15-251: Great Theoretical Ideas In Computer Science

Recitation 12 : Randomized Min-Cut and Interactive Proofs

- Midterm 2 in **DH 2210** on Wednesday next week
- It covers weeks 6 to 11 (inclusive)
- Midterm Practice Problems have been released
- Solution Sessions for HW10 **Friday 5-6pm** and **Saturday 2-3pm** in **GHC 4301**
- Graph review on **Saturday** from **12-1:30pm**, NP review on **Sunday** from **12-1:30pm**, Approximation and Probability review on **Sunday** from **4-5:30pm**

Lecture Review

Randomized Min-Cut

- The Min-Cut Problem: Given a connected graph $G = (V, E)$, find a non-empty subset $S \subset V$ s.t. number of edges from S to $V - S$ is minimized
- A Randomized Algorithm: On a single iteration from G_i to G_{i+1},
  - Pick an edge (u, v) randomly
  - Contract u and v into a single vertex u', so edges with an endpoint in u or v have that endpoint be u' instead.
  - Delete self-loops which result (edges that went from u to v in G_i). Note: we can have multiple edges between two vertices

  Repeat until we have only two super-vertices. Note that each super-vertex represents a set of vertices in the original graph G. Output one of these sets as S.
- Analysis: $Pr[\text{We output a minimum cut}] \geq 1/n^2$. Using repeated trials and the inequality $1 + x \leq e^x$, we can boost success probability to $\geq 1 - 1/e^n$

A language A is in IP if

- There is a probabilistic poly-time **Verifier** and a computationally unbounded **Prover**
- To determine if a string n is in A, the Verifier and Prover exchange $p(|n|)$ number of messages, then:
  - (Completeness) If $n \in A$ there exists a sequence of messages s.t. Verifier accepts
  - (Soundness) If $n \notin A$ no matter what messages are sent, Verifier rejects with at least $1/2$ probability

A Zero-Knowledge proof is a protocol in the IP model where the Verifier learns nothing about why $n \in A$.

Max Min-Cuts

Show that a graph can have at most $n(n-1)/2$ distinct min-cuts. (Hint. use the analysis of min-cut from lecture)

A Simpler Algorithm

Instead of contracting edges, suppose that in each round, we pick 2 vertices at random and contract them into a single vertex. When we have two vertices left, we output one of the vertex sets represented by the final two vertices. Prove or show a counterexample: The probability that this algorithm outputs a min-cut is $1/n^k$ for some constant k.

Zero-Knowledge Sudoku

Consider the following extension of the familiar Sudoku puzzle. Let $SUDOKU$ be the language of all $n^2 \times n^2$ boards B with $n \in \mathbb{N}$ s.t.

- Each space $B_{ij}, (i, j) \in [n^2] \times [n^2]$ is either marked with a number $\in [n^2]$ or is left blank.
- There exists a way to mark all the blank spaces in B with numbers $\in [n^2]$ s.t.
  - In each row of the board, all of the numbers are unique
  - In each column of the board, all of the numbers are unique
  - Dividing the board evenly into $n \times n$ subsquares (so there are n^2 subsquares total), in each subsquare all of the numbers are unique

Note that classic 9x9 sudoku is the special case where $n = 3$. Show that there is a zero-knowledge proof for $SUDOKU$ (Hint: permute the numbers in $[n^2]$ similarly to permuting the colors in the 3-coloring zero-knowledge proof from class).