# Bipartite Perfect Matching is in Quasi-NC

Alon Gurny

January 19, 2025

# Outline

[

Abstract] This is a summary of "Bipartite Perfect Matching is in Quasi-NC" by Fenner, Gurjar, and Thierauf.

1. Introduction

2. Combinatorics and Probability

3. Isolation

4. Cycles and Circulation

5. The Theorem

## Notation

### Notation

Throughout this presentation, *ALL* the graphs are:

- undirected
- bipartite
- balanced
- labeled

Usually we call our graph $G$ and the set of edges $E$.

The set of edges can be regarded as a relation $E \subseteq [n] \times [n]$.

# NC

### Definition

- We define $\mathcal{NC}^k$ to be the class of problems that can be solved by a polynomial-time uniform family of circuits of polynomial size and depth $\mathcal{O}(\log^k n)$.
- Equivalently, $\mathcal{NC}^k$ is the class of problems that can be solved by a polynomial number of processors in $\mathcal{O}(\log^k n)$ time.
- 

$$\mathcal{NC} = \bigcup_{k \geq 0} \mathcal{NC}^k$$

### Fact

DET, *the problem of computing the determinant of an $n \times n$ matrix with* poly($n$)*-bounded entries, is in* $\mathcal{NC}^2$.

## Perfect Matching

### Definition

- A *perfect matching* of a graph $G$ is a set of edges such that every vertex is incident to exactly one edge.

- The *perfect matching problem* is to determine whether a graph has a perfect matching, or to find one.

- The *decision version* of the perfect matching problem is denoted PM.

- The *search version* of the perfect matching problem is denoted SearchPM.

## State of the Art

It has already been known that perfect matching (whether decision or search) can be solved in randomized $\mathcal{NC}$.

### Open Problem

Can perfect matching be solved in $\mathcal{NC}$?

### Today

There exist algorithms in:

- Quasi$-\mathcal{NC}^2$ for PM (that is, with $\mathcal{O}(n^{\log n})$ processors and $\mathcal{O}(\log^2 n)$ depth)
- randomized $\mathcal{NC}^2$ for PM with only $\mathcal{O}(\log^2 n)$ random bits.
- (We will not see this) Quasi$-\mathcal{NC}^2$ for PM (that is, with $\mathcal{O}(n^{\log n})$ processors and $\mathcal{O}(\log^2 n)$ depth)
- (We will not see this) $\mathcal{NC}^3$ for SearchPM with only $\mathcal{O}(\log^2 n)$ random bits.

### Definitions (Bi-adjacency Matrix)

- The *bi-adjacency matrix*: $\mathbf{A}_G = \mathbf{A}_E = A$ of $G$ (or $E$) is an $n \times n$ matrix where $A_{ij} = 1_{(i,j) \in E}$
- We write $B \leq C$ iff $\forall i, j. B_{ij} \leq C_{ij}$
- A *permutation matrix* is a matrix $\mathbf{A}_\Gamma$ where $\Gamma = \{(i, \sigma i) : i \in [n]\}$ for some permutation $\sigma \in S_n$

### Exercise

*For which $E \subseteq [n] \times [n]$ is $\mathbf{A}_E$ a permutation matrix?*

### Exercise

*For which $B \in \mathbb{R}_{\geq 0}^{n \times n}$ and $E$ does $B \leq \mathbf{A}_E$ hold?*

### Definitions (Weight Functions)

- A *weight function* is a function $w : E \to \mathbb{N}$.
- We extend it naturally to a function $w : 2^E \to \mathbb{N}$ by setting $w(S) = \sum_{e \in S} w(e)$ for all $S \subseteq E$.
- Even more generally (why?), we extend it to a *linear function* $w : \mathbb{R}^{n \times n} \to \mathbb{R}$ by setting $w(A) = \sum_{ij \in E} w(ij) A_{ij}$ for all $A \in \mathbb{R}^{n \times n}$.

### Definitions (Perfect Matching)

- A *perfect matching* is a set of edges $M$ such that every vertex is incident to exactly one edge in $M$.
- Equivalently, $M$ is a perfect matching iff $\mathbf{A}_M$ is a permutation matrix.

Introduction
0000

Combinatorics and Probability
000●●0

Isolation
0000

Cycles and Circulation
000

The Theorem
00000000000

## Birkhoff's Theorem I

### Definition (Doubly Stochastic Matrix)

- A matrix $M \in \mathbb{R}^{n \times n}_{\geq 0}$ is *doubly stochastic* if the sum of the entries in each row and column is 1.
- Equivalently, $M$ is doubly stochastic if $M\mathbf{1} = M^T\mathbf{1} = \mathbf{1}$.

### Definition (Convex Hull)

The *convex hull* of a set $S$ is the smallest convex set containing $S$, denoted $\mathbf{CH}(S)$.

It is precisely the set of all convex combinations of elements of $S$, i.e., $\mathbf{CH}(S) = \left\{\sum_{i=1}^{k} \lambda_i x_i : x_i \in S, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1\right\}$.

Introduction
0000

Combinatorics and Probability
000●●0

Isolation
0000

Cycles and Circulation
000

The Theorem
00000000000

# Birkhoff's Theorem II

### Theorem (Birkhoff, 1946)

*The set of doubly stochastic matrices, denoted $\mathcal{B}_n$, is the convex hull of the permutation matrices.*

### Hint

Use Hall's marriage theorem.

Introduction
○○○○

Combinatorics and Probability
○○○○○●

Isolation
○○○○

Cycles and Circulation
○○○

The Theorem
○○○○○○○○○○○

# Perfect Matching Polytope

### Theorem (Birkhoff, 1946)

*The set of doubly stochastic matrices is the convex hull of the permutation matrices.*

### Definition (Perfect Matching Polytope)

The *perfect matching polytope* $\mathcal{P}_G$ is the convex hull of the bi-adjacency matrices of all the perfect matchings of $G$.

### Corollary

*The perfect matching polytope $P_G$ is exactly the matrices $B$ in the Birkhoff polytope $B_n$ such that $B \leq \mathbf{A}_G$:*

$$\mathcal{P}_G = \{B : B \in \mathcal{B}_n \wedge B \leq \mathbf{A}_G\}$$

### Definition

Let $M$ be a perfect matching. We define its *sign* $\operatorname{sgn} M = \operatorname{sgn} \sigma$ where $\sigma$ is the permutation given by $M$.

### Definition

Let $\{w_i : E \to \mathbb{N}\}_{i \in [k]}$ be weight functions.
We define the *weighted Edmonds matrix* $D^{E,w}$ as follows:

$$\left( D^{E,w} \right)_{ij} = \begin{cases} x_{ij}^{(k)\,w_k(ij)} & \text{if } (i,j) \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Let $a \in \mathbb{N}^k$ be a vector of variables. We also denote
$D_a^{E,w} = D^{E,w}(x_{ij}^{(k)} := a_k)$

### Definition

A weight function $w : E \to \mathbb{N}$ is called *isolating* for $E$ if the existence of a perfect matching in $E$ implies that $E$ has a unique minimum weight perfect matching, which is then called *isolated*.

### Corollary

- If $E$ has no perfect matchings, then $\det D^{E,w} = 0$.
- If $w$ is isolating for $E$, then $\det D^{E,w} \neq 0 \iff$ there is a perfect matching.

### Example

Let $E = \{e_k\}_k$ be an enumeration of the edges. Let $w : E \to \mathbb{N}$ be defined by $w(e_k) = 2^k$. *Every* subset of $E$ has a unique weight. In particular, $w$ is isolating for $E$.
Is this enough?

## Isolation Lemma

### Lemma (Mulmuley, Vazirani & Vazirani 1987)

*Let $B$ be a finite set.*

*Let $k$ be a positive integer.*

*Let $\mathcal{F} \subseteq 2^B$ be a nonempty family of subsets of $B$.*

*Let $w : B \to k$ be a be chosen uniformly at random among all functions from $B$ to $[k]$.*

*Then, with probability at least $1 - |B|/k$, there exists a unique set $S \in \mathcal{F}$ with a minimum weight among all sets in $\mathcal{F}$.*

## Corollary

Let $w : E \to [n^3]$ be a random weight function.
Then with probability at least $1 - 1/n$, $w$ is isolating for $G$.

## Proof.

Take $\mathcal{F}$ as the family of perfect matchings of $G$.
As, $|E| \leq n^2$, by the isolation lemma, with probability at least

$$(1 - |E|/n^3) \geq 1 - n^2/n^3 = 1 - 1/n$$

$w$ is isolating for $G$. □

## Corollary

There exists an RNC algorithm that can solve PM, which uses
poly($n$) random bits.

# Circulation

### Definition

Let $w : E \to \mathbb{N}$ be a weight function. The *w-circulation* of a cycle $C = e_1, \ldots, e_{2k}$ is defined as

$$c_w(C) = |w(e_1) - w(e_2) + \ldots + w(e_{2k-1}) - w(e_{2k})|$$

This is well defined because we take the absolute value.

### Remark

Let $M_1$ and $M_2$ be two perfect matchings of $G$, and suppose $C \subseteq M_1 \triangle M_2$.
Then $c_w(C) = |w(C \cap M_1) - w(C \cap M_2)|$.

### Claim

*The symmetric difference of two perfect matchings is a union of disjoint cycles.*
*Each cycle consists of interleaved edges from the two matchings.*

### Proof.

The degree of each vertex is 1 in a perfect matching.
Thus, in the symmetric difference of two perfect matchings, each vertex has degree 0 or 2.
Therefore it is a union of disjoint cycles. The rest is easy to see. □

### Lemma

*Let $w : E \to \mathbb{N}$ be a weight function.*
*If every cycle in $G$ has a nonzero circulation, then $w$ is isolating for*
*$G$.*

### Proof.

On the contrary, suppose that $M_1$ and $M_2$ are two minimum
perfect matchings of $G$. Choose some cycle $C \subseteq M_1 \triangle M_2$.
Since $c_w(C) > 0$, we have $w(C \cap M_1) \neq w(C \cap M_2)$. WLOG,
assume that $w(C \cap M_1) < w(C \cap M_2)$. Then $M_2 \triangle C$ is a perfect
matching with weight less than $w(M_2) = w(M_1)$, contradicting
minimality. □

### Definition

Suppose $G$ has a perfect matching. Let $w : E \to \mathbb{N}$ be a weight function.

Then $G_w \subseteq G$ is the union of all minimum weight perfect matchings of $G$, relatively to $w$.

### Theorem

Let $G^0 = G$ be and $G^{i+1} = \left(G^i\right)_{w_i}$.

Let $k \geq \log n - 2$ and let $w_0, \ldots, w_k : E \to \mathbb{N}$ be weight functions such that $w_i$ gives nonzero circulation to all the cycles of size at most $4 \cdot 2^i$ in $G_i$.

Then the joint weight function $w = (w_0, \ldots, w_k)$ is isolating.

| Introduction | Combinatorics and Probability | Isolation | Cycles and Circulation | The Theorem |
| :--- | :--- | :--- | :--- | :--- |
| oooo | oooooo | oooo | ooo | oo●ooooooooooo |

### Lemma

Let $r \geq 2$ be even. Suppose $G$ has no cycles of size at most $2r$. Then $G$ has at most $n^4$ cycles of size at most $4r$.

### Proof.

- Equivalently, there is at most one path of length $\leq r$ between any two vertices.

- Let $v_0, v_1, v_2, v_3$ be vertices in $V_1$, such that the distance between $v_i$ and $v_{i+1 \mod 4}$ is $\leq r$.

- There exists a *partial function* from $V_1^4$ to cycles in $G$ that maps $(v_0, v_1, v_2, v_3)$ to the cycle composed of the unique paths of length $\leq r$ between $v_i$ and $v_{i+1 \mod 4}$.

- Let $C$ be a cycle of size $\leq 4r$.
  We can choose arbitrarily $v_0, v_1, v_2, v_3 \in C$ such that the distance between $v_i$ and $v_{i+1 \mod 4}$ is $\leq r$.

- This function is onto the set of cycles of size $\leq 4r$. Thus, there are at most $|V_1|^4 = n^4$ cycles of size $\leq 4r$.

$\square$

### Lemma

*Suppose G has a perfect matching and let $w : E \rightarrow \mathbb{N}$ be a weight function.*
*Then every perfect matching in $G_w$ has the same weight as every minimum weight matching in G.*

### Proof.

If $w$ is isolating, $G_w$ is just a single perfect matching.

Otherwise, suppose the minimum weight for perfect matchings in $G$ is $m$. Suppose there exist $t$ such matchings and let $X$ be their average. Then, $w(X) = m$.

Let $N$ be a perfect matching in $G_w$. Every edge is contained in some minimum weight perfect matching, so $X - 1/tN \geq 0$.

It can easily be seen that the sum of every row and column is $(t-1)/t$ and thus the matrix $\frac{t}{t-1}X - \frac{1}{t-1}N$ is doubly stochastic. Therefore, it lies in $\mathcal{P}_G$ and thus has weight at least $m$. That is,

$$ m \leq w\left(\frac{t}{t-1}X - \frac{1}{t-1}N\right) = m \cdot \frac{t}{t-1} - w(N) \cdot \frac{1}{t-1} $$

From that it follows that $w(N) \leq m$. □

### Lemma

*Suppose $G$ has a perfect matching and let $w : E \to \mathbb{N}$ be a weight function.*
*Then the $w$-circulation of every cycle in $G_w$ is zero.*

### Proof.

Let $X$ be the average of all perfect matchings in $G_w$.
Let $t$ be the number of perfect matchings, $\varepsilon = 1/t$, and let $M_1, \ldots, M_t$ be the perfect matchings. Then $X = \varepsilon \sum_{i=1}^{t} M_i$.
Since each edge is contained in some perfect matching, we have $X_{ij} \geq \varepsilon$ for all $i, j$ such that $(i, j) \in E$.
Let $C = e_1, \ldots, e_{2p}$ be a cycle in $H$.
Define $Y$ by

$$Y_{ij} = \begin{cases} X_{ij} + (-1)^k \varepsilon & \text{if } (i,j) = e_k \in C, \\ X_{ij} & \text{otherwise.} \end{cases}$$

Then clearly $Y \geq 0$ and $Y\mathbf{1} = Y^T\mathbf{1} = \mathbf{1}$. Therefore, $Y$ lies in the perfect matching polytope.
Since all the perfect matchings have the same weight, $w(Y) = w(X)$ and thus $w(Y - X) = 0$. But $c_w(C) = \varepsilon w(Y - X)$, and thus $c_w(C) = 0$. □

### Lemma

*Using $\mathcal{O}(\log n)$ random bits we can generate a weight assignment $w : E \to \mathbb{N}$ with $w \le \mathrm{poly}(n)$ such that for every set of $n^4$ cycles, $w$ gives nonzero circulation to all of them with probability at least $1 - 1/n$.*

### Proof.

Let $w(e_k) = 2^k$. Let the cycles be $C_1, \ldots, C_s$. Then, $c_w(C_i) \ne 0$ for all $i$ is equivalent to $\prod_{i=1}^{n^4} c_w(C_i) \ne 0$. This product is bounded by $\mathrm{poly}(n)^{n^4} = 2^{\mathrm{poly}(n)}$.

Thus, it has at most $\mathrm{poly}(n)$ prime factors, say $k$ prime factors. Choose $t = kn$.

Then if we choose a random prime amongst the first $t$ primes $[p_1, \ldots, p_t]$, then if the product is nonzero, with probability at least $1 - 1/n$ it is still true modulo the chosen prime. $\qquad\square$

## Theorem

*Let $G^0 = G$ be and $G^{i+1} = \left(G^i\right)_{w_i}$.*
*Let $k \geq \log n - 2$ and let $w_0, \ldots, w_k : E \to \mathbb{N}$ be weight functions*
*such that for every set of $w_i$ gives nonzero circulation to all the*
*cycles of size at most $4 \cdot 2^i$ in $G_i$.*
*Then the joint weight function $w = (w_0, \ldots, w_k)$ is isolating.*

## Proof.

Since $w_i$ gives nonzero circulation to all the cycles in $G^i$, all those
cycles do not appear in $G^{i+1}$.
In particular, $G^k$ has no cycles of size at most $4 \cdot 2^k \geq n$.
That is, $G^k$ has a unique perfect matching. We want to show that
it is isolated by $w$. This follows from the next lemma. $\qquad\square$

### Lemma

Suppose $M_1$ is a matching that appears in $G^i$ but not in $G^{i+1}$ and $M_2$ is a matching that appears in $G_{i+1}$.
Then $w_i(M_2) < w_i(M_1)$.

### Proof.

Since $M_2$ appears in $G_{i+1}$, it has the same weight as any $w_i$-minimum weight matching in $G_i$. That is $w_i(M_2) \leq w_i(M_1)$.
But if $w_{i+1}(M_1) = w_{i+1}(M_2)$ held, then $M_1$ would have been in $G^{i+1}$ by its definition. □

## Deciding PM in randomized $\mathcal{NC}^2$

The following algorithm solves PM in randomized $\mathcal{NC}^2$ with $\mathcal{O}(\log^2 n)$ random bits.

---

**Algorithm 1** Decide PM (randomized)

---

Let $k = \log n - 2$.
Generate random weight functions $w_0, \ldots, w_k$.
Generate random numbers $r_0, \ldots, r_k$.
Create $w_0, \ldots, w_k$.
Combine $w = (w_0, \ldots, w_k)$.
Calculate det $D_r^{G,w}$.
**return** det $D_r^{G,w} \neq 0$

---

# Deciding PM in randomized $Quasi - \mathcal{NC}^2$

The following algorithm solves PM in $\mathcal{NC}^2$ with $\mathcal{O}(\log^2 n)$ random bits.

---

**Algorithm 2** Decide PM (deterministic)

---

Let $k = \log n - 2$.
**for all** Possible weight functions $w_0, \ldots, w_k$ and $r$ **do**
  Calculate $\det D_2^{G,w}$.
  **if** $\det D_2^{G,w} \neq 0$ **then**
    **return** True
  **end if**
  **return** False
**end for**

---