Bipartite Matching is in NC

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

Thomas Thierauf ¶

June 15, 2026

Abstract

We show that the bipartite matching problem is in NC. We extend the result to weighted bipartite matching and the computation of the noncommutative rank of a symbolic matrix. In particular, this implies that the decision version of linear matroid intersection is in NC as well. The techniques are based on the 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.

*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@osu.edu.

¶Ulm University and Aalen University. Email: thomas.thierauf@uni-ulm.de.

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 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.

The algorithm easily generalizes to the weighted case. 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. The degree is not exactly related to the maximum weight, but 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 (also observed in [GG17], see Section 2.4 for more details). 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 Non-commutative rank

In the context of bipartite matching, Edmonds introduced the following problem: let $x_1, x_2, \ldots, x_m$ be variables. Given a set of $n \times n$ matrices $A_1, A_2, \ldots, A_m$ 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 $A_1, A_2, \ldots, A_m$ (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 $\mathrm{rank}(\mathcal{A}_G)$ 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's 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 $\alpha_1, \ldots, \alpha_m$ with $\sum_i A_i \alpha_i$ 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 so called *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, like the "shrunk subset" of Hall's theorem.

Definition 1.2. *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 1.3. *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 [?, 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

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

This can be shown by using a Hall's 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].

Despite the existence of multiple polynomial-time algorithms, no NC-algorithm is known for computing nc-rank. The crucial ingredient of our bipartite matching algorithm is the concept of a Hall's 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

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

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

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 1.4. *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]).

Linear matroid intersection. The linear matroid intersection problem is a generalization of bipartite matching, which asks whether two given linear matroids have a common base. Equivalently, for two given $k \times m$ matrices ($k \leq m$) M_1 and M_2, the problem is to determine whether there is a subset of k column indices such that the corresponding set of columns is linearly independent in both the matrices. The linear matroid intersection problem 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.

Gurvits [Gur04] showed that the linear matroid intersection problem (NC)-reduces to non-commutative rank computation. The reduction gives the following symbolic matrix:

$$\sum_{i=1}^{m} x_i M_1(i) M_2(i)^T,$$

where $M_1(i), M_2(i)$ are the i-th columns of M_1, M_2. Thus, our NC-algorithm for nc-rank also implies an NC-algorithm for the decision version of the linear matroid intersection.

1.2 Origins of the main ideas

All the proofs presented in the paper are elementary. They only use the folded Wronskian criterion of linear independence of polynomials and the Hall's theorem (and its appropriate generalization for non-commutative rank). But their origin 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.

- MR tensor codes [GHK+17]. These are codes which have the same correctable erasure patterns as the tensor product of two generic codes. [GHK+17] gave a combinatorial characterization of the correctable erasure patterns in a special case called $(m, n, 1, b)$-MR.
- GZP(ℓ) 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(ℓ) codes and the associated generalized Hall Theorem, we showed that bipartite matching reduces to testing correctable erasure patterns for $(m, n, 1, b)$-MR tensor codes. The algorithm in [BCDZ26] is 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 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 based on the polynomial method inspired from Guruswami-Kopparty's [GK16] construction of subspace designs. They essentially boil down to the following amazing fact [GK16]: polynomials which have many disjoint high-multiplicity (or high folded-multiplicity) zeroes are linearly independent. Our proof can also be written using subspace designs.

Organization of the paper. Section 2 introduces necessary preliminaries. Section 3, 4, and 5 give NC algorithms for deciding existence of a perfect matching in a bipartite graph, computing the maximum weight of a perfect matching, and deciding whether nc-rank of a given symbolic matrix is full, respectively. Appendix A gives an alternative NC algorithm for deciding existence of a perfect matching with slightly better parameters (presented using subspace designs).

2 Preliminaries

For a number $n \in \mathbb{N}$, we denote $[n] = \{1, 2, \ldots, n\}$. 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

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

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

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

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.*

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

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 $s + t > n$.*

A generalization of the Hall's Theorem gives a certificate of a symbolic matrix not having full non-commutative rank (see [GGdOW20, Theorem 1.4]).

Theorem 2.3 ([GGdOW20], [?])**.** *Given $n \times n$ matrices $A_1, \ldots, A_m$ 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 $s + t > n$.*

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

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

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

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 (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 $p(\alpha\gamma^j) = 0$ for each $0 \leq j \leq r-1$.*

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 $\gamma \in \mathbb{F}$ be such that the set*

$$\{ \alpha\gamma^j \mid \alpha \in T,\ 0 \leq j \leq r-1 \}$$

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

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,*

$$\sum_{\alpha \in T} Z_r(\mathcal{P}, \alpha) \leq \frac{sD}{r-s+1}. \tag{2}$$

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 $\{\alpha\gamma^j\}_{j=0}^{r-s}$ 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 $\{\alpha\gamma^j\}_{j=0}^{r-s}$ 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). □

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

2.4 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 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_1 as

$$A_1 = \begin{pmatrix} 11\cdots1 & & & \\ & 11\cdots1 & & 0 \\ 0 & & \ddots & \\ & & & 11\cdots1 \end{pmatrix}$$

Matrix A_1 has n rows. The 1-block in each row has length $n-1$. Hence, A_1 has $n(n-1)$ columns. All other entries are 0. Combining A and A_1, we define the $n \times n^2$ extension matrix $\widehat{A} = (A \quad A_1)$.

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

$$\{\, \alpha_i \gamma^j \mid 1 \le i \le n^2,\ 0 \le j \le r-1 \,\}$$

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, $M(G) = (M_0 \quad M_1)$, 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_1.

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*

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

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.

$$p^T M(G) = 0. \tag{3}$$

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) 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

$$\{\, \alpha_j \mid n + (i-1)(n-1) + 1 \leq j \leq n + i(n-1) \,\}. \tag{4}$$

- From the M_0-part of $M(G)$, we get $\sum_{i\in[s]:(i,j)\in E} p_i^T V(\alpha_j) = 0$, for each $j \in [n]$. Define polynomial $q_j(x)$ as

$$q_j(x) = \sum_{i\in[s]:(i,j)\in E} p_i(x)\,. \tag{5}$$

$$\text{Then } q_j(x) \text{ has } \alpha_j \text{ as an r-folded root for each } j \in [n]. \tag{6}$$

Note that for $j \notin N([s])$, the sum in (5) is empty, and hence q_j is zero. For $j \in N([s])$, there are summands in (5), 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 $\mathcal{P} = \text{span}\{p_1(x), p_2(x), \ldots, p_s(x)\}$ have dimension $\ell \le s$. 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 $\delta \ge n$, 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 (4) is $s(n-1)$. Thus, we have $\ell n > s(n-1)$. Hence, we get

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

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

Now, we know that $\mathcal{P} = \text{span}\{p_1(x), p_2(x), \ldots, p_s(x)\}$ 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 (4) is $s(n-1)$.
- From (6), 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 $\{\alpha_j\}_j$ 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 $\delta \ge n \ge s$. Comparing the lower and upper bounds, we have

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

Thus, from Hall's 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.

4 Weighted bipartite matching in NC

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 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 $\widehat{A} = (A\, A_1)$. As in Section 3, 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, 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

$$(A^{r,\delta})_{i,j} = [(M(G^{r,\delta}))_{i,j} \neq 0].$$

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

Definition 4.1 (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)

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

Dual LP
(Node Potentials)

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

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

Lemma 4.2. *Let w^* be a 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 $y \leq 0$ and $z \geq 0$. 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 4.3. *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 of only tight edges.*

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

Lemma 4.4. *Let w^* be the weight of the maximum weight perfect matching and W be the maximum weight of any edge in G. Then*

$$|\deg(\mathcal{D}_w(t)) - 2rw^*| \leq 4n^3\delta W. \tag{7}$$

Proof. Recall that $M(G, w)$ is a $nD \times n^2r$ matrix. For a subset $S \subseteq [n^2r]$ 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

$$\mathcal{D}_w(t) = \sum_{\substack{S \subseteq [n^2r] \\ |S| = nD}} \det(M(G, w)[S])^2. \tag{8}$$

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 4.5. *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 4.2. 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 4.5. □

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

$$\deg(\mathcal{D}_w(t)) \leq 2rw^* + 4n^3\delta W. \tag{9}$$

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 $(\widehat{y}, \widehat{z})$. 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 4.3, 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. Let S be a subset of D columns such that $\det(M(H)[S])$ is nonzero. Clearly, $H^{r,\delta}[S]$ must have a perfect matching.

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

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

Claim 4.6. *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. Observe that $H^{r,\delta}[S]$ precisely consists of the tight edges of $G^{r,\delta}[S]$. Hence, from Lemma 4.3, 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 $\deg(\mathcal{D}_w(t)) \geq 2\widehat{w}_S$. By Lemma 4.3, $\widehat{w}_S$ is equal to the sum of dual values in $G^{r,\delta}[S]$. Consider another set

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

with cardinality nD. Observe that 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 $2n^3\delta W$. Also note that the sum of the dual values for $G^{r,\delta}[S']$ is

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

Hence, we get the lower bound

$$\widehat{w}_S \geq rw^* - 2n^3\delta W. \tag{10}$$

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 $\deg(\det(M(G,w))[S^*]) \geq \widehat{w}_S$. 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

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

Hence, we conclude that $\deg(\mathcal{D}_w(t)) \geq 2\widehat{w}_S$. By (10), we get that

$$\deg(\mathcal{D}_w(t)) \geq 2rw^* - 4n^3\delta W. \tag{11}$$

Now (7) follows from (9) and (11). □

Lemma 4.4 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 (7) 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 2.4, 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 2.4 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 4.7. *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 4.8. *A perfect matching in a bipartite graph can be computed in* NC^3.

[2] assuming the underlying field is rationals

5 Non-commutative rank in NC

In this section, we prove Theorem 1.4. 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*

$$\begin{pmatrix} A_1x_{1,1} & I\,x_{1,2} & 0 & \cdots & 0 \\ A_2x_{2,1} & I\,x_{2,2} & I\,x_{2,3} & \cdots & 0 \\ A_3x_{3,1} & 0 & I\,x_{3,3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{m-1}x_{m-1,1} & 0 & \cdots & I\,x_{m-1,m-1} & I\,x_{m-1,m} \\ A_mx_{m,1} & 0 & \cdots & 0 & I\,x_{m,m} \end{pmatrix}.$$

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

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

where each $A_{i,j}$ is $n \times n$. 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 $m \times nm^2$ block-symbolic matrix $\widehat{\mathcal{A}}$ where each block is $n \times n$.

$$\widehat{\mathcal{A}} = \begin{pmatrix} A_{1,1}x_{1,1} & \ldots & A_{1,m}x_{1,m} & Iz_{1,1} \cdots Iz_{1,mn-1} & & \\ \vdots & \ddots & \vdots & & Iz_{2,1} \cdots Iz_{2,mn-1} & \\ \vdots & \ddots & \vdots & 0 & & \ddots \\ A_{m,1}x_{m,1} & \ldots & A_{m,m}x_{m,m} & & & Iz_{m,1} \cdots Iz_{m,mn-1} \end{pmatrix}$$

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 $\geq nmr$. 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

$$\{\, \alpha_i \gamma^j \mid 1 \leq i \leq nm^2,\ 0 \leq j \leq r-1 \,\}$$

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

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

$$D = nm(r-\delta). \tag{12}$$

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

$$\delta \ge mn \quad \text{and} \quad r > m^2n^2\delta. \tag{13}$$

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

We show that the row rank of $N(\mathcal{A})$ determines whether $\mathcal{A}$ is of full non-commutative rank.

Theorem 5.2. *Given an $mn \times mn$ symbolic matrix $\mathcal{A}$ of the form*

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

where each $A_{i,j}$ is $n \times n$,

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

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 2.3), 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 $a + b \ge mn + 1$. As $\mathcal{A}$ has the block structure with one variable appearing in exactly one block, we can assume, without loss of generality, that B and C are block diagonal with $n \times n$ matrices as blocks, say $B_1, B_2, \ldots, B_m$ and $C_1, C_2, \ldots, C_m$. 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.

$$p^T N(\mathcal{A}) = 0 \qquad \text{i.e.} \quad p^T(N_0 \;\; N_1) = 0. \tag{14}$$

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 (14) 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

  $$\sum_{j=m+1}^{nm^2} Z_r(\mathcal{P}, \alpha_j) \geq (nm-1) \sum_{i=1}^{m} d_i = (nm-1)\Delta. \tag{15}$$

- 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 $1 \leq j \leq m$

  $$Z_r(\mathcal{P}, \alpha_j) \geq \dim \left\{ \sum_{i,k} A_{i,j}(k,\ell) p_{i,k}(x) : 1 \leq \ell \leq n \right\}. \tag{16}$$

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

$$\sum_{j=1}^{nm^2} Z_r(\mathcal{P}, \alpha_j) \leq \frac{q(D-1)}{r-q+1} < qmn\left(\frac{r-\delta}{r-q+1}\right) < qmn. \tag{17}$$

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

Claim 5.3.

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

Proof. Combining (17) with (15), 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 (16), 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

$$\sum_{j=1}^{m} \text{rank}\left(\sum_{i=1}^{m} P_i A_{i,j}\right), \tag{18}$$

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

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 5.3, 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 (18) 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 1.2), 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 $\text{rank}(U) = \Delta$, and $\sum_{j=1}^{m} \text{rank}(UA_j) = L \geq \Delta$. Thus, we get

$$\sum_{j=1}^{m} Z_r(\mathcal{P}, \alpha_j) \geq L \geq \Delta. \tag{19}$$

.

Combining (15) and (19), we have

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

This together with (17) gives a contradiction, as $q = \Delta$. □

Given a symbolic matrix $\sum_{i=1}^{m} A_i x_i$, we can construct the nc-rank-certificatematrix $N(\mathcal{A})$ 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 5.5. *Deciding if a symbolic matrix $\sum_{i=1}^{m} A_i x_i$ is of full nc-rank is in NC^2.*

As mentioned in the introduction, linear matroid intersection reduces to nc-rank.

Corollary 5.6. *Deciding if two given linear matroids have a common base 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 5.2.

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 from this extension, we designed an alternative algorithm for bipartite matching decision (Section 3), which we subsequently generalized to weighted bipartite matching (Section 4) and non-commutative rank (Section 5).

References

[ACM24] Vikraman Arvind, Abhranil Chatterjee, and Partha Mukhopadhyay. Trading determinism for noncommutativity in Edmonds' problem. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, 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 Berlin Heidelberg, 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 Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 619–630. ACM, 2026.

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

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

[BGM23] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic reed-solomon codes achieve list-decoding capacity. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1488–1501. ACM, 2023.

[Csa76] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM J. Comput.*, 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 *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 741–748, New York, NY, USA, 2008. Association for Computing Machinery.

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

[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.

[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 J. Comput.*, 50(3), 2021.

[GG17] Shafi Goldwasser and Ofer Grossman. Bipartite perfect matching in pseudo-deterministic NC. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*, 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 Irit Dinur, editor, *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, Hyatt Regency, New Brunswick, New Jersey, USA, October 9-11, 2016*, pages 109–117. IEEE Computer Society, 2016.

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

[GHK+17] Parikshit Gopalan, Guangda Hu, Swastik Kopparty, Shubhangi Saraf, Carol Wang, and Sergey Yekhanin. Maximally recoverable codes for grid-like topologies. In Philip N. Klein, editor, *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, 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 *Proceedings of the 28th Annual Symposium on Foundations of Computer Science, FOCS 1987*, pages 166–172, 1987.

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

[GKMT17] Rohit Gurjar, Arpita Korwar, Jochen Messner, and Thomas Thierauf. Exact perfect matching in complete graphs. *ACM Trans. Comput. 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.

[GPV88] A. V. Goldberg, S. A. Plotkin, and P. M. Vaidya. Sublinear-time parallel algorithms for matching and related problems. In *Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, SFCS '88, page 174–185, USA, 1988. IEEE Computer Society.

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

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

[Gur04] Leonid Gurvits. Classical complexity and quantum entanglement. *J. Comput. Syst. Sci.*, 69(3):448–484, November 2004.

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

[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.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Comput. Complex.*, 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 Annual Symposium on Foundations of Computer Science, FOCS 2025, Sydney, Australia, December 14-17, 2025*, 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 *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 644–652, New York, NY, USA, 1998. Association for Computing Machinery.

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

[NSV94] H. Narayanan, Huzur Saran, and Vijay V. Vazirani. Randomized parallel algorithms for matroid union and intersection, with applications to arboresences and edge-disjoint spanning trees. *SIAM J. Comput.*, 23(2):387–397, 1994.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, October 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 Annual IEEE 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. Automata, Languages and Programming (ICALP 2006).

[San18] Piotr Sankowski. NC algorithms for weighted planar perfect matching and related problems. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, Prague, Czech Republic, July 9-13, 2018*, 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, Berlin, Heidelberg, New York, N.Y., et al., 2003.

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

[ST17] Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In *58th IEEE Annual 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 *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, page 249–261, New York, NY, USA, 1979. Association for Computing Machinery.

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

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. Note that in Section 3, 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 $H_1, H_2, \ldots, H_m \subseteq \mathbb{F}^t$ is called a (k, K) subspace design, if for every subspace $W \subseteq \mathbb{F}^t$ 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 $r \leq t < |\mathbb{F}|$ and $m < |\mathbb{F}|/r$ be parameters. There exists subspaces $H_1, H_2, \ldots, H_m \in \mathbb{F}^t$, each of co-dimension r, which form a $(k, k(t-1)/(r-k+1))$ subspace design for every $k \leq r$.*

Now, we describe their construction and make some observations.

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

$$\{\, \alpha_i \gamma^j \mid 1 \leq i \leq m,\ 0 \leq j \leq r-1 \,\}$$

has mr distinct elements. Moreover let γ have order more than t. For $1 \leq i \leq m$, $H_i \leq \mathbb{F}^t$ is defined to be the subspace orthogonal to the following set of r vectors

$$\{(1, \alpha_i\gamma^j, (\alpha_i\gamma^j)^2, \ldots, (\alpha_i\gamma^j)^{t-1}) : 0 \leq j \leq r-1\}.$$

Remark. *[GK16, Theorem 7] does 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.*

Note that the construction is based on Vandermonde matrices, which are known to have full rank. Thus, we get the following observation.

Observation A.3. *For any $S \subseteq [m]$, we have $\dim(\cap_{j \in S} H_j) = \max\{0, t - r|S|\}$.*

Now, we describe the algorithm to decide existence of a perfect matching. Let $G(U, V, E)$ be a bipartite graph with n vertices on both sides and m edges. Let $U = \{u_1, u_2, \ldots, u_n\}$ and $V = \{v_1, v_2, \ldots, v_n\}$. Let d_i be the degree of u_i, for $1 \leq i \leq n$ (we assume $d_i \geq 1$). For each $1 \leq i \leq n$, we define a set of indices $S_i \subseteq [m]$ of size $n-1$, which contains the indices of non-neighboring vertices of u_i, plus $d_i - 1$ additional distinct indices. Formally,

$$S_i = \{\, j \in [n] \mid (i, j) \notin E \,\} \cup S_i',$$

where $S'_1, S'_2, \ldots, S'_n$ form a partition of $[m] \setminus [n]$ and $|S'_i| = d_i - 1$ for each $1 \le i \le n$. The choice of the partition can be arbitrary.

Setting parameters: Let us choose parameters

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

and set $t = n(r - \delta)$. Let $H_1, H_2, \ldots, H_m \le \mathbb{F}^t$ be a subspace design from Theorem A.2. We get the following inequality from the definition of subspace design and $\delta \ge n$.

Lemma A.4. *For every subspace $W \subseteq \mathbb{F}^t$ of dimension at most $k \le n$, we have*

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

Algorithm.

1. For $1 \le i \le n$, construct the subspaces $Z_i = \cap_{j \in S_i} H_j$. We have $\dim(Z_i) = t - r|S_i| = t - r(n-1) = r - n\delta$.
2. Compute $\dim(Z_1 \cup Z_2 \cup \cdots \cup Z_n)$. Output yes, if and only if it is $n(r - n\delta)$.

Theorem A.5. *G has a perfect matching if and only if* $\dim(Z_1 \cup Z_2 \cup \cdots \cup Z_n) = n(r - n\delta)$.

Proof. ($\Longleftarrow$) Suppose G does not have a perfect matching then there is a Hall's block i.e, for some $X \subseteq [n]$ and $Y \subseteq [n]$ with $|X| + |Y| \ge n + 1$, we have $j \in S_i$ for each $i \in X$ and $j \in Y$. Then we know that $\cup_{i \in X} Z_i \subseteq \cap_{j \in Y} H_j$. Thus, from Observation A.3,

$$\begin{aligned} \dim(\cup_{i \in X} Z_i) &\le t - r|Y| \\ &\le n(r - \delta) + r|X| - r(n+1) \\ &= r|X| - r - n\delta \end{aligned}$$

Hence, we get

$$\begin{aligned} \dim(Z_1 \cup Z_2 \cup \cdots \cup Z_n) &\le \dim(\cup_{i \in X} Z_i) + \sum_{i \in [n] \setminus X} \dim(Z_i) \\ &\le r|X| - r - n\delta + (n - |X|)(r - n\delta). \\ &= n(r - n\delta) + n|X|\delta - r - n\delta. \\ &< n(r - n\delta). \end{aligned}$$

The last inequality is using $|X| \le n$ and $r \ge n^2\delta$.

($\Longrightarrow$) Suppose $\dim(Z_1 \cup Z_2 \cup \cdots \cup Z_n) < n(r - n\delta)$. Then, without loss of generality, let there be a minimally dependent set of nonzero vectors $q_1 \in Z_1, q_2 \in Z_2, \ldots, q_{k+1} \in Z_{k+1}$ for some $k < n$. Let W be the k-dimensional subspace spanned by $q_1, q_2, \ldots, q_{k+1}$. Recall that if $j \in S_i$ then $q_i \in H_j$, for any i and j. Let us define $n_j = |\{\, i \in [k+1] \mid j \in S_i \,\}|$ for $1 \le j \le m$. Then,

$$\dim(H_j \cap W) \ge \min\{k, n_j\}. \tag{20}$$

Let Y be the set of indices of non-neighbors of $\{u_1, u_2, \ldots, u_{k+1}\}$, i.e., $Y = S_1 \cap S_2 \cap \cdots \cap S_{k+1}$. Then, observe that

$$\dim(H_j \cap W) = k = n_j - 1 \text{ for } j \in Y \text{ and}$$

$$\dim(H_j \cap W) \geq n_j \text{ for } j \in [m] \setminus Y.$$

Combining the two equations, we get

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

Using this with Lemma A.4, we get

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

This implies $n - |Y| < k + 1$. Observe that $n - |Y|$ is the number of neighbors of $\{u_1, u_2, \ldots, u_{k+1}\}$. That is, $\{u_1, u_2, \ldots, u_{k+1}\}$ is a Hall's block. From Theorem 2.1, G does not have a perfect matching. □