Polynomial Identity Testing

Assume that P is given as a black box oracle

$$x \to \boxed{P} \to P(x)$$

??

$$\boxed{\forall x \; P(x) = Q(x)}$$

Given P, Q, check if $P(\cdot) = Q(\cdot)$

Aside

Why b.b.?

$$P(x) = (x+3)^{38}(x-4)^{83}$$

[Can expand BUT exponentially many terms]

Define $R(x) \equiv P(x) - Q(x)$

Check if $R(\cdot) = 0$?

Strategy: Try some values of x

Assume: $R(\cdot)$ has degree d

$$\Rightarrow R(x) = (x-\alpha_1)(x-\alpha_2) \cdots\cdots (x-\alpha_d)$$

IF $R(\cdot) \neq 0$

then only d inputs can make it 0

SO, try $(d+1)$ inputs ☺

Randomized:

For any set $S \subseteq F$

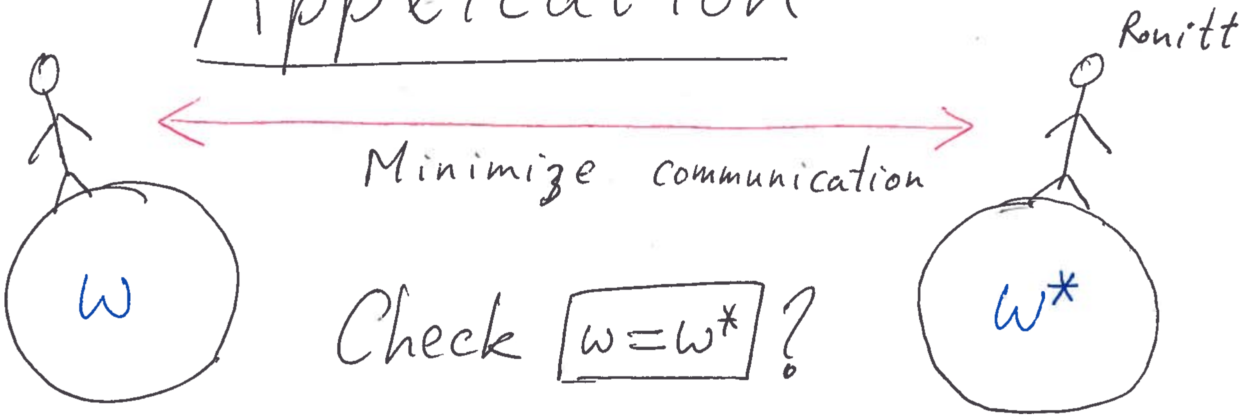
$> S$ contains $\leq d$ roots

$\Updownarrow$

Pick $x \in_R S$:

$$\underbrace{\mathbb{P}[R(x) = 0]}_{\text{Assuming } R(\cdot) \neq 0} \leq \frac{d}{|S|} \quad \left(\begin{array}{c}\text{Choose}\\ |S| = 2d\end{array}\right)$$

Application



$$w = \underbrace{w_1 \quad w_2 \quad w_3 \quad \cdots\cdots \quad w_n}_{\text{bits}}$$

coefficients of $P(x)$

$$\boxed{P(x) = \sum_{i=1}^{n} w_i \cdot x^i}$$

$$\boxed{P^*(x) = \sum_{i=1}^{n} w_i^* \cdot x^i}$$

Best deterministic algorithm requires

$\Omega(n)$ bits

(we get $\log n$)

Choose $x \in_R [1\ 2 \ldots 2n] = S$

Repeat $\log(n)$ times

Check if $P(x) = P^*(x)$?

Multi-variate Case

Check if $\underbrace{R(x,y)}_{\text{Infinitely many roots}} = 0 \quad \forall_{x,y}$?

Infinitely many roots ☹

Total degree :

> $\underbrace{2x}_{1} + \underbrace{3xy^2}_{1+2=3}$

Take the max $\boxed{3}$

> $\underbrace{xyz^3}_{1+1+3=5} + \underbrace{x^4}_{4}$

Take max: $\boxed{5}$

[Schwartz – Zippel] Lemma

$R(x_1, x_2, \ldots\ldots, x_n)$ has t. degree d over F

1. Pick $S \subseteq F$
2. Choose $r_1, r_2, r_3 \ldots\ldots r_n \in_R S$
3. $\mathbb{P}_{\langle r_1 \ldots r_n \rangle} \left[R(r_1 \ldots r_n) = 0 \right] \leq \frac{d}{|S|}$

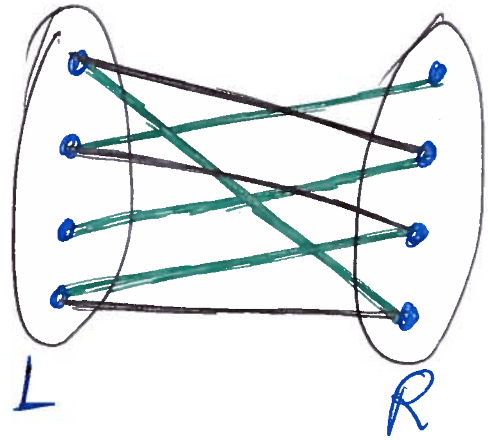
Assuming $R(\cdot) \neq 0$

Proof by induction on d

Behavior:

- $R(\circ) = 0$ Always detected
- $R(\circ) \neq 0$ Detected w.p. $\boxed{1 - \frac{d}{|S|}}$

Bipartite Perfect Matching



Green edges $\Rightarrow$ Perfect Matching

$|L| = n$ $\quad$ $|R| = n$

Matching: $M \subseteq E$

$\leftarrow$ No two edges share endpoint

Perfect Matching: Each vertex is represented

$\rightarrow$ Only possible if $|L| = |R|$

Q: Is there a perfect matching?

A: Can be solved using flows

Q: What if we want to solve in parallel?

(full discussion relegated to pset 2)

Tutte Matrix:

$$\boxed{A_G = \{a_{u,v}\}_{\substack{u \in L \\ v \in R}}}$$

Variable

$$a_{u,v} = \begin{cases} X_{u,v} & \text{if } (u,v) \in E \\ \boxed{0} & \text{o.w} \end{cases}$$

Polynomial on $\{X_{u,v}\}$

Claim: G has p.m. iff. $\mathrm{Det}[A_G] \neq 0$

Pf: $\mathrm{Det}[A_G] = \sum \underbrace{\mathrm{sign}(\sigma)}_{\text{(NOT important here)}} \prod_{i=1}^{n} a_{i,\sigma(i)}$

σ is a permutation of $[n]$

Notice: permutation σ (of $[n]$) $\longleftrightarrow$ Matching M

---

i — $\sigma(i)$ is an edge in the matching

$$\sum_{\substack{M \text{ is a } \cancel{\text{potential}} \text{ matching} \\ \text{in } G}} \underbrace{\mathrm{sign}(M)}_{\text{ignore}} \prod_{\substack{e \in M \\ e=(u,v)}} X_{u,v}$$

If σ is not a matching, then this is 0

$\Rightarrow$ Product is 0

Also Note: No cancellations!
(All monomials are distinct)

Why do this?

Det. polynomial has ($n!$) terms
(too many)

- Instead, use [Schwartz – Zippel]

- Det can be computed FAST!
  - $O(n^\omega)$ – sequential ($\omega \simeq 2.38\ldots$)
  - $O(\log^2 n)$ – parallel w/ poly(n) processors

DNF Sampling (OR of ANDs)

$\phi = (x_1 \wedge x_2) \vee (\neg x_2 \wedge x_3) \wedge \cdots\cdots$

$\phi = C_1 \vee C_2 \vee \cdots\cdots$

$\boxed{\begin{array}{ll} n & \text{variables} \\ m & \text{clauses} \end{array}}$

How to Satisfy?

Pick one clause & satisfy it!

DNF-SAT $\longrightarrow$ easy

Q: Find random satisfying assignment
uniformly

Strategy:

- Pick ~~random~~ arbitrary clause C_i
- Set vars in C_i to make it true
- Set other vars randomly.

Define $A_i = \{ \vec{x} \in \{0,1\}^n \mid \vec{x} \text{ satisfies } C_i \}$

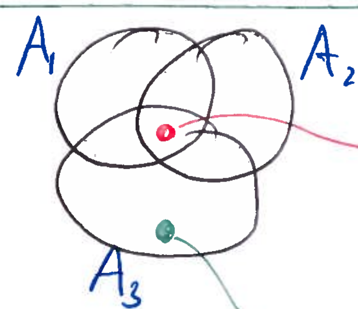
Strategy samples uniformly from A_i

Note: Can compute $|A_i| \rightarrow 2^{(\#\text{ vars not in } C_i)}$

Idea: 1. Choose $\boxed{i}$ w.p. $\dfrac{|A_i|}{\sum_{j=1}^{m} |A_j|}$

2. Return uniform sample from A_i

Problem: (not uniform)



This element is returned three times as often as this element

Solution: For a proposed $\boxed{\vec{x}}$

Let $C_{\vec{x}} = \underbrace{\left| \{ A_i \text{ s.t. } \vec{x} \in A_i \} \right|}_{\#\text{ of ways } \vec{x} \text{ can be returned}}$

3. Return $\boxed{\vec{x}}$ w.p. $\boxed{\dfrac{1}{C_{\vec{x}}}}$ Makes prob. of any $\vec{x}$ the same

Otherwise, try again (w.p. $1 - \frac{1}{C_{\vec{x}}}$)