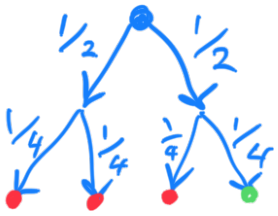
# Randomised Complexity

**Def:** Probabilistic TM $M$ has ability to toss a fair coin: a config has two successor configs, each taken with prob. $1/2$




$M(x)$ is a random var.

Assume every branch tosses same # coins

$Pr[M(x)=1]$ = fraction of accepting leaves

**Note** NTM $M \iff$ PTM $M'$ $\quad x \in L \iff Pr[M(x)=1] > 0$

**Def** $BPTIME(t(n)) \ni L : \{0,1\}^n \to \{0,1\}$

bounded-error probabilistic

iff $\exists$ PTM $M$, runtime $O(t(n))$

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

Bounded error

$$BPP = \bigcup_{k \in \mathbb{N}} BPTIME(n^k)$$

2-sided error

**Note** $P \subseteq BPP$ (Believed equal)

$BPP \overset{?}{\subseteq} NP$ (open)

Book: $BPP \subseteq \Sigma_2 P \cap \Pi_2 P$

**Ex:** Polynomial Identity Testing (PIT)

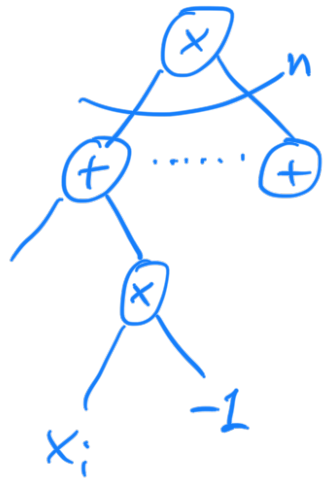
Input: $p(x_1, \ldots, x_n) \overset{e.g.}{=} x_1 x_2^2 - 3x_5 + 10 x_7^3$

Q: $p(x) \overset{?}{\equiv} 0$ total deg = 3

$p(x)$ is often given implicitly by a poly-sized arithmetic circuit

Var $x_i \in \mathbb{Z}$
gates $\oplus$ $\otimes$

E.g. $p(x) = \prod_{i=1}^{n} (1 - x_i) \equiv$




**Claim** PIT $\in$ BPP [open: PIT $\in$ P]

**Schwartz-Zippel**

Suppose $p(x_1, \ldots, x_n) \not\equiv 0$ has degree $d$.
Then for any $S \subseteq \mathbb{Z}$:

$$\Pr_{(a_1, \ldots, a_n) \sim S^n} [p(a) \neq 0] \geq 1 - \frac{d}{|S|}$$

**Proof** $n = 1$: $p$ has at most $d$ roots
$n > 1$: Induction [exercise]

**PIT algo:**

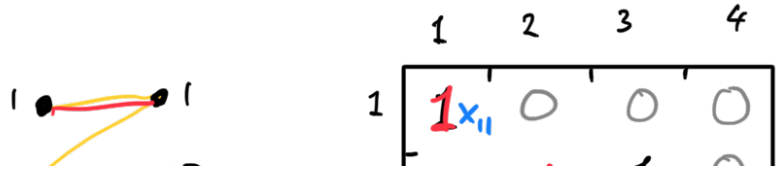
$|S| > 2^{\text{ckt size}}$

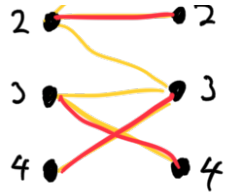
$\mathbb{Z}_N$ arithmetic

$N = 2^{2 \cdot \text{size}}$

---

**Ex:** Bipartite perfect matching






| | 2 | 3 | 4 |
|---|---|---|---|
| 2 | $1x_{21}$ | $1x_{22}$ | $1x_{23}$ |
| 3 | 0 | 0 | $1x$ $1x$ |
| 4 | 0 | 0 | $1x$ 0 |

$= A = (a_{ij})$

$$\det(A) = \sum_{\sigma:[n]\to[n]} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}^{x_{i\sigma(i)}}$$

$\operatorname{sgn}(\sigma) \in \{\pm 1\}$

Replace 1-entries with vars $x_{ij}$, get $X$

$\det(X) \neq 0$ iff $G$ has perfect matching

SZ: Take $|S| \geq 2n$. Do arithmetic in $\mathbb{Z}_p$

---

**Def** $L \in RP \overset{\text{def}}{\iff} \exists$ polytime PTM $M$: ("randomized")

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

NP $\geq 2^{-\text{poly}(n)} = 0$

**Note**

- $RP \subseteq NP$

  Certificate: sequence of coin tosses causing $M$ to accept

  1-sided error

- $PIT \in \text{co}RP$

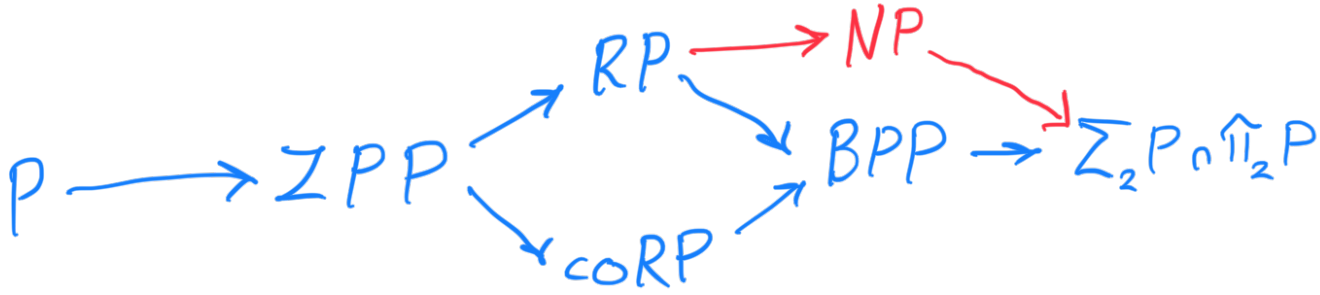
**Def** $ZPP \ni L \overset{\text{def}}{\iff} \exists$ PTM $M$ s.t. $\forall x$:

$\mathbb{E}[\text{time } M(x)] \leq n^{O(1)}$

- $\mathbb{E}[\text{runtime } M(x)] = n$
- $\Pr_r[M(x) = L(x)] = 1$

0-sided error

Exercise: $ZPP = RP \cap coRP$




Adleman thm $BPP \subseteq P/poly$

Take $L \in BPP$. Let $M$ be polytime PTM for $L$.

BPP: error $1/3$ $\xrightarrow[\text{out MAJ}]{\text{repeat } m}$ $\leq 2^{-\Omega(m)}$

RP: error $1/2$ $\xrightarrow[\text{out OR}]{\text{[Chernoff]}}$ $\leq 2^{-m}$

$\forall x \in \{0,1\}^n$: $\Pr_r[M_r(x) \neq L(x)] < 2^{-2n}$

Union bound

$\Pr_r[\exists x \in \{0,1\}^n : M_r(x) \neq L(x)] < 2^n \cdot 2^{-2n} = 2^{-n}$

$\exists r$: $M_r(x) = L(x)$ $\forall x \in \{0,1\}^n$

↑ hardcode random seed in ckt