# Randomized Computation

NSPACE
PSPACE = coPSPACE

oracle TM — PH — hierarchy essn — Nice collapsing prop
pure imagination but captured constant-round debates/games

CONP — NP — unintuitive non deterministic comp$^n$, but captured problems we cared
One sided
NL = CONL

P — eff computation

P/poly

L — space resource

One thing was missing, arguably even more natural at capturing eff comp$^n$ then P.

## Randomized Computation.

Eg: Find a quadratic non-residue.

This is a functional problem.

$\mathbb{Z}_p \equiv \mathbb{Z}$ mod prime $p$ (odd)
collection of remainders/Residue.

- is a field
  - addition
  - multiplication
  - divison (of non-zero elements)
- ring (add$^n$, mult$^n$)

We say $a \in \mathbb{Z}_p^*$ is a quadratic residue if $\exists\ b \in \mathbb{Z}_p^*$ s.t. $b^2 = a$.

Consider the following map:

$$\psi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$
$$x \longrightarrow x^2$$

(this is a homomorphism) $\psi(xy) = \psi(x)\cdot\psi(y)$




2 to 1 map

$\Rightarrow \exists\ \frac{p-1}{2}$ quadratic residues

Everything not in the image($\psi$) is a quadratic non residue (qNR).

$\frac{p-1}{2}$ qns.

So, if $\mathbb{Z}_p^*$ $\frac{1}{2}$ qr, $\frac{1}{2}$ qnr

Q// Given $p$, find a qnr in $\mathbb{F}_p^*$ or $\mathbb{Z}_p^*$ in poly(log p) time.

- Randomized algo. Pick a random element.
- Det algo (Open).




(Not to scale)

Can you think of a way to traverse through $\mathbb{Z}_p^*$ to get a non-residue in poly(log p) steps?

**Notation**: Lengendre Symbol.

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 0 & \text{if } a \equiv_p 0 \\ 1 & \text{if } a \text{ is qr} \\ -1 & \text{if } a \text{ is qnr.} \end{cases}$$

$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$ when $p$ is odd prime.

Note $a^{p-1} \equiv_p 1 \quad \forall\ a \in \mathbb{Z}_p^*$

sqrt 1 is 1 or −1.

What about decision problem?

① Primality Testing

PRIMES = $\{ \langle n \rangle_2 \mid n \text{ is prime} \}$

Q// Given $n$, check if its a prime? in binary.

$\mathbb{Z}_n \equiv$ residues/remainders modulo $n$.

This is a ring not a field.
$\mathbb{Z}_6 \ni 2\cdot 3 = 0$ no inverse for 2 or 3.

$$\boxed{a^{n-1} \equiv_n 1 \quad \forall\ a \in \mathbb{Z}_n \setminus \{0\} \text{ iff } n \text{ is a prime.}}$$

Extending quadratic residues to non-primes.

$$\psi : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$x \longmapsto x^2$$

$a \in \mathrm{Im}(\psi) \subseteq \mathbb{Z}_n^*$ is a quad-residue (n)

$\Updownarrow$

$\exists\ b$ s.t. $a \equiv b^2 \mod n$.

Jacobi Symbol $\quad n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$

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

$a^{\phi(n)} \equiv_n 1 \qquad a \in \mathbb{Z}_n^*$

Computing $\phi(n) \equiv$ factoring $n$
(Excercise) — polytime reducible

Properties of Jacobi Symbol

1. $a \equiv_n b \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ multiplicative
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

Q// What if $a \notin \mathbb{Z}_n^*$, $\left(\frac{a}{n}\right)$?

4. Quadratic Reciprocity Law.
   $m, n$ odd pos. $\mathbb{Z}$.
   $$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}} (-1)^{\frac{n-1}{2}} \left(\frac{n}{m}\right) \quad \text{flipped}$$
5. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ $\quad n$ - odd

Compute $\left(\frac{1001}{9907}\right)$.

Conclusion: Jacobi symbol can be compute in $O(\log n \cdot \log a)$ time.

Randomized algo for PRIMALITY

$n$ - odd composite
$\exists\ a$ s.t. $\left(\frac{a}{n}\right) \neq_n a^{\frac{n-1}{2}}$.

$S_n = \{ a \in \mathbb{Z}_n^* \mid \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \mod n \}$
is a subgroup of $\mathbb{Z}_n^*$ (group theory)

$|S_n| \leq \frac{|\mathbb{Z}_n^*|}{2}$

Solvay-Strassen Algorithm.

1. Pick $a \in \mathbb{Z}_n \setminus \{0\}$ randomly.
2. Compute $\gcd(a, n)$
3. If $(a,n) \neq 1$ output composite
4. If $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \mod n$ output composite
   else prime

If $n$ is prime
$\Pr_a [SS(n) = \text{prime}] = 1$

$n$ - composite

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

Work for all $n$ (WHP) not some/most $n$.

---

## Polynomial Identity Testing.

Q// Given a multivariate poly $f \in \mathbb{F}[x_1, \ldots, x_n]$ test if $f \equiv 0$?

Polynomial-Identity = $\{ f \in \mathbb{F}[x_1, \ldots, x_n] \mid f \equiv 0 \}$

Representation of polynomials
- Such reps$^n$ ensure
  - Arithmetic/Algebraic Circuits/Determinants.

JEE Put value method.

- Size of the input.
- Univariate instance.

- Univariate degree $d$ polynomial has atmost $d$ roots.

$f = f_d y^d + f_{d-1} y^{d-1} + \cdots + f_0$

Multivariate Extension of this

Schwartz Zippel / PIT Lemma
total-degree $d$.

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

$(a_1, a_2, \ldots, a_n) \leftarrow S \times S \times \cdots S$

$\Pr_{a_1 \ldots a_n} [f = 0] \leq \Pr[f_d = 0] + \Pr[f \mid f_d \neq 0]$
$\leq \frac{d-e}{|S|} + \frac{e}{|S|} = \frac{d}{|S|}$ $\square$

Combinatorial nullstellsatz

Matching

# Issue with Fermat Primality Test

Note $N = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{k_1}}^* \otimes \mathbb{Z}_{p_2^{k_2}}^* \otimes \cdots \otimes \mathbb{Z}_{p_m^{k}}$$

CRT

$\mathbb{Z}_n^*$ is not-necc. cyclic group

In $\mathbb{Z}_p^*$ there exist a generator

$\alpha \in \mathbb{Z}_p^*$ st $\mathrm{Ord}(\alpha) = p-1$

$\alpha^{p-1} = 1$ (and no smaller)

$n = pq$

$$\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \otimes \mathbb{Z}_q^*$$

the max order of $\alpha \in \mathbb{Z}_n^*$

is $\mathrm{lcm}(p-1, q-1)$

and not

## Carmichael numbers

$n = 561$
$= 3 \cdot 11 \cdot 17$

$$\mathbb{Z}_{561}^* \cong \mathbb{Z}_3^* \otimes \mathbb{Z}_{11}^* \otimes \mathbb{Z}_{17}^*$$

max order here $\mathrm{lcm}(2, 10, 16) = 80$.

and $80 \mid 560$, thus $\forall \alpha \in \mathbb{Z}_{561}^*$

satisfy $\alpha^{560} = 1 \mod 561$.

[[Fact]] There are $\infty$ many carmichael numbers.

$$\frac{|\mathbb{Z}_n^*|}{|\mathbb{Z}_n|} \to 1 \quad \text{as } n \to \infty$$

# Randomized Complexity Classes.

PTM : TM M with two trans$^n$ f$^n$ $\delta_0, \delta_1$

- Every step choosen ind. at random $\delta_0$ or $\delta_1$

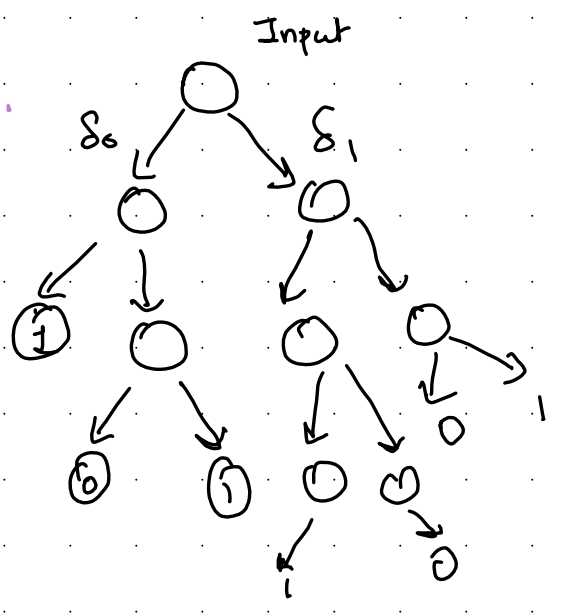
(only accpt/Rej)

- $M(x)$ is a r.v. "output".
- $T: \mathbb{N} \to \mathbb{N}$, M stops in $T(|x|)$ steps, for any x, for any random choice.

We say PTM M decides $L \subseteq \{0,1\}^*$ in time $T(n)$ if $\forall x \in \{0,1\}^*$

① $\Pr[M(x) = L(x)] \geq 2/3$

② M halts in $T(|x|)$ regardless of random choice.




## BPP

$BPTIME(T(n)) \equiv$ Lang. decidable by PTM in $O(T(n))$ time.

$$BPP = \bigcup_{c \geq 1} BPTIME(n^c).$$

Note : Consistency check we want things to work on all inputs. Although any such variation for most inputs w/ or w/o randomness makes sense $\equiv$ average case complexity.

If Not a fan of NTM, here is another alternate (equiv) def$^n$ of BPP.

$L \in BPP$ if $\exists$ poly time (deterministic) TM M and $p: \mathbb{N} \to \mathbb{N}$ (poly-bounded) s.t. $\forall x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{p(|x|)}} [M(x,r) = L(x)] \geq 2/3$$

Q// What the error in yes/no case for PIT/ Primality?

In SS, if n is a prime (yes instance) No error

In PIT, s

This motivates prob. algorithms / classes. w/ one sided error.

RTIME(T(n)) : $L \in RTIME(T(n))$ if there is a PTM M running in time $T(n)$ s.t.

$$x \in L \implies \Pr(M(x) = 1) \geq 2/3$$
$$x \notin L \implies \Pr[M(x) = 1] = 0$$

$$RP = \bigcup_{c>0} RTIME(n^c).$$

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

Equiv : Error free on accpt, some error on reject.

Zero-sided Error

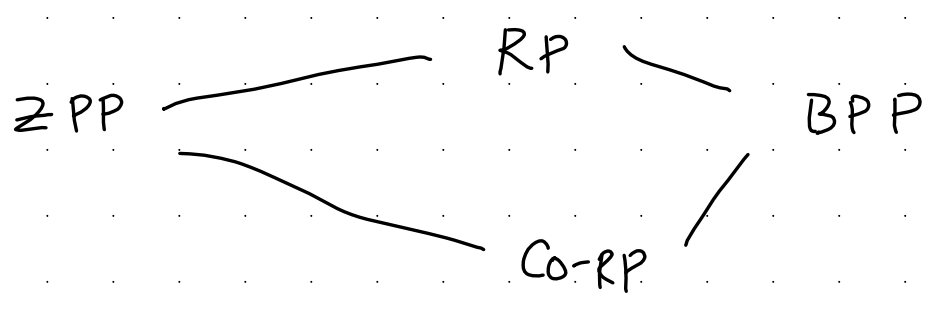
For a PTM M,

Let $T_{M,x}$ be a r.v.

$\Pr_{\text{random choice}}[T_{M,x} = T] = p$ if w/ prob p over randomness, M will halt on x in $T(|x|)$ steps.

▷ If no error and Expected run time $O(T(|x|)) \equiv ZTIME(T(n))$

$$ZPP = \bigcup_{c>1} ZTIME(n^c).$$




In fact, Theorem $ZPP = RP \cap Co\text{-}RP$. (Exercise)

# Error Reduction in BPP.

$$BPP_{\frac{1}{2}+n^{-c}} = BPP_{2/3} = BPP_{\frac{1}{2}+2^{-n}}$$

≡ with succ. prob.

We can transform a machine w.s.p. $\frac{1}{2}+n^{-c}$ into machine w.s.p $2/3$. We can convert it to exponentially close to 1.

<u>Thm</u>: Let $L \subseteq \{0,1\}^*$ decidable by PTM $M$ (polytime) s.t. $\forall\, x \in \{0,1\}^*$

$$\Pr[M(x) = L(x)] \geq \frac{1}{2} + |x|^{-c}$$

Then for every const. $d > 0$ $\exists$ PTM $M'$

s.t. $\forall\, x \in \{0,1\}^*$, $\Pr[M'(x) = L(x)] \geq 1 - 2^{-|x|^d}$.

<u>Proof</u>: Run $M(x)$ for $k = 8|x|^{2c+d}$ times and take Majority. ($M'$ does the following; say $y_1, y_2, \ldots, y_k \in \{0,1\}$)

$$X_i = \begin{cases} 1 & \text{if } y_i = L(x) \\ 0 & \text{ow.} \end{cases}$$

$$E[X_i] = \Pr[X_i = 1] \geq p \quad \left(p = \frac{1}{2} + |x|^{-c}\right)$$

We want to analyze prob: $\Pr_{y_1,\ldots,y_k}\left[\text{Majority}(y_1,\ldots,y_k) \neq L(x)\right]$

$\Updownarrow$

$\sum X_i < \frac{k}{2}$

$\sum X_i - \left(\frac{1}{2} + \frac{1}{n^{10}}\right)k$

$\Delta > \frac{k}{n^{10}}$

**Chernoff Bounds**

$X_1, \ldots, X_n$ be ind. r.v. over $\{0,1\}$

Let $\mu = \sum_{i=1}^{n} E[X_i]$ and let $\mu = \sum_{i=1}^{n} E[X_i]$

Then for every/any $c > 0$

$$\Pr\left[\left|\sum_{i=1}^{n} X_i - \mu\right| \geq c\mu\right] \leq 2 \cdot e^{-\frac{c^2}{4}\mu}.$$

set $\delta = |x|^{-c}/2$ guarantees that,

$$\sum_{i=1}^{k} X_i \geq pk - \delta pk$$

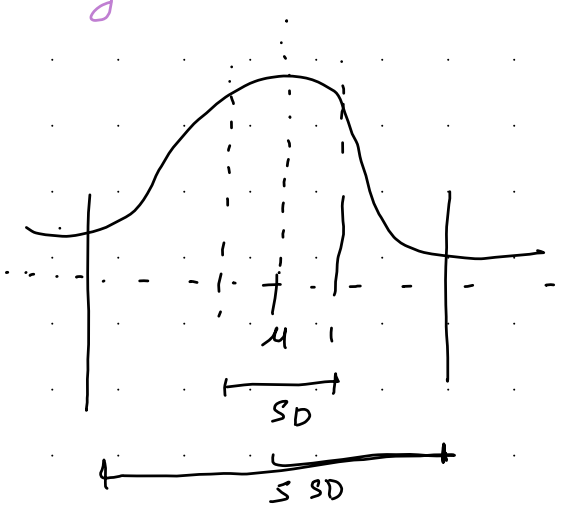
with err prob bounded by

$$e^{-\frac{1}{4|x|^2} \cdot \frac{1}{2} \cdot 8 \cdot |x|^{2c+d}} \leq 2^{-|x|^d}.$$

$\square$

That is Pr of deviating from mean is $2^{-\Omega(\mu)}$

Bell curve




Q// Does the universe has endless stream of randomness?

perfect?

# $BPP \subseteq P/poly$

- All BPP lang. have poly sized ckt.

- Big Picture: unless PH collapses not randomized poly-time algo for SAT.

$$\boxed{\text{Theorem 7.14} \qquad BPP \subseteq P/poly}$$

Proof: $L \in BPP$

$\Updownarrow$

$\exists$ TM $M$ on inputs of size $n$, uses $m = poly(n)$ random bits s.t.

$$\Pr_{r \in \{0,1\}^m}\left[M(x,r) = L(x)\right] \geq 2/3$$

(By error reduction via Majority) $1 - \frac{1}{2^{n+1}}$

Bad string $r \in \{0,1\}^m$

$$M(x,r) \neq L(x).$$

Good string $r \in \{0,1\}^m$

$$M(x,r) \equiv L(x).$$

$$\#\text{ bad strings for } x \text{ (fixed)} \leq \frac{2^m}{2^{n+1}}.$$

$$\#\text{ bad strings for any } x \leq 2^n \cdot \frac{2^m}{2^{n+1}} \leq \frac{2^m}{2}.$$

$\Rightarrow \exists\, r \in \{0,1\}^m$ (say $r_0$) that is good for every input of length $n$.

Cook Levin $\rightarrow$ $M(x, r_0)$ is the required poly-sized ckt.

$BPP \subseteq \Sigma_2 \cap \Pi_2$

Set-size Estimation algorithm
(in $\Sigma_2 \cap \Pi_2$)

$L \in BPP$

$\Downarrow$ Error Red$^n$

$x \in L \implies \Pr_r [M(x,r) = 1] \geq 1 - 2^{-n}$

$x \notin L \implies \Pr_r [M(x,r) = 1] \leq 2^{-n}$

For any (fixed) $x \in \{0,1\}^n$,

$$S_x = \{ r \in \{0,1\}^m \mid M(x,r) = 1 \}$$

Then either

$$|S_x| \geq (1-2^{-n}) 2^m \quad \text{or} \quad |S_x| \leq 2^{-n} 2^m.$$

For $S \subseteq \{0,1\}^m$ and $u \in \{0,1\}^m$

$S + u := \{ x + u : x \in S \}$

$+ = \oplus$, mod 2.

$K = \lceil \frac{m}{n} \rceil + 1$

<u>Claim</u> 1: If $|S| \leq 2^{m-n}$

$K$ vectors $u_1, \ldots, u_K$ (any)

$$\bigcup_{i=1}^{K} (S + u_i) \neq \{0,1\}^m.$$

Claim 2: For every set $S \subseteq \{0,1\}^m$ with $|S| \geq (1-2^{-n})2^m$, there exists $u_1, \ldots, u_k$ s.t. $\bigcup_{i=1}^{k} (S+u_i) = \{0,1\}^m$.

Proof: $u_1, \ldots, u_k \xrightarrow[\text{random} \in \{0,1\}^m]{\text{uni}}$

$$\Pr\left[\bigcup_{i=1}^{k} (S+u_i) = \{0,1\}^m\right] > 0$$

$B_r \equiv$ Bad even that $r \in \{0,1\}^m$ is not covered by $S+u_i$'s

$$r \notin \bigcup_{i=1}^{k} (S+u_i).$$

T.S.T $\Pr\left[\exists_{r \in \{0,1\}^m} B_r\right] < 1$

$\Uparrow$ union bound

Note

$$\forall r \quad \Pr[B_r] < 2^{-m}.$$

$$B_r = \bigcap_{i \in [k]} B_r^i$$

$$B_r^i \equiv r \notin S+u_i \underset{\text{over } \mathbb{F}_2}{\iff} r+u_i \notin S$$

But $r+u_i$ is a random element of $\{0,1\}^m$

$$\Rightarrow \Pr[B_r^i] \leq 2^{-n}$$

$$\Rightarrow \Pr[B_r] = \left(\Pr[B_r^i]\right)^k \leq 2^{-nk} < 2^{-m}.$$

Thus $\Sigma_2$ machine: $x \in L \iff$

$$\exists\, u_1, u_2 \cdots u_k \in \{0,1\}^m \ \forall r \in \{0,1\}^m$$

$$r \in \bigcup_{i=1}^{k} (S_x + u_i)$$

$$\Updownarrow$$

$$\exists\, u_1, \ldots u_k \in \{0,1\}^m \ \forall r \in \{0,1\}^m$$

$$\bigvee_{i=1}^{k} M(x, r \oplus u_i) \text{ accepts.}$$

---

Complete problems for BPP ?

BPTIME hierarchy ?

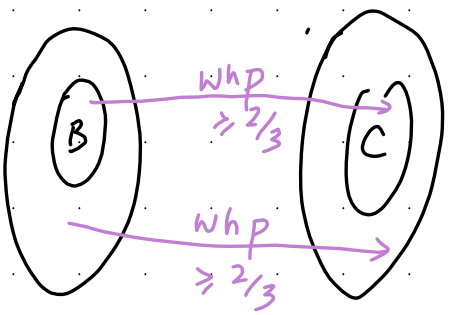
Semantic def$^n$ / Syntatic def$^n$

# Randomized Reductions

Def$^n$ $\quad B \leq_r C$ (Transitive?)

iff PTM $M$ s.t. poly-time $M$.

$x \in \{0,1\}^*$, $\Pr[B(M(x)) = C(x)] \geq 2/3$.




$x \longmapsto M(x)$

Def$^n$: $\quad BP \cdot NP = \{ L : L \leq_r 3SAT \}$

Ex: $\quad \overline{3SAT} \in BP \cdot NP$?

Randomized space-bounded Compn

BPL

$O(\log n)$-spaced PTM $M$ s.t.

$$\Pr[M(x) = L(x)] \geq 2/3$$

RL

$O(\log n)$-spaced PTM $M$ s.t.

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq 2/3$$

$$x \notin L \Rightarrow \Pr[M(x) = 1] = 0.$$

Thm: UPATH $\in$ RL.

Note, $RL \subseteq NL \subseteq P$

Is $BPL \subseteq P$? Ex

UPATH $\in$ RL: (Ex?)

Take a random walk of length $\ell = 100\, n^{10}$ from $s$.

Note it is known that,

$$BPL \subseteq L^{3/2} \quad \text{(Saks-Zhou)}$$

$\boxed{\text{Project}}$