Exercise X, Computational Complexity 2024

These exercises are for your own benefit. Feel free to collaborate and share your answers with other students. Solve as many problems as you can and ask for help if you get stuck for too long. Problems marked * are more difficult but also more fun :).

Communication complexity

1 Suppose Alice has a set $A \subseteq [n]$ of size $|A| \geq n/2$ and Bob has a set $B \subseteq [n]$ of size $|B| < n/2$. Find an $O(\log^2 n)$-bit protocol that outputs some element $i \in [n]$ such that $i \in A \setminus B$.

Solution: We will see sets as indicator vectors, so that Alice has a vector $x \in \{0, 1\}^n$ where $x_i = 1$ if and only if $i \in A$. Likewise Bob holds $y \in \{0, 1\}^n$ and they want to output a coordinate $i \in [n]$ such that $x_i = 1$ and $y_i = 0$, which is promised to exist because $|A| > |B|$.

The idea is that Alice and Bob splits x and y in half and send each other the hamming weight of each part (this requires $O(\log(n))$ bits of communication). Now, there must be some half for which Alice has more elements that Bob, and they recurse on that part. The recursion finishes after $O(\log(n))$ steps at i such that $x_i \neq y_i$.

2 Define the *Set-Intersection* function $\mathrm{SI}\colon \{0,1\}^{2n} \to \{0,1\}$ by $\mathrm{SI}(x,y) = \bigvee_{i\in[n]}(x_i \wedge y_i)$. (If we think of x and y as subsets of $[n]$, then $\mathrm{SI}(x,y) = 1$ iff $x \cap y \neq \emptyset$.)

(a) Show that $\mathrm{N}_1^{\mathrm{cc}}(\mathrm{SI}) \leq O(\log n)$.

(b) Show that $|\mathrm{SI}^{-1}(0)| = 3^n$

(c) Show that every 0-chromatic rectangle for SI is of size at most 2^n.

(d) Use (b) and (c) to conclude a lower bound on $\mathrm{N}_0^{\mathrm{cc}}(\mathrm{SI})$.

Solution:

(a) A certificate here is simply an index $i \in [n]$. Alice accepts if $x_i = 1$ and Bob accepts if $y_i = 1$. Note that if $(x,y) \in \mathrm{SI}^{(-1)}(1)$, then there must be an index $i \in [n]$ that will make both Alice and Bob accept. If $(x,y) \notin \mathrm{SI}^{(-1)}$, then no index can fool both Alice and Bob. Finally, this certificate has size $\log(n)$, so that $\mathrm{N}_1^{\mathrm{cc}}(\mathrm{SI}) \leq O(\log n)$.

(b) We prove this by induction on $n \geq 1$. For the base-case $n = 1$, we have $\mathrm{SI}_1^{-1}(0) = \{00, 01, 10\}$ so that the claim holds. Now, let k_{ab} be the number of disjoint strings $(x,y) \in \{0, 1\}^{2(n+1)}$ where $x_1 = a$ and $y_1 = b$. Note that $|S_{n+1}^{-1}(0)| = k_{00} + k_{01} + k_{10}$. Using the induction hypothesis, $k_{00} = k_{01} = k_{10} = 3^n$ so that $|S_{n+1}^{-1}(0)| = 3^{n+1}$ as desired.

(c) Suppose toward contradiction that $A \times B$ is a 0-chromatic rectangle with size $> 2^n$. Now, for a set $S \subseteq \{0, 1\}^n$, let $\#1(S)$ be the number of coordinates which appear with a 1 in S. More formally:

$$\#1(S) = |\{i \in [n] : \exists s \in S \text{ with } s_i = 1\}|$$

Note that $\#1(S) \geq \log_2(|S|)$ and so we have:

$$\#1(A) + \#1(B) \geq \log_2(|A|) + \log_2(|B|) = \log_2(|A \times B|) > \log_2(2^n) = n$$

Therefore, it must be that there is some string $a \in A$ and $b \in B$ and an index $i \in [n]$ such that $a_i = b_i = 1$: a contradiction with the fact that $A \times B$ is 0-chromatic.

(d) Since each rectangle can only cover at most 2^n entries of M_{SI} and there are 3^n 0-entries, any 0-covering of M_{SI} must use $\geq (3/2)^n$ rectangles. Hence, $\mathrm{N}_0^{\mathrm{cc}}(SI) \geq \log_2((3/2)^n) \geq \Omega(n)$ as desired.

3 We saw in the lecture that $\mathrm{D}^{\mathrm{cc}}(\textsc{Maj}_{2n}) \leq O(\log n)$. Prove a matching lower bound by a reduction from the *Greater-Than* function.

Solution: We show how to transform a communication protocol for $\textsc{Maj}_{2^n}$ that communicates at most k bits into a communication protocol solving GT_n with k bits of communication. As seen in class, $k \geq \mathrm{D}^{\mathrm{cc}}(\mathrm{GT}_n) \geq \Omega(n)$ so that $\mathrm{D}^{\mathrm{cc}}(\textsc{Maj}_n) \geq \Omega(\log(n))$.

On input $x, y \in \{0,\, 1\}^n$, Alice first computes the string a with Hamming weight $|a|_H = N(x)$ where $N(x)$ is the integer represented by x. On its side, Bob crafts the string b with Hamming weight $|b|_N = n - N(y)$. Note that $a, b \in \{0,\, 1\}^{2^n}$. Then, they run the majority protocol on a, b and output accordingly. This protocol uses k bits of communication. For the correctness, notice that on input x, y, the protocol accepts if and only if:

$$\textsc{Maj}(a, b) = 1 \iff |a|_H + |b|_H \geq n \iff N(x) + n - N(y) \geq n \iff N(x) \geq N(y)$$

4 The *Clique vs. Independent Set* (CIS) problem is defined relative to an n-vertex graph $G = ([n], E)$ as follows: Alice holds a clique $C \subseteq [n]$, Bob holds an independent set $I \subseteq [n]$, and their goal is to output $\mathrm{CIS}_G(C, I) = |C \cap I|$. (Note that $|C \cap I| \in \{0, 1\}$.)

(a) Show that $\mathrm{D}^{\mathrm{cc}}(\mathrm{CIS}_G) \leq O(\log^2 n)$ for every G.

(Hint: If Alice's C contains a vertex v of degree $\leq n/2$, Alice can send the name of v to Bob and they can wlog restrict G to the neighbourhood of v by discarding half the vertices. What is the analogous property for Bob? How can you use this idea recursively?)

(b) Find a graph $G = ([n], E)$ such that every *one-way* (Alice sends one message to Bob, and Bob outputs the answer) deterministic protocol for CIS_G requires $\Omega(n)$ bits.

Solution:

(a) As suggested in the hint, if there exists $v \in C$ with $\deg(v) \leq n/2$, then the graph G can be restricted to the neighborhood of v. Indeed, since C is a clique, all of C remains which guarantees that a solution remains if there exists one. On the other hand, if there exists $v \in I$ such that $\deg(v) \geq n/2$, then those vertices can be removed from the graph, indeed if a solution exists, then it cannot be in the neighborhood of I (as it is an independent set). Note that if no such vertex exists for Alice and Bob, then it means that:

$$\begin{cases} \forall v \in C : \deg(v) > n/2 \\ \forall v \in I : \deg(v) > n/2 \end{cases} \implies \mathrm{CIS}_G(C, I) = 0$$

This suggest a communication protocol that at each rounds agrees on $v \in C$ or $v \in I$ to cut the graph in half. Each round has bit-complexity $O(\log(n))$ for sending the identifier of a vertex and after $O(\log(n))$ rounds, the graph is empty so the process is done.

(b) Pick G to be the complete graph and suppose that Alice has a way to communicate $\leq n-1$ bits and solve the problem. This implies that there are two different cliques $C_1, C_2 \subseteq [n]$ that are mapped to the same message m. Without loss of generality, let $v \in C_1 \setminus C_2$. If Bob gets input $I = \{v\}$, then it will err on C_1 or C_2: a contradiction with the correctness of the protocol.

5 Let $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and define a language $L_f = f^{-1}(1) = \{xy : f(x,y) = 1\}$.

(a) Show that if L_f is accepted by a deterministic (resp. nondet.) finite automaton with s states, then f has deterministic (resp. nondet.) communication complexity $O(\log s)$.

(b) Use the above connection and the equality function $f = \mathrm{EQ}_n$ to construct a language L that is accepted by a nondeterministic automaton with $n^{O(1)}$ states but such that every nondeterministic automaton for the complement language $\overline{L}$ requires $2^{\Omega(n)}$ states.

Solution:

(a) We do the deterministic version first. Alice simply runs the DFA on her part of the input x, transmits the state q of the DFA to Bob using $O(\log(s))$ bits. Bob finishes the computation with his part of the input and outputs accordingly. Correctness follows from the correctness of the DFA.

For the non-deterministic counter-part, a certificate is simply a state q which Alice can reach on x and from which Bob can reach the accepting state on y.

(b) Pick $L = \overline{L_f}$, i.e.:

$$L = \{x, y \in \{0,\, 1\}^n : x \neq y\}$$

Note that $\mathrm{N}_1^{\mathrm{cc}}(f) \geq \Omega(n)$ so that using the above, any NFA computing L must have $2^{\Omega(n)}$ states. On the other hand, there is a NFA with $O(n^2)$ that solves L. Indeed, it just "guesses" at which position the two string disagrees.