Computational Complexity

Mohammad Mahmoody

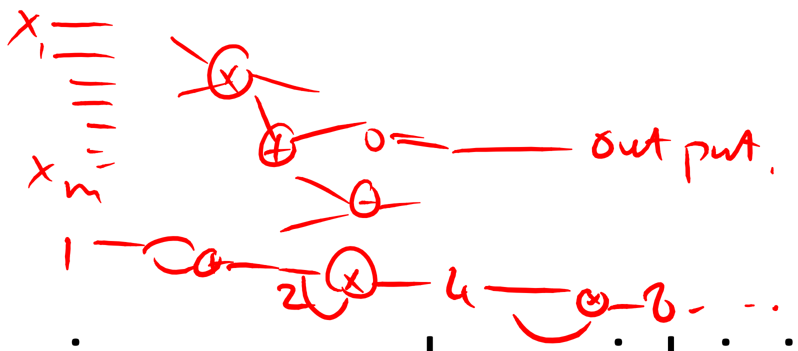
Session 24
April 2014

Polynomial Identity Testing: Where randomness seems to help

Q1 • Given a **two** polynomials: are they the **same**? given in form of circuits

P_1

P_2



$\prod_{i=1}^{n}(1+x_i)$

Q2 • Equivalent to: given one polynomial: is it **always zero**?

always zero.

$Q_2 \le_p Q_1$: given $\underline{(P_1)} \xrightarrow[\text{map}]{f(.)} \underline{(P_1, 0)}$

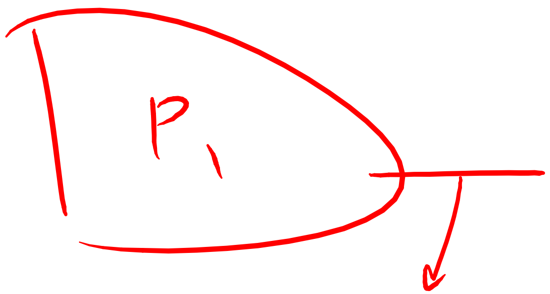
$Q_1 \le_p Q_2$; given $(P_1, P_2) \xrightarrow{\text{map}} (P_1 - P_2)$;

$(x_1+x_2)\cdot(x_3+x_4) = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$

Why not "opening up" the polynomial?

$\prod_{i=1}^{m}(1+x_i)$

given



$P_1(x_1 \dots x_m)$

$P_2(x_1 - x_m)$

Alg: go over gates $g_1 - - g_k$:

gives us $P_1(\cdot\cdot -)$: $2x_1x_2 + x_2^2x_3 + 4$

and $P_2(\cdot\cdot\cdot\cdot)$: $x_1x_2 + x_2x_3^2 + 4$

for $i=1$ to k

compute $P_1^i(\cdot)$ by looking at the polynomials of the input gates to g_i

if $P(\cdot) \equiv 0 \longrightarrow$ No $P(\cdot) \not\equiv 0 \longrightarrow$ yes

$= \alpha_0 + \alpha_1 x^1 + \alpha_2 x^2 \dots x$

Warm-up: Single Variable Polynomials

- Fact: every non-zero polynomial of degree d has at most d roots.

proof: if r is a root $p(r)=0 \Rightarrow$ divide $p(x)$ by $(x-r)$

$\Rightarrow \underbrace{q(x)}_{\text{smaller degree}}(x-r) = p(x)$

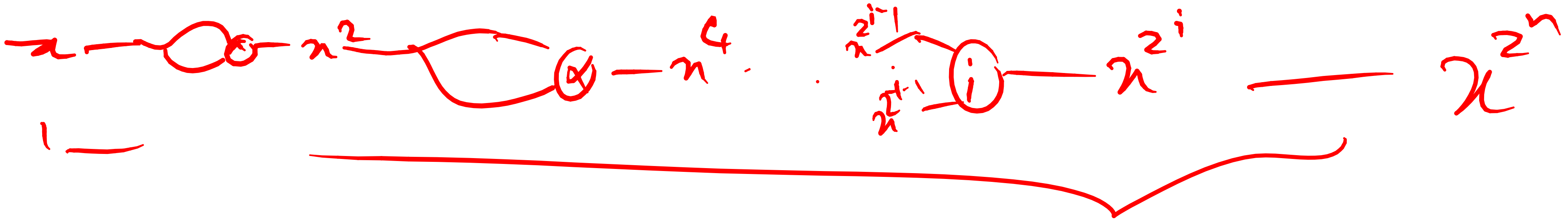
High level idea,

RP alg. { Compute $P(x)$ for a random x

{ if $P(x)=0 \longrightarrow$ always set 0 output

if $P(x) \neq 0 \longrightarrow$ for $\leq d$ possible x we get 0

Choose $x \in_R \{1,\dots,3d\} \Longrightarrow \Pr_x[P(x)=0] \leq \frac{1}{3}$



$d \le 2^n$

Alg:

Choose $x \xleftarrow{\$} \{1, \ldots, \underbrace{\overbrace{4d}^{2^{n+2}}}_{\approx 2^n}\}$

n gate

induction: the degree of $p_i(\cdot) \le 2^i$

$g_j \; g_k \to g_i$ $\begin{cases} \text{if } g_i = + \Rightarrow \deg \le 2^{i-1} \\ \text{if } g_i = \times \quad \deg \le 2^{i-1} + 2^{i-1} = 2^i \end{cases}$

Claim: $\deg(p(\cdot)) \le 2^k$ if $p(\cdot)$ is computed by a k-gate circuit

Multi-variable case:

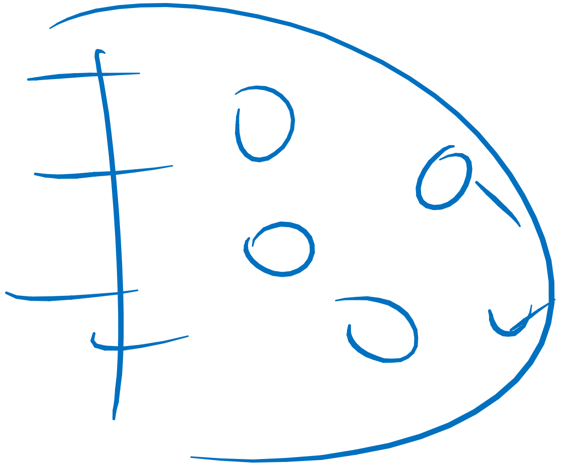
Lemma: let $p(x)$ be of degree $\leq d \Longrightarrow$ if choose $x \in S$ $\Pr[p(x)] \leq \frac{d}{|S|}$

Lemma 7.5 *Let $p(x_1, x_2, \ldots, x_m)$ be a nonzero polynomial of total degree*[6] *at most d. Let S be a finite set of integers. Then, if $a_1, a_2, \ldots, a_m$ are randomly chosen with replacement from S, then*

$$\Pr[p(a_1, a_2, \ldots, a_m) \neq 0] \geq 1 - \frac{d}{|S|}$$

Swartz-Zipple Lemma

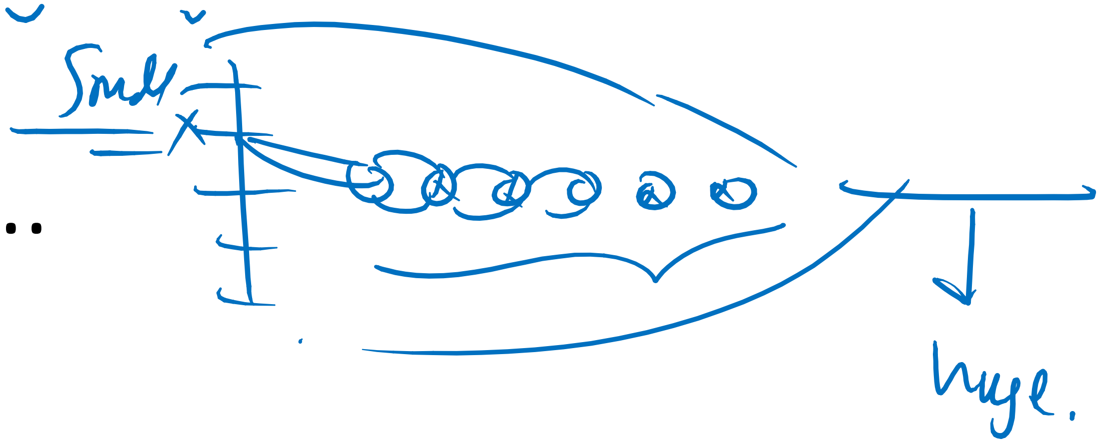
$[\quad \sim \quad = 0] \leq \frac{d}{|S|}$



Claim: the total deg $(p(\cdot)) \leq 2^n$

sub/add/mult. two number of d digits can be done in time $O(d^2)$

Issue: numbers grow fast...



digits for 2^{2^n}

is 2^n

$2^{2^n} = x^{2^n}$, $2^n = d$

---

hint. only care if $p(x) \neq 0$

work mod β $\left\{ \begin{array}{l} + \\ - \\ * \end{array} \right.$ keep remainder mod β

get $\boxed{p(x) \bmod \beta}$ $\downarrow$ α

if $\alpha \neq 0 \Longrightarrow p(x) \neq 0 \longrightarrow$ output yes

$2d$ digit : 2^{2d} { if $\beta \mid p(x) \Longrightarrow \boxed{\text{small}}$