TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

Tel Aviv University
Raymond and Beverly Sackler Faculty of Exact Sciences
The Blavatnik School of Computer Science

COMMUNICATION COMPLEXITY OF SET DISJOINTNESS OVER PRODUCT DISTRIBUTIONS

by

Peleg Kazaz

under the supervision of
Dr. Rotem Oshman

Thesis submitted in partial fulfillment of the requirements
for the degree of Master of Science

2025

Abstract

Communication Complexity of Set Disjointness Over Product Distributions

Peleg Kazaz
Master of Science
School of Computer Science
Tel Aviv University

Yao's two-party communication complexity is a well-studied model. The most simple settings are the deterministic settings. In these settings, we want to find an algorithm that gets the exact solution for every input. This model has two somewhat similar extensions. The first one is the randomized settings. In this model, every player gets a random string (private or public) and can use it in the protocol. In this case, we want the protocol to solve the problem with an error of up to ϵ (over the randomized strings).

Another model is when the inputs themselves are randomized. In this model, we need to design a protocol that solves the problem with an error of up to ϵ for every distribution on the inputs. Another interesting problem is to design a protocol that solves the problem for every product distribution (in which the players' inputs are independent.

One of the most important problems (sometimes called the "mother of problems") is the Set Disjointness problem. In this problem, every player gets an n-bit array and they are asked whether there is an index i where the i'th bit is turned on in all of their inputs.

This problem has been studied thoroughly on different models. It has been proved that every randomized protocol must use $\Omega(n)$ in order to achieve constant error bound from $\frac{1}{2}$. Also, it has been proved that the distributional communication complexity of this problem is also $\Omega(n)$ using the corruption methods. Another interesting question is what happens when we limit ourselves to product distribution. In this case, a tight bound of $\Theta(\sqrt(n))$ has been proved but only for two players.

In this paper, we tried to expand this bound for every number of players k. We have succeeded to prove the upper bound of $O(kn^{\frac{1}{k}})$. In the two-player protocol, Bob reveals a large number of his zeros to Alice using the public randomness and the fact that the inputs are drawn from known product distribution. This method is not easy to generalize since every player may eliminate $\frac{n}{k}$ zeros

Acknowledgements

I would like to thank my advisor, Rotem Oshman, for her patience, empathy and help throughout the long process. I would also like to thank my colleagues, Or Fischer and Tal Roth, for helping form and finalize the ideas.

Contents

Chapter 1

Introduction

1.1 k-n relation analysis

Let us pay attention that the mentioned upper bound may be not significant in some cases. Let us pay attention to the case in which $k = \alpha \log(n)$.

$$n^{1/k} = n^{\frac{1}{\alpha \log(n)}} = 2^{\frac{\log(n)}{\alpha \log(n)}} = 2^{1/\alpha}$$

In this case

$$n^{1-\frac{1}{k}} > n/2 \in \Omega(n)$$

It may seems that our protocol is not very helpful in this case.
Let us consider even bigger number of players: $k \in \omega(\log(n))$.
Now things act differently - For hard distribution most of the elements in the players' input should be 1.

1.2 $O(k + n\log^2(n))$-Protocol

Let us present a protocol which is useful only where we have many players ($k \in \omega(\log(n))$. In this case, most of the bits in our input should be 1's. For simplicity, let us denote

$$k = \log(n)\alpha(n)$$

1.3 Extra

Binary Distribution Let us consider a specific interesting distribution for $n = 2^{k-1}$. We think of $X_i \subseteq \{0, 1, ..., n-1\}$

For $i \in [k-1]$

$$X_i = \begin{cases} \{0 \leq m \leq n-1 \| m_{i-1} = 0\} \text{ w.p } 0.5 \\ \{0 \leq m \leq n-1 \| m_{i-1} = 1\} \text{ w.p } 0.5 \end{cases}$$

and for $i = k$

$$X_k = \begin{cases} \{0 \leq m \leq n-1 \| \bigoplus_{i=1}^{k-1} m_i = 0\} \text{ w.p } 0.5 \\ \{0 \leq m \leq n-1 \| \bigoplus_{i=1}^{k-1} m_i = 1\} \text{ w.p } 0.5 \end{cases}$$

where m_i is the i'th bit of m in binary representation. ($m_i := (m \,\&\, 2^{i-1}) \gg i-1$).
Let us pay attention for some simple properties. First of all $\forall_i |X_i| = \frac{n}{2}$. Moreover, it does not matter if we permute the players, for $i < k, |A_i| = 0.5|A_{i-1}|$ and generally for $i < k, |A_i| = 2^{k-1-i}$. $\Pr[DISJ] = 0.5$. The thing is that this distribution has a little entropy (k).

1.4 Appendix

Chapter 2

Related Work

2.1 2 Players Protocol

In [?], Babai, Frankl and Simon prove the following for two players:

Theorem 1. *For all product distributions μ,*

$$D^{\mu}(\mathit{DISJ}_n) \in O(\sqrt{n}\log n)$$

They presented a protocol that maintains a universe set U where $\bigcup_{i=1}^{k} X_i \subseteq U$ throughout the protocol. The protocol operates in iterations where in every iteration it reduces the universe's size.
The fact that the input's distribution is a product distribution is used in the part it reduces the universe's size. Every iteration operates as follows:

1. If Alice or Bob has a small input, calculate the precise solution and halt.

2. Bob calculate the probability for disjointness in the current universe over Alice's input distribution (Bob knows his own input).

3. If the probability is small, guess ”Intersecting”.

4. Otherwise, Bob finds in the public randomness a sample of Alice's input which is disjoint to his and sends the index of the sample to Alice.

5. They both reduce the universe by the sample set (which is disjoint to Bob's input).

In this protocol there are few important points. It depends strongly on the independence of the inputs where firstly Bob can calculate the probability for disjointness given its input and secondly both of them can sample Alice's input using the public randomness. Moreover, the index of the sample is short since the probability for disjointness isn't insignificant.

This protocol is not easily extended to multiplayer settings since in multiplayer, we need somehow choose who talks and which event's probability is used.

In the following paper, I tried to solve this issue using a sequential point of view for the disjointness problem.

Chapter 3

Preliminaries

3.1 Notation

For a vector x of length n, we let x_{-i} denote the vector of length $n-1$ obtained by dropping the i-th coordinate of x (where $i \in [n]$).

3.2 Multi-party Communication complexity

Multi-party Protocol Let f be a boolean function defined on k inputs with the same length n.

$$f : \{0,1\}^{nk} \to \{0,1\}$$

We usually denote $f(x_1, ..., x_k)$ where $x_i \in \{0,1\}^n$.
k parties wish to collaboratively evaluate f; the ith party knows only her input argument x_i; and each party has unlimited computational power. They share a blackboard, viewed by all parties, where they can exchange messages. The objective is to minimize the number of bits written on the board.

Multi-party Variations There are two variations of multi-party protocol which will not be discussed in this paper:

- NOF (Number on Forhead) - Every party knows each input argument except hers.
- Coordinator (Different communication scheme) - There is additional party named ”coordinator” which has private communication channel with each player.

Deterministic Communication Complexity For a function f, let Π be a deterministic protocol computing it. Given inputs $x = (x_1, ..., x_k)$ we denote the transcript by $\Pi(x)$. The cost of Π is the maximal length of a transcript:

$$\mathrm{CC}(\Pi) = \max_x(|\Pi(x)|)$$

The *deterministic communication complexity* of a function f is denoted by $D(f)$ and is the minimal cost of a protocol computing f:

$$D(f) = \min_{\Pi}(\mathrm{CC}(\Pi))$$

where the minimum is taken over all deterministic protocols that compute f with no errors.

Randomized Communication Complexity Randomized protocol is a protocol in which every player in addition to his input can use a random string to determine his message. The are two models of randomized communication complexity, based on whether or not the strings used by the different players are the same or not (public or private coins).

We say that a protocol computes a function f with error up to ϵ if

$$\Pr_R[\pi(x;R) \text{ computes } f \text{ incorrectly}] \leq \epsilon$$

where R is the random string (private or public).

For random protocols we define $\mathrm{CC}(\Pi)$ as the expected length of Π.

$$\mathrm{CC}(\Pi) = \max_x(\mathbb{E}_R[|\pi(x,R)|])$$

The *private-coin ϵ-error communication complexity of f* is defined as

$$R_\epsilon(f) = \min_{\Pi:\Pi \text{ computes } f \text{ with error } \epsilon} \mathrm{CC}(\Pi).$$

The *public-coin ϵ-error communication complexity of f* is defined similarly and denoted $R_\epsilon^{pub}(f)$.

Distributional Communication Complexity For a distribution μ over the inputs $\{0,1\}^{nk}$ and $\epsilon > 0$, Π is a *μ-distributional ϵ-error protocol of f* if

$$\Pr_{x \sim \mu}[\Pi(x) \text{ computes } f \text{ incorrectly}] \leq \epsilon$$

The length of such protocol is

$$|\Pi| = \mathbb{E}_{x\sim\mu}[\Pi(x)]$$

The *μ-distributional ϵ-error communication complexity of f* defined as

$$D_\epsilon^\mu(f) = \min_{\Pi:\ \mu\text{-distributional } \epsilon\text{-error}}(|\Pi|)$$

In this paper, we allow distributional protocol use random strings.

Distributional v.s. Randomized The following is a direct relations among randomized communication complexity and distributional communication complexity

Theorem 2. *For and f, μ and $\epsilon > 0$,*

$$R_\epsilon(f) \geq R_\epsilon^{pub}(f) \geq D_\epsilon^\mu(f),$$

3.3 Information Theory

Definition 3. *KL-Divergence for $D_{KL}(\frac{a}{b})$ is defined by*

$$D_{KL}(\tfrac{a}{b}) = \sum_{x \in \Omega} a(x) \log\left(\frac{a(x)}{b(x)}\right)$$

Lemma 4. *For X, Y, Z random variables*

$$I(X; Y|Z) = \mathbb{E}_{Y,Z}[D_{KL}\left(\tfrac{X|Y,Z}{X|Z}\right)]$$

Chapter 4

Upper bound for small parties

4.1 Overview of the Protocol

Lemma 5. *Suppose we have a set $A \subseteq [N]$ which is known to all players, and a set $A_i \subseteq A$ that is known to some player $i \in [k]$. Let $m, n \in \mathbb{N}$ be such that $m \leq |A| \leq n$, and assume further that $|A_i| \leq |A|/m$. Then there is a deterministic protocol where only player i speaks, that allows all players to learn a set $B \subseteq A \setminus A_i$ of size $|B| \geq m/2$, using $\log n$ bits of communication.*

Proof. Fix in advance a partition of A into sets $B_1, \ldots, B_\ell$, where $|B_j| = m/2$ for each $j = 1, \ldots, \ell - 1$, and the last set has size $m/2 \leq B_\ell \leq m - 1$. Note that we have $\ell > |A_i|$:
each B_j comprises $m/2$ elements, therefore:

$$\ell \geq \frac{|A|}{m/2} - 1$$

Simplifying the expression and using A_i's size assumption:

$$\frac{|A|}{m/2} - 1 = 2\frac{|A|}{m} - 1 > \frac{|A|}{m} \geq |A_i|.$$

Therefore, there exists $j \in [\ell]$ such that $B_j \cap A_i = \emptyset$: assume by contradiction that A_i intersects all ℓ sets $B_1, \ldots, B_\ell$.

$$|A_i| = |\bigcup_{j=1}^{\ell} (B_j \cap A_i)| \geq \sum_{j=1}^{\ell} |B_j \cap A_i| \geq \sum_{j=1}^{\ell} 1 = \ell$$

The protocol is therefore to have player i send the index $j \in [\ell]$ of a set B_j such that $A_i \cap B_j = \emptyset$. The requirements are satisfied: we have $B_j \subseteq A \setminus A_i$, and $|B_j| \geq m/2$. Specifying the index j requires $\log \ell \leq \log n$ bits.

□

4.1.1 Overview of the Protocol

Throughout the protocol, we maintain a *universe*, $U \subseteq [N]$, with the property that $\bigcap_i x_i \subseteq U$. Initially, $U = [N]$.

The protocol operates in *iterations*, where each iteration has two possible outcomes:

1. We eliminate at least a $1/\Theta(|U|^{1/k})$-fraction of elements from U
2. We halt and guess 0 as the answer. This output is not always correct, but it is correct with high probability over the inputs.

The protocol operates in iterations until the universe is small enough ($|U| < N^{\frac{1}{k}}$). This happens after at most $4N^{1-1/k}$ iterations. At this point each player i shares his input $x_i \cap U$, and the players calculate the exact answer and output it (output 1 iff $\bigcap_{i=1}^{k}(x_i \cap U) = \emptyset$).

Let us dive in to the method to eliminate a significant fraction of elements from the universe.

4.2 Sequential Point of View

Finding a player that can reduce the universe size. Consider a process where we start with some universe U (where $\bigcap_{i=1}^{k} x_i \subseteq U$), and gradually intersect it with more and more players' inputs, obtaining a sequence of sets

$$\bigcap_{j=1}^{k} x_j = U \cap \bigcap_{j=1}^{k} x_j \subseteq U \cap \bigcap_{j=1}^{k-1} x_j \subseteq \ldots \subseteq U \cap x_1 \cap x_2 \subseteq U \cap x_1 \subseteq U$$

Let us denote these sets $A_i(U) = U \cap (\bigcap_{j \leq i} x_j)$ (and in particular, $A_0(U) = U$).

$$\bigcap_{j=1}^{k} x_j = A_k(U) \subseteq A_{k-1}(U) \subseteq \ldots \subseteq A_1(U) \subseteq A_0(U) = U$$

We omit the universe U from our notation when it is clear from the context.

Pay attention that any element that is missing from some A_i is definitely not in the intersection. Our goal is to try to find two consecutive sets A_i, A_{i+1} such that A_{i+1} is *significantly smaller* than A_i, and then use this fact to eliminate many elements from consideration, reducing the universe size.

Definition 6. *With respect to a universe $U \subseteq [N]$ of size $n = |U| > 0$ and inputs $x_1, \ldots, x_k \subseteq [N]$, we say that an index $i \in [k]$ is* good *if*

1. $|A_i(U)|/|A_{i-1}(U)| < 1/n^{1/k}$*, and*
2. $|A_{i-1}(U)| \geq n^{1-(i-1)/k}$.

Lemma 7. *Fix a universe $U \subseteq [N]$ of size $|U| = n > 0$ and inputs $x_1, \ldots, x_k \subseteq [N]$, and suppose that $\bigcap_{i=1}^k x_i = \emptyset$. Then there is some good index $i \in [k]$.*

Proof. We first prove that there is an index $j \in [k]$ that satisfies the first property in Def. **??**, and then we show that the minimal such index j also has the second property.

Let $j \in [k]$ be the maximal index such that

$$A_{j-1} \neq \emptyset.$$

There is such a j, because $A_0 = U \neq \emptyset$.

Observe that $A_j = \emptyset$: if $j < k$ then this is immediate (otherwise j would not be maximal), and if $j = k$, then $A_j = A_k = U \cap \bigcap_{i=1}^k x_i = \emptyset$ by assumption. Thus,

$$\frac{|A_j|}{|A_{j-1}|} = \frac{0}{|A_{j-1}|} = 0 < \frac{1}{n^{1/k}},$$

so we know that (1) holds for j.

Let j^* denote the minimal index in $[k]$ that satisfies (1). Because of its minimality, for all $i \in [j^* - 1]$ we have

$$\frac{|A_i|}{|A_{i-1}|} \geq \frac{1}{n^{1/k}}.$$

Therefore,

$$\frac{|A_{j^*-1}|}{|A_0|} = \frac{|A_{j^*-1}|}{|A_{j^*-2}|} \cdot \frac{|A_{j^*-2}|}{|A_{j^*-3}|} \cdot \ldots \cdot \frac{|A_1|}{|A_0|} \geq \left(\frac{1}{n^{1/k}}\right)^{j^*-1} = \frac{1}{n^{\frac{j^*-1}{k}}}.$$

Since $|A_0| = n$,

$$|A_{j^*-1}| \geq n^{1-\frac{j^*-1}{k}}.$$

□

Let $D_i(U)$ be an indicator for the event that $\bigcap_{j=1}^k x_j = \emptyset$ and in addition i is a good index with respect to the universe U. The lemma implies that for any $U \subseteq [n]$ and inputs $x_1, \ldots, x_n$ such that $\bigcap_{i=1}^k x_i \subseteq U$, we have $\bigcap_{i=1}^k x_i = \emptyset$ iff $\bigvee_{i=1}^k D_i(U) = 1$. As usual, we omit the universe U from our notation where possible.

Significant players. A player $i \in [k]$ does not know whether or not i is good, as this depends on the inputs of the other players. However, player i can compute the *probability* that the conditions hold: define

$$\gamma_i = \gamma_i(x_i, U) := \Pr_{(X_{-i}) \sim \mu} \left[D_i(U) \mid X_i = x_i\right].$$

We say that player i is *significant* if $\gamma_i \geq \epsilon/(kN^{1-1/k})$.

4.3 The Protocol

For a given product distribution $\mu : \left(\{0,1\}^N\right)^k \to [0,1]$, we describe a protocol that errs with probability ϵ. Our protocol uses public randomness and has $\tilde{O}(kN^{1-\frac{1}{k}})$ bits of expected communication.

Initially, $U = [N]$, and $n = |U| = N$. The protocol proceeds in iterations, and in each iteration, we either halt and output 0, or we reduce the size of the universe by a $1/N^{1/k}$-fraction. Eventually, when $|U| \leq N^{1-1/k}$, each player i announces $x_i \cap U$. We then halt and output 1 if $\bigcap_{i=1}^k (x_i \cap U) = \emptyset$, or 0 otherwise.

Each iteration proceeds as follows:

(1) Termination condition: if $|U| \leq N^{1-1/k}$, each player i sends x_i to the coordinator, who computes and outputs the answer.

(2) Otherwise, the coordinator asks each player i whether i is significant in U (i.e., whether $\gamma_i(x_i, U) \geq \epsilon/kN^{1-\frac{1}{k}}$).

(3) If no player is significant, the coordinator outputs "not disjoint". Otherwise, let i be the first significant player. The coordinator informs every player that player i has been selected.

(4) The coordinator and the players use the public randomness to sample ***TODO: how many needed?*** sets $A_{i-1}^{(1)}, \ldots$ from the distribution of $A_{i-1}(U)$.

(5) Player i finds the index j of the first set $A_{i-1}^{(j)}(U)$ such that player i is critical. It sends the index j to the coordinator, who forwards it to the other players.

(6) The participants use the protocol from lemma 2.1 in order to discover $B \subseteq A_{i-1}^{(j)} \setminus X_i$ where $|B| > \frac{n^{1/k}}{2}$

(7) All participants set:

- $U \leftarrow U \setminus B$,
- $n \leftarrow |U|$,
- $x_i \leftarrow x_i \cap U$,
- $\mu \leftarrow \mu$ (not updated)

4.4 Properties of Our Protocol

Our protocol uses random coins and is described in the coordinator model. It uses an expected value of $O(kn^{1-\frac{1}{k}})$ bits of communication between the players.

4.4.1 Analysis

Rounds analysis We argue that the protocol should run only $4N^{1-\frac{1}{k}}$ rounds. As described above, every round where $|U| = n$, we omit $\frac{n^{1-\frac{1}{k}}}{2}$ indexes. Therefore if $f(n)$ is the function of number of rounds when starting with universe sized n, we can define it by

$$f(n) = \begin{cases} 1 & n \leq N^{\frac{1}{k}} \\ 1 + f(n - \frac{n^{1/k}}{2}) & \text{otherwise} \end{cases}$$

We use two simple technical claims in order to prove that $f(n) \leq 4n^{1-\frac{1}{k}}$.

Claim 8. *For $k \geq 2$ and every n: $n^{1-\frac{1}{k}} - \left(n - \frac{n^{1/k}}{2}\right)^{1-\frac{1}{k}} \geq 0.25$*

Proof. Let us define a function $g(x) = x^{1-\frac{1}{k}}$. We want to analyze:

$$n^{1-\frac{1}{k}} - \left(n - \frac{n^{1/k}}{2}\right)^{1-\frac{1}{k}} = g(n) - g\left(n - \frac{n^{1/k}}{2}\right)$$

By Lagrange's theorem, there exists a $c \in [0, \frac{n^{1/k}}{2}]$ such that

$$g(n) - g\left(n - \frac{n^{1/k}}{2}\right) = \frac{n^{1/k}}{2} g'(n - c)$$

By calculation:

$$g'(x) = \left(1 - \frac{1}{k}\right) x^{-1/k}$$

Therefore

$$g(n) - g\left(n - \frac{n^{1/k}}{2}\right) = \frac{n^{1/k}}{2}\left(1 - \frac{1}{k}\right)(n-c)^{-1/k} = \frac{(1-\frac{1}{k})}{2}\left(\frac{n}{n-c}\right)^{1/k} \geq \frac{(1-\frac{1}{k})}{2} \geq 0.25$$

for $k \geq 2$ □

Claim 9. *For $f(n)$ which is defined by*

$$f(n) = \begin{cases} 1 & n \leq N^{\frac{1}{k}} \\ 1 + f(n - \frac{n^{1/k}}{2}) & \textit{otherwise} \end{cases}$$

It is true that $f(n) \leq 4n^{1-\frac{1}{k}}$.

Proof. Let us prove it by induction:

a. Induction base (for $n \leq N^{1/k}$)

$$f(n) = 1 < 4 \leq 4n^{1-\frac{1}{k}}$$

b. The induction step

By definition, we know that

$$f(n) = 1 + f(n - \frac{n^{1/k}}{2})$$

In this point, we can use the inductive hypothesis

$$1 + f(n - \frac{n^{1/k}}{2}) \leq 1 + 4(n - \frac{n^{1/k}}{2})^{1-\frac{1}{k}}$$

Using the previous claim:

$$(n - \frac{n^{1/k}}{2})^{1-\frac{1}{k}} \leq n^{1-\frac{1}{k}} - 0.25$$

$$1 + 4(n - \frac{n^{1/k}}{2})^{1-\frac{1}{k}} \leq 1 + 4(n^{1-\frac{1}{k}} - 0.25)$$

Now we got exactly what we needed.

$$1 + 4(n^{1-\frac{1}{k}} - 0.25) = 4(n^{1-\frac{1}{k}})$$

To summarize, we proved that

$$f(n) \leq 4n^{1-\frac{1}{k}}$$

□

Error Analysis Let there be a round r. In this round, we error only if there was no significant player (in U_r) and therefore the coordinator answered ”not disjoint” but actually the inputs were disjoint.

$$\mu(\text{Err in round r}) \leq \mu(DISJ \wedge \forall_i \text{ i is not signficant})$$

Using the definition of ”significant player” we may rewrite it as:

$$\mu(\text{Err in round r}) \leq \mu(DISJ \wedge \forall_i \gamma_i(X_i, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}})$$

As proved in lemma 1.2, if the inputs are disjoint, there is a good player. $DISJ = \bigcup_{j=1}^{k} D_j(U_r)$

$$\mu(DISJ \wedge \forall_i \gamma_i(X_i, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}) = \mu(\bigcup_{j=1}^{k} D_j(U_r) \wedge \forall_i \gamma_i(X_i, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}})$$

Using union bound we may consider the sum of these probabilities.

$$\mu(\bigcup_{j=1}^{k} D_j(U_r) \wedge \forall_i \gamma_i(X_i, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}) \leq \sum_j \mu(D_j(U_r) \wedge \forall_i \gamma_i(X_i, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}})$$

For every element in the sum, we relax the event the only the specific player is good.

$$\sum_j \mu(D_j(U_r) \wedge \forall_i \gamma_i(X_i, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}) \leq \sum_j \mu(D_j(U_r) \wedge \gamma_j(X_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}})$$

At this point, we stop the calculation and consider a specific element in this sum. Every element is actually the event in which a player is good but not significant or in other words, the player is good but the probability that he is good is small. Using this definition it is pretty clear that the probability of this event is small.
Let us consider the expectation of this probability over the player's input.

$$\mu(D_j(U_r) \wedge \gamma_j(X_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}) = \mathop{\mathbb{E}}_{x_j \sim \mu}[\mu(D_j(U_r) \wedge \gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}} | X_j = x_j)]$$

Now the player's input is constant and the event that he is significance is also a constant.

$$\mathop{\mathbb{E}}_{x_j \sim \mu}[\mu(D_j(U_r) \wedge \gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}} | X_j = x_j)] = \mathop{\mathbb{E}}_{x_j \sim \mu}[\mu(D_j(U_r) | X_j = x_j) 1_{\gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}}]$$

Recall the definition of significance player $\gamma_i(x_i, U) := \Pr_{(X_{-i}) \sim \mu}[D_i(U) \mid X_i = x_i]$.

$$\mathop{\mathbb{E}}_{x_j \sim \mu}[\mu(D_j(U_r) | X_j = x_j) 1_{\gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}}] = \mathop{\mathbb{E}}_{x_j \sim \mu}[\gamma_j(x_j, U_r) 1_{\gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}}]$$

Now we got an expectation over a non-negative r.v ($\gamma_j(x_j, U_r)$) multiplied by the indicator of the event it is in smaller than $\frac{\epsilon}{kN^{1-\frac{1}{k}}}$. We may replace the r.v with $\frac{\epsilon}{kN^{1-\frac{1}{k}}}$.

$$\mathop{\mathbb{E}}_{x_j \sim \mu}[\gamma_j(x_j, U_r) 1_{\gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}}] \leq \mathop{\mathbb{E}}_{x_j \sim \mu}[\frac{\epsilon}{kN^{1-\frac{1}{k}}} 1_{\gamma_j(x_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}}] \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}$$

At this point, we finished considering the specific element (case in which a player is good but not significant) and we can resume the calculation of the whole error in round r.

$$\sum_j \mu(DISJ_j(U_r) \wedge \gamma_j(X_j, U_r) \leq \frac{\epsilon}{kN^{1-\frac{1}{k}}}) \leq \sum_j \frac{\epsilon}{kN^{1-\frac{1}{k}}} = k\frac{\epsilon}{kN^{1-\frac{1}{k}}} = \frac{\epsilon}{N^{1-\frac{1}{k}}}$$

To conclude, we just proved that the error in a specific round r:

$$\mu(\text{Err in round r}) \leq \frac{\epsilon}{N^{1-\frac{1}{k}}}$$

Now we are consider the overall error of the protocol (summing over all rounds):

$$\mu(Err) = \sum_r \mu(\text{Err in round r}) \leq \#\{\text{number of rounds}\}\frac{\epsilon}{N^{1-\frac{1}{k}}}$$

In our protocol there are $O(N^{1-\frac{1}{k}})$ so

$$\mu(Err) \in O(\epsilon)$$

Communication Analysis Let us first analyze the expected communication for a single round:

1. Every player sends a bit whether he is significant or not - k bits.

2. The coordinator informs everyone who is the chosen significant - $klogk$ bits.

3. The index j of $A_{i-1}^{(j)}$ is sent.

4. The player uses lemma 2.1 - $k\log(N)$ bits.

Let us calculate the 3rd part - j.
This index is a random variable which has a geometric distribution since $A_{i-1}^{(j)}$ are independent.

Recall that j is chosen where i is good in U.
Therefore we are looking for the following probability:

$$\Pr[\text{i is good in U}|X_i = x_i]$$

Since $D_i(U) = DISJ \cap \{\text{i is good in U}\}$ (by definition), $\{\text{i is good in U}\} \subseteq D_i(U)$ which leads to

$$\Pr[\text{i is good in U}|X_i = x_i] \geq \Pr[D_i(U)|X_i = x_i]$$

By definition of $\gamma_i(x_i, U)$:

$$\Pr[\text{i is good in U}|X_i = x_i] \geq \Pr[D_i(U)|X_i = x_i] = \gamma_i(x_i, U)$$

Since i is significant

$$\gamma_i(x_i, U) \geq \frac{\epsilon}{N^{1-\frac{1}{k}}}$$

To conclude

$$\Pr[\text{i is good in U}|X_i = x_i] \geq \frac{\epsilon}{N^{1-\frac{1}{k}}}$$

Now we can calculate easily the size of j

$$\mathbb{E}[J] = \frac{1}{\Pr[\text{i is good in U}|X_i = x_i]} \leq \frac{1}{\gamma_i(x_i, U)} \leq \frac{kN^{1-\frac{1}{k}}}{\epsilon}$$

By Jensen's inequality

$$\mathbb{E}[\log(J)] \leq \log(\mathbb{E}[J]) \leq \log(\frac{kN^{1-\frac{1}{k}}}{\epsilon}) \leq \log(N) + \log(k) + \log(\frac{1}{\epsilon})$$

So in total the cost of the round is

$$k + k\log(k) + k(\log(N) + \log(k) + \log(\frac{1}{\epsilon})) + k\log(N) \in O(k(\log(N) + \log(\frac{1}{\epsilon}))$$

The protocol operates at most $4(N^{1-\frac{1}{k}})$ rounds.
For the round where we terminate, we pay at most $kN^{\frac{1}{k}}\log(N)$.
So the total communication cost is

$$O(kN^{1-\frac{1}{k}}(\log(\frac{1}{\epsilon}) + \log(N)))$$

Chapter 5

Upper bound for large parties

5.1 Protocol and Properties

Critical Indexes Let us name an index i critical if:

$$\Pr[i \in \bigcap_{j=1}^{k} X_j] > \frac{\epsilon}{n}$$

This is a global term (not for a specific player).

The Protocol The protocol is pretty simple and straight-forward using the fact that there is a small number of zeros in the input.

(1) Without any communication, the players calculate what are the critical indexes (using the knowledge about the distribution but not about any current input): $U = \{i | \Pr[i \in \bigcap_{j=1}^{k} X_j] > \frac{\epsilon}{n}\}$.

(2) Every player j sends the indexes of his critical zeros to the coordinator: $Y_j = U \setminus X_j$

(3) The coordinator declares intersection iff $\bigcup_j Y_j \neq U$.

Communication The only communication done in this protocol is done in stage 2. In this stage, every player sends his critical zeros. We should calculate the expectation for the number of critical zeros for all players and pay $\log(n)$ for each one.
Let us examine a specific critical index i.
Let us denote:

$$p_{ij} = \Pr[i \in X_j]$$

By definition of critical index

$$\Pr[i \in \bigcap_{j=1}^{k} X_j] > \frac{\epsilon}{n}$$

Since μ is a product distribution

$$\Pr[i \in \bigcap_{j=1}^{k} X_j] = \prod_{j=1}^{k} p_{ij}$$

Combining these two equations:

$$\prod_{j=1}^{k} p_{ij} > \frac{\epsilon}{n}$$

Using Lagrange multipliers:

$$\sum_{j=1}^{k} p_{ij} \geq k\left(\frac{\epsilon}{n}\right)^{\frac{1}{k}}$$

At this point, let us examine the zeros in index i

$$\mathbb{E}[\text{Zeros in i}] = k - \sum_{j=1}^{k} p_{ij} \leq k\left(1 - \left(\frac{\epsilon}{n}\right)^{\frac{1}{k}}\right)$$

The total number of zeros:

$$\mathbb{E}[\text{Zeros}] = \sum_{i=1}^{n} \mathbb{E}[\text{Zeros in i}] \leq nk\left(1 - \left(\frac{\epsilon}{n}\right)^{1/k}\right)$$

Using log definition

$$nk\left(1 - \left(\frac{\epsilon}{n}\right)^{1/k}\right) = nk\left(1 - e^{\frac{\log\frac{\epsilon}{n}}{k}}\right)$$

since $k \in \omega(\log(n))$

$$\frac{\log\frac{\epsilon}{n}}{k} = -\frac{\log\frac{n}{\epsilon}}{k} \to 0^{-}$$

Now we can use the limit $x \sim 1 - e^{x}$ for $x \to 0^{-}$

$$nk\left(1 - e^{\frac{\log\frac{\epsilon}{n}}{k}}\right) \sim nk\frac{\log\frac{n}{\epsilon}}{k} = n\log\frac{n}{\epsilon}$$

So total expected communication complexity for this protocol is

$$k + n\log\frac{n}{\epsilon}\log n$$

Error We error only if there is an intersection outiside important indexes (in this case we falsly output disjoint).

$$\Pr[\text{ERROR}] = \Pr[\bigcup_{i \notin U}\{i \in \bigcap_{j} X_j\}]$$

Using union bound

$$\Pr[\bigcup_{i\notin U}\{i \in \bigcap_j X_j\}] \leq \sum_{i\notin U} \Pr[i \in \bigcap_j X_j]$$

Using the definition of uncritical index $\Pr[i \in \bigcap_{j=1}^k X_j] \leq \frac{\epsilon}{n}$

$$\sum_{i\notin U} \Pr[i \in \bigcap_j X_j] \leq n\frac{\epsilon}{n} = \epsilon$$

Claim 10. *TODO-Move to appendix?*
For $p_1, p_2, ..., p_k \in [0,1]$
If

$$\prod_{i=1}^k p_i \geq \frac{\epsilon}{n}$$

We can know that

$$\sum_{i=1}^k p_i \geq k\left(\frac{\epsilon}{n}\right)^{1/k}$$

Proof. By lagrange multipliers let us denote a target function

$$f(x_1, ..., x_k) = \sum_{i=1}^k x_i$$

A constraint function

$$g(x_1, ..., x_k) = \prod_{i=1}^k x_i - \frac{\epsilon}{n}$$

Lagrange function

$$\mathcal{L}(x_1, ..., x_k, \lambda) = \sum_{i=1}^k x_i - \lambda\left(\prod_{i=1}^k x_i - \frac{\epsilon}{n}\right)$$

$$\frac{\partial \mathcal{L}}{\partial x_i} = 1 - \lambda \prod_{j\neq i} x_j$$

$$\frac{\partial \mathcal{L}}{\partial \lambda} = \prod_{i=1}^k x_i - \frac{\epsilon}{n}$$

By (2):

$$\begin{aligned}
\prod_{i=1}^{k} x_i &= \frac{\epsilon}{n} \\
1 &= \frac{\lambda \frac{\epsilon}{n}}{x_i} \\
x_i &= \lambda \frac{\epsilon}{n} \\
\left(\lambda \frac{\epsilon}{n}\right)^k &= \frac{\epsilon}{n} \\
\lambda &= \left(\frac{\epsilon}{n}\right)^{\frac{1}{k}-1} \\
x_i &= \left(\frac{\epsilon}{n}\right)^{\frac{1}{k}} \\
f_{\text{min}} &= k\left(\frac{\epsilon}{n}\right)^{\frac{1}{k}}
\end{aligned}$$

□

Chapter 6

Lower bound for AND_k for small parties

6.1 Lower Bound

Introduction Usually in lower bound using information theory techniques, we firstly move to the problem of disjointness where $n = 1$ denoted as AND$_k$ which is the problem where every player has one bit and they need to answer whether they all got 1 or not. After moving to this problem, we calculate how much information is needed in order to solve it.

6.1.1 AND_k Information Cost

Introduction We are going to bound the information cost for a protocol that solves AND_k. Our analysis is divided into three blocks:
1 - Using the error of the protocol in order to conclude it must know some information about specific player's input.
2 - Distinguishing this input is leaking some information (specifically KL-Divergence)
3 - Concluding this for the general information cost of the protocol

Definitions

Definition 11. *Denote two sets of transcripts:*
T_1 *- transcripts which are ended with positive answers (there is an intersection).*
T_0 *- transcripts which are ended with negative answers (there is no intersection).*

Protocol properties For a transcript π and player i there is a function $q_i(\pi, x_i) \in [0, 1]$ where

$$Pr[\pi|x] = \prod_{i=1}^{k} q_i(\pi, x_i)$$

Definition 12.

$$\lambda_i(\pi) = \frac{q_i(\pi,0)}{q_i(\pi,1)}$$

We should think about this as how much this transcript prefers that $x_i = 0$ over $x_i = 1$.

Definition 13. *For $\alpha \in \mathbb{R}$ where $\alpha \geq 1$, let us define a set of transcripts*

$$A = \{\pi | \forall_{i\in[k]} \lambda_i(\pi) < \alpha\}$$

Part 1 - Protocol Error Analysis

Lemma 14. *For any input $x \in \{0,1\}^k$, and any transcript π. For $Z(x) = \{i \in k | x_i = 0\}$, it is true that*

$$\frac{Pr[\pi|X = x]}{Pr[\pi|X = 1^k]} = \prod_{i\in Z(x)} \lambda_i(\pi)$$

Proof. By definition of q function

$$\frac{Pr[\pi|X = x]}{Pr[\pi|X = 1^k]} = \frac{\prod_{i\in[k]} q_i(\pi, x_i)}{\prod_{i\in[k]} q_i(\pi, 1)}$$

By definition of $Z(x)$

$$\frac{\prod_{i\in[k]} q_i(\pi, x_i)}{\prod_{i\in[k]} q_i(\pi, 1)} = \prod_{i\in Z(x)} \frac{q_i(\pi,0)}{q_i(\pi,1)}$$

By definition of $\lambda_i(\pi)$

$$\prod_{i\in Z(x)} \frac{q_i(\pi,0)}{q_i(\pi,1)} = \prod_{i\in Z(x)} \lambda_i(\pi)$$

□

Lemma 15.

$$\Pr[A|x = 0^k] \leq \epsilon(1 + \alpha^k)$$

The set in which the transcripts do not prefer 0 over 1 is not very common under $x = 0^k$.

Proof. For T_0, T_1 defined as mentioned, let us bound the probability for $A \bigcap T_0$ and $A \bigcap T_1$.

1. For $A \bigcap T_0$:

Let there be $\pi \in A \bigcap T_0$.

For this π, let us use the previous lemma for $x = 0^k$

$$\frac{Pr[\pi|X = 0^k]}{Pr[\pi|X = 1^k]} = \prod_{i\in Z(0^k)} \lambda_i(\pi)$$

Since $Z(0^k) = [k]$

$$\frac{Pr[\pi|X = 0^k]}{Pr[\pi|X = 1^k]} = \prod_{i \in [k]} \lambda_i(\pi)$$

Since $\pi \in A$, we know that $\forall_{i \in [k]} \lambda_i(\pi) < \alpha$

$$\frac{Pr[\pi|X = 0^k]}{Pr[\pi|X = 1^k]} < \alpha^k$$

Summing over all $\pi \in A \bigcap T_0$

$$\Pr[A \bigcap T_0 | x = 0^k] < \alpha^k \Pr[A \bigcap T_0 | x = 1^k]$$

Since $A \bigcap T_0 \subseteq T_0$

$$\alpha^k \Pr[A \bigcap T_0 | x = 1^k] \leq \alpha^k \Pr[T_0 | x = 1^k]$$

Since the answer of disjointness is 1 for the input $x = 1^k$, we know that $\{T_0 | x = 1^k\} = \{\text{ERROR} | x = 1^k\}$
.

$$\alpha^k \Pr[T_0 | x = 1^k] = \alpha^k \Pr[\text{ERROR} | x = 1^k]$$

For a protocol which errors ϵ for any input

$$\Pr[\text{ERROR} | x = 1^k] \leq \epsilon$$

We now have that

$$\Pr[A \bigcap T_0 | x = 0^k] \leq \alpha^k \epsilon$$

2. For $A \bigcap T_1$:
Since $A \bigcap T_1 \subseteq T_1$

$$\Pr[A \bigcap T_1 | x = 0^k] \leq \Pr[T_1 | x = 0^k]$$

Since the answer of disjointness is 0 for the input $x = 0^k$, we know that $\{T_1 | x = 0^k\} = \{\text{ERROR} | x = 0^k\}$
.

$$\Pr[T_1 | x = 0^k] = \Pr[\text{ERROR} | x = 0^k]$$

For a protocol which errors ϵ for any input

$$\Pr[\text{ERROR} | x = 0^k] \leq \epsilon$$

We now have that

$$\Pr[A \bigcap T_1 | x = 0^k] \leq \epsilon$$

3. To conclude:

$$\Pr[A|x = 0^k] =\leq \Pr[A \bigcap T_0|x = 0^k] + \Pr[A \bigcap T_1|x = 0^k] < \epsilon(1 + \alpha^k)$$

□

Lemma 16. *For $A_i^{\complement} = \{\pi|\lambda_i(\pi) \geq \alpha\}$, there exists i where*

$$\Pr[A_i^{\complement}|x = 0^k] \geq \frac{1 - \epsilon(1 + \alpha^k)}{k}$$

Proof. Using the previous lemma,

$$\Pr[A|x = 0^k] \leq \epsilon(1 + \alpha^k)$$

Using set compliment

$$\Pr[A^{\complement}|x = 0^k] \geq 1 - \epsilon(1 + \alpha^k)$$

Since $A^{\complement} = \{\pi|\exists_i \lambda_i(\pi) \geq \alpha\}$, we know that

$$A^{\complement} = \bigcup_i A_i^{\complement}$$

Therefore

$$\sum_{i=1}^{k} \Pr[A_i^{\complement}|x = 0^k] \geq \Pr[A^{\complement}|x = 0^k]$$

Combining these facts

$$\sum_{i=1}^{k} \Pr[A_i^{\complement}|x = 0^k] \geq 1 - \epsilon(1 + \alpha^k)$$

Therefore there exists i where

$$\Pr[A_i^{\complement}|x = 0^k] \geq \frac{1 - \epsilon(1 + \alpha^k)}{k}$$

□

That is the finish line of this part. We got a set of transcripts that has a nice probability under $x = 0^k$ where the transcripts prefer strongly 0 over 1 for some index. We may use this technique in different ways depends on our distribution of inputs. For small k our distribution gives a high probability for 0^k which is pretty convenient. For other distribution, we want to use the other method.
This is a rough method in order to use the fact that the protocol has to be ”biased” in terms of λ_i in order to have a low error.

Part 2 - Divergence In this part, we are going to show that the set we found in the last part is contributing large enough divergence. This will be enough since $x = 0^k$ has a high probability under our distribution.

Let us analyze the connection between $\lambda_i(\pi)$ to its divergence.

Lemma 17. *For 0-1 distribution μ, player i and transcript π*

$$\Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi] = \frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}}$$

$$\Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi] = \frac{\mu(1)}{\lambda_i(\pi)\mu(0) + \mu(1)}$$

Proof. By Bayes theorem

$$\Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi] = \frac{\Pr[\pi|X = 0^k]\Pr[X_i = 0|X_{-i} = 0^{k-1}]}{Pr[\pi|X_{-i} = 0^{k-1}]} =$$

By the law of total probability for $\pi|X_{-i} = 0^{k-1}$ with $X_i = 0, 1$

$$\frac{\Pr[\pi|X = 0^k]\Pr[X_i = 0|X_{-i} = 0^{k-1}]}{Pr[\pi, X_i = 0|X_{-i} = 0^{k-1}] + Pr[\pi, X_i = 1|X_{-i} = 0^{k-1}]} =$$

Using conditional probability for the denominator

$$\frac{\Pr[\pi|X = 0^k]\Pr[X_i = 0|X_{-i} = 0^{k-1}]}{\Pr[\pi|X = 0^k]\Pr[X_i = 0|X_{-i} = 0^{k-1}] + \Pr[\pi|X = 0^{i-1}10^{k-i}]\Pr[X_i = 1|X_{-i} = 0^{k-1}]} =$$

Since the input is drawn using product distribution

$$\frac{\Pr[\pi|X = 0^k]\mu(0)}{\Pr[\pi|X = 0^k]\mu(0) + \Pr[\pi|X = 0^{i-1}10^{k-i}]\mu(1)} =$$

Divide both with $\Pr[\pi|X = 0^k]$

$$\frac{\mu(0)}{\mu(0) + \frac{\Pr[\pi|X=0^{i-1}10^{k-i}]}{\Pr[\pi|X=0^k]}\mu(1)} =$$

Using the definition of $\lambda_i(\pi)$

$$\frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}}$$

This proves the first equation. For the second equation

$$\Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi] = 1 - \Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi]$$

Using the first equation

$$1 - \Pr[X_i = 0 | X_{-i} = 0^{k-1}, \pi] = 1 - \frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}}$$

Some algebraic expansion

$$1 - \frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}} = \frac{\frac{\mu(1)}{\lambda_i(\pi)}}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}} = \frac{\mu(1)}{\lambda_i(\pi)\mu(0) + \mu(1)}$$

□

Lemma 18. *For a specific transcript π and player i where $\lambda_i(\pi) \geq \alpha$, for big enough n*

$$D_{KL}\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}=0^{k-1}}\right) \geq \frac{\mu(1)}{4}$$

Proof. By definition of KL-Divergence

$$D_{KL}\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}=0^{k-1}}\right) =$$

$$\Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi] \log\left(\frac{\Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi]}{\Pr[X_i = 0|X_{-i} = 0^{k-1}]}\right) +$$

$$\Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi] \log\left(\frac{\Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi]}{\Pr[X_i = 1|X_{-i} = 0^{k-1}]}\right)$$

Part 1 of the divergence: Since the input is drawn using product distribution

$$\Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi] \log\left(\frac{\Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi]}{\Pr[X_i = 0|X_{-i} = 0^{k-1}]}\right) = \Pr[X_i = 0|X_{-i} = 0^{k-1}, \pi] \log\left(\frac{\Pr[X_i = 0|X_{-i} = 0^{k-1}}{\mu(0)}\right.$$

Using the previous lemma

$$\frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}} \log\left(\frac{\frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}}}{\mu(0)}\right) =$$

Some algebraic expansion

$$\frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}} \log\left(\frac{1}{\mu(0) + \frac{\mu(1)}{\lambda_i(\pi)}}\right) \geq$$

Using $\lambda_i(\pi) \geq \alpha$

$$\frac{\mu(0)}{\mu(0) + \frac{\mu(1)}{\alpha}} \log\left(\frac{1}{\mu(0) + \frac{\mu(1)}{\alpha}}\right) =$$

Since $\mu(0) = 1 - \mu(1)$

$$\frac{\mu(0)}{1 - \mu(1) + \frac{\mu(1)}{\alpha}} \log\left(\frac{1}{1 - \mu(1) + \frac{\mu(1)}{\alpha}}\right) =$$

Some algebraic expansion

$$\frac{\mu(0)}{1 - \mu(1)(1 - \frac{1}{\alpha})} \log\left(\frac{1}{1 - \mu(1)(1 - \frac{1}{\alpha})}\right) =$$

Some more algebraic expansion

$$\frac{\mu(0)}{1 - \mu(1)(1 - \frac{1}{\alpha})} \log\left(1 + \frac{\mu(1)(1 - \frac{1}{\alpha})}{1 - \mu(1)(1 - \frac{1}{\alpha})}\right) \geq$$

Using $\log(1 + x) \sim x$ for $x \to 0$

$$\frac{\mu(0)(\mu(1)(1 - \frac{1}{\alpha}))}{2\left(1 - \mu(1)(1 - \frac{1}{\alpha})\right)^2} \geq \frac{\mu(1)}{2}$$

Part 2 of the divergence: Since the input is drawn using product distribution

$$\Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi] \log\left(\frac{\Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi]}{\Pr[X_i = 1|X_{-i} = 0^{k-1}]}\right) = \Pr[X_i = 1|X_{-i} = 0^{k-1}, \pi] \log\left(\frac{\Pr[X_i = 1|X_{-i} = 0^{k-1}}{\mu(1)}\right.$$

Using the previous lemma

$$\frac{\mu(1)}{\lambda_i(\pi)\mu(0) + \mu(1)} \log\left(\frac{\frac{\mu(1)}{\lambda_i(\pi)\mu(0)+\mu(1)}}{\mu(1)}\right) =$$

Some algebraic expansion

$$\frac{\mu(1)}{\lambda_i(\pi)\mu(0) + \mu(1)} \log\left(\frac{1}{\lambda_i(\pi)\mu(0) + \mu(1)}\right) = -\mu(1)\frac{\log(\lambda_i(\pi)\mu(0) + \mu(1))}{\lambda_i(\pi)\mu(0) + \mu(1)}$$

Pay attention that since $\mu(1) \geq 0$, $\mu(0) \geq \frac{1}{2}$ and $\lambda_i(\pi) \geq \alpha$

$$\lambda_i(\pi)\mu(0) + \mu(1) \geq \lambda_i(\pi)\mu(0) \geq \frac{\lambda_i(\pi)}{2} \geq \frac{\alpha}{2}$$

Since $\frac{log(x)}{x} \to 0$ when $x \to \infty$, for big enough α

$$-\mu(1)\frac{\log(\lambda_i(\pi)\mu(0) + \mu(1))}{\lambda_i(\pi)\mu(0) + \mu(1)} \geq -\frac{\mu(1)}{4}$$

For conclusion If $\lambda_i(\pi) \geq \alpha$, for big enough n:

$$D_{KL}\left(\frac{X_i|\pi,X_{-i}=0^{k-1}}{X_i|X_{-i}=0^{k-1}}\right) \geq \frac{\mu(1)}{2} - \frac{\mu(1)}{4} = \frac{\mu(1)}{4}$$

□

Part 3 - Information Summary

Theorem 19.

$$I(X;\Pi) \in \Omega\left(\frac{n^{-\frac{1}{k}}}{k}\right)$$

Proof. By definition of X

$$I(X;\Pi) = I(X_i, X_{-i};\Pi)$$

Using chain rule for mutual information

$$I(X_i, X_{-i};\Pi) = I(X_{-i};\Pi) + I(X_i;\Pi|X_{-i})$$

Since mutual information is nonnegative

$$\overbrace{I(X_{-i};\Pi)}^{\geq 0} + I(X_i;\Pi|X_{-i}) \geq I(X_i;\Pi|X_{-i})$$

Using the mutual information - kl-divergence relation

$$I(X_i;\Pi|X_{-i}) = \mathbb{E}_{x,\pi\sim\mu}\left(D_{KL}\left(\frac{X_i|\pi,X_{-i}}{X_i|X_{-i}}\right)\right)$$

Picking only a specific element ($x = 0^k$) in the expectation sum

$$\mathbb{E}_{x,\pi\sim\mu}\left(D_{KL}\left(\frac{X_i|\pi,X_{-i}}{X_i|X_{-i}}\right)\right) \geq \mu(0^k)\mathbb{E}_{\pi\sim x=0^k}\left(D\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}}\right)\right)$$

Looking only at transcripts in $A_i^{\complement}$

$$\mu(0^k)\mathbb{E}_{\pi\sim x=0^k}\left(D\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}}\right)\right) \geq \mu(0^k)\Pr[A_i^{\complement}|x=0^k]\mathbb{E}_{\pi\sim x=0^k|\pi\in A_i^{\complement}}\left(D\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}}\right)\right)$$

Using Part 1

$$\mu(0^k)\Pr[A_i^{\complement}|x=0^k]\mathbb{E}_{\pi\sim x=0^k|\pi\in A_i^{\complement}}\left(D\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}}\right)\right) \geq \mu(0^k)\frac{1-\epsilon(1+\alpha^k)}{k}\mathbb{E}_{\pi\sim x=0^k|\pi\in A_i^{\complement}}\Bigg(D\Bigg(\frac{X_i|\pi, X_{-i}=}{X_i|X_{-i}}$$

Using Part 2

$$\mu(0^k)\frac{1-\epsilon(1+\alpha^k)}{k}\mathbb{E}_{\pi\sim x=0^k|\pi\in A_i^{\complement}}\left(D\left(\frac{X_i|\pi, X_{-i}=0^{k-1}}{X_i|X_{-i}}\right)\right)\geq\mu(0^k)\frac{1-\epsilon(1+\alpha^k)}{k}\frac{\mu(1)}{4}$$

Since $\mu(1)=n^{-\frac{1}{k}}$ and $\mu(0)=1-n^{-\frac{1}{k}}$

$$\mu(0^k)\frac{1-\epsilon(1+\alpha^k)}{k}\frac{\mu(1)}{4}=\left(1-n^{-\frac{1}{k}}\right)^k\cdot\frac{1-\epsilon(1+\alpha^k)}{k}\cdot\frac{n^{-\frac{1}{k}}}{4}\in\Omega\left(\frac{n^{-\frac{1}{k}}}{k}\right)$$

□

תקציר

מודל סיבוכיות התקשורת של יאו בשני שחקנים הוא מודל נפוץ שנחקר רבות. למודל זה מספר וריאציות, כשהפשוטה ביניהן היא המודל הדטרמניסטי. במודל זה, אנחנו מנסים למצוא פרוטוקול שעבור כל קלט מצליח למצוא את הפתרון.

למודל זה קיימות שתי הרחבות דומות במידה. הרחבה ראשונה היא המודל הרנדומי. במודל זה כל שחקן מקבל מחרוזת רנדומית (פרטית או פומבית). מטרת הפרוטוקול היא להצליח בסיכוי טוב לכל קלט (סיכוי טוב על פני כלל המחרוזות הרנדומיות שהשחקנים קיבלו).

הרחבה שניה של המודל הדטרמיניסטי היא המודל ההתפלגותי. במודל זה הקלטים אותם השחקנים מקבלים נבחרים מתוך התפלגות נתונה. במודל זה, מטרת הפרוטוקול היא להצליח בסיכוי על פני התפלגות הקלטים (ובמקרה זה יכולים להיות מעט קלטים עבורם הפרוטוקול נכשל דטרמיניסטית). תחת מודל זה ניתן לבחון ספציפית פרוטוקול שמצליח למול התפלגויות מכפלה – התפלגויות עבורן הקלטים של השחקים השונים הם בלתי תלויים (בדומה לבעיות רבות בעולם האמיתי).

אחת הבעיות החשובות בעולם סיבוכיות התקשורת היא Set Disjointness. בבעיה זו, כל שחקן מקבל מערך ביטים (או לחלופין מחרוזת בינארית). על השחקנים לענות האם קיים אינדקס i עבורו הביט בכל אחד המערכים של השחקנים במקום הi – דלוק.

בעיה זו נחקרה רבות במודלים שונים עבור שני שחקנים. הוכח כי כל פרוטוקול רנדומי שמצליח להשיג שגיאה חסומה מ1/2 חייב להשתמש ב$\Omega(n)$ ביטים (כלומר לא יותר טוב מהפרוטוקול הנאיבי). בנוסף, הוכח כי גם סיבוכיות התקשורת במודל ההתפלגותי חסומה מלרע ב$\Omega(n)$ ביטים.

וריאציה מעניינת של בעיה זו היא הגבלת ההתפלגויות להתפלגויות במכפלה. במקרה זה הוכח כי סיבוכיות התקשורת ההדוקה עבור שני שחקנים היא $\Theta(\sqrt{n})$.

בעבודה זו, אנו מרחיבים חסם זה למספר רב של שחקנים. עבור מספר שחקנים קטן אך קבוע k – סיבוכיות התקשורת של הבעיה היא $O(n^{1-\frac{1}{k}})$. עבור מספר רב של שחקנים $\omega(\log(n))$ חסם זה אינו משמעותי אך הצלחנו למצוא חסם אחר של $O(k+nlog^2(n))$ ביטים.

בעבודה זו, לא הצלחנו להוכיח חסם תחתון לבעיית הDisjointness אך תוך עבודה על חסם זה הצלחנו להוכיח חסם תחתון עבור בעיית AND_k של ב$\Omega(\frac{1}{kn^{1/k}})$ ביטים.

TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

הפקולטה למדעים מדויקים ע״ש ריימונד ובברלי סאקלר

בית הספר למדעי המחשב ע״ש בלבטניק

סיבוכיות תקשורת
בעיית Disjointness
תחת התפלגות מכפלה

חיבור זה הוגש כחלק מהדרישות לקבלת התואר

"מוסמך האוניברסיטה(M.Sc.)"

על ידי

פלג קזז

עבודת המחקר בוצעה בהנחייתה של

ד"ר רותם אושמן