Exercise 7: Lost in Complexity

Task 1: Why is everything so Hard?!?

In this exercise, we always consider connected, simple, weighted graphs $G = (V, E, W)$, restrict message size to $O(\log n)$ bits, and assess worst-case round complexity as a function of the (hop) diameter $D$ and $n$.

a) Show that finding any approximation to the (weighted) distance between a given pair of nodes $s, t \in V$ takes $\Omega(\sqrt{n}/\log n + D)$ rounds.

Hint: Use the same technique and graph as in the lecture, just change the weights.

b) Show that finding a Steiner tree requires $\Omega(\sqrt{n}/\log n + D)$ rounds, regardless of the size of the subset $T$ of nodes that needs to be connected to each other (unless it is 1).

Hint: Attach some irrelevant nodes to the construction from a) for $|T| \leq n/2$ and to the MST construction for $|T| > n/2$.

c) For $s, t \in V$, an $s$-$t$ cut is a subset $S \subseteq V \setminus \{t\}$. The weight of the cut is the sum of weights of all edges $\{v, w\} \in E \cap (S \times (V \setminus S))$ crossing the cut. Show that finding any approximation to the weight of a minimum $s$-$t$ cut takes $\Omega(\sqrt{n}/\log n + D)$ rounds.

d) Conclude that finding an approximate maximum flow or even approximating the value of such a flow requires $\Omega(\sqrt{n}/\log n + D)$ rounds.

Task 2: Harder, Better, Slower

Consider graphs $G = (V, E)$ and message size $O(\log n)$. In this exercise, we show that determining the diameter $D$ of a graph more accurately than factor $3/2$ requires $\Omega(n/\log n)$ rounds or large messages.

a) For a set disjointness instance $(x, y)$ and input size $N$, construct a graph with $O(\sqrt{N})$ nodes that has diameter 2 if $x$ and $y$ encode disjoint sets, and diameter 3 otherwise. The graph must have a cut with $O(\sqrt{N})$ edges between the parts encoding $x$ and $y$, respectively.

Hint: Start from $2k$ nodes $l_1, \ldots, l_k, r_1, \ldots, r_k$ where the edge $\{l_i, r_j\}$ is included if and only if $i = j$. Enumerate the bits of $x$ in some convenient way as $x_{i,j}$ so that $i$ and $j$ stay in $O(\sqrt{N})$; likewise for $y$. Then add edges so that for all $1 \leq i, j \leq k$ there is some path of length 2 from $l_i$ to $r_j$ (you may assume $i \neq j$) if $x_{i,j} = 0$ or $y_{i,j} = 0$, but not if $x_{i,j} = y_{i,j} = 1$.

Finally, add two nodes $l$ and $r$ and some edges to make sure that the diameter is 2 if $x$ and $y$ encode disjoint sets and 3 otherwise.

b) Assume for a moment a distributed algorithm exists that uses $B$-bit messages to compute (or approximate) the diameter of such a graph in $T$ rounds. Show that Alice and Bob can simulate each execution with a total communication complexity of $O(\sqrt{NBT})$.

Hint: Don’t think “It can’t be that easy!”.

c) Conclude that $T \in \Omega(\sqrt{N}/B)$ in the worst case, no matter what algorithm is used. Specifically, conclude that if $B \in O(\log n)$, it requires $\Omega(n/\log n)$ rounds to determine the diameter of a graph more accurately than up to factor of $3/2$. 
**Task 3**: Be more Constructive!

a) Check up on the prime number theorem!

b) Show that for any $k \in \mathbb{N}$ and any constant $C \in \mathbb{N}$, the number of primes in the range $[2^k, 2^{k+C}]$ is in $2^{\Theta(k+C)}/k$.

c) Prove that for an $N$-bit number, the number of different $\Theta(\log N)$-bit primes that divides it is bounded by $\Theta(N/\log N)$. Use this to find suitable choices of $k$ and $C$ such that the number of primes in the range $[2^k, 2^{k+C}]$ is polynomial in $N$ and the probability that, for a fixed $N$-bit number, a uniformly random prime from this range divides it is at most $N^{-\Theta(1)}$.

d) Check up on the AKS primality test!

e) Infer that there is a protocol solving equality with error probability $N^{-\Theta(1)}$ that uses private randomness, communicates $O(\log N)$ bits, and requires only polynomial computations, both for construction and execution!

f) Check up on your ability to explain this to others in the exercise session!