Communication Complexity

Suhas Vittal

Lecture outline:

1. Introduction to big O, Θ, Ω notation.
   (a) Examples:
      i. $n^2 + 2n + 1 = \Theta(n^2)$.
      ii. $n^3 + 2n^2 \log(n) + 1 = \Theta(n^3)$.
      iii. $2^{(2n)} = \Theta((2^n)^2)$
      iv. $n^{\log n} = \Theta(2^{(\log n)^2})$.
      v. $1/f(n) = O(1)$ for all polynomials f.
2. Deterministic communication complexity.
   (a) Some "communication games". Given two 8-bit binary numbers x and y, how long does it take to:
      i. Check if $x = y$ in the worst case?
      ii. Check if $x \equiv y \mod 5$ in the worst case?
   (b) Motivation: suppose we have two parties called Alice and Bob. Given some function f that returns YES (1) or NO (0) on two inputs x, y, how many bits do Alice and Bob need to communicate to compute $f(x, y)$? In communication complexity, we deal with protocols, which are "algorithms involving communication." Deterministic communication complexity of a function f is denoted $C(f)$.
   (c) Fundamental bound: $C(f) \le \log(N)+1$ for a function $f : [N] \times [N] \to \{0, 1\}$. (Why is this true?)
   (d) Proving lower bounds on communication for a function f.
      i. Theorem. $C(f) \ge \log(\chi(f))$. Show proof involving combinatorial rectangles over domain of some function f. Introduce $\chi(f)$. Why does this work?
      ii. Corollary. $C(\texttt{EQ}_N) = \log(N) + 1$.
      iii. Challenge problem: let $\texttt{LE}_N : [N] \times [N] \to \{0, 1\}$ such that $\texttt{LE}_N(x, y) = 1$ iff $x \le y$. Prove $C(\texttt{LE}_N) = \log(N) + 1$.
      iv. Challenge problem: let $\texttt{DISJ}_n : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ such that $\texttt{DISJ}_n(x, y) = 1$ iff for all $1 \le i \le n$, $x_i = 0 \vee y_i = 0$. Prove $C(\texttt{DISJ}_n) \ge \Omega(n)$.
3. Randomized communication complexity.
   (a) Two ideas in complexity theory: bounded-error probablistic algorithms/protocols, and unbounded-error probablistic algorithms/protocols. What's the difference?
      i. Bounded-error: want to return the correct answer with probability $p \ge 2/3$.
      ii. Unbounded-error: want to return the correct answer with probability $p > 1/2$.

   Bounded-error communication complexity of f is denoted $R(f)$. Unbounded-error communication complexity of f is denoted $U(f)$.

(b) Randomized protocols have two flavors: public coin and private coin. Flipping a coin yields a random bit: heads (1) or tails (0).

(c) Public coin complexity.

   i. Another game: use a coin to generate a random 8-bit string. What's the fastest way you can think of checking if two numbers x, y are equal using this public random string?

   ii. Theorem. $U_{\texttt{pub}}(\texttt{EQ}_N) \leq 2$.

   iii. Challenge Problem: prove $U_{\texttt{pub}}(\texttt{DISJ}_n) \leq O(\log n)$.

(d) Private coin complexity.

   i. Theorem. $R(\texttt{EQ}_N) \leq O(\log \log N)$. Preliminary information:

      A. Chebyshev's theorem: for all $n > 1$, there exists a prime p such that $n < p < 2n$.

      B. Any polynomial $f \in \mathbb{F}_q[X]$ has at most $\deg(f)$ roots.