Today
- Promise Problems
- Samplers
- Expansion

CS5.413.1
Pseudorandomness
Lecture 06 (2021-9-9)
Instructor: Prahladh Harsha.

Recap: BPP- randomized complexity class

prototype problem for BPP ("complete" problem).

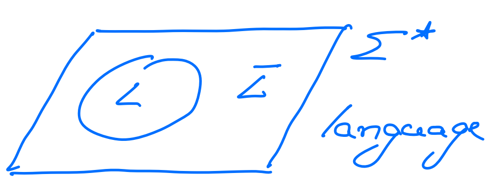
— **Promise Problem** (Generalization of Decision Problems / Languages)

Σ - alphabet (constant-size), typically $\Sigma = \{0,1\}$

Π - Promise Problem $\Pi = (\Pi_Y, \Pi_N)$

- **$\Pi_Y, \Pi_N \subseteq \Sigma^*$**
- **$\Pi_Y \cap \Pi_N = \phi$**

$\Sigma^* \setminus (\Pi_Y \cup \Pi_N)$ - Don't care instances



prBPP: promise-BPP is the set of promise problems $\Pi = (\Pi_Y, \Pi_N)$ s.t. there exists a polynomial rand. algorithm A satisfying

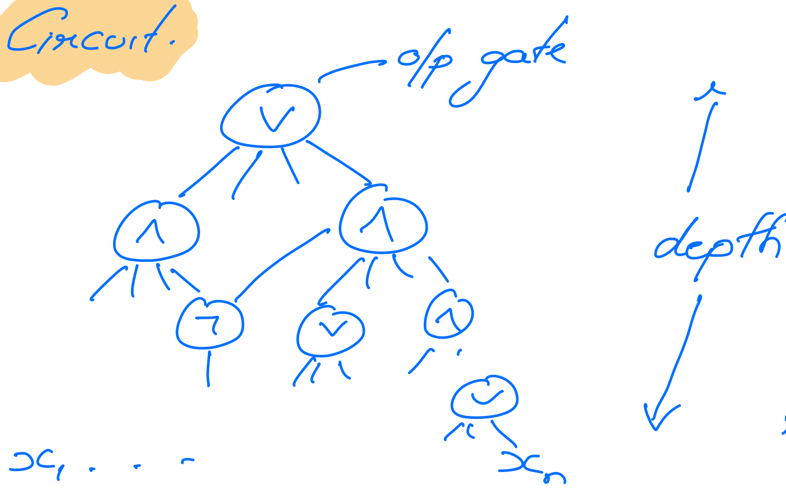
$$x \in \Pi_Y \Rightarrow \Pr_r [A(x,r) = acc] \geq 2/3$$

$$x \in \Pi_N \Rightarrow \Pr_r [A(x,r) = acc] \leq 1/3$$

Obs: BPP $\subseteq$ prBPP

– "Complete" Problem for prBPP:

Circuit.



Permissible gates
NOT – fanin 1
AND, OR – arbitrary fanin

fan-out is arbitrary

single output gate

Size – # gates in the circuit.

– Π – has a det alg running in time $t(n)$

$\Downarrow$

$\forall n$, $\exists$ circuit C_n of size $\tilde{O}(t(n))$

that compute $\Pi|_{\{0,1\}^n}$ → restriction

Circuit: C, $\quad \mu(C) = \dfrac{|\{x \in \{0,1\}^n \mid C(x) = 1\}|}{2^n}$

$\Pi \in prBPP$ - rand Alg A

$x \in \Pi_Y \cup \Pi_N$

$A(x, \cdot)$: $\quad x \to \boxed{A} \to A(x,r)$, with r fed in from above

$A(x, \cdot) : \{0,1\}^m \to \{0,1\}$

corresponding ckt $\rightsquigarrow C(x) : \{0,1\}^m \to \{0,1\}$

$x \in \Pi_Y \Rightarrow \mu(C(x)) \geq 2/3$

$x \in \Pi_N \Rightarrow \mu(C(x)) \leq 1/3$

$[\pm\varepsilon]$-Apprx-Ckt-Value: Input length - m, $\varepsilon \in (0,1)$

promise problem $CA^\varepsilon = (CA^\varepsilon_Y, CA^\varepsilon_N)$

$$CA^\varepsilon_Y = \{(C, p) \mid C\text{- ckt}, p \in [0,1], \mu(C) \geq p + \varepsilon\}$$

$$CA^\varepsilon_N = \{(C, p) \mid C\text{- ckt}, p \in [0,1], \mu(C) \leq p - \varepsilon\}$$

Observations: (1) $[\pm\varepsilon]$-Apprx-Ckt-Value $\in prBPP$

(2) $CA^\varepsilon \in prP \Rightarrow prBPP = prP$

Proof of (2). $\Pi \in \text{prBPP}$

$\Downarrow$

$\exists$ $\cancel{A}$, rand alg A

$\Downarrow$

$\cancel{\exists}$ $\forall x$, $\exists$ ckt $C(x)$

s.t. $\mu(C(x)) \geq 2/3$ if $x \in \Pi_Y$

$\mu(C(x)) \leq 1/3$ if $x \in \Pi_N$

Hence $(C(x), 1/2) \in CA_Y^{1/10}$ if $x \in \Pi_Y$

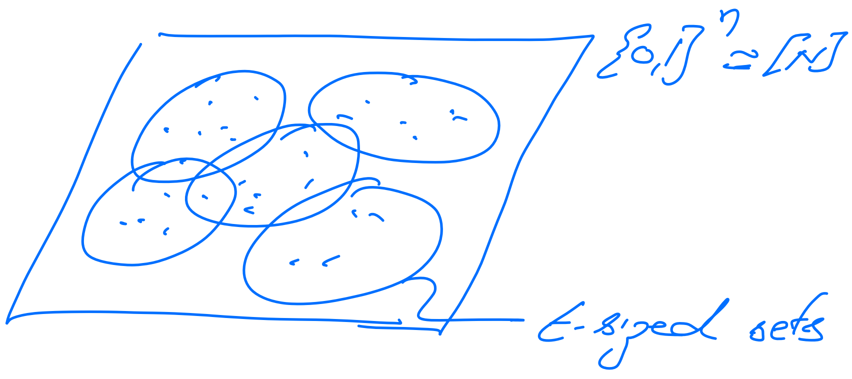
$(C(x), 1/2) \in CA_N^{1/10}$ if $x \in \Pi_N$.

Use prP alg for $CA^{1/10}$ to determine if $x \in \Pi_Y$ or $x \in \Pi_N$.

Sampling:

Oracle: $f : \{0,1\}^n \to [0,1]$

Goal: Estimate an ε-additive appx of $\mu(f)$ w/ high probability.



A (δ,ε)-sampler is a t-uniform hypergraph $H=(V,F)$ $=(h_e)_{e\in F}$

Vertices $V = [N] = \{0,1\}^n$.

$F \subseteq [N]^t$ or $\binom{[N]}{t}$

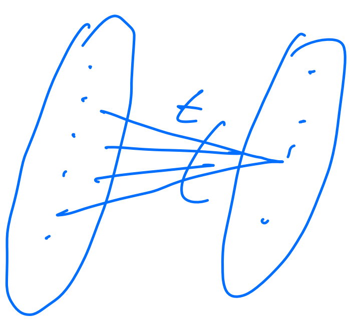
$\forall\, e \in F$, $h_e : [0,1]^t \to [0,1]$. (typically h_e : average)

s.t. $\forall\, f : \{0,1\}^n \to [0,1]$

$$\Pr_{e \leftarrow F}\Big[\,\big|h_e\big(f(v)_{v\in e}\big) - \mu(f)\big| > \varepsilon\,\Big] \le \delta \quad \ldots (*)$$

$e = (v_1 \ldots v_t) \to f(v_1), f(v_2), \ldots f(v_t)$
$h_e(f(v_1), \ldots f(v_t))$

—



$[N]$ $\quad$ $[M]$ = hyperedges

Ref:
Goldreich
"A sampler of samplers"

Remarks: (1) If h_e – averaging, averaging sampler.

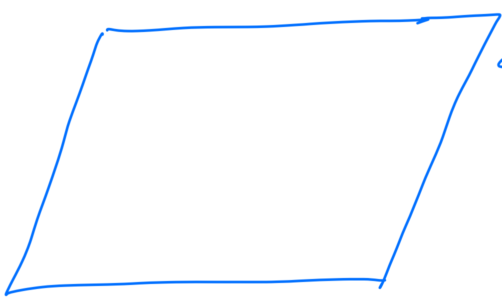
(2) If $(*)$ holds only for Boolean fns $f : \{0,1\}^n \to \{0,1\}$

(not $[0,1]$)

then Boolean sampler

(3). Efficient: Given $e \in [M]$ - (edge label)
& $i \in [t]$,
can compute v_i in
time poly$(\log M, \log t)$
(poly in the i/p length)

Goal: Construct efficient samplers with as few hyperedges as possible.



$\{0,1\}^n = [N]$

Graph whose vertex set is $[N]$

Clouds of size t:

- Walks of length t
- Balls of size t around each vertex

Degree of graph is bounded, say $D << N$
(possibly even a const)

- Then # walks of length t $= N \cdot D^{t-1}$

balls of size t $\leftarrow N$

- Do such graphs exist?

Constant-degree graph that

local average $\approx$ global average

$\forall$ functions f.

- Vertex-expansion
- Edge-expansion
- Random walk mixes well
- Quasi-randomness
- Spectral Expansion

} Same Object "Expanders"

Vertex Expansion

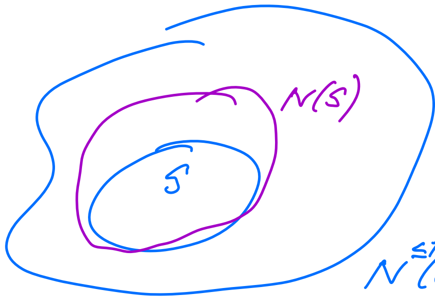
A graph $G = (V, E)$ where $|V| = N$

is a (K, A)-vertex expander

where $1 \leq K \leq N$, & $A \geq 1$

if $\forall$ sets $S \subseteq V$.

$$|S| \leq K \Rightarrow |N(S)| \geq A|S|$$



$$N(S) = \{v \in V \mid \exists u \in S,\ \{u,v\} \in E\}$$

$$N^{\le 1}(S) = N^{+}(S) = N(S) \cup S$$

Interested in constant-degree graphs

w/ $K = \Omega(N)$ e.g. $\frac{N}{100}$

$D > A = 1+\varepsilon$ for some constant $\varepsilon > 0$.

Qns: (1) Do such graphs exist?

(2) Are they useful?

(3) Can such graphs be constructed efficiently?