LECTURE 13 7/1/2021

RANDOMIZED VERIFYING POLYNOMIAL IDENTITIES

Def: a polynomial P is identicaly 0 (notation: $P \equiv 0$), if all its coefficients are zero

(note: $x^2 - x$ in $\mathbb{Z}_2$ is not identicaly zero)

Test of identity: for P of degree n, trivialy in $O(n)$ time

BUT: sometimes - no direct access to the coefficients
- we need it faster (in parallel)

Def: for a multivariate polynomial $Q(x_1, \dots, x_n)$
degree of a term - the sum of exponents of the variables
total degree of Q - the maximum of the degrees of its terms

E.g., for $Q(x_1, x_2) = \underset{2}{x_1^2} + \underset{2}{x_1 x_2} + \underset{3}{2x_2^3} + \underset{0}{5}$ .... total degree $= 3$

Theorem: Let $P(x_1, \dots, x_n) \not\equiv 0$ be a polynomial over the field K of total degree d, and let $S \subseteq K$ be a non-empty finite subset, and let $r_1, \dots, r_n \in S$ be chosen independently uniformly at random. Then

$$\Pr[P(r_1, \dots, r_n) = 0] \leq \frac{d}{|S|}.$$

Proof: by induction on n

$n = 1$: as $P \not\equiv 0$, P has at most d distinct roots
$\Rightarrow$ at most d choices for r_1 s.t. $P(r_1) = 0$
$\Rightarrow \Pr[P(r_1) = 0] \leq \frac{d}{|S|}$

inductive step: Factor out the largest exponent of x_1 in P ... say k

$(*)$ $P(x_1, \dots, x_n) = x_1^k \underbrace{A(x_2, \dots, x_n)}_{\text{total degree } d-k} + B(x_1, x_2, \dots, x_n)$

degree of x_1 is $< k$

For any two events E and F:
$$\Pr[E] \leq \Pr[F] + \Pr[E / \bar{F}]$$
$$\left(\Pr[E] = \cancel{\Pr[E/F]} \cdot \Pr[F] + \Pr[E/\bar{F}] \cdot \cancel{\Pr[\bar{F}]}\right)$$

event $E = (P(r_1,\dots,r_n)=0)$, event $F = (A(r_2,\dots,r_n)=0)$

$$Pr[F] = Pr[A(r_2,\dots,r_n)=0] \le \frac{d-k}{|S|}$$

ind. assumption – A is poly. of $n-1$ variables

$$Pr[E|\bar{F}] = Pr[P(r_1,r_2,\dots,r_n)=0 \mid A(r_2,\dots,r_n)\neq 0] \le \frac{k}{|S|}$$

$P(x_1, \underbrace{r_2,\dots,r_n}_{\text{random choices}})$ .... univariate polynomial of degree k, and not identically 0, if $A(r_2,\dots,r_n)\neq 0$ see (*)

by ☼ : $Pr[E] \le \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}$ ∎

TEST for $P \equiv 0$? d = total degree of P

fix $S \subseteq K$ of size $2d = |S|$

randomly, ind. select $r_1,\dots,r_n \in S$

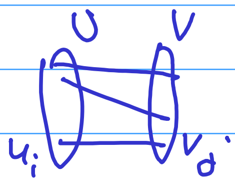
if $P(r_1,\dots,r_n) \neq 0$ then declare "$P \not\equiv 0$" ... always correct

otherwise declare "$P \equiv 0$" ... error prob. $\le \frac{1}{2}$

PARALLEL ALGORITHM FOR PERFECT MATCHING

Goal: $O(\log^2 n)$-time algorithm with $n^{O(1)}$ processors for G with n vertices, with error probability $\le \frac{1}{2}$.

BIBARTITE GRAPHS

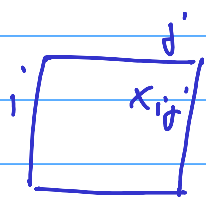


$G = (U,V,E)$, $U \cap V = \emptyset$, $E \subseteq U \times V$

assume $U = \{u_1,\dots,u_n\}$, $V = \{v_1,\dots,v_n\}$

Def: Edmond's matrix

$$A_{ij} = \begin{cases} x_{ij} & \text{...if } (u_i,v_j)\in E \\ 0 & \text{otherwise} \end{cases}$$



Theorem (Edmond's): $G=(U,V,E)$ with $|U|=|V|$ has a perfect matching $\iff \det(A) \not\equiv 0$.

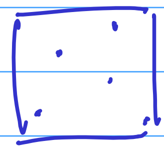
Proof:

by definition $\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot A_{1\pi(1)} \cdot A_{2\pi(2)} \cdots A_{n,\pi(n)}$

as each x_{ij} occurres at most once in A, there is no cancelation of terms in the summation

$\det(A) \not\equiv 0 \iff \exists\, \pi$ s.t. $A_{1\pi(1)} \cdot A_{2,\pi(2)} \cdots A_{n,\pi(n)} \neq 0$

$\iff \{(u_i, v_{\pi(i)}) \mid i=1,\dots,n\}$ is a perfect matching.



Verifying the existence of a perfect matching in bipartite graph can be done using the test for polynomial identities.

Fact: The determinant of $n \times n$ matrix with k-bit numbers can be computed in $O(\log^2 n)$-time with $O(n^{3.5} \cdot k)$ processors.

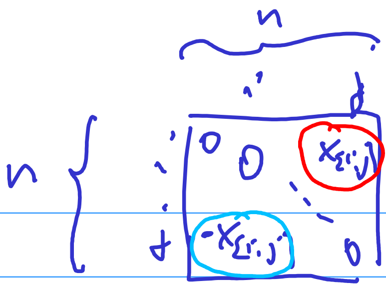
$\Rightarrow$ Test whether $G=(U,V,E)$ has a perfect matching can be implemented in $O(\log^2 n)$-time with $O(n^{3,5} \log n)$ processors with error probability $\leq \frac{1}{2}$ (or $\leq \frac{1}{2^k}$, if you run it k-times)

$\det(A)$ ---- $P(\overbrace{x_{11}, \dots \quad x_{nn}}^{n^2})$

$P \equiv 0$?

$r_{11}, r_{12} \dots \quad r_{nn}$

$$\begin{vmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ & & & \\ \dots & & \dots & r_{nn} \end{vmatrix}$$



GENERAL GRAPHS

$G=(V,E)$ $\quad V=\{1,\dots,n\}$

Def: Tutte's matrix

$$A_{ij}=\begin{cases} X_{\{i,j\}} & \text{if } \{i,j\}\in E,\ i<j \\ -X_{\{i,j\}} & \text{—''—},\ i>j \\ 0 & \text{if } \{i,j\}\notin E \end{cases}$$

Theorem (Tutte's): Graph $G=(V,E)$ has a perfect matching iff $\det(A)\neq 0$.

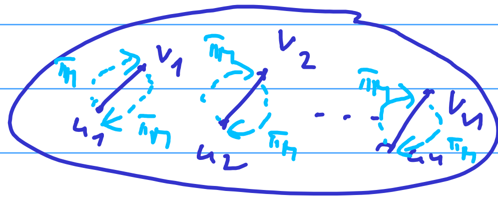
Proof:

$$\text{det } f_\pi=\prod_{i=1}^{n} A_{i,\pi(i)}$$

$\Rightarrow$ consider a perfect matching $M=\{\{u_1,v_1\},\dots,\{u_{\frac{n}{2}},v_{\frac{n}{2}}\}\}$

define π_M:

$$\pi_M(u_i)=v_i \quad \forall i$$
$$\pi_M(v_i)=u_i \quad \forall i$$



Then

$$f_{\pi_M}=\prod_{i=1}^{n/2} X_{\{i,\pi_M(i)\}}\cdot\left(-X_{\{i,\pi_M(i)\}}\right)=\prod_{i=1}^{n/2}\left(-X^2_{\{i,\pi(i)\}}\right)$$

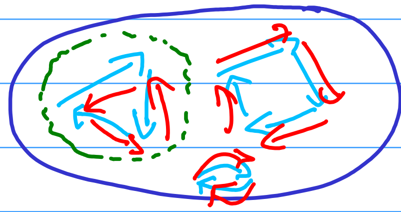
Note: there is no $\pi\in S_n$, $\pi\neq\pi_M$, s.t. $f_\pi=\pm f_{\pi_M}$

$\rightsquigarrow$ the term f_{π_M} has a non-zero coefficient

$\Rightarrow \det(A)\neq 0$.

$\Leftarrow$ $\det(A)\neq 0$

consider a $\pi\in S_n$ that contains an odd cycle

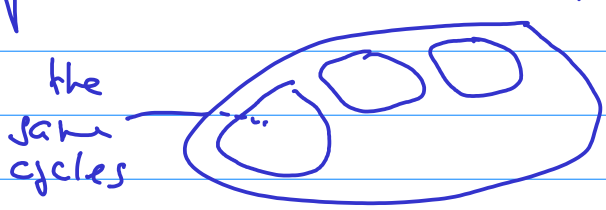


$\rightsquigarrow$ define π' .... same as π but going in the other direction on the odd cycle

note: $f_\pi=-f_{\pi'}$, $\text{sgn}(\pi)=\text{sgn}(\pi')$

Lemma (Contribution of π's with odd cycle)

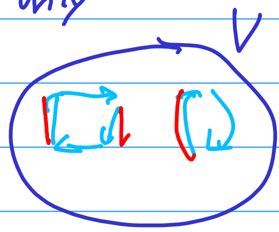
$$\sum_{\substack{\pi\in S_n,\\ \pi \text{ contains} \\ \text{odd cycle}}} \text{sgn}(\pi)\, f_\pi = 0$$



Proof – homework...

by the assumption $\det(A) \neq 0$ and Lemma

$\Rightarrow$ there is $\pi \in S_n$ consisting of even cycles only s.t. $f_\pi \neq 0$.

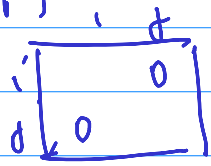


$\Rightarrow$ by selecting every other edge from each cycle in π, we get a perfect matching.

How to find a perfect matching? How to do it in parallel?

- Assume G has a unique perfect matching M;

How does the removal of an edge $\begin{cases} \{i,j\} \in M \\ \{i,j\} \notin M \end{cases}$ affect $\det(..)$? $\rightarrow$ goes to 0 / $\rightarrow$ remains $\neq 0$ $\Rightarrow$ We have a TEST!



- To get rid of the unrealistic assumption about unique perfect matching, we introduce random weights on edges, that ensure, w.h.p., unique min weight matching.

Lemma (Isolating lemma): Suppose that $\mathcal{F}$ is a family of subsets of a finite set $X = \{x_1, \dots, x_m\}$. Let $w : X \to \{1, 2, \dots, 2m\}$ be a positive weight function defined by assigning to each element of X a random weight chosen uniformly at random from $\{1, 2, \dots, 2m\}$. Then $\Pr[\text{there is a unique min weight set in } \mathcal{F}] \geq \frac{1}{2}$.

PARALLEL MATCHING ALGORITHM INPUT – $G = (V, E)$, $m = |E|$

1. $M = \emptyset$. For all edges $\{i,j\} \in E$ in parallel choose weight $w_{\{i,j\}} \in \{1, 2, \dots, 2m\}$, uniformly independently at random
2. Compute $\det(B)$ for the Tutte matrix B with $x_{\{i,j\}} = 2^{w_{\{i,j\}}}$
3. Find W s.t. 2^{2W} is the largest power of 2 dividing $\det(B)$
4. For all edges $\{i,j\} \in E$ in parallel compute $d = \det(B^{ij})$ where B^{ij} is B with ith & jth columns and rows deleted. If $(d \cdot 2^{2w_{\{i,j\}}})/2^{2W}$ is odd, add $\{i,j\}$ to M
5. For all vertices $i \in V$ in parallel check that $d_M(i) = 1$ (degree of i in M). If YES, then output M.

BONUS NOTES – not covered in class

Main Lemma (on weights and unique min weight PM):

Suppose that there is a unique minimum weight perfect matching in G and that its weight is W.

Then $\det(B) \neq 0$ and $\frac{\det(B)}{2^{2W}}$ is odd.

Moreover, an edge $\{i,j\} \in M \iff \frac{\det(B^{ij}) \cdot 2^{2w_{\{i,j\}}}}{2^{2W}}$ is odd.

As before: the matrix B is obtained from the Tutte matrix A by assigning $2^{w_{\{i,j\}}}$ for $x_{\{i,j\}}$, and B^{ij} is obtained from B by deletion of columns and rows i, j.

The lemma is a generalization of the Tuttes theorem and the proof goes along the same lines.

Proof of the Main Lemma: for $\pi \in S_n$, let $\text{value}(\pi) = \prod_{i=1}^{n} B_{i\pi(i)}$

$\text{value}(\pi) \neq 0 \iff \forall i \in V,\ \{i, \pi(i)\} \in E$

Note that each $\pi \in S_n$ corresponds to a set of vertex disjoint oriented cycles in G (orientation given by π)

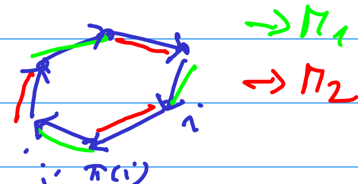
We say: π is odd if π contains ≥ 1 odd-lenght cycle
π is even if π contains only even-lenght cycles

Claim: $\sum_{\substack{\pi \in S_n, \\ \pi \text{ odd}}} \text{sgn}(\pi) \cdot \text{value}(\pi) = 0$

$\Rightarrow \det(B)$ is completely determined by even permutations.

(by 💡1)

Consider an even permutation $\pi \in S_n$ s.t. value$(\pi) \neq 0$. Then the set $\{\{i, \pi(i)\} \mid i \in V\}$ can be partitioned into two disjoint perfect matchings M_1, M_2, by considering alternating edges from each cycle (even!)



💡2 $|\text{value}(\pi)| = \left|\prod_{i=1}^{n} B_{i\pi(i)}\right| = \left|2^{\sum_{i=1}^{n} w_{\{i,\pi(i)\}}}\right| = 2^{w(M_1)+w(M_2)}$

by def. of value; def of B (where $w(M_k) = \sum_{e \in M_k} w(e)$, $k=1,2$)

Observe:

- if an even $\pi \in S_n$ s.t. value$(\pi) \neq 0$ contains a cycle of lenght 4 or more, then $M_1 \neq M_2$
  $\Rightarrow$ at most one of M_1, M_2 is the unique min weight PM
  $\Rightarrow$ $|\text{value}(\pi)| > 2^{2W}$

- if an even $\pi \in S_n$ s.t. value$(\pi) \neq 0$ contains cycles of length 2 only, then $M_1 = M_2$
  $\Rightarrow$ $|\text{value}(\pi)| \geq 2^{2W}$ and
  $|\text{value}(\pi)| = 2^{2W}$ iff $M_1 = M_2$ is the unique min weight PM

Thus • the absolute contribution of each even $\pi \in S_n$, s.t. value$(\pi) \neq 0$, is a power of 2, and at least 2^{2W}.
• exactly one $\pi \in S_n$ has contribution exactly 2^{2W}, in absolute value – – cannot be canceled out.

$\Rightarrow \det(B) \neq 0$

$\Rightarrow$ the highest power of 2 that divides $\det(B)$ is 2^{2W},

$\Rightarrow \dfrac{\det(B)}{2^{2W}}$ is odd

Recall: $B_{ij} = 2^{w_{\{i,j\}}}$, $B_{ji} = -2^{w_{\{i,j\}}}$

$$\text{value}(\pi) = \prod_{i=1}^{n} B_{i\pi(i)}$$

$$Q = \begin{array}{c|ccccc|} & i & & & j & \\ \hline i & 0 & \cdots & & B_{ij} & 0 \\ & \vdots & & & \vdots & \\ j & 0 & B_{ji} & \cdots & & 0 \\ & 0 & & & 0 & \\ \hline \end{array}$$

Consider now a fixed pair $\{i,j\}$.

Let Q be an $n \times n$ matrix derived from B by setting every value in the columns and rows i, j to zero, except for B_{ij} and B_{ji}

By expansion of $\det(Q)$ on the j-th column we get

☺3 $\det(Q) = -2^{2w_{\{i,j\}}} \cdot \det(B^{ij})$

As the contribution of every $\pi \in S_n$ with $\pi(i) \neq j$, or $\pi(j) \neq i$, to $\det(Q)$, we also have

$$\det(Q) = \sum_{\substack{\pi \in S_n, \\ \pi(i) = j, \\ \pi(j) = i}} \text{sgn}(\pi) \cdot \text{value}(\pi)$$

As in the analysis of the matrix B (see the previous pages) it is possible to show

- the total contribution of odd permutations to $\det(Q)$ is zero,
- if $\{i,j\} \in M$, then exactly one even permutation contributes exactly 2^{2W} (in abs. value) to $\det(Q)$
  & the absolute contribution of every other even $\pi \in S_n$, s.t. $\pi(i) = j$, $\pi(j) = i$ is $> 2^{2W}$

Thus, if $\{i,j\} \in M$, then $\det(Q) = 2^{2W} \cdot$ "something odd" $\overset{\text{by ☺3}}{=} -2^{2w_{\{i,j\}}} \cdot \det(B^{ij})$

$$\Rightarrow \frac{2^{2w_{\{i,j\}}} \cdot \det(B^{ij})}{2^{W}} \text{ is odd.} \quad (*)$$

For the other direction of the equivalence, we assume $(*)$ is odd, and for contradiction, also $\{i,j\} \notin M$

Then all even $\pi \in S_n$ with non-zero contribution to $\det(Q)$, contribute $> 2^{2W}$

$\Rightarrow \det(Q)$ is divisible by 2^{2W+1}

$\Rightarrow (*)$ is even - a contradiction.

end of proof of the Main Lemma ■

MISSING PROOFS - 1

8/1/2021

Lemma (Isolating lemma): Suppose that $\mathcal{F}$ is a family of subsets of a finite set $X = \{x_1, \dots, x_m\}$.
Let $w: X \to \{1, 2, \dots, 2m\}$ be a positive weight function defined by assigning to each element of X a random weight chosen uniformly at random from $\{1, 2, \dots, 2m\}$.
Then $Pr[$there is a unique min weight set in $\mathcal{F}] \geq \frac{1}{2}$.

Proof: assume, wlog, that every element $x \in X$ appears in at least one set $F \in \mathcal{F}$, and that no $x \in X$ appears in all sets from $\mathcal{F}$.

Fix an element $x \in X$ and define:

$$W = \min_{F \in \mathcal{F}: x \in F} \sum_{\substack{y \in F \\ y \neq x}} w(y), \quad \overline{W} = \min_{F \in \mathcal{F}: x \notin F} \sum_{y \in F} w(y), \quad \alpha = \overline{W} - W$$

assume that the weights of all elements, except for x, have been selected (principle of deffered choices)

Then: 1. for every weight $w(x) < \alpha$, every set not containing x has larger weight ($> W$) than the minimum weight set containing x

$\Rightarrow$ x must be in every min weight set

2. for every weight $w(x) > \alpha$, no min weight set contains x.

We say that the element x is ambiguous, if $w(x) = \alpha$

As the weights are chosen randomly independently,

$Pr[x$ is ambiguous$] \leq \frac{1}{2m}$ (if $\alpha \leq 0$, the prob. is $0 \leq \frac{1}{2m}$)

$\Rightarrow Pr[\exists$ an ambiguous $x \in X] \leq m \cdot \frac{1}{2m} = \frac{1}{2}$

i.e., with probability $\geq \frac{1}{2}$, no $x \in X$ is ambiguous

$\Rightarrow$ there is a unique min weight $F \in \mathcal{F}$ ∎

MISSING PROOFS - 2

Def: a permutation π is odd if it contains at leas one odd cycle

Lemma (Contribution of odd permutations, p.4)

$$\sum_{\substack{\pi \in S_n, \\ \pi \text{ is odd}}} \operatorname{sgn}(\pi) f_{\pi_1} = 0$$

Proof: For an odd permutation π, a canonical odd cycle is the odd cycle that is the longest, and that contains the smallest vertex (among the longest odd cycles)

For an odd permutation π, let $\overline{\pi}$ denote the odd permutation obtained from π by reversing the orientation of edges in the canonical cycle

💡1 : $\overline{(\overline{\pi})} = \pi$

💡2 : $\operatorname{sgn}(\pi) = \operatorname{sgn}(\overline{\pi})$

💡3 : $f_\pi = -f_{\overline{\pi}}$

$\Rightarrow$ the odd permutations can be paired (💡1) in such a way, that the contribution of each pair to $\det(B)$ is 0 (as $\operatorname{sgn}(\pi) \cdot f_\pi = -\operatorname{sgn}(\overline{\pi}) \cdot f_{\overline{\pi}}$, by 💡 2, 3) ∎

The same proof works for the Claim on p.6.