Randomness in Computing

CS 537

LECTURE 3

Last time

- Probability amplification
- Verifying matrix multiplication

Today

- More probability amplification
- Randomized Min-Cut
- Random variables

Review question: balls and bins

We have two bins with balls.

- Bin 1 contains 3 black balls and 2 white balls.
- Bin 2 contains 1 black ball and 1 white ball.

We pick a bin uniformly at random. Then we pick a ball uniformly at random from that bin.

What is the probability that we picked bin 1, given that we picked a white ball?

Bayesian Approach to Amplification

How does our confidence increase with the number of trials?

- C = event that identity is correct
- A = event that test accepts

Our analysis of Basic Frievalds:

- $\Pr[\mathrm{A}|\bar{C}] \leq 1/2$
- 1-sided error: Pr[A|C]=1

Assumption (initial belief or ``prior''): $\Pr[C] = 1/2$

By Bayes' Law

$$\Pr[C|A] = \frac{\Pr[A|C] \cdot \Pr[C]}{\Pr[A|C] \cdot \Pr[C] + \Pr[A|\bar{C}] \cdot \Pr[\bar{C}]}$$

$$\geq \frac{1 \cdot \frac{1}{2}}{1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2}} = \frac{2}{3}$$

Bayesian Approach to Amplification

How does our confidence increase with the number of trials?

- C = event that identity is correct
- A = event that test accepts

Our analysis of Basic Frievalds:

- $\Pr[A|\bar{C}] \leq 1/2$
- 1-sided error: Pr[A|C]=1

Assumption (initial belief or ``prior''): $\Pr[C] = \mathbf{2/3}$

By Bayes' Law

$$\Pr[C|A] = \frac{\Pr[A|C] \cdot \Pr[C]}{\Pr[A|C] \cdot \Pr[C] + \Pr[A|\bar{C}] \cdot \Pr[\bar{C}]}$$

$$\geq \frac{1 \cdot \frac{\mathbf{2}}{\mathbf{3}}}{1 \cdot \frac{\mathbf{2}}{\mathbf{3}} + \frac{1}{2} \cdot \frac{\mathbf{1}}{\mathbf{3}}} = \frac{\mathbf{4}}{\mathbf{5}}$$

Bayesian Approach to Amplification

How does our confidence increase with the number of trials?

- C = event that identity is correct
- A = event that test accepts

Our analysis of Basic Frievalds:

- $\Pr[A|\bar{C}] \geq 1/2$
- 1-sided error: Pr[A|C]=1

Assumption (initial belief or ``prior''): $\Pr[C] = \mathbf{2^i/(2^i+1)}$

By Bayes' Law

$$\Pr[C|A] = \frac{\Pr[A|C] \cdot \Pr[C]}{\Pr[A|C] \cdot \Pr[C] + \Pr[A|\bar{C}] \cdot \Pr[\bar{C}]}$$

$$\leq \frac{1 \cdot \frac{\mathbf{2^i}}{\mathbf{2^i+1}}}{1 \cdot \frac{\mathbf{2^i}}{\mathbf{2^i+1}} + \frac{1}{2} \cdot \frac{\mathbf{1}}{\mathbf{2^i+1}}} = \frac{\mathbf{2^{i+1}}}{\mathbf{2^{i+1}+1}}$$

CS 537 §1.5 (MU) Randomized Min Cut

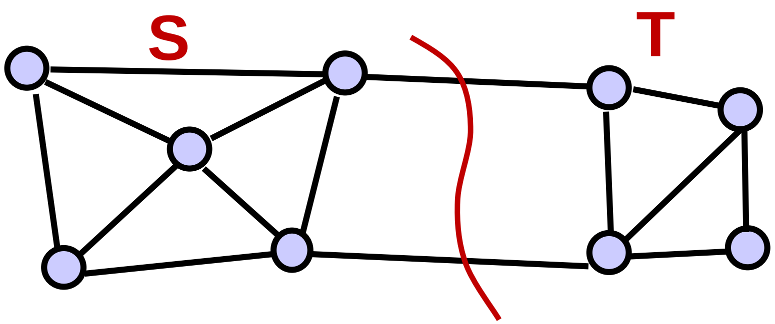
Given: undirected graph $G = (V, E)$

A ***global cut*** of G is a partition of V into non-empty, disjoint sets S, T.

The ***cutset*** of the cut is the set of edges that connect the parts:

$$\{(u, v) | u \in S, v \in T\}$$

Goal: Find the min cut in G (a cut with the smallest cutset).



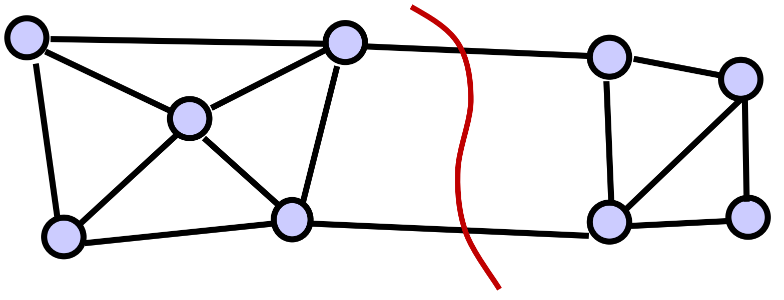
Applications: Network reliability, network design, clustering

Exercise: How many distinct cuts are there in a graph G with n nodes?

Min Cut Algorithms

Given: undirected graph $G = (V, E)$ with n nodes and m edges.

Goal: Find the min cut in G.



Algorithms for Min Cut:

- Deterministic [Stoer-Wagner `97] $O(mn + n^2 \log n)$ time
- Randomized [Karger `93] $O(n^2 m \log n)$ time

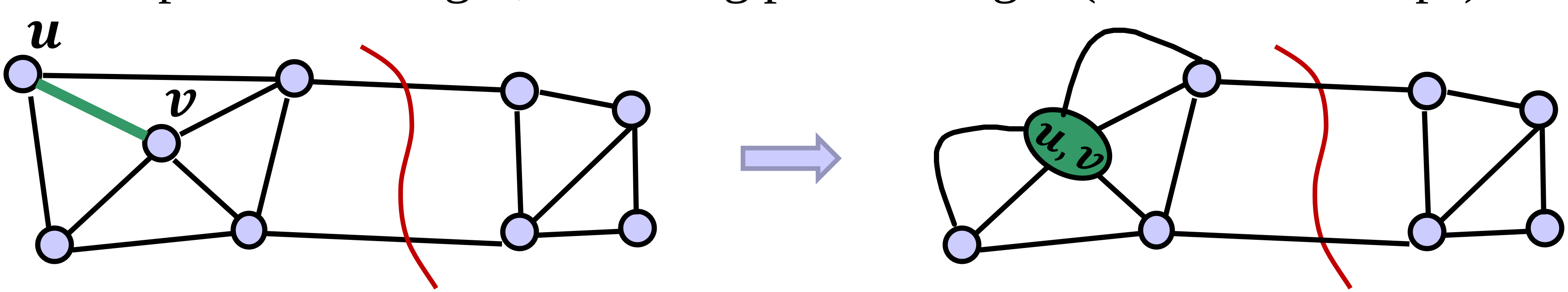
but there are improvements

§1.5 (MU) Karger's Min Cut Algorithm

Idea: Repeatedly pick a random edge and put its endpoints on the same side of the cut.

Basic operation: ***Edge contraction of an edge*** $(\boldsymbol{u}, \boldsymbol{v})$

- Merge u and v into one node
- Eliminate all edges connecting u and v
- Keep all other edges, including parallel edges (but no self-loops)



Claim

A cutset of the contracted graph is also a cutset of the original graph.

CS 537

§1.5 (MU) Karger's Min Cut Algorithm

Algorithm Basic Karger (input: undirected graph $G = (V, E)$)

1. While $|V| > 2$
2. choose $e \in E$ uniformly at random
3. $G \leftarrow$ graph obtained by contracting e in G
4. **Return** the only cut in G.

Theorem

Basic-Karger returns a min cut with probability $\geq \frac{2}{n(n-1)}$.

Probability Amplification: Repeat $r = n(n-1)\ln n$ times and return the smallest cut found.

Running time of Basic Karger: Best known implementation: $O(m)$

- Easy: $O(m)$ per contraction, so $O(mn)$
- View as Kruskal's MST algorithm in G with $w(e_i) = \pi(i)$ run until two components are left: $O(m \log n)$

Measurements in random experiments

- Example 1: coin flips
  - Measurement X: number of heads.
  - E.g., if the outcome is HHTH, then X=3.
- Example 2: permutations
  - n students exchange their hats, so that everybody gets a random hat
  - Measurement X: number of students that got their own hats.
  - E.g., if students 1,2,3 got hats 2,1,3 then X=1.

Random variables: definition

- A random variable X on a sample space Ω is a function $X: \Omega \to \mathbb{R}$ that assigns to each sample point $\omega \in \Omega$ a real number $X(\omega)$.
- For each random variable, we should understand:
  - The set of values it can take.
  - The probabilities with which it takes on these values.
- The distribution of a discrete random variable X is the collection of pairs $\{(a, \Pr[X = a])\}$.