6.897 Advanced Data Structures (Spring'05)

Prof. Erik Demaine TA: Mihai Pătraşcu

Problem 6 *Due: Monday, Mar. 14*

In this problem, we are considering a symmetric communication game involving Alice and Bob, in which players alternate sending m-bit messages (m is the same for both players; using the notation from class, $m = a = b$). Let t be the total number of messages sent. We will be interested in optimizing m, for given t and input size n.

Alice and Bob each receive an n-bit number (call these x and y), and they must compute the greater-than function: $GT(x, y) = 1$ if $x > y$, and 0 otherwise. At the end of the protocol, one player (it doesn't matter who) must announce $GT(x, y)$. This is not considered a round; it's just the way the result of the computation is made public.

We are interested in "public-coin" protocols which compute $GT(\cdot, \cdot)$ with error probability at most $\frac{1}{3}$. At the beginning, before they see their inputs, Alice and Bob toss some random coins, and the outcomes are known to both players. Then, they receive x and y respectively, and they execute the communication protocol. It must be true that for any fixed x and y, the probability over the coin tosses that $GT(x, y)$ is announced correctly is at least $\frac{2}{3}$.

Upper Bound. Prove that one can solve the problem with $m = O(n^{1/t} \lg n)$.

Hints: Think of the van Emde Boas recursion (but note that you need to divide integers into more than 2 chunks). Remember that if you pick a random function from a universal family mapping some arbitrary universe to $\lg n$ bits, the probability that two different inputs look identical through the hash function is $\frac{1}{n}$. Alice and Bob can pick a random hash function ahead of time (this is what "public coins" really means). The player who announces $GT(x, y)$ depends on the parity of t.

Lower Bound. Prove that the problem does not have a solution unless $m = \Omega(n^{1/t}/t^2)$.

You will probably want to use the round elimination lemma. For convenience, we are restating it here. For any communication game deciding a function f, we define the k-fold of f, denoted $f^{(k)}$, as follows. Alice receives $(x_1, \ldots, x_k)$ and Bob receives $(y, i, x_1, \ldots, x_{i-1})$. The players want to compute $f(x_i, y)$.

Lemma 1 (round elimination lemma). *Assume $f^{(k)}$ has a protocol with error probability δ, in which Alice speaks first, players send m bits per message, and there are t messages in total. Then, f has a protocol with error probability $\delta + O(\sqrt{m/k})$, in which Bob speaks first, players send m bits per message, and there are $t - 1$ messages in total.*