Randomness in Computation
2/22/21 10:41 AM

Administrivia.

- Midterm 2 next Tuesday (3/2).
  - Everything about TM. P vs NP. reductions.
- HW6 due this Friday (2/26)

Main Question: '80-

¡ Probability!

How does allowing dice throws affect computations?

- More flexible when errors are allowed.
- Finding hard to construct avg. instances.
- Symmetric breaking

- crypto
- non-determinism.

Fingerprinting.

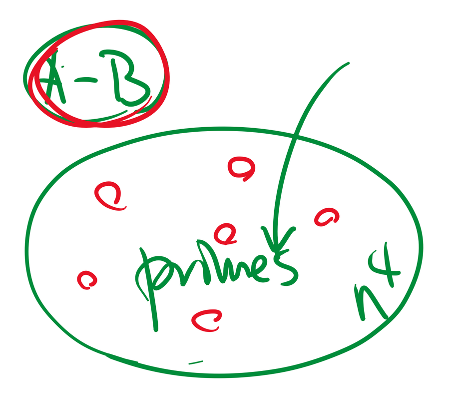
Data. A. B. N bits

check $A=B$ efficiently?

- check subset: S random $\subseteq [1..n]$
  $A[i]=B[i] \quad \forall i \in S$.
- checksum: $A \bmod p = B \bmod p$?

Data is NOT random. so prime p must be random!

- $(A-B) \bmod p = 0$, $\leq n$ prime divisors.
  $A-B = p_1 \cdot \ldots \cdot p_k \geq 2^k \Rightarrow k \leq \underbrace{\log_2(A-B)}_{\leq n}$



Choose prime randomly from $[1..n^4]$.

- at least $n^4/\ln n$ primes $\leq n^4$

w/ error pr. $n/\left(\frac{n^4}{\ln n}\right) \sim \frac{\ln n}{n^3}$.

Rabin-Karp(A, B):

> input: $A[1..n]$. $B[1..l]$.
> output: Is B substring in A?
>
> choose random $p \sim \boxed{4\log n \text{ bits}}$
>
> for i from 0 to $n-l$:
>
> if $\boxed{A[i+1..i+l]}^{A'} = B \bmod p$:
>
> ~~return yes~~ $A=B$?
>
> $A' \leftarrow 2A' - 2^l \cdot A[i+1]$
> $+ A[i+l+1] \bmod p$.

$p \mid A-B$
$\Rightarrow (A-B) \bmod p \neq 0$ w.h.p.

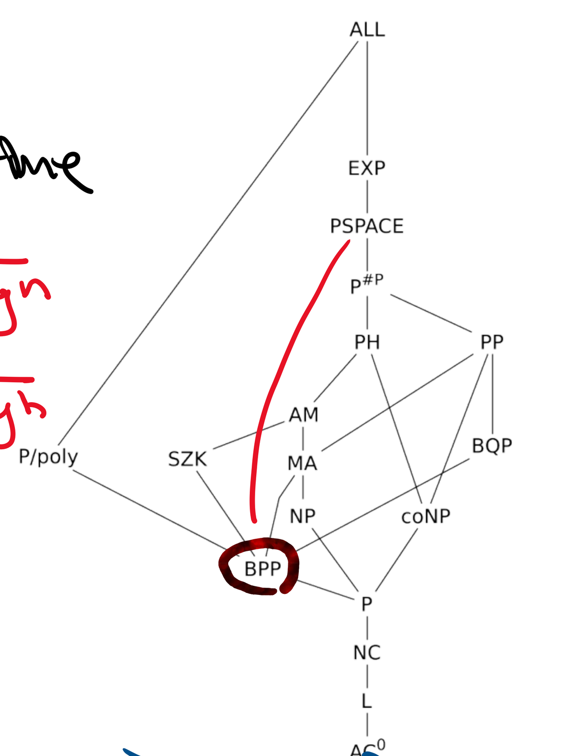
error pr.
$\log n / n^3 . \leq \frac{1}{n}$

time:
$O(n+l) \cdot \frac{n-1}{n}$
$+$
$O(n \cdot l) \cdot \frac{1}{n}$
$= O(n+l)$

BPP: problems decided by TM + dice in poly-time

yes inst. $\Rightarrow$ Pr. $\geq \boxed{3/4}$ $\quad \frac{1}{2} + \frac{1}{\text{poly } n}$

no inst. $\Rightarrow$ Pr $\leq \boxed{1/4}$ $\quad \frac{1}{2} - \frac{1}{\text{poly } n}$



error reduction.

repeat alg. X_i, output majority.

Chernoff bound: $\Pr\left[\,\left|\sum X_i - 3k/4\right| > \alpha \cdot k\,\right] \leq C^{-\alpha k}$.

Question. Is BPP bigger than P?

Think about algebraic version of SAT:

$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x}_2) =: \phi$

$[1-(1-x_1)(1-x_2)(1-x_3)] \cdot [1-(1-x_1)(x_2)] =: P(x_1, x_2, x_3)$

ϕ not sat. $\Leftrightarrow \forall x \in \cancel{\{0,1\}^n} \ \mathbb{R}^n$. s.t. $P(x) = 0$.

Polynomial Identity Testing

> input: Polynomial P, as alg. circuit. deg d. n var.
> output: Is $P=0$.

Thm. PIT is in BPP.

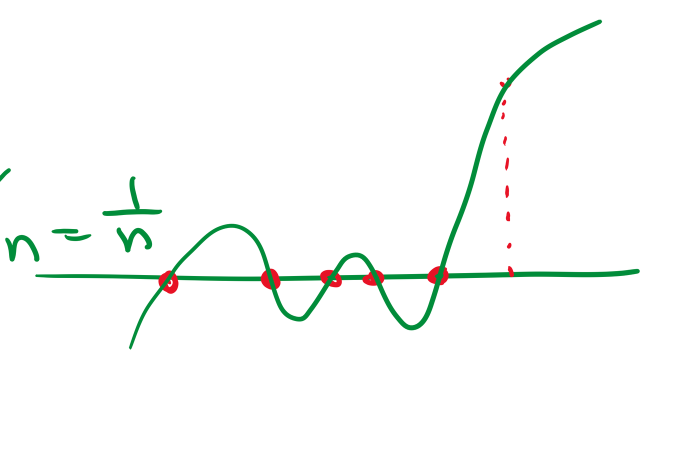
DeMillo-Lipton-'78
Schwartz-Zippel Lemma. '80 '79

Polynomial $P \neq 0$. deg d. n var.
S any set of integers.
Choose $a_1, \ldots, a_n$ from S at random.
then $\Pr[P[a_1, \ldots, a_n] \neq 0] \geq 1 - d/|S|$

PIT(P):

> Let $S = [1..d \cdot n]$
> Pick random $a \in S$
> return $[P(a) = 0?]$

by SZ lemma.
error pr. $\leq d/d \cdot n = \frac{1}{n}$



time:
P(a) might take exp time!

$P(x) = (1+x)^{2^n}$

$(1+x) \xrightarrow[\bmod p]{} (1+x)^2 \xrightarrow[\bmod p]{} (1+x)^4 \xrightarrow[\bmod p]{} \ldots \rightarrow (1+x)^{2^n}$

$a \in [1..2^n \cdot n]$

$P(a) = (1+2^n)^{2^n}$

Solution. Fingerprinting! choose $p \sim n^2$ digits.

Thm. PRIMES is in ~~BPP~~ P
[Miller-Rabin'76]
[AKS'04]

Conclusion. BPP $\neq$ P?

No. Strong evidence that BPP = P.

[IW'97]
- $\exists$ "hard" problem $\Rightarrow$ BPP = P.

[KI'04]
- PIT $\in$ P $\Rightarrow$ some problems are hard.

$\boxed{\text{Hardness} \Leftrightarrow \text{Derandomization}}$ mid '90 -