DSC 180A: Exercise Solutions

Ciro, Darren, Ivy, Ryan

November 24, 2025

Contents

1 Chapter 1 Exercises

Exercise 1.1

Exercise 1 Let $f : X \times Y \to \{0, 1\}$ have a 1-fooling set of size m, i.e. there are pairs (x_i, y_i) for $i \in [m]$ such that

- $f(x_i, y_i) = 1$ for all i, and
- for all $i \neq j$, at least one of $f(x_i, y_j)$ or $f(x_j, y_i)$ equals 0.

Show that any deterministic communication protocol for f must use at least $\log m$ bits.

Proof. Partition the first m elements of $[n]$ into $m = \lfloor n/k \rfloor$ disjoint blocks $S_1, \ldots, S_m$, each of size k. For each i, take the input pair $(A_i, B_i) = (S_i, S_i)$, $f(A_i, B_i) = 1$ since they intersect. While for $i \neq j$, $f(S_i, S_j) = 0$ since the blocks are disjoint.

Thus $\{(S_i, S_i) : i \in [m]\}$ is a 1-fooling set of size m, so any deterministic protocol needs at least $\log m = \log\lfloor n/k \rfloor$ bits. □

Exercise 1.3

Exercise 2 Alice and Bob each get a subset of size k of $[n] = \{1, 2, \ldots, n\}$. They want to know whether their sets intersect. Show that any deterministic protocol needs at least $\log\big(\lfloor n/k \rfloor\big)$ bits of communication.

Proof. Let $m = \lfloor n/k \rfloor$ and split the first mk elements into m disjoint blocks

$$S_1, S_2, \ldots, S_m$$

each of size k.

Now only look at inputs where Alice gets exactly one of these blocks and Bob also gets exactly one block. Then:

$$f(S_i, S_i) = 1 \quad \text{(same block, so they intersect)}$$

$$f(S_i, S_j) = 0 \text{ for } i \neq j \quad \text{(different blocks, disjoint)}$$

So we have m different 1-inputs that all have to lead to different transcripts. That forces at least $\log m = \log\lfloor n/k \rfloor$ bits. □

Exercise 1.6

Exercise 3 (1.6) Recall the protocol for the median of two lists discussed in the introduction. Consider the following varaint of the median problem. Alice is given a set $X \subseteq [n]$, Bob is given a set $Y \subseteq [n]$, and their goal is to compute the median of the set $X \cup Y$. The difference here is that we take the union as sets, so there are no repetitions. Show that the communication complexity of this problem is at least $\Omega(n/\log n)$. *Hint: Compute the median of the union of sets, as well as the union of sets.*

Proof. We take the set $[n]$, and divide it into $\log n$ non-overlapping continuous intervals. We know then that the combination of intervals which fall into $X \cup Y$ will then determine the median of the set. Since there are $2^{\frac{n}{\log n}}$ possible intervals, it will take $\omega(\log 2^{\frac{n}{\log n}}) = \Omega(\frac{n}{\log n})$ □

2 Chapter 2 Exercises

Exercise 2.1

Exercise 4 (2.1) Show that there is a matrix whose rank is 1, yet its communication complexity is 2. Conclude that +1 is necessary in "The communication complexity of M is at most $\text{rank}(M) + 1$.

Proof. Take $M = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. It has rank 1 but clearly takes 2 bits of communication. □

Exericse 2.6

Exercise 5 (2.6) For any symmetric matrix $M \in \{0,1\}^{n \times n}$, with ones in diagonal entries, show that $2^c \geq n^2/|M|$ where $|M|$ is the number of ones in M and c is the deterministic communication complexity of M.

Proof. The protocol partitions the matrix into at most $R \leq 2^c$ monochromatic rectangles. Consider only the 1-rectangles, labelling them R_1 to R_t where $t \leq R$.

For each 1-rectangle R_r, let its row set be A_r and its column set B_r. The diagonal entries are all 1, so they are exactly the $d_r := |A_r \cap B_r|$. There are n diagonals so

$$\sum_{r=1}^{t} k_r = n.$$

If $i, j \in A_r \cap B_r$, then (i, j) is in R_r and evaluates to 1. There must be at least k_r^2 of these entries. Hence $|M|$ must be at least the sum of all these:

$$\sum_{r=1}^{t} k_r^2 \leq |M|.$$

We can apply Cauchy-Schwarz, $(\sum k_r)^2 \leq t \sum k_r^2$, to get

$$n^2 = \left(\sum_{r=1}^{t} k_r\right)^2 \leq t \sum_{r=1}^{t} k_r^2 \leq r|M|.$$

Since $t \leq R \leq 2^c$ we have $2^c \geq n^2/|M|$ as desired. □

3 Chapter 3 Exercises

Problem 3.2

Exercise 6 (3.2) Show that there is a protocol for computing greater-than with communication complexity $\lceil \log(1/\epsilon) \rceil$ such that if the inputs are sampled uniformly and independently, then the average case error of the protocol is at most ϵ.

Proof. We suppose that Alice and Bob each have some input $x, y \in [k]$. We then can divide this set into $\frac{1}{\epsilon}$ intervals. Alice Identifyies which interval her input lands in, and communicates this to Bob, using $\log \frac{1}{\epsilon}$ bits. If Bobs input is in a smaller interval, the function returns 1, and in all other cases the function returns 0. The function will have error in the worst case whenever Alice and Bobs inputs are in the same interval. The communication of the function is $\log \frac{1}{\epsilon}$, for Alice to tell Bob which interval her input is in, and the probability that the inputs are in the same interval is $\frac{1}{\frac{1}{\epsilon}}$, or ϵ. □

4 Chapter 4 Exercises

Exercise 4.1

Exercise 7 (4.1) Suppose there are k parties in the number-on-forehead model. The ith party has the bit $X_i \in 0, 1$ written on their forehead, and $X_1, \ldots, X_k$ are sampled independently and uniformly at random. Show that there is a protocol for each party to privately write down a guess for the bit on their own forehead, without *any* communication, in such a way that the probability that all parties guess correctly is 1/2.

Proof. Let $X_1, X_2, \ldots, X_k \in \{0, 1\}$ be independent and uniformly random bits. In the number-on-forehead model, the i-th player sees all bits except X_i and must guess that value. We use the protocol below to guess the value of X_i:

$$g_i = \sum_{j \neq i}^{k} X_j \mod 2,$$

The condition for our guess to be correct is then,

$$X_i = \sum_{j \neq i}^{k} X_j \mod 2$$

We can determine whether or not the sum of all bits is zero by the following equation:

$$X_i + \sum_{j \neq i}^{k} X_j \mod 2 = 0$$

Which is the same as:

$$X_i = \sum_{j \neq i}^{k} X_j \mod 2$$

Therefore, we know that $X_i = g_i$ only if the sum of all bits is even.Given that $X_1, X_2, \ldots, X_k \in \{0, 1\}$ are independent and uniformly random bits there are 2^k unique bytes, assuming $k \geq 1$, we know that 2^{k-1} of the unique bytes sum to an even number. This results in:

$$P(Correct) = \frac{\textbf{number of bytes with even sums}}{\textbf{total number of bytes}} = \frac{2^{k-1}}{2^k} = \frac{1}{2}$$

□