CS 591 B1: Communication Complexity, Fall 2019

Problem Set 1

Due: 5:00PM, Friday, September 27, 2019.

Homework Policies:

- Submit your completed assignment by email to `mbun[at]bu[dot]edu`. Please include the string "CS591PS1" somewhere in your subject line.

- Solutions must be typeset, e.g., using LaTeX or Microsoft Word.

- To help your instructor calibrate the length and difficulty of future assignments, please include with each problem an estimate of how long it took you to solve it.

- You are encouraged to collaborate on the homework problems with each other in small groups (2-3 people). Collaboration may include brainstorming or exploring possible solutions together on a whiteboard, but should not include one person telling the others how to solve a problem. You must also write up the solutions independently (in your own words) and acknowledge your collaborators at the beginning of the first page.

- You may freely use without proof any results proved in class, in Mark's lecture notes posted on the class webpage, or in the main body of the texts assigned as reading. Note that this excludes results that appear in the texts as problems and exercises. You may, of course, use such results but you have to prove them first.

- You may read papers and other outside sources to help you solve these problems. If you do so, you must acknowledge these sources and write the solutions in your own words.

- Start early! The problems are presented roughly in the order of the course content they correspond to, so you may get started on the first few problems as soon as the assignment is released. Late assignments will receive credit only with prior permission of the instructor.

The problem set looks longer than it actually is. This is because some of the problems introduce additional background and concepts that were not covered in the lecture, but which will enhance your understanding of the material and which I hope you will find interesting. Please do not hesitate to ask questions about any of the new material on Piazza or during office hours.

Problem 1 (Partial Functions). A partial function is one which is defined only on a subset of its domain. More formally, a partial function is a mapping $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,\star\}$. Inputs x for which $f(x) = \star$ should be interpreted as inputs where f is not defined. A (deterministic) protocol Π computes a partial function f if $\Pi(x,y) = f(x,y)$ for every (x,y) with $f(x,y) \neq \star$. This problem investigates which of the results we've seen also apply to partial functions.

(a) For $b \in \{0,1\}$, call a combinatorial rectangle R *b-monochromatic* with respect to a partial function f if $f(x) \in \{b,\star\}$ for every $x \in R$. Consider the partial function $\mathrm{PrEQ}_n : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1,\star\}$ defined by

$$\mathrm{PrEQ}_n(x,y) = \begin{cases} 1 & \text{if } (x_1,\ldots,x_n) = (y_1,\ldots,y_n) \text{ and } (x_{n+1},\ldots,x_{2n}) \neq (y_{n+1},\ldots,y_{2n}), \\ 0 & \text{if } (x_1,\ldots,x_n) \neq (y_1,\ldots,y_n) \text{ and } (x_{n+1},\ldots,x_{2n}) = (y_{n+1},\ldots,y_{2n}), \\ \star & \text{otherwise.} \end{cases}$$

Show that $2n$ 0-monochromatic rectangles suffice to cover $\mathrm{PrEQ}_n^{-1}(0)$ and $2n$ 1-monochromatic rectangles suffice to cover $\mathrm{PrEQ}_n^{-1}(1)$.

(b) Show that $\mathbf{P^{cc}}(\mathrm{PrEQ}_n) \geq \Omega(n)$. (Hint: Reduce to the fact that $\mathbf{P^{cc}}(\mathrm{EQ}_{2n}) = 2n + 1$.)

Combined with part (b), this shows that $\mathbf{P^{cc}}(f)$ can be much larger than $\mathbf{NP^{cc}}(f) \cdot \mathbf{coNP^{cc}}(f)$ for partial functions. Recall that $\mathbf{P^{cc}}(f) \leq O(\mathbf{NP^{cc}}(f) \cdot \mathbf{coNP^{cc}}(f))$ for all total f. No need to hand an explanation in, but where in that proof do we use the fact that f is total?

(c) Let f be a partial function. Show that if every 1-monochromatic rectangle with respect to f has size at most s, then it has nondeterministic communication complexity $\mathbf{NP^{cc}}(f) \geq \log(f^{-1}(1)/s)$.

(d) Define the Unambiguous-Disjointness function $\mathrm{UDISJ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1,\star\}$ by

$$\mathrm{UDISJ}_n(x,y) = \begin{cases} 1 & \text{if } |x \wedge y| = 0, \\ 0 & \text{if } |x \wedge y| = 1, \\ \star & \text{otherwise.} \end{cases}$$

(Here, $x \wedge y$ denotes the bitwise AND between x and y.) This is a variant of Disjointness which only asks to distinguish the case where the sets represented by x and y are disjoint from the case where they intersect in only one element.

Prove that $\mathbf{NP^{cc}}(\mathrm{UDISJ}_n) \geq \Omega(n)$.

Problem 2 (Diverse Functions). Let $f : X \times Y \to \{0, 1\}$ be a function whose communication matrix M_f has at least k distinct rows. Prove that $\mathbf{P^{cc}}(f) \geq \log \log k$.

Problem 3 (Reductions and Completeness). Let $f_n, g_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be families of functions. We say that $\{f_n\}_{n \in \mathbb{N}}$ *reduces to* $\{g_n\}_{n \in \mathbb{N}}$, written $\{f_n\} \leq_{cc} \{g_n\}$, if there exists a function $m(n) = 2^{\mathrm{polylog}(n)}$ for which the following holds. For every n there exist functions $R_A, R_B : \{0,1\}^n \to \{0,1\}^{m(n)}$ such that $f(x, y) = g(R_A(x), R_B(y))$ for every $x, y \in \{0,1\}^n$. The functions R_A and R_B allow Alice and Bob to reduce the evaluation of f to the evaluation of g through independent preprocessing of their inputs; the upper bound on $m(n)$ is a criterion for what it means for this preprocessing to be "efficient."

By analogy to Karp reductions for Turing machine classes, these reductions allow us to define completeness with respect to communication classes. For a communication complexity *measure* $\mathcal{C}^{\mathbf{cc}}$, recall that we define the *class* $\mathcal{C}^{\mathbf{cc}}$ to be the set of function families $\{f_n\}$ with $\mathcal{C}^{\mathbf{cc}}(f_n) = \mathrm{polylog}(n)$. We say that a family $\{g_n\}$ is *complete* for $\mathcal{C}^{\mathbf{cc}}$ if 1) $\{g_n\} \in \mathcal{C}^{\mathbf{cc}}$ and 2) $\{f_n\} \leq_{cc} \{g_n\}$ for every $\{f_n\} \in \mathcal{C}^{\mathbf{cc}}$.

(a) Prove that the disjointness function DISJ_n is complete for $\mathbf{coNP^{cc}}$.

(b) Using the fact that the $\mathbf{NP^{cc}}$ cost of any protocol is characterized up to constants by its 1-covering number, we can alternatively define the class $\mathbf{NP^{cc}}$ as the class of functions which have 1-covers of quasipolynomial size. That is, $\mathbf{NP^{cc}}$ is exactly the class of function families $\{f_n\}$ which can be expressed as

$$f_n(x, y) = \bigvee_{i=1}^{2^{\mathrm{polylog}(n)}} R_n^i(x, y)$$

where each function R_n^i is the indicator of a rectangle.

This perspective gives us a natural way of defining a polynomial hierarchy in communication complexity without the need to reason about "alternating" protocols, and of defining an analog of **PSPACE** without even needing to define space! For instance, we may define $\mathbf{\Sigma_2^{cc}}$ as the sequences of functions $\{f_n\}$ which can be expressed as

$$f_n(x, y) = \bigvee_{i=1}^{2^{\mathrm{polylog}(n)}} \bigwedge_{j=1}^{2^{\mathrm{polylog}(n)}} \bar{R}_n^{i,j}(x, y),$$

where each function $\bar{R}_n^{i,j}$ is the indicator for the *complement* of a rectangle.

Identify a complete problem for $\mathbf{\Sigma_2^{cc}}$ and prove its completeness.

Problem 4 (Corruption and Disjointness)**.** In class, we'll see that the Disjointness function has large discrepancy, at least $\Omega(1/n)$, and hence the discrepancy method cannot be used to prove strong lower bounds. Intuitively, this is because the hardness of Disjointness is "one-sided": It has large 0-rectangles which are easy to certify membership in, but no large 1-rectangles. The one-sided discrepancy (or corruption) bound uses the fact that large rectangles must have many 0s, and is actually enough to prove a tight $\Omega(n)$ lower bound on the randomized communication of DISJ_n. This problem will walk you through an elegant combinatorial proof of an $\Omega(\sqrt{n})$ lower bound due to Babai, Frankl, and Simon.

(a) (Corruption Bound) Let $f : X \times Y \to \{0,1\}$ and let μ be a distribution over $X \times Y$ such that
$$\mu(R \cap f^{-1}(0)) \geq \varepsilon\mu(R)$$
for every rectangle with $\mu(R) \geq 2^{-2c}$. Suppose $1/3 < \mu(f^{-1}(1)) < 2/3$. Prove that (for ε sufficiently small and c sufficiently large) no deterministic protocol computes f to error $\varepsilon/4$ under inputs sampled from the distribution μ with communication cost $\leq c$.

(b) Suppose without loss of generality that n is a perfect square which is divisible by 12. Let μ be the distribution over DISJ_n which is uniform over all pairs (x, y) with $|x| = |y| = \sqrt{n}$, i.e., Alice and Bob's inputs indicate random sets of size exactly $\sqrt{n}$. Let $R = A \times B$ be a rectangle with $|A| > 2^{-\delta\sqrt{n}} \cdot \binom{n}{\sqrt{n}}$ for some constant $\delta > 0$ sufficiently small (but independent of n).

Prove by induction that for $k = \sqrt{n}/3$, there exist rows $x_1, \ldots, x_k \in A$ that are "well-separated" in the sense that for every $i = 1, \ldots, k$, we have $|x_i \setminus (x_1 \cup \cdots \cup x_{i-1})| \geq \sqrt{n}/2$.

(c) Suppose $\mu(R \cap \mathrm{DISJ}_n^{-1}(0)) < \varepsilon\mu(R)$ for $\varepsilon > 0$ sufficiently small. By deleting at most half of the rows of A, we may assume that every $x \in A$ intersects at most $2\varepsilon|B|$ of the rows of B. Similarly, by deleting most half of the rows of B, we may assume that every $y \in B$ intersects with at most $4\varepsilon k$ of the rows in the well-separated set $\{x_1, \ldots, x_k\}$ constructed in part (b).

Prove that under these assumptions,
$$|B| \leq \binom{k}{4\varepsilon k} \cdot \binom{n - (1 - 4\varepsilon)k\sqrt{n}/2}{\sqrt{n}} \leq 2^{-\delta\sqrt{n}} \cdot \binom{n}{\sqrt{n}}$$
for some constant $\delta > 0$.

(d) Conclude that for any rectangle R with $\mu(R \cap \mathrm{DISJ}_n^{-1}(0)) < \varepsilon\mu(R)$, we must have $\mu(R) < 2^{-\delta\sqrt{n}}$.

(e) Use part (a) to conclude that $\mathbf{BPP^{cc}}(\mathrm{DISJ}_n) \geq \Omega(\sqrt{n})$.

4