# Matchings and algebra 

Peter Hajnal

Bolyai Institute, University of Szeged, Hungary

## 2023 fall

## The problem

## The problem

Given $G$ simple bipartite graph, $|L|=|U|=n$.

## The problem

## The problem

Given $G$ simple bipartite graph, $|L|=|U|=n$.
Is there a perfect matching in $G$ ?

## The problem

## The problem

Given $G$ simple bipartite graph, $|L|=|U|=n$.
Is there a perfect matching in $G$ ?

The assumption of the bipartite property is not necessary, but it makes our life easier.

## Coding with matrices

## Definition <br> Let $G$ be a simple graph.

## Coding with matrices

## Definition

Let $G$ be a simple graph.
The adjacency matrix of $G$, denoted as $A_{G}$, is a matrix with rows and columns identified with vertices, furthermore

$$
\left(A_{G}\right)_{u} v= \begin{cases}1, & u \text { and } v \text { are adjacent } \\ 0, & u \text { and } v \text { are not adjacent }\end{cases}
$$

## Coding with matrices

## Definition

Let $G$ be a simple graph.
The adjacency matrix of $G$, denoted as $A_{G}$, is a matrix with rows and columns identified with vertices, furthermore

$$
\left(A_{G}\right)_{u} v= \begin{cases}1, & u \text { and } v \text { are adjacent } \\ 0, & u \text { and } v \text { are not adjacent }\end{cases}
$$

## Definition

Let $G$ be a bipartite graph with color classes $L \dot{U} U$.

## Coding with matrices

## Definition

Let $G$ be a simple graph.
The adjacency matrix of $G$, denoted as $A_{G}$, is a matrix with rows and columns identified with vertices, furthermore

$$
\left(A_{G}\right)_{u} v= \begin{cases}1, & u \text { and } v \text { are adjacent } \\ 0, & u \text { and } v \text { are not adjacent }\end{cases}
$$

## Definition

Let $G$ be a bipartite graph with color classes $L \dot{U} U$.
The bipartite adjacency matrix of $G$ is a matrix $B_{G} \in \mathbb{R}^{L \times U}$ :

$$
\left(B_{G}\right)_{\ell, u}= \begin{cases}1, & \ell \text { and } u \text { are adjacent } \\ 0, & \ell \text { and } u \text { are not adjacent }\end{cases}
$$

## The relation of matrices

## The relation of matrices

In a bipartite graph there is no adjacency between lower vertices, and no adjacency between upper vertices.

## The relation of matrices

In a bipartite graph there is no adjacency between lower vertices, and no adjacency between upper vertices.

In $A_{G}$ this property means a big block of 0 's.

## The relation of matrices

In a bipartite graph there is no adjacency between lower vertices, and no adjacency between upper vertices.

In $A_{G}$ this property means a big block of 0's.

$$
A_{G}=\left(\begin{array}{cc}
0 & B_{G} \\
B_{G}^{T} & 0
\end{array}\right)
$$

## The relation of matrices

In a bipartite graph there is no adjacency between lower vertices, and no adjacency between upper vertices.

In $A_{G}$ this property means a big block of 0's.

$$
A_{G}=\left(\begin{array}{cc}
0 & B_{G} \\
B_{G}^{T} & 0
\end{array}\right)
$$

$B_{G}$ is a condensed version of the adjacency matrix.

## The simple bipartite graph $G$ and $B_{G}$

## The simple bipartite graph $G$ and $B_{G}$

The $B_{G}$ matrix is a code of the simple bipartite graph $G$.

## The simple bipartite graph $G$ and $B_{G}$

The $B_{G}$ matrix is a code of the simple bipartite graph $G$. There is a dictionary between the linear algebraic language and graph theoretical language.

## The simple bipartite graph $G$ and $B_{G}$

The $B_{G}$ matrix is a code of the simple bipartite graph $G$. There is a dictionary between the linear algebraic language and graph theoretical language.
possible edges of $G \equiv$ positions of $B_{G}=A \times F$

$$
\begin{aligned}
E(G) & \equiv \text { the } 1 \text { 's of } B_{G} \\
|A|=|F| & \equiv B_{G} \text { is a square matrix }
\end{aligned}
$$

M is a matching $\equiv 1$ 's s.t. there is maximum one 1 in each row and column
M is a perfect matching $\equiv n$ 1's s.t. there is exactly one 1 in each row and column
$\equiv n$ 1's s.t. their product is a term of the determinant

## The determinant

## Reminder

$$
\operatorname{det} M=\sum_{\pi \in S_{n}} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i \pi(i)}
$$

## The determinant

## Reminder

$$
\operatorname{det} M=\sum_{\pi \in S_{n}} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i \pi(i)}
$$

## Corollary

If $\operatorname{det} B_{G} \neq 0$ then the above expansion of $\operatorname{det} B_{G}$ has a non-zero term.

## The determinant

## Reminder

$$
\operatorname{det} M=\sum_{\pi \in S_{n}} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i \pi(i)}
$$

## Corollary

If $\operatorname{det} B_{G} \neq 0$ then the above expansion of $\operatorname{det} B_{G}$ has a non-zero term.

This is equivalent to the fact that there is a perfect matching in $G$.

## The determinant

## Reminder

$$
\operatorname{det} M=\sum_{\pi \in S_{n}} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i \pi(i)}
$$

Corollary
If $\operatorname{det} B_{G} \neq 0$ then the above expansion of $\operatorname{det} B_{G}$ has a non-zero term.

This is equivalent to the fact that there is a perfect matching in $G$.

The reverse direction of the Corollary is not true.

## The permanent

## The permanent

## Definition

The permanent of $M \in \mathbb{R}^{n \times n}$

$$
\operatorname{per} M_{n \times n}=\sum_{\pi \in S_{n}} \prod_{i=1}^{n} M_{i \pi(i)}
$$

## The permanent

## Definition

The permanent of $M \in \mathbb{R}^{n \times n}$

$$
\operatorname{per} M_{n \times n}=\sum_{\pi \in S_{n}} \prod_{i=1}^{n} M_{i \pi(i)}
$$

## Observation

(i) per $B_{G} \neq 0$ iff there is a perfect matching in $G$. (ii) per $B_{G}$ is the number of perfect matchings in $G$.

## The permanent

## Definition

The permanent of $M \in \mathbb{R}^{n \times n}$

$$
\operatorname{per} M_{n \times n}=\sum_{\pi \in S_{n}} \prod_{i=1}^{n} M_{i \pi(i)}
$$

## Observation

(i) per $B_{G} \neq 0$ iff there is a perfect matching in $G$.
(ii) per $B_{G}$ is the number of perfect matchings in $G$.

Unfortunately computing per $B_{G}$ is $\# P$-hard.

## The permanent

## Definition

The permanent of $M \in \mathbb{R}^{n \times n}$

$$
\operatorname{per} M_{n \times n}=\sum_{\pi \in S_{n}} \prod_{i=1}^{n} M_{i \pi(i)}
$$

## Observation

(i) per $B_{G} \neq 0$ iff there is a perfect matching in $G$.
(ii) per $B_{G}$ is the number of perfect matchings in $G$.

Unfortunately computing per $B_{G}$ is $\# P$-hard.

## Reminder

There are efficient algorithms to compute the determinant of a square matrix.

## Polynomials

## Polynomials

## Definition <br> $X_{G} \in \mathbb{R}\left[x_{e}: e \in E(G)\right]^{n \times n}: \forall e \in E(G)$ we substitute the 1 of $B_{G}$, corresponding to $e$ with $x_{e}$.

## Definition

$X_{G} \in \mathbb{R}\left[x_{e}: e \in E(G)\right]^{n \times n}: \forall e \in E(G)$ we substitute the 1 of $B_{G}$, corresponding to $e$ with $x_{e}$.

## Theorem

$\operatorname{det}\left(X_{G}\right)$ is a non-zero polynomial if and only if there is a perfect matching in $G$.

## Definition

$X_{G} \in \mathbb{R}\left[x_{e}: e \in E(G)\right]^{n \times n}: \forall e \in E(G)$ we substitute the 1 of $B_{G}$, corresponding to $e$ with $x_{e}$.

## Theorem

$\operatorname{det}\left(X_{G}\right)$ is a non-zero polynomial if and only if there is a perfect matching in $G$.

## Observation

(i) The number of perfect matchings in $G$ is the number of monomials of $\operatorname{det}\left(X_{G}\right)$.
(ii) It is possible that to write down $\operatorname{det}\left(X_{G}\right)$ takes too long. But evaluate $\left.\operatorname{det}\left(X_{G}\right)\right|_{x_{e}=\alpha_{e}}$ is easy.

## A randomized algorithm

## A randomized algorithm

## Randomized algorithm

## A randomized algorithm

## Randomized algorithm

Random substitution: For each edge $e$ generate $r_{e} \in\{1, \ldots, N\}$, a random value (uniform distribution, independence).

## A randomized algorithm

## Randomized algorithm

Random substitution: For each edge $e$ generate $r_{e} \in\{1, \ldots, N\}$, a random value (uniform distribution, independence).
Calculating DET: Compute $\left.\operatorname{det}\left(X_{G}\right)\right|_{x_{e}=r_{e}}$.

## A randomized algorithm

## Randomized algorithm

Random substitution: For each edge $e$ generate $r_{e} \in\{1, \ldots, N\}$, a random value (uniform distribution, independence).
Calculating DET: Compute $\left.\operatorname{det}\left(X_{G}\right)\right|_{X_{e}=r_{e}}$.

## Evaluation:

If the value is non- 0 , then the output is „There is perfect matching".

## A randomized algorithm

## Randomized algorithm

Random substitution: For each edge $e$ generate $r_{e} \in\{1, \ldots, N\}$, a random value (uniform distribution, independence).
Calculating DET: Compute $\left.\operatorname{det}\left(X_{G}\right)\right|_{X_{e}=r_{e}}$.

## Evaluation:

If the value is non- 0 , then the output is „There is perfect matching".
If the value is 0 , then the output is „Probably there is no perfect matching".

## Error

Our algorithm can make errors. But how?

## Error

Our algorithm can make errors. But how?

- „There is a perfect matching" : the answer is guaranteed to be correct.


## Error

Our algorithm can make errors. But how?

- „There is a perfect matching": the answer is guaranteed to be correct.
- „Probably there is no perfect matching":


## Error

Our algorithm can make errors. But how?

- „There is a perfect matching": the answer is guaranteed to be correct.
- „Probably there is no perfect matching":
- if $\operatorname{det}\left(X_{G}\right)$ is the 0 polynomial, then the answer is correct;


## Error

Our algorithm can make errors. But how?

- „There is a perfect matching": the answer is guaranteed to be correct.
- „Probably there is no perfect matching":
- if $\operatorname{det}\left(X_{G}\right)$ is the 0 polynomial, then the answer is correct;
- if $\operatorname{det}\left(X_{G}\right)$ is a non-0 polynomial, and we generate an unfortunate $r_{e}$ 's, one of the roots of $\operatorname{det}\left(X_{G}\right)$ : the algorithm fails.


## Error

Our algorithm can make errors. But how?

- „There is a perfect matching": the answer is guaranteed to be correct.
- „Probably there is no perfect matching":
- if $\operatorname{det}\left(X_{G}\right)$ is the 0 polynomial, then the answer is correct;
- if $\operatorname{det}\left(X_{G}\right)$ is a non-0 polynomial, and we generate an unfortunate $r_{e}$ 's, one of the roots of $\operatorname{det}\left(X_{G}\right)$ : the algorithm fails.

Our goal is to reduce the probability of error.

## Schwartz' lemma

## Schwartz' lemma

## Theorem (Schwartz-lemma)

Let $p\left(x_{1}, \ldots, x_{k}\right) \in \mathbb{R}\left[x_{1}, \ldots, x_{k}\right]$ be a non-zero polynomial and let $r_{i} \in\{1, \ldots, N\}$ be uniform independent random variables, $(1 \leq i \leq k)$. Then

$$
\mathbb{P}\left(p\left(r_{1}, \ldots, r_{k}\right)=0\right) \leq \frac{\operatorname{deg} p}{N}
$$

For $k=1$ we have $p \in \mathbb{R}[x]$.

For $k=1$ we have $p \in \mathbb{R}[x]$.
We know that $|\{r \in \mathbb{R}: p(r)=0\}| \leq \operatorname{deg} p$,

## Proof by induction on $k: k=1$

For $k=1$ we have $p \in \mathbb{R}[x]$.
We know that $|\{r \in \mathbb{R}: p(r)=0\}| \leq \operatorname{deg} p$, hence the probability that the value of $r$ is a root of $p$ is at most $\frac{\operatorname{deg} p}{N}$.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+ & p_{\alpha-1}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots
\end{aligned} p_{0}\left(x_{1}, \ldots, x_{k-1}\right), ~ \$
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non- 0 polynomial.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+ & p_{\alpha-1}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots
\end{aligned} p_{0}\left(x_{1}, \ldots, x_{k-1}\right), ~ \$
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non-0 polynomial.
It is obvious that $\operatorname{deg} p \geq \operatorname{deg} p_{\alpha}+\alpha$.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
& p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+ p_{\alpha-1}( \\
&\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots+p_{0}\left(x_{1}, \ldots, x_{k-1}\right),
\end{aligned}
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non- 0 polynomial.
It is obvious that $\operatorname{deg} p \geq \operatorname{deg} p_{\alpha}+\alpha$.
Let $R_{k}=\left\{\left(r_{1}, \ldots, r_{k}\right): p\left(r_{1}, \ldots, r_{k}\right)=0\right\}$, the set of choices for $\left(r_{1}, \ldots, r_{k}\right)$, that is a root of $p$.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
& p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+ p_{\alpha-1}( \\
&\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots+p_{0}\left(x_{1}, \ldots, x_{k-1}\right),
\end{aligned}
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non- 0 polynomial.
It is obvious that $\operatorname{deg} p \geq \operatorname{deg} p_{\alpha}+\alpha$.
Let $R_{k}=\left\{\left(r_{1}, \ldots, r_{k}\right): p\left(r_{1}, \ldots, r_{k}\right)=0\right\}$, the set of choices for $\left(r_{1}, \ldots, r_{k}\right)$, that is a root of $p$. We need to bound $\mathbb{P}\left(R_{k}\right)$.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+ & p_{\alpha-1}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots+p_{0}\left(x_{1}, \ldots, x_{k-1}\right)
\end{aligned}
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non-0 polynomial.
It is obvious that $\operatorname{deg} p \geq \operatorname{deg} p_{\alpha}+\alpha$.
Let $R_{k}=\left\{\left(r_{1}, \ldots, r_{k}\right): p\left(r_{1}, \ldots, r_{k}\right)=0\right\}$, the set of choices for $\left(r_{1}, \ldots, r_{k}\right)$, that is a root of $p$. We need to bound $\mathbb{P}\left(R_{k}\right)$.

Let $R_{k-1}=\left\{\left(r_{1}, \ldots, r_{k}\right): p_{\alpha}\left(r_{1}, \ldots, r_{k-1}\right)=0\right\}$.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
& p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+p_{\alpha-1}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots+p_{0}\left(x_{1}, \ldots, x_{k-1}\right),
\end{aligned}
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non-0 polynomial.
It is obvious that $\operatorname{deg} p \geq \operatorname{deg} p_{\alpha}+\alpha$.
Let $R_{k}=\left\{\left(r_{1}, \ldots, r_{k}\right): p\left(r_{1}, \ldots, r_{k}\right)=0\right\}$, the set of choices for $\left(r_{1}, \ldots, r_{k}\right)$, that is a root of $p$. We need to bound $\mathbb{P}\left(R_{k}\right)$.

Let $R_{k-1}=\left\{\left(r_{1}, \ldots, r_{k}\right): p_{\alpha}\left(r_{1}, \ldots, r_{k-1}\right)=0\right\}$.
Let
$Q=\left\{\left(r_{1}, \ldots, r_{k}\right):\left(r_{1}, \ldots, r_{k-1}\right) \notin R_{k-1}\right.$, but $\left.\left(r_{1}, \ldots, r_{k}\right) \in R_{k}\right\}$.

## Proof by induction on $k$ : The induction step

Assume that we know the claim for $k-1$ variables. Write $p$ as:

$$
\begin{aligned}
& p\left(x_{1}, \ldots, x_{k}\right)=p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha}+p_{\alpha-1}\left(x_{1}, \ldots, x_{k-1}\right) \cdot x_{k}^{\alpha-1}+ \\
& \cdots+p_{0}\left(x_{1}, \ldots, x_{k-1}\right),
\end{aligned}
$$

where $p_{\alpha}\left(x_{1}, \ldots, x_{k-1}\right)$ is a non-0 polynomial.
It is obvious that $\operatorname{deg} p \geq \operatorname{deg} p_{\alpha}+\alpha$.
Let $R_{k}=\left\{\left(r_{1}, \ldots, r_{k}\right): p\left(r_{1}, \ldots, r_{k}\right)=0\right\}$, the set of choices for $\left(r_{1}, \ldots, r_{k}\right)$, that is a root of $p$. We need to bound $\mathbb{P}\left(R_{k}\right)$.
Let $R_{k-1}=\left\{\left(r_{1}, \ldots, r_{k}\right): p_{\alpha}\left(r_{1}, \ldots, r_{k-1}\right)=0\right\}$.
Let
$Q=\left\{\left(r_{1}, \ldots, r_{k}\right):\left(r_{1}, \ldots, r_{k-1}\right) \notin R_{k-1}\right.$, but $\left.\left(r_{1}, \ldots, r_{k}\right) \in R_{k}\right\}$.
Easy to see that $R_{k} \subseteq R_{k-1} \cup Q$.

Based on the induction hypothesis we can bound the probability of $R_{k-1}$.

Based on the induction hypothesis we can bound the probability of $R_{k-1}$.

Based on the analysis of case $k=1$ we can estimate the probability of $Q$.

## Proof by induction on $k$ : The induction step (cont'd)

Based on the induction hypothesis we can bound the probability of $R_{k-1}$.

Based on the analysis of case $k=1$ we can estimate the probability of $Q$.

After summing our bounds we obtain

$$
\mathbb{P}\left(R_{k}\right) \leq \mathbb{P}\left(R_{k-1}\right)+\mathbb{P}(Q) \leq \frac{\operatorname{deg} p_{\alpha}}{N}+\frac{\alpha}{N} \leq \frac{\operatorname{deg} p}{N}
$$

Based on the induction hypothesis we can bound the probability of $R_{k-1}$.

Based on the analysis of case $k=1$ we can estimate the probability of $Q$.

After summing our bounds we obtain

$$
\mathbb{P}\left(R_{k}\right) \leq \mathbb{P}\left(R_{k-1}\right)+\mathbb{P}(Q) \leq \frac{\operatorname{deg} p_{\alpha}}{N}+\frac{\alpha}{N} \leq \frac{\operatorname{deg} p}{N}
$$

This proves the claim of the Theorem.

## Methods to reduce the error

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ (deg $p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ (deg $p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.
We can reduce the error probability.

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ (deg $p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.
We can reduce the error probability.
(I) Increase the value of $N$.

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ ( $\operatorname{deg} p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.
We can reduce the error probability.
(I) Increase the value of $N$.
(II) Independently repeat the algorithm $M$ times $(N=2 n)$.

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ (deg $p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.
We can reduce the error probability.
(I) Increase the value of $N$.
(II) Independently repeat the algorithm $M$ times $(N=2 n)$. As soon as one determinant computation gives a non-0 value stop and announce "The graph has a perfect matching".

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ (deg $p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.
We can reduce the error probability.
(I) Increase the value of $N$.
(II) Independently repeat the algorithm $M$ times $(N=2 n)$. As soon as one determinant computation gives a non-0 value stop and announce "The graph has a perfect matching". If all $M$ execution evaluate a 0 determinant, then announce "Probably the graph has NO perfect matching".

## Methods to reduce the error

We can apply Schwartz' Lemma for $p=\operatorname{det}\left(X_{G}\right)$ (deg $p=n(=|A|=|F|)$ ) we get that in the case of the choice $N=2 n$ the probability of error is at most $\frac{1}{2}$.
We can reduce the error probability.
(I) Increase the value of $N$.
(II) Independently repeat the algorithm $M$ times $(N=2 n)$. As soon as one determinant computation gives a non-0 value stop and announce "The graph has a perfect matching". If all $M$ execution evaluate a 0 determinant, then announce "Probably the graph has NO perfect matching".

## Theorem

After $M$ independent repetition as above

$$
\mathbb{P}(\text { error }) \leq \frac{1}{2^{M}}
$$

Break


## Introduction

## The problem

Let $G$ be a bipartite graph, $c: E(G) \rightarrow \mathbb{R}^{+}$. Find a matching $M$, that $c(M)=\sum_{e \in M} c(e)$ has the maximum value.

## Introduction

## The problem

Let $G$ be a bipartite graph, $c: E(G) \rightarrow \mathbb{R}^{+}$. Find a matching $M$, that $c(M)=\sum_{e \in M} c(e)$ has the maximum value.

## Definition

For an edges set $M \subseteq E(G)=\left\{e_{1}, \ldots, e_{m}\right\}$ the characteristic vector of $M$ is $\underline{\chi}_{M}=\left(v_{i}\right) \in \mathbb{R}^{m}$, where $v_{i}=1$, if $e_{i} \in M$, otherwise 0.

## Introduction

## The problem

Let $G$ be a bipartite graph, $c: E(G) \rightarrow \mathbb{R}^{+}$. Find a matching $M$, that $c(M)=\sum_{e \in M} c(e)$ has the maximum value.

## Definition

For an edges set $M \subseteq E(G)=\left\{e_{1}, \ldots, e_{m}\right\}$ the characteristic vector of $M$ is $\underline{\chi}_{M}=\left(v_{i}\right) \in \mathbb{R}^{m}$, where $v_{i}=1$, if $e_{i} \in M$, otherwise 0.

Note that $m=|E(G)|$, hence

$$
\mathbb{R}^{E(G)} \equiv \mathbb{R}^{m}
$$

## Algebraization

## Algebraization

$$
c(M)=\left\langle\underline{c}, \underline{\chi}_{M}\right\rangle, \text { where } \underline{c} \in \mathbb{R}^{E(G)} .
$$

## Algebraization

$c(M)=\left\langle\underline{c}, \underline{\chi}_{M}\right\rangle$, where $\underline{c} \in \mathbb{R}^{E(G)}$.
The new form of our problem:

$$
\begin{aligned}
\max \left\{\left\langle\underline{c}, \underline{\chi}_{M}\right\rangle\right. & : M \text { is a matching }\} \\
& =\max \left\{\langle\underline{c}, \underline{x}\rangle: \underline{x} \in\left\{\underline{\chi}_{M}: M \text { is a matching }\right\}\right\} \\
\gtreqless & =\max \left\{\langle\underline{c}, \underline{x}\rangle: \underline{x} \in \operatorname{conv}\left\{\underline{\chi}_{M}: M \text { is a matching }\right\}\right\}
\end{aligned}
$$

## Geometry

## Geometry

## Definition

Let $P \subseteq \mathbb{R}^{m}$ be a set of vectors/points. Then the convex hull of $P$ is,

$$
\operatorname{conv} P=\left\{\sum_{i=1}^{k} \lambda_{i} \underline{p}_{i}: \lambda_{i} \geq 0, \sum \lambda_{i}=1, \underline{p}_{i} \in P\right\}
$$

the minimal convex set containing $P$.

## Geometry

## Definition

Let $P \subseteq \mathbb{R}^{m}$ be a set of vectors/points. Then the convex hull of $P$ is,

$$
\operatorname{conv} P=\left\{\sum_{i=1}^{k} \lambda_{i} \underline{p}_{i}: \lambda_{i} \geq 0, \sum \lambda_{i}=1, \underline{p}_{i} \in P\right\}
$$

the minimal convex set containing $P$.

The vectors/points of the sets are called the convex combinations of the elements of $P$.

## Geometry

## Definition

Let $P \subseteq \mathbb{R}^{m}$ be a set of vectors/points. Then the convex hull of $P$ is,

$$
\operatorname{conv} P=\left\{\sum_{i=1}^{k} \lambda_{i} \underline{p}_{i}: \lambda_{i} \geq 0, \sum \lambda_{i}=1, \underline{p}_{i} \in P\right\}
$$

the minimal convex set containing $P$.

The vectors/points of the sets are called the convex combinations of the elements of $P$.

## Notation

The set conv $\left\{\underline{\chi}_{M}: M\right.$ is a matching $\}$ is denoted as $M P(G)$.

## The relation of the continuous and discrete set

## The relation of the continuous and discrete set

$M P(G)$ is a geometrical/continuous set of points, $\left\{\chi_{M}: M\right.$ is a matching $\}$ is a combinatorial/discrete set of points.

## The relation of the continuous and discrete set

$M P(G)$ is a geometrical/continuous set of points, $\left\{\chi_{M}: M\right.$ is a matching $\}$ is a combinatorial/discrete set of points.

$$
\left\{\chi_{M}: M \text { is a matching }\right\} \subset \operatorname{conv}\left\{\underline{\chi}_{M}: \text { Mis a matching }\right\}
$$

## The relation of the continuous and discrete set

$M P(G)$ is a geometrical/continuous set of points, $\left\{\chi_{M}: M\right.$ is a matching $\}$ is a combinatorial/discrete set of points.

$$
\left\{\chi_{M}: M \text { is a matching }\right\} \subset \operatorname{conv}\left\{\underline{\chi}_{M}: \text { Mis a matching }\right\}
$$

Usually extending the set of feasible solutions effects the optimization problem.

## The relation of the continuous and discrete set

$M P(G)$ is a geometrical/continuous set of points, $\left\{\chi_{M}: M\right.$ is a matching $\}$ is a combinatorial/discrete set of points.

$$
\left\{\chi_{M}: M \text { is a matching }\right\} \subset \operatorname{conv}\left\{\underline{\chi}_{M}: \text { Mis a matching }\right\}
$$

Usually extending the set of feasible solutions effects the optimization problem. In our problem this not the case.

## The relation of the continuous and discrete set

$M P(G)$ is a geometrical/continuous set of points, $\left\{\chi_{M}: M\right.$ is a matching $\}$ is a combinatorial/discrete set of points.

$$
\left\{\chi_{M}: M \text { is a matching }\right\} \subset \operatorname{conv}\left\{\underline{\chi}_{M}: M \text { is a matching }\right\}
$$

Usually extending the set of feasible solutions effects the optimization problem. In our problem this not the case.
$M P(G)$ convex, bounded, closed set.

## The relation of the continuous and discrete set

$M P(G)$ is a geometrical/continuous set of points, $\left\{\chi_{M}: M\right.$ is a matching $\}$ is a combinatorial/discrete set of points.

$$
\left\{\chi_{M}: M \text { is a matching }\right\} \subset \operatorname{conv}\left\{\underline{\chi}_{M}: \text { Mis a matching }\right\}
$$

Usually extending the set of feasible solutions effects the optimization problem. In our problem this not the case.
$M P(G)$ convex, bounded, closed set.
If we optimize a linear function on $M P(G)$ then the optimal value is obtained at a point $\underline{\chi}_{M}$ :

$$
\left\langle\underline{c}, \sum \lambda_{i} \underline{p}_{i}\right\rangle=\sum \lambda_{i}\left\langle\underline{c}, \underline{p}_{i}\right\rangle \leq \max \left\langle\underline{c}, \underline{p}_{i}\right\rangle .
$$

## Linear programming/LP

## Linear programming/LP

Solving

$$
\max \{\langle\underline{c}, \underline{x}\rangle: \underline{x} \in M P(G)\}
$$

is an LP problem.

## Linear programming/LP

Solving

$$
\max \{\langle\underline{c}, \underline{x}\rangle: \underline{x} \in M P(G)\}
$$

is an LP problem.
The standard usage of an LP algorithm requires the description of $M P(G)$ as an intersection of finitely many closed halfspaces (solution set of a system of linear inequalities).

## Linear programming/LP

Solving

$$
\max \{\langle\underline{c}, \underline{x}\rangle: \underline{x} \in M P(G)\}
$$

is an LP problem.
The standard usage of an LP algorithm requires the description of $M P(G)$ as an intersection of finitely many closed halfspaces (solution set of a system of linear inequalities).
Bellow we describe few linear inequalities that is satisfied by the vectors of $\left\{\chi_{M}: M\right.$ is a matching $\}$.

## Linear programming/LP

Solving

$$
\max \{\langle\underline{c}, \underline{x}\rangle: \underline{x} \in M P(G)\}
$$

is an LP problem.
The standard usage of an LP algorithm requires the description of $M P(G)$ as an intersection of finitely many closed halfspaces (solution set of a system of linear inequalities).
Bellow we describe few linear inequalities that is satisfied by the vectors of $\left\{\chi_{M}: M\right.$ is a matching $\}$.

## Definition

Let
$\widehat{M P}(G)=\left\{\underline{x} \in \mathbb{R}^{E(G)}: x_{e} \geq 0 \forall e \in E(G)\right.$, and $\left.\sum_{e: v l e} x_{e} \leq 1 \forall v \in V(G)\right\}$,
where $\underline{x}=\left(x_{e}: e \in E(G)\right) \in \mathbb{R}^{E(G)}$.

## The relation of the two polytope

## The relation of the two polytope

One inclusion is obvious

$$
M P(G) \subseteq \widehat{M P}(G)
$$

## The relation of the two polytope

One inclusion is obvious

$$
M P(G) \subseteq \widehat{M P}(G)
$$

In general the inclusion is strict.

## The relation of the two polytope

One inclusion is obvious

$$
M P(G) \subseteq \widehat{M P}(G)
$$

In general the inclusion is strict.
One example is $G=C_{2 k+1}$.

## The relation of the two polytope

One inclusion is obvious

$$
M P(G) \subseteq \widehat{M P}(G)
$$

In general the inclusion is strict.
One example is $G=C_{2 k+1}$.
Let $\underline{x} \in \mathbb{R}^{E(G)}$ the vector with all $\frac{1}{2}$ components. $\underline{x} \in \widehat{M P}(G)$ and $\underline{x} \notin M P(G)\left(\sum_{e \in E(G)} x_{e}=k+1 / 4\right.$ hyperplane separate $\underline{x}$ from $M P(G))$.

## The goal

## The goal

Our goal is to prove that if $G$ is a bipartite graph then $M P(G)=\widehat{M P}(G)$.

## The goal

Our goal is to prove that if $G$ is a bipartite graph then $M P(G)=\widehat{M P}(G)$.

It is enough to show that the vertices of $\widehat{M P}(G)$ have integer coordinates.

## The goal

Our goal is to prove that if $G$ is a bipartite graph then $M P(G)=\widehat{M P}(G)$.
It is enough to show that the vertices of $\widehat{M P}(G)$ have integer coordinates.
Indeed: The elements of $\widehat{M P}(G)$ with integer coordinates are exactly the set $\left\{\chi_{M}: M\right.$ is a matching $\}$ !

## The goal

Our goal is to prove that if $G$ is a bipartite graph then $M P(G)=\widehat{M P}(G)$.
It is enough to show that the vertices of $\widehat{M P}(G)$ have integer coordinates.
Indeed: The elements of $\widehat{M P}(G)$ with integer coordinates are exactly the set $\left\{\chi_{M}: M\right.$ is a matching $\}$ !

## The Lemma, that implies the Goal

## The Lemma, that implies the Goal

## Lemma

Let $\operatorname{Inc} c_{G} \in \mathbb{R}^{V \times E}$ be the vertex-edge incidence matrix of the bipartite graph $G$. Then each square submatrix $R$ of $\operatorname{Inc}_{G}$ has determinant $-1,0$, or 1 .

## The Lemma, that implies the Goal

## Lemma

Let $\operatorname{Inc}_{G} \in \mathbb{R}^{V \times E}$ be the vertex-edge incidence matrix of the bipartite graph $G$. Then each square submatrix $R$ of $\operatorname{Inc} c_{G}$ has determinant $-1,0$ or 1 .

If we want to see a generic vertex of $\widehat{M P}(G)$, then we take suitable $|E|$ defining inequalities of $\widehat{M P}(G)$. Substitute the inequality signs with equality signs. We obtain a system of linear equations, that has a unique solution.

## The Lemma, that implies the Goal

## Lemma

Let $\operatorname{Inc}_{G} \in \mathbb{R}^{V \times E}$ be the vertex-edge incidence matrix of the bipartite graph $G$. Then each square submatrix $R$ of $\operatorname{Inc}_{G}$ has determinant $-1,0$ or 1 .

If we want to see a generic vertex of $\widehat{M P}(G)$, then we take suitable $|E|$ defining inequalities of $\widehat{M P}(G)$. Substitute the inequality signs with equality signs. We obtain a system of linear equations, that has a unique solution.

The unique solution is the vertex, chosen.

## The Lemma, that implies the Goal

## Lemma

Let $\operatorname{Inc}_{G} \in \mathbb{R}^{V \times E}$ be the vertex-edge incidence matrix of the bipartite graph $G$. Then each square submatrix $R$ of $\operatorname{Inc}_{G}$ has determinant $-1,0$ or 1 .

If we want to see a generic vertex of $\widehat{M P}(G)$, then we take suitable $|E|$ defining inequalities of $\widehat{M P}(G)$. Substitute the inequality signs with equality signs. We obtain a system of linear equations, that has a unique solution.

The unique solution is the vertex, chosen.
To see the unique solution use Cramer's rule. Its coordinates are fractions of two determinants. The two determinants are integers, and the denominator is non-zero.

## The Lemma, that implies the Goal

## Lemma

Let $\operatorname{Inc}_{G} \in \mathbb{R}^{V \times E}$ be the vertex-edge incidence matrix of the bipartite graph $G$. Then each square submatrix $R$ of $I n c_{G}$ has determinant $-1,0$, or 1 .

If we want to see a generic vertex of $\widehat{M P}(G)$, then we take suitable $|E|$ defining inequalities of $\widehat{M P}(G)$. Substitute the inequality signs with equality signs. We obtain a system of linear equations, that has a unique solution.

The unique solution is the vertex, chosen.
To see the unique solution use Cramer's rule. Its coordinates are fractions of two determinants. The two determinants are integers, and the denominator is non-zero. By the Lemma the denominator must be $\pm 1$.

## The Lemma, that implies the Goal

## Lemma

Let $\operatorname{Inc}_{G} \in \mathbb{R}^{V \times E}$ be the vertex-edge incidence matrix of the bipartite graph $G$. Then each square submatrix $R$ of $I n c_{G}$ has determinant $-1,0$, or 1 .

If we want to see a generic vertex of $\widehat{M P}(G)$, then we take suitable $|E|$ defining inequalities of $\widehat{M P}(G)$. Substitute the inequality signs with equality signs. We obtain a system of linear equations, that has a unique solution.

The unique solution is the vertex, chosen.
To see the unique solution use Cramer's rule. Its coordinates are fractions of two determinants. The two determinants are integers, and the denominator is non-zero. By the Lemma the denominator must be $\pm 1$. This implies that the ratios are integers and the Goal is achieved.

## The proof of the Lemma

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $I n c_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $\operatorname{Inc}_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $I n c_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $\operatorname{Inc}_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column. Using the induction hypothesis we are done.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $\operatorname{Inc}_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column. Using the induction hypothesis we are done.

Case 2: Each column of $R$ has two 1's.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $I n c c_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column. Using the induction hypothesis we are done.

Case 2: Each column of $R$ has two 1's. // we know that one is in a lower row, and one in an upper row.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $\operatorname{Inc}_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column. Using the induction hypothesis we are done.

Case 2: Each column of $R$ has two 1's. // we know that one is in a lower row, and one in an upper row. This implies that the sum of lower rows of $R$ is the same as the sum of the upper rows.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $\operatorname{Inc}_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column. Using the induction hypothesis we are done.

Case 2: Each column of $R$ has two 1's. // we know that one is in a lower row, and one in an upper row. This implies that the sum of lower rows of $R$ is the same as the sum of the upper rows. This implies a non-trivial linear combination of rows gives $\overrightarrow{0}$.

## The proof of the Lemma

Let $R$ be a square submatrix of size $k \times k$.
We prove the claim with induction on $k$.
The case $k=1$ is obvious.
The rows of $\operatorname{Inc}_{G}$ (hence the rows of $R$ two) can be classified as lower and upper rows.

Case 1: $R$ has a column with at most one 1 . We can expand the determinant according to this column. Using the induction hypothesis we are done.

Case 2: Each column of $R$ has two 1's. // we know that one is in a lower row, and one in an upper row. This implies that the sum of lower rows of $R$ is the same as the sum of the upper rows. This implies a non-trivial linear combination of rows gives $\overrightarrow{0}$. That means the determinant of $R$ is 0 .

## Summary of our results

## Summary of our results

## Definition

A $M$ istotally unimodular, if each square submatrix of it has determinant 0 or $\pm 1$.

## Summary of our results

## Definition

A $M$ istotally unimodular, if each square submatrix of it has determinant 0 or $\pm 1$.

## Corollary

If $G$ is bipartite, then
a) $\operatorname{lnc}_{G}$ is totally unimodular,
b) $M P(G)=\widehat{M P}(G)$.

## The LP algorithm

## The LP algorithm

## Algorithm based on linear programming

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.
(Algebraization) Write down the linear inequalities describing $M P(G)=\widehat{M P}(G)$.

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.
(Algebraization) Write down the linear inequalities describing $M P(G)=\widehat{M P}(G)$. Introduce the objective function is $\langle w, x\rangle$

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.
(Algebraization) Write down the linear inequalities describing $M P(G)=\widehat{M P}(G)$. Introduce the objective function is $\langle w, x\rangle$
(Optimization) Solve the above LP problem (for example use the simplex method).

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.
(Algebraization) Write down the linear inequalities describing $M P(G)=\widehat{M P}(G)$. Introduce the objective function is $\langle w, x\rangle$
(Optimization) Solve the above LP problem (for example use the simplex method).
// The solution is guaranteed to be an integer solution. Hence it is a $0 / 1$ vector.

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.
(Algebraization) Write down the linear inequalities describing $M P(G)=\widehat{M P}(G)$. Introduce the objective function is $\langle w, x\rangle$
(Optimization) Solve the above LP problem (for example use the simplex method).
// The solution is guaranteed to be an integer solution. Hence it is a $0 / 1$ vector.
(Combinatorialization) We interpret the optimal solution a characterization of an edge set $M$.

## The LP algorithm

## Algorithm based on linear programming

Given an edge weighted graph. Let $w \in \mathbb{R}^{E(G)}$ the vector of the weights. Find the maximum weight matching.
(Algebraization) Write down the linear inequalities describing $M P(G)=\widehat{M P}(G)$. Introduce the objective function is $\langle w, x\rangle$
(Optimization) Solve the above LP problem (for example use the simplex method).
// The solution is guaranteed to be an integer solution. Hence it is a $0 / 1$ vector.
(Combinatorialization) We interpret the optimal solution a characterization of an edge set $M . M$ is the output.

## Thank you for your attention!

