Admin

Method of Conditional Probabilities and Expectations

Derandomization.

- Theory: is P=RP?
- practice: avoid chance of error, chance of slow.

Conditional Expectation. Max-Cut

- Imagine placing one vertex at a time.
- $x_i = 0$ or 1 for left or right side
- $E[C] = (1/2)E[C|x_1 = 0] + (1/2)E[C|x_1 = 1]$
- Thus, either $E[C|x_1 = 0]$ or $E[C|X_1 = 1] \geq E[C]$
- Pick that one, continue
- More general, whole tree of element settings.
  - Let $C(a) = E[C \mid a]$.
  - For node a with children b, c, $C(b)$ or $C(c) \geq C(a)$.
- By induction, get to leaf with expected value at least $E[C]$
- But no randomness left, so that is actual cut value.
- Problem: how compute node values? Easy.

Conditional Probabilities. Set balancing. (works for wires too)

- Review set-balancing Chernoff bound
- Think of setting item at a time
- Let Q be bad event (unbalanced set)
- We know $\Pr[Q] < 1/n$.
- $\Pr[Q] = 1/2 \Pr[Q \mid x_{i0}] + 1/2 \Pr[Q \mid x_{i1}]$
- Follows that one of conditional probs. less than $\Pr[Q] < 1/n$.
- More general, whole tree of element settings.
  - Let $P(a) = \Pr[Q \mid a]$.
  - For node a with children b, c, $P(b)$ or $P(c) < P(a)$.
  - $P(r) < 1$ sufficient at root r.
  - at leaf l, $P(l) = 0$ or 1.
- One big problem: need to compute these probabilities!

Pessimistic Estimators.

[Raghavan Thompson]
Alternative to computing probabilities
three neceessary conditions:

- $\hat{P}(r) < 1$
- $\min\{\hat{P}(b), \hat{P}(c)\} < \hat{P}(a)$
- $\hat{P}$ computable

Imply can use $\hat{P}$ instead of actual.
Our application:

- Let $Q_i = \Pr[\text{unbalanced set } i]$
- Let $\hat{P}(a) = \sum \Pr[Q_b \mid a]$ at tree node a
  - (union bound)
  - what we actually worked with
- Claim 3 conditions.
  - HW
- Result: deterministic $O(\sqrt{n \ln n})$ bias.

more sophisticated pessimistic estimator (based on chernoff) for wiring.

Pairwise Independence

pseudorandom generators.

- Motivation.
- Idea of randomness as (complexity theoretic) resource like space or time.
- sometime full independence unnecessary
- pairwise independent vars.
- generating over Z_p.
  - Want random numbers in range $[1, \ldots, p]$
  - pick random a, b
  - i^{th} random number $ai + b$
  - Works because invertible over field
- If want over nonprime field, use "slightly larger" p

Max Cut

- Expected value $m/2$
- Requires only pairwise independence
- try all possible seeds

Conserving Random Bits

- Recall Chebyshev inequality
- pairwise sufficient for chebyshev.
- Suppose RP algorithm using n bits.
- What do with $2n$ bits?
- two direct draws: error prob. 1/4.
- pseudorandom generators gives error prob. $1/t$ for t trials.
- $\mu = t/2$. $\sigma = \sqrt{t}/2$.
- error if no cert, i.e. $Y - E[Y] \geq t/2$, prob. $1/t$.