Michael Forbes
miforbes@illinois.edu

2017-09-13.4 →
2017-09-18.2 ←
2017-09-18.1
CS598: Pseudorandomness

13→14

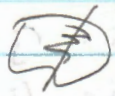
CS 598 Pseudorandomness: lecture 6

<u>admin</u>: ps 1 back monday

<u>today</u>: conditional expectations
pairwise independence

<u>Max cut</u>

$G = (V, E)$ $\quad V = S \sqcup T \quad$ cut(S,T) = # edges between S, T



<u>thm</u>: $1/2$ approx maxcut in randomized polytime

<u>pf</u>: <u>algo</u>. draw $|E|+1$ random cuts
select best cut

<u>correctness</u>: $\mathbb{E}[\text{cut}] = E/2$
Markov $\Rightarrow$ $\Pr[\text{cut} \geq E/2] \geq \frac{1}{E+1}$

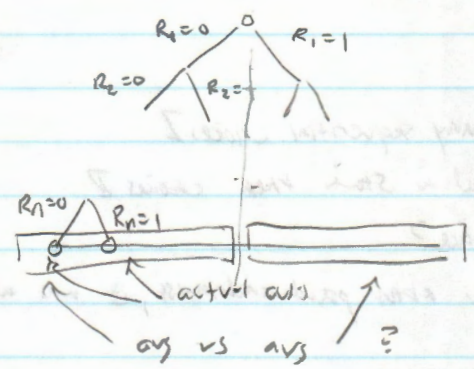
<u>time</u>: work $O(E^2)$ [$E+1$ cuts, each processes each edge once] (or twice depending on model)
parallel time polylg(E, V) [can do cuts in parallel, computing cuts is easy]
space $\Omega(n)$ [need to store random bits]

<u>Q</u>: derandomize? = Questions?

<u>conditional expectations</u>:

rephrase: pick $R_1, \dots, R_n \in \{0,1\}$ randomly
$S = \{i : R_i = 0\}$
$T = \{i : R_i = 1\}$

eg



[avg cut is good]

<u>idea</u>: walk down tree to actual cut

<u>defn</u>: $P(r_1, \dots, r_i) = \mathbb{E}_{R_1, \dots, R_n}[\text{cut} \mid R_1 = r_1, \dots R_i = r_i]$
$r_1 \in \{0,1\}$, $r_i \in \{0,1\}$

<u>eg</u>: $P(\emptyset) = \mathbb{E}[\text{cut}] = E/2$
$P(r_1, \dots, r_n) =$ size of single cut

Michael Forbes
miforbes@illinois.edu
2017-09-18.2 ← 2017-09-18.1
→ 2017-09-18.3

CS598: Pseudorandomness

lem: X, Y, Z random vars $\mathbb{E}_{X,Y}[Z] = \mathbb{E}_Y[\mathbb{E}_X[Z|Y]]$

lem: $P(r_1, \dots, r_i) = \mathbb{E}_{R_{i+1}} P(r_1, \dots, r_i, R_{i+1})$
$= \frac{1}{2} P(r_1, \dots, r_i, 0) + \frac{1}{2} P(r_1, \dots, r_i, 1)$

$\Rightarrow \exists r_{i+1}$ st $P(r_1, \dots, r_i, r_{i+1}) \geq P(r_1, \dots, r_i)$ [so it easy to compute then done]

$\Rightarrow \exists r_1, \dots, r_n$ st $P(r_1, \dots, r_n) \geq \dots \geq P(r_1) \geq P(\emptyset) = E/2$
↖ value of cut

lem: for $r_1, \dots, r_i$ $S_i := \{j \leq i : r_j = 0\}$
$T_i := \{j \leq i : r_j = 1\}$

then $P(r_1, \dots, r_i) = \text{cut}(S_i, T_i) + \frac{1}{2}\text{cut}(V - (S_i \cup T_i), V)$
[edges w/ 2 vertex outside $S_i \cup T_i$]

Pf. $= \mathbb{E}[\text{cut} \mid R_1 = r_1, \dots, R_i = r_i]$
$= \sum_{(u,v) \in E} \Pr[(u,v) \text{ is cut} \mid R_1 = r_1, \dots, R_i = r_i]$
$\hookrightarrow = \begin{cases} 1 & u,v \in S_i \cup T_i, (u,v) \in \text{cut}(S_i, T_i) \\ 0 & \emptyset \\ 1/2 & \{u,v\} \not\subseteq S_i \cup T_i \end{cases}$

Rmk: - easily computable
- is independent of $r_1, \dots, r_i$

lem: $P(r_1, \dots, r_i, 1) - P(r_1, \dots, r_i, 0) = \text{cut}(S, \{i+1\}) - \text{cut}(T, \{i+1\})$

algo: $S, T = \emptyset$
for $i = 1, \dots, n$
if $\text{cut}(S, \{i\}) > \text{cut}(T, \{i\})$ put i into S
else i into T

correctness: clear

time: $\tilde{O}(m)$ work
$\Omega(n)$ parallel time [many sequential choices]
$\Omega(n)$ space [need to store these choices]

Q: derand into parallel / small space?
= Question. Rmk: this wasn't really about pseudorandomness, it was white box derand

pairwise independence:

defn. $X_1, \dots, X_n$ pairwise independent if $\forall i \neq j$ X_i indep of X_j
$\forall i$ X_i uniform

Recall: $\mathbb{E}[\text{cut}] = \sum_{(i,j) \in E} \Pr[(i,j) \text{ is cut}] = E/2$
$= \Pr[R_i \neq R_j] = 1/2$ ← holds under pairwise indep!

goal: - construct pairwise indep vars w/ few rand bits
- derand via enumeration

Michael Forbes
Miforbes@illinois.edu

2017-09-18.2 →
← 2017-09-18.3
2017-09-18.4

CS 598 Bardovardanner

<u>defn</u>: $h : [N] \times [H] \to [M]$ is a <u>pairwise indep hash function</u>
if $\forall i \in [N]: h(i, \mathcal{U}_H) = \mathcal{U}_M$
$\forall i \neq j \in [N]$, $h(i, \mathcal{U}_H)$ indep of $h(j, \mathcal{U}_H)$
same h

is <u>explicit</u> if h computable in $\mathrm{poly}(\lg N, \lg H)$ time

<u>Rmk</u>: hash functions are <u>practical</u> [resemble random functions, but take a lot less space]

<u>Q</u>: how to construct

recall finite fields:

$\mathbb{F}$ field if: addition
multiplication
inverse for nonzero elements

↳ eg $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/\langle p \rangle$ ← finite!
<u>not</u> $\mathbb{Z}, \mathbb{Z}/\langle 4 \rangle$

$\mathbb{F}_q$ finite field $f \in \mathbb{F}_p[x]$ irred deg k ⇒ $\mathbb{F}_q[x]/\langle f \rangle \cong \mathbb{F}_{q^k}$
exist $\forall k$

all operations in $\mathrm{poly}(k \log p)$ time

<u>fact</u>: finding f of deg k: deterministically in $\mathrm{poly}(k, p)$ time
randomly in $\mathrm{poly}(k, \log p)$ time
finding f of deg k: deterministic $\mathrm{poly}(k, \lg p)$ time
we assume these algs

<u>Prop</u>: $h : \mathbb{F}_q \times \mathbb{F}_q^2 \to \mathbb{F}_q$ is pairwise independent
$h : x, (a,b) \longmapsto ax + b$ and explicit [this is clear]

<u>Pf</u>: $x \neq y \in \mathbb{F}$ want $\Pr_{a,b}[h_{a,b}(x) = \alpha \wedge h_{a,b}(y) = \beta] = \frac{1}{\mathbb{F}^2}$
$\alpha, \beta \in \mathbb{F}$

[interpolation] $\dfrac{\#\text{ lines through } (x,\alpha), (y,\beta)}{\#\text{ lines}} = \dfrac{1}{q^2} = 1/q^2$

<u>Rmk</u>: uses $2 \lg \mathbb{F}$ rand bits
vs $\mathbb{F} \lg \mathbb{F}$ rand bits for true rand

<u>Cor</u>: $h : \{0,1\}^\ell \times \{0,1\}^{2\ell} \to \{0,1\}$ explicit pairwise indep

<u>Pf</u>: take $\mathbb{F}_{2^\ell} \cong \{0,1\}^\ell$ get $h : \mathbb{F}_{2^\ell} \times (\mathbb{F}_{2^\ell})^2 \to \mathbb{F}_{2^\ell} \cong \{0,1\}^\ell \to \{0,1\}$
truncate output

<u>Cor</u> 1/2 approx to maxcut in $\tilde{O}(|E| h^2)$ work ← comparable to rand algo

<u>Pf</u>: get n pairwise indep bits $\mathrm{poly}(|E|, n)$ parallel time ← matches rand algo
w/ $2 \cdot \lg n$ bits of rand logspace ← <u>better</u> than rand algo
then enumerate

Michael Forbes
mforbes@illinois.edu
2017-09-18 14 ⟵ 2017-09-18 13 ⟶
CS 598 Pseudorandomness

<u>next time</u>: k wise independence
averaging samplers