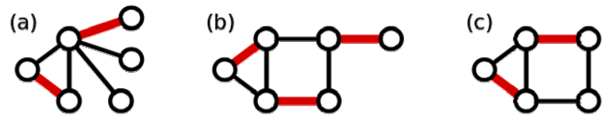
§5 Randomization: Motivation

Simple polyn.-time decision whether a (not necessarily bipartite nor planar) graph admits a perfect matching.

Let x_{ij}, $1 \le i < j \le n$, denote variables and consider Tutte's skew-symmetric *symbolic* matrix A_G with entries

$a_{ij} := x_{ij}$ if $\{i,j\} \in E$ and $i<j$
$a_{ij} := -x_{ji}$ if $\{i,j\} \in E$ and $i>j$
$a_{ij} := 0$ otherwise.



$\det(A_G) = \sum_\pi \mathrm{sign}(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot a_{3,\pi(3)} \cdots a_{n,\pi(n)}$

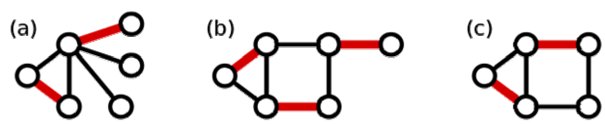
- is an n^2-variate integer polynomial of total degree n
- that can be *evaluated* using $O(n^3)$ tests & arith. op.s
- <u>is identically zero iff G has *no* perfect matching!</u>

Recall: *A perfect matching* in a graph $G=(V,E)$ of $|V|=2n$ vertices is a set $M \subseteq E$ of n edges without common vertices.

Lemma on Tutte's Determinant

$\det(A_G) = \sum_\pi \mathrm{sign}(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot a_{3,\pi(3)} \cdots a_{n,\pi(n)}$
is identically zero iff G has *no* perfect matching!

$a_{ij} := x_{ij}$ if $\{i,j\} \in E$ and $i<j$
$a_{ij} := -x_{ji}$ if $\{i,j\} \in E$ and $i>j$
$a_{ij} := 0$ otherwise.



Proof '⇒' A perfect matching is a permutation $\mu: V \to V$ s.t. $\forall i: \{i,\mu(i)\} \in E$ (*) and all cycles have length 2. Let $x_{i,\mu(i)} := 1$, $x_{ij} := 0$ for $j \ne \mu(i)$. Then $\det(A_G)(\underline{x}) = 1$ (why?)

'⇐' Let $\det(A_G) = \sum'_{\pi \text{ has odd cycle}} + \sum''_{\pi \text{ only of even cycles}}$
Then $\sum'_\pi \equiv 0$. Let π consist of only even cycles s.t. (*). This gives rise to a perfect matching.

negative sign

Recap: symmetry, cycle decompos., multivar. polyn.

Polynomial Identity Testing

KAIST CS500 M. Ziegler

$\det(A_G) = \sum_\pi \operatorname{sign}(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot a_{3,\pi(3)} \cdots a_{n,\pi(n)}$

- is identically zero iff G has *no* perfect matching;
- n^2-var. polyn., evaluated using Gauss.Elim. in $O(n^3)$

Recap (by example): The *total degree* of $x^2 \cdot y^3$ is 5.

Univariate polynom. of degree d has (at most) d roots.

Lemma (*Schwartz-Zippel*)**:** Fix domain D, finite $S \subseteq D$, and let $0 \neq p \in D[x_1,\ldots x_n]$ have total degree $\leq d$. Sample $r_1,\ldots r_n$ from S independently uniformly at random (*iid*).

Then (*) $\Pr[\, p(r_1,\ldots r_n)=0 \,] \leq d/|S|$.

Let j max s.t. $p_j \neq 0$

Proof (induct): $0 \neq p(x_1,\ldots x_n) = \sum_{0\leq j\leq d} p_j(x_1,\ldots x_{n-1}) \cdot x_n^j$

$(*) \leq \Pr[\, p_j(r_1,\ldots r_{n-1})=0] + \Pr[\, p(r_1,\ldots r_n)=0 \mid p_j(r_1,\ldots r_{n-1}) \neq 0]$

$\Pr[A] = \Pr[A \wedge B] + \Pr[A \wedge \neg B] \leq \Pr[B] + \Pr[A|\neg B] \cdot$ ~~$\Pr[\neg B]$~~

Error Amplification (Decision)

KAIST CS500 M. Ziegler

One-sided error:

Suppose algorithm $\mathcal{A}$, when reporting `true`, is always correct; but answer `false` may be erroneous with probability $p<1$.

Error probability p^k

k-times repeat $\mathcal{A}$; if all report `false`, report `false`.

Fact (Hoeffding): Let $X_1,\ldots,X_k$ be independent random variables in $[0;1]$, $\underline{X} := (X_1+\ldots+X_k)/k$. Then

$$\mathbb{P}[\ \underline{X} - \mathbb{E}[\underline{X}] \ \geq\ t\ ] \ \leq\ e^{-2kt^2}$$

Two-sided error:

Suppose algorithm $\mathcal{B}$ errs with probability $p<½$.

k-times repeat $\mathcal{B}$ and report the majority answer.

Markov Chain Algorithm for 3SAT

- 1-sided error: Suppose $\underline{z}$ is a satisfying assignment
- and $\underline{y}$ guessed in line 3 differs from $\underline{z}$ at ℓ places.
- After one iteration of innermost loop (lines 5 to 8):
- With probability ≥⅓ differs $\underline{y}$ only at $\leq \ell-1$ places.
- Loop arrives at $\underline{y}=\underline{z}$ with probability $\geq (⅓)^{\ell}$.
- Naïve choice $k:=\ell:=n/2$ and $K:=3^k$.
- Better $k:=\ell:=n/4$ and $K := 3^k \cdot 2^n / \binom{n}{k} \approx (1.5)^n$
- Current record $k:=3n$ and $K := (4/3^n)$

runtime $(1.33)^n \cdot \mathrm{poly}(n)$

```
1 Given 3CNF term φ(x_1,…,x_n)
2 Repeat K times:
3   Guess assignment y∈{0,1}^n
4   Repeat k times:
5       If φ(y)=1, accept and stop.
6       C be 1st clause in φ st C(y)=0
7       Guess a literal in C  (1 of 3),
8       flip its assigned value in y.
9 Reject!
```

$1/\binom{n}{cn} \approx c^{cn} \cdot (1-c)^{(1-c)n}$