Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 143 (2012)

Direct Products in Communication Complexity

Mark Braverman[*] Anup Rao[†] Omri Weinstein[‡] Amir Yehudayoff[§]

November 22, 2012

Abstract

We give exponentially small upper bounds on the success probability for computing the direct product of any function over any distribution using a communication protocol. Let $\mathsf{suc}(\mu, f, C)$ denote the maximum success probability of a 2-party communication protocol for computing $f(x, y)$ with C bits of communication, when the inputs (x, y) are drawn from the distribution μ. Let μ^n be the product distribution on n inputs and f^n denote the function that computes n copies of f on these inputs.

We prove that if $T \log^{3/2} T \ll C\sqrt{n}$ and $\mathsf{suc}(\mu, f, C) < \frac{2}{3}$, then $\mathsf{suc}(\mu^n, f^n, T) \leq \exp(-\Omega(n))$. When μ is a product distribution, we prove a nearly optimal result: as long as $T \log^2 T \ll Cn$, we must have $\mathsf{suc}(\mu^n, f^n, T) \leq \exp(-\Omega(n))$.

1 Introduction

The *direct sum* question is about quantifying the resources needed to compute n independent copies of a function in terms of the resources needed to compute one copy of it. If one copy can be computed with C resources, then n copies can be computed using nC resources, but is this optimal?

When the inputs are drawn from a distribution (or the computational model is randomized), one can also measure the probability of success of computing the function. The *direct product* question is about understanding what the maximum probability of success of computing n copies of the function is. If there is a way to compute one copy with C resources and success probability ρ, then n copies can be computed using nC resources with success probability ρ^n, but is this optimal?

In this work, we study the direct product question in the model of distributional communication complexity [Yao79]. Direct sum theorems for this model were proved in [BBCR10], and we strengthen their results to give direct product theorems. For a longer introduction to direct sums and direct products in communication complexity and their significance, we refer the reader to the introductions of [BBCR10, JPY12].

[*] Department of Computer Science, Princeton University, mbraverm@cs.princeton.edu, Research supported in part by an Alfred P. Sloan Fellowship, an NSF CAREER award, and a Turing Centenary Fellowship.

[†] Computer Science and Engineering, University of Washington, anuprao@cs.washington.edu. Supported by an Alfred P. Sloan Fellowship, the National Science Foundation under agreement CCF-1016565, an NSF Career award, and by the Binational Science Foundation under agreement 2010089.

[‡] Department of Computer Science, Princeton University, oweinste@cs.princeton.edu.

[§] Department of Mathematics, Technion-IIT, Haifa, Israel, amir.yehudayoff@gmail.com. Horev Fellow – supported by the Taub Foundation. Supported by the Israel Science Foundation and by the Binational Science Foundation under agreement 2010089.

ISSN 1433-8092

Let $\mathsf{suc}(\mu, f, C)$ denote the maximum success probability of a 2-party communication protocol of communication complexity C for computing a function $f(x, y)$ when the inputs are drawn from the distribution μ. Let $f^n(x_1, \ldots, x_n, y_1, \ldots, y_n)$ denote the function that maps its inputs to the tuple $(f(x_1, y_1), f(x_2, y_2), \ldots, f(x_n, y_n))$ and μ^n denote the product distribution on n pairs of inputs, where each pair is sampled independently according to μ. Our goal in this work is to prove new upper bounds on $\mathsf{suc}(\mu^n, f^n, T)$ for $T \gg C$. It is easy to prove that $\mathsf{suc}(\mu^n, f^n, nC) \geq \mathsf{suc}(\mu^n, f^n, C)^n$, and $\mathsf{suc}(\mu^n, f^n, C) \leq \mathsf{suc}(\mu, f, C)$. Shaltiel [Sha03] showed that there exist μ, f, C such that $\mathsf{suc}(\mu^n, f^n, \frac{3}{4}nC) \geq \frac{3}{4}$, even though $\mathsf{suc}(\mu, f, C) \leq \frac{2}{3}$. Roughly, his ideas show that if $T \geq 2(1 - \mathsf{suc}(\mu, f, C))Cn$, there are examples where $\mathsf{suc}(\mu^n, f^n, T) > \mathsf{suc}(\mu, f, C)$.

Much past work has found success in proving upper bounds on $\mathsf{suc}(\mu^n, f^n, T)$ in special cases: for example, when f is the disjointness function [Kla10], or f is known to have small discrepancy [Sha03, LSS08, She11], or have a smooth rectangle bound [JY12], or the protocols computing f^n and f are restricted to using a bounded number of rounds of interaction [JPY12, MWY13], or restricted to behaving somewhat independently on each coordinate of the input [PRW97]. We refer the reader to [BBCR10, JPY12] for more references.

Prior to our work, the only known general upper bounds on $\mathsf{suc}(\mu^n, f^n, T)$, for $T > C$, are a consequence of the direct sum theorem proved in [BBCR10]: If $\mathsf{suc}(\mu, f, C) \leq \frac{2}{3}$, then $\mathsf{suc}(\mu^n, f^n, T) \leq \frac{2}{3}$, as long as $T \log T \ll C\sqrt{n}$. They also proved the same upper bound when $T\mathsf{polylog}(T) \ll Cn$ and μ is a product distribution.

In this work, we give new upper bounds that are exponentially small in n. When $\mathsf{suc}(\mu, f, C) \leq \frac{2}{3}$, we prove that $\mathsf{suc}(\mu^n, f^n, T) \leq \exp(-\Omega(n))$, as long as $T \log^{3/2} T \ll C\sqrt{n}$. By Yao's minimax principle [Yao79], we get an analogous statement for randomized worst case computation. If $\mathsf{suc}(f, C)$ denotes the maximum success probability for the best C-bit public coin randomized protocol computing f in the worst case, and if $\mathsf{suc}(f, C) \leq \frac{2}{3}$, then $\mathsf{suc}(f^n, T) \leq \exp(-\Omega(n))$ as long as $T \log^{3/2} T \ll C\sqrt{n}$. Formally, we prove:

Theorem 1 (Main Theorem)**.** *There is a universal constant $\alpha > 0$ such that if $\gamma = 1 - \mathsf{suc}(\mu, f, C)$, $T \geq 2$, and $T \log^{3/2} T < \alpha\gamma^{5/2}C\sqrt{n}$, then $\mathsf{suc}(\mu^n, f^n, T) \leq \exp\left(-\alpha\gamma^2 n\right)$.*

When μ is a product distribution, we prove an almost optimal result. We show that if $\mathsf{suc}(\mu, f, C) \leq \frac{2}{3}$ and $T \log^2 T \ll Cn$, then $\mathsf{suc}(\mu^n, f^n, T) \leq \exp(-\Omega(n))$.

Theorem 2 (Main Theorem for Product Distributions)**.** *There is a universal constant $\alpha > 0$ such that for every product distribution μ, if $\gamma = 1 - \mathsf{suc}(\mu, f, C)$, $T \geq 2$, and $T \log^2 T \leq \alpha\gamma^6 Cn$, then $\mathsf{suc}(\mu^n, f^n, T) \leq \exp\left(-\alpha\gamma^2 n\right)$.*

Our proofs heavily rely on methods from information theory [Sha48] which have been applied to a variety of problems in communication complexity [Raz92, NW93, Abl96, CSWY01, BYJKS04, BBCR10], and ideas developed to prove the parallel repetition theorem [Raz98, Hol07]. We give an overview of our proofs next.

1.1 Overview of the Proofs

The notation used below is formally defined in Section 2. Before we describe our proof in detail, we give a high level overview of the proof of the direct sum theorem proved in [BBCR10]. The theorem is proved by reduction. For T, C roughly as in the theorems above, they show that any protocol π for computing n copies of f with communication complexity $\|\pi\| = T$ can be used to obtain a protocol for computing one copy, with communication complexity less than C. This proves that computing n copies requires communication complexity more than T. The reduction itself has two steps. In the first step, they show that π can be used to obtain a protocol for computing f with small *information cost* (which we discuss below). In the second step, they show that any protocol with small information cost can be compressed to obtain a protocol that actually has small communication.

[CSWY01] were the first to define the (external) information cost of protocols. Let the inputs to a protocol be X, Y, the messages be M and the public randomness be R. The *external information cost* [CSWY01] of the protocol is the mutual information between the inputs and the messages, conditioned on the public randomness: $I(XY; M|R)$. It is the information that an observer learns about the inputs by watching the execution of the protocol. The *internal information cost* [BYJKS04, BBCR10] of the protocol is defined to be $I(X; M|YR) + I(Y; M|XR)$. It is the information learnt by the parties about each others inputs during the execution of the protocol. The external information is always at least as large as the internal information.

The first step of the reduction in [BBCR10] gives a protocol with internal information cost bounded by $\sim T/n$ and communication bounded by T. In the second step, they show that any protocol with internal information I and communication N can be compressed to get a protocol with communication $\sim \sqrt{I \cdot N}$. Thus one obtains a protocol with communication $\sim T/\sqrt{n}$ for computing f. When μ is a product distribution, the first step of the reduction gives a protocol with external information cost bounded by $\sim T/n$. They show how to compress any protocol with small external information almost optimally, and so obtain a protocol with communication $\sim T/n$ for computing f. In both cases, the intuition for the first step of the reduction is that the T bits of the messages can reveal at most $\sim T/n$ bits of information about an average input coordinate.

To prove our direct product theorems, we modify the approach above using ideas inspired by the proof of the parallel repetition theorem [Raz98]. Let E be the event that π correctly computes f^n. For $i \in [n]$, let W_i denote the event that the protocol π correctly computes $f(x_i, y_i)$. Let $\pi(E)$ denote the probability of E, and let $\pi(W_i|E)$ denote the conditional probability of the event W_i given E. We shall prove that if $\pi(E)$ is not very small, then $(1/n)\sum_i \pi(W_i|E) < 1$, which is a contradiction. In fact, we shall prove that this holds for an arbitrary event W, not just E.

Lemma 3 (Main Lemma)**.** *There is a universal constant $\alpha > 0$ so that the following holds. For every $\gamma > 0$, and event W such that $\pi(W) \geq 2^{-\gamma^2 n}$, if $\|\pi\| \geq 2$, and $\|\pi\| \log^{3/2} \|\pi\| < \alpha\gamma^{5/2} C\sqrt{n}$, then $(1/n)\sum_{i\in[n]} \pi(W_i|W) \leq \mathsf{suc}(\mu, f, C) + \gamma/\alpha$.*

Lemma 4 (Main Lemma for Product Distributions)**.** *There is a universal constant $\alpha > 0$ such that if μ is a product distribution, the following holds. For every $\gamma > 0$, and event W such that $\pi(W) \geq 2^{-\gamma^2 n}$, if $\|\pi\| \geq 2$, and $\|\pi\| \log^2 \|\pi\| \leq \alpha\gamma^6 Cn$, then $(1/n)\sum_{i\in[n]} \pi(W_i|W) \leq \mathsf{suc}(\mu, f, C) + \gamma/\alpha$.*

The proofs of the lemmas proceed by reduction, and can be broken up into two steps as in [BBCR10]. However there are substantial differences in our proof, which are discussed in detail below. First let us see how Lemma 3 implies Theorem 1. Theorem 2 follows from Lemma 4 in the same way.

Proof of Theorem 1. Let E denote the event that π computes f correctly in all n coordinates. So, $(1/n)\sum_{i\in[n]} \pi(W_i|E) = 1$. Set $\gamma = \alpha(1 - \mathsf{suc}(\mu, f, C))/2$ so that $\mathsf{suc}(\mu, f, C) + \gamma/\alpha < 1$. Then by Lemma 3, either $\|\pi\| < 2$, $\|\pi\| \log^{3/2} \|\pi\| \geq \alpha^{7/2} 2^{-5/2} (1-\mathsf{suc}(\mu, f, C))^{5/2} C\sqrt{n}$, or $\pi(E) < 2^{-\gamma^2 n}$. □

We give the formal proofs of the main lemmas in Section 3. At a high level, the proofs of the lemmas are quite similar to each other, though there are some technical differences. We discuss Lemma 4 first, which avoids some complications that come from the fact that the inputs are correlated under μ. We give a protocol with communication complexity C that computes f correctly with probability at least $(1/n)\sum_i \pi(W_i|W) - O(\gamma)$. Let m denote the messages of π, and $\pi(x_iy_im)$ denote the joint distribution of x_i, y_i, m. For fixed x_i, y_i, let $\pi(m|x_iy_iW)$ denote the conditional distribution of m.

Using standard subadditivity based arguments, one can show that for average i, $\pi(x_iy_i|W) \overset{\gamma}{\approx} \pi(x_iy_i) = \mu(x_iy_i)$, where here the approximation is in terms of the ℓ_1 distance of the distributions. Intuitively, since W has probability $2^{-\gamma^2 n}$, it cannot significantly alter all n of the inputs. We can hope to obtain a protocol that computes $f(x,y)$ by picking a random i, setting $x_i = x, y_i = y$ and simulating the execution of π conditioned on the event W. There are two challenges that need to be overcome:

The protocol must simulate $\pi(m|x_iy_iW)$ In the probability space of π conditioned on W, the messages sent by the first party can become correlated with the input of the second party, even though they were initially independent. Thus (unlike in [BBCR10]), $\pi(m|x_iy_iW)$ is no longer distributed like the messages of a communication protocol, and it is non-trivial for the parties to sample a message from this distribution.

The protocol must communicate at most $C \ll |m|$ **bits** To prove the lemma, the parties need to sample m using communication that is much smaller than the length of m.

To solve the first challenge, we use a protocol θ. The parties publicly sample a uniformly random coordinate i in $[n]$ and set $x_i = x, y_i = y$. The also publicly sample a variable r_i that contains a subset of the variables $x_1, \ldots, x_n, y_1, \ldots, y_n$. Each message m_j sent by the first party in π is sampled according to the distribution $\pi(m_j|m_{<j}x_ir_iW)$, and each message sent by the second party is sampled according to the distribution $\pi(m_j|m_{<j}y_ir_iW)$. We prove that for average i, $\theta(x_iy_ir_im) \overset{\gamma}{\approx} \pi(x_iy_ir_im|W)$. [JPY12] analyzed a different protocol θ, which used a different definition of r_i, and showed that for average i, $\theta(x_iy_ir_im) \overset{\gamma t}{\approx} \pi(x_iy_ir_im|W)$, where here t is the number of rounds of communication in π. Our bound is independent of t, a feature that is essential to our results. A crucial technical feature of our protocol is the definition of r_i, which allows us to split the dependencies between inputs to π in a new way. This allows us to control the effect of the dependencies introduced by W using a bound that is independent of the number of rounds in π.

To solve the second challenge, we need to come up with a way to *compress* the protocol θ. To use the compression methods of [BBCR10], we need to bound the *external information cost* of θ. We did not succeed in bounding this quantity, and so cannot apply the compression methods of [BBCR10] directly. Instead, we are able to bound $I_\pi(X_iY_i; M|W)$ for average i, the corresponding quantity for the variables in the probability space of π.

This does not show that the information cost of θ is small, even though the distribution of the variables in θ is close in ℓ_1 distance to the distribution of the corresponding variables of π conditioned on W. For example, suppose θ is such that with small probability the first party sends her own input, and otherwise she sends a random string. Then θ is close to a protocol that reveals 0 information, but its information cost may be arbitrarily large.

Nevertheless, we show that any protocol that is close to having small external information cost can be simulated by a protocol that actually has small external information cost. In our example from above, the first party can simulate the protocol θ bit by bit and decide to abort it if she sees that her transmissions are significantly correlated with her input. This does not change the protocol most of the time, but does significantly reduce the amount of information that is revealed. Our general solution is very similar to this. The parties simulate θ and abort the simulation if they find that they are revealing too much information. We prove that any protocol that is close to having low information can be simulated with small communication (the term "δ-simulates" in the theorem statement is formally defined in Subsection 2.2):

Theorem 5 (Simulation for External Information)**.** *Suppose θ is a protocol with inputs x, y, public randomness r, and messages m, and q is another distribution on these variables such that $\theta(xyrm) \overset{\epsilon}{\approx} q(xyrm)$. Then, there exists a protocol τ that $O(\epsilon)$-simulates θ with $\|\tau\| \leq 2\|\theta\|$ and*

$$I_\tau(XY; M|R) \leq 2\left(\frac{I_q(XY; M|R) + 1/(e\ln 2) + 2\log(\|\theta\| + 1)}{\epsilon}\right) + \log(\|\theta\| + 1) + 2\log(1/\epsilon) + 4.$$

We give the formal proof of Theorem 5 in Section 4.2. The final protocol computing f is obtained by compressing τ using the methods of [BBCR10].

The high level outline of the proof of Lemma 3 is similar to the proof of Lemma 4. When μ is not a product distribution, we obtain a bound on the internal information cost associated with π conditioned on W, namely we bound $I_\pi(X_i; M|Y_iR_iW) + I_\pi(Y_i; M|X_iR_iW)$. We are unable to prove an analogue of Theorem 5 for the internal information cost (and it remains an interesting open question whether such a theorem is true or not). Instead, to prove Lemma 3, we reanalyze the compression method of [BBCR10] for internal information cost, and show that it can be used here. We prove:

Theorem 6 (Compression for Internal Information)**.** *Suppose θ is a protocol so that $\|\theta\| \geq 2$ with inputs x, y and messages m, and q is another distribution on these variables such that $\theta(xym) \overset{\epsilon}{\approx} q(xym)$. Then, there exists a protocol τ that $O(\epsilon)$-simulates θ such that*

$$\|\tau\| \leq \frac{\log\|\theta\|\sqrt{(I_q(X; M|Y) + I_q(Y; M|X) + 1 + \log\|\theta\|) \cdot \|\theta\|}}{\epsilon^{3/2}}.$$

Remark 7. *Theorem 6 can also be used to compress protocols θ that have public randomness. Indeed if the inputs are x', y', the public randomness is r and the messages are m, one can set $x = x'r, y = y'r$. Then $I_q(X; M|Y) + I_q(Y; M|X) = I_q(X'; M|Y'R) + I_q(Y'; M|X'R)$, so one can apply the theorem.*

The intuition for the proof is quite similar to the intuition for the proof of Theorem 5. We show that the compression goes well most of the time, and there is a small probability that the messages of the protocol will lead to a failure in the simulation, but this does not affect the outcome of the simulation by much. We formally prove Theorem 6 in Section 4.1.

2 Preliminaries

2.1 Notation

Unless otherwise stated, logarithms in this text are computed base two. Random variables are denoted by capital letters and values they attain are denoted by lower-case letters. For example,

A may be a random variable and then a denotes a value A may attain and we may consider the event $A = a$. Given $a = a_1, a_2, \ldots, a_n$, we write $a_{\leq i}$ to denote $a_1, \ldots, a_i$. We define $a_{>i}$ and $a_{\leq i}$ similarly.

We use the notation $p(a)$ to denote both the distribution on the variable a, and the number $\Pr_p[A = a]$. The meaning will usually be clear from context, but in cases where there may be confusion we shall be more explicit about which meaning is being used. We write $p(a|b)$ to denote either the distribution of A conditioned on the event $B = b$, or the number $\Pr[A = a|B = b]$. Again, the meaning will usually be clear from context. Given a distribution $p(a, b, c, d)$, we write $p(a, b, c)$ to denote the marginal distribution on the variables a, b, c (or the corresponding probability). We often write $p(ab)$ instead of $p(a, b)$ for conciseness of notation. If W is an event, we write $p(W)$ to denote its probability according to p. We denote by $\mathbb{E}_{p(a)}\left[g(a)\right]$ the expected value of $g(a)$ with respect to a distributed according to p.

For two distributions p, q, we write $|p(a) - q(a)|$ to denote the ℓ_1 distance between the distributions p and q. We write $p \overset{\epsilon}{\approx} q$ if $|p - q| \leq \epsilon$. Given distributions $p_1, \ldots, p_n$ and $q_1, \ldots, q_n$, we sometimes say "in expectation over i sampled according to $\eta(i)$, $p_i \overset{\gamma}{\approx} q_i$" when we mean that $\mathbb{E}_{\eta(i)}\left[|p_i - q_i|\right] \leq \gamma$.

The *divergence* between p, q is defined to be

$$\mathsf{D}\left(\frac{p(a)}{q(a)}\right) = \sum_a p(a) \log \frac{p(a)}{q(a)}.$$

For three random variables A, B, C with underlying probability distribution $p(a, b, c)$, the *mutual information* between A, B conditioned on C is defined as

$$I_p(A; B|C) = \mathop{\mathbb{E}}_{p(cb)}\left[\mathsf{D}\left(\frac{p(a|bc)}{p(a|c)}\right)\right] = \mathop{\mathbb{E}}_{p(ca)}\left[\mathsf{D}\left(\frac{p(b|ac)}{p(b|c)}\right)\right] = \sum_{a,b,c} p(abc) \log \frac{p(a|bc)}{p(a|c)}.$$

We shall often work with multiple distributions over the same space. To avoid confusion, we shall always explicitly specify the distribution being used when computing the mutual information. We shall sometimes work with an event W. In this case, we denote $I_p(A; B|CW) = I_q(A; B|C)$ where $q(abc) = p(abc|W)$.

2.2 Communication Complexity

Given a protocol π that operates on inputs x, y drawn from a distribution μ using public randomness[1] r and messages m, we write $\pi(xymr)$ to denote the joint distribution of these variables. We write $\|\pi\|$ to denote the *communication complexity* of π, namely the maximum number of bits that may be exchanged by the protocol.

Our work relies heavily on ways to measure the information complexity of a protocol (see [BBCR10, Bra12] and references within for a more detailed overview). The *internal information cost* of π is defined to be $I_\pi(X; M|YR) + I_\pi(Y; M|XR)$. The *external information cost* is $I_\pi(XY; M|R)$.

[1] In our paper we define protocols where the public randomness is sampled from a continuous (i.e. non-discrete) set. Nevertheless, we often treat the randomness as if it were supported on a discrete set, for example by taking the sum over the set rather than the integral. This simplifies notation throughout our proofs, and does not affect correctness in any way, since all of our public randomness can be approximated to arbitrary accuracy by sufficiently dense finite sets..

The internal information cost is always at most the external information cost, and the two measures are equal when $\pi(xy) = \pi(x)\pi(y)$ is a product distribution. Both measures are at most the communication complexity of the protocol.

Let $q(x, y, a)$ be an arbitrary distribution. We say that π *δ-simulates* q, if there is a function g and a function h such that

$$\pi(x, y, g(x, r, m)) \overset{\delta}{\approx} q(x, y, a) \quad \text{and} \quad \pi(g(x, r, m) \neq h(y, r, m)) \leq \delta.$$

We say that π computes[2] f with success probability $1 - \delta$, if π δ-simulates $\pi(x, y, f(x, y))$. If λ is a protocol with inputs x, y, public randomness r' and messages m', we say that π δ-simulates λ if π δ-simulates $\lambda(x, y, (r', m'))$.

The following lemma will be useful in our simulation protocols. It shows that messages sent by each party remain independent of the other party's input even after some part of the input is fixed.

Lemma 8. *Let x, y be inputs to a protocol π with public randomness r and let r' be a variable such that $\pi(xy|rr') = \pi(x|rr')\pi(y|rr')$. Let $m_1, \ldots, m_j$ be messages in π such that m_j is transmitted by Alice. Then $\pi(m_j|m_{<j}rr') = \pi(m_j|m_{<j}rr'y)$.*

Proof sketch. Conditioned on rr', the variables x, y are independent. Since $m_{<j}$ defines a rectangle over x, y, even conditioned on $m_{<j}rr'$, the variables x, y are independent. Since Alice sends the j'th message, $\pi(m_j|m_{<j}rr'xy) = \pi(m_j|m_{<j}rr'x)$. Thus:

$$\begin{aligned}\pi(m_j|m_{<j}rr') &= \sum_x \pi(x|m_{<j}rr') \cdot \pi(m_j|m_{<j}rr'x) \\ &= \sum_x \pi(x|m_{<j}rr'y) \cdot \pi(m_j|m_{<j}rr'xy) \\ &= \sum_x \pi(xm_j|m_{<j}rr'y) = \pi(m_j|m_{<j}rr'y).\end{aligned}$$

□

2.3 Useful Protocols

The following lemma was proved by Holenstein [Hol07].

Lemma 9 (Correlated Sampling)**.** *Suppose Alice is given a distribution p and Bob a distribution q over a common universe. Then there is a randomized sampling procedure that allows Alice and Bob to use shared randomness to jointly sample elements A, B such that A is distributed according to p, B is distributed according to q, and $\Pr[A \neq B] = |p - q|$.*

We use the following lemma of Feige et al. [FPRU94]:

Lemma 10 (Location of First Difference)**.** *There is a randomized public coin protocol with communication complexity $O(\log(k/\epsilon))$ such given two k-bit strings x, y as input, it outputs the first index $i \in [k]$ such that $x_i \neq y_i$ with probability at least $1 - \epsilon$, if such an i exists.*

[2] Our definition is different (weaker) than assuming that the messages m determine the value of f. We just assume that the parties eventually know f. Under our definition the communication complexity of a function can be significantly smaller if f maps to a large set. We believe that this definition is the right definition for what it means to compute a function.

The following compression theorem from [BBCR10] will be useful:

Theorem 11. *For every protocol π, and every $\epsilon > 0$, there exists a protocol λ that ϵ-simulates π with*

$$\|\lambda\| \leq O\left(\frac{I_\pi(XY;M|R) \cdot \log(\|\pi\|/\epsilon)}{\epsilon^2}\right) .$$

2.4 Basic Lemmas

The proofs of the following two lemmas can be found in [CT91]:

Lemma 12 (Divergence is Non-negative)**.** $\mathsf{D}\left(\frac{p(a)}{q(a)}\right) \geq 0.$

Lemma 13 (Chain Rule)**.** *If $a = a_1, \ldots, a_s$, then*

$$\mathsf{D}\left(\frac{p(a)}{q(a)}\right) = \sum_{i=1}^{s} \mathop{\mathbb{E}}_{p(a_{<i})}\left[\mathsf{D}\left(\frac{p(a_i|a_{<i})}{q(a_i|a_{<i})}\right)\right].$$

Pinsker's inequality bounds statistical distance in terms of the divergence:

Lemma 14 (Pinsker)**.** *If $p(b) = q(b)$, then $|p(a,b) - q(a,b)|^2 \leq \mathbb{E}_{p(b)}\left[\mathsf{D}\left(\frac{p(a|b)}{q(a|b)}\right)\right]$.*

Proof. By Pinsker's inequality [CT91] and concavity of square root,

$$|p - q| = \mathbb{E}_{p(b)}|p(a|b) - q(a|b)| \leq \mathbb{E}_{p(b)}\sqrt{D(p(a|b)||q(a|b)|)} \leq \sqrt{\mathbb{E}_{p(b)}D(p(a|b)||q(a|b)|)}.$$

□

The following lemma bounds the probability of getting a large term in the divergence:

Lemma 15 (Reverse Pinsker)**.** *Let $S = \left\{(a,b) : \log\frac{p(a|b)}{q(a|b)} > 1\right\}$. Then, $p(S) < 2|p(a,b) - q(a,b)|$.*

Proof. Let $\epsilon = |p(a,b) - q(a,b)| = 2\max\{p(S') - q(S') : S'\}$. Thus,

$$\begin{aligned}
p(S) &\leq \epsilon/2 + q(S) \\
&< \epsilon/2 + (1/2)\sum_{(a,b)\in S} q(b) \cdot p(a|b) \\
&\leq \epsilon/2 + p(S)/2 + (1/2)\sum_{(a,b)\in S} |q(b) - p(b)| \cdot p(a|b) \\
&\leq \epsilon/2 + p(S)/2 + (1/2)\sum_{b} |q(b) - p(b)| \\
&\leq \epsilon + p(S)/2.
\end{aligned}$$

□

The following bounds the contribution of the negative terms to the divergence:

Lemma 16. *Let* $S = \{a : p(a) < q(a)\}$. *Then,* $\sum_{a \in S} p(a) \log \frac{p(a)}{q(a)} \geq -1/(e \ln 2)$.

Proof.

$$\begin{aligned}
\sum_{a \in S} p(a) \log \frac{p(a)}{q(a)} &= -p(S) \sum_{a \in S} \frac{p(a)}{p(S)} \log \frac{q(a)}{p(a)} \\
&\geq -p(S) \log \left(\sum_{a \in S} \frac{p(a)}{p(S)} \frac{q(a)}{p(a)} \right) && \text{by concavity of log} \\
&\geq p(S) \log p(S).
\end{aligned}$$

The minimum value of the function $x \ln x$ is $-1/e$. □

2.5 Inequalities that Involve Conditioning

The following lemmas bound the change in divergence when extra conditioning is involved.

Lemma 17. *Let* W *be an event and* A, B, M *be random variables in the probability space* p. *Then,*

$$\mathop{\mathbb{E}}_{p(bm|W)} \left[\mathsf{D} \left(\frac{p(a|bmW)}{p(a|b)} \right) \right] \leq \log \frac{1}{p(W)} + I_p(A; M|BW).$$

Proof.

$$\begin{aligned}
\mathop{\mathbb{E}}_{p(bm|W)} \left[\mathsf{D} \left(\frac{p(a|bmW)}{p(a|b)} \right) \right] &= \sum_{a,b,m} p(abm|W) \log \frac{p(a|bmW)}{p(a|b)} \\
&= \sum_{a,b} p(ab|W) \log \frac{p(a|bW)}{p(a|b)} + \sum_{a,b,m} p(abm|W) \log \frac{p(a|bmW)}{p(a|bW)} \\
&= \sum_{a,b} p(ab|W) \log \frac{p(W|ab)}{p(W|b)} + I_p(A; M|BW).
\end{aligned}$$

The first term can be bounded by:

$$\begin{aligned}
\sum_{a,b} p(ab|W) \log \frac{p(W|ab)}{p(W|b)} &\leq \sum_{a,b} p(ab|W) \log \frac{1}{p(W|b)} \\
&= \sum_{b} p(b|W) \log \frac{1}{p(W|b)} \\
&\leq \log \sum_{b} \frac{p(b|W)}{p(W|b)} && \text{by concavity of log} \\
&= \log \sum_{b} \frac{p(b)}{p(W)} = \log \frac{1}{p(W)}.
\end{aligned}$$

□

Lemma 18 (Conditioning does not decrease divergence)**.**

$$\mathop{\mathbb{E}}_{p(b)}\left[\mathsf{D}\left(\frac{p(a|b)}{q(a)}\right)\right] \geq \mathsf{D}\left(\frac{p(a)}{q(a)}\right).$$

Proof.

$$\begin{aligned}
\mathop{\mathbb{E}}_{p(b)}\left[\mathsf{D}\left(\frac{p(a|b)}{q(a)}\right)\right] &= \sum_b p(b) \sum_a p(a|b) \log \frac{p(a|b)}{q(a)} \\
&= -\sum_a p(a) \sum_b p(b|a) \log \frac{q(a)}{p(a|b)} \\
&\geq -\sum_a p(a) \log \left(\sum_b p(b|a) \frac{q(a)}{p(a|b)}\right) \qquad\qquad \text{by concavity of log} \\
&= -\sum_a p(a) \log \left(\sum_b \frac{p(b)q(a)}{p(a)}\right) \\
&= \mathsf{D}\left(\frac{p(a)}{q(a)}\right).
\end{aligned}$$

□

The following lemma gives a key estimate that is used crucially in our proof. It allows us to remove the effect of conditioning on an event W on the second argument of a divergence expression. The lemma states that, on average, $\mathsf{D}\left(\frac{p(a|brW}{p(a|rW)}\right)$ cannot be larger than $\mathsf{D}\left(\frac{p(a|brW)}{p(a|r)}\right)$. Intuitively this is true because in both cases the first distribution is conditioned on W, but in the second case the second distribution is not conditioned on W. The second part of the lemma shows that conditioning on an event W of probability 2^{-s} can create a mutual information of up to s between two formerly independent random variables.

Lemma 19. *Let W be an event and A, B, R be random variables. Then,*

$$I_p(A;B|RW) \leq \mathop{\mathbb{E}}_{p(br|W)}\left[\mathsf{D}\left(\frac{p(a|brW)}{p(a|r)}\right)\right].$$

If in addition $p(abr) = p(r)p(a|r)p(b|r)$, then

$$I_p(A;B|RW) \leq \mathop{\mathbb{E}}_{p(br|W)}\left[\mathsf{D}\left(\frac{p(a|brW)}{p(a|br)}\right)\right] \leq \log \frac{1}{p(W)}.$$

Proof.

$$\begin{aligned}
I_p(A;B|RW) &= \sum_{a,b,r} p(abr|W) \log \frac{p(a|brW)}{p(a|rW)} \\
&= \sum_{a,b,r} p(abr|W) \log \frac{p(a|brW)}{p(a|r)} + \sum_{a,r} p(ar|W) \log \frac{p(a|r)}{p(a|rW)}.
\end{aligned}$$

The second term is $-\mathbb{E}_{p(r|W)}\left[\mathsf{D}\left(\frac{p(a|rW)}{p(a|r)}\right)\right] \leq 0$. This proves the first part.

To prove the second part, observe that $p(a|r) = p(a|br)$. Lemma 17 (with M being the empty variable) implies that

$$\mathop{\mathbb{E}}_{p(br|W)}\left[\mathsf{D}\left(\frac{p(a|brW)}{p(a|br)}\right)\right] \leq \log\frac{1}{p(W)}.$$

□

2.6 Variable Truncation

We shall need to analyze protocols that are statistically close to having low information. The following lemmas show that if a variable A is statistically close to having low information, then some prefix $A_{\leq K}$ of A usually has low information. By truncating the variable to $A_{\leq K}$, we obtain a new variable that is statistically close to the old one, yet has low information.

Lemma 20. *Let $p(a,b,c) \overset{\epsilon}{\approx} q(a,b,c)$. Then, $q\left(\log\frac{q(a|bc)}{q(a|c)} > \beta - 2\right) > p\left(\log\frac{p(a|bc)}{p(a|c)} > \beta\right) - 9\epsilon/2$, for every real β.*

Proof.

$$\log\frac{q(a|bc)}{q(a|c)} = \log\frac{p(a|bc)}{p(a|c)} - \log\frac{p(a|bc)}{q(a|bc)} - \log\frac{q(a|c)}{p(a|c)}.$$

By Lemma 15, $p(\log\frac{p(a|bc)}{q(a|bc)} > 1) < 2\epsilon$, and $q(\log\frac{q(a|c)}{p(a|c)} > 1) < 2\epsilon$. Thus,

$$\begin{aligned}
&q\left(\log\frac{q(a|bc)}{q(a|c)} > \beta - 2\right)\\
&\geq q\left(\log\frac{p(a|bc)}{p(a|c)} > \beta \text{ and } \log\frac{p(a|bc)}{q(a|bc)} \leq 1\right) - q\left(\log\frac{q(a|c)}{p(a|c)} > 1\right)\\
&> p\left(\log\frac{p(a|bc)}{p(a|c)} > \beta \text{ and } \log\frac{p(a|bc)}{q(a|bc)} \leq 1\right) - 5\epsilon/2 && \text{using } q \overset{\epsilon}{\approx} p\\
&\geq p\left(\log\frac{p(a|bc)}{p(a|c)} > \beta\right) - 9\epsilon/2.
\end{aligned}$$

□

Lemma 21 (Truncation Lemma)**.** *Let $p(a,b,c) \overset{\epsilon}{\approx} q(a,b,c)$ where $a = a_1, \ldots, a_s$. For every a, b, c, define k to be the minimum number j in $[s]$ such that*

$$\log\frac{p(a_{\leq j}|bc)}{p(a_{\leq j}|c)} > \beta.$$

If no such index exists, set $k = s+1$. Then,

$$p(k < s+1) < \frac{I_q(A;B|C) + \log(s+1) + 1/(e\ln 2)}{\beta - 2} + 9\epsilon/2.$$

Remark 22. *One can also prove that $I_p(A_{<K}, B|C) \leq \beta + \log(s+1)$, in Lemma 21. We do not need this conclusion, so we omit its proof.*

Proof of Lemma 21. Define

$$H = \begin{cases} K, A_{\leq K} & \text{if } K \leq s, \\ \perp & \text{else.} \end{cases}$$

Then

$$\begin{aligned} I_q(A;B|C) + \log(s+1) &\geq I_q(AK;B|C) \\ &\geq I_q(H;B|C) && \text{since } AK \text{ determines } H \\ &= \sum_{h,b,c} q(hbc) \log \frac{q(h|bc)}{q(h|c)}. && (1) \end{aligned}$$

By Lemma 16, we know that the negative terms contribute at least $-1/(e \ln 2)$ to (1). We shall lower bound the contribution of the positive terms using $p(k < s+1)$. By Lemma 20,

$$q\left(\log \frac{q(h|bc)}{q(h|c)} > \beta - 2\right) > p\left(\log \frac{p(h|bc)}{p(h|c)} > \beta\right) - 9\epsilon/2. \tag{2}$$

Observe that if $h = j, a_{\leq j}$ and $p(hbc) > 0$, then $p(K = j | A_{\leq j} = a_{\leq j}, bc) = 1$, and so:

$$\begin{aligned} \frac{p(h|bc)}{p(h|c)} &= \frac{p(A_{\leq j} = a_{\leq j}|bc)}{p(A_{\leq j} = a_{\leq j}|c)} \cdot \frac{p(K = j|A_{\leq j} = a_{\leq j}, bc)}{p(K = j|A_{\leq j} = a_{\leq j}, c)} \\ &= \frac{p(A_{\leq j} = a_{\leq j}|bc)}{p(A_{\leq j} = a_{\leq j}|c)} \cdot \frac{1}{p(K = j|A_{\leq j} = a_{\leq j}, c)} \\ &\geq \frac{p(A_{\leq j} = a_{\leq j}|bc)}{p(A_{\leq j} = a_{\leq j}|c)} > 2^{\beta}. \end{aligned}$$

So,

$$p\left(\log \frac{p(h|bc)}{p(h|c)} > \beta\right) \geq p(k < s+1). \tag{3}$$

The sentence after (1), and equations (2), (3) imply

$$\begin{aligned} & I_q(A;B|C) + \log(s+1) + 1/(e \ln 2) > (\beta - 2)(p(k < s+1) - 9\epsilon/2) \\ \Rightarrow\ & p(k < s+1) < \frac{I_q(A;B|C) + \log(s+1) + 1/(e \ln 2)}{\beta - 2} + 9\epsilon/2. \end{aligned}$$

□

3 Proofs of the Main Lemmas

In this section we prove Lemma 3 and Lemma 4. We write $M = M_1, M_2, \ldots, M_{2t}$ to denote the messages in π. Let $(X_1, Y_1), \ldots, (X_n, Y_n)$ be the inputs. We write $\overline{X} = X_1, \ldots, X_n$ and $\overline{Y} = Y_1, \ldots, Y_n$. Without loss of generality, we assume that n is even.

Consider the protocol η in Figure 1. We show that η computes f with good probability, although with a lot of communication. The protocol η has public randomness $i, \mathbf{g}, \mathbf{h}$ and runs protocol $\theta_{i,\mathbf{g},\mathbf{h}}$ given in Figure 2 as a subroutine with inputs $(x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}})$. Eventually, we shall argue that in expectation over $i, \mathbf{g}, \mathbf{h}$ sampled according to $\eta(i\mathbf{gh})$,

$$\eta\big((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}})\big) \overset{O(\gamma)}{\approx} \theta_{i,\mathbf{g},\mathbf{h}}((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}})),$$

and that, on average, $\theta_{i,\mathbf{g},\mathbf{h}}$ is statistically close to having small internal information, and statistically close to having small external information in the case that μ is product. We shall apply Theorem 6 to compress the communication to obtain our final protocol for computing f and so prove Lemma 3. We shall apply Theorem 5 and Theorem 11 to obtain the protocol that proves Lemma 4.

Our first goal is to show that W does not change the distribution in a typical coordinate.

Lemma 23. *In expectation over i sampled according to $\eta(i)$, $\pi(x_i y_i) \overset{\gamma}{\approx} \pi(x_i y_i | W)$.*

The proof of Lemma 23 is somewhat standard, so we defer it to Section 6. Next we eliminate a corner case:

Lemma 24. *If $\|\pi\| \leq \gamma^2 n$, then in expectation over i sampled according to $\eta(i)$, $\pi(m x_i y_i | W) \overset{\sqrt{2}\gamma}{\approx} \pi(m|W) \cdot \pi(x_i y_i)$.*

The proof of Lemma 24 is also a straightforward application of subadditivity, and we defer it to Section 6. Lemma 24 implies that if $\|\pi\| \leq \gamma^2 n$, then a protocol with 0 communication can approximate the messages of π conditioned on W. So

$$(1/n) \sum_{i=1}^{n} \pi(W_i|W) - \gamma/\sqrt{2} \leq \mathsf{suc}(\mu, f, 0) \leq \mathsf{suc}(\mu, f, C),$$

which completes the proof. The more interesting case is when $\|\pi\| \geq \gamma^2 n$, and so we assume that this holds in the rest of this section.

Given subsets $\mathbf{g}, \mathbf{h} \subset [n]$, let $\overline{X}_{\mathbf{h}}$ and $\overline{Y}_{\mathbf{g}}$ denote $\overline{X}$ and $\overline{Y}$ projected on to the relevant coordinates. Define

$$R_{i,\mathbf{g},\mathbf{h}} = \overline{X}_{\mathbf{h} \setminus \{i\}}, \overline{Y}_{\mathbf{g} \setminus \{i\}}.$$

The random variable $R_{i,\mathbf{g},\mathbf{h}}$ helps to break the dependencies between Alice and Bob.

It turns out that choosing the right distribution for $i, \mathbf{g}, \mathbf{h}$ in η is crucial to our proofs. We need the distribution to be symmetric in $\mathbf{g}, \mathbf{h}$. It is important that $\mathbf{g} \cup \mathbf{h} = [n]$ so that $x_i, y_i, r_{i,\mathbf{g},\mathbf{h}}$ split the dependences between $\overline{x}, \overline{y}$. In the analysis we shall repeatedly use the fact that for every fixing of $\mathbf{h}$, $\eta(i\mathbf{g}|\mathbf{h})$ has the property that i is distributed uniformly over a large set, and $i \in \mathbf{g} \cap \mathbf{h}$. This allows us to apply the chain rule. In Section 3.3, we provide some intuition for the choice of the variable $r_{i,\mathbf{g},\mathbf{h}}$.

Now we argue that $\eta(i\mathbf{gh})$ has the properties we need. Observe that we can sample $\eta(i\mathbf{gh})$ by the following different yet equivalent process. Let $\mathbf{h}$ be distributed as in η. For fixed $\mathbf{h}$, let $\kappa_{\mathbf{h}} : [n] \to [n]$ be a permutation sampled uniformly from the set of permutations that map $[|\mathbf{h}|]$ to $\mathbf{h}$. Let ℓ be a uniformly random element of $[n/2]$. Given $\mathbf{h}, \kappa_{\mathbf{h}}, \ell$, set $i = \kappa_h(\ell)$ and $\mathbf{g} = \kappa_{\mathbf{h}}(\{\ell, \ell+1, \ldots, n\})$. Then note that $\mathbf{g}, \mathbf{h}, i$ are distributed as defined in the protocol η. Further, note that $(i, x_i, r_{i,\mathbf{g},\mathbf{h}})$ and $(\kappa_{\mathbf{h}}(\ell), \overline{x}_{\mathbf{h}}, \overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})})$ determine each other.

Protocol η for computing $f(x,y)$ when inputs are sampled according to μ.

1. Let s_h, s_g be uniformly random numbers from the set $\{n/2+1,\ldots,n\}$. Let $\kappa : [n] \to [n]$ be a uniformly random permutation. Set $\mathbf{h} = \kappa([s_h])$ and $\mathbf{g} = \kappa(\{n-s_g+1,\ldots,n\})$. Let i be a uniformly random element of $\mathbf{g} \cap \mathbf{h}$ (which must be non-empty by the choice of s_g, s_h).
2. Alice sets $x_i = x$ and Bob sets $y_i = y$.
3. Alice and Bob use Lemma 9 to sample $r_{i,\mathbf{g},\mathbf{h}}$: Alice uses the distribution $\pi(r_{i,\mathbf{g},\mathbf{h}}|x_iW)$ and Bob uses the distribution $\pi(r_{i,\mathbf{g},\mathbf{h}}|y_iW)$. Write $r'_{i,\mathbf{g},h}$ to denote Alice's sample and $r''_{i,\mathbf{g},\mathbf{h}}$ to denote Bob's sample.
4. Alice and Bob run protocol $\theta_{i,\mathbf{g},\mathbf{h}}$ from Figure 2 with inputs $(x_i, r'_{i,\mathbf{g},\mathbf{h}})$ and $(y_i, r''_{i,\mathbf{g},\mathbf{h}})$.

Figure 1: Protocol for computing f.

Protocol $\theta_{i,\mathbf{g},\mathbf{h}}$ for computing $f(x_i,y_i)$ when inputs $(x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}})$ are sampled according to $\pi((x_i, r_{i,\mathbf{g},\mathbf{h}}), (y_i, r_{i,\mathbf{g},\mathbf{h}})|W)$.

Alice sends each message M_j, j odd, according to the distribution $\pi(m_j|x_ir'_{i,\mathbf{g},\mathbf{h}}m_{<j}W)$. Bob sends each message M_j, j even, according to the distribution $\pi(m_j|y_ir''_{i,\mathbf{g},\mathbf{h}}m_{<j}W)$.

Figure 2: Simulation in the i'th coordinate.

Lemma 25. *In expectation over $i, \mathbf{g}, \mathbf{h}$ sampled according to $\eta(i\mathbf{gh})$,*

$$\pi(x_iy_i)\pi(r_{i,\mathbf{g},\mathbf{h}}|x_iW) \overset{3\gamma}{\approx} \pi(x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W) \overset{3\gamma}{\approx} \pi(x_iy_i)\pi(r_{i,\mathbf{g},\mathbf{h}}|y_iW).$$

Proof. To prove the lemma, we bound

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})}\left[\mathop{\mathbb{E}}_{\pi(r_{i,\mathbf{g},\mathbf{h}}x_i|W)}\left[\mathsf{D}\left(\frac{\pi(y_i|r_{i,\mathbf{g},\mathbf{h}}x_iW)}{\pi(y_i|x_i)}\right)\right]\right] \\
&= \mathop{\mathbb{E}}_{\eta(i\mathbf{gh})}\left[\mathop{\mathbb{E}}_{\pi(r_{i,\mathbf{g},\mathbf{h}}x_i|W)}\left[\mathsf{D}\left(\frac{\pi(y_i|r_{i,\mathbf{g},\mathbf{h}}x_iW)}{\pi(y_i|r_{i,\mathbf{g},\mathbf{h}}x_i)}\right)\right]\right],
\end{aligned}$$

since given x_i, the variable y_i is independent of $r_{i,\mathbf{g},\mathbf{h}}$ in π. This quantity can be expressed as:

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\eta(\mathbf{h},\kappa_{\mathbf{h}},\ell)}\left[\mathop{\mathbb{E}}_{\pi(\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})}|W)}\left[\mathsf{D}\left(\frac{\pi(y_{\kappa_{\mathbf{h}}(\ell)}|\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})}W)}{\pi(y_{\kappa_{\mathbf{h}}(\ell)}|\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})})}\right)\right]\right] \\
&= \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\sum_{\ell=1}^{n/2}\mathop{\mathbb{E}}_{\pi(\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})}|W)}\left[\mathsf{D}\left(\frac{\pi(\overline{y}_{\kappa_{\mathbf{h}}(\ell)}|\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})}W)}{\pi(\overline{y}_{\kappa_{\mathbf{h}}(\ell)}|\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})})}\right)\right]\right].
\end{aligned}$$

We apply the chain rule to show that this is equal to

$$\frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\mathop{\mathbb{E}}_{\pi(\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})}|W)}\left[\mathsf{D}\left(\frac{\pi(\overline{y}_{\kappa_{\mathbf{h}}([n/2])}|\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})}W)}{\pi(\overline{y}_{\kappa_{\mathbf{h}}([n/2])}|\overline{x}_{\mathbf{h}},\overline{y}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})})}\right)\right]\right].$$

This last expression is at most $(2/n)(\gamma^2 n) = 2\gamma^2$ by Lemma 18. Lemma 23 and Lemma 14 imply that in expectation over $\eta(i\mathbf{gh})$,

$$\begin{aligned}\pi(x_i y_i r_{i,\mathbf{g},\mathbf{h}}|W) &= \pi(x_i|W)\cdot\pi(r_{i,\mathbf{g},\mathbf{h}}|x_iW)\cdot\pi(y_i|r_{i,\mathbf{g},\mathbf{h}}x_iW)\\ &\overset{\sqrt{2}\gamma}{\approx} \pi(x_i|W)\cdot\pi(y_i|x_i)\cdot\pi(r_{i,\mathbf{g},\mathbf{h}}|x_iW)\\ &\overset{\gamma}{\approx} \pi(x_iy_i)\cdot\pi(r_{i,\mathbf{g},\mathbf{h}}|x_iW).\end{aligned}$$

The second approximation is symmetric and is proved similarly. □

Claim 26. *In expectation over $i,\mathbf{g},\mathbf{h}$ sampled according to $\eta(i\mathbf{gh})$,*

$$\theta_{i,\mathbf{g},\mathbf{h}}(x_iy_ir_{i,\mathbf{g},\mathbf{h}}m) \overset{2\gamma}{\approx} \pi(x_iy_ir_{i,\mathbf{g},\mathbf{h}}m|W).$$

.

Proof. Consider

$$\begin{aligned}&\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})}\left[\mathop{\mathbb{E}}_{\pi(x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W)}\left[\mathsf{D}\left(\frac{\pi(m|x_iy_ir_{i,\mathbf{g},\mathbf{h}}W)}{\theta_{i,\mathbf{g},\mathbf{h}}(m|x_iy_ir_{i,\mathbf{g},\mathbf{h}})}\right)\right]\right]\\ &=\sum_{j=1}^{2t}\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})}\left[\mathop{\mathbb{E}}_{\pi(m_{<j}x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W)}\left[\mathsf{D}\left(\frac{\pi(m_j|x_iy_ir_{i,\mathbf{g},\mathbf{h}}m_{<j}W)}{\theta_{i,\mathbf{g},\mathbf{h}}(m_j|x_iy_ir_{i,\mathbf{g},\mathbf{h}}m_{<j})}\right)\right]\right] \qquad \text{by the chain rule} \qquad (4)\end{aligned}$$

The odd j's correspond to the cases when Alice speaks. These terms contribute:

$$\begin{aligned}&\sum_{\text{odd } j}\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})}\left[\mathop{\mathbb{E}}_{\pi(m_{<j}x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W)}\left[\mathsf{D}\left(\frac{\pi(m_j|x_iy_ir_{i,\mathbf{g},\mathbf{h}}m_{<j}W)}{\pi(m_j|x_ir_{i,\mathbf{g},\mathbf{h}}m_{<j}W)}\right)\right]\right]\\ &=\sum_{\text{odd } j}\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})}\left[I_\pi(M_j;Y_i|X_iR_{i,\mathbf{g},\mathbf{h}}M_{<j}W)\right].\end{aligned}$$

As in the proof of Lemma 25, we can express this as

$$\begin{aligned}&\frac{2}{n}\sum_{\text{odd } j}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\sum_{\ell=1}^{n/2}I_\pi(M_j;Y_{\kappa_{\mathbf{h}}(\ell)}|\overline{X}_{\mathbf{h}}\overline{Y}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})}M_{<j}W)\right]\\ &=\frac{2}{n}\sum_{\text{odd } j}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[I_\pi(M_j;\overline{Y}_{\kappa_{\mathbf{h}}([n/2])}|\overline{X}_{\mathbf{h}}\overline{Y}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})}M_{<j}W)\right]. \qquad \text{by the chain rule}\end{aligned}$$

By Lemma 19, we can upper bound this by

$$\leq\frac{2}{n}\sum_{\text{odd } j}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\mathop{\mathbb{E}}_{\pi(m_{<j}\overline{x}_{\mathbf{h}}\overline{y}|W)}\left[\mathsf{D}\left(\frac{\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y}W)}{\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})})}\right)\right]\right].$$

Conditioned on $\overline{x}_{\mathbf{h}}\overline{y}_{\kappa_{\mathbf{h}}(\{n/2+1,\dots,n\})}$, the inputs $\overline{x},\overline{y}$ are independent. Thus Lemma 8 gives

$$\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y}_{\kappa_{\mathbf{h}}(\{n/2+1,\dots,n\})}) = \pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y}),$$

and we can continue to bound

$$= \frac{2}{n}\sum_{\text{odd } j}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\mathop{\mathbb{E}}_{\pi(m_{<j}\overline{x}_{\mathbf{h}}\overline{y}|W)}\left[\mathsf{D}\left(\frac{\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y}W)}{\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y})}\right)\right]\right].$$

Since the divergence is always non-negative, we can add in the even terms in the sum over j to bound

$$\begin{aligned}
&\le \frac{2}{n}\sum_{j=1}^{2t}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\mathop{\mathbb{E}}_{\pi(m_{<j}\overline{x}_{\mathbf{h}}\overline{y}|W)}\left[\mathsf{D}\left(\frac{\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y}W)}{\pi(m_j|m_{<j}\overline{x}_{\mathbf{h}}\overline{y})}\right)\right]\right] \\
&= \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\mathop{\mathbb{E}}_{\pi(\overline{x}_{\mathbf{h}}\overline{y}|W)}\left[\mathsf{D}\left(\frac{\pi(m|\overline{x}_{\mathbf{h}}\overline{y}W)}{\pi(m|\overline{x}_{\mathbf{h}}\overline{y})}\right)\right]\right] && \text{by the chain rule} \\
&\le \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\gamma^2 n\right] = 2\gamma^2. && \text{by Lemma 17}
\end{aligned}$$

Repeating the same argument for even j gives (4) $\le 4\gamma^2$. We apply Lemma 14 to conclude the proof. □

3.1 Completing the Proof of Lemma 3

Claim 27. *The expected value of the expression for the internal information cost according to π conditioned on W can be bounded:*

$$\mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[(I_\pi(X_i;M|Y_iR_{i,\mathbf{g},\mathbf{h}}W) + I_\pi(Y_i;M|X_iR_{i,\mathbf{g},\mathbf{h}}W))\right] \le 4\|\pi\|/n.$$

Proof. As in the previous claims, we can write

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[I_\pi(Y_i;M|X_iR_{i,\mathbf{g},\mathbf{h}}W)\right] \\
&= \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\sum_{\ell=1}^{n/2} I_\pi(Y_{\kappa_{\mathbf{h}}(\ell)};M|\overline{X}_{\mathbf{h}}\overline{Y}_{\kappa_{\mathbf{h}}(\{\ell+1,\dots,n\})}W)\right] \\
&= \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[I_\pi(\overline{Y}_{\kappa_{\mathbf{h}}([n/2])};M|\overline{X}_{\mathbf{h}}\overline{Y}_{\kappa_{\mathbf{h}}(\{n/2+1,\dots,n\})}W)\right] && \text{by the chain rule} \\
&\le 2\|\pi\|/n.
\end{aligned}$$

Repeating the argument for the second term gives the final bound. □

In the probability space of π, let $i,\mathbf{g},\mathbf{h}$ be independent of all other variables, and distributed as in η. Let $x' = (i,\mathbf{g},\mathbf{h},x_i,r_{i,\mathbf{g},\mathbf{h}})$ and $y' = (i,\mathbf{g},\mathbf{h},y_i,r_{i,\mathbf{g},\mathbf{h}})$. Define the protocol θ that gets inputs $(i,\mathbf{g},\mathbf{h},x_i,r'_{i,\mathbf{g},\mathbf{h}})$ and $(i,\mathbf{g},\mathbf{h},y_i,r''_{i,\mathbf{g},\mathbf{h}})$, where the inputs are distributed according to

$$\pi((i,\mathbf{g},\mathbf{h},x_i,r_{i,\mathbf{g},\mathbf{h}}),(i,\mathbf{g},\mathbf{h},y_i,r_{i,\mathbf{g},\mathbf{h}})|W),$$

and executes $\theta_{i,\mathbf{g},\mathbf{h}}((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}}))$.

By Lemma 9 and Lemma 25, $\Pr_\eta[R'_{i,\mathbf{g},\mathbf{h}} \neq R''_{i,\mathbf{g},\mathbf{h}}] \leq O(\gamma)$. Thus in expectation over $i, \mathbf{g}, \mathbf{h}$ sampled according to $\eta(i\mathbf{gh})$,

$$\eta((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}})) \overset{O(\gamma)}{\approx} \eta((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r'_{i,\mathbf{g},\mathbf{h}})),$$

where here $\eta((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r'_{i,\mathbf{g},\mathbf{h}}))$ denotes the distribution where Bob's sample for $r''_{i,\mathbf{g},\mathbf{h}}$ is set to be the same as Alice's sample. By Lemma 25 and Lemma 23,

$$\eta(i\mathbf{gh}xyr'_{i,\mathbf{g},\mathbf{h}}) \overset{O(\gamma)}{\approx} \pi(i\mathbf{gh}x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W).$$

Therefore the protocol η can be viewed as executing θ as a subroutine with inputs that are $O(\gamma)$-close to $\theta(x', y')$. Claim 26 implies that $\theta(x'y'm) \overset{O(\gamma)}{\approx} \pi(x'y'm|W)$. Claim 27 implies that

$$\begin{aligned} &I_\pi(X'; M|Y'W) + I_\pi(Y'; M|X'W) \\ &\qquad = \mathop{\mathbb{E}}_{\eta(i\mathbf{gh})} [I_\pi(X_i; M|Y_iR_{i,\mathbf{g},\mathbf{h}}W) + I_\pi(Y_i; M|X_iR_{i,\mathbf{g},\mathbf{h}}W)] \\ &\qquad \leq 4\|\pi\|/n. && \text{since } \|\pi\| \geq \gamma^2 n \end{aligned}$$

To prove Lemma 3, we apply Theorem 6 to conclude that there exists a protocol that $O(\gamma)$-simulates θ with communication at most

$$\frac{\log\|\pi\|\sqrt{4\|\pi\|/n + 1 + \log\|\pi\|)\|\pi\|}}{\gamma^{3/2}} < O\left(\frac{\|\pi\| \cdot \log^{3/2}\|\pi\|}{\sqrt{n}\gamma^{5/2}}\right) < C,$$

where the first inequality appealed to the fact that $\|\pi\|/n > \gamma^2$ and the second is by our choice of α in the statement of Lemma 3. The proof of Lemma 3 is complete, since η computes f with probability of success at least $(1/n)\sum_{i=1}^n \pi(W_i|W) - O(\gamma)$. □

3.2 Completing the proof of Lemma 4

Claim 28. *The expected value of the expression for the external information cost according to π conditioned on W can be bounded:*

$$\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})} [I_\pi(X_iY_i; M|R_{i,\mathbf{g},\mathbf{h}}W)] \leq 2\gamma^2 + 4\|\pi\|/n.$$

Proof. By the chain rule,

$$\mathop{\mathbb{E}}_{\eta(i\mathbf{gh})} [I_\pi(X_iY_i; M|R_{i,\mathbf{g},\mathbf{h}}W)] = \mathop{\mathbb{E}}_{\eta(i\mathbf{gh})} [I_\pi(Y_i; M|R_{i,\mathbf{g},\mathbf{h}}W) + I_\pi(X_i; M|Y_iR_{i,\mathbf{g},\mathbf{h}}W)].$$

The second term was upper bounded in Claim 27 by $2\|\pi\|/n$. It remains to bound the first term:

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[I_\pi(Y_i;M|R_{i,\mathbf{g},\mathbf{h}}W)\right] \\
&\leq \mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[\mathop{\mathbb{E}}_{\pi(mr_{i,\mathbf{g},\mathbf{h}}|W)}\left[\mathsf{D}\left(\frac{\pi(y_i|mr_{i,\mathbf{g},\mathbf{h}}W)}{\pi(y_i|r_{i,\mathbf{g},\mathbf{h}})}\right)\right]\right] && \text{by Lemma 19} \\
&\leq \mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[\mathop{\mathbb{E}}_{\pi(m\overline{xy}_{\mathbf{g}\setminus\{i\}}|W)}\left[\mathsf{D}\left(\frac{\pi(y_i|m\overline{xy}_{\mathbf{g}\setminus\{i\}}W)}{\pi(y_i|r_{i,\mathbf{g},\mathbf{h}})}\right)\right]\right] && \text{by Lemma 18} \\
&\leq \mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[\mathop{\mathbb{E}}_{\pi(m\overline{xy}_{\mathbf{g}\setminus\{i\}}|W)}\left[\mathsf{D}\left(\frac{\pi(y_i|m\overline{xy}_{\mathbf{g}\setminus\{i\}}W)}{\pi(y_i|\overline{x}y_{\mathbf{g}\setminus\{i\}})}\right)\right]\right]. && \text{since } \mu \text{ is product}
\end{aligned}$$

Given $\mathbf{h}$, let $\kappa_{\mathbf{h}}, \ell$ be distributed as explained before Lemma 25. Then the expression of interest is

$$\begin{aligned}
&= \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\sum_{\ell=1}^{n/2}\mathop{\mathbb{E}}_{\pi(\overline{xy}_{\kappa_h(\{\ell+1,\ldots,n\})}|W)}\left[\mathsf{D}\left(\frac{\pi(y_{\kappa_{\mathbf{h}}(\ell)}|m\overline{xy}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})}W)}{\pi(y_{\kappa_{\mathbf{h}}(\ell)}|\overline{xy}_{\kappa_{\mathbf{h}}(\{\ell+1,\ldots,n\})})}\right)\right]\right] \\
&= \frac{2}{n}\mathop{\mathbb{E}}_{\eta(\mathbf{h}\kappa_{\mathbf{h}})}\left[\mathop{\mathbb{E}}_{\pi(\overline{xy}_{\kappa_h(\{n/2+1,\ldots,n\})}|W)}\left[\mathsf{D}\left(\frac{\pi(y_{\kappa_{\mathbf{h}}([n/2])}|m\overline{xy}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})}W)}{\pi(y_{\kappa_{\mathbf{h}}([n/2])}|\overline{xy}_{\kappa_{\mathbf{h}}(\{n/2+1,\ldots,n\})})}\right)\right]\right],
\end{aligned}$$

where the last equality follows from the chain rule. By Lemma 17, this expression is at most $(2/n)(\gamma^2 n + \|\pi\|) = 2\gamma^2 + 2\|\pi\|/n$. This proves the claim. □

In the probability space of π, let $i, \mathbf{g}, \mathbf{h}$ be distributed as in η, independent of all other variables. Let $x' = x_i$ and $y' = y_i$ and $r' = i, \mathbf{g}, \mathbf{h}, r_{i,\mathbf{g},\mathbf{h}}$. Define the protocol θ that gets inputs x' and y' and uses public randomness r', where all variables are distributed according to $\pi(i\mathbf{g}\mathbf{h}x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W)$. Given these inputs, θ executes $\theta_{i,\mathbf{g},\mathbf{h}}$ with inputs $((x_i, r_{i,\mathbf{g},\mathbf{h}}), (y_i, r_{i,\mathbf{g},\mathbf{h}}))$.

By Lemma 9 and Lemma 25, $\Pr_\eta[R'_{i,\mathbf{g},\mathbf{h}} \neq R''_{i,\mathbf{g},\mathbf{h}}] \leq O(\gamma)$. Thus in expectation over $i, \mathbf{g}, \mathbf{h}$ sampled according to $\eta(i\mathbf{g}\mathbf{h})$,

$$\eta((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r''_{i,\mathbf{g},\mathbf{h}})) \overset{O(\gamma)}{\approx} \eta((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r'_{i,\mathbf{g},\mathbf{h}}))$$

where here $\eta((x_i, r'_{i,\mathbf{g},\mathbf{h}}), (y_i, r'_{i,\mathbf{g},\mathbf{h}}))$ denotes the distribution where Bob's sample for $r''_{i,\mathbf{g},\mathbf{h}}$ is set to be the same as Alice's sample. By Lemma 25 and Lemma 23,

$$\eta(i\mathbf{g}\mathbf{h}xyr'_{i,\mathbf{g},\mathbf{h}}) \overset{O(\gamma)}{\approx} \pi(i\mathbf{g}\mathbf{h}x_iy_ir_{i,\mathbf{g},\mathbf{h}}|W).$$

Therefore the protocol η can be viewed as executing θ as a subroutine with inputs and public randomness that are $O(\gamma)$-close to $\theta(x'y'r')$. Claim 26 implies that $\theta(x'y'r'm) \overset{O(\gamma)}{\approx} \pi(x'y'r'm|W)$. Claim 28 implies that

$$\begin{aligned}
I_\pi(X'Y';M|R'W) &= \mathop{\mathbb{E}}_{\eta(i\mathbf{g}\mathbf{h})}\left[I_\pi(X_iY_i;M|R_{i,\mathbf{g},\mathbf{h}}W)\right] \\
&\leq 2\gamma^2 + 4\|\pi\|/n \leq 6\|\pi\|/n. && \text{since } \|\pi\| \geq \gamma^2 n
\end{aligned}$$

We apply Theorem 5 to obtain a protocol τ simulating θ with error $O(\gamma)$, whose external information cost is $O\left(\frac{\|\pi\|/n+\log\|\pi\|}{\gamma}\right) = O\left(\frac{\|\pi\|\log\|\pi\|}{\gamma^3 n}\right)$, where here we used $\|\pi\| \geq 2$ and $\|\pi\| \geq \gamma^2 n$. Finally, we apply Theorem 11 with error parameter γ, to obtain a protocol that computes f with probability $(1/n)\sum_i \pi(W_i|W) - O(\gamma)$, with communication

$$O\left(\frac{\|\pi\| \cdot \log\|\pi\| \cdot \log(\|\pi\|/\gamma)}{\gamma^5 n}\right) \leq O\left(\frac{\|\pi\| \cdot \log^2\|\pi\|}{\gamma^6 n}\right) \leq C,$$

by our choice of α in Lemma 4. □

3.3 Intuition for the Choice of the Conditioning Variables

In this section we provide additional intuition for the selection of the publicly sampled variables $r_{i,\mathbf{g},\mathbf{h}}$, since this selection is different than the selection of the corresponding variables in previous works [BYJKS04, BBCR10, BR11]. This section is particularly useful to readers familiar with one of these previous works.

Without the conditioning on W, the goal of the publicly sampled variables is to break the dependence between the inputs that are not publicly sampled on Alice's side and on Bob's side. Suppose that i is the coordinate into which inputs (x, y) are embedded, so $(x_i, y_i) = (x, y)$. To break the dependence, it suffices to publicly sample one of the two variables x_j, y_j in each coordinate $j \neq i$. For example, if $n = 6$ and $i = 3$, a typical choice of publicly sampled variables is of the form $r = (x_1, x_2, y_4, y_5, y_6)$. In this case, Alice and Bob can then privately sample x_4, x_5, x_6 and y_1, y_2, respectively, and run the 6-copy protocol. If the first message of the protocol is m sent by Alice, then the amount of information Bob learns about $x = x_3$ from m is given by $I(X_3; M|X_1X_2\overline{Y})$. We would like to say that this quantity is typically bounded by $|M|/n$, where $|M|$ is the length of the message. Unfortunately, as stated, we can only bound it by $|M|$. Luckily, one can show that *typically* this type of expression is bounded by $|M|/n$. The key is to collect several of them and apply the chain rule:

$$I(X_1; M|\overline{Y}) + I(X_2; M|X_1\overline{Y}) + \ldots + I(X_6; M|X_1X_2X_3X_4X_5\overline{Y}) = I(\overline{X}; M|\overline{Y}) \leq H(M) \leq |M|,$$

giving us the desired bound.

We continue to explain the main challenge we face, glossing over some details. Above, since M is generated by Alice who knows $X_1X_2X_3Y_4Y_5Y_6$, we have $I(Y_3; M|X_1X_2X_3Y_4Y_5Y_6) = 0$. This in turn implies that Alice can perfectly simulate her messages in the protocol. However, the event W may introduce dependencies that could cause $I(Y_3; M|X_1X_2X_3Y_4Y_5Y_6W)$ to be fairly high. This quantity is the amount of information about Y_3 (which Alice does not know) needed to produce M. A priori, the best general bound we can get on the amount of dependence introduced by W is at most $\log\frac{1}{\pi(W)} \leq \gamma^2 n$. Such a poor bound will not provide any guarantee on the ability of Alice to faithfully simulate her part in the protocol[3]. To carry out our proof we need to bound this quantity by $O(\gamma^2)$. As before, the solution is to combine many (order n) expressions into one that is still bounded by $\gamma^2 n$. We are left with trying to combine terms of the form

$$I(Y_1; M|X_1Y_2Y_3Y_4Y_5Y_6W), I(Y_2; M|X_1X_2Y_3Y_4Y_5Y_6W), I(Y_3; M|X_1X_2X_3Y_4Y_5Y_6W), \ldots$$

[3] However, a round-by-round argument can provide a non-trivial bound. This was the approach taken in [JPY12].

Unfortunately, these terms do not add up using the chain rule. On the other hand, for example, the sum

$$I(Y_1; M|X_1X_2X_3Y_4Y_5Y_6W) + I(Y_2; M|X_1X_2X_3Y_1Y_4Y_5Y_6W) + I(Y_3; M|X_1X_2X_3Y_1Y_2Y_4Y_5Y_6W)$$

adds up using the chain rule to $I(Y_1Y_2Y_3; M|X_1X_2X_3Y_4Y_5Y_6W)$, which is also bounded by $\gamma^2 n$. Thus, on average, these terms are bounded by $\gamma^2 n/3$. To apply the chain rule in this fashion, we had to use terms with overlaps between the X part and the Y part of the conditioned variables: one with an overlap of 0 coordinates ($X_1X_2X_3Y_4Y_5Y_6$), one with an overlap of 1 coordinate ($X_1X_2X_3Y_1Y_4Y_5Y_6$), and one with and overlap of 2 coordinates ($X_1X_2X_3Y_1Y_2Y_4Y_5Y_6$). So instead of selecting only R's with 0 overlap (as before), we make the size of the overlap vary uniformly between 0 and $n/2 - 1$. This allows us to bound the mutual information in a typical term by $2\gamma^2$. It is an interesting question whether selecting R's with overlaps is necessary for our proof to go through.

As a final remark, we note that even with the new choice of R, the conditioning on W creates more complications. Due to the conditioning on W, Alice can no longer just sample $X_4X_5X_6$ privately, even when $X_1X_2Y_1Y_2Y_4Y_5Y_6$ is publicly known. For example, if x_i, y_i are bits, consider the event W that $\sum_i x_i + y_i = 0 \mod 2$. In this case, the distribution of $X_4X_5X_6$ depends on Y_3 which Alice does not know. What does she do then? She just samples M conditioned on her knowledge $X_1X_2X_3Y_1Y_2Y_4Y_5Y_6$ and on W, and hopes for the best. This turns out to be a good enough approximation of the true distribution of M conditioned on W.

4 Proofs of the Compression/Simulation Theorems

4.1 Compressing Protocols that are Close to Low Internal Information

Here we prove Theorem 6, showing how to compress protocols that are close to having low internal information. For the rest of this proof, denote

$$I = I_q(X; M|Y) + I_q(Y; M|X).$$

The simulating protocol τ is given in Figure 3.

4.1.1 Analysis

The communication complexity of τ is bounded by C by definition. Define $m \in \{0,1\}^{\|\theta\|}$ inductively by:

$$m_j = \begin{cases} a_{m_{<j}} & \text{if } j \text{ is odd,} \\ b_{m_{<j}} & \text{if } j \text{ is even.} \end{cases}$$

The string m is the intended simulation that Alice and Bob should converge to at the end of τ. The first observation is that m is correctly distributed, i.e., as the messages of θ.

Claim 29. *$\tau(xym) = \theta(xym)$.*

Proof. By the definition of m, for odd j, $\theta(m_j|xym_{<j}) = \theta(m_j|xm_{<j}) = \tau(m_j|xym_{<j})$, and similarly for even j, $\theta(m_j|xym_{<j}) = \tau(m_j|xym_{<j})$. □

Protocol τ for simulating θ

Phase 1: For every binary string m' of length at most $\|\theta\|$, the parties use shared randomness to sample a uniformly random number $\rho_{m'} \in [0,1]$. Alice uses this number to compute a bit

$$a_{m'} = \begin{cases} 0 & \text{if } \theta(M_j = 0|xm') > \rho_{m'}, \\ 1 & \text{else.} \end{cases}$$

Similarly, Bob computes

$$b_{m'} = \begin{cases} 0 & \text{if } \theta(M_j = 0|ym') > \rho_{m'}, \\ 1 & \text{else.} \end{cases}$$

Phase 2: The parties repeat the following steps as long as at most $C = \frac{\log\|\theta\|\sqrt{(I+1+\log\|\theta\|)\|\theta\|}}{\epsilon^{3/2}}$ bits are communicated:

1. Alice computes the messages $a \in \{0,1\}^{\|\theta\|}$ defined inductively by $a_j = a_{a_{<j}}$ for each j. Similarly, Bob computes the messages $b \in \{0,1\}^{\|\theta\|}$ defined inductively by $b_j = b_{b_{<j}}$ for each j.
2. Alice and Bob use the protocol of Lemma 10 with error parameter $1/10$ to find the smallest location j such that $a_j \neq b_j$. If j is odd Bob resets $b_{b_{<j}} = a_j$. If j is even, Alice resets $a_{a_{<j}} = b_j$. If no such j is found, the parties do nothing.

Alice (resp. Bob) considers the final a (resp. b) the simulated outcome of the protocol.

Figure 3: Compression according to internal information cost.

We shall argue that the probability $\tau(a = m = b)$ is very close to 1. Say that there is a *mistake at coordinate* j if $a_{m_{<j}} \neq b_{m_{<j}}$. The location of the first (uncorrected) mistake is exactly the same as the location of the first disagreement between a, b in Phase 2 of τ. As long as the number of successful executions of the algorithm from Lemma 10 in Phase 2 exceeds the number of mistakes in Phase 1, we will eventually have $a = m = b$. Let $\ell \geq \Omega(C/\log\|\theta\|)$ denote the number of times that the application of Lemma 9 is run in Phase 2. By the Chernoff bound, at least $\ell/2$ executions of the algorithm from Lemma 10 find the correct coordinate, except with probability $\exp(-\Omega(\ell))$.To complete the proof of the theorem, we shall argue that the number of mistakes is at most $\ell/2$ with high probability.

Let

$$\beta = \frac{I + 1/(e\ln 2) + \log(\|\theta\| + 1)}{\epsilon} + 2.$$

For any x, y, r, m, let k denote the smallest index j such that either

$$\log\frac{\theta(m_{\leq j}|xy)}{\theta(m_{\leq j}|x)} > \beta \text{ or } \log\frac{\theta(m_{\leq j}|xy)}{\theta(m_{\leq j}|y)} > \beta. \tag{5}$$

If no such index exists, define $k = \|\theta\| + 1$. The random variable[4] K is a function of X, Y, M.

Claim 30. *The expected number of mistakes up to the k'th coordinate is small:*

$$\mathop{\mathbb{E}}_{\theta}\left[\left|\{j < k : a_{m_{<j}} \neq b_{m_{<j}}\}\right|\right] \leq \sqrt{\frac{\beta \cdot \|\theta\|}{2}}.$$

Proof. Suppose j is odd. There is a mistake in the j'th step only when $\rho_{m_{<j}}$ lies in between $\theta(m_j|xym_{<j}) = \theta(m_j|xm_{<j})$ and $\theta(m_j|ym_{<j})$. The probability of a mistake in the j'th message contributing to the expectation is at most

$$(1/2) \sum_{x,y,m_{<j},k} \theta(xym_{<j}k) \cdot \mathbf{1}_{j<k} \cdot |\theta(m_j|xym_{<j}) - \theta(m_j|ym_{<j})|,$$

where $\mathbf{1}_{j<k}$ is the indicator variable for whether or not $j < k$. We bound this by

$$\begin{aligned} &(1/2) \sum_{x,y,m_{<j},k} \theta(xym_{<j}k) \cdot \mathbf{1}_{j<k} \cdot \sqrt{\mathsf{D}\left(\frac{\theta(m_j|xym_{<j})}{\theta(m_j|ym_{<j})}\right)} && \text{by Lemma 14} \\ &\leq (1/2) \sqrt{\sum_{x,y,m_{<j},k} \theta(xym_{<j}k) \cdot \mathbf{1}_{j<k} \cdot \mathsf{D}\left(\frac{\theta(m_j|xym_{<j})}{\theta(m_j|ym_{<j})}\right)} && \text{by concavity} \\ &= (1/2) \sqrt{\sum_{x,y,m,k} \mathbf{1}_{j<k} \cdot \theta(xymk) \log \frac{\theta(m_j|xym_{<j})}{\theta(m_j|ym_{<j})}}. \end{aligned}$$

A similar bound applies for even j, and the expected number of mistakes in the j'th step for all j is at most

$$(1/2) \sqrt{\sum_{x,y,m,k} \mathbf{1}_{j<k} \cdot \theta(xymk) \log \frac{\theta(m_j|xym_{<j})^2}{\theta(m_j|xm_{<j})\theta(m_j|ym_{<j})}}.$$

The expected number of mistakes before the k'th message is therefore at most

$$\begin{aligned} &(1/2) \sum_j \sqrt{\sum_{x,y,m,k} \mathbf{1}_{j<k} \cdot \theta(xymk) \log \frac{\theta(m_j|xym_{<j})^2}{\theta(m_j|xm_{<j})\theta(m_j|ym_{<j})}} \\ &\leq (1/2) \sqrt{\|\theta\| \cdot \sum_{x,y,m,j,k} \mathbf{1}_{j<k} \cdot \theta(xymk) \log \frac{\theta(m_j|xym_{<j})^2}{\theta(m_j|xm_{<j})\theta(m_j|ym_{<j})}} && \text{by Cauchy-Schwartz} \\ &= (1/2) \sqrt{\|\theta\| \cdot \sum_{x,y,m,k} \theta(xymk) \log \frac{\theta(m_{<k}|xy)^2}{\theta(m_{<k}|x)\theta(m_{<k}|y)}} \leq \sqrt{\frac{\beta \cdot \|\theta\|}{2}}. && \text{by the definition of } k \end{aligned}$$

□

[4] Since it can be ambiguous whether the expression $p(m_k)$ refers to $p(M_K = m_k)$ or $p(M_k = m_k)$, we shall be more explicit with the notation in the rest of this section. However, observe that $p(m_k, k)$ has only one interpretation, so in such cases we use the more concise notation.

Next we show that, with high probability, $k = \|\theta\| + 1$.

Claim 31. *$\theta(k \leq \|\theta\|) < 11\epsilon$.*

Proof. Define k_1 and k_2 to be the minimum indices so that

$$\log \frac{\theta(m_{\leq k_1}|xy)}{\theta(m_{\leq k_1}|x)} > \beta \quad \text{and} \quad \log \frac{\theta(m_{\leq k_2}|xy)}{\theta(m_{\leq k_2}|y)} > \beta,$$

respectively (if no such index exists, set the value to be $\|\theta\|+1$). Then $k = \min\{k_1, k_2\}$. By Lemma 21 we have

$$\theta(k_1 \leq \|\theta\|) < \frac{I_q(M;Y|X) + \log(\|\theta\|+1) + 1/(e\ln 2)}{\beta - 2} + 9\epsilon/2 \leq 11\epsilon/2.$$

Similarly, $\theta(k_2 \leq \|\theta\|) < 11\epsilon/2$, and the claim is proved by the union bound. □

By Claim 29, Claim 30, Claim 31 and Markov's inequality, the probability that the number of mistakes in τ exceeds $\ell/2$ is at most $\frac{\sqrt{2\beta\cdot\|\theta\|}}{\ell} + 11\epsilon$. The simulation, therefore, computes m except with probability

$$\frac{\sqrt{2\beta\cdot\|\theta\|}}{\ell} + 11\epsilon + \exp(-\Omega(\ell)) = O\left(\frac{\log\|\theta\|\sqrt{(I+1+\log\|\theta\|)\cdot\|\theta\|}}{\sqrt{\epsilon}C} + \epsilon\right) = O(\epsilon),$$

where here we used the fact that $C \neq 0$. □

4.2 Simulating Protocols that are Close to Low External Information

In this section we prove Theorem 5, showing that protocols that are statistically close to having low external information cost can be modified so that they actually have low external information cost.

4.2.1 The Simulating Protocol τ

The protocol τ is defined as follows. Let

$$\beta = \frac{I_q(XY;M|R) + 1/(e\ln 2) + \log(\|\theta\|+1)}{\epsilon} + \log(1/\epsilon) + 2.$$

The parties simulate θ, but before each message m_j sent by Alice, she checks whether the sequence of messages $m_{<j}$ sent by her so far, including the message m_j that will result from her transmission, satisfies

$$\sum_{d\leq j, d \text{ odd}} \log \frac{\theta(m_d|xrm_{<d})}{\theta(m_d|rm_{<d})} \leq \beta.$$

If this is not the case, she sends a bit e_j to Bob indicating that the protocol must be aborted. If the condition is met, she sends a bit e_j indicating that the protocol will continue, and then transmits the sampled bit m_j.

Similarly, before each message m_j sent by Bob, he checks whether the sequence of messages $m_{<j}$ sent by him so far, including the message m_j that will result from his transmission, satisfies

$$\sum_{d \leq j, d \text{ even}} \log \frac{\theta(m_d | yrm_{<d})}{\theta(m_d | rm_{<d})} \leq \beta.$$

If this is not the case, he sends a bit e_j to Alice indicating that the protocol must be aborted. If the condition is met, he sends a bit e_j indicating that the protocol will continue, and transmits the sampled bit m_j .

For clarity of notation, we accomplish the aborts by having Alice and Bob transmit 0's for the rest of the protocol, so that all full transcripts are of the same length. This gives $\|\tau\| \leq 2\|\theta\|$. The full transcript of the parties in τ is denoted by the random variables E, M, where E is the concatenation of all the abort bits E_j, and M is the protocol transcript of θ.

4.2.2 Analysis

For any x, y, r, m, let k denote the smallest index j such that either

$$\sum_{d \leq j, d \text{ odd}} \log \frac{\theta(m_d | xrm_{<d})}{\theta(m_d | rm_{<d})} > \beta \quad \text{or} \quad \sum_{d \leq j, d \text{ even}} \log \frac{\theta(m_d | yrm_{<d})}{\theta(m_d | rm_{<d})} > \beta. \tag{6}$$

If no such index, define $k = \|\theta\| + 1$. The random variable[5] K is a function of X, Y, R, M.

Claim 32. *For each $x, y, r, m_{<k}, k$, $\theta(xyrkm_{<k}) = \tau(xyrkm_{<k})$.*

Proof. Fix any $x, y, r, m_{<k}, k$. If there exists a $j < k$ such that the messages $m_{\leq j}$ cause an abort in the j'th step, then we must have that $\theta(xyrm_{<k}k) = 0 = \tau(xyrm_{<k}k)$. So, we can assume that there is no such j.

By definition, $\tau(xyr) = \theta(xyr)$. We prove by induction on j that for all $j < k$, $\tau(M_j = m_j | xyrm_{<j}) = \theta(m_j | xyrm_{<j})$. In τ the sender of the j'th message samples $M_j = m_j$ with probability $\theta(m_j | xyrm_{<j})$. Since we have assumed that the sender does not abort, this m_j is transmitted, and we have proved the inductive step. This shows that for every fixed k,

$$\tau(M_{<k} = m_{<k}, xyr) = \prod_{j<k} \tau(m_j | xyrm_{<j}) = \prod_{j<k} \theta(m_j | xyrm_{<j}) = \theta(M_{<k} = m_{<k}, xyr).$$

We have $\tau(K = k | M_{<k} = m_{<k}, xyr) = \theta(K = k | M_{<k} = m_{<k}, xyr)$, since both numbers are the probability that the k'th message leads to an abort. □

Claim 33. *$I_\tau(XY; ME|R) \leq 2\beta + \log(\|\theta\| + 1)$.*

[5] Since it can be ambiguous whether the expression $p(m_k)$ refers to $p(M_K = m_k)$ or $p(M_k = m_k)$, we shall be more explicit with the notation in the rest of this section. However, observe that $p(m_k, k)$ has only one interpretation, so in such cases we use the more concise notation.

Proof. The random variables $K, M_{<K}$ determine M, E in τ. Thus,

$$\begin{aligned}
&I_\tau(XY; ME|R) \\
&\le I_\tau(XY; KM_{<K}|R) \\
&= I_\theta(XY; KM_{<K}|R) && \text{Claim 32} \\
&= \sum_{x,y,r,k,m_{<k}} \theta(xyrkm_{<k}) \log \frac{\theta(km_{<k}|xyr)}{\theta(km_{<k}|r)} \\
&= \sum_{x,y,r,k,m_{<k}} \theta(xyrkm_{<k}) \left(\log \frac{\theta(M_{<k} = m_{<k}|xyr)}{\theta(M_{<k} = m_{<k}|r)} + \log \frac{\theta(K = k|M_{<k} = m_{<k}, xyr)}{\theta(K = k|M_{<k} = m_{<k}, r)} \right). && (7)
\end{aligned}$$

The second term can be bounded as follows:

$$\begin{aligned}
\sum_{x,y,r,k,m_{<k}} &\theta(xyrkm_{<k}) \log \frac{\theta(K = k|M_{<k} = m_{<k}, xyr)}{\theta(K = k|M_{<k} = m_{<k}, r)} \\
&\le \sum_{r,k,m_{<k}} \theta(rkm_{<k}) \log \frac{1}{\theta(K = k|M_{<k} = m_{<k}, r)} \\
&\le \log \sum_{r,k,m_{<k}} \frac{\theta(rkm_{<k})}{\theta(K = k|M_{<k} = m_{<k}, r)} && \text{by concavity of log} \\
&= \log \sum_{r,k,m_{<k}} \theta(M_{<k} = m_{<k}, r) = \log(\|\theta\| + 1). && (8)
\end{aligned}$$

Next we bound the first term in (7):

$$\log \left(\frac{\theta(M_{<k} = m_{<k}|xyr)}{\theta(M_{<k} = m_{<k}|r)} \right) = \sum_{j<k, j \text{ odd}} \log \frac{\theta(m_j|xrm_{<j})}{\theta(m_j|rm_{<j})} + \sum_{j<k, j \text{ even}} \log \frac{\theta(m_j|yrm_{<j})}{\theta(m_j|rm_{<j})},$$

where here we used the fact that since θ is a protocol, each (odd) message m_j sent by Alice satisfies $\theta(m_j|xyrm_{<j}) = \theta(m_j|xrm_{<j})$, and that a similar statement holds for Bob's messages. Thus by the definition of K,

$$\sum_{x,y,r,k,m_{<k}} \theta(xyrkm_{<k}) \log \frac{\theta(M_{<k} = m_{<k}|xyr)}{\theta(M_{<k} = m_{<k}|r)} \le 2\beta. \tag{9}$$

Combining (7), (8) and (9), we conclude that $I_\tau(X; ME|R) \le 2\beta + \log(\|\theta\| + 1)$. □

Next, we argue that the probability that the protocol aborts is small.

Claim 34. $\tau(k \le \|\theta\|) = \theta(k \le \|\theta\|) < 15\epsilon/2$.

Proof. For any x, y, r, m, let k' denote the smallest index such that

$$\log \frac{\theta(m_{\le k'}|xyr)}{\theta(m_{\le k'}|r)} = \sum_{j \le k', j \text{ odd}} \log \frac{\theta(m_j|xrm_{<j})}{\theta(m_j|rm_{<j})} + \sum_{j \le k', j \text{ even}} \log \frac{\theta(m_j|yrm_{<j})}{\theta(m_j|rm_{<j})} > \beta - \log(1/\epsilon).$$

If no such index, define $k' = \|\theta\| + 1$. By Lemma 21, we have

$$\theta(k' \le \|\theta\|) < \frac{I_q(XY; M|R) + 1/(e \ln 2) + \log(\|\theta\| + 1)}{\beta - 2 - \log(1/\epsilon)} + 9\epsilon/2 \le 11\epsilon/2. \tag{10}$$

We shall show that $\theta(k < k') < 2\epsilon$, which will complete the proof. Define

$$S_1 = \left\{ (x, y, r, m) : k(x, y, r, m) \le \|\theta\| \text{ and } \sum_{d \le k, d \text{ odd}} \log \frac{\theta(m_d | x r m_{<d})}{\theta(m_d | r m_{<d})} \le -\log(1/\epsilon) \right\},$$

$$S_2 = \left\{ (x, y, r, m) : k(x, y, r, m) \le \|\theta\| \text{ and } \sum_{d \le k, d \text{ even}} \log \frac{\theta(m_d | y r m_{<d})}{\theta(m_d | r m_{<d})} \le -\log(1/\epsilon) \right\}.$$

Observe that $k < k'$ implies that $(x, y, r, m) \in S_1 \cup S_2$. We shall prove that $\theta(S_1) \le \epsilon$ and $\theta(S_2) \le \epsilon$. Consider the distribution

$$\theta'(xyrm) = \theta(xyr) \cdot \prod_{d \text{ odd}} \theta(m_d | r m_{<d}) \cdot \prod_{d \text{ even}} \theta(m_d | y r m_{<d}).$$

Fix any $(x, y, r, m) \in S_1$, and let $k = k(x, y, r, m)$ be defined as above. We have:

$$\begin{aligned}
&\log \frac{\theta(k m_{\le k} | xyr)}{\theta'(k m_{\le k} | xyr)} \\
&= \sum_{d \le k, d \text{ odd}} \log \frac{\theta(m_d | x r m_{<d})}{\theta(m_d | r m_{<d})} + \sum_{d \le k, d \text{ even}} \log \frac{\theta(m_d | y r m_{<d})}{\theta(m_d | y r m_{<d})} + \log \frac{\theta(K = k | M_{\le k} = m_{\le k}, xyr)}{\theta'(K = k | M_{\le k} = m_{\le k}, xyr)} \\
&= \sum_{d \le k, d \text{ odd}} \log \frac{\theta(m_d | x r m_{<d})}{\theta(m_d | r m_{<d})} \le -\log(1/\epsilon).
\end{aligned}$$

Thus $\theta(xyrkm_{\le k}) \le \epsilon \cdot \theta'(xyrkm_{\le k})$. So (here we set $k = k(x, y, r, m)$ in the sum):

$$\begin{aligned}
\theta(S_1) &= \sum_{(x,y,r,m) \in S_1} \theta(xyrm) \\
&= \sum_{(x,y,r,m) \in S_1} \theta(xyrkm_{\le k}) \cdot \theta(m | xyrkm_{\le k}) \\
&\le \epsilon \sum_{(x,y,r,m) \in S_1} \theta'(xyrkm_{\le k}) \cdot \theta(m | xyrkm_{\le k}) \le \epsilon.
\end{aligned}$$

A similar argument proves $\theta(S_2) \le \epsilon$. Thus, by (10), we have that $\theta(k \le \|\theta\|) \le \theta(k' \le \|\theta\|) + \theta(k < k') < 11\epsilon/2 + 2\epsilon = 15\epsilon/2$ as required. □

5 Open Problem: Direct Products for Information Complexity

Both the direct sum result of [BBCR10] and our direct product result rely on methods to compress protocols. So it is natural to ask whether our ability to prove direct product results is limited only by our ability to compress protocols with low information cost. In fact, information cost can be made into a meaningful complexity measure. The *information complexity* of a function f with respect to a distribution μ is the lowest internal information cost attainable by a protocol computing f with respect to μ and error $1/3$ [BR11, Bra12]. It turns out that the amortized communication complexity of f is exactly equal to its information complexity [BR11]. [BW11, KLL^{+}12] showed that many communication lower bound techniques actually give lower bounds on the information complexity.

Given this new complexity measure, we might have hoped that direct sum and direct product theorems holds with respect to it. Indeed [BBCR10] show that an optimal direct sum theorem holds for information complexity. However, a direct product theorem (with small success probability) cannot hold, because of the following counterexample. Let f be a function with information complexity I. Consider the protocol that computes f^n as follows. Let $\epsilon > 0$ be an arbitrary parameter. With probability ϵ, the protocol executes n copies of the optimal protocol for computing f. With probability $1-\epsilon$ the protocol transmits nothing and fails. This protocol computes f^n with probability ϵ, yet its information complexity is at most $\epsilon I n$. For example, setting $\epsilon = 1/n$ shows that even without increasing the information complexity, one can compute f^n with success probability $1/n$.

The following question is still interesting, and may be easier than proving new direct product results for communication complexity:

Open Problem 35. *Is there a universal constant α such that if the information complexity of f with respect to the distribution μ is I, $T \geq 2$, and $T < \alpha I n$, then $\mathsf{suc}(\mu^n, f^n, T) \leq \exp\left(-\alpha\gamma^2 n\right)$?*

A potential avenue of attack on Problem 35 would be to prove an analogue of Theorem 5 for general distributions μ, showing that any protocol that is close to having low internal information cost can be simulated by a protocol with low internal information cost. Thus, one can hope to solve Problem 35 without giving an improved compression scheme for internal information cost.

6 Proofs of the Standard Lemmas

Proof of Lemma 23.

$$\begin{aligned}
\gamma^2 n &\geq \log(1/\pi(W)) \\
&\geq \mathsf{D}\left(\frac{\pi(\overline{x}\overline{y}|W)}{\pi(\overline{x}\overline{y})}\right) && \text{by Lemma 17} \\
&= \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\pi(\overline{x}_{<i}\overline{y}_{<i}|W)}\left[\mathsf{D}\left(\frac{\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i}W)}{\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i})}\right)\right] && \text{by the chain rule}
\end{aligned}$$

Since $\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i}) = \pi(x_i y_i)$, we can write this

$$\begin{aligned}
&= \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\pi(\overline{x}_{<i}\overline{y}_{<i}|W)}\left[\mathsf{D}\left(\frac{\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i}W)}{\pi(x_i y_i)}\right)\right] \\
&\geq \sum_{i=1}^{n} \mathsf{D}\left(\frac{\pi(x_i y_i|W)}{\pi(x_i y_i)}\right). && \text{by Lemma 18}
\end{aligned}$$

The proof is completed by applying Lemma 14. □

Proof of Lemma 24.

$$\begin{aligned}
2\gamma^2 n &\geq \log(1/\pi(W)) + I(XY;M|W) \\
&\geq \mathop{\mathbb{E}}_{\pi(m|W)}\left[\mathsf{D}\left(\frac{\pi(\overline{xy}|mW)}{\pi(\overline{xy})}\right)\right] && \text{by Lemma 17} \\
&= \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\pi(m\overline{x}_{<i}\overline{y}_{<i}|W)}\left[\mathsf{D}\left(\frac{\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i}mW)}{\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i})}\right)\right] && \text{by the chain rule}
\end{aligned}$$

Since $\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i}) = \pi(x_i y_i)$, we can write this

$$\begin{aligned}
&= \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\pi(m\overline{x}_{<i}\overline{y}_{<i}|W)}\left[\mathsf{D}\left(\frac{\pi(x_i y_i|\overline{x}_{<i}\overline{y}_{<i}mW)}{\pi(x_i y_i)}\right)\right] \\
&\geq \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\pi(m|W)}\left[\mathsf{D}\left(\frac{\pi(x_i y_i|mW)}{\pi(x_i y_i)}\right)\right]. && \text{by Lemma 18}
\end{aligned}$$

Thus, by Lemma 14, in expectation over i sampled according to $\eta(i)$, we have $\pi(x_i y_i m|W) \overset{\sqrt{2}\gamma}{\approx} \pi(x_i y_i)\pi(m|W)$. □

Acknowledgements

We thank Penghui Yao for finding an error in an earlier version of this paper. We thank Paul Beame, Ankit Garg, and David Xiao for useful comments.

References

[Abl96] F. Ablayev. Lower bounds for one-way probabilistic communication complexity and their application to space complexity. *Theoretical Computer Science*, 157(2):139–159, 1996.

[BBCR10] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. In *Proceedings of the 2010 ACM International Symposium on Theory of Computing*, pages 67–76, 2010.

[BR11] Mark Braverman and Anup Rao. Information equals amortized communication. In Rafail Ostrovsky, editor, *FOCS*, pages 748–757. IEEE, 2011.

[Bra12] Mark Braverman. Interactive information complexity. In *Proceedings of the 44th symposium on Theory of Computing*, STOC '12, pages 505–524, New York, NY, USA, 2012. ACM.

[BW11] Mark Braverman and Omri Weinstein. A discrepancy lower bound for information complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:164, 2011.

[BYJKS04] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *Journal of Computer and System Sciences*, 68(4):702–732, 2004.

[CSWY01] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew 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. J. Wiley and Sons, New York, 1991.

[FPRU94] Uriel Feige, David Peleg, Prabhakar Raghavan, and Eli Upfal. Computing with noisy information. *SIAM Journal on Computing*, 23(5):1001–1018, 1994.

[Hol07] Thomas Holenstein. Parallel repetition: Simplifications and the no-signaling case. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, 2007.

[JPY12] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A direct product theorem for bounded-round public-coin randomized communication complexity. *CoRR*, abs/1201.1666, 2012.

[JY12] Rahul Jain and Penghui Yao. A strong direct product theorem in terms of the smooth rectangle bound. *CoRR*, abs/1209.0263, 2012.

[Kla10] Hartmut Klauck. A strong direct product theorem for disjointness. In *STOC*, pages 77–86, 2010.

[KLL$^+$12] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:38, 2012.

[LSS08] Troy Lee, Adi Shraibman, and Robert Spalek. A direct product theorem for discrepancy. In *CCC*, pages 71–80, 2008.

[MWY13] Marco Molinaro, David Woodruff, and Grigory Yaroslavtsev. Beating the direct sum theorem in communication complexity with implications for sketching. In *SODA*, page to appear, 2013.

[NW93] Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. *SIAM Journal on Computing*, 22(1):211–219, February 1993.

[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 29th Annual ACM Symposium on the Theory of Computing (STOC '97)*, pages 363–372, New York, May 1997. Association for Computing Machinery.

[Raz92] Razborov. On the distributed complexity of disjointness. *TCS: Theoretical Computer Science*, 106, 1992.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, June 1998. Prelim version in STOC '95.

[Sha48] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27, 1948. Monograph B-1598.

[Sha03] Ronen Shaltiel. Towards proving strong direct product theorems. *Computational Complexity*, 12(1-2):1–22, 2003. Prelim version CCC 2001.

[She11] Alexander A. Sherstov. Strong direct product theorems for quantum communication and query complexity. In *STOC*, pages 41–50, 2011.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing. In *STOC*, pages 209–213, 1979.