Today

- Randomized Computation
- Examples
  * Primality
  * Polynomial Identity Testing
  * Matching
  * Quadratic Factorization

CSS.203.1 Computational Complexity

- Lecture #13 (31 Mar '21)

Instructor: Prahladh Harsha

'Tis best to live at random, as one can

- Sophocles

Randomized Computation

Motivating Examples:

(1) Primality

PRIME = $\{\langle n\rangle \mid n \text{ is prime}\}$

$\langle n\rangle$ - binary encoding of an integer.

Problem: Given a number n (in binary), determine if it is prime or composite?

2003: Agrawal, Kayal, Saxena (IIT Kanpur) deterministic algorithm for primality

Today, randomized algorithm for primality

- Miller-Rabin
- Solovay-Strassen

Solovay-Strassen Algorithm

n - integer positive.

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$ - which are co-prime to n.

n - prime.

$\mathbb{Z}_n$ - field - $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$

$\mathbb{Z}_n$ - ring $\left\{\begin{array}{l}\text{addition}\\ \text{multiplication}\end{array}\right.$ (all operations performed modulo n)

$\mathbb{Z}_n$ - field if n is prime.

n - prime. ($n \neq 2$)

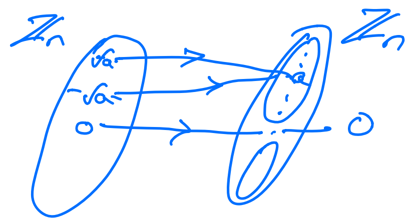
$\mathbb{Z}_n$. $\mathbb{Z}_n^* = \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$, is there an $x \in \mathbb{Z}_n^*$ s.t. $x^2 = a \pmod n$. ?

If it exists, there are exactly 2 square roots of a

$sq: \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n$

$x \longmapsto x^2$



n is prime.

$n = p$

$|\text{Image of } sq|$

p - odd.

$0 \quad \frac{p-1}{2} + 1$

$Im(sq) = \{0\} \cup QR(n)$

quadratic residue

$|QR(p)| = \frac{p-1}{2}$.

$a \in \mathbb{Z}_n^*$: a is quadratic residue if $a = x^2$ for some $x \in \mathbb{Z}_n$

o.w a is a non-quad residue.

Legendre Symbol: n - prime, a - any integer

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{n} \\ +1 & \text{if } a \pmod{n} \text{ is a } QR \text{ } \& \text{ } a \neq 0 \\ -1 & \text{if } a \pmod{n} \text{ is a non-}QR. \end{cases}$$

Fact: n is prime. & $(a,n) = 1$ (a is not a multiple of n)

$$\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod{n}$$

If a is QR, $a^{\frac{n-1}{2}} \equiv (x^2)^{\frac{n-1}{2}} \equiv 1 \pmod{n}$.

a is a non-QR: $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$

Extend Legendre symbol defn to non-prime odd n:

Jacobi Symbol:

$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$ (prime factorization)

$$\left.\left(\frac{a}{n}\right) \triangleq \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{k_i} \right\}$$ Jacobi Symbol.

Properties of Jacobi symbol:

1. $a \equiv b \pmod{n}$ $\quad \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

4. Quadratic Reciprocity Law.
   m & n - odd positive integers
   $$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{n-1}{2}}\left(\frac{n}{m}\right)$$

5. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ $\quad n$ - odd integer

$$\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right)(-1)^{\frac{9906}{2}}(-1)^{\frac{1000}{2}}$$

$$= \left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right)$$

$$= \left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right)$$

$$= \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) = \left(\frac{103}{37}\right)$$

$$= \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{2}{29}\right)^3 = -1$$

Conclusion: Jacobi Symbol $\left(\frac{a}{n}\right)$ can be computed efficiently in time $O(\log n \cdot \log a)$.

$\bar{n}$ - prime. $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$.

n - odd composite. $\exists a$, $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod{n}$

$$S_n = \left\{ a \in \mathbb{Z}_n^* \,\middle|\, \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n} \right\}.$$

Qn S_n - subgroup of $\mathbb{Z}_n^*$ (multiplicative)

n - odd composite, $|S_n| \leq \frac{|\mathbb{Z}_n^*|}{2}$

Motivates the SS algorithm.

On input n.

1. Pick $a \leftarrow_R \mathbb{Z}_n \setminus \{0\}$
2. Compute (a,n).
3. If $(a,n) \neq 1$, output composite.
4. If $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \pmod n$, output composite

   else output prime.

---

n - prime : For every a, SS outputs prime

$$\Pr_a [SS(n) = PRIME] = 1$$

n - composite : SS errs if $a \in S_n$

$$\Pr_a [SS(n) = PRIME] = \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}.$$

Polynomial Identity Testing

Qn: Give a multivariate poly $p \in \mathbb{F}[x_1, \dots, x_n]$.
(in some form), is

$$p \equiv 0 \; ?$$

Easy: p is given in monomial representation

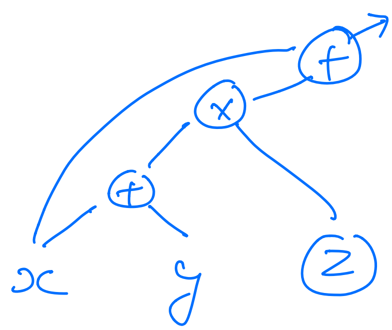
In some form:

$$p = \det\begin{pmatrix} x+x_2 & x_3+x_5 \\ 0 & x_8+6x_9 \end{pmatrix} \qquad \begin{pmatrix} x_1 & x_2' & x_1+x_2 \\ y_1 & y_2 & y_1+y_2 \\ z_1 & z_2 & z_1+z_2 \end{pmatrix}$$

- polynomial - presented as an arithmetic circuit.

Arithmetic Circuit

- Boolean Circuit (DAG).
- Inputs: $x_1 \dots x_n$, variables
  $0, 1,$ - field constants
- Gates: $\times$ - multiplication gate
  $+$ - addition gates

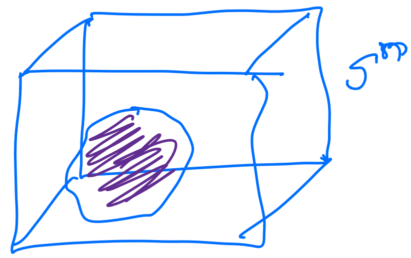


Schwartz-Zippel Lemma / Polynomial Identity Lemma

Let $p(x_1 \dots x_n) \in \mathbb{F}[x_1 \dots x_n]$ be a nonzero poly of total degree at most d.
$S \subseteq \mathbb{F}$, finite subset.

$$\Pr_{a \leftarrow S^n}\left[p(a)=0\right] \leq \frac{d}{|S|}$$

$(a_1 .. a_n) \leftarrow S \times .. \times S$



Proof: By induction

Base case : $n=1$ ✓

Assume it is true for $\leq n-1$

$$p(x_1 \dots x_n) = \sum_{t=0}^{e} x_1^t \, p_t(x_2 .. x_n)$$

$e \leq d$.

$$\Pr\left[p(a_1 \dots a_n)=0\right]$$

$$\leq \Pr\left[p_e(a_2 .. a_n)=0\right]$$

$$+ \Pr\left[\sum_{t=0}^{e} a_1^t \, p_t(a_2 .. a_n)=0 \,/\, p_e(a_2 .. a_n)\neq 0\right]$$

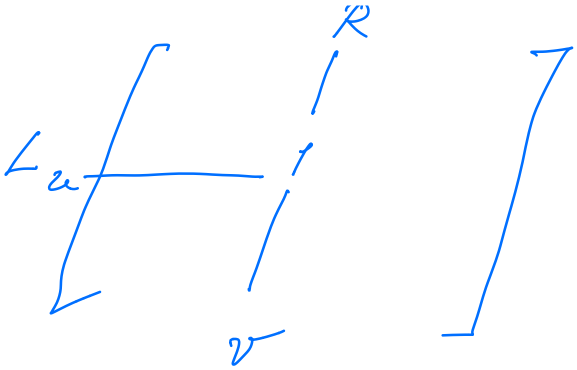
$$\leq \frac{d-e}{|S|} + \frac{e}{|S|} = \frac{d}{|S|}$$

$\boxtimes$

Matching.

Given: A bipartite graph $G=(L,R,E)$ w/ $|L|=|R|$, does G have a perfect matching.

BI MATCHING



Bipartite Adjacency Matrix

$$M(u,v) = \begin{cases} 0 & \text{if } (u,v) \notin E \\ 1 & \text{otherwise} \end{cases}$$

Consider $x_{u,v}$ for every $(u,v) \in E$

$$M(\bar{x})_{u,v} = \begin{cases} 0 & \text{if } (u,v) \notin E \\ x_{u,v} & \text{if } (u,v) \in E \end{cases}$$

Obs: $\det(M(x)) \equiv 0$ iff G does not have a perfect matching.

Let $|L| = |R| = n$.

Choose $S \subseteq \mathbb{Z}$ of size $10n$.

Lovasz Alg:

On input $G = (L, R, E)$

- Write $M(x)$
- Choose $S = \{1, 2, \dots, 10n\}$ $\quad n = |L| = |R|$
- $a \leftarrow_R S^{|E|}$
- Compute $z = \det(M(a))$

- Output Matching if $Z \neq 0$
  no-matching o.w.

No matching $\quad \Pr[\mathrm{Lov}(G) = \text{matching}] = 0$

Matching $\quad \Pr[\mathrm{Lov}(G) = \text{matching}] \geq \frac{9}{10}$

$\mathrm{Det} \in NC_2 \quad$; Bi-Matching $\in$ Randomized-NC.

Quadratic Polynomial Factorization (finding square roots).

- Next time.