Today
- Is Randomness needed
- Method of conditional expectations
- Limited Independence

CSS.413.1
Pseudorandomness
Lecture 03 (2021-08-31)
Instructor: Prahladh Harsha.

"Is randomness needed?"

Recall: MAXCUT

Input: A graph $G=(V,E)$.

Output: Cut $(S, V\setminus S)$ that cuts as many edges as possible.

Algorithm:
Output a random $S \subseteq V$.
(Formally, for each $i \in [n]$, $(|V|=n)$
Toss R_i. If $R_i=1$, add v_i to S else don't.)

$$\mathbb{E}[|cut(S)|] = \mathbb{E}\left[\sum_{e\in E} \mathbb{1}[S \text{ cuts } e]\right]$$

$$= \sum_{e\in E} \frac{1}{2} = |E|/2.$$

Qn: How can one eliminate/reduce randomness in the above alg?

Technique 1: Enumeration.

- Enumerate over all possible choices of the random coins

☺ - Eliminates Randomness.

☹ - Expensive (#choices $= 2^m$, m = #random coins tossed)

Technique: Method of Conditional Expectations

$R_1 \ldots R_n$ - random coins.

$r_1 \ldots r_n$ - particular choice for r.v.s $R_1 \ldots R_n$.

Qn: Fixed first i coins to $r_1 \ldots r_i$, what is the best choice for the $(i+1)$-st coin?

Cond. Exp

$$e(r_1 \ldots r_i) = \mathbb{E}_{R_{i+1} \ldots R_n}[\text{cut}(S)] \mid R_1 = r_1, R_2 = r_2 \ldots R_i = r_i]$$

Note: $e(\cdot) = \mathbb{E}[\text{cut}(S)] = \mathbb{E}/2$

$$e(x_1 \ldots x_i) = \mathop{\mathbb{E}}_{R_{i+1} \ldots R_n} [e(x_1 \ldots x_i, R_{i+1} \ldots R_n)]$$

$$= \mathbb{E}[e(x_1 \ldots x_i, R_{i+1})]$$

$$= \frac{1}{2} e(x_1 \ldots x_i, 0) + \frac{1}{2} e(x_1 \ldots x_i, 1).$$

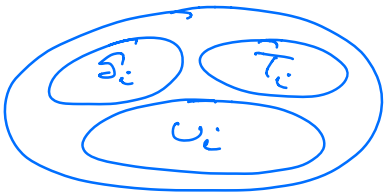
$$e(\cdot) = \frac{e(0) + e(1)}{2}$$

- $e(\cdot) = |E|/2$.
- For $i = 0 \ldots$ to $n-1$
- {Compute $e(x_1 \ldots x_i, 0)$
  $e(x_1 \ldots x_i, 1)$
  If $e(x_1 \ldots x_i, 0) \geq e(x_1 \ldots x_i)$
  set $x_{i+1} \leftarrow 0$
  else $x_{i+1} \leftarrow 1$
- Output S corresponding to $x_1 \ldots x_n$.

$$\frac{|E|}{2} \leq e(\cdot) \leq e(x_1) \leq e(x_1, x_2) \leq \ldots \leq e(x_1 \ldots x_n)$$

Qn: Are the conditional exp $e(x_1 \ldots x_i)$ easily computable?

$x_1 \ldots x_i$



$V = S_i \cup T_i \cup U_i$

$S_i \cup T_i = \{1 \ldots i\}$

$S_i = \{j \le i \mid x_j = 1\}$ $\quad T_i = \{j \le i \mid x_j = 0\}$ $\quad U_i = [n] \setminus (S_i \cup T_i)$

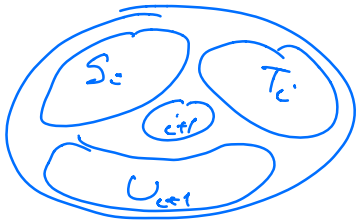
$$e(x_1 .. x_i) = |cut(S_i, T_i)| + \frac{1}{2}|cut(U_i, [n])|$$

$$e(x_1 .. x_i) = \mathbb{E}\left[|cut(S)| \;\forall j \le i,\ R_i = x_i\right]$$

$$= \sum_{e \in E} \mathbb{E}\left[\mathbb{1}[S \text{ cuts } e] \;\forall j \le i,\ R_i = x_i\right]$$

$$= |cut(S_i, T_i)| + \frac{1}{2}|cut(U_i, [n])|$$

$$e(x_1 .. x_i, 1) = |cut(S_i, T_i)| + |cut(\{i+1\}, T_i)| + \frac{1}{2}|cut(U_{i+1}, [n])|$$



Similarly,

$$e(x_1 \ldots x_i, 0) = |cut(S_i, T_i)| + |cut(\{i+1\}, S_i)| + \frac{1}{2}|cut(U_{i+1}, [n])|$$

$$e(x_1 .. x_i, 1) - e(x_1 .. x_i, 0) = |cut(\{i+1\}, T_i)| - |cut(\{i+1\}, S_i)|$$

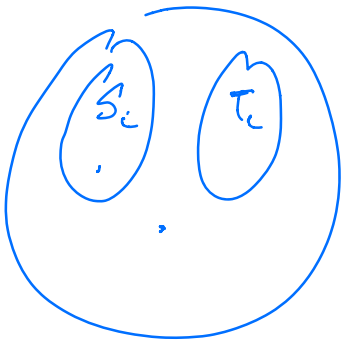
Alg: $S_0, T_0 \leftarrow \emptyset,\ U_0 \leftarrow [n]$

For $i \leftarrow 0$ to $n-1$

{ compute $cut(\{i+1\}, T_i) = cut(\{i+1\}, S_i)$

if $cut(\{i+1\}, T_i) \ge cut(\{i+1\}, S_i)$

$\subset$ Set $x_{i+1} \leftarrow 1$ else $x_{i+1} \leftarrow 0$



Greedy Algorithm

Technique 3: Limited Independence

$$\mathbb{E}[\text{cut}(S)] = \sum_{e=(i,j)\in E} \Pr[S \text{ cuts } (i,j)]$$

$$= \sum_{e=(i,j)\in E} \Pr[R_i \neq R_j]$$

$$= \frac{|E|}{2}$$

Obs: (1) For above argument, the following suffices.

$\forall i \neq j \quad \Pr[R_i \neq R_j] = \frac{1}{2}$.

(2) For the rand alg, it suffices if $R_1 \ldots R_n$ - pairwise independent (i.e., $\forall i \neq j$.

$\forall b_i, b_j \in \{0,1\} \quad \Pr[R_i = b_i, R_j = b_j] = \frac{1}{4}$

Qn: Can pairwise indep r.v. coins be

generated using fewer bits of randomness!

3 coins: R_1, R_2 (independently), $R_3 = R_1 \oplus R_2$

N coins: $N = 2^k - 1$

$R_1 \dots R_k$ – independent random coins.

For each $\emptyset \neq S \subseteq [k]$

$$R_S = \bigoplus_{i \in S} R_i$$

Note: $R_{\{i\}} = R_i$

Claim: $\{R_S\}_{\emptyset \neq S \subseteq [k]}$ is a pairwise ind set of $(2^k - 1)$ coins.

In fact,

$\forall S \neq T$, $\forall a, b \in \{0,1\}$

$$\Pr[R_S = a, R_T = b] = \frac{1}{4}$$

Pf: $R_S = R_{S \cap T} \oplus R_{S \setminus T}$

$R_T = R_{S \cap T} \oplus R_{T \setminus S}$

$S \neq T \Rightarrow S, T$ non-empty, $\Rightarrow$ at least 2

if $S \cap T$, $S \setminus T$, $T \setminus S$ are non-empty

Also, $R_{S \cap T}$, $R_{S \setminus T}$, $R_{T \setminus S}$ - independent

Hence R_S, R_T are rnd w/ uniform marginals ☒

Concl: To obtain N pairwise independent one only needs $\log(N+1)$ (fully) independent coins.

Pairwise independent family of hash functions

N random coins - pairwise independent

N random elements (each in the range $[M]$)

$\in_U [M]$

Qn: Generate N random samples. $R_1 \ldots R_N$ s.t

(1) $\forall i \cdot \forall a \in [M] \; \mathbb{P}_R[R_i = a] = 1/M$

(2) $\forall i \neq j$, R_i & R_j are independent.

$M = \{0,1\}^m$

Repeat the above (+) process m times.

truly independent coins needed

$= m \cdot (\log(N+1))$

$= (\log M) \cdot (\log(N+1))$

Experiment:

$\mathbb{F}_q$ – finite field of size q.

$q \geq \max\{M, N\}$.

- $a, b \in_R \mathbb{F}_q$;
- $\forall \alpha \in \mathbb{F}_q$. $R_\alpha \leftarrow a\alpha + b$.

Claim: $\{R_\alpha\}_{\alpha \in \mathbb{F}_q}$ over random choice of $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ – pairwise independent.

Infact, $\forall (c,d) \in \mathbb{F}_q \times \mathbb{F}_q$

& $\alpha \neq \beta \in \mathbb{F}_q$

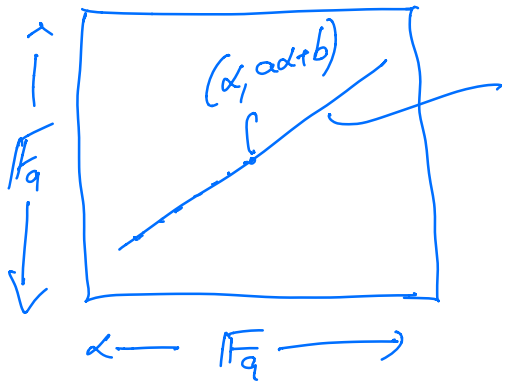
$$\Pr_{(a,b)}\left[R_\alpha = c \text{ and } R_\beta = d\right] = \frac{1}{|\mathbb{F}_q|^2}.$$

Pf:
$$\Pr_{(a,b)}\begin{bmatrix} a\alpha+b = c \\ a\beta+b = d \end{bmatrix} = \Pr_{(a,b)}\begin{bmatrix} a(\alpha-\beta) = c-d \\ a\alpha+b = c \end{bmatrix}$$

$$= \Pr_a\left[a = \frac{c-d}{\alpha-\beta}\right] \cdot \Pr_b\left[b = c - a\alpha \,\middle|\, a = \frac{c-d}{\alpha-\beta}\right]$$

$$= \frac{1}{|\mathbb{F}|} \cdot \frac{1}{|\mathbb{F}|} = \frac{1}{|\mathbb{F}|^2}.$$

□



a, b.

$y = ax+b$.

$R_\alpha = a\alpha+b. \rightsquigarrow (\alpha, a\alpha+b)$