Matching: Algebraic Algorithms, Polynomial Identity Testing, Schwartz-Zippel Lemma

Perfect Matching on a Bipartite Graph

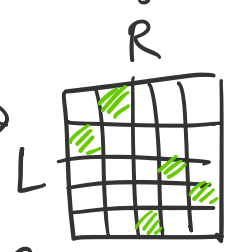
Given a bipartite graph with $|L| = |R|$, does there exist a perfect matching? $L = \{u_1 \dots u_n\}$, $R = \{v_1 \dots v_n\}$

Consider the adjacency matrix:

$$A = \begin{array}{c|c} & j \quad R \\ \hline i \; L & \boxed{} \end{array}$$

Consider $\det A$:

$$\det A = \sum_{\substack{\text{bijection} \\ \sigma:[n]\to[n]}} \underbrace{\text{sign}(\sigma)}_{\pm 1} \prod_{i \in [n]} A_{u_i v_{\sigma(i)}} \qquad A_{ij} = 1 \text{ if } (u_i, v_j) \in E, \ 0 \text{ otherwise.}$$



Each bijection $\sigma:[n]\to[n]$ is

① a potential matching in G

② an actual matching iff $\prod_{i \in [n]} A_{u_i v_{\sigma(i)}} = 1$.

<u>Ideal:</u> $\exists$ perfect matching in $G \overset{?}{\iff} \det A \neq 0$.

$\Leftarrow$ is true

$\Rightarrow$ can have false negatives from cancellation

Algorithm (Lovasz): A_{ij} = random number $\forall (u_i, v_j) \in E$.

Then $\exists$ PM in $G \Rightarrow \det A \neq 0$ with high proba

<u>Def</u>: the Edmonds matrix $E(G)$ is the symbolic matrix

$$E(G) = \begin{array}{c|c} & R \\ \hline L & \square \end{array}$$

$E(G)_{ij} = x_{ij}$ if $(u_i, v_j) \in E$, $\emptyset$ otherwise.

Then $\det E(G)$ is a polynomial in $\{x_{ij}\}$.

<u>Fact</u>: $\exists$ perfect matching in $G \iff \det E(G)$ is not the zero polynomial.

Polynomial Identity Testing: Given (multivariate) polynomial P (implicitly represented) decide whether P is the zero poly

Deterministic: open! solved $\Rightarrow BPP = P$

Randomized: if P has "low" degree, random assignments succeed w.h.p.

<u>Schwartz-Zippel Lemma</u>: Let $p(x_1, \dots, x_n)$ be a non-zero polynomial over a field $\mathbb{F}$, and let d be the degree of p. Consider any subset $S \subseteq \mathbb{F}$ and assign $x_i = r_i \sim R$ uniformly at random. Then

$$\Pr[p(r_1, \dots, r_n) = \emptyset] \leq \frac{d}{|S|}.$$

Remark: since $\det E(G)$ has degree $|L| = n/2$,
$\mathbb{F} = \mathbb{F}_p$ for $p \approx n^3$ and $S = \mathbb{F}$.
If $\det E(G) \neq \emptyset$ then $\det E(G)(r_{uv} : (u,v) \in E) \neq \emptyset$
with prob $\geq 1 - \frac{d}{} \geq 1 - \frac{n/2}{}$

If $\det E(G) \neq 0$ then $\det E(G)(r_{uv} : (u,v) \in E) \neq 0$
with prob $\geq 1 - \frac{d}{|S|} \geq 1 - \frac{n/2}{n^3}$

<u>Proof</u>: Induct on n (# variables).

$n=1$: $p(x)$ has $\leq d$ roots (Fund. Thm. of Algebra)

So $\Pr[x \sim S \text{ is a root}] \leq \frac{\#\text{roots}}{|S|} \leq \frac{d}{|S|}$.

$n>1$: Let k be the highest power of x_n^k in (the expansion of) $p(x_1, \dots, x_n)$. Write $p(x_1, \dots, x_n)$ as

$$p(x_1, \dots, x_n) = x_n^k \underbrace{q(x_1, \dots, x_{n-1})}_{\substack{\bullet \text{ no } x_n \text{ term since} \\ k \text{ was largest} \\ \bullet \text{ degree} \leq d-k.}} + \underbrace{r(x_1, \dots, x_n)}_{\text{highest power of } x_n^k \text{ is } \leq k-1}$$

Let $\mathcal{E}$ be the event that $q(r_1, \dots, r_{n-1}) = 0$.

$$\Pr[p(r_1, \dots, r_n) = 0]$$
$$= \underbrace{\Pr[p(r_1 \dots r_n) = 0 \mid \mathcal{E}]}_{\leq 1} \Pr[\mathcal{E}] + \Pr[\text{"} \mid \bar{\mathcal{E}}] \underbrace{\Pr[\bar{\mathcal{E}}]}_{\leq 1}$$
$$\leq \Pr[\mathcal{E}] + \Pr[\text{"} \mid \bar{\mathcal{E}}]$$

By induction, $\Pr[\mathcal{E}] \leq \frac{d-k}{|S|}$.

To bound $\Pr[\text{"} \mid \bar{\mathcal{E}}]$, observe that if $\bar{\mathcal{E}}$ then $p(r_1, \dots, r_{n-1}, x_n) = x_n^k q(r_1, \dots, r_{n-1}) + r(r_1, \dots, r_{n-1}, x_n)$ is a univariate polynomial in x_n of deg $\leq k$.

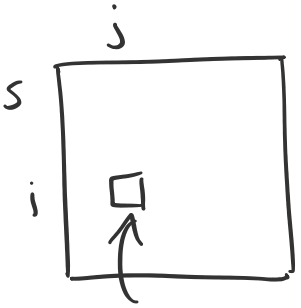
So $\Pr[\text{"} \mid \bar{\mathcal{E}}] \leq \frac{k}{|S|}$.

$\leq \frac{d-k}{|S|} + \frac{k}{|S|}$ completing the induction.

$\leq \frac{d-k}{|S|} + \frac{k}{|S|}$, completing the induction.

General Graphs

Def: the Tutte matrix $T(G)$ is



$V = \{v_1, \dots, v_n\}$

$$T(G)_{ij} = \begin{cases} \emptyset & \text{if } (v_i, v_j) \notin E \\ x_{ij} & \text{if } (v_i, v_j) \in E \text{ and } i < j \\ -x_{ij} & \text{if } (v_i, v_j) \in E \text{ and } i > j \end{cases}$$

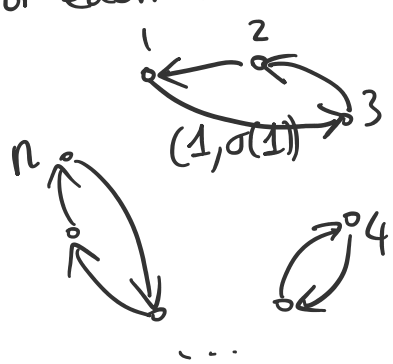
Fact: $\exists$ PM in $G \iff \det T(G) \neq \emptyset$.

Proof: ($\Rightarrow$) Let $\sigma : [n] \to [n]$ map $i \to j$, $j \to i$ for each $(v_i, v_j) \in M$

$$\prod_{i \in [n]} T(G)_{i,\sigma(i)} = \prod_{(v_i,v_j) \in M} (-x_{ij}^2).$$ Only this σ can produce monomial $\prod_{(v_i,v_j) \in M} x_{ij}^2$ so $T(G) \neq \emptyset$.

($\Leftarrow$) Suppose $\det T(G) \neq \emptyset$.

For each $\sigma : [n] \to [n]$, consider the permutation graph with arcs $(i, \sigma(i))$ $\forall i \in [n]$.



It's a disjoint union of cycles.

If all cycles even length, then get PM.

Otherwise $\exists$ odd cycle. Take the odd cycle containing

If all cycles even, done.
Otherwise $\exists$ odd cycle. Take the odd cycle containing the lowest index. Flip the cycle: get σ' s.t.

$$\text{sign}(\sigma)\prod_{i\in[n]} T(G)_{i,\sigma(i)} = -\,\text{sign}(\sigma')\prod_{i\in[n]} T(G)_{i,\sigma'(i)}$$

So σ, σ' cancel each other in $\det T(G)$.

Since $\det T(G) \neq 0$, $\exists\, \sigma$ with only even cycles.

<u>Red-Blue PMs</u>: <u>Only</u> algo is algebraic. (No det. algo!)

Given a bipartite graph with edges colored red/blue, find PM with exactly k red edges.

Algo: define matrix M: $M_{ij} = \begin{cases} 0 & \text{if } (v_i, v_j) \notin E \\ x_{ij} & \text{if } (v_i,v_j) \in E \text{ blue} \\ y x_{ij} & \text{if } (v_i, v_j) \in E \text{ red} \end{cases}$

$\exists$ PM in $G \iff \det M \neq 0$.

$\exists$ PM with exactly k red edges $\iff \det M$ has a monomial with y^k.

Write $\det M = y^k Q(\{x_{ij}\}) + \underbrace{R(\{x_{ij}\}, y)}_{\text{no } y^k \text{ term}}$

First, sample $x_{ij} \sim \mathbb{F}_p$.

By Schwartz-Zippel, with prob $\geq 1 - \frac{1}{\text{poly}(n)}$ $Q(\{r_{ij}\}) \neq 0$.

Now consider univariate $\det M(\{r_{ij}\}, y)$ on y.

Is coefficient of y^k nonzero?

Lagrange Interpolation: get entire polynomial!