Today

- Randomized Computation
- (quadratic factorization)
- RP, coRP, BPP
- Error Reduction

CSS.203.1
Computational Complexity
– Lecture #14
Instructor: (5 Apr '21)
Prahladh Harsha

Last time: Power of Randomness
- Primality
- Matching (Polynomial Identity Testing).
- Factorization of quadratic polynomials over finite fields.

Field – $\mathbb{F}_p$ (p - large prime, $p>2$)

Given: quadratic poly
$x^2 + cx + d$ $\quad c, d \in \mathbb{F}_p$

Goal: Find factorization if one exists.

- Cases:
  - (1) Irreducible
  - (2) $x^2+cx+d = (x-\alpha)^2$ for some $\alpha \in \mathbb{F}_p$
  - (3) $x^2+cx+d = (x-\alpha)(x-\beta)$ for $\alpha \neq \beta \in \mathbb{F}_p$

Obs: $x^p - x = \prod_{\alpha \in \mathbb{F}_p} (x-\alpha)$

(2) Identifying – perfect sq – easy

(1) $$\gcd(x^p - x,\ x^2+cx+d) = \begin{cases} 1 & \text{irreducible} \\ x-\alpha & \text{– perfect sq} \\ x^2+cx+d & \text{– linear distinct factors} \end{cases}$$

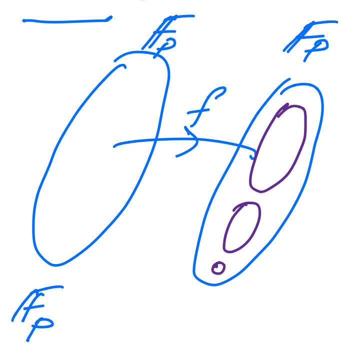
Suppose $x^2+cx+d = (x-\alpha)(x-\beta)$ for some $\alpha \neq \beta \in \mathbb{F}_p$

$p \neq 2$

$$x^p - x = \underbrace{x}_{0}\ \underbrace{\left(x^{\frac{p-1}{2}} - 1\right)}_{QR}\ \underbrace{\left(x^{\frac{p-1}{2}} + 1\right)}_{QNR}$$

Special Case: $\alpha \in QR;\ \beta \in QNR$

$$\gcd\left(x^2+cx+d,\ x^{\frac{p-1}{2}} - 1\right) = x-\alpha$$



$f_{a,b}: \mathbb{F}_p \to \mathbb{F}_p \qquad a, b \in \mathbb{F}_p$

$z \mapsto az+b$

$\alpha \mapsto a\alpha+b$

$\beta \mapsto a\beta+b$

$a\alpha+b$ – QR ; $a\beta+b$ – QNR

$$(x-(a\alpha+b))(x-(a\beta+b)) = x^2+c'x+d'$$

$c = -(\alpha+\beta) \qquad c' = -a(\alpha+\beta)+2b = ac+2b$

$d = \alpha\beta \qquad d' = (a\alpha+b)(a\beta+b) = a^2\alpha\beta + ab(\alpha+\beta) + b^2$

$= a^2 d - abc + b^2$

$x^2 + c'x + d'$

Idea: Pick a, b randomly

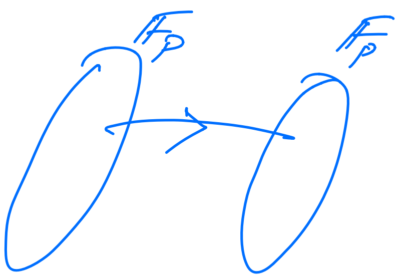
Fix $\alpha \neq \beta \in \mathbb{F}_p$

$$\Pr_{a,b}\left[a\alpha + b \in QR,\ a\beta + b \in QNR\right]$$

$\gamma, \delta \in \mathbb{F}_p$ (not necessarily distinct)

$$\Pr_{a,b}\left[\begin{matrix} a\alpha + b = \gamma \\ a\beta + b = \delta \end{matrix}\right] = \Pr_{a,b}\left[\begin{matrix} a(\alpha - \beta) = \gamma - \delta \\ a\alpha + b = \gamma \end{matrix}\right]$$

$$= \Pr\left[\begin{matrix} a = (\gamma - \delta)/(\alpha - \beta) \\ b = \gamma - a\alpha \end{matrix}\right] = \frac{1}{p^2}$$



$z \mapsto az + b$

For any 2 $\alpha \neq \beta \in \mathbb{F}_p$

$$\Pr\left[\begin{matrix} f_{a,b}(\alpha) = \gamma \\ f_{a,b}(\beta) = \delta \end{matrix}\right] = \frac{1}{p^2}$$

$$\Pr_{a,b}\left[\begin{matrix} f_{a,b}(\alpha) \in QR \\ f_{a,b}(\beta) \notin QR \end{matrix}\right] = \sum_{(\gamma,\delta) \in QR \times QNR} \frac{1}{p^2}$$

$$= \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\frac{1}{p^2} = \frac{1}{4}\left(1 - \frac{1}{p^2}\right)$$

$$\Pr_{a,b}\left[\begin{matrix} f_{a,b}(\alpha) \notin QR \\ f_{a,b}(\beta) \in QR \end{matrix}\right] = \frac{1}{4}\left(1 - \frac{1}{p^2}\right)$$

$$\Pr_{a,b}\left[\begin{array}{l}\text{One root of } x^2+c'x+d' \text{ is} \\ \text{QR \& the other is QNR}\end{array}\right] = \frac{1}{2}\left(1-\frac{1}{p^2}\right)$$

$$\geq \frac{1}{2}\left(1-\frac{1}{9}\right)$$

Input: x^2+cx+d.

1. $\gcd(x^2+cx+d,\ x^p-x)$
2. If gcd is x^2+cx+d.

   Pick $a,b \leftarrow_R \mathbb{F}_p$

   $c', d' \leftarrow$

   If $\gcd(x^2+c'x+d',\ x^{\frac{p-1}{2}}-1)$ is linear

   we have obtained a factor.

   else

Probabilistic Complexity Classes

RP, BPP, coRP, ZPP.

Probabilistic TM: similar to a NTM

δ_0, δ_1: transition functions.

RP: Randomized Polynomial time

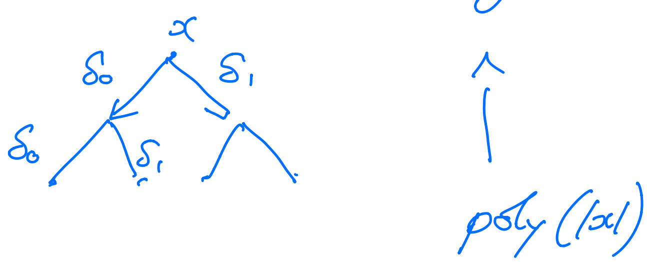
$L \in RP$ if there exists a PTM (ie, a prob. TM) M s.t.

$$x \in L \Rightarrow \Pr_M[M(x) = \text{accept}] \geq 2/3$$

$$x \notin L \Rightarrow \Pr_M[M(x) = \text{accept}] = 0$$

RP - one-sided error

& furthermore M runs in fixed poly time (irrespective of random choices)



$coRP = \{L \mid \bar{L} \in RP\}$

coRP: $x \in L \Rightarrow \Pr[M(x) - \text{accepts}] = 1$

$x \notin L \Rightarrow \Pr[M(x) - \text{accepts}] \leq 1/3$

BPP: $x \in L \Rightarrow \Pr[M(x) - \text{accepts}] \geq 2/3$

$x \notin L \Rightarrow \Pr[M(x) - \text{accepts}] \leq 1/3$

Alternate viewpoint:

Two types of input: x - actual input

r - random input.

M- deterministic TM.

RP: $L \in RP$ if there exists a DTM M that runs in poly time:

$x \in L \Rightarrow \Pr_r[M(x,r) = \text{accept}] \geq 2/3$

$x \notin L \Rightarrow \forall r, M(x,r) \neq \text{accept}$

Key point: RP, coRP, BPP

- machines run in a fixed poly time (irrespective of random i/p) but may err w/ some prob

Note: quad factorization

- Zero error
- expected poly time

ZPP: (zero error prob. polynomial time).

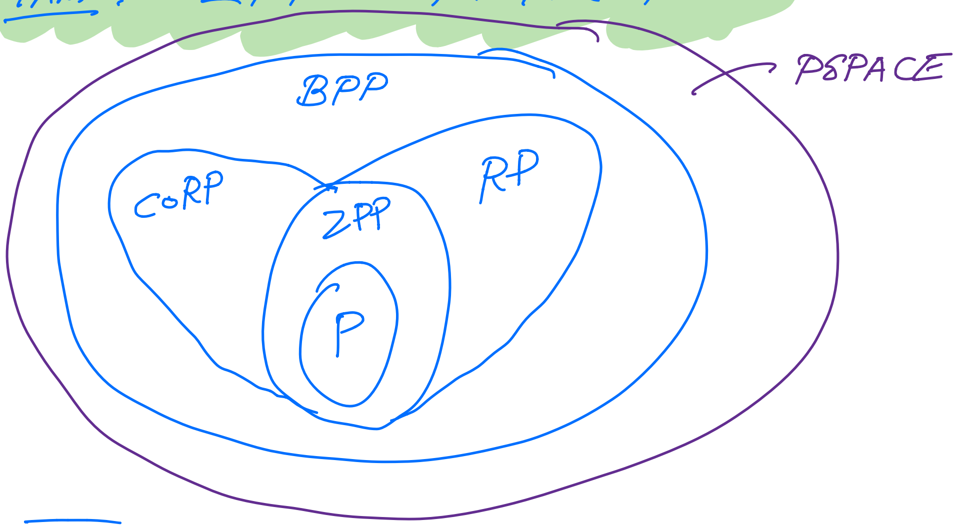
$L \in ZPP$ if a prob. TM M. s.t.

$\forall x, \quad \Pr_M[M(x) = L(x)] = 1$ (no error)

$E[\text{running time of } M \text{ on } x] \leq poly(|x|)$.

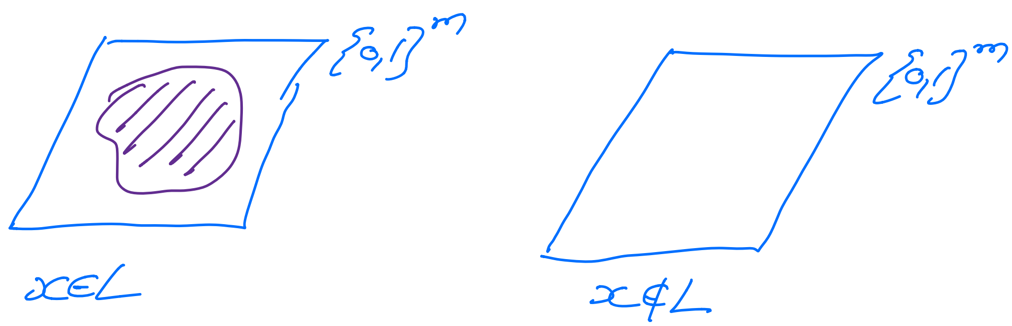
Obs: $ZPP \subseteq RP \cap coRP$

Thm: $ZPP = RP \cap coRP$



Error Reduction:

RP_ρ: $x \in \{0,1\}^n$, $r \in \{0,1\}^m$



$$ACC(x) \triangleq \{r \mid M(x,r) = accept\}$$

$$x \in L \Rightarrow |ACC(x)| \geq \rho \cdot 2^m$$

$$x \notin L \Rightarrow |ACC(x)| = 0$$

Given $L \in RP_\rho$, ie there exist a PTM that accs w/ prob ρ in YES, 0 in NO.

RP - Error Redn

$\underline{\underline{M_t}}$: 1. Run the RP m/c independently for t times

2. Acc if any of the runs acc & reject otherwise.

$x \in L \Rightarrow \Pr[M_t(x)\text{-accepts}] = 1-(1-p)^t$

$x \notin L \Rightarrow \Pr[M_t(x)\text{-accepts}] = 0$

$RP_{1/n^c} = RP_{2/3}$ for all constant c

$= RP_{1-1/2^{n^d}}$ $\forall d$.

BPP - error reduction

BPP : $\forall x, \Pr_r[M(x,r)\text{-errs}] \leq 1/3$

& M runs in fixed poly time.

$BPP_{\frac{1}{2}-\varepsilon}$: $\forall x : \Pr_r[M(x,r)\text{-errs}] \leq \frac{1}{2}-\varepsilon$

& M runs in fixed poly time.

$BPP \stackrel{\Delta}{=} BPP_{1/3}$

As in RP.

$\forall c, \; BPP_{1/2 - \frac{1}{n^c}} = BPP_{1/3}$

$= BPP_{1/2^{n^d}} \; \forall d.$ $\Bigg\}$ Consequence of Chernoff Bound.

M_t: On input x

1. Pick $r_1 \ldots r_t$
2. Run $M(x, r_1) \ldots M(x, r_t)$
3. Accept if a majority of them accept & reject otherwise. $\boxtimes$