COMS 6998 Communication Complexity Assignment
Due: April 27, 2022

1. $MED(x, y)$ is defined to be the median of the multiset $x \cup y$. Using binary search, one can show that $D(MED) = O(\log^2 n)$. Give an $O(\log n)$-bit protocol for MED.

2. In class we proved one direction of the KW theorem, showing that for any function f, the minimum circuit depth of f is at least as large as the deterministic communication complexity of KW_f. Prove the other direction, showing that the deterministic communication complexity of KW_f is at least the minimum circuit depth of f.

3. (Exercise from RY Book.) Let $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a 2-party function that requires c bits of communication. Prove that computing $\wedge_{i=1}^k g(x_i, y_i)$ and $\vee_{i=1}^k g(x_i, y_i)$ requires $k(\sqrt{c/2} - \log n - 1)$ bits of communiction. (Hint: Find a small 1-cover using the protocol for the OR of the g's, and a small 0-cover using the protocol for the AND of the g's.)

4. For randomized communication complexity, we showed that public and private coins are nearly equivalent. In the easy direction, any randomized protocol with private randomness can be converted into a protocol with public randomness, and Newman's theorem showed the reverse direction, that any cost c public coin protocol can be converted into a private coin protocol of communication complexity $c + O(\log n)$. This question asks about private versus public coins for internal information complexity.

   (a) (Newman's Theorem for Information Complexity) Show that for any public coin protocol Π with internal information cost c, Π can be converted into a private coin protocol with information cost $O(c)$.

   (b) What about the easy direction (converting private to public coin) for information complexity? Give an example of a randomized protocol that has linear information complexity with respect to public coins, but $O(1)$ information complexity with respect to private coins. Note that you do not have to exhibit a function witnessing a separation between public versus private coin information complexity. Instead I am just asking for a simple protocol where the information complexity is vastly different if the randomness is public versus private.

5. Recall the inner product function $IP(x, y) =< x, y > \bmod 2$. Let M_{IP} be the 2^n-by-2^n communication matrix for IP.

   (a) Prove that the rank of M_{IP} over F_2 equals n.

   (b) Prove that the rank of M_{IP} over the reals is 2^{n-1}. Conclude that the deterministic communication complexity of IP is $\Omega(n)$.

   (c) Prove that the co-nondeterministic communication complexity of IP is $\theta(n)$.