A strong direct product theorem for two-way public coin communication complexity

Rahul Jain*

October 5, 2010

Abstract

We show a direct product result for two-way public coin communication complexity of all relations in terms of a new complexity measure that we define. Our new measure is a generalization to non-product distributions of the two-way product subdistribution bound of J, Klauck and Nayak [JKN08], thereby our result implying their direct product result in terms of the two-way product subdistribution bound.

1 Introduction

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\varepsilon > 0$. Let Alice with input $x \in \mathcal{X}$, and Bob with input $y \in \mathcal{Y}$, wish to compute a $z \in \mathcal{Z}$ such that $(x, y, z) \in f$. We consider the model of public coin two-way communication complexity in which Alice and Bob exchange messages possibly using pubic coins and at the end output z. Let $\mathsf{R}^{2,\mathsf{pub}}_{\varepsilon}(f)$ denote the communication of the best protocol $\mathcal{P}$ which achieves this with error at most ε (over the public coins) for any input (x, y). Now suppose that Alice and Bob wish to compute f simultaneously on k inputs $(x_1, y_1), \ldots, (x_k, y_k)$ for some $k \geq 1$. They can achieve this by running k independent copies of $\mathcal{P}$ in parallel . However in this case the overall success could be as low as $(1 - \varepsilon)^k$. Strong direct product conjecture for f states that this is roughly the best that Alice and Bob can do. We show a direct product result in terms of a new complexity measure, the ε error two-way conditional relative entropy bound of f, denoted $\mathsf{crent}^2_{\varepsilon}(f)$, that we introduce.

Theorem 1.1 *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation. Let $k \geq 1$ be a natural number. Then,*

$$\mathsf{R}^{2,\mathsf{pub}}_{1-2^{-\Omega(k)}}(f^k) \geq \Omega(k \cdot \mathsf{crent}^2_{1/3}(f)) \ .$$

*Centre for Quantum Technologies and Department of Computer Science, National University of Singapore. rahul@comp.nus.edu.sg

Our measure $\mathsf{crent}^2_\varepsilon(f)$ forms a lower bound on $\mathsf{R}^{2,\mathsf{pub}}_\varepsilon(f)$ and forms an upper bound on the two-way product subdistribution bound of J., Klauck, Nayak [JKN08], thereby implying their direct product result in terms of the two-way product subdistribution bound.

There has been substantial prior work on the strong direct product question and the weaker direct sum and weak direct product questions in various models of communication complexity, e.g. [IRW94, PRW97, CSWY01, Sha03, JRS03, KŠdW04, Kla04, JRS05, BPSW07, Gav08, JKN08, JK09, HJMR09, BBR10, BR10, Kla10].

In the next section we provide some information theory and communication complexity preliminaries that we need. We refer the reader to the texts [CT91, KN97] for good introductions to these topics respectively. In section 3 we introduce our new bound and show the direct product result.

2 Preliminaries

Information theory

Let $\mathcal{X}, \mathcal{Y}$ be sets and k be a natural number. Let $\mathcal{X}^k$ represent $\mathcal{X} \times \cdots \times \mathcal{X}$, k times. Let μ be a distribution over $\mathcal{X}$ which we denote by $\mu \in \mathcal{X}$. We use $\mu(x)$ to represent the probability of x under μ. The entropy of μ is defined as $S(\mu) = -\sum_{x\in\mathcal{X}} \mu(x) \log \mu(x)$. Let X be a random variable distributed according to μ which we denote by $X \sim \mu$. We use the same symbol to represent a random variable and its distribution whenever it is clear from the context. For distributions $\mu, \mu_1 \in \mathcal{X}$, $\mu \otimes \mu_1$ represents the product distribution $(\mu \otimes \mu_1)(x) = \mu(x) \otimes \mu_1(x)$ and μ^k represents $\mu \otimes \cdots \otimes \mu$, k times. The ℓ_1 distance between distributions μ, μ_1 is defined as $||\mu - \mu_1||_1 = \frac{1}{2}\sum_{x\in\mathcal{X}} |\mu(x) - \mu_1(x)|$. Let $\lambda, \mu \in \mathcal{X} \times \mathcal{Y}$. We use $\mu(x|y)$ to represent $\mu(x,y)/\mu(y)$. When we say $XY \sim \mu$ we assume that $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$. We use μ_x and Y_x to represent $Y|\ X = x$. The conditional entropy of Y given X, is defined as $S(Y|X) = \mathbb{E}_{x\leftarrow X} S(Y_x)$. The relative entropy between λ and μ is defined as $S(\lambda||\mu) = \sum_{x\in\mathcal{X}} \lambda(x) \log \frac{\lambda(x)}{\mu(x)}$. We use the following properties of relative entropy at many places without explicitly mentioning.

Fact 2.1 1. *Relative entropy is jointly convex in its arguments, that is for distributions* $\lambda_1, \lambda_2, \mu_1, \mu_2$

$$S(p\lambda_1 + (1-p)\lambda_2 \ || \ p\mu_1 + (1-p)\mu_2) \leq p \cdot S(\lambda_1||\mu_1) + (1-p) \cdot S(\lambda_2||\mu_2) \ .$$

2. *Let* $XY, X^1Y^1 \in \mathcal{X} \times \mathcal{Y}$. *Relative entropy satisfies the following chain rule,*

$$S(XY||X^1Y^1) = S(X||X^1) + \mathbb{E}_{x\leftarrow X} S(Y_x||Y^1_x) \ .$$

This in-particular implies, using joint convexity of relative entropy,

$$S(XY||X^1 \otimes Y^1) = S(X||X^1) + \mathbb{E}_{x\leftarrow X} S(Y_x||Y^1) \geq S(X||X^1) + S(Y||Y^1) \quad .$$

3. *For distributions* λ, μ : $||\lambda - \mu||_1 \leq \sqrt{S(\lambda||\mu)}$ *and* $S(\lambda||\mu) \geq 0$.

The relative min-entropy between λ and μ is defined as $S_\infty(\lambda||\mu) = \max_{x\in\mathcal{X}} \log \frac{\lambda(x)}{\mu(x)}$. It is easily seen that $S(\lambda||\mu) \leq S_\infty(\lambda||\mu)$. Let X, Y, Z be random variables. The mutual information between X and Y is defined as

$$I(X:Y) = S(X) + S(Y) - S(XY) = \mathbb{E}_{x\leftarrow X} S(Y_x||Y) = \mathbb{E}_{y\leftarrow Y} S(X_y||X).$$

The conditional mutual information is defined as $I(X:Y|\ Z) = \mathbb{E}_{z\leftarrow Z} I(X:Y|\ Z=z)$. Random variables XYZ form a Markov chain $Z \leftarrow X \leftarrow Y$ iff $I(Y:Z|\ X=x) = 0$ for each x in the support of X.

Two-way communication complexity

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation. We only consider complete relations, that is for all $(x,y) \in \mathcal{X} \times \mathcal{Y}$, there exists a $z \in \mathcal{Z}$ such that $(x,y,z) \in f$. In the two-way model of communication, Alice with input $x \in \mathcal{X}$ and Bob with input $y \in \mathcal{Y}$, communicate at the end of which they are supposed to determine an answer z such that $(x,y,z) \in f$. Let $\varepsilon > 0$ and let $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution. We let $\mathsf{D}^{2,\mu}_\varepsilon(f)$ represent the two-way distributional communication complexity of f under μ with expected error ϵ, i.e., the communication of the best deterministic two-way protocol for f, with distributional error (average error over the inputs) at most ε under μ. Let $\mathsf{R}^{2,\mathsf{pub}}_\epsilon(f)$ represent the public-coin two-way communication complexity of f with worst case error ε, i.e., the communication of the best public-coin two-way protocol for f with error for each input (x,y) being at most ε. The following is a consequence of the min-max theorem in game theory [KN97, Theorem 3.20, page 36].

Lemma 2.2 (Yao principle) $\mathsf{R}^{2,\mathsf{pub}}_\epsilon(f) = \max_\mu \mathsf{D}^{2,\mu}_\epsilon(f)$.

3 A strong direct product theorem for two-way communication complexity

3.1 New bounds

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation, $\mu, \lambda \in \mathcal{X} \times \mathcal{Y}$ be distributions and $\varepsilon > 0$. Let $XY \sim \mu$ and $X_1Y_1 \sim \lambda$ be random variables. Let $S \subseteq \mathcal{Z}$.

Definition 3.1 (Error of a distribution) *Error of distribution μ with respect to f and answer in S, denoted $\mathsf{err}_{f,S}(\mu)$, is defined as*

$$\mathsf{err}_{f,S}(\mu) \stackrel{\mathrm{def}}{=} \min\{\Pr_{(x,y)\leftarrow\mu}[(x,y,z) \notin f] \mid z \in S\} \ .$$

Definition 3.2 (Essentialness of an answer subset) *Essentialness of answer in S for f with respect to distribution μ, denoted $\mathsf{ess}^\mu(f,S)$, is defined as*

$$\mathsf{ess}^\mu(f,S) \stackrel{\mathrm{def}}{=} 1 - \Pr_{(x,y)\leftarrow\mu}[\textit{there exists } z \notin S \textit{ such that } (x,y,z) \in f].$$

For example $\mathsf{ess}^\mu(f, \mathcal{Z}) = 1$.

Definition 3.3 (One-way distributions) *λ is called one-way for μ with respect to $\mathcal{X}$, if for all (x, y) in the support of λ we have $\mu(y|x) = \lambda(y|x)$. Similarly λ is called one-way for μ with respect to $\mathcal{Y}$, if for all (x, y) in the support of λ we have $\mu(x|y) = \lambda(x|y)$.*

Definition 3.4 (SM-like) *λ is called SM-like (simultaneous-message-like) for μ, if there is a distribution θ on $\mathcal{X} \times \mathcal{Y}$ such that θ is one-way for μ with respect to $\mathcal{X}$ and λ is one-way for θ with respect to $\mathcal{Y}$.*

Definition 3.5 (Conditional relative entropy) *The $\mathcal{Y}$-conditional relative entropy of λ with respect to μ, denoted $\mathsf{crent}^\mu_{\mathcal{Y}}(\lambda)$, is defined as*

$$\mathsf{crent}^\mu_{\mathcal{Y}}(\lambda) \stackrel{\mathrm{def}}{=} \mathbb{E}_{y \leftarrow Y_1} S((X_1)_y || X_y).$$

Similarly the $\mathcal{X}$-conditional relative entropy of λ with respect to μ, denoted $\mathsf{crent}^\mu_{\mathcal{X}}(\lambda)$, is defined as

$$\mathsf{crent}^\mu_{\mathcal{X}}(\lambda) \stackrel{\mathrm{def}}{=} \mathbb{E}_{x \leftarrow X_1} S((Y_1)_x || Y_x).$$

Definition 3.6 (Conditional relative entropy bound) *The two-way ε-error conditional relative entropy bound of f with answer in S with respect to distribution μ, denoted $\mathsf{crent}^{2,\mu}_\varepsilon(f, S)$, is defined as*

$$\mathsf{crent}^{2,\mu}_\varepsilon(f, S) \stackrel{\mathrm{def}}{=} \min\{\mathsf{crent}^\mu_{\mathcal{X}}(\lambda) + \mathsf{crent}^\mu_{\mathcal{Y}}(\lambda) \mid \lambda \textit{ is SM-like for } \mu \textit{ and } \mathsf{err}_{f,S}(\lambda) \leq \varepsilon\} \ .$$

The two-way ε-error conditional relative entropy bound of f, denoted $\mathsf{crent}^2(f)$, is defined as

$$\mathsf{crent}^2_\varepsilon(f) \stackrel{\mathrm{def}}{=} \max\{\mathsf{ess}^\mu(f, S) \cdot \mathsf{crent}^{2,\mu}_\varepsilon(f, S) \mid \mu \textit{ is a distribution over } \mathcal{X} \times \mathcal{Y} \textit{ and } S \subseteq \mathcal{Z}\} \ .$$

The following bound is analogous to a bound defined in [JKN08] where it was referred to as the two-way subdistribution bound. We call it differently here for consistency of nomenclature with the other bounds. [JKN08] typically considered the cases where $S = \mathcal{Z}$ or S is a singleton set.

Definition 3.7 (Relative min entropy bound) *The two-way ε-error relative min entropy bound of f with answer in S with respect to distribution μ, denoted $\mathsf{ment}^{2,\mu}_\varepsilon(f, S)$, is defined as*

$$\mathsf{ment}^{2,\mu}_\varepsilon(f, S) \stackrel{\mathrm{def}}{=} \min\{S_\infty(\lambda || \mu) | \ \lambda \textit{ is SM-like for } \mu \textit{ and } \mathsf{err}_{f,S}(\lambda) \leq \varepsilon\} \ .$$

The two-way ε-error relative min entropy bound of f, denoted $\mathsf{ment}^2_\varepsilon(f)$, is defined as

$$\mathsf{ment}^2_\varepsilon(f) \stackrel{\mathrm{def}}{=} \max\{\mathsf{ess}^\mu(f, S) \cdot \mathsf{ment}^{2,\mu}_\varepsilon(f, S) \mid \mu \textit{ is a distribution over } \mathcal{X} \times \mathcal{Y} \textit{ and } S \subseteq \mathcal{Z}\} \ .$$

The following is easily seen from definitions.

Lemma 3.1

$$\mathsf{crent}^{\mu}_{\mathcal{X}}(\lambda) + \mathsf{crent}^{\mu}_{\mathcal{X}}(\lambda) \leq 2 \cdot S_\infty(\lambda || \mu)$$

and hence

$$\mathsf{crent}^{2,\mu}_{\varepsilon}(f,S) \leq 2 \cdot \mathsf{ment}^{2,\mu}_{\varepsilon}(f,S) \quad \textit{and} \quad \mathsf{crent}^{2}_{\varepsilon}(f) \leq 2 \cdot \mathsf{ment}^{2}_{\varepsilon}(f).$$

It can be argued using the substate theorem [JRS02] (proof skipped) that when μ is a product distribution then $\mathsf{ment}^{2,\mu}_{\varepsilon}(f,S) = O(\mathsf{crent}^{2,\mu}_{\varepsilon/2}(f,S))$. Hence our bound $\mathsf{crent}^{2}_{\varepsilon}(f)$ is an upper bound on the product subdistribution bound of [JKN08] (which is obtained when in Definition 3.7 maximization is done only over product distributions μ).

3.2 Strong direct product

Notation: Let B be a set. For a random variable distributed in B^k, or a string in B^k, the portion corresponding to the ith coordinate is represented with subscript i. Also the portion except the ith coordinate is represented with subscript $-i$. Similarly portion corresponding to a subset $C \subseteq [k]$ is represented with subscript C. For joint random variables MN, we let M_n to represent $M|\ (N=n)$ and also $MN|\ (N=n)$ and is clear from the context.

We start with the following theorem which we prove later.

Theorem 3.2 (Direct product in terms of ment and crent) *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation, $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution and $S \subseteq \mathcal{Z}$. Let $0 < \varepsilon < 1/3$, $0 < 200\delta < 1$ and k be a natural number. Fix $z \in \mathcal{Z}^k$. Let the number of indices $i \in [k]$ with $z_i \in S$ be at least $\delta_1 k$. Then*

$$\mathsf{ment}^{2,\mu^k}_{1-(1-\varepsilon/2)^{\lfloor \delta\delta_1 k \rfloor}}(f^k, \{z\}) \geq \delta \cdot \delta_1 \cdot k \cdot \mathsf{crent}^{2,\mu}_{\varepsilon}(f,S) \ .$$

We now state and prove our main result.

Theorem 3.3 (Direct product for two-way communication complexity) *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation, $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution and $S \subseteq \mathcal{Z}$. Let $0 < \varepsilon < 1/3$ and k be a natural number. Let $\delta_2 = \mathsf{ess}^{\mu}(f,S)$. Let $0 < 200\delta < \delta_2$. Let $\delta' = 3(1-\varepsilon/2)^{\lfloor \delta\delta_2 k/2 \rfloor}$. Then,*

$$\mathsf{D}^{2,\mu^k}_{1-\delta'}(f^k) \geq \delta \cdot \delta_2 \cdot k \cdot \mathsf{crent}^{2,\mu}_{\varepsilon}(f,S) - k \ .$$

In other words, by maximizing over μ, S and using Lemma 2.2.

$$\mathsf{R}^{2,\mathsf{pub}}_{1-2^{-\Omega(k)}}(f^k) \geq \Omega(k \cdot \mathsf{crent}^{2}_{1/3}(f)) \ .$$

Proof: Let $\mathsf{crent}^{\mu}_{2,\varepsilon}(f,S) = c$. For input $(x,y) \in \mathcal{X}^k \times \mathcal{Y}^k$, let $b(x,y)$ be the number of indices i in $[k]$ for which there exists $z_i \notin S$ such that $(x_i, y_i, z_i) \in f$. Let

$$B = \{(x,y) \in \mathcal{X}^k \times \mathcal{Y}^k |\ b(x,y) \geq (1-\delta_2/2)k\}.$$

By Chernoff's inequality we get,

$$\Pr_{(x,y) \leftarrow \mu^k}[(x,y) \in B] \leq \exp(-\delta_2^2 k/2).$$

Let $\mathcal{P}$ be a protocol for f^k with inputs $XY \sim \mu^k$ with communication at most $d = (kc\delta\delta_2/2) - k$ bits. Let $M \in \mathcal{M}$ represent the message transcript of $\mathcal{P}$. Let

$$B_M = \{m \in \mathcal{M} | \ \Pr[(XY)_m \in B] \geq \exp(-\delta_2^2 k/4)\}.$$

Then $\Pr[M \in B_M] \leq \exp(-\delta_2^2 k/4)$. Let

$$B_M^1 = \{m \in \mathcal{M} | \ \Pr[M = m] \leq 2^{-d-k}\}.$$

Then $\Pr[M \in B_M^1] \leq 2^{-k}$. Fix $m \notin B_M \cup B_M^1$. Let z_m be the output of $\mathcal{P}$ when $M = m$. Let $b(z_m)$ be the number of indices i such that $z_{m,i} \notin S$. If $b(z_m) \geq 1 - \delta_2 k/2$ then success of $\mathcal{P}$ when $M = m$ is at most $\exp(-\delta_2^2 k/4) \leq (1-\varepsilon/2)^{\lfloor \delta\delta_2 k/2 \rfloor}$. If $b(z_m) < 1 - \delta_2 k/2$ then from Theorem 3.2 (by setting $z = z_m$ and $\delta_1 = \delta_2/2$), success of $\mathcal{P}$ when $M = m$ is at most $(1-\varepsilon/2)^{\lfloor \delta\delta_2 k/2 \rfloor}$. Therefore overall success of $\mathcal{P}$ is at most

$$\begin{aligned} \delta' &= 2^{-k} + \exp(-\delta_2^2 k/4) + (1 - 2^{-k} - \exp(-\delta_2^2 k/4)(1-\varepsilon/2)^{\lfloor \delta\delta_2 k/2 \rfloor} \\ &\leq 3(1-\varepsilon/2)^{\lfloor \delta\delta_2 k/2 \rfloor}. \end{aligned}$$

■

Proof of Theorem 3.2: Let $c = \mathsf{crent}_\varepsilon^{2,\mu}(f, S)$. Let $\lambda \in \mathcal{X}^k \times \mathcal{Y}^k$ be a distribution which is SM-like for μ^k and with $S_\infty(\lambda || \mu^k) < \delta\delta_1 ck$. We show that $\mathsf{err}_{f^k,\{z\}}(\lambda) \geq 1 - (1-\varepsilon/2)^{\lfloor \delta\delta_1 k \rfloor}$. This shows the desired.

Let $XY \sim \lambda$. For a coordinate i, let the binary random variable $T_i \in \{0,1\}$, correlated with XY, denote success in the ith coordinate. That is $T_i = 1$ iff $XY = (x,y)$ such that $(x_i, y_i, z_i) \in f$. We make the following claim which we prove later. Let $k' = \lfloor \delta\delta_1 k \rfloor$.

Claim 3.4 *There exists k' distinct coordinates $i_1, \ldots, i_{k'}$ such that* $\Pr[T_{i_1} = 1] \leq 1 - \varepsilon/2$ *and for each $r < k'$,*

1. *either* $\Pr[T_{i_1} \times T_{i_2} \times \cdots \times T_{i_r} = 1] \leq (1-\varepsilon/2)^{k'}$,
2. *or* $\Pr[T_{i_{r+1}} = 1 | \ (T_{i_1} \times T_{i_2} \times \cdots \times T_{i_r} = 1)] \leq 1 - \varepsilon/2$.

This shows that the overall success is

$$\Pr[T_1 \times T_2 \times \cdots \times T_k = 1] \leq \Pr[T_{i_1} \times T_{i_2} \times \cdots \times T_{i_{k'}} = 1] \leq (1-\varepsilon/2)^{k'} \ .$$

■

Proof of Claim 3.4: Let us say we have identified $r < k'$ coordinates $i_1, \ldots i_r$. Let $C = \{i_1, i_2, \ldots, i_r\}$. Let $T = T_1 \times T_2 \times \cdots \times T_r$. If $\Pr[T = 1] \leq (1-\varepsilon/2)^{k'}$ then we will be done. So assume that $\Pr[T = 1] > (1-\varepsilon/2)^{k'} \geq 2^{-\delta\delta_1 k}$. Let $X'Y' \sim \mu$. Let $X^1Y^1 = (XY | \ T = 1)$. Let D be uniformly distributed in $\{0,1\}^k$ and independent of X^1Y^1. Let $U_i = X_i^1$ if $D_i = 0$ and $U_i = Y_i^1$ if $D_i = 1$. Let $U = U_1 \ldots U_k$. Below for any random variable $\tilde{X}\tilde{Y}$, we let $\tilde{X}\tilde{Y}_{d,u}$, represent the random variable obtained by appropriate conditioning on $\tilde{X}\tilde{Y}$: for all i, $\tilde{X}_i = u_i$ if $d_i = 0$ otherwise $\tilde{Y}_i = u_i$ if $d = 1$. Let I be the set of indices i such that $z_i \in S$. Consider,

$$\begin{aligned}
\delta\delta_1 k + \delta\delta_1 ck &> S_\infty(X^1Y^1||XY) + S_\infty(XY||(X'Y')^{\otimes k}) \\
&\geq S_\infty(X^1Y^1||(X'Y')^{\otimes k}) \geq S(X^1Y^1||(X'Y')^{\otimes k}) = \mathbb{E}_{d\leftarrow D} S(X^1Y^1||(X'Y')^{\otimes k}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((X^1Y^1)_{d,u,x_C,y_C}||((X'Y')^{\otimes k})_{d,u,x_C,y_C}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S(X^1_{d,u,x_C,y_C}||X'_{d_1,u_1,x_C,y_C} \otimes \ldots \otimes X'_{d_k,u_k,x_C,y_C}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} \sum_{i\notin C, i\in I} S((X^1_{d,u,x_C,y_C})_i||X'_{d_i,u_i}) \\
&= \sum_{i\notin C, i\in I} \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((X^1_{d,u,x_C,y_C})_i||X'_{d_i,u_i}) \ . \qquad (3.1)
\end{aligned}$$

Similarly,

$$\delta\delta_1 k + \delta\delta_1 ck > \sum_{i\notin C, i\in I} \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((Y^1_{d,u,x_C,y_C})_i||Y'_{d_i,u_i}) \ . \qquad (3.2)$$

From Eq. 3.1 and Eq. 3.2 and using Markov's inequality we get a coordinate j outside of C but in I such that

1. $\mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}) \leq \frac{2\delta(c+1)}{(1-\delta)} \leq 4\delta c$, and
2. $\mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((Y^1_{d,u,x_C,y_C})_j||Y'_{d_j,u_j}) \leq \frac{2\delta(c+1)}{(1-\delta)} \leq 4\delta c$.

Therefore,

$$\begin{aligned}
4\delta c &\geq \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}) \\
&= \mathbb{E}_{(d_{-j},u_{-j},x_C,y_C)\leftarrow(D_{-j}U_{-j}X_C^1Y_C^1)} \mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}).
\end{aligned}$$

And,

$$\begin{aligned}
4\delta c &\geq \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((Y^1_{d,u,x_C,y_C})_j||Y'_{d_j,u_j}) \\
&= \mathbb{E}_{(d_{-j},u_{-j},x_C,y_C)\leftarrow(D_{-j}U_{-j}X_C^1Y_C^1)} \mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((Y^1_{d,u,x_C,y_C})_j||Y'_{d_j,u_j}).
\end{aligned}$$

Now using Markov's inequality, there exists set G_1 with $\Pr[Y^1_{-j} \in G_1] \geq 1 - 0.2$, such that for all $(d_{-j}, u_{-j}, x_C, y_C) \in G_1$,

1. $\mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}) \leq 40\delta c$, and
2. $\mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((Y^1_{d,u,x_C,y_C})_j||Y'_{d_j,u_j}) \leq 40\delta c$.

Fix $(d_{-j}, u_{-j}, x_C, y_C) \in G_1$. Conditioning on $D_j = 1$ (which happens with probability 1/2) in inequality 1. above we get,

$$\mathbb{E}_{y_j\leftarrow Y_j^1|(D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((X^1_{d_{-j},u_{-j},y_j,x_C,y_C})_j||X'_{y_j}) \leq 80\delta c. \qquad (3.3)$$

Conditioning on $D_j = 0$ (which happens with probability 1/2) in inequality 2. above we get,

$$\mathbb{E}_{x_j\leftarrow X_j^1|(D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((Y^1_{d_{-j},u_{-j},x_j,x_C,y_C})_j||Y'_{x_j}) \leq 80\delta c. \qquad (3.4)$$

Let $X^2Y^2 = ((X^1Y^1)_{d_{-j},u_{-j},x_C,y_C})_j$. Note that X^2Y^2 is SM-like for μ. From Eq. 3.3 and Eq. 3.4 we get that

$$\mathsf{crent}^{\mu}_{\mathcal{X}}(X^2Y^2) + \mathsf{crent}^{\mu}_{\mathcal{Y}}(X^2Y^2) \leq c.$$

Hence,

$$\mathsf{err}_f(((X^1Y^1)_{d_{-j},u_{-j},x_C,y_C})_j) \geq \varepsilon.$$

This implies,

$$\Pr[T_j = 1 |\ (1, d_{-j}, u_{-j}, x_C, y_C) = (TD_{-j}U_{-j}X_CY_C)] \leq 1 - \varepsilon.$$

Therefore overall

$$\Pr[T_j = 1 |\ (T = 1)] \leq 0.8(1 - \varepsilon) + 0.2 \leq 1 - \varepsilon/2.$$

■

References

[BBR10] X. Chen B. Barak, M. Braverman and A. Rao. How to compress interactive communication. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, 2010.

[BPSW07] Paul Beame, Toniann Pitassi, Nathan Segerlind, and Avi Wigderson. A direct sum theorem for corruption and a lower bound for the multiparty communication complexity of Set Disjointness. *Computational Complexity*, 2007.

[BR10] M. Braverman and A. Rao. Efficient communication using partial information. Technical report, Electronic Colloquium on Computational Complexity, `http://www.eccc.uni-trier.de/report/2010/083/`, 2010.

[CSWY01] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew C.-C. Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 270–278, 2001.

[CT91] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley Series in Telecommunications. John Wiley & Sons, New York, NY, USA, 1991.

[Gav08] Dmitry Gavinsky. On the role of shared entanglement. *Quantum Information and Computation*, 8, 2008.

[HJMR09] Prahladh Harsha, Rahul Jain, David McAllester, and Jaikumar Radhakrishnan. The communication complexity of correlation. *IEEE Transactions on Information Theory*, 56(1):438 – 449, 2009.

[IRW94] Russell Impagliazzo, Ran Raz, and Avi Wigderson. A direct product theorem. In *Proceedings of the Ninth Annual IEEE Structure in Complexity Theory Conference*, pages 88–96, 1994.

[JK09] Rahul Jain and Hartmut Klauck. New results in the simultaneous message passing model via information theoretic techniques. In *Proceeding of the 24th IEEE Conference on Computational Complexity*, pages 369–378, 2009.

[JKN08] Rahul Jain, Hartmut Klauck, and Ashwin Nayak. Direct product theorems for classical communication complexity via subdistribution bounds. In *Proceedings of the 40th ACM Symposium on Theory of Computing*, pages 599–608, 2008.

[JRS02] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 429–438, 2002.

[JRS03] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A direct sum theorem in communication complexity via message compression. In *Proceedings of the Thirtieth International Colloquium on Automata Languages and Programming*, volume 2719 of *Lecture notes in Computer Science*, pages 300–315. Springer, Berlin/Heidelberg, 2003.

[JRS05] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Prior entanglement, message compression and privacy in quantum communication. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 285–296, 2005.

[Kla04] Hartmut Klauck. Quantum and classical communication-space tradeoffs from rectangle bounds. In *Proceedings of the 24th Annual IARCS International Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 3328 of *Lecture notes in Computer Science*, pages 384–395. Springer, Berlin/Heidelberg, 2004.

[Kla10] Hartmut Klauck. A strong direct product theorem for disjointness. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, pages 77–86, 2010.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, UK, 1997.

[KŠdW04] Hartmut Klauck, Robert Špalek, and Ronald de Wolf. Quantum and classical strong direct product theorems and optimal time-space tradeoffs. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 12–21, 2004.

[PRW97] Itzhak Parnafes, Ran Raz, and Avi Wigderson. Direct product results and the GCD problem, in old and new communication models. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 363–372, 1997.

[Sha03] Ronen Shaltiel. Towards proving strong direct product theorems. *Computational Complexity*, 12(1–2):1–22, 2003.