1986.

[LMS25] Matan Levi, Jonathan Mosheiff, and Nikhil Shagrithaya. Random Reed-Solomon codes and random linear codes are locally equivalent. In *66th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 2097–2131. IEEE, 2025.

[Lov79] László Miklós Lovász. On determinants, matchings, and random algorithms. In *International Symposium on Fundamentals of Computation Theory*, 1979.

[LSW98] Nathan Linial, Alex Samorodnitsky, and Avi Wigderson. A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents. In *13th ACM Symposium on Theory of Computing (STOC)*, page 644–652. ACM, 1998.

[Mur96] Kazuo Murota. Valuated matroid intersection i: Optimality criteria. *SIAM Journal on Discrete Mathematics*, 9(4):545–561, 1996.

[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 Journal on Computing*, 23(2):387–397, 1994.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Science*, 49(2):149–167, 1994.

[Ore22] Øystein Ore. Über höhere Kongruenzen. *Norsk Matematisk Forenings Skrifter*, 1(7):15, 1922.

[PV05] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *46th Symposium on Foundations of Computer Science (FOCS)*, pages 285–294. IEEE Computer Society, 2005.

[San09] Piotr Sankowski. Maximum weight bipartite matching in matrix multiplication time. *Theoretical Computer Science*, 410(44):4480–4488, 2009.

[San18] Piotr Sankowski. NC algorithms for weighted planar perfect matching and related problems. In *45th International Colloquium on Automata, Languages, and Programming (ICALP)*, LIPIcs, pages 97:1–97:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

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

[Sch03a] A. Schrijver. *Combinatorial Optimization - Polyhedra and Efficiency*. Springer, 2003.

[Sch03b] Alexander Schrijver. *Combinatorial optimization : polyhedra and efficiency. Vol. B. , Matroids, trees, stable sets. chapters 39-69*. Algorithms and combinatorics. Springer-Verlag, 2003.

[Sin64] Richard Sinkhorn. A Relationship Between Arbitrary Positive Matrices and Doubly Stochastic Matrices. *The Annals of Mathematical Statistics*, 35(2):876 – 879, 1964.

[Sri25] Shashank Srivastava. Improved list size for folded Reed-Solomon codes. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2040–2050. SIAM, 2025.

[ST17] Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In *58th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 696–707. IEEE Computer Society, 2017.

[ST23] Chong Shangguan and Itzhak Tamo. Generalized singleton bound and list-decoding Reed-Solomon codes beyond the Johnson radius. *SIAM Journal on Computing*, 52(3):684–717, 2023.

[Tut47] William T. Tutte. The factorization of linear graphs. *Journal of The London Mathematical Society-second Series*, pages 107–111, 1947.

[TV12] Raghunath Tewari and N. V. Vinodchandran. Green's theorem and isolation in planar graphs. *Information and Computation*, 215:1–7, 2012.

[Val79] L. G. Valiant. Completeness classes in algebra. In *11th ACM Symposium on Theory of Computing (STOC)*, page 249–261. ACM, 1979.

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

A Bipartite matching via subspace design

In this section, we give an alternative NC-algorithm to decide if a given bipartite graph has a perfect matching, and present it using *subspace designs*. This algorithm and its proof of correctness can also be presented using the folded Vandermonde, like in Section 3.1. Note that in Section 3.1, we reduced bipartite matching to rank computation of a matrix of size $O(n^5)$. Here, we get a smaller matrix of size $O(n^4)$. We start by defining subspace designs and describe an explicit construction.

Definition A.1 (Subspace design [GK16]). *A collection of subspaces $H_1, H_2, \ldots, H_m \subseteq \mathbb{F}^D$ is called a (k, K) subspace design, if for every subspace $W \subseteq \mathbb{F}^D$ of dimension k, we have*

$$\sum_{j=1}^{m} \dim(H_j \cap W) \leq K.$$

Guruswami and Kopparty [GK16] gave an explicit construction of a subspace design.

Theorem A.2 ([GK16, Theorem 7]). *Let $\mathbb{F}$ be field and $r \leq D < |\mathbb{F}|$ and $m < |\mathbb{F}|/r$ be parameters. There exists subspaces $H_1, H_2, \ldots, H_m \in \mathbb{F}^D$, each of co-dimension r, which form a $(k, k(D-1)/(r-k+1))$ subspace design for every $k \leq r$.*

Remark. *Guruswami and Kopparty [GK16, Theorem 7] do not explicitly say that the above collection is a subspace design* for every *$k \leq r$, but it is easy to see that the construction is independent of k.*

Now, we describe their construction and make some observations.

Construction of $(k, k(D-1)/(r-k+1))$ subspace designs [GK16]. Let $\alpha_1, \alpha_2, \ldots, \alpha_m, \gamma \in \mathbb{F}$ be elements such that the set

$$\{\, \alpha_j \gamma^\ell \mid 1 \leq j \leq m,\ 0 \leq \ell \leq r-1 \,\}$$

has mr distinct elements. Moreover let γ have order more than D. For $j \in [m]$, let $H_j \leq \mathbb{F}^D$ be the subspace orthogonal to the columns of the $D \times r$ folded Vandermonde matrix $V(\alpha_j)$ with parameter γ.

Note that for any $S \subseteq [m]$, the columns of $\{V(\alpha_j)\}_{j \in S}$ are linearly independent if $r|S| \leq D$. Thus, we get

$$\forall\, S \subseteq [m] \quad \dim(\cap_{j \in S} H_j) = \max\{0, D - r|S|\}. \tag{A.1}$$

We choose parameters δ and r as follows.

$$\delta \geq n \text{ and } r \geq n^2 \delta,$$

and set $D = n(r - \delta)$.

By our choice of parameters, we get the following corollary to Theorem A.2.

Corollary A.3. *Let $H_1, H_2, \ldots, H_m \leq \mathbb{F}^D$ be a subspace design from Theorem A.2. For every subspace $W \subseteq \mathbb{F}^D$ of dimension at most $k \leq n$, we have*

$$\sum_{j=1}^{m} \dim(H_j \cap W) \leq k \left(\frac{D-1}{r-k+1} \right) < kn \left(\frac{r-\delta}{r-k+1} \right) < kn.$$

Let $G(L \cup R, E)$ be a bipartite graph with $|L| = |R| = n$ and $|E| = m$. Let d_i be the degree of $i \in L$, for $i \in [n]$. We may assume that $d_i \geq 1$, because otherwise G cannot have a perfect matching.

Let A be its $n \times n$ bi-adjacency matrix. We extend A to $\widetilde{A}$ by attaching $m - n$ columns to it. We define the extension matrix A_1 as

$$A_1 = \begin{pmatrix} 00\cdots 0 & & & \\ & 00\cdots 0 & & \mathbf{1} \\ \mathbf{1} & & \ddots & \\ & & & 00\cdots 0 \end{pmatrix}$$

Matrix A_1 has n rows. The 0-block in the i-th row has length $d_i - 1$. Hence, A_1 has $\sum_{i=1}^{n}(d_i - 1) = m - n$ columns. All other entries are 1. Combining A and A_1, we define the $n \times m$ extension matrix $\widetilde{A} = (A \ \ A_1)$. Note that each row of $\widetilde{A}$ has $(n - d_i) + (d_i - 1) = n - 1$ zeros.

For $i \in [n]$, define subspaces Z_i as the intersection of those H_j's for which $\widetilde{A}_{i,j} = 0$. That is,

$$Z_i = \bigcap_{j : \widetilde{A}_{i,j} = 0} H_j.$$

As each row in $\widetilde{A}$ has $n - 1$ zeros, by (A.1), we have for each $i \in [n]$,

$$\dim(Z_i) = D - r(n-1) = r - n\delta. \tag{A.2}$$

Let

$$Z = Z_1 + Z_2 + \cdots + Z_n. \tag{A.3}$$

By (A.2), we have $\dim(Z) \leq n(r - n\delta)$. We show that G has a perfect matching, if and only if Z has full dimension.

Theorem A.4. *Let G be a balanced bipartite graph and Z as defined in (A.3). Then*

$$G \in \mathrm{PM} \iff \dim(Z) = n(r - n\delta).$$

Proof. For the direction from right to left, assume that G does not have a perfect matching. Then there is a Hall block in G. By Corollary 2.2, there are sets $S, T \subseteq [n]$ with $|S| + |T| > n$, such that the bi-adjacency matrix A of G has a zero submatrix $A_{S,T}$. From the definition of Z_i's, it follows that for every $i \in S$, we have $Z_i \subseteq \cap_{j \in T} H_j$. Therefore

$$\bigcup_{i \in S} Z_i \subseteq \bigcap_{j \in T} H_j.$$

Thus, by (A.1),

$$\begin{aligned} \dim(\cup_{i \in S} Z_i) &\leq \dim(\cap_{j \in T} H_j) \\ &= D - r|T| \\ &\leq n(r - \delta) + r|S| - r(n+1) \\ &= r|S| - r - n\delta. \end{aligned}$$

Hence, we get

$$\begin{aligned}
\dim(Z) &\leq \dim(\cup_{i\in S} Z_i) + \sum_{i\in[n]\setminus S} \dim(Z_i) \\
&\leq r|S| - r - n\delta + (n - |S|)(r - n\delta). \\
&= n(r - n\delta) + n|S|\delta - r - n\delta. \\
&< n(r - n\delta).
\end{aligned}$$

The last inequality is using $|S| \leq n$ and $r \geq n^2\delta$.

For the reverse direction, assume that $\dim(Z) < n(r-n\delta)$. Recall that $\sum_i \dim(Z_i) = n(r-n\delta)$. Therefore, we have, $\dim(Z) < \sum_i \dim(Z_i)$. Hence, the map $\phi : Z_1 \times Z_2 \times \cdots \times Z_n \to \sum_i Z_i$ given by $\phi(q_1, q_2, \ldots, q_n) = \sum_i q_i$ has a nontrivial kernel. Without loss of generality, let $q_1 \in Z_1, q_2 \in Z_2, \ldots, q_{k+1} \in Z_{k+1}$ be a minimum size set of vectors such that $q_1 + q_2 + \cdots + q_{k+1} = 0$ for some $k < n$. Define the k-dimensional subspace W as

$$W = \operatorname{span}\{q_1, q_2, \ldots, q_{k+1}\}.$$

Recall that by the definition of Z_i, for every $i \in [n]$ and $j \in [m]$, we have

$$\widetilde{A}_{i,j} = 0 \;\Rightarrow\; q_i \in Z_i \subseteq H_j. \tag{A.4}$$

Let us define $S = [k+1]$ and let $\widetilde{A}_S$ be the first $k+1$ rows of the extension matrix $\widetilde{A}$. For $j \in [m]$, define n_j as the number of 0's in the jth column of $\widetilde{A}_S$,

$$n_j = \{\, i \in S \mid (\widetilde{A}_S)_{i,j} = 0 \,\}.$$

By (A.4), we have that H_j contains n_j vectors from $\{q_1, q_2, \ldots, q_{k+1}\}$. In case that $n_j = k+1$, we have a zero-column in $\widetilde{A}_S$. This can only happen for $j \in [n]$, because in the extension part A_1 there is no column with more than one zero. Define

$$T = \{\, j \in [n] \mid n_j = k+1 \,\}.$$

By definition of n_j and T, we get that $A_{S,T}$ is a zero submatrix in A. We will show that $T \neq \emptyset$ and that it yields a Hall block via Corollary 2.2.

To apply Corollary A.3, we consider $\dim(H_j \cap W)$.

- For $j \in T$, we have $n_j = k+1$. By (A.4), we get that $H_j \cap W = W$, and therefore
$$\dim(H_j \cap W) = \dim(W) = k = n_j - 1.$$
- For $j \notin T$, we have $n_j \leq k$. Because H_j contains n_j of vectors $\{q_i\}$, we have $\dim(H_j \cap W) \geq n_j$.

Combining the two items, we get

$$\begin{aligned}
\sum_{j=1}^{m} \dim(H_j \cap W) &\geq \sum_{j\in T} (n_j - 1) + \sum_{j\in[m]\setminus T} n_j \\
&= \sum_{j\in[m]} n_j - |T| \\
&= (k+1)(n-1) - |T|.
\end{aligned}$$

For the last equation, note that $\sum_{j\in[m]} n_j$ adds *all* zeros in $\widetilde{A}_S$. Since there are $n-1$ zeros in each row, we get $|S|(n-1) = (k+1)(n-1)$ zeros in total.

By Corollary A.3, we conclude that

$$(k+1)(n-1) - |T| < kn.$$

This implies $|S| + |T| = k + 1 + |T| > n$. But recall that $A_{S,T}$ is a zero submatrix of A. By Corollary 2.2, G does not have a perfect matching. $\square$

Size of the matrix. Theorem A.4 reduces the bipartite matching problem to computing the rank of a matrix – which consists of the basis vectors of $Z_1, Z_2, \ldots, Z_n$. As Z_i's are subspaces of $\mathbb{F}^D$ and each of their dimensions is $r - n\delta$. We get that the matrix has size $O(nr) = O(n^4)$.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il