The Role of Interaction in Common Randomness and Secret Key Generation

The Role of Interaction in Common Randomness and Secret Key Generation

Noah Golowich

Submitted in partial fulfillment of

the honors requirements

for the degree of Bachelor of Arts with Honors

to the Department of Mathematics

and the Department of Computer Science

Harvard University
Cambridge, Massachusetts
March 25, 2019

Contents

1 Preface **4**
- 1.1 Common randomness and secret key generation . . . 4
- 1.2 Motivation . . . 5

2 Introduction **6**
- 2.1 Notation . . . 7
- 2.2 Common Randomness and Secret Key Generation . . . 8
  - 2.2.1 Communication Protocols . . . 8
  - 2.2.2 Amortized Setting . . . 10
  - 2.2.3 Non-Amortized Setting . . . 11
- 2.3 Limiting behavior of achievable rate regions . . . 12
- 2.4 Some common sources . . . 14
- 2.5 Overview of Main Results . . . 15
  - 2.5.1 Does Interaction Help? . . . 15
  - 2.5.2 Main Results: Analogue of Pointer-Chasing Separations for CRG & SKG . . . 16

3 History **18**
- 3.1 Non-amortized CRG and SKG . . . 18
- 3.2 Single-letter Characterization of Rate Regions for Amortized CRG and SKG . . . 20
- 3.3 Strong Data Processing Constant, Hypercontractivity . . . 24
  - 3.3.1 1-round protocols . . . 24
  - 3.3.2 Multi-round protocols; concave envelopes . . . 25
- 3.4 Proof of the Converse Direction of Theorem 3.4 . . . 26

4 Rounds-Communication Tradeoffs in Non-Amortized Setting **32**
- 4.1 Pointer chasing source . . . 33
- 4.2 Proving indistinguishability of $\mu_{r,n,\ell}$ and $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$ . . . 35
- 4.3 Proof of Theorem 4.10 . . . 41
- 4.4 Proof of Lemma 4.15: Setting up the Induction . . . 42
- 4.5 The Base Case: Proof of Lemma 4.18 . . . 46
- 4.6 The Inductive Step: Proof of Lemma 4.17 . . . 53

5 Rounds-Communication Tradeoffs in Amortized Setting **62**
- 5.1 Using the Compression of Information to Communication . . . 63
- 5.2 Proof of Theorem 5.1 . . . 67
- 5.3 Separations in MIMK, CBIB, and KBIB . . . 68

6 Information Theoretic Lemmas **70**

A Alternate Definitions of Rate Regions **78**
- A.1 Amortized CRG . . . 78
- A.2 Amortized SKG . . . 79
- A.3 Non-amortized CRG . . . 79

Acknowledgements

Part of this thesis (Sections 4.3 to 4.6 in particular) is based off of joint work with Mitali Bafna, Badih Ghazi, and Madhu Sudan, that appeared in the 2019 Symposium on Discrete Algorithms [BGGS19].

I am very grateful to my thesis advisor, Professor Madhu Sudan, for introducing me to a variety of problems in communication complexity, and for numerous enlightening discussions and advice. I would also like to thank Professor Clifford Taubes for being my mathematics advisor on this thesis. I am additionally grateful to Badih Ghazi for insightful discussions about common randomness generation, and to Professor Venkat Anantharam for an insightful conversation on the topic. I would like to thank Professors Salil Vadhan and Les Valiant for being my thesis readers.

I would also like to thank my other advisors throughout my undergraduate experience – Professors David Parkes, Sanjeev Arora, Sasha Rakhlin, and Tomaso Poggio – for their invaluable support, as well as the additional wonderful collaborators I have had the privilege of working with as an undergraduate – Professor Ohad Shamir, Harikrishna Narasimhan, Nadav Cohen, Wei Hu, Mitali Bafna, and Badih Ghazi.

Abstract

In this work we study the problems of common randomness generation (CRG) and secret key generation (SKG). In the CRG problem, two parties, Alice and Bob, receive samples X and Y, respectively, from some joint *source distribution* μ. The two parties wish to agree on a *key* consisting of many bits of randomness, by exchanging messages that depend on each party's respective input and the previous messages. The SKG problem is the same as CRG, except that an eavesdropper who observes the messages must not be able to determine much information about the key. We study the tradeoff between the minimum total length of all messages for a protocol generating a given number of bits of randomness and the minimum possible number of rounds in such a protocol. We construct a source distribution $\mu_{r,n,\ell}$, parametrized by $r, n, \ell \in \mathbb{N}$, achieving such a tradeoff in a strong sense: when Alice and Bob can use $r+2$ rounds of communication and $\ell \geq n$, they can agree on ℓ bits of entropy by communicating only $O(\log n)$ bits, but when they are restricted to r rounds of communication, they require communication of $\Omega(\sqrt{n}/\operatorname{poly}\log n)$ bits to agree on ℓ bits of entropy. We also prove an analogous result for the setting in which Alice and Bob can *amortize*, meaning that they receive N i.i.d. samples of $(X, Y) \sim \mu$, and the communication and key length, respectively, are measured by the ratio of the actual number of bits communicated and the actual key length, respectively, to N.

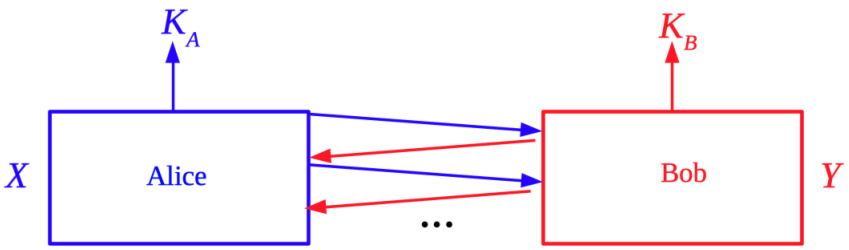

Figure 1: Common randomness generation.

1 Preface

1.1 Common randomness and secret key generation

In this work we study the problems of *common randomness generation* and *secret key generation*, which play a central role in information theory and cryptography. In each of these problems (Figure 1), there are two parties, Alice and Bob, who receive correlated random strings of bits, X and Y. For instance, X may be a string of n uniform and independent bits, and Y may be the string obtained by flipping each bit of X independently with probability $1/3$. (This source distribution is an example of a *binary symmetric source*.) In the problem of common randomness generation, Alice and Bob have a goal of agreeing on a common random string K, also known as a *key*, with high probability. They do so by interacting in several *rounds* of communication: in the first round, Alice sends Bob a string of bits, also called a *message*, that depends on her input X and possibly some random coin flips Alice performs. In each round thereafter, each of Alice and Bob alternates sending the other party a string of bits that depends on his/her input, the previous messages, and possibly some random coin flips. After some number r of rounds, Alice and Bob compute keys $K_{\mathtt{A}}$ and $K_{\mathtt{B}}$, respectively, belonging to some *key set* $\mathcal{K}$. The key $K_{\mathtt{A}}$ ($K_{\mathtt{B}}$, respectively) is a function of Alice's (Bob's, respectively) input and the collection of all messages exchanged. That Alice and Bob *agree on the key* K means that $K_{\mathtt{A}} = K_{\mathtt{B}} = K$ with high probability.

Without further requirements on K, the problem of common randomness generation is trivial (i.e., requires no communication), since Alice and Bob can set K to be a constant and always set $K_{\mathtt{A}} = K_{\mathtt{B}} = K$. In order for K to represent "useful" common randomness, we therefore require that K is distributed uniformly over the set $\mathcal{K}$ of possible keys. The problem of secret key generation is the same as that of common randomness generation, except that there is an additional secrecy requirement on K: an eavesdropper Eve that observes the messages that Alice and Bob exchange in the protocol but not the parties' inputs X, Y can only know a negligible amount of information about K at the conclusion of the protocol.

In this thesis we are concerned primarily with resource-limited common randomness and secret key generation. There are two resources in particular that are very natural to study: (1) the total number of bits Alice and Bob communicate throughout the execution of the protocol, called the *communication cost* of the protocol, and (2) the number of messages Alice and Bob exchange, i.e., the number of *rounds* of the protocol. From a practical perspective there are clear motivations to limit utilization of each of these resources: a communication channel with low bandwidth will take a long time to transmit an excessively long string of bits, whereas high latencies over a network

imply that protocols with large numbers of rounds will take a long time to terminate. The theme of this thesis is the natural question regarding the relationship between the number of rounds and the communication cost of a protocol for common randomness generation:

> *Is there some sort of tradeoff between the minimum number of rounds and the minimum communication cost of a protocol for common randomness generation from a given input distribution* (X, Y)*?*

In the different (though related) setting of *computing functions via communication protocols*, it is well-known [NW93] that the answer to the above question is the affirmative. In particular, there are functions f such that if Alice and Bob wish to compute the value of $f(X, Y) \in \{0, 1\}$, then they can do so by communicating few bits over many rounds, but if they are restricted to a smaller number of rounds, computing the value of $f(X, Y)$ requires communicating many bits.[1] Remarkably, until the work of this thesis, the corresponding problem remained nearly entirely open for common randomness and secret key generation. In fact, some recent work on common randomness and secret key generation [LCV17, Tya13] has exhibited that for many natural distributions over Alice's and Bob's inputs X, Y, including the binary symmetric source mentioned above, there is no such tradeoff: in particular, there is a protocol with the minimum possible amount of communication for generating common randomness that also has only 1 round. *However, our main result is that such a tradeoff does exist in general for the problems of common randomness and secret key generation.* We construct an explicit family of distributions over inputs X, Y that achieves such a tradeoff, and prove that the resulting tradeoff is very strong: the difference in communication cost between the most efficient (i.e., lowest-communication) protocols with many rounds and the most efficient protocols with few rounds is an exponential-sized gap.

1.2 Motivation

One of the principal motivations for studying common randomness generation and secret key generation, and in particular the latter, is in cryptography. A fundamental problem in cryptography is that of developing algorithms for two parties, Alice and Bob, to securely communicate a message when their communication channel can be eavesdropped by an adversary. There are efficient algorithms for the two parties to communicate securely when they can first agree on a *secret key* K that the adversary does not know (which in practice, is usually a string of a few hundred bits). However, agreeing on a secret key in the first place is nontrivial, and is also important in providing authentication, which in turn is necessary when the adversary can tamper with messages Alice and Bob send to each other.

The celebrated Diffie-Hellman key exchange algorithm [DH76] and the RSA public-key cryptosystem [RSA78] have been enormously successful in providing for secure key agreement and authentication over the internet. However, their security rests on unproven computational assumptions. Moreover, it is known [Sho97] that Diffie-Hellman and RSA are insecure against quantum adversaries, which will increasingly become a threat over the next few decades. Therefore, it is useful to study secret key agreement from an information theoretic point of view and to derive results that do not depend on assumptions on the computational power of an adversary. Such was

[1] Notice that a trivial way to compute $f(X, Y)$ is for Alice to send Bob her entire input X, and for Bob, having Y, to then compute $f(X, Y)$ directly. When Alice and Bob are restricted to few rounds, the aforementioned result [NW93] states that this strategy is near-optimal.

the motivation for Maurer [Mau91, Mau92, Mau93] and Ahlswede and Csiszár [AC93] to introduce the framework of (information theoretic) secret key generation we study in this thesis.

Similar ideas to those in [Mau91, Mau92, Mau93, AC93] are also needed to implement quantum key agreement [BBB+92, HAD+95]. In particular, a quantum key agreement protocol between Alice and Bob proceeds via Alice sending Bob a stream of photons encoding a key K. However, the stream Bob receives may be corrupted by channel noise or by an eavesdropper Eve purposefully tampering with some of the photons. Such tampering also may give Eve information about some bits of K. To recover a secret key K' upon which Alice and Bob agree exactly and which Eve knows essentially nothing about, Alice and Bob must communicate over a public channel that Eve can observe. This is exactly the problem considered in [Mau91, Mau92, Mau93, AC93], and indeed, many of the techniques (such as privacy amplification) in those works are also used for quantum key agreement.

Shared randomness also plays a central role in *identification capacity*: typically, if Alice transfers N bits over a noisy channel to Bob, she can encode exponentially many (i.e., 2^{rN}, for a constant r) different messages so that the probability of Bob recovering the correct message is very close to 1. Using common randomness as a resource, Ahlswede and Dueck [AD89b, AD89a] showed the following remarkable result: by transmitting N bits over the channel, Alice can encode *doubly exponentially* many (i.e., $2^{2^{rN}}$, for a constant r) different messages, so that for any *particular* message m, Bob can determine with high probability whether Alice originally transmitted m.

More broadly, common random bits are an extremely valuable resource for communication protocols between two parties, in which each party receives some input and they want to compute some joint function of their inputs by communicating as few bits as possible. In particular, for many such functions, the parties can compute it *exponentially* more efficiently if they can use common random bits as a resource. (See Section 2 for a formal definition of communication complexity.) An interesting question [CGMS17, GKS15, GS17, BGI14] is then how many additional bits must be communicated if the parties only share their randomness *imperfectly* (e.g., if each shared random bit is corrupted with some small probability). If the parties can generate perfectly shared randomness efficiently from the imperfectly shared randomness, then sharing randomness imperfectly (as opposed to perfectly) does not significantly increase the number of bits necessary to communicate. Thus the communication complexity of generating shared randomness becomes central to the question of efficiency of communication in the presence of imperfectly shared randomness [CGMS17].

Common randomness has further applications in locality-sensitive hashing [GJ18] and in coding theory [BBT60, CN91].

2 Introduction

In this section we formally define the problems of *common randomness generation* (CRG) and *secret key generation* (SKG). In particular, we will define the *rate regions* for each of these tasks, which make precise, for a given distribution of the parties' inputs, the relationship between the amount of communication needed to agree on a common random string (or secret key) and the entropy of the key, using a given number of rounds of communication.

2.1 Notation

We first describe some of the basic notational conventions we use throughout the paper. We use capital script font, such as $\mathcal{S}, \mathcal{X}, \mathcal{Y}$, to denote sets, and capital letters, such as X, Y, Z, to denote random variables. We will occasionally have sets that are random variables, and in this case, we will use capital (non-script) leters. We typically use the letters μ, ν, D to denote distributions. If X is distributed according to a distribution μ on a sample space $\mathcal{X}$, then we will write $X \sim \mu$. We use lower case letters to denote specific instantiaions of random variables; e.g., for $x \in \mathcal{X}$, we may write $\mathbb{P}_\mu[X = x]$ to denote the probability that $X = x$ under $X \sim \mu$.

If $\mathcal{E} \subset \mathcal{X}$ is some event, then we will write $\mathbb{1}[X \in \mathcal{E}]$ to denote the random variable that is 1 if $X \in \mathcal{E}$, and 0 otherwise. We will slightly abuse notation, e.g., if $(X, Y) \sim \nu$ then $\mathbb{1}[X = Y]$ is 1 when $X = Y$ and 0 otherwise. If $f : \mathcal{X} \to \mathbb{R}$, then $\mathbb{E}_\mu[f(X)]$ denotes the expectation of $f(X)$ when X is distributed according to μ. For $\mathcal{E} \subset \mathcal{X}$, $\mathbb{P}_\mu[\mathcal{E}] := \mathbb{E}_\mu[\mathbb{1}[X \in \mathcal{E}]]$ is the probability that $X \in \mathcal{E}$ when $X \sim \mu$. This notation extends naturally to conditional expectations: if $(X, Y) \sim \nu$, and $f : \mathcal{X} \to \mathbb{R}$, let X_y be the random variable supported on X distributed as $\mathbb{P}[X_y = x] = \mathbb{P}[X = x, Y = y]/\mathbb{P}[Y = y]$. Then $\mathbb{E}_\nu[f(X)|Y = y] = \mathbb{E}[f(X_y)]$, and $\mathbb{E}_\nu[f(X)|Y] = \mathbb{E}_{Y\sim\nu}[\mathbb{E}_\nu[f(X)|Y = y]]$.

For random variables X, X' distributed according to μ, μ', respectively, on a finite set $\mathcal{X}$, $\Delta(\mu, \mu') := \frac{1}{2}\sum_{x\in\mathcal{X}} |\mathbb{P}_\mu[X = x] - \mathbb{P}_{\mu'}[X' = x]|$ denotes the *total variational distance* between X and x'. It is well-known that $\Delta(\mu, \mu') = \max_{\mathcal{E}\subset\mathcal{X}}(\mathbb{P}_\mu[\mathcal{E}] - \mathbb{P}_{\mu'}[\mathcal{E}])$. The *entropy* of X is denoted by $H(X) := \sum_{x\in\mathcal{X}} \mathbb{P}[X = x] \log(1/\mathbb{P}[X = x])$. The *min-entropy* of X is denoted by $H_\infty(X) := \min_{x\in\mathcal{X}}\{\log(1/\mathbb{P}[X = x])\}$.

Now suppose (X, Y) are random variables with $X \in \mathcal{X}, Y \in \mathcal{Y}$ jointly distributed according to some distribution ν. Recalling our notation X_y from above, then $H(X|Y = y) := H(X_y)$. Then the *conditional entropy* $H(X|Y)$ is given by $H(X|Y) =: \mathbb{E}_{y\sim\nu}[H(X|Y = y)]$. The *mutual information* is given by $I(X; Y) := H(X) - H(X|Y)$; it is well-known that $I(X; Y) = H(Y) - H(Y|X)$. If (X, Y, Z) are jointly distributed according to some distribution, then the *conditional mutual information* $I(X; Y|Z)$ is given by $I(X; Y|Z) := H(X|Z) - H(X|Y, Z)$.

For distributions μ and ν supported on a set $\mathcal{X}$, the *KL divergence* between μ, ν, denoted $\mathrm{KL}(\mu||\nu)$, is defined as follows: for $X \sim \mu, Y \sim \nu$, we have $\mathrm{KL}(\mu||\nu) := \sum_{x\in\mathcal{X}} \mathbb{P}[X = x] \cdot \log\left(\frac{\mathbb{P}[X=x]}{\mathbb{P}[Y=x]}\right)$. For random variables $(X, Y) \sim \mu$ distributed jointly, with $X \in \mathcal{X}, Y \in \mathcal{Y}$, we will often write $XY \in \mathcal{X} \times \mathcal{Y}$ to denote the pair. The *marginals* $X \sim \mu_X, Y \sim \mu_Y$ are the distributions on $\mathcal{X}$ and $\mathcal{Y}$ respectively, given by $\mathbb{P}_{X\sim\mu_X}[X = x] := \mathbb{P}_{XY\sim\mu}[X = x]$, and similarly for μ_Y. Then $X \otimes Y \in \mathcal{X} \times \mathcal{Y}$ denotes the random variable distributed according to the product of the marginals $\mu_X \otimes \mu_Y$. It is well known that for $(X, Y) \sim \mu$, we have $I(X; Y) = \mathrm{KL}(\mu||\mu_X \otimes \mu_Y)$. We will often abuse notation when denoting KL divergences or total variation distances: for $X \sim \mu, Y \sim \nu$ supported on a set $\mathcal{X}$, we will write $\Delta(X, Y) = \Delta(\mu, \nu)$ and $\mathrm{KL}(X||Y) = \mathrm{KL}(\mu||\nu)$.

For a sequence of random variables $X_1, X_2, \ldots, X_i, \ldots$, for any $j \geq 1$, we let X^j denote the tuple $(X_1, \ldots, X_j)$, and for $1 \leq j \leq j'$, let $X_j^{j'}$ denote the tuple $(X_j, X_{j+1}, \ldots, X_{j'})$. One common usage of this notation is as follows: for $N \in \mathbb{N}$, and a distribution $Z \sim \mu$, the random variable distributed according to N i.i.d. copies of μ is denoted as $Z^N = (Z_1, \ldots, Z_N)$.

We say that jointly distributed random variables X, Y, Z form a *Markov chain* if $X \perp Z|Y$ (i.e., if X and Z are conditionally independent given Y). We will write this condition as $X - Y - Z$.

We denote by $\{0, 1\}^* = \cup_{n\in\mathbb{N}}\{0, 1\}^n$ the set of all strings of bits. For a string $x \in \{0, 1\}^*$, we denote by $|x| \in \mathbb{N}$ the *length* of x, i.e., the unique n such that $x \in \{0, 1\}^n$.

For jointly distributed random variables X, Y such that X is a deterministic function of Y, we

will often denote this deterministic function by X, i.e., $X = X(Y)$. To reduce clutter in notation, for random variables X, Y that are jointly distributed, we will often abbreviate the tuple (X, Y) as XY. For a positive integer r, let $[r] = \{1, 2, \ldots, r\}$. Let $\mathcal{O}^r$ denote the odd integers in $[r]$ and $\mathcal{E}^r$ denote the even integers in $[r]$. Let $\mathcal{S}_n$ denote the set of all permutations on $[n]$.

2.2 Common Randomness and Secret Key Generation

We now formally introduce the problems of common randomness and secret key generation. We first introduce *interactive communication protocols*, which were first studied by Yao [Yao79].

2.2.1 Communication Protocols

There are two parties, Alice and Bob, and finite sets $\mathcal{X}, \mathcal{Y}$. Alice receives an element $X \in \mathcal{X}$, and Bob receives an element $Y \in \mathcal{Y}$. The pair (X, Y) is referred to as the *input* of the protocol. We will usually assume that (X, Y) are random variables distributed jointly on $\mathcal{X} \times \mathcal{Y}$ according to some distribution μ. In the setting of common randomness or secret key generation, μ is called the *source (distribution)*.

Depending on the setting, Alice and Bob may additionally have access to private coins $R_{\mathtt{A}}, R_{\mathtt{B}}$, respectively, and public coins $R_{\mathtt{Pub}}$. Formally, $R_{\mathtt{A}}, R_{\mathtt{B}}, R_{\mathtt{Pub}}$ may be interpreted as infinite strings of independently and uniformly distributed random bits. Alice can see $R_{\mathtt{A}}, R_{\mathtt{Pub}}$ (if they are available), while Bob can see $R_{\mathtt{B}}, R_{\mathtt{Pub}}$ (if they are available). A protocol in which Alice and Bob have access to the public coins $R_{\mathtt{Pub}}$ is known as a *public-coin* protocol, and a protocol in which Alice and Bob have access to the private coins $R_{\mathtt{A}}, R_{\mathtt{B}}$, respectively, but not to $R_{\mathtt{Pub}}$, is known as a *private-coin* protocol. Finally, a protocol in which Alice and Bob do not have access to any of $R_{\mathtt{A}}, R_{\mathtt{B}}, R_{\mathtt{Pub}}$ is known as a *deterministic protocol*.

An *interactive r-round protocol* Π consists of a sequence of r *messages*, $\Pi_1, \ldots, \Pi_r \in \{0,1\}^*$ (i.e., each message is a finite string of bits). The messages $\Pi_1, \ldots, \Pi_r$ are also referred to as the *rounds* of the protocol, and each message is a deterministic function of the previous messages, one party's input, and any randomness (public and/or private) available to that party; in other words, each message is a randomized function of the previous messages and one party's input. We assume that Alice always starts by sending the message Π_1 to Bob, where $\Pi_1 = \Pi_1(X, R_{\mathtt{A}}, R_{\mathtt{Pub}})$, meaning that Π_1 is a deterministic function of $X, R_{\mathtt{A}}, R_{\mathtt{Pub}}$. (If the protocol is only allowed to use private coins, then $\Pi_1 = \Pi_1(X, R_{\mathtt{A}})$, and if it is not allowed to use either public or private coins then $\Pi_1 = \Pi_1(X)$.) Bob responds with the message $\Pi_2 = \Pi_2(Y, R_{\mathtt{B}}, R_{\mathtt{Pub}}, \Pi_1)$, with analogous modifications if the protocol is not allowed to use public or private coins. In general, for $1 \le t \le r$, recalling our notation $\Pi^t := (\Pi_1, \ldots, \Pi_t)$, the t-th message Π_t is given by

$$\Pi_t = \Pi_t(X, R_{\mathtt{A}}, R_{\mathtt{Pub}}, \Pi^{t-1})$$

if t is odd and

$$\Pi_t = \Pi_t(Y, R_{\mathtt{B}}, R_{\mathtt{Pub}}, \Pi^{t-1})$$

if t is even (with the obvious modifications if the randomness used by the protocol is restricted). Moreover, for each t and each instantiation of Π^{t-1}, the set of possible values of Π_t (over all possible instantiations of $X, Y, R_{\mathtt{A}}, R_{\mathtt{B}}, R_{\mathtt{Pub}}$) must be prefix-free.[2] The *communication cost* of Π,

[2]This technical condition is required so that Alice or Bob knows when to "start speaking" when the other player finishes sending his or her previous message.

denoted by $\mathrm{CC}(\Pi)$, is the maximum of $\sum_{t=1}^{r} |\Pi_t|$, taken over all inputs $X \in \mathcal{X}, Y \in \mathcal{Y}$, and all settings of the random coins $R_{\mathtt{A}}, R_{\mathtt{B}}, R_{\mathtt{Pub}}$ (if applicable). In other words, the communication cost is the maximum number of bits that Alice and Bob will communicate when executing Π. The tuple consisting of all the messages, i.e., $\Pi^r = (\Pi_1, \ldots, \Pi_r)$, is referred to as the *transcript* of the protocol Π. In general, protocols Π need not have a constant number of rounds (i.e., the number of rounds may depend on the inputs and values of the public and private randomness). In such a case, we refer to the number of rounds r of Π as the maximum number of messages Π_t sent over all instiations of $X, Y, R_{\mathtt{A}}, R_{\mathtt{B}}, R_{\mathtt{Pub}}$ (we will also say that Π *has a maximum of* r *rounds*). If, for certain instantiations of $X, Y, R_{\mathtt{A}}, R_{\mathtt{B}}, R_{\mathtt{Pub}}$, Alice and Bob only communicate r' messages $\Pi_1, \ldots, \Pi_{r'}$ in an r-round protocol, with $r > r'$, we consider $\Pi_t = \emptyset$ for $r' + 1 \leq t \leq r$. We will often use the following basic facts (Propositions 2.1 and 2.2) about the structure of r-round protocols:

Proposition 2.1. *Suppose* $(X, Y) \sim \mu$*, and that* $\Pi_1, \ldots, \Pi_r$ *are random variables distributed on finite sets. Then* $\Pi_1, \ldots, \Pi_r$ *are the random variables representing the messages in some* r*-round communication protocol* $\Pi = (\Pi_1, \ldots, \Pi_r)$ *if and only if the following Markov conditions hold:*

$$\Pi_t - X\Pi^{t-1} - Y, \ t \in \mathcal{O}^r \qquad X - Y\Pi^{t-1} - \Pi_t, \ t \in \mathcal{E}^r.$$

In such a case, we will call Π *the communication protocol induced by the random variables* $\Pi_1, \ldots, \Pi_r$*.*

The Markov condition $\Pi_t - X\Pi^{t-1} - Y$ means that Π_t is a randomized function of $X\Pi^{t-1}$. The proof of the "if" direction of the above proposition proceeds by having Alice use her random bits $R_{\mathtt{A}}$ to implement this randomized function of X, Π^{t-1} (and similarly for Bob). The "only if" direction follows immediately from the definitions.

Proposition 2.2 (Moniticity of correlation [STW19])**.** *If* $\Pi = (\Pi_1, \ldots, \Pi_r)$ *is a communication protocol with inputs* $(X, Y) \sim \mu$*, then*

$$I_\mu(X; Y | \Pi^r) \leq I_\mu(X; Y).$$

In particular, if X, Y are independent, then they remain so after conditioning on the transcript of any protocol.

Typically [KN97] communication protocols are introduced in the context of computing functions. In particular, for a function $f : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$, we say that a deterministic protocol Π (i.e., one with no private or public random bits) as above *computes* f if for all $X \in \mathcal{X}, Y \in \mathcal{Y}$, the last bit of the transcript of Π equals $f(X, Y)$. The *deterministic communication complexity* of a function f, denoted $\mathrm{D}(f)$, is the minimum of $\mathrm{CC}(\Pi)$ over all protocols Π that compute f. A randomized protocol Π (i.e., one with private and/or public random bits) *computes* f *with probability* $1 - \epsilon$ if for all $X \in \mathcal{X}, Y \in \mathcal{Y}$, the probability (over the random bits) that the last bit of the transcript equals $f(X, Y)$ is at least $1 - \epsilon$. The *private-coin randomized communication complexity* of a function f, denoted $\mathrm{R}_\epsilon(f)$, for $\epsilon \in (0, 1)$, is the minimum of $\mathrm{CC}(\Pi)$ over all private-coin protocols Π that compute f with probability $1 - \epsilon$. The *public-coin randomized communication compelxity* of f, denoted $\mathrm{R}^{\mathrm{pub}}_\epsilon(f)$, is defined similarly except the protocols Π are also allowed to use public coins. Newman's theorem [KN97] states for all $f, \epsilon > 0, \delta > 0$, $\mathrm{R}_{\epsilon+\delta}(f) \leq \mathrm{R}^{\mathrm{pub}}_\epsilon(f) + O(\log n/\delta)$.

Finally, if μ is a distribution on $\mathcal{X} \times \mathcal{Y}$ and $\epsilon \in (0, 1)$, then the *distributional communication complexity* of f over μ, denoted $\mathrm{D}_{\mu,\epsilon}(f)$, is the minimum of $\mathrm{CC}(\Pi)$ over all protocols that compute f with probability at least $1 - \epsilon$, where the probability is additionally over $(X, Y) \sim \mu$. It is easy to see by an averaging argument that it is in fact sufficient to consider only deterministic

protocols when computing $\mathrm{D}_{\mu,\epsilon}(f)$. It follows from the von Neumann minimax theorem [KN97] that $\sup_\mu \mathrm{D}_{\mu,\epsilon}(f) = \mathrm{R}_\epsilon(f)$, where the supremum is over all distributions μ on $\mathcal{X} \times \mathcal{Y}$.

Although protocols for computing functions will show up in our proofs, our main focus will be on protocols that perform the tasks of common randomness generation and secret key generation. Roughly speaking, there are two settings of common randomness and secret key generation to consider: the *amortized* setting and the *non-amortized* setting. In both settings, we do not allow the parties access to public randomness, so the protocols will be private-coin or deterministic protocols; notice that if the parties had access to public randomness, then there would be no need to generate a shared common string.

2.2.2 Amortized Setting

We begin by describing the amortized setting, which was introduced independently by Maurer [Mau91, Mau92, Mau93] and by Ahlswede and Csiszár [AC93, AC98] and has since received much attention in the information theory community [GK73, Wyn75, CN00, CN04, ZC11, Tya13, LCV15, Liu16, LCV17, Ye05, GA10a, GA10b]. In amortized CRG, Alice and Bob receive some large number N of copies (X, Y) from the source, are allowed to communicate some number of bits that grows linearly with N, and must agree upon a key whose entropy grows linearly with N with probability tending to 1 as $N \to \infty$. The word "amortized" refers to the fact that the communication and key entropy both grow linearly with N. There are two different ways [AC98, LCV17, GJ18] to precisely define achievable rates for amortized CRG. Definition 2.1 follows the exposition of [LCV17]; an alternative definition, which turns out to be equivalent, can be found in [AC98, GJ18], and is also presented in Appendix A.

Definition 2.1 (Amortized common randomness generation (CRG))**.** We say that a tuple (C, L) is *r-achievable for CRG* for a source distribution $(X, Y) \sim \nu$ if for every $N \in \mathbb{N}$, there is some ϵ_N with $\epsilon_N \to 0$ as $N \to \infty$, a key set $\mathcal{K}_N$, and a private-coin protocol[3] $\Pi = \Pi(N)$ that takes as input $(X^N, Y^N) \sim \nu^{\otimes N}$, such that if $\Pi(N)_t \in \{0,1\}^*$ denotes the message sent in the t-th round of $\Pi(N)$, $1 \le t \le r$, and $K_{\mathtt{A}} = K_{\mathtt{A}}(N), K_{\mathtt{B}} = K_{\mathtt{B}}(N) \in \mathcal{K}_N$ denote the output keys of Alice and Bob for the protocol $\Pi(N)$, then:

1. $\limsup_{N\to\infty} \frac{1}{N} \cdot \mathrm{CC}(\Pi(N)) \le C$.
2. $\liminf_{N\to\infty} \frac{1}{N} \log |\mathcal{K}_N| \ge L$.
3. Letting K_N be the random variable that is uniformly distributed on $\mathcal{K}_N$, then
$$\Delta((K_{\mathtt{A}}(N)K_{\mathtt{B}}(N)), (K_N K_N)) \le \epsilon_N.$$
In particular, there exists a coupling of $K_{\mathtt{A}}(N)K_{\mathtt{B}}(N)$ with $K_N K_N$ such that $\mathbb{P}[K_{\mathtt{A}}(N) = K_{\mathtt{B}}(N) = K_N] \ge 1 - \epsilon_N \to 1$ as $N \to \infty$. (To be clear, $K_N K_N$ denotes the tuple (K_N, K_N) which is distributed uniformly on the set $\{(k,k) : k \in \mathcal{K}_N\}$.)

We denote the subset of pairs $(C, L) \subset \mathbb{R}^2_{\ge 0}$ that are r-achievable from the source $(X, Y) \sim \nu$ by $\mathcal{T}_r(X, Y)$; this set $\mathcal{T}_r(X, Y)$ is known as the *achievable rate region for r-round CRG* (or simply *rate region*, with r and the task of CRG implicit) for the source μ. Notice that C *denotes the communication of the protocols* $\Pi = \Pi(N)$*, whereas* L *denotes the entropy of the key produced (approximately).*

[3] That is, Π can use private *but not public* coins.

Corresponding to Definition 2.1 for CRG we have the following Definition 2.2 for SKG in the amortized setting:

Definition 2.2 (Amortized SKG)**.** A tuple (C, L) is *r-achievable for SKG* for a distribution ν if there is some choice of a sequence $\epsilon_N \to 0$ such that the following holds: for each $N \in \mathbb{N}$ there is some choice of private coin protocol[4] $\Pi = \Pi(N)$ such that, first, conditions (1) – (4) of Definition 2.1 are satisfied for these $\epsilon_N, \Pi(N), N$, and, second,

$$\Delta(K_{\mathtt{A}}(N)K_{\mathtt{B}}(N)\Pi(N)^r, K_{\mathtt{A}}(N)K_{\mathtt{B}}(N) \otimes \Pi(N)^r) \leq \epsilon_N. \tag{1}$$

We denote the set of pairs (C, L) that are r-achievable for SKG from ν by $\mathcal{S}_r(X, Y)$.

It is clear from the definition that r-achievability for SKG is a stronger requirement than r-achievability for CRG; that is, for every source $(X, Y) \sim \nu$, we have $\mathcal{S}_r(X, Y) \subset \mathcal{T}_r(X, Y)$. It is also well-known [LCV17, Han03] that both $\mathcal{T}_r(X, Y)$ and $\mathcal{S}_r(X, Y)$ are closed.

In Definition 2.2 we require an upper bound of ϵ on the total variational distance between $K_{\mathtt{A}}K_{\mathtt{B}}\Pi(N)^r$ and the product distribution $K_{\mathtt{A}}K_{\mathtt{B}} \otimes \Pi(N)^r$ when the key is independent of the transcript. This choice is known as *strong security*, which is commonly used today in applications to cryptography [STW19]. Notice that it does not make sense to have the upper bound depend on N (i.e., as in $N\epsilon$) since variational distance is always bounded above by 1 and N can grow arbitrarily large. In the past *weak security* (e.g., [AC93], Equation (2.5)), in which (1) is replaced by the rquirement that $I(K_{\mathtt{A}}K_{\mathtt{B}}; \Pi(N)^r) \leq N\epsilon$, which a priori is weaker than (1). However, in our setting (and many others) these two notions of strong and weak security turn out to be equivalent (i.e., lead to equivalent rate regions) [MW00, MW99].

2.2.3 Non-Amortized Setting

The non-amortized setting is similar to the amortized setting, in that Alice and Bob receive arbitrarily many i.i.d. samples of $(X, Y) \sim \mu$, except the entropy of their key and their communication no longer grow linearly with the number of samples. In fact, the keys lie in some fixed set $\mathcal{K}$, and the goal is to use as little communication (and rounds) as possible to generate a single key uniformly distributed in $\mathcal{K}$. Moreover, whereas the agreement probability $1 - \epsilon_N$ in the amortized case was assumed to approach 1 asymptotically, in the non-amortized case, it is often of interest to study settings in which the parties may disagree with some probability that is bounded away from 0. In fact, this probability of disagreement may be arbitrarily close to 1. The non-amortized setting has recently received much attention among the theoretical computer science community [BM11, CGMS17, GR16, GJ18, BGGS19], where it is also known as the *agreement distillation problem*.

In the below definition we assume that $(X, Y) \sim \nu$ and ν is supported on a set $\mathcal{X} \times \mathcal{Y}$.

Definition 2.3 (Non-amortized common randomness generation)**.** For $r, C \in \mathbb{N}$, and $L, \epsilon \in \mathbb{R}_{\geq 0}$, we say that *the tuple (C, L, ϵ) is r-achievable from the source ν (for CRG)* if there is some $N \in \mathbb{N}$ and an r-round protocol Π with private randomness that takes as input $(X^N, Y^N) \sim \nu^{\otimes N}$, such that at the end of Π, Alice and Bob output keys $K_{\mathtt{A}}, K_{\mathtt{B}} \in \mathcal{K}$ given by deterministic functions $K_{\mathtt{A}} = K_{\mathtt{A}}(X^N, R_{\mathtt{A}}, \Pi^r)$, $K_{\mathtt{B}} = K_{\mathtt{B}}(Y^N, R_{\mathtt{B}}, \Pi^r)$, such that:

1. $\mathrm{CC}(\Pi) \leq C$.

[4] As for CRG, the protocol Π cannot use public coins.

2. $|\mathcal{K}| \geq 2^L$.

3. There is a random variable K uniformly distributed on $\mathcal{K}$ such that $\mathbb{P}_\nu[K = K_{\mathtt{A}} = K_{\mathtt{B}}] \geq 1-\epsilon$.

As in the amortized case, for tuples (C, L, ϵ), observe that C denotes communication and L denotes entropy.

Definition 2.3 differs slightly from the definition of achievable rates for non-amortized CRG in [BM11, CGMS17, GR16, GJ18, BGGS19], which do not limit the size of the key space $\mathcal{K}$, but rather require a lower bound on the min-entropy of each of $K_{\mathtt{A}}, K_{\mathtt{B}}$. We present this latter definition in Appendix A (Definition A.3) and show that it is essentially equivalent to Definition 2.3.

As in the amortized setting, in the non-amortized setting secret key generation is the same as common randomness generation except the key is additionally required to be "almost independent" from the transcript of the protocol:

Definition 2.4 (Non-amortized secret key generation)**.** For $r, C \in \mathbb{N}$ and $L \in \mathbb{R}_{\geq 0}$, $\epsilon, \delta \in [0, 1)$, we say that *the tuple (C, L, ϵ, δ) is r-achievable from the source ν (for SKG)* if the tuple (C, L, ϵ) is r-achievable for CRG from the source ν, and if there exists a protocol $\Pi = (\Pi^1, \ldots, \Pi^r)$ achieving the tuple such that

$$I(\Pi^r; K_{\mathtt{A}} K_{\mathtt{B}}) \leq \delta. \tag{2}$$

Notice that condition (2) is quite strong: it implies, for instance, that $\Delta(\Pi^r K_{\mathtt{A}} K_{\mathtt{B}}, \Pi^r \otimes K_{\mathtt{A}} K_{\mathtt{B}}) \leq \sqrt{\delta/2}$, by Pinsker's inequality.

2.3 Limiting behavior of achievable rate regions

The requirement for amortized CRG that both the communication of the protocol and the entropy of the key grow linearly with the number of samples N may seem somewhat restrictive. Therefore, one may try to relax this condition; the correct way to do so turns out to be to focus on the ratio of the entropy of the key, $\log |\mathcal{K}|$, and the communication of Π:

Definition 2.5 (Common random bits per r-round interaction bit (r-round CBIB))**.** Consider a source $(X, Y) \sim \mu$. For $\epsilon \in [0, 1]$, the *ϵ-common randomness per bit of r-round communication*, $\Gamma^{\mathtt{cr}}_{r,\epsilon}(X, Y)$, is the maximum real number $\Gamma \geq 0$ such that there is a sequence $\epsilon_N \to 0$, of key sets $\mathcal{K}_N$, and of r-round protocols $\Pi = \Pi(N) = (\Pi(N)_1, \ldots, \Pi(N)_r)$ that take as inputs $(X^N, Y^N) \sim \mu^{\otimes N}$, such that the following conditions are satisfied:

1. $\liminf_{N\to\infty} \frac{\log |\mathcal{K}_N|}{\mathrm{CC}(\Pi(N))} \geq \Gamma$.

2. $\lim_{N\to\infty} \log |\mathcal{K}_N| = \infty$.

3. If K_N denotes the random variable that is uniformly distributed on $\mathcal{K}_N$, then

$$\Delta(K_{\mathtt{A}}(N) K_{\mathtt{B}}(N), K_N K_N) \leq \epsilon.$$

The *common random bits per r-round interaction bit (CBIB)* is then defined as:

$$\Gamma^{\mathtt{cr}}_r(X, Y) := \inf_{\epsilon > 0} \Gamma^{\mathtt{cr}}_{r,\epsilon}(X, Y).$$

Definition 2.6 (Secret key bits per r-round interaction bit (r-round KBIB)). For $\epsilon \in [0,1]$, the *ϵ-secret key per bit of r-round communication*, $\Gamma^{\mathtt{sk}}_{r,\epsilon}(X,Y)$ is defined identically to $\Gamma^{\mathtt{cr}}_{r,\epsilon}(X,Y)$ in Definition 2.5 except that item (3) is replaced with the requirement that

$$\Delta(K_{\mathtt{A}}(N)K_{\mathtt{B}}(N)\Pi(N)^r, K_{\mathtt{A}}(N)K_{\mathtt{B}}(N) \otimes \Pi(N)^r) \leq \epsilon.$$

Then the *secret key bits per r-round interaction bit (KBIB)* is defined as:

$$\Gamma^{\mathtt{sk}}_r(X,Y) := \inf_{\epsilon>0} \Gamma^{\mathtt{sk}}_{r,\epsilon}(X,Y).$$

Intuitively, the r-round CBIB (KBIB, respectively) can be roughly interpreted as the maximum number of additional bits of common randomness (secret key, respectively) that Alice and Bob can obtain by communicating an additional bit, where the maximum is over "all protocols and any communication rate".

For a given source $(X,Y) \sim \mu$, the r-round CBIB and KBIB can be determined from the achievable rate regions $\mathcal{T}(X,Y)$ and $\mathcal{S}(X,Y)$, respectively:

Theorem 2.3 ([LCV17], Corollary 2). *For a source $(X,Y) \sim \mu$ and $r \in \mathbb{N}$, we have:*

$$\Gamma^{cr}_r(X,Y) = \sup\left\{\frac{L}{C} : (C,L) \in \mathcal{T}_r(X,Y), C > 0\right\}$$

and

$$\Gamma^{sk}_r(X,Y) = \sup\left\{\frac{L}{C} : (C,L) \in \mathcal{S}_r(X,Y), C > 0\right\}.$$

Moreover, whenever $\Gamma^{sk}_r(X,Y)$ or $\Gamma^{cr}_r(X,Y)$ is finite, we have $\Gamma^{cr}_r(X,Y) = 1 + \Gamma^{sk}_r(X,Y)$.

Notice that $\Gamma^{\mathtt{cr}}_r(X,Y)$ and $\Gamma^{\mathtt{sk}}_r(X,Y)$ can be infinite, if, for instance, there are functions $f_{\mathtt{A}} : \mathcal{X} \to \{0,1\}$ and $f_{\mathtt{B}} : \mathcal{Y} \to \{0,1\}$ such that $\mathbb{P}_\mu[f_{\mathtt{A}}(X) = f_{\mathtt{B}}(Y)] = 1$ and $H(f_{\mathtt{A}}(X)) = H(f_{\mathtt{B}}(Y)) > 0$. In such a case, Alice and Bob can generate infinitely many bits of entropy with perfect agreement and 0 communication by setting their keys to be $(f_{\mathtt{A}}(X_1), \ldots, f_{\mathtt{A}}(X_N)) = (f_{\mathtt{B}}(Y_1), \ldots, f_{\mathtt{B}}(Y_N))$, for any $N \in \mathbb{N}$.

Remark 2.7. It follows from Theorem 2.3 and Lemma 3.13 that $\Gamma^{\mathtt{cr}}_r(X,Y)$ is the derivative of the function $C \mapsto \sup_{L:(C,L)\in\mathcal{T}_r(X,Y)}\{L\}$ at $C = 0$.

The r-round CBIB and KBIB describe the maximum possible achievable rates if samples $(X,Y) \sim \mu$ are abundant and communication is restricted: in particular, by maximizing the ratio $\frac{\log|\mathcal{K}_N|}{\mathrm{CC}(\Pi(N))}$, as in Definition 2.5, we only focus on the "part of the input (X,Y)" that yields the maximum key rate per bit of communication. For instance, consider the source (X,Y), where $X = (X_0, X_1) \in \{0,1\}^2, Y = (Y_0, Y_1) \in \{0,1\}^2$ are each two bits, the marginals of X, Y are uniform in $\{0,1\}^2$, (X_0, Y_0) and (X_1, Y_1) are independent, and the following hold:

$$\mathbb{P}[X_0 = Y_0] = 1, \quad \mathbb{P}[X_1 = Y_1] = 2/3.$$

By the observation following Theorem 2.3, $\Gamma^{\mathtt{cr}}_1(X,Y)$ is infinite, as Alice and Bob can set their keys to be $X_0^N = Y_0^N$ given N i.i.d. samples (X^N, Y^N). However, doing so does not "squeeze all possible common randomness" out of the samples: in particular, the second bits of each pair, (X_1, Y_1), are still correlated, though it requires some communication in order to distill keys from these bits which

are equal with probability tending to 1. The ratio of additional key length to communication in such a distillation procedure is certainly less than $\infty = \Gamma_1^{\mathtt{cr}}(X, Y)$.

One can then ask what occurs for the opposite setting, in which samples $(X, Y) \sim \mu$ are not so abundant and communication is not as restricted. The following classical result states that if communication is not restricted at all, then the maximum key length per sample $(X, Y) \sim \mu$ is exactly given by $I(X; Y)$:

Theorem 2.4 ([AC93])**.** *If $(X, Y) \sim \mu$, then*

$$\sup_{(C,L)\in\mathcal{S}_r(X,Y)} \{L\} = I(X; Y).$$

Even if we care about maximizing the key rate L more than minimizing communication C, it is natural, as a second-order concern, to avoid "wasting" communication: we may want to determine the *minimum communication C achieving the maximum key rate $L = I(X; Y)$*. Formally, we define:

Definition 2.8. Suppose $(X, Y) \sim \mu$ is a source and $r \geq 1$. Then define the *minimum r-round interactive rate for achieving the maximum key rate* (i.e., the *r-round MIMK*) by

$$\mathscr{I}_r(X; Y) := \inf_{(C,I(X;Y))\in\mathcal{S}_r(X,Y)} \{C\}.$$

2.4 Some common sources

In this brief section we introduce some source distributions that will be mentioned in passing at later points.

Definition 2.9 (Binary symmetric source)**.** For a parameter $p \in [0, 1]$, the *binary symmetric source* BSS_p is the distribution over bits $X, Y \in \{0, 1\}$ defined by:

$$\mathbb{P}_{\mathrm{BSS}_p}[X = 0, Y = 0] = \mathbb{P}_{\mathrm{BSS}_p}[X = 1, Y = 1] = (1 - p)/2,$$

and

$$\mathbb{P}_{\mathrm{BSS}_p}[X = 0, Y = 1] = \mathbb{P}_{\mathrm{BSS}_p}[X = 1, Y = 0] = p/2.$$

Definition 2.10 (Binary gaussian source)**.** For a parameter $\rho \in [-1, 1]$, the *binary gaussian source* BGS_ρ is the distribution over real numbers $X, Y \in \mathbb{R}$ such that the marginal of each of X, Y is a standard gaussian and $\mathbb{E}_{\mathrm{BGS}_\rho}[XY] = \rho$.

Definition 2.11 (Binary erasure source)**.** For a pararmeter $p \in [0, 1]$, the *binary erasure source* BES_p is the distribution over elements $X, Y \in \{0, 1, ?\}$ defined by:

$$\mathbb{P}_{\mathrm{BES}_p}[X = 0, Y = 0] = \mathbb{P}_{\mathrm{BES}_p}[X = 1, Y = 1] = (1 - p)/2,$$

and

$$\mathbb{P}_{\mathrm{BES}_p}[X = 0, Y =?] = \mathbb{P}_{\mathrm{BES}_p}[X = 1, Y =?] = p/2.$$

Compare the binary erasure source, in which Bob always knows if the bit Y is corrupted (i.e., not equal to the bit X), to the binary symmetric source, in which Bob does not know if this is the case.

2.5 Overview of Main Results

2.5.1 Does Interaction Help?

Curiously, for many of the distributions under which CRG and SKG has been studied, including the binary symmetric source (BSS) and the binary Gaussian source (BGS), the "optimal" protocols turn out to have only a single round of communication. We stress that optimality, with respect to a certain measure of efficiency of communication (such as CBIB), holds over *all* protocols, i.e., those with arbitrarily many rounds. For instance, in the amortized setting, [LCV17] showed that the r-round CBIB and the r-round KBIB (Definitions 2.5 and 2.6) are equal to the 1-round CBIB and 1-round KBIB, respectively, when (X, Y) are distributed according to the binary symmetric source BSS_p with any parameter $p \in (0, 1)$, or the binary gaussian source BGS_ρ for any correlation $\rho \in [-1, 1]$.

Moreover, [Tya13] showed that for any binary symmetric source BSS_p, the r-round MIMK does not depend on r, the number of rounds. In other words, there is a 1-round protocol that achieves the minimum communication cost for generating a key of rate $I_{\mathrm{BSS}_p}(X;Y) = (1-2p)^2$, *where the minimum is taken over protocols with arbitrarily many rounds.* Notice how Theorem 2.3 and Definition 2.8 present the r-round CBIB, KBIB, and MIMK as certain geometric properties of the rate regions $\mathcal{S}_r(X, Y)$ and $\mathcal{T}_r(X, Y)$. The following stronger result regarding BSS_p has been conjectured [LCV17, Conjecture 1]: for any $r \geq 1$, $p \in [0, 1]$, when $(X, Y) \sim \mathrm{BSS}_p$ for any p, $\mathcal{S}_1(X, Y) = \mathcal{S}_r(X, Y)$. That is, increasing the number of rounds of interaction does not increase the size of the rate region at all for the binary symmetric source.

The story for non-amortized CRG is similar. (We remark that work in the non-amortized setting has mostly focused on CRG as opposed to SKG). [GR16] showed that for any $p \in [0, 1]$, and $\mu = \mathrm{BSS}_p$ or $\mu = \mathrm{BES}_p$, for a given disagreement probability $1 - \epsilon$ and communication C, the maximum L such that (C, L, ϵ) is r-achievable does not depend on the number of rounds r (up to lower order terms).[5] This result builds on earlier work of [CGMS17], which proved similar, but looser bounds.

The results mentioned above naturally point to the following question, which is the main focus of this thesis:

Question 2.12 (Informal)**.** Are there some distributions μ for which additional interaction (i.e., rounds) *does* help? More precisely:

(1) For a given communication rate C (and error rate ϵ, in the non-amortized setting), can the maximum achievable rate L (i.e., the entropy) of a common random string or secret key increase if we allow Alice and Bob to use additional rounds of communication?

(2) In particular, in the amortized setting, can having additional rounds of communication lead to a strictly larger CBIB or KBIB, or a strictly smaller MIMK? (Notice that MIMK is measured as a minimum amount of *communication* of a protocol achieving the maximum key rate, hence it will only decrease if we increase the number of allowed rounds.)

(3) Moreover, if any of the above questions have answers in the affirmative, then by how much can the relevant quantity increase or decrease as we increase the number of rounds?

[5] We remark that this result only holds for a somewhat restricted class of protocols, namely those in which Alice's key depends only on her input, while Bob's key can depend on an r-round transcript between Alice and Bob.

Very little was known about Question 2.12 prior to our work. Tyagi [Tya13] constructed a source for which the 2-round MIMK is smaller than the 1-round MIMK by a (small) constant factor. Orlitsky [Orl90, Orl91] studied a slightly different version of CRG in which the key K is required to be equal to Alice's input X; thus the problem becomes that of Bob learning Alice's input. Orlitsky showed that 2-round protocols can require exponentially less communication than 1-round protocols. However, for any $r > 2$, r-round protocols can save on communication cost over 2-round protocols by at most a factor of 4.

2.5.2 Main Results: Analogue of Pointer-Chasing Separations for CRG & SKG

The main results presented in this thesis include those in the SODA 2019 paper co-authored by the author [BGGS19]. This thesis also contains further results that solve open problems of [BGGS19].

Question 2.12 was considered in [BGGS19] for the non-amortized setting, where the following partial answer was given, establishing a separation in communication cost between $(r+2)$-round and $\lfloor (r+1)/2 \rfloor$-round protocols, for any $r \in \mathbb{N}$:

Theorem 4.1 (Thms. 1.1 & 1.2 of [BGGS19])**.** *For each $r \in \mathbb{N}, \epsilon \in [0,1)$, there exists $\eta > 0$, $\beta < \infty$, $n_0 \in \mathbb{N}$ such that for any $n \geq n_0$ and any $\ell \in \mathbb{N}$, there is a source $\mu_{r,n,\ell}$ such that, in the non-amortized setting:*

1. *The tuple $(O(\log n), \ell, 0)$ is $(r+2)$-achievable for SKG from $\mu_{r,n,\ell}$ (and thus $(O(\log n), \ell)$ is $(r+2)$-achievable for CRG).*
2. *For any $L \in \mathbb{N}$ and $C \leq O(\min\{L, n/\operatorname{poly}\log n\})$, the tuple (C, L, ϵ) is not $\lfloor (r+1)/2 \rfloor$-achievable for CRG (and thus the tuple (C, L, ϵ, δ) is not $\lfloor (r+1)/2 \rfloor$-achievable for all $\delta \geq 0$).*

To interpret the above theorem, fix any $r \in \mathbb{N}, \epsilon \in [0,1)$, and consider parameters $\ell = n \to \infty$. Then with only $O(\log n)$ communication, ℓ bits of entropy can be generated in $r+2$ rounds, but if we have only roughly have half as many rounds (i.e., $\lfloor (r+1)/2 \rfloor$ rounds) then generating ℓ bits of entropy takes at least $n/\operatorname{poly}\log n$ communication, which is exponentially larger than $\log n$. Moreover, this exponential-sized gap in communication complexity is essentially optimal for $\lfloor (r+1)/2 \rfloor \geq 2$, as any protocol with communication cost C can be simulated by a 2-round protocol with communication cost at most 2^{C+2}.[6]

Theorem 4.1 leaves two immediate open problems, solutions to which would present an affirmative answer to parts (1) and (3) of Question 2.12:

Problem 2.13. In the context of Theorem 4.1:

[6] To see this claim, first note that any round protocol with communication cost C and fixed inputs $X = x, Y = y$, can be viewed as a binary tree. Each node in the tree is *owned* by a single party, where the owner does not depend on X, Y. The 2 edges from each node to its children are labeled by real numbers in $[0,1]$ that sum to 1. We say that those edges are also owned by the party owning v, and the labels of the edges owned by Alice (Bob, resp.) must only depend on X (Y, resp.). The protocol proceeds as follows: at each node v, the party owning that node chooses one of its children with probability given by the edges from v to the child, and transmits a 0 or 1 to Bob to communicate which child was chosen. Then the party owning the chosen child of v communicates the next bit, and so on. To simulate this protocol with a 2-round protocol, Alice can perform, for each of the nodes owned by Alice (of which there are at most 2^{C+1}), the coin flips to determine which child she would choose at that node, and then send Bob the resulting at most 2^{C+1} bits. Bob can do the same for the nodes owned by him, and then both parties can simulate the protocol.

(1) Can the gap between $r+2$ and $\lfloor (r+1)/2 \rfloor$ rounds of communication be improved to, say, $r+2$ and $r+1$ rounds?

(2) Can the source $\mu_{r,n,\ell}$ be used to obtain an analogous separation of the rate regions for $(r+2)$-round and $\lfloor (r+1)/2 \rfloor$-round (or even $(r+2)$-round and $(r+1)$-round) protocols in the *amortized* setting?

In this thesis, we solve both of these problems and in fact obtain a close-to-optimal answer to nearly all parts of Question 2.12. Below we present informally our main results:

Theorem 4.2 (Tighter round dependence than Thms. 1.1 & 1.2 of [BGGS19] for non-amortized setting; informal)**.** *For each $r \in \mathbb{N}, \epsilon \in [0,1)$, there are sufficiently large n such that for any ℓ, there is a source $\mu_{r,n,\ell}$ such that, in the non-amortized setting:*

1. *The tuple $(O(\log n), \ell, 0)$ is $(r+2)$-achievable for SKG from $\mu_{r,n,\ell}$ (and thus $(O(\log n), \ell)$ is $(r+2)$-achievable for CRG).*
2. *For any $L \in \mathbb{N}$, $C \leq O\left(\min\{L, \sqrt{n}/\operatorname{poly}\log n\}\right)$, the tuple (C, L, ϵ) is not r-achievable for CRG from $\mu_{r,n,\ell}$ (and thus for any $\delta \geq 0$, the tuple (C, L, ϵ, δ) is not r-achievable for SKG).*

Theorem 5.1 (Amortized setting; informal)**.** *For each $r \in \mathbb{N}, \gamma \in (0,1)$, there are sufficiently large n such that for any ℓ, there is a source $\mu_{r,n,\ell}$ such that:*

1. *The tuple $(O(\log n), \ell)$ is $(r+2)$-achievable for SKG (and thus for CRG) from $\mu_{r,n,\ell}$.*
2. *Set $\ell = n$. For any $L > \gamma n$ and $C \leq O(n/\operatorname{poly}\log n)$, the tuple (C, L) is not $\lfloor (r+1)/2 \rfloor$-achievable for CRG (and thus for SKG) from $\mu_{r,n,n}$.*
3. *Again set $\ell = n$. For any $L > \gamma n$ and $C \leq O(\sqrt{n}/\operatorname{poly}\log n)$, the tuple (C, L) is not r-achievable for CRG (and thus for SKG) from $\mu_{r,n,n}$.*

Remark 2.14. Theorem 5.1 shows the existence of separations between $\mathcal{T}_{r+2}(X,Y)$ and $\mathcal{T}_r(X,Y)$ (i.e., the existence of tuples $(C,L) \in \mathcal{T}_{r+2}(X,Y)$ but that are not in $\mathcal{T}_r(X,Y)$). In Theorem 5.9 we show how these separations imply corresponding separations between $\mathscr{I}_{r+2}(X;Y)$ and $\mathscr{I}_r(X;Y)$, thus giving a partial answer to the second part of Question 2.12. We are not quite able to use Theorem 5.1 to derive analogous separations between $\Gamma^{\mathsf{cr}}_{r+2}(X,Y)$ and $\Gamma^{\mathsf{cr}}_r(X,Y)$ (or even between $\Gamma^{\mathsf{cr}}_{r+2}(X,Y)$ and $\Gamma^{\mathsf{cr}}_{\lfloor (r+1)/2 \rfloor}(X,Y)$), and leave this problem for future woek (Problem 5.1).

The source $\mu_{r,n,\ell}$ referred to in Theorems 4.2 and 5.1 is a variant of the well-known *pointer chasing distribution* from communication complexity [NW93, DGS84, PS82]. This distribution was introduced to show a similar type of rounds/communication tradeoff as in the above theorems, except for the task of *computing functions* rather than generating a shared string. (Recall the definition of communication complexity of functions in Section 2.2.1.)

A typical example of such a pointer chasing function is as follows: for an integer n and odd r, Alice receives functions indexed by even integers $\Sigma_1, \Sigma_3, \ldots, \Sigma_r : [n] \to [n]$, and Bob receives functions indexed by odd integers $\Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1} : [n] \to [n]$, as well as an integer $I_0 \in [n]$. The goal is to compute $\Sigma_r \circ \Sigma_{r-1} \circ \cdots \Sigma_1(I_0) \in [n]$.[7] If they can communicate in $r+2$ rounds, then Bob

[7] In our pointer chasing variants (e.g., Definition 4.1), the $\Sigma_1, \ldots, \Sigma_r$ will actually taken to be *permutations* on $[n]$ for technical reasons.

can send Alice I_0 when he first speaks, Alice can then send Bob $\Sigma_1(I_0) \in [n]$, Bob can respond with $\Sigma_2(\Sigma_1(I_0)) \in [n]$, and so on, until they compute $\Sigma_r \circ \Sigma_{r-1} \circ \cdots \Sigma_1(I_0) \in [n]$ in the last round, which takes $(r \log n)$ bits of communication. However, computing this value in fewer than $r+2$ rounds seems to be difficult with $O(\log n)$ (or even $o(n)$) communication. This intuition is formalized by [NW93], who show that any r-round protocol computing $\Sigma_r \circ \cdots \circ \Sigma_1(I_0)$ must communicate $\Omega(n)$ bits (in contrast to the $(r+2)$-round protocol we discussed with communication cost $r \log n$). This "round hierarchy result" has spawned a great number of follow-up papers presenting generalizations and extensions (e.g., [DJS96, CCM16, PRV01, GM08, GM09, Yeh16]), and has also found diverse applications such as proving bounds on monotone circuit depth [NW93] and establishing lower bounds for graph streaming problems [GO16].

Our Theorems 4.2 and 5.1 (and the earlier results in [BGGS19]) then can be interpreted as establishing an analogous "round hierarchy" for the settings of common randomness and secret key generation. In light of this interpretation, it is natural to ask whether such results for CRG and SKG can be derived as a consequence (in a black-box manner) of the functional versions in [NW93, DGS84]. The achievability of the rates $(O(\log n), \ell)$, representing a protocol with $O(\log n)$ communication cost that outputs keys with ℓ bits of entropy, follows in a trivial way nearly identical to that of the functional problem discussed above. Therefore, the main content to Theorems 4.1, 4.2, and 5.1 is the *lower bound* establishing that certain tuples are *not* achievable, i.e., item (2) of each statement. However, it does not seem to be possible to derive these lower bounds as a black-box consequence of the corresponding lower bounds of [NW93]. This results from the following two facts: first, to generate common randomness or a secret key from a pointer chasing distribution, it is not clear that Alice and Bob have to compute a version of the pointer chasing function in the first place. Second, suppose that we could overcome the first difficulty and show that Alice and Bob do in fact have to compute such a pointer chasing function; this is essentially the first step in the proof of Theorem 4.1, presented in Proposition 4.5 and Theorem 4.6. But then it turns out that we need some lower bound on the *distributional communication complexity* of such a pointer chasing function for a very particular distribution in which Alice's and Bob's inputs are correlated. Such a result does not appear to exist in the literature: typically lower bounds are proven for the distributional communication complexity of a distribution in which Alice's and Bob's inputs are independent, which greatly simplifies the analysis. Indeed, the bulk of the proof of Theorem 4.1 rests in the proof of Theorem 4.10, which presents such a distributional communication complexity lower bound for a certain pointer chasing function.

However, once the distributional complexity lower bound on a pointer chasing function is established in Theorem 4.10, it turns out that we can use this lower bound as a black box to establish Theorems 4.2 and 5.1, thus solving both parts of Problem 2.13.

3 History

In this section we review some of the relevant history on work studying the CRG and SKG problems.

3.1 Non-amortized CRG and SKG

Some of the earliest work on common randomness generation was in the *zero-communication* case, in which the problem is known as non-interactive correlation distillation. Witsenhausen [Wit75] and Gács and Körner [GK73] studied the following question: suppose N pairs $(X_i, Y_i) \sim \mu$ are drawn

i.i.d., and Alice and Bob wish to compute functions $f_N(X_1, \ldots, X_N) \in \{0,1\}$ and $g_N(Y_1, \ldots, Y_N) \in \{0,1\}$, respectively, such that $\mathbb{P}[f_N(X_1, \ldots, X_N) = 1]$ and $\mathbb{P}[g_N(Y_1, \ldots, Y_N) = 1]$ remain bounded away from 0 and 1 as $N \to \infty$, but that $\mathbb{P}[f_N(X_1, \ldots, X_N) \neq g_N(Y_1, \ldots, Y_N)] \to 0$. In other words, Alice and Bob wish to agree with probability bounded away from 0 on a single bit with positive entropy. [GK73, Wit75] show that this is possible if and only if the *Hirschfeld-Gebelein-Rényi (HGR) maximal correlation* of X, Y, defined below, is equal to 1:

Definition 3.1 (HGR Maximal correlation)**.** The maximal correlation of $(X, Y) \sim \mu$ is defined as

$$\rho_{\mathrm{m}}^2(X, Y) := \sup_{(f(X), g(Y))} \mathbb{E}_\mu[f(X)g(Y)],$$

where the supremum is over all real-valued measurable functions $f(X), g(Y)$, such that $\mathbb{E}_\mu[f(X)] = \mathbb{E}_\mu[g(Y)] = 0$ and $\mathbb{E}_\mu[f(X)^2] = \mathbb{E}_\mu[g(Y)^2] = 1$.

It is also shown in [GK73, Wit75] that $\rho_{\mathrm{m}}^2(X, Y) = 1$ if and only if the distribution $(X, Y) \sim \mu$ is *decomposable* in the following sense: there exist subsets $\mathcal{A} \subset \mathcal{X}, \mathcal{B} \subset \mathcal{Y}$ such that $\mathbb{P}[X \in \mathcal{A}], \mathbb{P}[X \in \mathcal{X} \backslash \mathcal{B}], \mathbb{P}[Y \in \mathcal{B}], \mathbb{P}[Y \in \mathcal{Y} \backslash \mathcal{B}]$ are all positive, yet

$$\mathbb{P}[X \in \mathcal{A}, Y \in \mathcal{B}] = \mathbb{P}[X \in \mathcal{X} \backslash \mathcal{A}, Y \in \mathcal{Y} \backslash \mathcal{B}] = 0.$$

(Notice that the "if" direction here is immediate.)

The generalization of this problem of non-interactive correlation distillation to the case where there are multiple parties and they all wish to agree on a bit was studied in [MO05, MOR+06]. In particular, these works consider the case where the distribution μ is over a bit, and each party's bit is flipped with some probability p. Yang [Yan07] considers a related problem for the 2-party case, and also allows the parties to communicate a single bit.

Bogdanov and Mossel [BM11] study common randomness generation in the zero-communication setting: for some $p \in [0,1]$ and $N \in \mathbb{N}$, suppose Alice and Bob receive N copies of a binary symmetric source BSS_p, denoted (X_i, Y_i) (so $\mathbb{P}[X_i \neq Y_i] = p$ for $1 \leq i \leq N$). For some $k \in \mathbb{N}$, without communicating, they wish to output approximately uniform strings of length k, $K_{\mathtt{A}}, K_{\mathtt{B}} \in \{0,1\}^k$, such that $K_{\mathtt{A}} = K_{\mathtt{B}}$ with high probability. It is shown in [BM11] that the maximum probability of agreement is approximately $2^{-kp/(1-p)}$. A follow-up work [CMN14] considers a generalization of the BSS to larger alphabets in the context of this problem: the source μ is now over pairs $(X, Y) \sim [s]$, for $s \in \mathbb{N}$, where X is uniform over $[s]$, $Y = X$ with probability $1 - p$, and otherwise Y is uniform over $[s] \backslash \{X\}$. [CMN14] shows that for some function $\delta(s) \to 0$ as $s \to \infty$, the best possible agreement probability is at most $(1 - \epsilon + \epsilon/s)^k \cdot (1 + \delta(s))^k$.

As discussed briefly in Section 2.5.1, [CGMS17, GR16] consider CRG from the binary symmetric source (BSS) and the binary erasure channel (BEC). Notice that for the binary symmetric source, this is the same problem as that considered by Bogdanov and Mossel [BM11], except that communication is allowed. [GR16] showed that for the source $\mu = \mathrm{BSS}_p$, letting $\alpha = 4p(1-p)$, and $\gamma \in (0,1)$, the tuple

$$(k(\alpha(1-\gamma) - 2\sqrt{\alpha(1-\alpha)\gamma}), k, 2^{-\gamma k - O(\log k)}) \tag{3}$$

is achievable by a 1-round protocol, and this is essentially optimal. They showed an analogous result for the BEC. In a follow-up work, Ghazi and Jayram [GJ18] showed that the protocols of [GR16] could be made *sample-efficient*, meaning that essentially the same rate (3) could be obtained, though with an explicitly-defined protocol that uses only $\mathrm{poly}(k)$ samples (X, Y) from BSS_p.

3.2 Single-letter Characterization of Rate Regions for Amortized CRG and SKG

The r-round rate region for amortized CRG and SKG is completely characterized by, for each communication rate C, the maximum real number L, known as the *capacity*, such that (C, L) is r-achievable for CRG or SKG:

Definition 3.2 (CR & SK capacity)**.** Suppose a source $(X, Y) \sim \mu$ is fixed. Then for $r \in \mathbb{N}, C \in \mathbb{R}_+$, define the *CR capacity with communication* C to be

$$\mathscr{C}_r^{\texttt{am-cr}}(C) := \sup_{(C,L)\in\mathcal{T}_r(X,Y)} L,$$

and the *SK capacity with communication* C to be

$$\mathscr{C}_r^{\texttt{am-sk}}(C) := \sup_{(C,L)\in\mathcal{S}_r(X,Y)} L.$$

(Recall the definitions of $\mathcal{T}_r(X, Y)$ and $\mathcal{S}_r(X, Y)$ in Definitions 2.1 and 2.2.) When we want to emphasize dependence of $\mathscr{C}_r^{\texttt{am-cr}}(\cdot), \mathscr{C}_r^{\texttt{am-sk}}(\cdot)$ on μ, we write $\mathscr{C}_r^{\texttt{am-cr}}(C|\mu)$ and $\mathscr{C}_r^{\texttt{am-sk}}(C|\mu)$, respectively.

In their seminal work on CRG in the amortized setting, Ahlwede and Csiszár [AC98] computed the following *single-letter characterization*[8] of $\mathscr{C}_1^{\texttt{am-cr}}(C)$, or equivalently, of $\mathcal{T}_1(X, Y)$:

Theorem 3.1 ([AC98])**.** *The 1-round CR capacity is given by:*

$$\mathscr{C}_1^{\texttt{am-cr}}(C) = \begin{cases} \max_U \{I(U;X) : I(U;X) - I(U;Y) \le C\} & : \quad C \le H(X|Y) \\ C + I(X;Y) & : \quad C > H(X|Y), \end{cases}$$

where the maximum in the first case is over all random variables U on a set $\mathcal{U}$ of size $|\mathcal{U}| \le |\mathcal{X}|$, satisfying the Markov condition $U - X - Y$.

Moreover, if we replace all definitions (i.e., of $\mathcal{T}_r(X, Y)$ and $\mathscr{C}_1^{\texttt{am-cr}}(C)$) with the corresponding ones where the protocols are not allowed to use private random bits, then the CR capacity at communication C simply becomes:

$$\max_U \{I(U;X) : I(U;X) - I(U;Y) \le C\}, \tag{4}$$

where the maximum is over the same random variables U as before.

The expression given in (4) deserves some additional discussion. Notice that a random variable $U \in \mathcal{U}$ with $|\mathcal{U}|$ finite and that satisfies the Markov condition $U - X - Y$ may be interpreted as a one-round private coin randomized protocol between Alice and Bob whose message (sent by Alice) is simply given by $\Pi_1 = U$ (which can be viewed as a string in $\{0,1\}^{\lceil \log |\mathcal{U}| \rceil}$); see Proposition 2.1. We make two observations about the quantities involving mutual information in (4):

[8] The term "single-letter characterization" is used relatively loosely in the information theory literature. Following [CK81], for any $k \in \mathbb{N}$ and a closed subset $\mathcal{S} \subset \mathbb{R}^k$, we call a characterization of $\mathcal{S}$ a *single-letter characterization* if it implies, for any $\eta > 0$, the existence of an algorithm that decides whether a point $x \in \mathbb{R}^k$ is of Euclidean distance at most η to $\mathcal{S}$. Moreover, this algorithm must run in time at most $T_{\mathcal{S}}(\eta)$, for some function $T_{\mathcal{S}} : \mathbb{R}_+ \to \mathbb{N}$. For instance, for the characterization given in Theorem 3.1, the set $\mathcal{S}$ is given by $\mathcal{T}_1(X, Y)$, and the algorithm iterates through all possible conditional distributions of $U|X$ where U is supported on some set $\mathcal{U}$ of size $|\mathcal{U}| \le |\mathcal{X}|$, with a sufficiently small granularity (depending on η). Correctness follows by the continuity of the Shannon entropy.

1. As $I(U;Y|X) = 0$ by the Markov condition, the quantity being maximized in (4), namely $I(U;X)$, is equal to $I(U;XY)$.

2. As $I(U;X) - I(U;Y) = I(U;X|Y)$, the constrained quantity in (4), namely $I(U;X) - I(U;Y)$ is equal to $I(U;X|Y) + I(U;Y|X)$.

These two quantities, namely $I(U;XY)$ and $I(U;X|Y) + I(U;Y|X)$, have independently found many applications in the computer science community [BBCR13, BR11, BRWY13, BGPW13, Bra12], where they are referred to as the *external information cost* and *internal information cost*, respectively, of the protocol induced by $\Pi_1 = U$. More generally, the external information cost of a (multiple-round) protocol Π describes how much information Π reveals about the inputs X, Y to an external observer who only sees the transcript of the protocol, while the internal information cost describes how much information Alice and Bob reveal to *each other* about their own inputs:

Definition 3.3 (External and internal information costs)**.** Given any communication protocol Π with a maximum of r rounds, public randomness $R_{\mathtt{Pub}}$, and a distribution $(X,Y) \sim \mu$ of inputs, the *external information cost* $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi)$ is given by:

$$\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) := I(\Pi^r, R_{\mathtt{Pub}}; X, Y).$$

If Π does not use public randomness, then $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) := I(\Pi^r; X, Y)$.

The *internal information cost* $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi)$ is given by

$$\mathrm{IC}_\mu^{\mathrm{int}}(\Pi) := I(\Pi^r, R_{\mathtt{Pub}}; X|Y) + I(\Pi^r, R_{\mathtt{Pub}}; Y|X).$$

If Π does not use public randomness, then $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi) := I(\Pi^r; X|Y) + I(\Pi^r; Y|X)$.

The original motivation behind the introduction of internal and external information costs in the computer science community was to understand the possibility of proving *direct sum* results for communication complexity [CSWY01, JRS03, HJMR07, BBCR13]. Such a direct sum result would state that the communication complexity of computing N independent copies of a function (i.e., with N independent pairs of inputs (X_i, Y_i)) is roughly N times the communication complexity of computing a single copy of the function. This problem was initially considered in [KRW95], where a direct sum result for deterministic communication complexity was conjectured for a certain relation, and it was shown that a proof of this conjecture would imply $\mathrm{P} \not\subseteq \mathrm{NC}^1$. A (weak) direct sum result was shown for the deterministic communication complexity of computing functions [FNKN95], where it was proven that if the deterministic communication complexity of computing f is C, then the deterministic communication complexity of computing n copies of f is $\Omega(\sqrt{C}n)$. For the case of randomized and distributional communication complexity, it is known that no tight direct sum theorem (i.e., one that states that the complexity of computing n copies of any function f, each correctly with probability $2/3$, is $\Omega(Cn)$) holds [GKR14, GKR16, RS18], but the possibility of a weak direct sum result still remains open [BGKR18].

In light of the connection with direct sum results, the fact that internal and external information costs appear in characterizations for amortized CRG and SKG is not too surprising. In particular, the amortized CRG and SKG problems can be viewed as the task of solving N independent instances of CRG or SKG from a source μ, with an additional requirement that each of Alice's N output strings must agree with each of Bob's N output strings *simultaneously* with high probability. In

fact, the proof of our Theorem 5.1 will involve many of the same tools that have been used to prove direct sum results for certain subclasses of functions [BR11].

Returning to our discussion of Theorem 3.1, which motivated our introduction of internal and external information complexities, we now work towards a statement of a generalization of it to the case of r-round protocols. It is useful to first consider the possible values for the pairs $(\mathrm{IC}^{\mathrm{int}}_\mu(\Pi), \mathrm{IC}^{\mathrm{ext}}_\mu(\Pi))$, for a given source μ, as Π ranges over all r-round protocols:

Definition 3.4. For a source $(X,Y) \sim \mu$, denote by $\mathcal{T}^{\mathrm{d}}_r(X,Y)$ the set of pairs (C,L) for which there exists an r-tuple $(\Pi_1,\ldots,\Pi_r)$ of random variables taking values in finite sets, satisfying the Markov conditions,

$$\Pi_t - X\Pi^{t-1} - Y,\ t \in \mathcal{O}^r \qquad X - Y\Pi^{t-1} - \Pi_t,\ t \in \mathcal{E}^r, \tag{5}$$

such that, letting $\Pi = (\Pi_1,\ldots,\Pi_r)$ denote the protocol induced by the random variables $\Pi_1,\ldots,\Pi_r$, $\mathrm{IC}^{\mathrm{int}}_\mu(\Pi) \le C$ and $\mathrm{IC}^{\mathrm{ext}}_\mu(\Pi) \ge L$. (See Proposition 2.1.)

Lemma 3.2. *$\mathcal{T}^{\mathrm{d}}_r(X,Y)$ is closed.*

Proof. By the support lemma [CK81, Lemma 15.4], we can restrict our attention to protocols $\Pi = (\Pi_1,\ldots,\Pi_r)$ such that Π_t, $1 \le t \le r$, falls in a finite set of size $\mathcal{U}_t$ at most $|\mathcal{X}||\mathcal{Y}| \prod_{t'=1}^{t-1} |\mathcal{U}_{t'}| + 1$. For each odd t, the space of all possible Π_t is the $|\mathcal{X}| \cdot \prod_{t'=1}^{t-1} |\mathcal{U}_{t'}|$-fold product of all probability distributions on $\mathcal{U}_t$ (as Π_t specifies a probability distribution on $\mathcal{U}_t$ for each possible value of $X\Pi^{t-1}$), which is compact, and in fact homeomorphic to a closed ball in some $\mathbb{R}^K$. We have an analogous statement for even t, and therefore the space of all possible Π is compact. Since the functions $\Pi \mapsto \mathrm{IC}^{\mathrm{int}}_\mu(\Pi)$ and $\Pi \mapsto \mathrm{IC}^{\mathrm{ext}}_\mu(\Pi)$ are continuous, it follows that the set of all possible $(\mathrm{IC}^{\mathrm{int}}_\mu(\Pi), \mathrm{IC}^{\mathrm{ext}}_\mu(\Pi)) \in \mathbb{R}^2_{\ge 0}$, over all r-round protocols Π, is compact (and in particular closed). Thus $\mathcal{T}^{\mathrm{d}}_r(X,Y)$ is closed as well. □

The reason for the similarity of notation between $\mathcal{T}^{\mathrm{d}}_r(X,Y)$ and $\mathcal{T}_r(X,Y)$ is as follows: recall (Definition 2.1) that $\mathcal{T}_r(X,Y)$ is the set of pairs (C,L) which are r-achievable by a protocol with *private randomness*. It turns out (Theorem 3.4) that $\mathcal{T}^{\mathrm{d}}_r(X,Y)$ is the set of pairs (C,L) which are r-achievable by a protocol with *no randomness*, i.e., a deterministic protocol.

Recall the definition of the minimum r-round interaction for achieving the maximum key rate (r-round MIMK; Definition 2.8). The following theorem provides a single letter characterization of the r-round MIMK in terms of $\mathcal{T}^{\mathrm{d}}_r(X,Y)$.

Theorem 3.3 ([Tya13], Theorem 4)**.** *Suppose we are given a source $(X,Y) \sim \mu$. Then for $r \in \mathbb{N}$, $C \in \mathbb{R}_+$, the minimum interaction for maximum key rate is*

$$\mathscr{I}_r(X;Y) = \inf\left\{ L - I(X;Y) \ :\ (L - I(X;Y), L) \in \mathcal{T}^{\mathrm{d}}_r(X;Y) \right\}. \tag{6}$$

Theorem 3.3 is proved by relating $\mathscr{I}_r(X;Y)$ to a generalization of Wyner's common information [Wyn75].

Notice that for all r, $\mathscr{I}_r(X;Y) \le H(X|Y)$, since the 1-round protocol Π in which Alice sends her input $X = \Pi_1$ satisfies $\mathrm{IC}^{\mathrm{int}}(\Pi) = I(X;X|Y) = H(X|Y)$ and $\mathrm{IC}^{\mathrm{ext}}(\Pi) = I(X;XY) = H(X)$, and thus $\mathrm{IC}^{\mathrm{ext}}(\Pi) - \mathrm{IC}^{\mathrm{int}}(\Pi) = I(X;Y)$. It follows similarly that for $r \ge 2$, $\mathscr{I}_r(X;Y) \le \min\{H(X|Y), H(Y|X)\}$.

Using Theorem 3.3, we come to the desired generalization of the single-letter characterization of Theorem 3.1 to multi-round protocols. It is stated most precisely in [STW19], but similar results are shown in [LCV17, GJ18, Liu16, Ye05, GA10a, GA10b].

Theorem 3.4 ([STW19], Theorem III.2)**.** *We have:*

(1) For a source $(X,Y)\sim\mu$, the r-round CR capacity is given by

$$\mathscr{C}_r^{\texttt{am-cr}}(C)=\begin{cases}\sup_{(C,L)\in\mathcal{T}_r^{\mathrm{d}}(X,Y)}\{L\} & : \quad C\le\mathscr{I}_r(X;Y)\\ I(X;Y)+C & : \quad C>\mathscr{I}_r(X;Y).\end{cases}\tag{7}$$

(2) The region $\mathcal{T}_r^{\mathrm{d}}(X,Y)\subset\mathcal{T}_r(X,Y)$ is exactly the set of tuples (C,L) that are achievable by deterministic protocols Π.

(3) $\mathscr{C}_r^{\texttt{am-sk}}(C)=\mathscr{C}_r^{\texttt{am-cr}}(C)-C$.

Remark 3.5. We briefly explain how Theorem 3.4 does in fact provide a single-letter characterization for $\mathcal{T}_r(X,Y)=\{(C,L):C\ge 0,L\le\mathscr{C}_r^{\texttt{am-cr}}(C)\}$, and thus for $\mathcal{S}_r(X,Y)$. It follows from the support lemma [CK81, Lemma 15.4] that the protocols $\Pi=(\Pi_1,\dots,\Pi_r)$ in the definition of $\mathcal{T}_r^{\mathrm{d}}(X,Y)$ can be restricted to the class of protocols where Π_t, $1\le t\le r$, falls in a finite set of size $\mathcal{U}_t$ at most $|\mathcal{X}||\mathcal{Y}|\prod_{t'=1}^{t-1}|\mathcal{U}_{t'}|+1$. Then by iterating through all possible distributions of $\Pi_t|\Pi^{t-1}X$, for $t\in\mathcal{O}^r$, and $\Pi_t|\Pi^{t-1}Y$, for $t\in\mathcal{E}^r$, at a sufficiently small granularity, we can approximate $\sup_{(C,L)\in\mathcal{T}_r^{\mathrm{d}}(X,Y)}\{L\}$ to any given precision. By Theorem 3.3, similar considerations apply regarding the computation of $\mathscr{I}_r(X;Y)$ (which is expressed in (6) entirely in terms of $\mathcal{T}_r^{\mathrm{d}}(X,Y)$).

When $C\le\mathscr{I}_r(X;Y)$, $\mathscr{C}_r^{\texttt{am-cr}}(C)$ may equivalently be written as:

$$\sup_{\Pi=(\Pi_1,\dots,\Pi_r):\mathrm{IC}_\mu^{\mathrm{int}}(\Pi)\le C}\{\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi)\},$$

where in the supremum $\Pi=(\Pi_1,\dots,\Pi_r)$ represents any r-round private-coin protocol.

Let $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ be the right-hand side of (7), so that part (1) of Theorem 3.4 states that $\mathscr{C}_r^{\texttt{am-cr}}(C)=\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$. The proof of part (1) of the theorem consists of two parts: first, the proof of *achievability*, namely that $\mathscr{C}_r^{\texttt{am-cr}}(C)\ge\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$, which states that for each pair (C,L) with $L<\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$, there is some r-round protocol achieving the rate (C,L). Second, one must prove the *converse* direction, that $\mathscr{C}_r^{\texttt{am-cr}}(C)\le\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$, which states that for each pair (C,L) with $L>\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$, there is no r-round protocol achieving the rate (C,L). We prove the converse direction in Section 3.4; notice that this is the only direction needed to establish Corollary 3.5 below, which is in turn the only consequence of Theorem 3.4 we use in the proofs of our results. The proof of achievability uses the likelihood encoder of Song et al. [SCP16] and can be found in [LCV17] (The proof of achievability in the special case for 1-round communication, Theorem 3.1, can also proceed by using standard machinery of jointly typical sequences [CT12, AC98].)

We remark that part (1) of Theorem 3.4 has the following immediate consequence:

Corollary 3.5. *For each tuple $(C,L)\in\mathcal{T}_r(X,Y)$ with $L<I(X;Y)$, there is some protocol $\Pi=(\Pi_1,\dots,\Pi_r)$ such that $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi)\le C$ and $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi)\ge L$.*

Proof. First suppose that $C\le\mathscr{I}_r(X;Y)$. Then the existence of the r-round protocol Π follows from (7) and Definition 3.4.

Next suppose $C>\mathscr{I}_r(X;Y)$. Notice that $(\mathscr{I}_r(X;Y),I(X;Y))\in\mathcal{T}_r(X,Y)$, since $\mathscr{C}_r^{\texttt{am-cr}}(\mathscr{I}_r(X;Y))=I(X;Y)+\mathscr{I}_r(X;Y)$. Therefore, the case $C\le\mathscr{I}_r(X;Y)$ gives that there is an r-round protocol Π such that $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi)\le\mathscr{I}_r(X;Y)<C$ and $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi)\ge I(X;Y)>L$, as desired. □

3.3 Strong Data Processing Constant, Hypercontractivity

In this section we discuss some connections between properties of the rate regions $\mathcal{T}_r(X,Y), \mathcal{S}_r(X,Y)$, such as the r-round CBIB and KBIB (Definitions 2.5 and 2.6), and other quantities considered in probability and information theory. The results discussed in this section give an alternate interpretation to some of our main results, but are not used directly in our proofs, so this section can be skipped.

3.3.1 1-round protocols

We begin with the one-round case, $r = 1$. The *strong data processing constant*, $s_1^*(X,Y)$, plays a key role in many of these connections; it is defined as follows:

$$s_1^*(X,Y) := \sup_{U: U-X-Y} \frac{I(U;Y)}{I(U;X)}, \tag{8}$$

where the supremum is over all random variables U such that the given Markov condition holds. Notice that by the data processing inequality, $s_1^*(X,Y) \leq 1$; thus, $s_1^*(X,Y)$ can be viewed as determining "how much stronger" the data processing inequality can be made for Markov chains $U - X - Y$, where the distribution of (X,Y) is fixed.

By comparing with Theorems 2.3 and 3.4, it follows easily that

$$s_1^*(X,Y) = \frac{\Gamma_1^{\mathtt{sk}}(X,Y)}{\Gamma_1^{\mathtt{sk}}(X,Y)+1} = \frac{\Gamma_1^{\mathtt{cr}}(X,Y)-1}{\Gamma_1^{\mathtt{cr}}(X,Y)}.$$

Thus determining $s_1^*(X,Y)$ is equivalent to determining the 1-round CBIB and KBIB for the source $(X,Y) \sim \mu$.

In turn, Ahlswede and Gács [AG76] showed a characterization of the strong data processing constant (SDPC) $s_1^*(X,Y)$ in terms of hypercontractivity properties of the Markov operator associated to the source $(X,Y) \sim \mu$. We first define the *Markov operator*: if $\mathscr{F}(\mathcal{X}), \mathscr{F}(\mathcal{Y})$ denote the real-valued functions defined on $\mathcal{X}$ and $\mathcal{Y}$, respectively[9], then the Markov operator $T_\mu : \mathscr{F}(\mathcal{Y}) \to \mathscr{F}(\mathcal{X})$ is defined by:

$$(T_\mu g)(x) := \mathbb{E}_\mu[g(Y)|X = x].$$

We now define the hypercontractivity ribbon associated with the Markov operator T_μ.

Definition 3.6 (Hypercontractivity ribbon)**.** Fix a distribution $(X,Y) \sim \mu$. For $p \geq 1$, define

$$q_{X,Y}^*(p) := \inf \left\{ q : \|T_\mu g(X)\|_p \leq \|g(Y)\|_q \forall g \in \mathscr{F}(\mathcal{Y}) \right\}.$$

(Recall that for a random variable Z, and $p > 0$, we define $\|Z\|_p = (\mathbb{E}[|Z|^p])^{1/p}$.) It follows by Jensen's inequality that $q_{X,Y}^*(p) \leq p$, i.e., that $\|T_\mu g(X)\|_p \leq \|g(Y)\|_p$ for all $p \geq 1$. Then the *hypercontractivity ribbon* is defined by $\{(q,p) : q_{X,Y}^*(p) \leq q \leq p\}$.

The hypercontractivity ribbon, which is defined in a purely probabilistic manner, characterizes the strong data processing constant, which is defined information theoretically:

Theorem 3.6 ([AG76, AGKN13])**.** *The following assertions hold for $p > 1$:*

[9] Here recall that we take $\mathcal{X}, \mathcal{Y}$ to be finite sets, which is the setting considered in [AG76].

1. $q^*_{X,Y}(1) = 1$.

2. $s^*_1(X,Y) = \lim_{p\to\infty} \frac{q^*_{X,Y}(p)-1}{p-1}$.

3. $s^*_1(Y,X) = \lim_{p\downarrow 1} \frac{q^*_{X,Y}(p)-1}{p-1}$.

The above characterization states that the SDPC $s^*_1(X,Y)$ is given by the limit of the lower chordal slope of the hypercontractivity ribbon (i.e., of the slope of the line connecting $(1,1)$ and $(p, q^*_{X,Y}(p))$, as $p \to \infty$).

It is also known [AG76] that for all p, $\frac{q^*_{X,Y}(p)-1}{p-1} \geq \rho^2_{\mathrm{m}}(X,Y)$, which implies that $\min\{s^*_1(X,Y), s^*_1(Y,X)\} \geq \rho^2_{\mathrm{m}}(X,Y)$; moreover, equality does not always hold.

3.3.2 Multi-round protocols; concave envelopes

Next we turn to the case of protocols with an arbitrary number r of rounds, which is of greater interest in interpreting our results. First we note that the notion of SDPC generalizes: the *r-round strong data processing constant (SDPC)* is defined as

$$s^*_r(X,Y) := \frac{\Gamma^{\mathtt{cr}}_r(X,Y) - 1}{\Gamma^{\mathtt{cr}}_r(X,Y)} = \sup_{\Pi \text{ satisfying (5)}} \frac{\sum_{t\in\mathcal{O}^r} I(\Pi_t; Y|\Pi^{t-1}) + \sum_{t\in\mathcal{E}^r} I(\Pi_t; X|\Pi^{t-1})}{\sum_{t\in\mathcal{O}^r} I(\Pi_t; X|\Pi^{t-1}) + \sum_{t\in\mathcal{E}^r} I(\Pi_t; Y|\Pi^{t-1})}.$$

We have written out the entire expression for $s^*_r(X,Y)$ to emphasize the similarity with the definition of $s^*_1(X,Y)$ given in (8).

There does not seem to be a generalization of the hypercontractivity ribbon that allows an anlogue of Theorem 3.6 to r-round protocols, but there is an alternate characterization of the r-round SDPC in terms of convex geometry due to Liu et al [LCV17]. To simplify notation in this section, for a distribution μ on a finite set $\mathcal{X}$, we write $\mu(x) = \mathbb{P}_{X\sim\mu}[X = x]$. Now, for distributions ν, μ, on a finite set $\mathcal{X}$, ν is *absolutely continuous* with respect to μ if there is a bounded function $f : \mathcal{X} \to \mathbb{R}$ such that $\nu(x) = f(x)\mu(x)$ (i.e., $\mu(x) = 0$ implies $\nu(x) = 0$). The following definition generalizes this notion of absolute continuity to the case of distributions over a product of sets $\mathcal{S} \times \mathcal{Y}$.

Definition 3.7 (X, Y, XY-absolute continuity [LCV17])**.** Consider distributions μ, ν defined on $\mathcal{X} \times \mathcal{Y}$. We say that ν is *X-absolutely continuous* with respect to μ, denoted $\nu \preceq_X \mu$, if there is a bounded function f such that for all $(x,y) \in \mathcal{X} \times \mathcal{Y}$, $\nu(x,y) = f(x)\mu(x,y)$. *Y-absolutely continuity* is defined similarly. Finally, ν is *XY-absolutely continuous* with respect to μ, denoted $\nu \preceq_{XY} \mu$, if there are bounded functions f, g such that $\nu(x,y) = f(x)g(y)\mu(x,y)$.

It is immediate that if $\nu \preceq_{XY} \mu$, then there is a distribution θ such that $\nu \preceq_X \theta \preceq_Y \mu$.

Let $\mathcal{D}$ be a set of distributions on $\mathcal{X}\times\mathcal{Y}$. A function $\sigma : \mathcal{D} \to \mathbb{R}$ is *X-concave* if for all $\nu_1, \nu_2 \in \mathcal{D}$, $\alpha \in [0,1]$ such that $\mu := \alpha\nu_1 + (1-\alpha)\nu_2 \preceq_X \nu_i$ for $i \in \{1,2\}$, $\sigma(\mu) \geq \alpha\sigma(\nu_1) + (1-\alpha)\sigma(\nu_2)$. Y-concavity and XY-concavity are defined similarly. Finally, the *concave envelope* of σ is the "smallest concave function σ' on $\mathcal{D}$ that dominates σ":

Definition 3.8 (Concave envelope, [LCV17])**.** For $\sigma : \mathcal{D} \to \mathbb{R}$ as above, the *X-concave envelope* σ' of σ, denoted $\sigma' := \mathrm{env}_X(\sigma)$, is the unique function $\sigma' : \mathcal{D} \to \mathbb{R}$ that is X-concave and such that for all $\mu \in \mathcal{D}$, $\sigma'' : \mathcal{D} \to \mathbb{R}$ that are X-concave, $\sigma(\mu) \leq \sigma'(\mu) \leq \sigma''(\mu)$. The Y-concave envelope and XY-concave envelope are defined similarly.

Let $\mathcal{D}$ denote the set of all distributions on $\mathcal{X} \times \mathcal{Y}$, $\lambda \in \mathbb{R}_+$, and define a functional $\omega_0^\lambda : \mathcal{D} \to \mathbb{R}$, by

$$\omega_0^\lambda(\mu) := \lambda H(X,Y) - I(X;Y),$$

where $(X,Y) \sim \mu$. For r odd, let $\omega_r^\lambda = \mathrm{env}_X\, \omega_{r-1}^\lambda$, and for r even, let $\omega_r^\lambda = \mathrm{env}_Y\, \omega_{r-1}^\lambda$. The following theorem relates the value of the concave envelopes ω_r^λ evaluated at a source μ, to the achievable rate region $\mathcal{T}_r(X,Y)$:

Theorem 3.7 ([LCV17], Theorem 2)**.** *Fix a source μ. Then for all $r \geq 1$, $\lambda > 0$,*

$$\omega_r^\lambda(\mu) = \lambda H(X,Y) - I(X;Y) + \sup_{(C,L) \in \mathcal{T}_r(X,Y)} \{L(1-\lambda) - C\},$$

where $(X,Y) \sim \mu$.

Since $\mathscr{C}_r^{\texttt{am-cr}}(C)$ is concave and strictly increasing (Lemma 3.13), Theorem 3.7 implies that the values of $\omega_r^\lambda(\mu)$, $\lambda > 0$, completely characterize $\mathcal{T}_r(X,Y)$. (In particular, $\omega_r^\lambda(\mu)$ determines the maximum Euclidean inner product of a tuple in $\mathcal{T}_r(X,Y)$ with $(-1,(1-\lambda))$, and the values of these for $0 < \lambda < 1$ completely determine the curve $C \mapsto \mathscr{C}_r^{\texttt{am-cr}}(C)$, which in turn completely determines $\mathcal{T}_r(X,Y)$.)

Using straightforward manipulations, the following characterizations (Theorems 3.8 and 3.9) of the r-round SDPC (which in turn determines the r-round CBIB and KBIB), and the r-round MIMK follow from Theorems 3.7 and 3.4.

Theorem 3.8 ([LCV17])**.** *For a source $(X,Y) \sim \mu$ and $r \geq 1$, $s_r^*(X,Y)$ is the infimum of all $\lambda > 0$ such that $\omega_r^\lambda(\mu) = \omega_0^\lambda(\mu)$.*

It is easy to see that for all $\lambda' > s_r^*(X,Y)$, $\omega_r^{\lambda'}(\mu) = \omega_0^{\lambda'}(\mu)$.

Theorem 3.9 ([LCV17], Theorem 8)**.** *For a source $(X,Y) \sim \mu$ and $r \geq 1$,*

$$\mathscr{I}_r(X;Y) = H(X|Y) + H(Y|X) - \lim_{\lambda \downarrow 0} \frac{1}{\lambda} \omega_r^\lambda(\mu).$$

Notice that Theorem 3.9 describes the r-round MIMK in terms of $\omega_r^\lambda(\mu)$ when λ is very small; in contrast, Theorem 3.8 describes the r-round SDPC (and thus CBIB and KBIB) in terms of $\omega_r^\lambda(\mu)$ when λ is large (in fact, as large as possible so that $\omega_r^\lambda(\mu)$ is not "trivial", i.e., not equal to $\omega_0^\lambda(\mu) = \lambda H(X,Y) - I(X;Y)$).

In Section 5.3, we describe how the above theorems lead to an alternate interpretation of our main results (i.e., an interpretation in terms of the concave envelopes $\omega_r^\lambda(\cdot)$ as opposed to the interpretation in terms of achievable rates for protocols that we have mostly focused on).

3.4 Proof of the Converse Direction of Theorem 3.4

Recall our definition of

$$\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C) := \begin{cases} \sup_{(C,L) \in \mathcal{T}_r^{\mathrm{d}}(X,Y)} L & : \quad C \leq \mathscr{I}_r(X;Y) \\ I(X;Y) + C & : \quad C > \mathscr{I}_r(X;Y). \end{cases}$$

Then point (1) of Theorem 3.4 states that $\mathscr{C}_r^{\texttt{am-cr}}(C) = \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$. Our goal in this section is to establish the following:

Theorem 3.10 (Converse direction of Theorem 3.4)**.** $\mathscr{C}_r^{\texttt{am-cr}}(C) \leq \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$.

Theorem 3.10 essentially states that any (private-coin) protocol Π for CRG can be converted into a (private-coin) protocol whose internal and external information costs are related to the communication and common randomness rates of Π in a particular way. We prove Theorem 3.10 by first establishing such a statement for deterministic protocols in Lemma 3.11 and Lemma 3.12 below. We will then use certain properties of $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ to "upgrade" this statement to apply to randomized protocols.

Lemma 3.11. *Suppose $(X,Y) \sim \mu$ for some source μ, and that the tuple (C,L), for $C, L \in \mathbb{R}_+$ is achievable by an r-round deterministic protocol (in the sense of Definition 2.1; that is, all properties of Definition 2.1 hold verbatim, except Π is not allowed to use private random coins). Then for any $L' < L, C' > C$, there is some N_0 such that for all $N \geq N_0$, there is an r-round deterministic protocol Π' with inputs $(X^N, Y^N) \sim \mu^{\otimes N}$ such that*

(1) $\mathrm{IC}^{\mathrm{ext}}_{\mu^{\otimes N}}(\Pi') \geq L'N$.

(2) $\mathrm{IC}^{\mathrm{int}}_{\mu^{\otimes N}}(\Pi') \leq C'N$.

Proof. Choose C'' with $C' > C'' > C$ and L'' with $L' < L'' < L$. By Definition 2.1, there is some N_0 so that for each $N \geq N_0$, there is an r-round protocol Π taking inputs from $\mu^{\otimes N}$ and producing keys $K_{\mathtt{A}}, K_{\mathtt{B}}$ in some set $\mathcal{K}_N$ with $|\mathcal{K}_N| \geq L'N$ so that $\mathrm{CC}(\Pi) = \sum_{t=1}^r |\Pi_t| \leq C''N$ and $\Delta(K_{\mathtt{A}}K_{\mathtt{B}}, KK) \leq \epsilon_N$ for some

$$\epsilon_N < \min\left\{\frac{C' - C'' - 2/N}{L'}, \frac{L'' - L' - 1/N}{L''}\right\}.$$

(Here $K \in \mathcal{K}_N$ denotes the random variable uniformly distributed on $\mathcal{K}_N$.) By truncating the keys we may assume without loss of generality that $|\mathcal{K}_N| \leq 2^{\lceil L'N \rceil}$. It follows from $\Delta(K_{\mathtt{A}}K_{\mathtt{B}}, KK) \leq \epsilon_N$ that $\mathbb{P}[K_{\mathtt{A}} \neq K_{\mathtt{B}}] \leq \epsilon_N$. Moreover, using Lemma 6.4, we obtain

$$\min\{H(K_{\mathtt{A}}), H(K_{\mathtt{B}})\} \geq \log|\mathcal{K}_N| - (h(\epsilon_N) + \epsilon_N \cdot \log|\mathcal{K}_N|) \geq (1-\epsilon_N)L''N - 1 \geq L'N, \qquad (9)$$

where we have used $\epsilon_N \leq \frac{L''-L'-1/N}{L''}$.

Now let Π' be the following protocol:

1. Alice and Bob first simulate Π, i.e., they exchange the messages $\Pi_1, \ldots, \Pi_r$.
2. Then the last person to speak in Π outputs their key (i.e., if it is Alice, then she outputs $K_{\mathtt{A}}$ and if it is Bob then he outputs $K_{\mathtt{B}}$).

Suppose for simplicity that r is odd, so that Alice is the last person to speak in Π (the case r even is nearly identical). Then since Π is deterministic, $K_{\mathtt{A}}, \Pi^r$ is a deterministic function of X, Y, so $H(K_{\mathtt{A}}, \Pi^r | X, Y) = 0$. Noting the transcript of Π' is given by $(\Pi_1, \ldots, \Pi_{r-1}, (\Pi_r, K_{\mathtt{A}}))$, it follows that

$$\mathrm{IC}^{\mathrm{ext}}(\Pi') = I(K_{\mathtt{A}}, \Pi^r; X, Y) = H(K_{\mathtt{A}}, \Pi^r) - H(K_{\mathtt{A}}, \Pi^r | X, Y) \geq H(K_{\mathtt{A}}, \Pi^r) \geq H(K_{\mathtt{A}}) \geq L'N,$$

where the last inequality uses (9).

To upper bound $\mathrm{IC}^{\mathrm{int}}(\Pi')$, notice that

$$\begin{aligned}
\mathrm{IC}^{\mathrm{int}}_{\mu^{\otimes N}}(\Pi') &= I(\Pi^r, K_{\mathtt{A}}; X^N|Y^N) + I(\Pi^r, K_{\mathtt{A}}; Y^N|X^N) \\
&= I(\Pi^r; X^N|Y^N) + I(K_{\mathtt{A}}; X^N|\Pi^r, Y^N) + I(\Pi^r; Y^N|X^N) \\
&= \mathrm{IC}^{\mathrm{int}}_{\mu^{\otimes N}}(\Pi) + I(K_{\mathtt{A}}; X^N|\Pi^r, Y^N) \\
&\leq \mathrm{CC}(\Pi) + H(K_{\mathtt{A}}|\Pi^r, Y^N) \\
&\leq C''N + \epsilon_N \lceil L'N \rceil + 1 \\
&\leq C'N,
\end{aligned}$$

where we have used Fano's inequality, the fact that $\mathbb{P}[K_{\mathtt{A}} \neq K_{\mathtt{B}}] \leq \epsilon_N$, and that $K_{\mathtt{B}}$ is a deterministic function of Π^R, Y^N. Moreover, the last inequality uses $\epsilon_N < \frac{C'-C''-2/N}{L'}$.

□

The next lemma, which states that the internal and external information complexities *tensorize* (i.e., they satisfy a direct sum property), was proved in [GJ18].

Lemma 3.12 ([GJ18], Lemma 14)**.** *Suppose that Π is an r-round private-coin protocol with inputs $(X^N, Y^N) \sim \nu^{\otimes N}$. Then there is an r-round private-coin protocol Π' with only private randomness, inputs $(X, Y) \sim \nu$, such that:*

(1) $\mathrm{IC}^{\mathrm{int}}_{\nu^{\otimes N}}(\Pi) = N \cdot \mathrm{IC}^{\mathrm{int}}_{\nu}(\Pi')$.

(2) $\mathrm{IC}^{\mathrm{ext}}_{\nu^{\otimes N}}(\Pi) \leq N \cdot \mathrm{IC}^{\mathrm{ext}}_{\nu}(\Pi')$.

We only sketch the proof of Lemma 3.12, so as to explain how the protocol Π' is constructed, and defer to [GJ18] for a full proof.

Proof sketch. We note the following properties of $\Pi = (\Pi_1, \ldots, \Pi_r)$:

(1) By the definition of a communication protocol, for every $t \in \mathcal{O}^r$, $I(Y^N; \Pi_t|X^N\Pi^{t-1}) = I(X^N; \Pi_{t+1}|Y^N\Pi^t) = 0$.

(2) For all $j \in [N]$ and $t \in \mathcal{O}^r$, $I(Y_j; \Pi_t|X^jY_{j+1}^N\Pi^{t-1}) = I(X_j; \Pi_{t+1}|X^{j-1}Y_j^N\Pi^t) = 0$, which follows by considering the graphical model corresponding to the distribution $\nu^{\otimes n}$ and the protocol Π and noting that the nodes Y_j and Π_t (X_j and Π_{t+1}, resp.) are D-separated by the conditioning set $X^jY_{j+1}^N\Pi^{t-1}$ ($X^{j-1}Y_j^N\Pi^t$, resp.).

Now the protocol Π' works as follows: first Alice uses private randomness to generate $J \in [N]$ uniformly at random, as well as X^{J-1}, Y_{J+1}^N (uniform in their respective domains), and sends them to Bob. (This is equivalent to using public randomness to generate J, X^{J-1}, Y_{J+1}^N.) Alice and Bob then use their private randomness to generate X_{J+1}^N and Y^{J-1} conditioned on J, X^{J-1}, Y_{J+1}^N, respectively.

Alice and Bob then simulate Π using the inputs as generated above. In particular, the distribution of the (simulated) messages $(\Pi_1, \ldots, \Pi_N)$ under Π' when $(X, Y) \sim \nu$ is identical to the distribution of the messages $(\Pi_1, \ldots, \Pi_N)$ under Π when $(X, Y) \sim \nu^{\otimes n}$. This follows since each pair (X_j, Y_j) $(1 \leq j \leq N)$ is distributed according to ν, and all of the pairs (X_j, Y_j) are distributed independently.

It was shown in [GJ18] using properties (1) and (2) above that $\mathrm{IC}^{\mathrm{int}}_{\nu^{\otimes N}}(\Pi) = N \cdot \mathrm{IC}^{\mathrm{int}}_{\nu}(\Pi')$ and $N \cdot \mathrm{IC}^{\mathrm{ext}}_{\nu}(\Pi') \geq \mathrm{IC}^{\mathrm{ext}}_{\nu^{\otimes N}}(\Pi)$, which verifies properties (1) and (2) in the lemma. □

Lemmas 3.11 and 3.12 are sufficient to prove the converse direction of Theorem 3.4 for deterministic protocols. In particular, they establish the direction of point (2) of Theorem 3.4 stating that any tuple $(C, L) \in \mathcal{T}_r(X, Y)$ achievable by a deterministic protocol in fact lies in $\mathcal{T}_r^{\mathrm{d}}(X, Y)$. To prove the converse direction for randomized protocols (i.e., Theorem 3.10), we first need to establish some properties of $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ in Lemma 3.13 below.

Lemma 3.13. *For each fixed $r \in \mathbb{N}$, $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\cdot)$ is a nondecreasing concave function on $\mathbb{R}_{\geq 0}$. In particular, it is continuous, and $\frac{d\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)}{dC} \geq 1$ for all $C \geq 0$.*

Proof. First we suppose $C' < C \leq \mathscr{I}_r(X;Y)$. That $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ is non-decreasing for C in this range is immediate from the definition. To show concavity, we use a simple time-sharing argument. In particular, pick any $L < \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ and $L' < \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C')$, and suppose some r-round protocol $\Pi = (\Pi_1, \ldots, \Pi_r)$ has $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) \geq L$, $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi) \leq C$, and that some r-round protocol $\Pi' = (\Pi'_1, \ldots, \Pi'_r)$ has $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi') \geq L'$ and $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi') \leq C'$. For any $0 < \delta < 1$, construct a protocol Π'' in which Alice, using her private randomness, generates a bit B which is 1 with probability δ, and sends it to Bob as part of the first message. If $B = 0$, Alice and Bob run the protocol Π', and if $B = 1$, then Alice and Bob run the protocol Π. Formally, we write:

$$\Pi''_i := \begin{cases} (B, \Pi_i) & : \quad i = 1, B = 1 \\ (B, \Pi'_i) & : \quad i = 1, B = 0 \\ \Pi_i & : \quad i > 1, B = 1 \\ \Pi'_i & : \quad i > 1, B = 0. \end{cases}$$

Then by linearity of expectation,

$$I(\Pi''_1; X|Y) = I(B; X|Y) + I(\Pi''_1; X|YB) = I(\Pi''_1; X|YB) = \delta \cdot I(\Pi_1; X|Y) + (1-\delta) \cdot I(\Pi'_1; X|Y).$$

and

$$I(\Pi''_1; XY) = I(B; XY) + I(\Pi''_1; XY|B) = \delta \cdot I(\Pi_1; XY) + (1-\delta) \cdot I(\Pi'_1; XY).$$

It follows in an even simpler manner that for all i,

$$I(\Pi''_i; XY|(\Pi'')^{i-1}) = \delta \cdot I(\Pi_i; XY|\Pi^{i-1}) + (1-\delta) \cdot I(\Pi'_i; XY|(\Pi')^{i-1}),$$

that for $i \in \mathcal{O}^r$,

$$I(\Pi''_i; X|Y(\Pi'')^{i-1}) = \delta \cdot I(\Pi_i; X|Y\Pi^{i-1}) + (1-\delta) \cdot I(\Pi'_i; X|Y(\Pi')^{i-1}),$$

and for $i \in \mathcal{E}^r$,

$$I(\Pi''_i; Y|X(\Pi'')^{i-1}) = \delta \cdot I(\Pi_i; Y|X\Pi^{i-1}) + (1-\delta) \cdot I(\Pi'_i; Y|X(\Pi')^{i-1}).$$

Thus $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi'') = \delta \cdot \mathrm{IC}_\mu^{\mathrm{int}}(\Pi) + (1-\delta) \cdot \mathrm{IC}_\mu^{\mathrm{int}}(\Pi')$ and $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi'') = \delta \cdot \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) + (1-\delta) \cdot \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi')$. In particular,

$$\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\delta C + (1-\delta)C') \geq \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\delta \mathrm{IC}_\mu^{\mathrm{int}}(\Pi) + (1-\delta)\mathrm{IC}_\mu^{\mathrm{int}}(\Pi')) \geq \delta \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) + (1-\delta)\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi') \geq \delta L + (1-\delta)L',$$

and taking $L \to \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ and $L' \to \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C')$ gives $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\delta C + (1-\delta)C') \geq \delta \cdot \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C) + (1-\delta) \cdot \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C')$, establishing that $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\cdot)$ is convex on $[0, \mathscr{I}_r(X;Y)]$.

To copmlete the proof of the lemma it suffices to show that (1) $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\mathscr{I}_r(X;Y)) = \mathscr{I}_r(X;Y) + I(X;Y)$, and (2) that the left-sided derivative of $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$ at $C = \mathscr{I}_r(X;Y)$ with respect to C is at least 1. For the first statement, by Lemma 3.2 and the definition of $\mathscr{I}_r(X;Y)$, we have that $(\mathscr{I}_r(X;Y) + I(X;Y), \mathscr{I}_r(X:Y)) \in \mathcal{T}_r^{\mathrm{d}}(X,Y)$, so we must have $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\mathscr{I}_r(X;Y)) \geq \mathscr{I}_r(X;Y) + I(X;Y)$. To see that $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\mathscr{I}_r(X;Y)) \leq \mathscr{I}_r(X;Y) + I(X;Y)$, we note that for any protocol Π, $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) \leq \mathrm{IC}_\mu^{\mathrm{int}}(\Pi) + I(X;Y)$ by the data processing inequality.

For the second statement, consider any $C < \mathscr{I}_r(X;Y)$, which implies that $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C) < C + I(X;Y)$. Let $\Pi = (\Pi_1, \ldots, \Pi_r)$ be any protocol with $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi) = C$ and $L := \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi)$ arbitrarily close to $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(C)$. For any $0 \leq \delta \leq 1$, consider the protocol Π' in which Alice uses private randomness to generate a bit $B \in \{0,1\}$ that is 1 with probability δ and otherwise 0 and sends it to Bob. Then, if $B = 1$, Alice sends Bob X and the protocol terminates (for a total of $1 \leq r$ rounds), and if $B = 0$, Alice and Bob simulate Π. In a similar manner as above, it is easy to see that

$$\begin{aligned} \mathrm{IC}_\mu^{\mathrm{int}}(\Pi') &= (1-\delta)C + \delta \cdot H(X|Y) \\ \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi') &= (1-\delta)L + \delta \cdot H(X). \end{aligned}$$

Since $C < \mathscr{I}_r(X;Y) \leq H(X|Y)$, there is some $\delta \in (0,1]$, which we denote by δ', such that $(1-\delta)C + \delta \cdot H(X|Y) = \mathscr{I}_r(X;Y)$. Then $(1-\delta')L + \delta' \cdot H(X) \leq \tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\mathscr{I}_r(X;Y))$. Then the secant line of the graph of $\tilde{\mathscr{C}}_r^{\texttt{am-cr}}(\cdot)$ between the points C and $\mathscr{I}_r(X;Y)$ has slope at least

$$\frac{(1-\delta')L + \delta' \cdot H(X) - L}{(1-\delta')C + \delta' \cdot H(X|Y) - C} = \frac{H(X) - L}{H(X|Y) - C} > 1,$$

where the last inequality follows since $I(X;Y) > L - C$ by assumption that $C < \mathscr{I}_r(X;Y)$. □

The case $r = 1$ of the next lemma was proven as part of the proof of Theorem 4.1 in [AC98]. It is also stated without proof in [STW19].

Lemma 3.14. *Suppose that ν is a distribution with samples $(XQ_A, YQ_B) \sim \nu$, where Q_A, Q_B are uniform and independent infinite strings of bits that are independent of (X,Y). Denote the marginal distribution of (X,Y) by μ. Suppose that Π is an r-round private-coin protocol with inputs $(XQ_A, YQ_B) \sim \nu$, and write $I^{\mathrm{int}} = \mathrm{IC}_\nu^{\mathrm{int}}(\Pi), I^{\mathrm{ext}} = \mathrm{IC}_\nu^{\mathrm{ext}}(\Pi)$. Then there is a non-negative real number α and a protocol Π' with inputs $(X,Y) \sim \mu$ such that*

$$\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi') = I^{\mathrm{ext}} - \alpha \tag{10}$$
$$\mathrm{IC}_\mu^{\mathrm{int}}(\Pi') = I^{\mathrm{int}} - \alpha. \tag{11}$$

Proof. The protocol Π' proceeds as follows: given inputs $(X,Y) \sim \mu$, Alice uses her private randomness to generate a uniform infinite string $Q_{\mathtt{A}}$ independent of X and Bob does the same to generate a uniform infinite string $Q_{\mathtt{B}}$. Then certainly the resulting pair $(XQ_{\mathtt{A}}, YQ_{\mathtt{B}})$ are distributed according to ν. Then Alice and Bob simply run the protocol Π. Notice that the joint distribution of $((\Pi')^r, (Q_{\mathtt{A}}X, Q_{\mathtt{B}}, Y))$ is identical to the joint distribution of $(\Pi^r, (Q_{\mathtt{A}}X, Q_{\mathtt{B}}Y))$.

That Π is a randomized (private-coin) protocol with inputs $(XQ_{\mathtt{A}}, YQ_{\mathtt{B}})$ means that the following Markov conditions hold:

$$\Pi_i - Q_{\mathtt{A}}X\Pi^{i-1} - Q_{\mathtt{B}}Y \qquad \forall i \in \mathcal{O}^r \tag{12}$$
$$Q_{\mathtt{A}}X - Q_{\mathtt{B}}Y\Pi^{i-1} - \Pi_i \qquad \forall i \in \mathcal{E}^r. \tag{13}$$

It follows immediately from (12) and (13) and the fact that $Q_{\mathtt{A}}$, $Q_{\mathtt{B}}$, and (X,Y) are all independent that the following Markov conditions also hold:

$$\Pi_i - X\Pi^{i-1} - Y \qquad \forall i \in \mathcal{O}^r \tag{14}$$

$$X - Y\Pi^{i-1} - \Pi_i \qquad \forall i \in \mathcal{E}^r. \tag{15}$$

It follows from (12) and (13) and the chain rule that

$$\begin{aligned} \mathrm{IC}_\nu^{\mathrm{ext}}(\Pi) &= \sum_{i\in\mathcal{O}^r} I(\Pi_i; Q_{\mathtt{A}}XQ_{\mathtt{B}}Y|\Pi^{i-1}) + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Q_{\mathtt{A}}XQ_{\mathtt{B}}Y|\Pi^{i-1}) \\ &= \sum_{i\in\mathcal{O}^r} I(\Pi_i; Q_{\mathtt{A}}X|\Pi^{i-1}) + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Q_{\mathtt{B}}Y|\Pi^{i-1}). \end{aligned} \tag{16}$$

In a similar manner, it follows from (14) and (15) that

$$\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) = \sum_{i\in\mathcal{O}^r} I(\Pi_i; X|\Pi^{i-1}) + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Y|\Pi^{i-1}). \tag{17}$$

Thus, from (16) and (17),

$$\mathrm{IC}_\nu^{\mathrm{ext}}(\Pi) - \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) = \sum_{i\in\mathcal{O}^r} I(\Pi_i; Q_{\mathtt{A}}|\Pi^{i-1}X) + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Q_{\mathtt{B}}|\Pi^{i-1}Y). \tag{18}$$

As for internal information cost, from (12) and (13) we have

$$\mathrm{IC}_\nu^{\mathrm{int}}(\Pi) = \sum_{i\in\mathcal{O}^r} I(\Pi_i; Q_{\mathtt{A}}X|\Pi^{i-1}) - I(\Pi_i; Q_{\mathtt{B}}Y|\Pi^{i-1}) + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Q_{\mathtt{B}}Y|\Pi^{i-1}) - I(\Pi_i; Q_{\mathtt{A}}X|\Pi^{i-1}), \tag{19}$$

and from (14) and (15), we have

$$\mathrm{IC}_\mu^{\mathrm{int}}(\Pi) = \sum_{i\in\mathcal{O}^r} I(\Pi_i; X|\Pi^{i-1}) - I(\Pi_i; Y|\Pi^{i-1}) + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Y|\Pi^{i-1}) - I(\Pi_i; X|\Pi^{i-1}), \tag{20}$$

Thus, from (19) and (20),

$$\begin{aligned} \mathrm{IC}_\nu^{\mathrm{int}}(\Pi) - \mathrm{IC}_\mu^{\mathrm{int}}(\Pi) &= \sum_{i\in\mathcal{O}^r} I(\Pi_i; Q_{\mathtt{A}}|\Pi^{i-1}X) - I(\Pi_i; Q_{\mathtt{B}}|\Pi^{i-1}Y) \\ &\quad + \sum_{i\in\mathcal{E}^r} I(\Pi_i; Q_{\mathtt{B}}|\Pi^{i-1}Y) - I(\Pi_i; Q_{\mathtt{A}}|\Pi^{i-1}X). \end{aligned}$$

Next we claim that for all $i \in \mathcal{O}^r$, $I(\Pi_i; Q_{\mathtt{B}}|Y\Pi^{i-1}) = 0$ and for all $i \in \mathcal{E}^r$, $I(\Pi_i; Q_{\mathtt{A}}|X\Pi^{i-1}) = 0$. For $i \in \mathcal{O}^r$, we have

$$\begin{aligned} & I(\Pi_i; Q_{\mathtt{B}}|Y, \Pi^{i-1}) - I(\Pi_i; Q_{\mathtt{B}}|Y, \Pi^{i-1}, X, Q_{\mathtt{A}}) \\ = \; & H(Q_{\mathtt{B}}|Y, \Pi^{i-1}) - H(Q_{\mathtt{B}}|Y, \Pi^i) - H(Q_{\mathtt{B}}|Y, \Pi^{i-1}, X, Q_{\mathtt{A}}) + H(Q_{\mathtt{B}}|Y, \Pi^i, X, Q_{\mathtt{A}}) \\ = \; & I(Q_{\mathtt{B}}; X, Q_{\mathtt{A}}|Y, \Pi^{i-1}) - I(Q_{\mathtt{B}}; X, Q_{\mathtt{A}}|Y, \Pi^i). \end{aligned}$$

Thus

$$\begin{aligned} I(\Pi_i; Q_{\mathtt{B}}|Y, \Pi^{i-1}) &= I(\Pi_i; Q_{\mathtt{B}}|Y, \Pi^{i-1}, X, Q_{\mathtt{A}}) + I(Q_{\mathtt{B}}; X, Q_{\mathtt{A}}|Y, \Pi^{i-1}) - I(Q_{\mathtt{B}}; X, Q_{\mathtt{A}}|Y, \Pi^i) \\ &= 0, \end{aligned} \tag{21}$$

where the first term of (21) is 0 by (12), and the second and third terms are 0 since $Q_{\mathtt{B}} \perp (X, Q_{\mathtt{A}})$ and by the monotinicity of correlation property of communication protocols (Proposition 2.2).

It follows in a similar manner that for $i \in \mathcal{E}^r$, $I(\Pi_i : Q_{\mathtt{A}} | Y\Pi^{i-1}) = 0$. Therefore, we obtain from (18) and (21) that

$$\alpha = \mathrm{IC}^{\mathrm{ext}}_{\nu}(\Pi) - \mathrm{IC}^{\mathrm{ext}}_{\mu}(\Pi) = \mathrm{IC}^{\mathrm{int}}_{\nu}(\Pi) - \mathrm{IC}^{\mathrm{int}}_{\mu}(\Pi) = \sum_{i \in \mathcal{O}^r} I(\Pi_i; Q_{\mathtt{A}} | \Pi^{i-1} X) + \sum_{i \in \mathcal{E}^r} I(\Pi_i; Q_{\mathtt{B}} | \Pi^{i-1} Y).$$

□

Now we may prove the converse direction of Theorem 3.4, i.e., Theorem 3.10.

Proof of Theorem 3.10. Fix a source $(X, Y) \sim \mu$ and any $C \geq 0$. By definition of $\mathscr{C}_r^{\mathtt{am\text{-}cr}}(\cdot)$, for any $L < \mathscr{C}_r^{\mathtt{am\text{-}cr}}(C)$, we have that $(C, L) \in \mathcal{T}_r(X, Y)$, i.e., there is a private-coin r-round protocol Π that achieves the rate (C, L). As in Lemma 3.14, we interpret Π as a deterministic protocol with respect to the tuple $(XR_{\mathtt{A}}, YR_{\mathtt{B}})$ (and denote the corresponding joint distribution by ν).

Then by Lemma 3.11, for any $C' > C$ and $L' < \mathscr{C}_r^{\mathtt{am\text{-}cr}}(C)$, there is some N such that there is an r-round protocol Π with inputs $(X^N R_{\mathtt{A}}^N, Y^N R_{\mathtt{B}}^N) \sim \nu^{\otimes N}$ such that $\mathrm{IC}^{\mathrm{ext}}_{\mu^{\otimes N}}(\Pi) \geq L'N$ and $\mathrm{IC}^{\mathrm{int}}_{\mu^{\otimes N}}(\Pi) \leq C'N$. Then by Lemma 3.12, there is an r-round private-coin protocol Π' for the inputs $(XR_{\mathtt{A}}, YR_{\mathtt{B}}) \sim \nu$ such that $\mathrm{IC}^{\mathrm{int}}_{\nu}(\Pi') \leq C'$ and $\mathrm{IC}^{\mathrm{ext}}_{\nu}(\Pi') \geq L'$. It follows from Lemma 3.14 with $Q_{\mathtt{A}} = R_{\mathtt{A}}, Q_{\mathtt{B}} = R_{\mathtt{B}}$ that there is an r-round private-coin protocol Π'' for the inputs $(X, Y) \sim \mu$ such that $\mathrm{IC}^{\mathrm{int}}_{\mu}(\Pi'') \leq C' - \alpha$ and $\mathrm{IC}^{\mathrm{ext}}_{\mu}(\Pi'') \geq L' - \alpha$, for some $\alpha \geq 0$.

By definition of $\mathcal{T}_r^{\mathrm{d}}(X, Y)$, it follows that $(C' - \alpha, L' - \alpha) \in \mathcal{T}_r^{\mathrm{d}}(X, Y)$; in particular, $\tilde{\mathscr{C}}_r^{\mathtt{am\text{-}cr}}(C' - \alpha) \geq L' - \alpha$. By Lemma 3.13, it follows that $\tilde{\mathscr{C}}_r^{\mathtt{am\text{-}cr}}(C') \geq L'$, or that for any $L'' < L$, $(C', L'') \in \mathcal{T}_r^{\mathrm{d}}(X, Y)$. By taking $C' \to C, L' \to \mathscr{C}_r^{\mathtt{am\text{-}cr}}(C)$, it follows by continuity of $\tilde{\mathscr{C}}_r^{\mathtt{am\text{-}cr}}(C)$ (Lemma 3.13) that $\tilde{\mathscr{C}}_r^{\mathtt{am\text{-}cr}}(C) \geq L$. Since $L < \mathscr{C}_r^{\mathtt{am\text{-}cr}}(C)$ is arbitrary, we get $\tilde{\mathscr{C}}_r^{\mathtt{am\text{-}cr}}(C) \geq \mathscr{C}_r^{\mathtt{am\text{-}cr}}(C)$, as desired. □

4 Rounds-Communication Tradeoffs in Non-Amortized Setting

In this section, our main goal is to prove Theorems 4.1 and 4.2, which establish tradeoffs between the communication cost and number of rounds of CRG and SKG prtocols from the source $\mu_{r,n,\ell}$ in the non-amortized setting. To see the difference between the theorems, we focus on CRG for simplicity, and note that for constant r, the tuple $(O(\log n), \ell)$ is r-achievable from the source $\mu_{r,n,\ell}$ (recall that this means that there is a protocol with communication $O(\log n)$ and which agrees on common random strings of entropy ℓ). Theorem 4.1 implies that if the protocol is only allowed to use $\lfloor (r+1)/2 \rfloor$ rounds, then in order to agree on common random strings of entropy ℓ, the protocol must communicate at least $\tilde{\Omega}(\min\{\ell, n\})$ bits total. Theorem 4.2 gives a tighter dependence on the number of rounds, but a weaker dependence on communication: it implies that if the protocol is allowed to use up to r rounds, then it must communicate at least $\tilde{\Omega}(\min\{\ell, \sqrt{n}\})$ bits to agree on common randomness of entropy ℓ.

Theorem 4.1 (Thms. 1.1 & 1.2 of [BGGS19])**.** *For each $r \in \mathbb{N}, \epsilon \in [0, 1)$, there exists $\eta > 0$, $\beta < \infty$, $n_0 \in \mathbb{N}$ such that for any $n \geq n_0$ and any $\ell \in \mathbb{N}$, there is a source $\mu_{r,n,\ell}$ such that, in the non-amortized setting:*

1. *The tuple* $((r+2)\lceil \log n \rceil, \ell, 0)$ *is* $(r+2)$*-achievable for SKG from* $\mu_{r,n,\ell}$ *(and thus* $((r+2)\lceil \log n \rceil, \ell)$ *is* $(r+2)$*-achievable for CRG).*

2. *For any* $L \in \mathbb{N}$ *and* $C \leq \min\{\eta L - \beta, n/\log^{\beta} n\}$*, the tuple* (C, L, ϵ) *is not* $\lfloor (r+1)/2 \rfloor$*-achievable for CRG (and thus the tuple* (C, L, ϵ, δ) *is not* $\lfloor (r+1)/2 \rfloor$*-achievable for SKG for all* $\delta \geq 0$*).*

Theorem 4.2 (Tighter round dependence than Theorem 4.1)**.** *For each* $r \in \mathbb{N}, \epsilon \in [0,1)$*, there exists* $\eta > 0$*,* $\beta < \infty$*,* $n_0 \in \mathbb{N}$ *such that for any* $n \geq n_0$ *and any* $\ell \in \mathbb{N}$*, there is a source* $\mu_{r,n,\ell}$ *such that, in the non-amortized setting:*

1. *The tuple* $((r+2)\lceil \log n \rceil, \ell, 0)$ *is* $(r+2)$*-achievable for SKG from* $\mu_{r,n,\ell}$ *(and thus* $((r+2)\lceil \log n \rceil, \ell)$ *is* r*-achievable for CRG).*

2. *For any* $L \in \mathbb{N}$*,* $C \leq \min\{\eta L - \beta, \sqrt{n}/\log^{\beta} n\}$*, the tuple* (C, L, ϵ) *is not* r*-achievable for CRG from* $\mu_{r,n,\ell}$ *(and thus for any* $\delta \geq 0$*, the tuple* (C, L, ϵ, δ) *is not* r*-achievable for SKG).*

4.1 Pointer chasing source

Next we define the source $\mu_{r,n,\ell}$ referred to in Theorems 4.1 and 4.2; we refer to it as the *pointer chasing source* due to its similarity to the distributions used in [NW93] to prove round hierarchy results for the communication complexity of functional problems.

Definition 4.1 (The Pointer Chasing Source $\mu_{r,n,\ell}$, [BGGS19])**.** For positive integers r, n and ℓ, the support of $\mu = \mu_{r,n,\ell}$ is $(\mathcal{S}_n^{\lceil r/2 \rceil} \times \{0,1\}^{n\ell}) \times ([n] \times \mathcal{S}_n^{\lfloor r/2 \rfloor} \times \{0,1\}^{n\ell})$. Denoting $X = (\Sigma_1, \Sigma_3, \ldots, \Sigma_{2\lceil r/2 \rceil - 1}, A_1, \ldots, A_n)$ and $Y = (I, \Sigma_2, \Sigma_4, \ldots, \Sigma_{2\lfloor r/2 \rfloor}, B_1, \ldots, B_n)$, a sample $(X, Y) \sim \mu$ is drawn as follows:

- $I \in [n]$ and $\Sigma_1, \ldots, \Sigma_r \in \mathcal{S}_n$ are sampled uniformly and independently.
- Let $J = \Sigma_r(\Sigma_{r-1}(\cdots \Sigma_1(I) \cdots)) \in [n]$.
- $A_J = B_J \in \{0,1\}^{\ell}$ is sampled uniformly and independently of I and Σ's.
- For every $k \neq J$, $A_k \in \{0,1\}^{\ell}$ and $B_k \in \{0,1\}^{\ell}$ are sampled uniformly and independently.

See also Figure 2.

We use the following notation convention for samples $(X, Y) \sim \mu_{r,n,\ell}$. We write $I_0 := I$, and for $1 \leq t \leq r$, $I_t := \Sigma_t(I_{t-1})$. Similarly, we write $J_0 := J$, and for $1 \leq t \leq r$, $J_{t-1} = \Sigma_t^{-1}(J_t)$. Over the distribution $\mu_{r,n,\ell}$, we thus have $I_t = J_{r-t}$ for $0 \leq t \leq r$ with probability 1.

We establish the following basic property of the pointer chasing source $\mu_{r,n,\ell}$ for future reference:

Lemma 4.3. *When* $(X, Y) \sim \mu_{r,n,\ell}$*,* $I(X;Y) = \ell$*.*

Proof. Notice that $H(X) = r\log(n!) + n\ell$ since $\Sigma_1, \Sigma_3, \ldots, \Sigma_{2\lceil r/2 \rceil - 1}$ are uniformly random in $\mathcal{S}_n$ and $A_1, \ldots, A_n$ are uniformly random in $\{0,1\}^{\ell}$. Moreover,

$$\begin{aligned} H(X|Y) &= H(\Sigma_1, \Sigma_3, \ldots, \Sigma_{2\lceil r/2 \rceil - 1}, A_1, \ldots, A_n | Y) \\ &= H(\Sigma_1, \ldots, \Sigma_{2\lceil r/2 \rceil - 1} | Y) + H(A_1, \ldots, A_n | Y, \Sigma_1, \ldots, \Sigma_{2\lceil r/2 \rceil - 1}) \\ &= r\log(n!) + (n-1)\ell. \end{aligned}$$

□

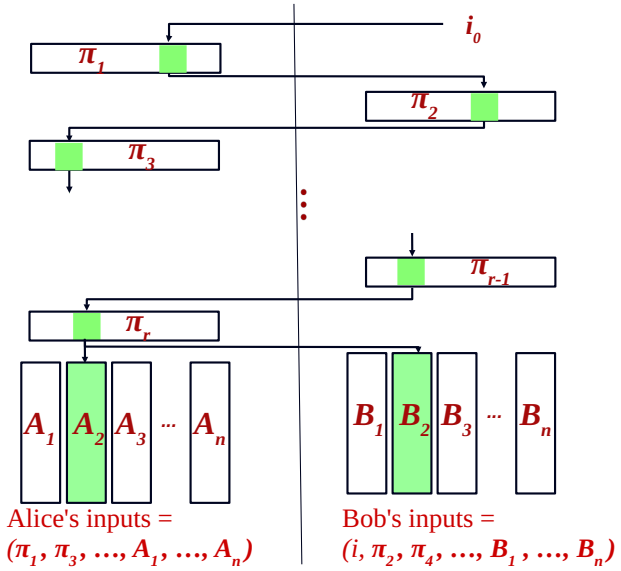

Figure 2: The pointer chasing source $\mu_{r,n,\ell}$ of Definition 4.1

It is immediate from the definition of $\mu_{r,n,\ell}$ that part (1) (i.e., the upper bound) of both Theorems 4.1 and 4.2 holds:

Lemma 4.4 (Upper bound for Theorems 4.1 & 4.2)**.** *For every r, n, ℓ, the tuple $((r+2)\lceil \log n \rceil, \ell, 0)$ is $(r+2)$-achievable for SKG (and thus $((r+2)\lceil \log n \rceil, \ell)$ is $(r+2)$-achievable for CRG) from $\mu_{r,n,\ell}$.*

Proof. Consider the protocol in which Alice sends Bob an arbitrary bit in the first round, and in round $t+1$, for $1 \leq t \leq r$, the next party to speak sends over $I_t = \Sigma_t(I_{t-1}) \in [n]$, which takes log n bits. Then Alice outputs A_{I_r} as her key and Bob outputs B_{I_r} (which is equal to A_{I_r} with probability 1 over $\mu_{r,n,\ell}$) as his key. By construction of $\mu_{r,n,\ell}$, $A_{I_r} = B_{I_r}$ is independent of $I_1, \ldots, I_r$, which is the transcript of the protocol. □

The main content of Theorems 4.1 and 4.2 is then in part (2) (i.e., the lower bound) of each; its proof, for both theorems, proceeds via arguments about indistinguishbility of inputs to protocols, which we now define:

Definition 4.2 ((r, C) protocols)**.** For $r, C \in \mathbb{R}_+$, we say that a communication protocol Π is an (r, C) *protocol* if Π has at most $\lfloor r \rfloor$ rounds and communication cost at most $\lfloor C \rfloor$.

Definition 4.3 (Indistinguishability)**.** Let $0 \leq \epsilon \leq 1$. Two distributions μ_1, μ_2 on pairs (X, Y) are *ϵ-distinguishable* to a protocol Π if the distribution of the transcript Π^r when $(X, Y) \sim \mu_1$ has total variation distance at most ϵ from the distribution of Π^r when $(X, Y) \sim \mu_2$.

Two distributions μ_1, μ_2 are *(ϵ, C, r)-indistinguishable* if they are ϵ-indistinguishable to every (r, C) protocol. The distributions μ_1, μ_2 are *(ϵ, C, r)-distinguishable* if they are not (ϵ, C, r)-indistinguishable. If Π is a protocol such that the total variation distance of the transcript between inputs $(X, Y) \sim \mu_1$ and inputs $(X, Y) \sim \mu_2$ is at least ϵ, then we say that Π distinguishes between μ_1 and μ_2 *with advantage* ϵ.

Proposition 4.5 reduces the problem of showing that certain tuples (C, L) are not achievable for CRG from $\mu_{r,n,\ell}$ to that of showing indistinguishability of $\mu_{r,n,\ell}$ from the product of its marginals $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$.

Proposition 4.5 ([BGGS19], Propositions 3.3 & 3.4)**.** *There are positive constants η, ξ such that the following holds. Suppose $\rho, C, L \in \mathbb{N}$ and $0 < \gamma < 1$. Suppose that $C < \eta L - 3/2 \cdot \log 1/\gamma - \xi$ and that the tuple $(C, L, 1-\gamma)$ is ρ-achievable for CRG from the source $\mu_{r,n,\ell}$. Then there is some $N \in \mathbb{N}$ such that $\mu_{r,n,N\ell}$ and $(\mu_{r,n,N\ell})_X \otimes (\mu_{r,n,N\ell})_Y$ are $(\gamma/10, C + \xi \log 1/\gamma, \rho + 1)$-distinguishable.*

Proof sketch. The crucial ingredient in the proof of Proposition 4.5 is the fact [CGMS17, Theorem 2.6] that there is a constant $\eta > 0$ such that for any $\rho, L \in \mathbb{N}$ and $\epsilon \in [0, 1)$, the tuple $(\eta L - 3/2 \log(1/(1-\epsilon)) - O(1), L, \epsilon)$ is not ρ-achievable from any product source distribution, so in particular from the source $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$. Using the assumption in the proposition about achievable tuples from $\mu_{r,n,\ell}$, Alice and Bob can distinguish $\mu_{r,n,N\ell}$ from the product of its marginals by running the protocol for CRG from the source $\mu_{r,n,\ell}$ and checking whether the resulting keys agree and have high entropy (i.e., represent valid CRG). If so, then the parties decide that the source is $\mu_{r,n,N\ell}$, and if not, then the parties decide that the source is $(\mu_{r,n,N\ell})_X \otimes (\mu_{r,n,N\ell})_Y$. The details (including the role of N) are unimportant and we refer the reader to [BGGS19] for a full proof. □

Using Proposition 4.5, the proofs of Theorems 4.1 and 4.2, respectively, follow from Theorems 4.6 and 4.7 below:

Theorem 4.6 ([BGGS19], Lemma 4.5)**.** *For every $\epsilon > 0$ and odd r there exists β, n_0 such that for every $n \geq n_0$ and ℓ, the distributions $\mu = \mu_{r,n,\ell}$ and $\mu_X \otimes \mu_Y$ are $(\epsilon, (r+3)/2, n/\log^\beta n)$-indistinguishable.*

Theorem 4.7. *For every $\epsilon > 0$ and $r \in \mathbb{N}$ there exists β, n_0 such that for every $n \geq n_0$ and ℓ, the distributions $\mu = \mu_{r,n,\ell}$ and $\mu_X \otimes \mu_Y$ are $(\epsilon, r+1, \sqrt{n}/\log^\beta n)$-indistinguishable.*

We present the proof of Theorem 4.2 below; the proof of Theorem 4.1 is omitted since it is very similar, and can be found in [BGGS19].

Proof of Theorem 4.2. Recall that item (1) of Theorem 4.2 was shown in Lemma 4.4, so we only have to prove item (2).

Fix $\epsilon > 0$ and $r \in \mathbb{N}$. Let ξ, η be the constants from Proposition 4.5. Also let β_0 be the constant β from Theorem 4.7 with $(1-\epsilon)/20$ as the variational distance parameter. Also let β be a constant such that $\beta > \max\{\beta_0, 3/2 \cdot \log 1/(1-\epsilon) + \xi\}$ and $\sqrt{n}/\log^\beta n + \xi \log 1/(1-\epsilon) \leq \sqrt{n}/\log^{\beta_0} n$, which is possible for sufficiently large n. Suppose for purpose of contradiction that for some $L > 0$, the tuple $(\min\{\eta L - \beta, \sqrt{n}/\log^\beta n\}, L, \epsilon)$ were r-achievable for CRG from $\mu_{r,n,\ell}$. Since $\beta > 3/2 \log 1/(1-\epsilon) + \xi$, it follows from Proposition 4.5 that for some $N \in \mathbb{N}$, $\mu_{r,n,\ell N}$ and $(\mu_{r,n,\ell N})_X \otimes (\mu_{r,n,\ell N})_Y$ are $((1-\epsilon)/10, \sqrt{n}/\log^{\beta_0} n, r+1)$-distinguishable. But this contradictions Theorem 4.7, which states that $(\mu_{r,n,\ell N})_X \otimes (\mu_{r,n,\ell N})_Y$ are $((1-\epsilon)/20, \sqrt{n}/\log^{\beta_0} n, r+1)$-indistinguishable. □

4.2 Proving indistinguishability of $\mu_{r,n,\ell}$ and $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$

Next we work towards the proofs of Theorems 4.6 and 4.7. The proofs proceed by eliminating each of two possible strategies Alice and Bob can use to distinguish $\mu_{r,n,\ell}$ and $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$: first,

they can try to follow the chain of pointers, compute I_r, and check if $A_{I_r} = B_{I_r}$ (which is true with probability 1 under $\mu_{r,n,\ell}$ but only with probability $1/2^\ell$ under $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$). Computing I_r, however, with fewer than $r+2$ rounds requires communication $\Omega(n)$ by standard results for the pointer chasing problem [NW93]. Alternatively, Alice and Bob can ignore the chain of pointers and try to determine if there is *any* i such that $A_i = B_i$ (under the product distribution the probability that such an i exists is at most $n/2^\ell \ll 1$). Determining the existence of such an i is no easier than solving the set disjointness problem [Raz92], which requires communcation $\Omega(n)$, as we show below. However, combining the pointer chasing and set disjointness lower bounds takes some care. We begin by recalling the $\Omega(n)$ lower bound on the communication complexity of disjointness:

Theorem 4.8 ([Raz92])**.** *For every $\epsilon > 0$ there exists $\delta > 0$ such that for all n the following holds. Let $\mathrm{Disj}^{\mathrm{Y}} = \mathrm{Disj}^{\mathrm{Y}}_n$ (respectively, $\mathrm{Disj}^{\mathrm{N}} = \mathrm{Disj}^{\mathrm{N}}_n$) denote the uniform distribution on pairs (U,V) with $U,V \subseteq [n]$ and $|U| = |V| = n/4$ such that $|U \cap V| = 1$ (respectively, $|U \cap V| = 0$). Then if Alice gets U and Bob gets V as inputs, $\mathrm{Disj}^{\mathrm{Y}}$ and $\mathrm{Disj}^{\mathrm{N}}$ are $(\epsilon, \delta n, \delta n)$-indistinguishable to Alice and Bob.*

For Theorem 4.7 we will need the following corollary.

Corollary 4.9. *For every $\epsilon > 0$ there exists $\delta > 0$ such that for all n the following holds. Let $\mathrm{Disj}^{\mathrm{Y}}_{n,\sqrt{n}}$ (respectively, $\mathrm{Disj}^{\mathrm{N}}_{n,\sqrt{n}}$) denote the uniform distribution on pairs (U,V) with $U,V \subseteq [n]$ and $|U| = |V| = n/4$ such that $|U \cap V| = \lfloor \sqrt{n} \rfloor$ (respectively, $|U \cap V| = 0$). Then if Alice gets U and Bob gets V as inputs, $\mathrm{Disj}^{\mathrm{Y}}_{n,\sqrt{n}}$ and $\mathrm{Disj}^{\mathrm{N}}_{n,\sqrt{n}}$ are $(\epsilon, \delta\sqrt{n}, \delta\sqrt{n})$-indistinguishable to Alice and Bob.*

Proof. A protocol Π that distinguishes $\mathrm{Disj}^{\mathrm{Y}}_{n^2,n}$ and $\mathrm{Disj}^{\mathrm{N}}_{n^2,n}$ with communication C may be converted into a protocol Π' with communication C that distinguishes $\mathrm{Disj}^{\mathrm{Y}}_n$ and $\mathrm{Disj}^{\mathrm{N}}_n$ with advantage ϵ. In particular, the protocol Π' proceeds as follows: given inputs (U,V), $|U| = n/4, |V| = n/4$, Alice and Bob construct an instance (U',V'), that is distributed according to $\mathrm{Disj}^{\mathrm{Y}}_{n^2,n}$ if $(U,V) \sim \mathrm{Disj}^{\mathrm{Y}}_n$ and that is distributed according to $\mathrm{Disj}^{\mathrm{N}}_{n^2,n}$ if $(U,V) \sim \mathrm{Disj}^{\mathrm{N}}_n$. In particular, Alice and Bob first construct sets $(\tilde{U},\tilde{V})$ as follows: for each $u \in U \subset [n]$, Alice places the elements $(u-1)n + j$, for $1 \le j \le n\}$ in $\tilde{U}$, and Bob constructs $\tilde{V}$ in an analogous fashion. Then, using public randomness, they randomly permute the elements of $\tilde{U}, \tilde{V}$ (according to the same permutation) to obtain sets U', V'. It is clear that $|\tilde{U}| = |\tilde{V}| = |U'| = |V'| = n \cdot |U| = n^2/4$. Moreover, if $|U \cap V| = 0$, then $|\tilde{U} \cap \tilde{V}| = |U' \cap V'| = 0$, and if $|U \cap V| = 1$, then $|U' \cap V'| = n = \sqrt{n^2}$.

By Theorem 4.8, for any $\epsilon > 0$, there is $\delta > 0$ such that the protocol Π' must have communication at least δn. Thus the protocol Π must have communication at least $\delta n = \sqrt{\delta^2 n^2}$.

It follows in a similar manner as the above argument that any protocol Π distinguishing $\mathrm{Disj}^{\mathrm{Y}}_{n',n}$ and $\mathrm{Disj}^{\mathrm{N}}_{n',n}$ with $n^2 \le n' < (n+1)^2$ with communication C may be converted into a protocol Π' with communication C that distinguishes $\mathrm{Disj}^{\mathrm{Y}}_n$ and $\mathrm{Disj}^{\mathrm{N}}_n$ with advantage ϵ. This completes the proof of the corollary even for non-perfect squares n. □

Next we state the second main ingredient in the proof of Theorems 4.7 and 4.6, which is a hardness result for a certain version of the pointer chasing problem. We call this problem the *pointer verification (PV)* problem. The main difference with pointer chasing is that Alice and Bob receive as inputs a final pointer J_0 in addition to the initial pointer I_0, and the goal is to determine if $\Sigma_r \circ \cdots \Sigma_1(I_0) = J_0$. We define a distinguishability version of this problem below:

Definition 4.4 ([BGGS19])**.** Let $r, n \in \mathbb{N}$ with r odd. Then the distributions $D^{\mathrm{Y}}_{\mathrm{PV}} = D^{\mathrm{Y}}_{\mathrm{PV}}(r,n)$ and $D^{\mathrm{N}}_{\mathrm{PV}} = D^{\mathrm{N}}_{\mathrm{PV}}(r,n)$ are both supported on $((\mathcal{S}_n^{\lceil r/2 \rceil}) \times ([n]^2 \times S_n^{\lfloor r/2 \rfloor})$, and are defined as follows:

- $D^{\mathrm{N}}_{\mathrm{PV}}$ is the uniform distribution on $((\mathcal{S}_n^{\lceil r/2 \rceil}) \times ([n]^2 \times S_n^{\lfloor r/2 \rfloor})$.
- $(X, Y) \sim D^{\mathrm{Y}}_{\mathrm{PV}}$, with $X = (\Sigma_1, \Sigma_3, \ldots, \Sigma_r), Y = (I_0, J_0, \Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1})$ is sampled by letting $\Sigma_1, \Sigma_2, \ldots, \Sigma_r$ be independent and uniform over $\mathcal{S}_n$, letting $I_0 \in [n]$ be uniform and independent of the Σ_t, and setting $J_0 = \Sigma_r \circ \cdots \circ \Sigma_1(I_0)$.

Notice that with $(r+5)/2$ rounds of communication, by communicating at most $1+(r+1)\lceil \log n \rceil$ bits, Alice and Bob can distinguish between $D^{\mathrm{Y}}_{\mathrm{PV}}(r,n)$ and $D^{\mathrm{N}}_{\mathrm{PV}}(r,n)$ with advantage $1 - 1/n$. In particular, Alice sends Bob an arbitrary bit in the first round, Bob sends I_0, J_0 in the second round, Alice responds with $I_1 = \Sigma_1(I_0)$ and $J_1 = \Sigma_r^{-1}(J_0)$, Bob responds with I_2 and J_2, and so on. After $(r+3)/2$ rounds either Alice or Bob will know both $I_{(r-1)/2}$ and $J_{(r-1)/2}$, and this person sends $\mathbb{1}[\Sigma_{(r+1)/2}(I_{(r-1)/2}) = J_{(r-1)/2}]$ (which is 1 with probability 1 under $D^{\mathrm{Y}}_{\mathrm{PV}}$ and only with probability $1/n$ under $D^{\mathrm{N}}_{\mathrm{PV}}$) as the final bit. Therefore, PV with r permutations is easier than the standard pointer chasing problem, which requires r rounds for a protocol with communication cost $O(\log n)$.

Theorem 4.10 states that if Alice and Bob are only allowed 1 fewer round, then they must communicate exponentially more bits to distinguish $D^{\mathrm{Y}}_{\mathrm{PV}}$ and $D^{\mathrm{N}}_{\mathrm{PV}}$:

Theorem 4.10 ([BGGS19], Theorem 4.2)**.** *For every $\epsilon > 0$ and odd r there exists β, n_0 such for every $n \geq n_0$, $D^{\mathrm{Y}}_{\mathrm{PV}}(r,n)$ and $D^{\mathrm{N}}_{\mathrm{PV}}(r,n)$ are $(\epsilon, (r+3)/2, n/\log^{\beta} n)$-indistinguishable.*

Using Theorem 4.10 and Corollary 4.9, we now prove Theorem 4.7.

Proof of Theorem 4.7. We introduce a new distribution, which we denote by $\hat{\mu}$ (or $\hat{\mu}_{r,n,\ell}$ when we want to emphasize dependence on r, n, ℓ); $\hat{\mu}$ is a distribution supported on $(\mathcal{S}_n^{\lceil r/2 \rceil} \times (\{0,1\}^\ell)^n \times (\mathcal{S}_n^{\lfloor r/2 \rfloor} \times [n] \times (\{0,1\}^\ell)^n)$. We denote a sample from $\hat{\mu}$ by (X, Y), with

$$X = (\Sigma_1, \Sigma_3, \ldots, \Sigma_{2\lceil r/2 \rceil - 1}, A_1, \ldots, A_n), \quad Y = (i, \Sigma_2, \Sigma_4, \ldots, \Sigma_{2\lfloor r/2 \rfloor}, B_1, \ldots, B_n),$$

which is distributed as follows:

- $I_0 \in [n]$ and $\Sigma_1, \ldots, \Sigma_r \in \mathcal{S}_n$ are sampled uniformly and independently. Let $I_r = \Sigma_r \circ \cdots \circ \Sigma_1(I_0)$.
- Let $P \subset [n]$ be a uniformly random subset of size $\lfloor \sqrt{n} \rfloor$, conditioned on the event that it contains I_r.
- For every $j \in P$, $A_j = B_j \in \{0,1\}^L$ is sampled uniformly and independently of i, Σ's, and P.
- For every $j \notin P$, $A_j, B_j \in \{0,1\}^L$ are sampled uniformly and independently (and independently of all Σ's, j, and P).

Claim 4.11. *For every $\epsilon > 0$, there exists $\delta > 0$ such that the distributions $\mu_{r,n,\ell}$ and $\hat{\mu}_{r,n,\ell}$ are $(\epsilon, \delta\sqrt{n}, \delta\sqrt{n})$-indistinguishable.*

Proof of Claim 4.11. We show that any protocol Π with $\mathrm{CC}(\Pi) \le C$ distinguishing $\mu = \mu_{r,n,\ell}$ and $\hat{\mu} = \hat{\mu}_{r,n,\ell}$ with advantage ϵ can be converted into a protocol Π' with $\mathrm{CC}(\Pi') \le C$ and which distinguishes $\mathrm{Disj}^{\mathrm{Y}}_{n,\sqrt{n}}$ and $\mathrm{Disj}^{\mathrm{N}}_{n,\sqrt{n}}$ (as in Corollary 4.9) with advantage ϵ.

The protocol Π' proceeds as follows: suppose Alice and Bob are given sets U, V, respectively, with $U, V \subseteq [n]$. Let $m = (\lfloor \sqrt{n} \rfloor + 1)^2$. Using public randomness, Alice and Bob sample a random injective function $\tau : [n] \to [m]$, and set $U' = \{\tau(u) : u \in U\}, V' = \{\tau(v) : v \in V\}$. Let $J_0 \in [m]$ denote the sole index not in the image of τ. Using public randomness, Alice and Bob sample r permutations $\Sigma_1, \dots, \Sigma_r \in S_m$ uniformly and independently, and let $I_0 = (\Sigma_r \circ \cdots \circ \pi_1)^{-1}(J_0)$. They also sample $3m$ strings $A_1, \dots, A_m, B_1, \dots, B_m, C_1, \dots, C_m \in \{0,1\}^\ell$ uniformly and independently using public randomness. Then for $1 \le u \le m$, Alice sets:

$$A'_u := \begin{cases} A_u & : u \notin U' \\ C_u & : u \in U', \end{cases}$$

and Bob sets:

$$B'_u := \begin{cases} B_u & : u \notin U' \\ C_u & : u \in U'. \end{cases}$$

It is now clear that the tuple

$$((\Sigma_1, \Sigma_3, \dots, \Sigma_r, A'_1, A'_2, \dots, A'_m), (I_0, \Sigma_2, \Sigma_4, \dots, \Sigma_{r-1}, B'_1, B'_2, \dots, B'_m)) \tag{22}$$

is distributed according to $\mu_{r,m,\ell}$ if $(U, V) \sim \mathrm{Disj}^{\mathrm{N}}_{n,\sqrt{n}}$ and is distributed according to $\hat{\mu}_{r,m,\ell}$ if $(U, V) \sim \mathrm{Disj}^{\mathrm{Y}}_{n,\sqrt{n}}$. Now Alice and Bob run the protocol Π with their inputs as in (22).

By Corollary 4.9, for each $\epsilon > 0$, there exists $\delta > 0$ such that $\mu_{r,m,\ell}$ and $\hat{\mu}_{r,m,\ell}$ are $(\epsilon, \delta\sqrt{n}, \delta\sqrt{n})$-indistinguishable. Using that $\sqrt{m} - \sqrt{n} = O(1)$, the lemma statement follows. □

Next, notice that the two distributions $(\mu_{r,n,\ell})_X \otimes (\mu_{r,n,\ell})_Y$ and $(\hat{\mu}_{r,n,\ell})_X \otimes (\hat{\mu}_{r,n,\ell})_Y$ are identical. Thus by Claim 4.11 and the triangle inequality for total variation distance, Theorem 4.7 will follow from the following claim:

Claim 4.12. *For every $\epsilon > 0$ and $r \in \mathbb{N}$ there exists β, n_0 such that for every $n \ge n_0$ and ℓ, the distributions $\hat{\mu} = \hat{\mu}_{r,n,\ell}$ and $\hat{\mu}_X \otimes \hat{\mu}_Y$ are $(2\epsilon, r+1, \sqrt{n}/\log^\beta n)$-indistinguishable.*

We next introduce a distribution $\mu^{\mathrm{mid}} = \mu^{\mathrm{mid}}_{r,n,\ell}$, which is the same as $\hat{\mu}_{r,n,\ell}$, except the distribution of the uniformly random subset $P \subset [n]$ with $|P| = \lfloor \sqrt{n} \rfloor$ is not conditioned on the event that it contains I_r (i.e. it is drawn uniformly at random from the set of all $\sqrt{n}$-element sets, independent of $I_0, \Sigma_1, \dots, \Sigma_r$). Thus, with probability at least $1 - 1/\sqrt{n}$, $I_r \notin P$ under μ^{mid}. Now Claim 4.12 follows directly from the triangle inequality and Claims 4.13 and 4.14 below.

Claim 4.13. *For every $\epsilon > 0$ and $r \in \mathbb{N}$ there exists $\beta, n_0 \in \mathbb{R}_+$ such that for all integers $n \ge n_0$ and ℓ, the distributions $\hat{\mu}_{r,n,\ell}$ and $\mu^{\mathrm{mid}}_{r,n,\ell}$ are $(\epsilon, r+1, \sqrt{n}/\log^\beta n)$-indistinguishable.*

Claim 4.14. *For every $\epsilon > 0$, there exists $\delta > 0$ such that $\mu^{\mathrm{mid}}_{r,n,\ell}$ and $(\hat{\mu}_{r,n,\ell})_X \otimes (\hat{\mu}_{r,n,\ell})_Y$ are $(\epsilon, \delta\sqrt{n}, \delta\sqrt{n})$-indistinguishable for all $n \in \mathbb{N}$.*

Now we prove each of Claims 4.13 and 4.14 in turn.

Proof of Claim 4.13. We first prove the statement of the claim for the case that n is a perfect square. Fix r, n, ℓ, and suppose that Π is a ρ-round protocol ($\rho \in \mathbb{N}$) with communication at most C that distinguishes between $\hat{\mu}_{r,n^2,\ell}$ from $\mu^{\text{mid}}_{r,n^2,\ell}$ with advantage ϵ. (Notice that we are replacing n with n^2 in the notation.)

We now construct a protocol Π' with the same number of rounds and communication as Π and which distinguishes between $D^{\text{Y}}_{\text{PV}}(2r-1,n)$ and $D^{\text{N}}_{\text{PV}}(2r-1,n)$ with advantage at least ϵ. Suppose Alice and Bob are given inputs $X = (\Sigma_1, \Sigma_3, \ldots, \Sigma_{2r-1})$ and $Y = (I_0, J_0, \Sigma_2, \Sigma_4, \ldots, \Sigma_{2r-2})$, respectively, which are distributed according to $D^{\text{Y}}_{\text{PV}}(2r-1,n)$ or $D^{\text{N}}_{\text{PV}}(2r-1,n)$. Next, for $1 \le t \le r-1$, let $\Sigma'_t = \Sigma_t$, and for $r+2 \le t \le 2r$, let $\Sigma'_t = \Sigma_{t-1}$. Finally let $\Sigma'_r, \Sigma'_{r+1} \in \mathcal{S}_n$ be uniformly random conditioned on $\Sigma'_{r+1} \circ \Sigma'_r = \Sigma_r$. Notice that each Σ'_t, $1 \le t \le 2r$ may be computed by either Alice or Bob. Next, interpret $[n^2] \simeq [n] \times [n]$, so that any pair $\sigma, \tau \in \mathcal{S}_n$ of permutations on $[n]$ determines a permutation on $[n^2]$, which we denote by $\sigma || \tau$, so that $(\sigma||\tau)((i,j)) = (\sigma(i), \tau(j))$. (Note that the vast majority of permutations on $[n^2]$ cannot be obtained in this manner, however.) The protocol Π' proceeds as follows:

1. Alice and Bob use their common randomness to generate uniformly random permutations $\tau_0, \tau_1, \ldots, \tau_r \in S_{n^2}$ and uniformly random strings $A_1, \ldots, A_{n^2-n}, B_1, \ldots, B_{n^2-n}, C_1, \ldots, C_n \in \{0,1\}^\ell$.
2. Bob computes $\hat{I}_0 := \tau_1((I_0, J_0)) \in [n] \times [n] \simeq [n^2]$.
3. For $t = 1, 3, \ldots, 2\lfloor (r+1)/2 \rfloor$, Alice computes $\hat{\Sigma}_t := \tau_t \circ (\Sigma'_t || (\Sigma'_{2r+1-t})^{-1}) \circ \tau_{t-1}^{-1} \in S_{n^2}$.
4. For $t = 2, 4, \ldots, 2\lfloor r/2 \rfloor$, Bob computes $\hat{\Sigma}_t := \tau_t \circ (\Sigma'_t || (\Sigma'_{2r+1-t})^{-1}) \circ \tau_{t-1}^{-1} \in S_{n^2}$.
5. For $1 \le i \le n$, Alice and Bob set $\hat{A}_{\tau_r((i,i))} = \hat{B}_{\tau_r((i,i))} = C_i$.
6. For the $n^2 - n$ pairs $(i,j) \in [n] \times [n]$ with $i \ne j$, Alice sets $\hat{A}_{(i,j)}$ to be equal to one of the A_k, $1 \le k \le n^2 - n$ so that each A_k is used once. Bob does the same with $\hat{B}_{(i,j)}$ with respect to the B_k.
7. Alice and Bob now run the protocol Π on the inputs $\hat{X} := (\hat{\Sigma}_1, \hat{\Sigma}_3, \ldots, \hat{\Sigma}_{2\lfloor (r+1)/2 \rfloor}, \hat{A}_1, \ldots, \hat{A}_{n^2})$ and $\hat{Y} := (\hat{I}_0, \hat{\Sigma}_2, \hat{\Sigma}_4, \ldots, \hat{\Sigma}_{2\lfloor r/2 \rfloor}, \hat{B}_1, \ldots, \hat{B}_{n^2})$.

Certainly the communication cost and number of rounds of Π' are both the same as the communication cost and number of rounds, respectively, of Π.

We will show that (1) if $(X,Y) \sim D^{\text{Y}}_{\text{PV}}(2r-1,n)$, then $(\hat{X},\hat{Y}) \sim \hat{\mu}_{r,n^2,\ell}$, and (2) if $(X,Y) \sim D^{\text{N}}_{\text{PV}}(2r-1,n)$, then $(\hat{X},\hat{Y}) \sim \mu^{\text{mid}}_{r,n^2,\ell}$.

We first prove (1). Suppose $(X,Y) \sim D^{\text{Y}}_{\text{PV}}(2r-1,n)$. That is, X, Y are uniformly random conditioned on $\Sigma_{2r-1} \circ \cdots \circ \Sigma_1(I_0) = J_0$; therefore,

$$\Sigma'_1, \Sigma'_2, \ldots, \Sigma'_{2r}, I_0, J_0$$

are uniformly random conditioned on $\Sigma'_{2r} \circ \cdots \circ \Sigma'_1(I_0) = J_0$. For $0 \le t \le 2r$, set $I'_t = \Sigma'_t \circ \Sigma'_{t-1} \circ \cdots \circ \Sigma'_1(I_0)$ (so that, in particular, $I'_0 = I_0$). Then the distribution of $\Sigma'_1, \ldots, \Sigma'_{2r}, I_0, J_0$ may be expressed equivalently as follows: X, Y are chosen as follows: $\Sigma'_1, \ldots, \Sigma'_{2r}$ are first drawn uniformly and independently form S_n, an index $I'_r \in [n]$ is chosen uniformly in $[n]$ independent of $\Sigma'_1, \ldots, \Sigma'_{2r}$, and then we set $J_0 = \Sigma'_{2r} \circ \cdots \circ \Sigma'_{r+1}(I'_r)$ and $I_0 = (\Sigma'_1)^{-1} \circ \cdots \circ (\Sigma'_r)^{-1}(I'_r)$.

Notice that the set $P := \{\tau_r((i,i)) : i \in [n]\}$ is a uniformly random set of size n in $[n^2] \simeq [n]\times[n]$. Next, note that if π is any distribution on S_{n^2} and τ is distributed uniformly on S_{n^2}, then $\pi \circ \tau$ is distributed uniformly on S_{n^2}. It follows from this fact $\hat{\Sigma}_1, \dots, \hat{\Sigma}_r$ are distributed uniformly and independently in S_{n^2}, all independent of the set $P = \{\tau_r((i,i)) : i \in [n]\}$. Next, we have that

$$\begin{aligned}
\hat{\Sigma}_r \circ \cdots \circ \hat{\Sigma}_1(\hat{I}_0) &= \tau_r \circ (\Sigma'_r || (\Sigma'_{r+1})^{-1}) \circ \tau_{r-1}^{-1} \circ \tau_{r-1} \circ \cdots \circ \tau_1^{-1} \circ \tau_1 \circ (\Sigma'_1 || (\Sigma'_{2r})^{-1}) \circ \tau_0^{-1} \circ \tau_0((I_0, J_0)) \\
&= \tau_r \circ (\Sigma'_r || (\Sigma'_{r+1})^{-1}) \circ \cdots \circ ((\Sigma'_1) || (\Sigma'_{2r})^{-1})((I_0, J_0)) \\
&= \tau_r((\Sigma'_r \circ \cdots \circ \Sigma'_1(I_0), (\Sigma'_{r+1})^{-1} \circ \cdots \circ (\Sigma'_{2r})^{-1}(J_0))) \\
&= \tau_r((I'_r, I'_r)),
\end{aligned}$$

where we have used the fact that $(X,Y) \sim D^{\mathrm{Y}}_{\mathrm{PV}}(2r-1, n)$ in the last line. Recall from the discussion above that I'_r is independent of $\Sigma'_1, \dots, \Sigma'_{2r}, \tau_0, \dots, \tau_r$, and therefore $\tau_r((I'_r, I'_r))$ is a uniformly random element of the set $P = \{\tau_r((i,i)) : i \in [n]\}$, independent of $\hat{\Sigma}_1, \dots, \hat{\Sigma}_r, P$. Therefore, $\hat{I}_0$ is a uniformly random element of $[2n]$, independent of $P, \hat{\Sigma}_1, \dots, \hat{\Sigma}_r$, conditioned on the event $\hat{\Sigma}_r \circ \cdots \circ \hat{\Sigma}_1(\hat{I}_0) \in P$. This establishes that $(\hat{X}, \hat{Y}) \sim \hat{\mu}_{r,n^2,\ell}$, finishing the proof of point (1).

We next prove (2); suppose that $(X,Y) \sim D^{\mathrm{N}}_{\mathrm{PV}}(2r-1, n)$. Then all of the random variables $\Sigma'_1, \dots, \Sigma'_{2r} \in S_{n^2}$, and $I_0, J_0 \in [n]$ are uniform and independent on their respective domains. Moreover, the set $P := \{\tau_r((i,i)) : i \in [n]\}$ is a uniformly random set of size n in $[n^2] \simeq [n] \times [n]$. Thus $\hat{\Sigma}_1, \dots, \hat{\Sigma}_r \in S_{n^2}$ are uniform and independent in S_{n^2}, independent of P, and $\hat{I}_0 \in [n^2]$ is uniform, independent of $P, \hat{\Sigma}_1, \dots, \hat{\Sigma}_r$. This establishes that in this case $(\hat{X}, \hat{Y}) \sim \mu^{\mathrm{mid}}_{r,n^2,\ell}$.

Thus the distribution of the transcript of Π' (excluding the additional public randomness used by Π' in the simulation above) when run on $D^{\mathrm{Y}}_{\mathrm{PV}}$ (respectively, $D^{\mathrm{N}}_{\mathrm{PV}}$) is the same as the distribution of the transcript of Π when run on $\hat{\mu}_{r,n^2,\ell}$ (respectively, $\mu^{\mathrm{mid}}_{r,n^2,\ell}$). It then follows from Theorem 4.10 and the fact that $((2r-1)+3)/2 = r+1$ that for every $\epsilon > 0$, there exists $\beta, n_0 \in \mathbb{R}_+$ such that for all $\ell \in \mathbb{N}$ and perfect squares $n \geq n_0$, the distributions $\hat{\mu}_{r,n,\ell}$ and $\mu^{\mathrm{mid}}_{r,n,\ell}$ are $(\epsilon, r+1, \sqrt{n}/\log^{\beta} n)$-indistinguishable.

The case that n is not a perfect square follows immediately: in particular, given a sample (X,Y) from either $\hat{\mu}_{r,n,\ell}$ or $\mu^{\mathrm{mid}}_{r,n,\ell}$, let m denote the smallest perfect square greater than n. Notice that by viewing $[n]$ as a subset of $[m]$ and using public randomness Alice and Bob can create a sample (X', Y') that is sampled from $\hat{\mu}_{r,m,\ell}$ if $(X,Y) \sim \hat{\mu}_{r,n,\ell}$ and that is sampled from $\mu^{\mathrm{mid}}_{r,m,\ell}$ if $(X,Y) \sim \mu^{\mathrm{mid}}_{r,n,\ell}$ with no communication. □

Next, Claim 4.14 follows as a simple corollary of Corollary 4.9.

Proof of Claim 4.14. The proof is similar to that of Claim 4.11. We reduce the task of distinguishing $\mu^{\mathrm{mid}}_{r,n,\ell}$ and $(\hat{\mu}_{r,n,\ell})_X \otimes (\hat{\mu}_{r,n,\ell})_Y$ to the task of distinguishing $\mathrm{Disj}^{\mathrm{Y}}_{n,\sqrt{n}}$ and $\mathrm{Disj}^{\mathrm{N}}_{n,\sqrt{n}}$ (See Corollary 4.9).

In particular, suppose Alice and Bob are given $U, V \subseteq [n]$. Alice and Bob share common random uniform strings $Z_1, \dots, Z_n \in \{0,1\}^{\ell}$. Given $U \subset [n]$, Alice sets $A_u = Z_u$ for $u \in U$ and samples $A_u \in \{0,1\}^{\ell}$ uniformly and independently for all $u \in [n] \backslash U$. Similarly, for $V \subset [n]$, Bob sets $B_v = Z_v$ for $v \in V$, and samples $B_v \in \{0,1\}^{\ell}$ uniformly and independently for all $v \in [n] \backslash V$. Alice also samples $\Sigma_1, \Sigma_3, \dots, \Sigma_r \in \mathcal{S}_n$ uniformly and independently and Bob samples $\Sigma_2, \Sigma_4, \dots, \Sigma_{r-1} \in \mathcal{S}_n$, $I, J \in [n]$ uniformly and independently. Letting $X = (\Sigma_1, \Sigma_3, \dots, \Sigma_r, A_1, \dots, A_n)$ and $Y = (I, J, \Sigma_2, \Sigma_4, \dots, \Sigma_{r-1}, B_1, \dots, B_n)$, it is easy to see that $(X,Y) \sim \mu^{\mathrm{mid}}_{r,n,\ell}$ if $(U,V) \sim \mathrm{Disj}^{\mathrm{Y}}_{n,\sqrt{n}}$ and

that $(X,Y) \sim (\hat{\mu}_{r,n,\ell})_X \otimes (\hat{\mu}_{r,n,\ell})_Y$ if $(U,V) \sim \mathrm{Disj}^{\mathrm{N}}_{n,\sqrt{n}}$. It follows from Corollary 4.9 that for any $\epsilon > 0$ there exists $\delta > 0$ such that $\mu^{\mathrm{mid}}_{r,n,\ell}$ and $(\hat{\mu}_{r,n,\ell})_X \otimes (\hat{\mu}_{r,n,\ell})_Y$ are $(\epsilon, \delta\sqrt{n}, \delta\sqrt{n})$-indistinguishble. □

We have now verified Claims 4.13, 4.14, which establishes Claim 4.12, which completes the proof of Theorem 4.7. □

The proof of Theorem 4.6 is similar to that of Theorem 4.7. The two main ingredeints are (1) the standard $\Omega(n)$ lower bound for disjointness, Theorem 4.7, and (2) Theorem 4.10 on the hardness of pointer verification. We omit the details, which can be found in [BGGS19].

4.3 Proof of Theorem 4.10

In this section we prove Theorem 4.10. The exposition nearly exactly follows that of Sections 5.2 – 5.5 of the author's paper [BGGS19].

In this section we state Lemma 4.15 which is a slight reformulation of Theorem 4.10 and then show how Theorem 4.10 follows from Lemma 4.15. The remaining subsections will then be devoted to the proof of Lemma 4.15.

We first introduce some additional notation for the pointer verification problem. For $s < t$, let $\Sigma^t_s = \Sigma_t \circ \Sigma_{t-1} \circ \cdots \Sigma_s$ and $(\Sigma^{-1})^s_t = \Sigma^{-1}_s \circ \cdots \circ \Sigma^{-1}_t$. Also recall from before that $I_s := \Sigma^s_1(I_0), J_s := (\Sigma^{-1})^{r-s+1}_r(J_0)$. Then over the distribution $D^{\mathrm{Y}}_{\mathrm{PV}}$, $J_r = I_0$ and $I_r = J_0$ with probability 1. We also write $\Sigma_{\mathtt{A}} = (\Sigma_1, \Sigma_3, \ldots, \Sigma_r)$ and $\Sigma_{\mathtt{B}} = (\Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1})$. Recall that Alice holds the permutations $\Sigma_{\mathtt{A}}$ while Bob holds the permutations $\Sigma_{\mathtt{B}}$. For technical reasons, in this section, we consider protocols that get inputs sampled from a single "mixed" distribution, $D^{\mathrm{Mix}}_{\mathrm{PV}} = \frac{1}{2}(D^{\mathrm{Y}}_{\mathrm{PV}} + D^{\mathrm{N}}_{\mathrm{PV}})$ and outputs a bit (last bit of the transcript) that aims to guess whether the input is a YES input to Pointer Verification ($\Sigma^r_1(I_0) = J_0$) or a NO input ($\Sigma^r_1(I_0) \neq J_0$). The success of a protocol is the probability with which this bit is guessed correctly. These terms are formally defined below.

Definition 4.5. For any odd integer r and any integer n, the distribution $D^{\mathrm{Mix}}_{\mathrm{PV}} = D^{\mathrm{Mix}}_{\mathrm{PV}}(r,n)$ is supported on $(\mathcal{S}_n^{\lceil r/2 \rceil}) \times ([n]^2 \times \mathcal{S}_n^{\lfloor r/2 \rfloor})$, and is defined by drawing $D^{\mathrm{N}}_{\mathrm{PV}}(r,n)$ with probability $1/2$ and drawing $D^{\mathrm{Y}}_{\mathrm{PV}}(r,n)$ with probability $1/2$.

A protocol Π is said to achieve *success* on a pair of inputs drawn from $D^{\mathrm{Mix}}_{\mathrm{PV}}$ if the last bit of the transcript of Π, which we take as the output bit, is 1 if and only if $\Sigma^r_1(I_0) = J_0$.

In Lemma 4.15 we show that Alice and Bob cannot achieve success with probability significantly greater than $1/2$ when their inputs are drawn from $D^{\mathrm{Mix}}_{\mathrm{PV}}$. Theorem 4.10 follows fairly easily from Lemma 4.15.

Lemma 4.15. *For every $\epsilon > 0$ and every odd r, there exists β, n_0 such that for every $n \geq n_0$ the following holds: Every $((r+3)/2, n/\log^{\beta}(n))$ protocol on $D^{\mathrm{Mix}}_{\mathrm{PV}}$ achieves success with probability at most $1/2 + \epsilon$.*

We defer the proof of Lemma 4.15 but first show how Theorem 4.10 follows from it.

Proof of Theorem 4.10. Lemma 4.15 gives that there exists β, n_0 such that for every $n \geq n_0$, no $((r+3)/2, n/\log^{\beta}(n))$ protocol Π on $D^{\mathrm{Mix}}_{\mathrm{PV}}(r,n)$ achieves success with probability greater than $1/2 + \epsilon/4$. Suppose for the purpose of contradiction that there were an $((r+3)/2, n/\log^{\beta}(n) - 1)$ protocol that ϵ-distinguishes $D^{\mathrm{Y}}_{\mathrm{PV}}(r,n)$ and $D^{\mathrm{N}}_{\mathrm{PV}}(r,n)$. Then by the definition of ϵ-distinguishability, by modifying this protocol to output an extra bit (which we interpret as the output bit), we get

an $((r+3)/2, n/\log^{\beta}(n))$ protocol Π' which outputs 1 with probability p_Y when the inputs are drawn from $D^{\mathrm{Y}}_{\mathrm{PV}}(r,n)$ and which outputs 1 with probability p_N when the inputs are drawn from $D^{\mathrm{N}}_{\mathrm{PV}}(r,n)$, where $p_Y \geq p_N + \epsilon$. Therefore, Π' has probability of success of at least $1/2 + \epsilon/2$ when the inputs are drawn from $D^{\mathrm{Mix}}_{\mathrm{PV}}(r,n)$, which contradicts Lemma 4.15.

□

4.4 Proof of Lemma 4.15: Setting up the Induction

Our approach to the proof of Lemma 4.15 is based on the "round-elimination" approach of [NW93]. Roughly, given inputs drawn from $D^{\mathrm{Mix}}_{\mathrm{PV}}(r,n)$, the approach here is to show that after a single message $\Pi = \Pi(\Sigma_{\mathtt{A}})$ from Alice to Bob, Alice and Bob are still left with essentially a problem from $D^{\mathrm{Mix}}_{\mathrm{PV}}(r-2,n)$ (with their roles reversed). Note that the distribution of $(\Sigma_2, \ldots, \Sigma_{r-1}; I_1, J_1)$, where $I_1 = \Sigma_1(I_0)$ and $J_1 = \Sigma_r^{-1}(J_0)$, is exactly $D^{\mathrm{Mix}}_{\mathrm{PV}}(r-2,n)$ (with the roles of Alice and Bob switched). The crux of the [NW93] approach is to show that this roughly remains the case even when conditioned on the message $\Pi = \Pi(\Sigma_{\mathtt{A}})$ sent in the first round. If implemented correctly, this would lead to an inductive strategy for proving the lower bound, with the induction asserting that an additional $(r-2)/2$ rounds of communication do not lead to non-trivially high success probability. Of course the distributions of the inputs after conditioning on m are not exactly the same as $D^{\mathrm{Mix}}_{\mathrm{PV}}(r-2,n)$. Bob can definitely learn a lot of information about Alice's input $\Sigma_{\mathtt{A}}$ from M. So the inductive hypothesis needs to deal with distributions that retain some of the features of $D^{\mathrm{Mix}}_{\mathrm{PV}}(r,n)$ while allowing Alice and Bob to have a fair amount of information about each others inputs. In Definition 4.6 we present the exact class of distributions with which we work. While most of the properties are similar to those used in [NW93] the exact definition is not immediate since we need to ensure that the bit "Is $\Sigma_1^r(I_0) = J_0$" is not determinable even after a few rounds of communication. (In our definition, Item 3 in particular is the non-trivial ingredient.) In Lemma 4.17 we then show that this definition supports induction on the number of rounds of communication. Finally in Lemma 4.18 we show that the base-case of the induction with $r = 1$ does not achieve non-trivial success probability. The proofs of Lemma 4.18 and Lemma 4.17 are deferred to Subsection 4.5 and Subsection 4.6 respectively. We conclude the current section with a proof of Lemma 4.15 assuming these two lemmas.

We start with our definition of the class of "noisy" distributions, containing $D^{\mathrm{Mix}}_{\mathrm{PV}}$. In particular, for n, r, δ, C satisfying $0 \leq \delta < 1$ and $0 \leq C < n$, we define the class of distributions $\mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r,n,\delta,C)$ in Definition 4.6 below.

Definition 4.6. The set of *noisy* distributions, denoted $\mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r,n,\delta,C)$, consists of those distributions D supported on $((\mathcal{S}_n^{\lceil r/2 \rceil}) \times ([n]^2 \times \mathcal{S}_n^{\lfloor r/2 \rfloor})$, satisfying the following properties. If we denote a sample from D as $(I_0, J_0, \Sigma_1, \ldots, \Sigma_r)$, then

1. (a) $H(I_0 | \Sigma_1, \ldots, \Sigma_r) \geq \log(n) - \delta$
   (b) $H(J_0 | \Sigma_1, \ldots, \Sigma_r) \geq \log(n) - \delta$.
2. $H(\Sigma_1, \ldots, \Sigma_r) \geq r \log(n!) - C$.
3. (a) $H(\mathbb{1}[\Sigma_1^r(I_0) = J_0] | I_0, \Sigma_1, \ldots, \Sigma_r) \geq 1 - \delta$.
   (b) $H(\mathbb{1}[\Sigma_1^r(I_0) = J_0] | J_0, \Sigma_1, \ldots, \Sigma_r) \geq 1 - \delta$.
4. (a) $H(J_0 | I_0, \Sigma_1, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - \delta$.

(b) $H(I_0|J_0, \Sigma_1, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - \delta$.

5. For all odd $1 \leq t \leq r$, the following conditional independence properties hold. For all $i_0, \ldots, i_t, j_0, \ldots, j_t \in [n]$, $\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-1} \in \mathcal{S}_n$,

$$\Sigma_{\mathtt{A}} \cap (\Sigma_1, \ldots, \Sigma_t, \Sigma_{r-t+1}, \ldots, \Sigma_r) \perp \Sigma_{\mathtt{B}} \quad | \quad (I_0, \ldots, I_t) = (i_0, \ldots, i_t), (J_0, \ldots, J_t) = (j_0, \ldots, j_t), \\ (\Sigma_{t+2}, \Sigma_{t+4}, \ldots, \Sigma_{r-t-1}) = (\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-1}).$$

and for all even t, $0 \leq t \leq r$, $i_0, i_1, \ldots, i_t, j_0, j_1, \ldots, j_t \in [n]$, $\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-1} \in \mathcal{S}_n$,

$$\Sigma_{\mathtt{B}} \cap (\Sigma_2, \ldots, \Sigma_t, \Sigma_{r-t+1}, \ldots, \Sigma_{r-1}) \perp \Sigma_{\mathtt{A}} \quad | \quad (I_0, \ldots, I_t) = (i_0, \ldots, i_t), (J_0, \ldots, J_t) = (j_0, \ldots, j_t), \\ (\Sigma_{t+2}, \Sigma_{t+4}, \ldots, \Sigma_{r-t-1}) = (\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-1}).$$

The set of *noisy-on-average* distributions, $\mathcal{D}^{\text{Mix}+}_{\text{PV}}(r, n, \delta, C)$, consists of those distributions D^+ supported on $((\mathcal{S}_n^{\lceil r/2 \rceil}) \times ([n]^2 \times \mathcal{S}_n^{\lfloor r/2 \rfloor}) \times \mathcal{Z}$ where $\mathcal{Z}$ is some finite set and a sample $(I_0, J_0, \Sigma_1, \ldots, \Sigma_r, Z) \sim D^+$ satisfies Properties (1)-(5) when all quantities above are additionally conditioned on Z. (In particular the conditional entropies are additionally conditioned on Z and the independences hold when conditioned on Z.)

We first state a version of Lemma 4.15 for every distribution $D \in \mathcal{D}^{\text{Mix}}_{\text{PV}}(r, n, \delta, C)$, for sufficiently small δ, C. We also show that $D^{\text{Mix}}_{\text{PV}}$ belongs to this set for the permissible δ, C, and thus Lemma 4.16 implies Lemma 4.15.

Lemma 4.16. *For every $\epsilon > 0$ and odd r, there exists β and n_0 such that for every $n \geq n_0$, and every $D \in \mathcal{D}^{\text{Mix}}_{\text{PV}}(r, n, 1/\log^{\beta} n, n/\log^{\beta} n)$ it is the case that every $((r+3)/2, n/\log^{\beta}(n))$-protocol achieves success with probability at most $1/2 + \epsilon$ on D.*

Remark 4.7. In the lemma statement we have suppressed the dependence of β on r. (The dependence of β on ϵ is minimal. Essentially only n_0 is affected by ϵ.) A careful analysis (based on the remarks after Lemma 4.18 and Lemma 4.17) yields that β grows exponentially in r, though we omit the simple but tedious bookkeeping.

The proof of Lemma 4.16 is via induction on r; the below lemma gives the main inductive step, which says that if one cannot solve the pointer verification problem with $r-2$ permutations then one cannot hope to solve the problem on r permutations even with an additional round of (not too long) communication.

Lemma 4.17 (Inductive step)**.** *For every $\epsilon_1 > \epsilon_2 > 0$, odd r and β_2 there exists β_1 and n_0 such that for every $n \geq n_0$ the following holds: Suppose there exists $D \in \mathcal{D}^{\text{Mix}}_{\text{PV}}(r, n, 1/\log^{\beta_1} n, n/\log^{\beta_1} n)$ and an $((r+3)/2, n/\log^{\beta_1} n)$-protocol Π that achieves success $1/2 + \epsilon_1$ on D. Then there exists $\tilde{D} \in \mathcal{D}^{\text{Mix}}_{\text{PV}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$ and an $((r+1)/2, n/\log^{\beta_2} n)$-protocol $\tilde{\Pi}$ that achieves success $1/2 + \epsilon_2$ on $\tilde{D}$.*

Remark 4.8. A careful analysis of the proof yields that β_2 grows linearly with β_1 with some mild conditions on n_0 and $\epsilon_1 - \epsilon_2$.

The proof of Lemma 4.16 proceeds by using Lemma 4.17 repeatedly, to reduce the case with general r to the case with $r = 1$. In the case $r = 1$, Alice is given one permutation Σ_1, Bob is given indices I_0, J_0, and Alice can communicate one message to Bob, who has to then decide whether

$\Sigma_1(I_0) = J_0$ or not. The next lemma, Lemma 4.18, asserts that the pointer verification problem with $r = 1$ cannot be solved in one round with less than $n/\log^{O(1)}(n)$ communication. In fact the lemma is a stronger one, where we show that if all the statements hold conditioned on a random variable Z, then the entropy of the indicator of the outcome is large even when conditioned on Z. Setting Z to be a constant immediately yields the base case of the induction with $r = 1$, as noted in Corollary 4.19. (We note that we need the stronger version stated in the lemma, i.e., with a general random variable Z, in the proof of Lemma 4.17.)

Lemma 4.18 (Base case)**.** *There exists $0 < \epsilon_1^* < 1$ and ϵ_2^* such that for every $\tilde{\beta}$ there is n_0 such that the following holds for every $n \geq n_0$. Let $\beta = (\tilde{\beta} + \epsilon_2^*)/\epsilon_1^*$, $\delta = 1/\log^{\beta} n$ and $C, C' = n/\log^{\beta} n$. Suppose (I, J, Σ, Z) are drawn from a distribution D, where Z is a random variable that takes on finitely many values, such that the following properties hold:*

1. *$H(I|\Sigma, Z) \geq \log(n) - \delta$.*
2. *$H(\Sigma|Z) \geq \log(n!) - C$.*
3. *$H(\mathbb{1}[\Sigma(I) = J]|\Sigma, I, Z) \geq 1 - \delta$.*
4. *$H(J|\Sigma, I, \mathbb{1}[\Sigma(I) \neq J], Z) \geq \log(n) - \delta$.*

Then for every deterministic function $\Pi_1 = \Pi_1(\Sigma, Z)$ with $\Pi_1 \in \{0,1\}^{C'}$ we have the following:

$$H(\Sigma(I)|I, \Pi_1, Z) \geq \log n - 1/\log^{\tilde{\beta}} n \tag{23}$$

$$\text{and} \quad H(\mathbb{1}[\Sigma(I) = J]|\Pi_1, I, J, Z) \geq 1 - 1/\log^{\tilde{\beta}} n. \tag{24}$$

Remark 4.9. The proof shows that β grows linearly with $\tilde{\beta}$ provided that n_0 is sufficiently large (as a function of $\tilde{\beta}$).

Corollary 4.19. *For every $\epsilon > 0$, there exists β_0 and n_0 such that for every $n \geq n_0$, and every $D \in \mathcal{D}^{\text{Mix}}_{\text{PV}}(1, n, 1/\log^{\beta_0} n, n/\log^{\beta_0} n)$ it is the case that every $(2, n/\log^{\beta_0}(n))$-protocol achieves success with probability at most $1/2 + \epsilon$ on D.*

Proof. Recall that a 1-round distribution $D \in \mathcal{D}^{\text{Mix}}_{\text{PV}}(1, n, \delta, C)$ is supported on triples (Σ, I, J) and the goal is to determine if $\Sigma(I) = J$. We apply Lemma 4.18 with $Z = 0$ (i.e., a constant). Given $\epsilon > 0$ we let $\tilde{\beta} = 1$ and let β be as given by Lemma 4.18. Further let n_0' denote the lower bound on n returned by Lemma 4.18. Let ϵ' be such that a binary variable of entropy at least $1 - \epsilon'$ is Bernoulli with bias in the range $[1/2 - \epsilon, 1/2 + \epsilon]$ ($\epsilon' = O(\epsilon^2)$ works). We prove the claim for $\beta_0 = \beta$ and $n_0 = \max\{n_0', 2^{1/(\epsilon')}\}$ (so that $\log^{\tilde{\beta}} n \leq \epsilon'$ for all $n \geq n_0$).

By definition of $\mathcal{D}^{\text{Mix}}_{\text{PV}}(1, n, 1/\log^{\beta_0} n, n/\log^{\beta_0} n)$, we have that for $(\Sigma, i, j) \sim D$, the conditions (1)-(4) of Lemma 4.18 hold for (Σ, i, j, Z) (where Z is simply the constant 0). Thus Lemma 4.18 asserts that $H(\mathbb{1}[\Sigma(I) = J]|\Pi_1, I, J, Z) \geq 1 - 1/\log^{\tilde{\beta}} n \geq 1 - \epsilon'$ for any message $\Pi_1 = \Pi_1(\Sigma) \in \{0,1\}^{C'}$ sent by Alice. Let $\Pi_2(\Pi_1, I, J)$ denote the output bit of the protocol output by Bob. Since this is a deterministic function of Π_1, I, J we have, by the data processing inequality, that $H(\mathbb{1}[\Sigma_1(I) = J]|\Pi_2(\Pi_1, I, J)) \geq 1 - \epsilon'$. By the choice of ϵ' and Jensen's inequality (to average over the conditioning on $\Pi_2(\Pi_1, I, J)$) we have that

$$\mathbb{P}\left[\mathbb{1}[\Sigma(I) = J] = \Pi_2(\Pi_1, I, J)\right] \leq 1/2 + \epsilon,$$

which verifies that the success probability of the protocol Π is at most $1/2 + \epsilon$ as asserted. □

Armed with Lemma 4.17 and Corollary 4.19 we are now ready to prove Lemma 4.16.

Proof of Lemma 4.16. We prove the lemma by induction on r. If $r = 1$, then Corollary 4.19 gives us the lemma. Assume now that the lemma holds for all odd $r' < r$. In particular, let β_{r-2} and $n_{0,r-2}$ be the parameters given by the lemma for $r-2$ rounds and parameter $\epsilon/2$. We now apply Lemma 4.17 with parameters $\epsilon_1 = \epsilon$, $\epsilon_2 = \epsilon/2$, r rounds and $\beta_2 = \beta_{r-2}$. Let n_0' and β_1 be the parameters given to exist by Lemma 4.17. We verify the inductive step with $n_{0,r} = \max\{n_{0,r-2}, n_0'\}$ and $\beta_r = \beta_1$. Fix $D \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r, n, 1/\log^{\beta_r} n, n/\log^{\beta_r} n)$ and assume for contradiction that an $((r+3)/2, n/\log^{\beta_r} n)$-protocol achieves success $1/2 + \epsilon$ on D. Then by Lemma 4.17 we have that there exists $\tilde{D} \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r-2, n, 1/\log^{\beta_{r-2}} n, n/\log^{\beta_{r-2}} n)$ and an $((r+1)/2, n/\log^{\beta_{r-2}} n)$-protocol $\tilde{\Pi}$ that achieves success $1/2 + \epsilon/2$ on $\tilde{D}$, which contradicts the inductive hypothesis. □

We finally show how Lemma 4.15 follows from Lemma 4.16 (which amounts to verifying the $D^{\mathrm{Mix}}_{\mathrm{PV}}$ satisfies the requirements of membership in $\mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}$ for appropriate choice of parameters).

Proof of Lemma 4.15. We claim that for each odd integer r, $D^{\mathrm{Mix}}_{\mathrm{PV}}(r, n) \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r, n, 2/n, 0)$ for sufficiently large n. To verify this, note that if $(\Sigma_1, \ldots, \Sigma_r, I_0, J_0)$ are drawn from $D^{\mathrm{Mix}}_{\mathrm{PV}}(r, n)$, then

1. $H(I_0|\Sigma_1, \ldots, \Sigma_r) = H(J_0|\Sigma_1, \ldots, \Sigma_r) = \log(n)$.
2. $H(\Sigma_1, \ldots, \Sigma_r) = r \cdot \log(n!)$.
3. $H(\mathbb{1}[\Sigma_1^r(I_0) = J_0]|I_0, \Sigma_1, \ldots, \Sigma_r) = H(\mathbb{1}[\Sigma_1^r(I_0) = J_0]|J_0, \Sigma_1, \ldots, \Sigma_r) = h(1/2 + 1/(2n)) \geq 1 - 1/n^2$.
4. $H(J_0|I_0, \Sigma_1, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) = H(I_0|J_0, \Sigma_1, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) = \log(n-1) \geq \log(n) - 2/n$, for sufficiently large values of n.
5. To verify the conditional independence properties (5) from Definition 4.6, first fix any odd t such that $1 \leq t \leq r$, and pick any $i_0, \ldots, i_t, j_0, \ldots, j_t \in [n]$ and $\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-2} \in \mathcal{S}_n$. Given that

   $$\{(I_0, \ldots, I_t) = (i_0, \ldots, i_t), (J_0, \ldots, J_t) = (j_0, \ldots, j_t), (\Sigma_{t+2}, \Sigma_{t+4}, \ldots, \Sigma_{r-t-1}) = (\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-1})\},$$

   and regardless of the choice of $\Sigma_{\mathtt{B}}$, note that the permutations in $\Sigma_{\mathtt{A}} \cap (\Sigma_1, \ldots, \Sigma_t, \Sigma_{r-t-1}, \ldots, \Sigma_r)$ are uniformly random subject to $\Sigma_s(i_{s-1}) = i_s$ for $s \in \{1, 3, \ldots, t\}$ and $\Sigma^{-1}_{r-s+1}(j_s) = j_{s-1}$ for $s \in \{1, 3, \ldots, t\}$. A similar argument verifies the analogous statement for even t.

In particular, it follows that for every $\beta > 0$ and every odd r, for sufficiently large n, we have that $D^{\mathrm{Mix}}_{\mathrm{PV}}(r, n) \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r, n, 1/\log^{\beta}(n), n/\log^{\beta}(n))$, and in particular this holds for the parameter β guaranteed to exist by Lemma 4.16. The lemma now follows immediately from the conclusion of Lemma 4.16, which asserts that every $((r+3)/2, n/\log^{\beta}(n))$-protocol achieves success with probability at most $1/2 + \epsilon$ on D. □

Thus the main lemma is proved assuming Lemma 4.18 and Lemma 4.17. In the rest of this section we prove these two lemmas.

4.5 The Base Case: Proof of Lemma 4.18

In the following we will fix β and argue that if $\tilde{\beta} \leq \epsilon_1^* \cdot \beta - \epsilon_2^*$ then the conditions (23) and (24) of Lemma 4.18 hold. Specifically we will prove (23) first and then derive (24) as a consequence. For (23), we will first bound $H(\Sigma(I)|I)$ when Σ is a nearly uniform *function* instead of a nearly random *permutation*, and then extend it to case that Σ is a nearly uniform permutation. Then using this result, we will bound $H(\Sigma(I)|I, \Pi)$, where Π is a short message that depends on Σ.

In the below Lemma 4.20, we will take $I \in [k]$ and $\Sigma : [k] \to [n]$ to be a nearly uniformly random function. We allow that $k \neq n$ in order to deal with the case that Σ is a nearly uniformly random permutation later on (in our application we will always have $k \leq n$).

Lemma 4.20. *For every $k, n \in \mathbb{Z}_+$ and every $\delta, C \in \mathbb{R}_+$ the following holds: Suppose (I, Σ) are drawn from a distribution D such that the resulting random variables, $I \in [k], \Sigma : [k] \to [n]$ have the following properties:*

1. *$H(I|\Sigma) \geq \log(k) - \delta$, with $\delta \in [1/n, 1/8)$.*
2. *$H(\Sigma) \geq k \log n - C$, with $C \leq k$.*

Then

$$H(\Sigma(I)|I) \geq \log(n) - \frac{C}{k} - 2\sqrt{2\delta}\log(n).$$

Proof. Let D be the joint distribution on (Σ, I) that satisfies (1),(2) and let D_I, D_Σ be its marginals on I and Σ respectively. Unless specified, all the following probability statements are with respect to D. Let U_k denote the random variable that is uniform on $[k]$.

We will first make a few observations and then bound $H(\Sigma(I)|I)$. Firstly, since $H(I) \geq \log k - \delta$, by Pinsker's inequality, we have that,

$$\Delta(D_I, U_k) = \frac{1}{2}\sum_{i=1}^{k} |\mathbb{P}[I = i] - 1/k| \leq \sqrt{\delta/2}. \tag{25}$$

Let $D_\Sigma \otimes D_I$ denote the joint distribution over (Σ, I), where Σ and I are independently drawn from their marginals D_Σ and D_I respectively. By Pinsker's inequality, we have that,

$$\Delta(D, D_\Sigma \otimes D_I) \leq \sqrt{I(\Sigma; I)/2} \leq \sqrt{\delta/2}.$$

It then follows that,

$$\sum_{i \in [k], j \in [n]} |\mathbb{P}[\Sigma(i) = j, I = i] - \mathbb{P}[\Sigma(i) = j] \cdot \mathbb{P}[I = i]| \leq \sqrt{2\delta}. \tag{26}$$

Now, for each $i \in [k]$, define,

$$\epsilon_i \quad = \quad \sum_{j \in [n]} |\mathbb{P}[\Sigma(i) = j, I = i] - \mathbb{P}[\Sigma(i) = j] \cdot \mathbb{P}[I = i]|,$$

so that $\sum_{i \in [k]} \epsilon_i \leq \sqrt{2\delta}$. We get that

$$\Delta((\Sigma(i)|I = i), \Sigma(i)) = \frac{1}{2}\sum_{j \in [n]} |\mathbb{P}[\Sigma(i) = j | I = i] - \mathbb{P}[\Sigma(i) = j]| = \frac{\epsilon_i}{2\mathbb{P}[I = i]},$$

which by Lemma 6.4 then gives,

$$|H(\Sigma(i)|I=i) - H(\Sigma(i))| \leq h\left(\frac{\epsilon_i}{2\mathbb{P}[I=i]}\right) + \left(\frac{\epsilon_i}{2\mathbb{P}[I=i]}\right)\log(n-1) := \beta_i. \tag{27}$$

We have that

$$\begin{aligned} H(\Sigma(I)|I) &= \sum_{i\in[k]} \mathbb{P}[I=i]\cdot H(\Sigma(I)|I=i) \\ &\geq \sum_i \mathbb{P}[I=i](H(\Sigma(i)) - \beta_i) \qquad (28) \\ &\geq \sum_i \frac{1}{k}H(\Sigma(i)) - \sqrt{\delta/2}\log n - \sum_i \mathbb{P}[I=i]\beta_i, \qquad (29) \end{aligned}$$

where (28) follows from (27), and (29) follows from (25) and the fact that $H(\Sigma(i)) \leq \log n$.

Using the chain rule for entropy we get that

$$\log n - C/k \leq \frac{1}{k}H(\Sigma) = \frac{1}{k}\sum_{i=1}^{k} H(\Sigma(i)|\Sigma(\{1,\ldots,i-1\})) \leq \frac{1}{k}\sum_{i=1}^{k} H(\Sigma(i)). \tag{30}$$

Recall that $\sum_i \epsilon_i \leq \sqrt{2\delta}$ and we have that $h(\sum_i \epsilon_i) \leq h(\sqrt{2\delta})$, since $\delta < 1/8$. Since the binary entropy function $h(\cdot)$ is concave, by Jensen's inequality, we have that,

$$\begin{aligned} \sum_{i=1}^{k} \mathbb{P}[I=i]\beta_i &= \sum_i \mathbb{P}[I=i]h\left(\frac{\epsilon_i}{2\mathbb{P}[I=i]}\right) + \sum_i \mathbb{P}[I=i]\left(\frac{\epsilon_i}{2\mathbb{P}[I=i]}\right)\log(n-1) \\ &\leq h\left(\sum_i \mathbb{P}[I=i]\cdot\frac{\epsilon_i}{2\mathbb{P}[I=i]}\right) + \sqrt{\delta/2}\log n \\ &\leq h\left(\sqrt{\delta/2}\right) + \sqrt{\delta/2}\log n. \qquad (31) \end{aligned}$$

Note that $h(x) \leq 2x\log(1/x)$ for $x \to 0$, so $h(\sqrt{\delta/2}) \leq \sqrt{2\delta}\log n$. Using this, and plugging (30) and (31) into (29), we get that

$$H(\Sigma(I)|I) \geq \log n - \frac{C}{k} - 2\sqrt{\delta/2}\log n \geq \log(n) - \frac{C}{k} - 2\sqrt{2\delta}\log(n). \qquad \square$$

Now we are ready to prove an analogous lemma for random permutations instead of random functions. We note that we cannot replicate the proof above since for a typical i the conditional entropy $H(\Sigma(i)|\Sigma(\{1,\ldots,i-1\}))$ is actually $\log n - \Theta(1)$ and this $\Theta(1)$ loss is too much for us. In the proof below we condition instead on I being contained in some smaller set $S \subseteq [n]$, with $|S| = k = o(n)$, where S itself is randomly chosen. This "conditioning" turns out to help with the application of the chain rule and this allows us to reproduce a bound that is roughly as strong as the bound above.

Lemma 4.21. *There exists constants $\epsilon_1^* > 0, \epsilon_2^*$ such that for every β there exists n_0 such that for all $n \geq n_0$ the following holds: Suppose $I \in [n]$, $\Sigma \in \mathcal{S}_n$ are random variables such that:*

1. $H(I|\Sigma) \geq \log(n) - \delta$, *with* $\delta \in [1/n, 1/\log^{\beta} n]$.

2. $H(\Sigma) \geq \log(n!) - C$, *with* $C \leq n/\log^{\beta}(n)$.

Then

$$H(\Sigma(I)|I) \geq \log n - 1/\log^{\tilde{\beta}} n,$$

where $\tilde{\beta} = \epsilon_1^* \cdot \beta - \epsilon_2^*$.

Proof. We will prove the lemma with $\epsilon_1^* = 1/16, \epsilon_2^* = 4$. Note that for $\beta \leq 8$, $\tilde{\beta} = \epsilon_1^*\beta - \epsilon_2^* \leq -3$, so by non-negativity of entropy, the lemma statement follows immediately. We therefore assume $\beta > 8$ for the remainder of the proof.

Let D be the distribution of (Σ, I) given in the lemma statement, where D_Σ, D_I are its marginals on I, Σ respectively. Let k be a parameter to be fixed later. We start by defining a joint distribution D' on triples (Σ, I, S) with $\Sigma \in \mathcal{S}_n$ and $I \in S \subset [n]$, $|S| = k$ that satisfies the condition that its marginal on (Σ, I) equals D while at the same time the distribution of (Σ, I) conditioned on $S = S'$ when $(\Sigma, I, S) \sim D'$ is the same as the distribution of $(\Sigma, I) \sim D$ conditioned on $I \in S'$. D' is defined as follows:

Let D_S be the distribution of (Σ, I), conditioned on $I \in S$. Now let $\mathcal{E}$ be the distribution over subsets $S \subset [n]$ of size k where the probability of $\mathbb{P}_{S\sim\mathcal{E}}[S = S'] = \frac{\sum_{i\in S'} \mathbb{P}_D[I=i]}{\binom{n-1}{k-1}}$. Now define the joint distribution D' of (Σ, I, S) of $\sigma \in \mathcal{S}_n, i \in S' \subset [n], |S'| = k$ so that

$$\begin{aligned}\mathbb{P}_{D'}[\Sigma = \sigma, I = i, S = S'] &= \mathbb{P}_{\mathcal{E}}[S = S'] \cdot \mathbb{P}_D[\Sigma = \sigma, I = i | I \in S'] \\ &= \mathbb{P}_{\mathcal{E}}[S = S'] \cdot \mathbb{P}_{D_{S'}}[\Sigma = \sigma, I = i].\end{aligned}$$

We claim that the marginal distribution of (Σ, I), where $(\Sigma, I, S) \sim D'$, is equal to D. To see this,

$$\begin{aligned}\mathbb{P}_{D'}[\Sigma = \sigma, I = i] &= \sum_{S'\subset[n], |S'|=k, S'\ni i} \mathbb{P}_{\mathcal{E}}[S = S'] \cdot \mathbb{P}_D[\Sigma = \sigma, I = i | I \in S'] \\ &= \sum_{S'\subset[n], |S'|=k, S'\ni i} \left(\sum_{i'\in S'} \frac{\mathbb{P}_D[I = i']}{\binom{n-1}{k-1}}\right) \cdot \frac{\mathbb{P}_D[\Sigma = \sigma, I = i]}{\mathbb{P}_D[I \in S']} \\ &= \frac{1}{\binom{n-1}{k-1}} \cdot \sum_{S'\subset[n], |S'|=k, S'\ni i} \mathbb{P}_D[\Sigma = \sigma, I = i] \\ &= \mathbb{P}_D[\Sigma = \sigma, I = i].\end{aligned}$$

Recall we wish to lower bound $H_D(\Sigma(I)|I)$. But notice that

$$H_D(\Sigma(I)|I) = H_{D'}(\Sigma(I)|I) \geq H_{D'}(\Sigma(I)|I, S) = \mathbb{E}_{S'\sim\mathcal{E}}[H_{D'}(\Sigma(I)|I, S = S')].$$

Hence it suffices to show that for every set $S', |S'| = k$, $H_{D'}(\Sigma(I)|I, S = S') \geq \log n - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n$ and we do so below.

Fix a subset $S' \subset [n]$, of size k, where k also satisfies

$$\delta^{1/4} \cdot n/k \leq \sqrt{2} - 1, \quad \delta^{1/4} n \log n/k \leq 1/10, \quad nC/k^2 \leq 1/10, \quad k \leq n/10. \tag{32}$$

We remark that for each $\beta > 4$, there is some n_0 such that for $n \geq n_0$, such a k satisfying (32) always exists. (Recall our assumption above that $\beta > 8$.)

We will specify the exact value of k below, but for now we note that our argument holds for any k satisfying (32). By the definition of D', we have that $H_{D'}(\Sigma(I)|I, S = S') = H_{D_{S'}}(\Sigma(I)|I)$. We show below that $(\Sigma(S'), I)$ where $(\Sigma, I) \sim D_{S'}$ satisfies the preconditions of Lemma 4.20. To show this, we need to choose $\gamma(n, k, \delta) \in [1/n, 1/8)$ and $\Gamma(n, k, \delta, C) \leq k$ satisfying the following:

1. $H_{D_{S'}}(I|\Sigma) = H_D(I|\Sigma, I \in S') \geq \log k - \gamma(n, k, \delta)$.
2. $H_{D_{S'}}(\Sigma(S')) = H_D(\Sigma(S')|I \in S') \geq k \log n - \Gamma(n, k, \delta, C)$.

The following claim helps with the choice of $\gamma(n, k, \delta)$.

Claim 4.22. *Suppose that $I \in [n]$ is a random variable such that $H(I) \geq \log n - \tau$ with $n\sqrt{\tau}/k \leq \sqrt{2} - 1$. Then $H_D(I|I \in S') \geq \log k - \frac{n\sqrt{\tau}}{k} \log\left(\frac{k^2}{n\sqrt{\tau}}\right)$.*

Proof of Claim 4.22. Let U_n denote the uniform distribution on $[n]$. By Pinsker's inequality we have that, $\Delta(D_I, U_n) \leq \sqrt{\tau/2}$, which in turn implies that $|\mathbb{P}_{D_I}[I \in S'] - k/n| \leq \sqrt{\tau/2}$. Let $U_{S'}$ be the uniform distribution over S'. We have that

$$\Delta((D_I|I \in S'), U_{S'}) \leq \sqrt{\tau/2} \cdot \frac{1}{k/n - \sqrt{\tau/2}} \leq \frac{n\sqrt{\tau}}{k},$$

since $n\sqrt{\tau}/k \leq \sqrt{2} - 1$. By Theorem 6.5, we get that,

$$H_D(I|I \in S') \geq \log k - \frac{n\sqrt{\tau}}{k} \log\left(\frac{k}{(n\sqrt{\tau}/k)}\right) = \log k - \frac{n\sqrt{\tau}}{k} \log\left(\frac{k^2}{n\sqrt{\tau}}\right)$$

□

By Markov's inequality, with probability at least $1 - \sqrt{\delta}$ when $\sigma \sim D_\Sigma$, we have $H(I|\Sigma = \sigma) \geq \log k - \sqrt{\delta}$. For such σ, by Claim 4.22 applied to the distribution $I|\Sigma = \sigma$ and $\tau = \sqrt{\delta}$ (note that the condition $n\delta^{1/4}/k = n\sqrt{\tau}/k \leq 1 - 1/\sqrt{2}$ holds by the conditions on k), we obtain

$$H_D(I|I \in S', \Sigma = \sigma) \geq \log k - \frac{n\delta^{1/4}}{k} \log\left(\frac{k^2}{\delta^{1/4} n}\right) \geq \log k - \frac{n\delta^{1/4}}{k} \log\left(\frac{k}{\delta^{1/4}}\right).$$

Hence

$$H_D(I|I \in S', \Sigma) \geq (1 - \sqrt{\delta}) \left(\log k - \frac{n\delta^{1/4}}{k} \log\left(\frac{k}{\delta^{1/4}}\right)\right) \geq \log k - \gamma(n, k, \delta),$$

where $\gamma(n, k, \delta) = \sqrt{\delta} \log n + \frac{n\delta^{1/4}}{k} \log(n^2)$, where we have used $k \leq n$ and $\delta \geq 1/n$.

Now we turn to determining $\Gamma(n, k, \delta, C)$ such that $H_{D_{S'}}(\pi(S')) \geq k \log n - \Gamma(n, k, \delta, C)$. Note that $H(\pi|\mathbb{1}[i \in S']) \geq \log n! - C - 1$. Applying Pinsker's inequality to the condition $H(i) \geq H(i|\pi) \geq \log n - \delta$ yields that $\Delta(i, U_n) \leq \sqrt{\delta/2}$, meaning that $|k/n - \mathbb{P}_D[i \in S']| \leq \sqrt{\delta/2}$. Hence

$$\begin{aligned}
H_D(\Sigma|I \in S') &\geq \frac{\log(n!) \cdot (k/n - \sqrt{\delta/2}) - C - 1}{k/n + \sqrt{\delta/2}} \\
&= \log(n!) \cdot \frac{1 - \sqrt{\delta/2} n/k}{1 + \sqrt{\delta/2} n/k} - \frac{C + 1}{k/n + \sqrt{\delta/2}} \\
&\geq \log(n!) \cdot (1 - \sqrt{2\delta} \cdot n/k) - \frac{C + 1}{k/n + \sqrt{\delta/2}} \\
&\geq \log(n!) - n \cdot \left(\sqrt{2\delta} \cdot n \log(n)/k + 2C/k\right),
\end{aligned}$$

where we have used that $n! \le n^n$. But since π is a permutation,

$$\begin{aligned} H_D(\Sigma(S')|I \in S') &= H_D(\Sigma|I \in S') - H_D(\Sigma([n]\backslash S')|I \in S', \Sigma(S')) \\ &\ge \log(n!) - n \cdot \left(\sqrt{2\delta} \cdot n \log(n)/k + 2C/k\right) - \log((n-k)!) \\ &\ge k \log(n-k) - n \cdot \left(\sqrt{2\delta} \cdot n \log(n)/k + 2C/k\right) \\ &\ge k \log n - k \cdot \left(\sqrt{2\delta} \cdot n^2 \log(n)/k^2 + 2nC/k^2 + \frac{2k}{n}\right), \end{aligned}$$

where we have used that $\log(1-x) \ge -2x$ for $0 \le x \le 1/2$, as well as $k \le n/2$. Hence with $\Gamma = \Gamma(n,k,\delta,C) = k \cdot \left(\sqrt{2\delta} \cdot n^2 \log(n)/k^2 + 2nC/k^2 + \frac{2k}{n}\right) \le k$ (by our assumption (32)), we have that $H(\pi(S')|i \in S') \ge k \log(n) - \Gamma$. It follows from Lemma 4.20 that, writing $\gamma = \gamma(n,k,\delta)$,

$$H_{D_{S'}}(\Sigma(I)|I) = H_D(\Sigma(I)|I, I \in S') \ge \log n - \frac{\Gamma}{k} - 2\sqrt{2\gamma} \cdot \log n. \tag{33}$$

Therefore,

$$H_D(\Sigma(I)|I) \ge \mathbb{E}_{S \sim \mathcal{E}}[H_{D_S}(\Sigma(I)|m, I)] \ge \log n - \frac{\Gamma}{k} - 2\sqrt{2\gamma} \cdot \log n, \tag{34}$$

since the inequality is true for each value $S' \subset [n]$, $|S'| = k$, by (33).

It is now easily verified that for each $\beta > 8$, for $k = n \cdot \log^{-\beta/8}(n)$, there is some n_0, depending only on β, so that (32) is satisfied for $n \ge n_0$. Moreover, for such k,

$$\begin{aligned} & \Gamma/k + 2\sqrt{2\gamma} \cdot \log n \\ \le\ & \sqrt{2} \log^{(-\beta/2+1+2\beta/8)} n + 2 \log^{(-\beta+2\beta/8)} n + 2 \log^{(-\beta/8)} n + 2\sqrt{2} \cdot \left(\log^{(-\beta/4+3/2)} n + 2 \log^{(-\beta/8+3/2+\beta/16)} n\right) \\ \le\ & 100 \log^{(3/2-\beta/16)} n \\ \le\ & \log^{(4-\beta/16)} n, \end{aligned}$$

where the last inequality holds for sufficiently large n. By (34) this implies that for each $\beta > 8$, there is some n_0 such that for $n \ge n_0$, $H_D(\Sigma(I)|I) \ge \log(n) - \log^{(4-\beta/16)} n$, which completes the proof. □

Now we are ready to lower bound the entropy $H(\Sigma(I)|\Pi, I, Z)$, that proves Lemma 4.18: Equation (23), via the following lemma.

Lemma 4.23. *There exists constants $\epsilon_1^* > 0, \epsilon_2^*$ such that for every $\beta > 0$ there exists n_0 such that for all $n \ge n_0$ the following holds: Let $\delta = 1/\log^{\beta} n$, $C = C' = \delta n$, and $\tilde{\beta} = \epsilon_1^* \cdot \beta - \epsilon_2^*$. Suppose (I, J, Σ, Z) are drawn from a distribution D, with Z taking on finitely many values, such that the following properties hold:*

1. *$H(I|\Sigma, Z) \ge \log(n) - \delta$.*
2. *$H(\Sigma|Z) \ge \log(n!) - C$.*

Then, for every deterministic function $\Pi = \Pi(\Sigma, Z)$ with $\Pi \in \{0,1\}^{C'}$, we have

$$H(\Sigma(I)|I, \Pi, Z) \ge \log(n) - 1/\log^{\tilde{\beta}} n.$$

Proof. In Lemma 4.21 we proved a lower bound on $H(\Sigma(I)|I)$, given the conditions that $H(I|\Sigma) \geq \log n - \delta$ and $H(\Sigma) \geq \log n! - C$. We would now like to prove a bound on $H(\Sigma(I)|I, \Pi, Z)$, where $\Pi = \Pi(\Sigma, Z)$ is a message of length $\leq C'$ and Z is the random variable in the lemma statement. Since $|\Pi| \leq C'$, (1) and (2) in the lemma hypothesis, along with the data processing inequality, imply that,

1. $H(I|\Sigma, \Pi, Z) \geq \log n - \delta$.
2. $H(\Sigma|\Pi, Z) \geq \log n! - C - C'$.

Let $\gamma = (C + C')/n$, so that $\gamma \leq 2/\log^{\beta}(n)$. By Markov's inequality (and the facts that I takes on at most n values and Σ takes on at most $n!$ values), we have the following, for every $\epsilon > 0$:

- With probability at least $1 - \sqrt{\delta}$ over the choice of $(\pi, z) \sim (\Pi, Z)$, we have that $H(I|\Sigma, \Pi = \pi, Z = z) \geq \log(n) - \sqrt{\delta}$.
- With probability at least $1 - \sqrt{\gamma}$ over the choice of $(\pi, z) \sim (\Pi, Z)$, we have that $H(\Sigma|\Pi = \pi, Z = z) \geq \log(n!) - n \cdot \sqrt{\gamma}$.

Let $\alpha = \max\{\delta, \gamma\}$. For sufficiently large n we have that $\sqrt{\alpha} \leq 1/\log^{(\beta/3)} n$. Then by Lemma 4.21, there is some n_0, depending only on β, such that for all (π, z) belonging to some set of measure at least $1 - 2\sqrt{\alpha}$, for $n \geq n_0$ we have that $H(\Sigma(I)|I, \Pi = \pi, Z = z) \geq \log n - \eta$, where $\eta = \log^{\mu_2^* - \beta\mu_1^*} n$, for absolute constants μ_1^*, μ_2^*. Then there are suitable absolute constants $\epsilon_1^* \in (0, 1), \epsilon_2^* > 0$ and n_0' (depending only on β) such that for $n \geq n_0$,

$$\begin{aligned} H(\Sigma(I)|I, \Pi, Z) &= \mathbb{E}_{(\pi,z)\sim(\Pi,Z)}[H(\Sigma(I)|I, \Pi = \pi, Z = z)] \\ &\geq (1 - 2\sqrt{\alpha}) \cdot (\log(n) - \eta) \\ &\geq \log(n) - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n. \end{aligned}$$

□

Next we work towards the proof of (24) in Lemma 4.18. The main difficulty in proving this inequality is to reason about the conditional entropy of the indicator random variable $\mathbb{1}[\Sigma(I) = J]$, conditioned on the random variable J. Roughly speaking, Lemma 4.24 below allows us to infer a statement such as $H(\mathbb{1}[\Sigma(I) = J]|J) \geq 1 - o(1)$ from an analogous statement of the form $H(\mathbb{1}[\Sigma(I) = J]|\Sigma(I)) \geq 1 - o(1)$, if $\Sigma(I), J \in [n]$ satisfy certain regularity conditions. This same argument is needed in the inductive step presented in Lemma 4.17. In these applications we need to additionally condition all entropies on some random variable Z.

Lemma 4.24. *There are absolute constants $\epsilon_1^* > 0, \epsilon_2^*, n_0$ such that the following holds for every $n \geq n_0$: Let X, Y, Z be random variables with $X, Y \in [n]$ and Z takes on finitely many values. Let $J = \mathbb{1}[X = Y]$. If there is some constant $\beta > 0$ such that $\delta \leq 1/\log^{\beta} n$, and*

1. *$H(X|Z) \geq \log(n) - \delta$.*
2. *$H(J|X, Z) \geq 1 - \delta$.*
3. *$H(Y|X, Z, J = 0) \geq \log(n) - \delta$*

Then $H(J|Y, Z) \geq 1 - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n$.

Proof. We will first prove the above statement assuming that $H(Z) = 0$ and then use Markov's inequality and a union bound to prove the lemma statement for general Z. That is, we first prove that if conditions (1), (2), (3) hold without the conditioning on Z then, $H(J|Y) \geq 1 - o(1)$.

We have that $H(X), H(Y) \leq \log n$ since $X, Y \in [n]$ and $H(J) \leq 1$. Also note that, by Pinsker's inequality,

$$\mathbb{P}[J = 0], \mathbb{P}[J = 1] \in [1/2 - \sqrt{\delta/2}, 1/2 + \sqrt{\delta/2}].$$

We also have that

$$\begin{aligned} H(J|Y) &= H(J) + H(Y|J) - H(Y) \\ &\geq (1 - \delta) + H(Y|J) - \log(n) \\ &\geq (1 - \delta) + \mathbb{P}[J = 0] \cdot H(Y|J = 0) + \mathbb{P}[J = 1] \cdot H(Y|J = 1) - \log n \\ &\geq (1 - \delta) + (1/2 - \sqrt{\delta/2})(\log n - \delta + H(Y|J = 1)) - \log n \end{aligned} \tag{35}$$

But notice that $H(Y|J = 1) = H(Y|X = Y) = H(X|J = 1)$, so it suffices to bound the latter. From the lemma hypothesis we get that

$$H(X|J) = H(X) + H(J|X) - H(J) \geq (\log n - \delta) + (1 - \delta) - 1 \geq \log n - 2\delta.$$

On the other hand we have that

$$\begin{aligned} H(X|J) &= \mathbb{P}[J = 0] \cdot H(X|J = 0) + \mathbb{P}[J = 1] \cdot H(X|J = 1) \\ &\leq (1/2 + \sqrt{\delta/2}) \cdot (\log n + H(X|J = 1)). \end{aligned} \tag{36}$$

Combining the upper and lower bounds on $H(X|J)$, we get that

$$H(X|J = 1) \geq \frac{\log(n) - 2\delta}{1/2 + \sqrt{\delta/2}} - \log n \geq \log(n) - 4\delta - \sqrt{8\delta} \log n.$$

Plugging the above into (35), we get that,

$$H(J|Y) \geq 1 - \frac{7\delta}{2} - 2\sqrt{\delta} \log n.$$

To get the lower bound while conditioning on Z, we use Markov's inequality and a union bound (in the same manner as Lemma 4.23) to get that

$$\begin{aligned} H(J|Y, Z) &\geq (1 - 3\sqrt{\delta}) \left(1 - \frac{7\sqrt{\delta}}{2} - 2\delta^{1/4} \log n\right) \\ &\geq 1 - 7\sqrt{\delta} - 2\delta^{1/4} \log n \\ &\geq 1 - 9\delta^{1/4} \log n \\ &\geq 1 - 9 \log^{(1-\beta/4)} n \\ &\geq 1 - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n, \end{aligned}$$

where the final inequality holds for $\epsilon_1^* = 1/4$, $\epsilon_2^* = 2$ and $n_0 = 2^9$ (so that $\log n \geq 9$). □

The proof of Lemma 4.18: Equation (24) follows as a consequence of Lemmas 4.23 and 4.24 above.

Proof of Lemma 4.18. We show that there exist $\epsilon_1^* > 0$ and ϵ_2^* such that if $\beta \geq (\tilde{\beta} + \epsilon_2^*)/\epsilon_1^*$ (or equivalently, if $\tilde{\beta} \leq \epsilon_1^* \cdot \beta - \epsilon_2^*$) then Equations (23) and (24) of Lemma 4.18 hold for every $n \geq n_0$ where $n_0 = \max\{n_{0,1}, n_{0,2}\}$ and $n_{0,1} = n_{0,1}(\beta)$ is as given by Lemma 4.23 and $n_{0,2} = n_{0,2}(\beta)$ is the constant given by Lemma 4.24. For this choice Lemma 4.23 already gives us (23), that is, $H(\Sigma(I)|I, m) \geq \log(n) - \log^{(\mu_2^* - \beta\mu_1^*)} n$ for some absolute constants $\mu_1^* \in (0,1), \mu_2^* > 0$. Note in particular that this implies that for every $\epsilon_2^* \geq \mu_2^*$ and for every $\epsilon_1^* \leq \mu_1^*$ we have $H(\Sigma(I)|I, \Pi) \geq \log(n) - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n$ and we will make such a choice below.

We next apply Lemma 4.24 with $Z^* = (\Pi, I, Z), X = \Sigma(I), Y = J$, and $J = \mathbb{1}[\Sigma(I) = J]$, where Z^* refers to the random variable in Lemma 4.24 and Z refers to the one in Lemma 4.18. We verify that each of the pre-conditions is met.

1. $X, Y \in [n], J \in \{0,1\}$ and Z^* takes finitely many values.
2. $H(X|Z^*) = H(\Sigma(I)|I, \Pi, Z) \geq \log(n) - \log^{(\mu_2^* - \mu_1^*\beta)} n$, by (23).
3. $H(J|X, Z^*) = H(\mathbb{1}[\Sigma(I) = J]|\Sigma(I), \Pi, I, Z) \geq H(\mathbb{1}[\Sigma(I) = J]|\Sigma, I, Z) \geq 1 - \delta$, by assumption.
4. $H(Y|X, Z^*, J = 0) = H(J|\Sigma(I), \Pi, I, Z, \mathbb{1}[\Sigma(I) = J]) \geq H(J|\Sigma, I, Z, \mathbb{1}[\Sigma(I) = J]) \geq 1 - \delta$, by assumption.

Then by Lemma 4.24, we have that for $n \geq n_0$,

$$H(\mathbb{1}[\Sigma(I) = J]|\Pi, I, J, Z) = H(J|Y, Z^*) \geq 1 - \log^{(\nu_2^* - (\mu_2^* - \beta\mu_1^*)\nu_1^*)} n,$$

where ν_1^*, ν_2^* denote the absolute constants of Lemma 4.24. Thus again we have that if $\epsilon_2^* \geq \nu_2^* - \mu_2^*\nu_1^*$ and $\epsilon_1^* \leq \mu_1^*\nu_1^*$ then we have that $H(\mathbb{1}[\Sigma(I) = J]|\Pi, I, J, Z) \geq 1 - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n$. Setting $\epsilon_1^* = \min\{\mu_1^*, \mu_1^*\nu_1^*\}$ and $\epsilon_2^* = \max\{\mu_2^*, \nu_2^* - \mu_2^*\nu_1^*\}$ thus ensures that both conditions of the lemma are satisfied. □

4.6 The Inductive Step: Proof of Lemma 4.17

We will prove the inductive step via a simulation argument. That is, we show that if Alice and Bob were able to succeed on $D \in \mathcal{D}_{\text{PV}}^{\text{Mix}}(r, n, \delta, C)$ with non-negligible probability, then they would also succeed on some $\tilde{D} \in \mathcal{D}_{\text{PV}}^{\text{Mix}}(r-2, n, \delta', C')$ by simulating the protocol for D given an instance from $\tilde{D}$.

Given a distribution D on which Alice and Bob can succeed with non-negligible probability, we consider the distribution $\tilde{D}$ on the resulting "inner inputs" (i.e. the original inputs minus Σ_1, Σ_r) after Alice sends a short message to Bob. More precisely, the distribution $\tilde{D}$ is the distribution of $(I_1, J_1, \Sigma_2, \ldots, \Sigma_{r-1})$ conditioned on Alice's first message Π_1 and Bob's indices (I_0, J_0), where $(I_1, J_1) = (\Sigma_1(I_0), \Sigma_r^{-1}(J_0))$. Moreover, the inputs of $\tilde{D}$ are given to the players as follows: Alice holds $(I_1, J_1, \Sigma_3, \Sigma_5, \ldots, \Sigma_{r-2})$, Bob holds $(\Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1})$, and it is Bob's turn to send the next message. Therefore, this corresponds to an instance of an $(r-2)$-Pointer Verification Problem with Alice and Bob's roles flipped. We will show in Lemma 4.27 that $\tilde{D} \in \mathcal{D}_{\text{PV}}^{\text{Mix}}(r-2, n, \delta', C')$, for some δ', C' not too much larger than δ, C, respectively. Then using the protocol for D, we will construct a protocol that succeeds when the inputs are drawn from $\tilde{D}$, with not much loss in the success probability. We will now prove two simple lemmas that will be used to prove Lemma 4.27.

Lemma 4.25. *There exists $\epsilon_1^* > 0$ and ϵ_2^* such that for every β there exists n_0 such that for all $n \geq n_0$ the following holds: Suppose I, J, τ_1, τ_2, Z are random variables, where $I, J \in [n]$, $\tau_1, \tau_2 \in \mathcal{S}_n$ and Z takes on finitely many values, satisfying the following conditions:*

1. *$H(I|\tau_1, \tau_2, Z) \geq \log(n) - \delta$, with $\delta \leq 1/\log^\beta n$.*
2. *$H(\tau_1, \tau_2|Z) \geq 2\log(n!) - C$, with $C \leq n/\log^\beta n$.*
3. *For each z for which the event $\{Z = z\}$ has positive probability, there is a permutation $f_z : [n] \to [n]$, such that $f_z(\tau_1(I)) = \tau_2(J)$ (which implies that $\tau_1(I) = f_z^{-1}(\tau_2(J))$.*

Suppose further that $\Pi = \Pi(\tau_1, \tau_2, Z)$ is a deterministic function and $\Pi \in \{0,1\}^{C'}$, with $C' \leq n/\log^\beta n$. Then $H(\tau_1(I)|I, J, \Pi, Z) \geq \log n - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n$.

Proof. Let us write $Z' = (\tau_2^{-1} \circ f_Z \circ \tau_1, Z)$. Then

1. $H(I|\tau_1, Z') = H(I|\tau_1, \tau_2^{-1} \circ f_Z \circ \tau_1, Z) = H(I|\tau_1, \tau_2, Z) \geq \log(n) - \delta$.
2. $H(\tau_1|Z') = H(\tau_1|\tau_2^{-1} \circ f_Z \circ \tau_1, Z) \geq \log(n!) - C$, where the last inequality follows from the following:

$$\begin{aligned} 2\log(n!) - C &\leq H(\tau_1, \tau_2|Z) \\ &= H(\tau_2^{-1} \circ f_Z \circ \tau_1, \tau_2|Z) \\ &= H(\tau_2^{-1} \circ f_Z \circ \tau_1|Z) + H(\tau_1|\tau_2^{-1} \circ f_Z \circ \tau_1, Z) \\ &\leq \log(n!) + H(\tau_1|\tau_2^{-1} \circ f_Z \circ \tau_1, Z). \end{aligned}$$

Then by Lemma 4.23, $H(\tau_1(I)|I, \Pi, Z') = H(\tau_1(I)|I, \Pi, \tau_2^{-1} \circ f_Z \circ \tau_1, Z) \geq \log n - \log^{(\epsilon_2^* - \beta\epsilon_1^*)} n$, for absolute constants $\epsilon_1^*, \epsilon_2^*$ and for n sufficiently large as a function of β. But since $J = \tau_2^{-1} \circ f_Z \circ \tau_1(I)$, we obtain that

$$H(\tau_1(I)|I, J, \Pi, \tau_2^{-1} \circ f_Z \circ \tau_1, Z) \geq \log n - \log^{\epsilon_2^* - \beta\epsilon_1^*} n.$$

Then the desired result follows since conditioning decreases entropy. □

Lemma 4.26. *Suppose A, B, C are random variables with finite ranges such that $A \perp B \mid C$. Let Ω_A denote the domain of A, and $f : \Omega_A \to \{0,1\}^*$ be a function. It follows that*

$$A \perp B \mid \{C, f(A)\}.$$

Proof. Pick any $x \in \{0,1\}^*$, $a \in \Omega_A, b \in \Omega_B, c \in \Omega_C$. We have that

$$\begin{aligned} &\mathbb{P}[A = a, B = b | C = c, f(A) = x] \\ = \ &\frac{\mathbb{P}[A = a, B = b, f(A) = x | C = c]}{\mathbb{P}[f(A) = x | C = c]}. \end{aligned} \tag{37}$$

If $f(a) \neq x$, then the above is 0, and also

$$\mathbb{P}[A = a | C = c, f(A) = x] \cdot \mathbb{P}[B = b | C = c, f(A) = x] = 0$$

as well. If $f(a) = x$, then (37) is equal to

$$\begin{aligned}\frac{\mathbb{P}[A=a, B=b|C=c]}{\mathbb{P}[f(A)=x|C=c]} &= \frac{\mathbb{P}[A=a|C=c]}{\mathbb{P}[f(A)=x|C=c]} \cdot \mathbb{P}[B=b|C=c] \\ &= \frac{\mathbb{P}[A=a, f(A)=x|C=c]}{\mathbb{P}[f(A)=x|C=c]} \cdot \mathbb{P}[B=b|f(A)=x, C=c] \\ &= \mathbb{P}[A=a|f(A)=x, C=c] \cdot \mathbb{P}[B=b|C=c, f(A)=x],\end{aligned}$$

where the second-to-last inequality follows since

$$\mathbb{P}[B=b|C=c] = \mathbb{P}[B=b|f(A)=x, C=c],$$

as B is conditionally independent of A given C. □

Given a distribution $D \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r, n, \delta, C)$ and a deterministic function $\Pi = \Pi(\Sigma_{\mathtt{A}})$ we define a distribution $\tilde{D}^+$ on the $r-2$ permutation pointer verification problem with some auxiliary randomness Z as follows: To generate a sample $(\Sigma_2, \ldots, \Sigma_{r-2}, I_1, J_1; Y)$ according to $\tilde{D}^+$ we first sample $(\Sigma_1, \ldots, \Sigma_r, I_0, J_0) \sim D$ and let $I_1 = \Sigma_1(I_0)$, $J_1 = \Sigma_r^{-1}(J_0)$ and $Y = (\Pi_1(\Sigma_{\mathtt{A}}), I_0, J_0)$.

$\tilde{D}^+$ as defined above is a candidate "noisy-on-average' (i.e., noisy when averaged over Y — see last paragraph of Definition 4.6) distribution on $r-2$ permutations, and the lemma below asserts that this is indeed the case for slightly larger values of δ and C provided $|\Pi|$ is small. Recall that $\Sigma_{\mathtt{A}} = (\Sigma_1, \Sigma_3, \ldots, \Sigma_r), \Sigma_{\mathtt{B}} = (\Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1})$.

Lemma 4.27. *There exist constants $\epsilon_1^* > 0, \epsilon_2^*$ such that for every odd $r \geq 3$ and $\beta > 0$ there exists n_0 such that for every $n \geq n_0$ the following holds: Suppose $D \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r, n, \delta, C)$, for some $\delta \leq 1/\log^{\beta} n$ and $C \leq n/\log^{\beta} n$. Also suppose that $C' \leq n/\log^{\beta} n$, and that $\Pi = \Pi(\Sigma_{\mathtt{A}})$ is a deterministic function of $\Sigma_{\mathtt{A}}$ such that $|\Pi| \leq C'$. Then for $\delta' = \log^{(\epsilon_2^* - \epsilon_1^* \cdot \beta)} n$ we have $\tilde{D}^+ \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}+}(r-2, n, \delta', \delta' n)$.*

Proof of Lemma 4.27. We need to verify statements (1) – (5) of Definition 4.6 in order to show that $\tilde{D}^+ \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}+}(r-2, n, \delta', \delta' n)$, for an appropriate choice of $\epsilon_1^*, \epsilon_2^*$ and for sufficiently large n (depending only on β). We will show that statement (5) (which does not depend on δ') holds for all $n \in \mathbb{N}$. To verify statements (1) – (4), we will show that for each of these statements, there are some absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$ and some $\hat{n}_0$ (depending only on β) such that for $n \geq \hat{n}_0$, the statement holds with $\delta' = \log^{(\hat{\epsilon}_2^* - \hat{\epsilon}_1^* \beta)} n$. The proof of the lemma will follow by choosing ϵ_2^* to be the maximum of the individual $\hat{\epsilon}_2^*$, ϵ_1^* to be the minimum of the individual $\hat{\epsilon}_1^*$, and n_0 to be the maximum of the individual $\hat{n}_0$.

We now proceed to verify each of the statements (1) – (5). We remark that the values of $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*, \hat{n}_0$ may change from line to line.

1. We first verify that $H(I_1|I_0, J_0, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi) \geq \log(n) - \delta'$. Since conditioning can only reduce entropy, it suffices to find a lower bound on $H(I_1|\mathbb{1}[\Sigma_1^r(I_0) = J_0], I_0, J_0, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi)$, and in particular, it suffices to find a lower bound on $H(I_1|\Sigma_1^r(I_0) \neq J_0, I_0, J_0, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi)$ and on $H(I_1|\Sigma_1^r(I_0) = J_0, I_0, J_0, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi)$.

   We first bound the former. Consider the distribution of $I_0, J_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_r$ conditioned on the event $\Sigma_1^r(I_0) \neq J_0$, and let $Z = (\Sigma_2, \Sigma_3, \ldots, \Sigma_{r-1}, \Sigma_r)$. We will now use Lemma 4.23 with $I = I_0, \pi = \Sigma_1$, and with the distribution being D conditioned on $\Sigma_1^r(I_0) \neq J_0$. To apply this lemma, we first verify its preconditions:

(a) $H(I_0|\Sigma_1, Z, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - 5\delta$ as long as n is large enough so that $\delta \leq 1/50$. To see this, conditions (1a) and (3a) of the distribution $D \in D_{\mathrm{PV}}^{\mathrm{Mix}}(r, n, \delta, C)$ (recall Definition 4.6) imply that

$$H((I_0, \mathbb{1}[\Sigma_1^r(I_0) = J_0])|\Sigma_1, \Sigma_2, \ldots, \Sigma_r) \geq 1 + \log(n) - 2\delta,$$

meaning that

$$\begin{aligned} & H(I_0|\mathbb{1}[\Sigma_1^r(I_0) = J_0], \Sigma_1, \Sigma_2, \ldots, \Sigma_r) \\ = \; & \mathbb{P}[\Sigma_1^r(I_0) = J_0] \cdot H(I_0|\Sigma_1^r(I_0) = J_0, \Sigma_1, \ldots, \Sigma_r) \\ & + \mathbb{P}[\Sigma_1^r(I_0) \neq J_0] \cdot H(I_0|\Sigma_1^r(I_0) \neq J_0, \Sigma_1, \ldots, \Sigma_r) \\ \geq \; & \log(n) - 2\delta. \end{aligned}$$

By Pinsker's inequality and condition (3a) of D we have that $|\mathbb{P}[\Sigma_1^r(I_0) = J_0] - 1/2| \leq \sqrt{\delta/2}$, so for sufficiently small δ (in particular, such that $\sqrt{\delta/2} \leq 1/10$), it follows that

$$\min\{H(I_0|\Sigma_1^r(I_0) = J_0, \Sigma_1, \ldots, \Sigma_r), H(I_0|\Sigma_1^r(I_0) \neq J_0, \Sigma_1, \ldots, \Sigma_r)\} \geq \log(n) - 5\delta. \quad (38)$$

(b) $H(\Sigma_1|Z, \Sigma_1^r(I_0) \neq J_0) \geq \log(n!) - 3C - 3\delta$ as long as n is large enough so that $\delta \leq 1/18$. The proof is similar to (a) above. In particular, condition (2) of the distribution D implies that

$$H(\Sigma_1|\Sigma_2, \Sigma_3, \ldots, \Sigma_r) \geq \log(n!) - C.$$

Since conditioning can only reduce entropy, condition (3a) of the distribution D implies that

$$H((\Sigma_1, \mathbb{1}[\Sigma_1^r(I_0) = J_0])|\Sigma_2, \ldots, \Sigma_r) \geq 1 + \log(n!) - C - \delta,$$

meaning that

$$\begin{aligned} & H(\Sigma_1|\mathbb{1}[\Sigma_1^r(I_0) = J_0], \Sigma_2, \ldots, \Sigma_r) \\ = \; & \mathbb{P}[\Sigma_1^r(I_0) = J_0] \cdot H(\Sigma_1|\Sigma_1^r(I_0) = J_0, \Sigma_2, \ldots, \Sigma_r) + \mathbb{P}[\Sigma_1^r(I_0) \neq J_0] \cdot H(\Sigma_1|\Sigma_1^r(I_0) \neq J_0, \Sigma_2, \ldots, \Sigma_r) \\ \geq \; & \log(n!) - C - \delta. \end{aligned}$$

By Pinsker's inequality and condition (3a) of D we have that $|\mathbb{P}[\Sigma_1^r(I_0) = J_0] - 1/2| \leq \sqrt{\delta/2}$, so for sufficiently small δ (in particular, such that $\sqrt{\delta/2} \leq 1/6$), it follows that

$$\min\{H(\Sigma_1|\Sigma_1^r(I_0) = J_0, \Sigma_2, \ldots, \Sigma_r), H(\Sigma_1|\Sigma_1^r(I_0) \neq J_0, \Sigma_2, \ldots, \Sigma_r)\} \geq \log(n!) - 3C - 3\delta. \quad (39)$$

Note also that indeed Π is a deterministic function of $(\pi, Z) = (\Sigma_1, \Sigma_2, \ldots, \Sigma_r)$. Therefore, by Lemma 4.23, we obtain that there are absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$, such that for some $\hat{n}_0$ depending only on β, if $n \geq \hat{n}_0$,

$$H(I_1|I_0, \Sigma_2, \ldots, \Sigma_r, \Pi, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n.$$

Condition (4a) of the distribution D implies that

$$H(J_0|I_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) = H(J_0|I_0, I_1, \Pi, \Sigma_1, \Sigma_2, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - \delta.$$

Since conditioning can only reduce entropy we have from the two above equations that

$$H((I_1, J_0)|I_0, \Pi, \Sigma_2, \Sigma_3, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) \geq 2\log(n) - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n - \delta,$$

so

$$H(I_1|I_0, J_0, \Pi, \Sigma_2, \Sigma_3, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n - \delta,$$

as desired.

Next we lower bound $H(I_1|\Sigma_1^r(I_0) = J_0, I_0, J_0, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi)$ using Lemma 4.25 with $Z = (\Sigma_2, \Sigma_3, \ldots, \Sigma_{r-1})$, $\tau_1 = \Sigma_1, \tau_2 = \Sigma_r^{-1}$, and with the distribution being D conditioned on $\Sigma_1^r(I_0) = J_0$. We first verify that the lemma's preconditions hold:

(a) The fact that $H(I_0|\Sigma_1, \Sigma_r, Z, \Sigma_1^r(I_0) = J_0) \geq \log(n) - 5\delta$ for $\delta \leq 1/50$ was proven in (38).

(b) To verify that $H(\Sigma_1, \Sigma_r|Z, \Sigma_1^r(I_0) = J_0) \geq \log(n) - 3C - 3\delta$ for $\delta \leq 1/18$, we may exactly mirror the proof of (39) except for replacing Σ_1 with (Σ_1, Σ_r) (and removing Σ_r from the random variables being conditioned on). We omit the details.

(c) Since we are conditioning on $\Sigma_1^r(I_0) = J_0$, we have that $\Sigma_r^{-1}(J_0) = \Sigma_{r-1}(\cdots\Sigma_2(\Sigma_1(I_0)))$, which means that we may take $f_Z = \Sigma_{r-1} \circ \cdots \circ \Sigma_2$.

Note also that indeed Π is a deterministic function of $(\tau_1, \tau_2, Z) = (\Sigma_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Sigma_r^{-1})$. Then by Lemma 4.25, it follows that for some absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$, there is some $\hat{n}_0$ (depending only on β) such that for $n \geq \hat{n}_0$, $H(I_1|I_0, J_0, \Pi, Z, \Sigma_1^r(I_0) = J_0) \geq \log n - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n$.

By the previous discussion, it then follows that for some absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$, there is some $\hat{n}_0$ (depending only on β) such that for $n \geq \hat{n}_0$, $H(I_1|I_0, J_0, \Pi, \Sigma_2, \ldots, \Sigma_{r-1}) \geq \log n - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n$.

In an identical manner, using conditions (1b), (2), (3b), (4b) of the distribution $D \in D_{\mathrm{PV}}^{\mathrm{Mix}}(r, n, \delta, C)$, we obtain that for the same $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*, \hat{n}_0$, if $n \geq n_0$ then $H(J_1|I_0, J_0, \Pi, \Sigma_2, \ldots, \Sigma_r) \geq \log(n) - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n$.

2. To prove statement (2) we claim that $H(\Sigma_2, \ldots, \Sigma_{r-1}|\Pi, I_0, J_0) \geq (r-2)\log(n!) - C - C' - 2\log(n)$; to see this note that

$$\begin{aligned} H(\Sigma_2, \ldots, \Sigma_{r-1}|\Pi, I_0, J_0) &= H(\Sigma_2, \ldots, \Sigma_{r-1}) + H(\Pi, I_0, J_0|\Sigma_2, \ldots, \Sigma_{r-1}) - H(\Pi, I_0, J_0) \\ &\geq H(\Sigma_2, \ldots, \Sigma_{r-1}) - H(\Pi, I_0, J_0) \\ &\geq (r-2)\log(n!) - C - C' - 2\log(n), \end{aligned}$$

since $|\Pi| \leq C'$. It readily follows that there exist absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$ and some $\hat{n}_0$ (depending only on β) such that for $n \geq \hat{n}_0$, $H(\Sigma_2, \ldots, \Sigma_{r-1}|\Pi, I_0, J_0) \geq (r-2)\log(n!) - n\log^{(\hat{\epsilon}_2^* - \hat{\epsilon}_1^*\beta)} n$.

3. We will next prove that 3(b) holds by applying Lemma 4.18, with $I = I_0, J = J_{r-1}, \Sigma = \Sigma_1, Z = (\Sigma_2, \ldots, \Sigma_r)$ (recall that $J_{r-1} = \Sigma_2^{-1} \circ \cdots \circ \Sigma_r^{-1}(J_0)$). We will first verify that the preconditions of Lemma 4.18 hold:

(a) $H(I|\Sigma, Z) = H(I_0|\Sigma_1, \Sigma_2, \ldots, \Sigma_r) \geq \log(n) - \delta$, by condition (1) of the distribution D.

(b) $H(\Sigma|Z) = H(\Sigma_1|\Sigma_2, \ldots, \Sigma_r) \geq \log n! - C$, by condition (2) of the distribution D.

(c) $H(\mathbb{1}[\Sigma(I) = J]|\Sigma, I, Z) = H(\mathbb{1}[\Sigma_1(I_0) = J_{r-1}]|\Sigma_1, I_0, \Sigma_2, \ldots, \Sigma_r)$
$= H(\mathbb{1}[\Sigma_1^r(I_0) = J_0]|I_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_r)$
$\geq 1 - \delta,$
by condition (3) of the distribution D.

(d) $H(J|\Sigma, I, \Sigma(I) \neq J, Z) = H(J_{r-1}|\Sigma_1, I_0, \Sigma_1(I_0) \neq J_{r-1}, \Sigma_2, \ldots, \Sigma_r)$
$= H(J_0|I_0, \Sigma_1, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0)$
$\geq \log(n) - \delta,$
by condition (4) of the distribution D,

where by assumption, there exists $\beta > 0$ such that δ, C, C' are such that $\max\{\delta, C/n, C'/n\} \leq 1/\log^\beta(n)$. Moreover, Π is a deterministic function of $(\Sigma, Z) = (\Sigma_1, \ldots, \Sigma_r)$. Therefore by Lemma 4.18 we get that, for some absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$, and for some $\hat{n}_0$ (depending only on β),

$$H(\mathbb{1}[\Sigma_1(I_0) = J_{r-1}]|\Sigma_2, \ldots, \Sigma_r, \Pi, I_0, J_{r-1}) = H(\mathbb{1}[\Sigma(I) = J]|\Pi, I, J, Z) \tag{40}$$
$$\geq 1 - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n, \tag{41}$$

Since $J_0 = \Sigma_r \circ \cdots \circ \Sigma_2(J_{r-1})$ and $J_1 = \Sigma_{r-1} \circ \cdots \circ \Sigma_2(J_{r-1})$, by the data processing inequality, we get that for $n \geq \hat{n}_0$,

$$H(\mathbb{1}[\Sigma_2^{r-2}(I_1) = J_1]|J_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi, I_0, J_0) \geq H(\mathbb{1}[\Sigma_1(I_0) = J_{r-1}]|\Sigma_2, \ldots, \Sigma_r, \Pi, I_0, J_{r-1})$$
$$\geq 1 - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n.$$

The proof of 3(a) (with the same $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*, \hat{n}_0$) follows in a symmetric manner.

4. Next we lower bound $H(J_1|I_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Sigma_1^r(I_0) \neq J_0, \Pi, I_0, J_0)$. We apply Lemma 4.23 with $Z = (I_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_{r-1})$, $I = J_0$, $\Sigma = \Sigma_r^{-1}$, with the distribution given by D conditioned on $\Sigma_1^r(I_0) \neq J_0$. We first verify that the preconditions are met:

   (a) $H(J_0|\Sigma_r, Z, \Sigma_1^r(I_0) \neq J_0) = H(J_0|I_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_r, \Sigma_1^r(I_0) \neq J_0) \geq \log(n) - \delta$, by condition (4a) of the distribution D.

   (b) As long as n is large enough so that $\delta \leq 1/18$,

   $$H(\Sigma_r|Z, \Sigma_1^r(I_0) \neq J_0) = H(\Sigma_r|I_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Sigma_1^r(I_0) \neq J_0) \geq \log(n!) - 3C - 3\delta - \log n,$$

   by an argument identical to that used to prove (39), as well as the fact that $I_0 \in [n]$, meaning that its entropy is at most $\log n$.

Moreover, Π is a deterministic function of $(\Sigma, Z) = (\Sigma_1, \Sigma_2, \ldots, \Sigma_r, I_0)$. Then by Lemma 4.23, it follows that there are absolute constants $\hat{\epsilon}_1^*, \hat{\epsilon}_2^*$ and some $\hat{n}_0$ (depending only on β) such that for $n \geq \hat{n}_0$,

$$\begin{aligned} & H(J_1|I_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_{r-1}, J_0, \Pi, \Sigma_1^r(I_0) \neq J_0) \\ = \;& H(J_1|I_1, \Sigma_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi, I_0, J_0, \Sigma_1^r(I_0) \neq J_0) \\ \geq \;& \log(n) - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n, \end{aligned}$$

which proves the desired statement since conditioning can only reduce entropy. Similarly, conditions (2), (3b), (4b) of D imply in a symmetric manner that for $n \geq \hat{n}_0$, $H(I_1|J_1, \Sigma_2, \Sigma_3, \ldots, \Sigma_{r-1}, \Sigma_1^r(I_0) \neq J_0, \Pi, I_0, J_0) \geq \log(n) - \log^{(\hat{\epsilon}_2^* - \beta\hat{\epsilon}_1^*)} n$.

5. To prove statement (5), first take t odd, and let $X = \Sigma_{\mathtt{A}} \cap (\Sigma_1, \Sigma_2, \ldots, \Sigma_t, \Sigma_{r-t+1}, \ldots, \Sigma_{r-1}, \Sigma_r)$, $Y = \Sigma_{\mathtt{B}}$, and note that condition (5) of the distribution D states that conditioned on:

$$E := \{(I_0, \ldots, I_t) = (i_0, \ldots, i_t), (J_0, \ldots, J_t) = (j_0, \ldots, j_t), (\Sigma_{t+2}, \Sigma_{t+4}, \ldots, \Sigma_{r-t-1}) = (\sigma_{t+2}, \sigma_{t+4}, \ldots, \sigma_{r-t-1})\},$$

we have that X is independent of Y. Note that conditioned on E, $\Pi = \Pi(\Sigma_1, \Sigma_3, \ldots, \Sigma_r)$ is a deterministic function of $(\Sigma_1, \Sigma_3, \ldots, \Sigma_t, \Sigma_{r-t+1}, \Sigma_{r-t+3}, \ldots, \Sigma_r) = X$. It follows by Lemma 4.26 that $X \perp Y | E, \Pi = \pi$, which implies that

$$\Sigma_{\mathtt{A}} \cap (\Sigma_2, \ldots, \Sigma_t, \Sigma_{r-t+1}, \ldots, \Sigma_{r-1}) \perp \Sigma_{\mathtt{B}} | E, \Pi = \pi.$$

Next take t even, take $X = \Sigma_{\mathtt{A}}$, $Y = \Sigma_{\mathtt{B}} \cap (\Sigma_1, \Sigma_2, \ldots, \Sigma_t, \Sigma_{r-t+1}, \ldots, \Sigma_r)$, and conditioned on:

$$E := \{(I_0, \ldots, I_t) = (i_0, \ldots, i_t), (J_0, \ldots, J_t) = (j_0, \ldots, j_t), (\Sigma_{t+2}, \Sigma_{t+4}, \ldots, \Sigma_{r-t-1}) = (\sigma_{t+2}, \pi_{t+4}, \ldots, \sigma_{r-t-1})\},$$

X is independent of Y. Note that conditioned on E, $\Pi = \Pi(\Sigma_1, \Sigma_3, \ldots, \Sigma_r)$ is a deterministic function of X. It follows by Lemma 4.26 that $X \perp Y | E, \Pi = \pi$, which implies that

$$\Sigma_{\mathtt{B}} \cap (\Sigma_2, \ldots, \Sigma_t, \Sigma_{r-t+1}, \ldots, \Sigma_{r-1}) \perp \Sigma_{\mathtt{A}} | E, \Pi = \pi.$$

□

Lemma 4.27 establishes that the "inner input" (after removing the Σ_1 and Σ_r and pushing pointers inwards) is from a noisy distribution (according to Definition 4.6) when averaged over the auxiliary variable Y. Intuitively this should imply that the pointer verification problem remains as hard (with one fewer round of communication), but this needs to be shown formally. In particular, Alice and Bob do have additional information such as $\Sigma_1, \Sigma_r, I_0, J_0, \Pi$ and all of this might help determine $\mathbb{1}[\Sigma_2^{r-1}(I_1) = J_1]$.

In Lemma 4.17 we formalize this intuition by creating an $(r+1)/2$ round protocol for a noisy distribution $\tilde{D}$ on $r-2$ permutations, using an $(r+3)/2$ round protocol for a related noisy distribution D solving the pointer verification problem on r permutations. This argument makes use of Property (5) of Definition 4.6, which we have not really used yet (except to argue that it holds inductively).

Proof of Lemma 4.17. Let $\epsilon_1^*, \epsilon_2^*$ be the absolute constants from Lemma 4.27. We will show that we can take $\beta_1 = \max\left\{\beta_2, \frac{2\beta_2 + \epsilon_2^*}{\epsilon_1^*}\right\}$.

Let $D \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r, n, 1/\log^{\beta_1} n, n/\log^{\beta_1} n)$ and let Π be a protocol for D with communication at most $n/\log^{\beta_1} n$. For sufficiently large n, we will give a distribution $\tilde{D} \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$, and will construct a protocol $\tilde{\Pi}$ for $\tilde{D}$, which uses no more communication than Π, and crucially uses one less round of communication than Π.

Definition of $\tilde{D}$. We denote the messages in each round of Π by $\Pi_1, \ldots, \Pi_{(r+3)/2}$. Recall that Alice sends $\Pi_1 = \Pi_1(\Sigma_1, \Sigma_3, \ldots, \Sigma_r)$, Bob sends $\Pi_2 = \Pi_2(\Pi_1, I_0, J_0, \Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1})$, Alice sends $\Pi_3 = \Pi_3(\Pi_1, \Pi_2, \Sigma_1, \Sigma_3, \ldots)$, and so on. Let (π_1, i_0, j_0) be a fixed instantiation of the random variables (Π_1, I_0, J_0). Given the distribution D on $(I_0, I_1, J_0, J_1, \Sigma_1, \ldots, \Sigma_r)$, consider the conditional distribution $D_{\pi_1, i_0, j_0} := D | (\Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0)$ on $(I_1, J_1, \Sigma_1, \ldots, \Sigma_r)$. Furthermore, let $\tilde{D}_{\pi_1, i_0, j_0}$ denote the marginal distribution of D_{π_1, i_0, j_0} on the inner inputs, that

is, $(I_1, J_1, \Sigma_2, \ldots, \Sigma_{r-1})$. One can interpret $\tilde{D}_{\pi_1,i_0,j_0}$, as an $(r-2)$-PV problem, and we will show how, for *each* tuple (π_1, i_0, j_0), Alice and Bob can simulate the protocol Π, given an instance from $\tilde{D}_{\pi_1,i_0,j_0}$. We will then show how it follows that for *some* tuple (π_1, i_0, j_0) this simulation will have success probability at least $1/2 + \epsilon_2$ and moreover for this tuple $\tilde{D}_{\pi_1,i_0,j_0} \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$.

The protocol $\tilde{\Pi}$. Consider any tuple (π_1, i_0, j_0), and an instance of $(r-2)$-PV drawn from $\tilde{D} = \tilde{D}_{\pi_1,i_0,j_0}$. We use the symbol $\tilde{}$ for the random variables drawn from $\tilde{D}$. We label the $r-2$ permutations drawn from $\tilde{D}$ as $\tilde{\Sigma}_2, \ldots, \tilde{\Sigma}_{r-1}$ (instead of $\Sigma_1, \ldots, \Sigma_{r-2}$), the initial indices as $(\tilde{I}_1, \tilde{J}_1)$ (instead of (I_0, J_0)). The roles of Alice and Bob are also flipped, in that Bob receives $\tilde{\Sigma}_2, \tilde{\Sigma}_4, \ldots, \tilde{\Sigma}_{r-1}$, and Alice receives $\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_3, \ldots, \tilde{\Sigma}_{r-2}$. The goal is to determine whether $\tilde{\Sigma}_2^{r-1}(\tilde{I}_1) = \tilde{J}_1$. The protocol $\tilde{\Pi}$ for $\tilde{D}$ is constructed as follows:

1. Bob sends the first message $\tilde{\Pi}_2 := \Pi_2(\pi_1, i_0, j_0, \tilde{\Sigma}_2, \ldots, \tilde{\Sigma}_{r-1})$. Recall that Π_2 was the second message of the protocol Π.

2. Alice then draws $(\tilde{\Sigma}_1, \tilde{\Sigma}_r)$ from its marginal in D_{π_1,i_0,j_0}, conditioned on the event $\{I_1 = \tilde{I}_1, J_1 = \tilde{J}_1, \Sigma_3 = \tilde{\Sigma}_3, \Sigma_5 = \tilde{\Sigma}_5, \ldots, \Sigma_{r-2} = \tilde{\Sigma}_{r-2}\}$, using private randomness. That is,

$$(\tilde{\Sigma}_1, \tilde{\Sigma}_r) \sim [(\Sigma_1, \Sigma_r)_{D_{\pi_1,i_0,j_0}} | \{I_1 = \tilde{I}_1, J_1 = \tilde{J}_1, \Sigma_3 = \tilde{\Sigma}_3, \Sigma_5 = \tilde{\Sigma}_5, \ldots, \Sigma_{r-2} = \tilde{\Sigma}_{r-2}\}]. \quad (42)$$

3. After receiving $\tilde{\Pi}_2$ from Bob, Alice then sends $\tilde{\Pi}_3 := \Pi_3(\pi_1, \tilde{\Pi}_2, \tilde{\Sigma}_1, \tilde{\Sigma}_3, \ldots, \tilde{\Sigma}_r)$. Starting with Alice's $\tilde{\Pi}_3$, Alice and Bob just simulate the remaining $(r+3)/2 - 2$ rounds of the protocol Π (incuding the output bit at the end of the last message), where Alice takes as her input $\tilde{\Sigma}_1, \tilde{\Sigma}_3, \ldots, \tilde{\Sigma}_{r-2}, \tilde{\Sigma}_r$ and Bob takes as his input $i_0, j_0, \tilde{\Sigma}_2, \ldots, \tilde{\Sigma}_{r-1}$.

Since the messages of $\tilde{\Pi}$ are given by $\Pi_2, \Pi_3, \ldots, \Pi_{(r+3)/2}$ for appropriate inputs of Π, $\tilde{\Pi}$ has $(r+1)/2$ rounds, and the communication cost of $\tilde{\Pi}$ is no greater than the communication cost of Π, namely $n/\log^{\beta_1} n$.

Success Probability. Now we will prove that for each tuple (i_0, j_0, π_1), the success probability of $\tilde{\Pi}$ when inputs are drawn from $\tilde{D}_{i_0,j_0,\pi_1}$ is equal to the success probability of Π on the distribution D conditioned on $\{\Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0\}$. This will ultimately allow us to choose an appropriate tuple (π_1, i_0, j_0) for which $\tilde{\Pi}$ achieves success probability at least $1/2 + \epsilon_2$ on $\tilde{D}_{\pi_1,i_0,j_0}$.

Notice that the protocol $\tilde{\Pi}$ induces a distribution on $(\tilde{\Sigma}_1, \ldots, \tilde{\Sigma}_r, \tilde{I}_1, \tilde{J}_1)$, which we will denote by $\tilde{D}_{\Pi}$, where $(\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_2, \ldots, \tilde{\Sigma}_{r-1})$ is drawn from $\tilde{D}_{\pi_1,i_0,j_0}$ and Alice draws $(\tilde{\Sigma}_1, \tilde{\Sigma}_r)$ from the conditional distribution specified in step (2) above, using private randomness.

We claim that the distribution of $(\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_1, \ldots, \tilde{\Sigma}_r)$ under $\tilde{D}_{\Pi}$ is the same as the distribution of $(I_1, J_1, \Sigma_1, \ldots, \Sigma_r)$ under D_{π_1,i_0,j_0}. One can think of drawing $(I_1, J_1, \Sigma_1, \ldots, \Sigma_r)$ from D_{π_1,i_0,j_0} as first drawing $(I_1, J_1, \Sigma_2, \ldots, \Sigma_{r-1})$ from its marginal distribution $\tilde{D}_{\pi_1,i_0,j_0}$ and then drawing (Σ_1, Σ_r) from $D_{\pi_1,i_0,j_0}|\{(I_1, J_1, \Sigma_2, \Sigma_3, \ldots, \Sigma_{r-1})\}$. By construction, the marginal distribution of $(\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_2, \ldots, \tilde{\Sigma}_{r-1})$ under $\tilde{D}_{\Pi}$ is the same as the marginal distribution of $(I_1, J_1, \Sigma_2, \ldots, \Sigma_{r-1})$ under D_{π_1,i_0,j_0}. Formally, for $i_1, j_1 \in [n], \sigma_2, \ldots, \sigma_{r-1} \in \mathcal{S}_n$,

$$\mathbb{P}_{\tilde{D}_{\Pi}}\left[\tilde{I}_1 = i_1, \tilde{J}_1 = j_1, \tilde{\Sigma}_2 = \sigma_2, \ldots, \tilde{\Sigma}_{r-1} = \sigma_{r-1}\right] = \mathbb{P}_{D_{\pi_1,i_0,j_0}}\left[I_1 = i_1, J_1 = j_1, \Sigma_2 = \sigma_2, \ldots, \Sigma_{r-1} = \sigma_{r-1}\right]. \quad (43)$$

It is not clear a priori that the conditional distributions of (Σ_1, Σ_r) under D_{π_1,i_0,j_0} and of $(\tilde{\Sigma}_1, \tilde{\Sigma}_r)$ under $\tilde{D}_\Pi$ are the same, since in $\tilde{D}_\Pi$, Alice draws $(\tilde{\Sigma}_1, \tilde{\Sigma}_r)$ with knowledge of only $(\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_3, \tilde{\Sigma}_5, \ldots, \tilde{\Sigma}_{r-2})$, whereas under D_{π_1,i_0,j_0}, (Σ_1, Σ_r) is drawn from the conditional distribution with knowledge of all the permutations $(\Sigma_2, \Sigma_3, \ldots, \Sigma_{r-1})$. Nevertheless we will show that these two distributions are the same. More formally, for any $\sigma_1, \ldots, \sigma_r \in \mathcal{S}_n, i_1, j_1 \in [n]$,

$$\begin{aligned}
& \mathbb{P}_{D_{\pi_1,i_0,j_0}}[\Sigma_1 = \sigma_1, \Sigma_r = \sigma_r | I_1 = i_1, J_1 = j_1, \Sigma_2 = \sigma_2, \Sigma_3 = \sigma_3, \ldots, \Sigma_{r-1} = \sigma_{r-1}] \\
= \; & \mathbb{P}_{D_{\pi_1,i_0,j_0}}[\Sigma_1 = \sigma_1, \Sigma_r = \sigma_r | I_1 = i_1, J_1 = j_1, \Sigma_3 = \sigma_3, \Sigma_5 = \sigma_5, \ldots, \Sigma_{r-2} = \sigma_{r-2}] \qquad (44) \\
= \; & \mathbb{P}_{\tilde{D}_\Pi}[\tilde{\Sigma}_1 = \sigma_1, \tilde{\Sigma}_r = \sigma_r | \tilde{I}_1 = i_1, \tilde{J}_1 = j_1, \tilde{\Sigma}_3 = \tilde{\sigma}_3, \tilde{\Sigma}_5 = \sigma_5, \ldots, \tilde{\Sigma}_{r-2} = \sigma_{r-2}], \qquad (45)
\end{aligned}$$

where the second equality follows from construction (i.e., (42)), and the first equality follows from property (5) of the distribution $D \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r, n, 1/\log^{\beta_1} n, n/\log^{\beta_1} n)$ with $t = 1$. That is, under the distribution D, for all $\pi_1, i_0, j_0, \sigma_3, \ldots, \sigma_{r-2}$,

$$(\Sigma_1, \Sigma_r) \perp (\Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1}) | \{\Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0, I_1 = i_1, J_1 = j_1, \Sigma_3 = \sigma_3, \Sigma_5 = \sigma_5, \ldots, \Sigma_{r-2} = \sigma_{r-2}\}.$$

As a consequence, under the distribution D_{π_1,i_0,j_0},

$$(\Sigma_1, \Sigma_r) \perp (\Sigma_2, \Sigma_4, \ldots, \Sigma_{r-1}) | \{I_1 = i_1, J_1 = j_1, \Sigma_3 = \sigma_3, \Sigma_5 = \sigma_5, \ldots, \Sigma_{r-2} = \sigma_{r-2}\},$$

which verifies (44) and therefore our claim that the distribution of $(\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_1, \ldots, \tilde{\Sigma}_r)$ under $\tilde{D}_\Pi$ is the same as the distribution of $(I_1, J_1, \Sigma_1, \ldots, \Sigma_r)$ under D_{π_1,i_0,j_0}.

It follows that for each tuple (i_0, j_0, π_1), $\tilde{\Pi}$ is a protocol for the $(r-2)$-PV problem with success probability equal to:

$$\begin{aligned}
& \mathbb{P}_{\tilde{D}_{\pi_1,i_0,j_0}}[\tilde{\Pi}(\tilde{I}_1, \tilde{J}_1, \tilde{\Sigma}_2, \tilde{\Sigma}_3, \ldots, \tilde{\Sigma}_{r-1}) = \mathbb{1}[\tilde{\Sigma}_2^{r-1}(\tilde{I}_1) = \tilde{J}_1]] \\
= \; & \mathbb{P}_D[\Pi(i_0, j_0, \Sigma_1, \Sigma_2, \ldots, \Sigma_r) = \mathbb{1}[\Sigma_1^r(I_0) = J_0] | I_0 = i_0, J_0 = j_0, \Pi_1 = \pi_1]. \qquad (46)
\end{aligned}$$

(In the above expression, for a protocol Π with inputs X, Y, we use $\Pi(X, Y)$ to denote the output bit of Π, which is the same as the last bit of the transcript of Π.)

Membership in $\mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$. By hypothesis, we have that

$$D \in \mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r, n, 1/\log^{\beta_1} n, n/\log^{\beta_1} n),$$

and that $|\Pi_1| \le n/\log^{\beta_1} n$. By Lemma 4.27, for some n_0 that depends only on β_1 (which in turn depends only on β_2), for $n \ge n_0$,

$$\tilde{D}^+ \in \mathcal{D}^{\mathrm{Mix}+}_{\mathrm{PV}}(r, n, \log^{(\epsilon_2^* - \epsilon_1^* \beta_1)} n, n \log^{(\epsilon_2^* - \epsilon_1^* \beta_1)} n).$$

By definition of β_1, we have that $\frac{\epsilon_1^* \beta_1 - \epsilon_2^*}{2} \ge \beta_2$, so $\sqrt{\log^{(\epsilon_2^* - \epsilon_1^* \beta_1)} n} \le 1/\log^{\beta_2} n$. We call the tuple (i_0, j_0, π_1) **good** if the distribution of $(I_1, J_1, \Sigma_2, \ldots, \Sigma_{r-1})$ under $\tilde{D}_{\pi_1,i_0,j_0}$ belongs to $\mathcal{D}^{\mathrm{Mix}}_{\mathrm{PV}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$. Recall that this means that

1. $H(I_1 | \Sigma_2, \ldots, \Sigma_{r-1}, \Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0) \ge \log(n) - 1/\log^{\beta_2} n$.
2. $H(\Sigma_2, \ldots, \Sigma_{r-1} | \Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0) \ge (r-2)\log(n!) - n/\log^{\beta_2} n$.

3. $H(\mathbb{1}[\Sigma_1^r(I_1) = J_1] | I_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0) \geq 1 - 1/\log^{\beta_2} n$.

4. $H(J_1 | I_1, \Sigma_2, \ldots, \Sigma_{r-1}, \Sigma_1^r(I_0) \neq J_0, \Pi_1 = \pi_1, I_0 = i_0, J_0 = j_0) \geq \log(n) - 1/\log^{\beta_2} n$,

and analogously the (b) statements in the definition of $\mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$ (Definition 4.6) hold as well.

By Lemma 4.27, Markov's inequality, and a union bound, if $n \geq n_0$, with probability at least $1 - 7/\log^{\beta_2} n$ over the tuple (I_0, J_0, Π_1) drawn from its marginal in D, (I_0, J_0, Π_1) is good. (Notice that there is a coefficient of 7, as opposed to 8, since there is no (b) statement for item (2) above.)

Choosing a good tuple (i_0, j_0, π_1). Now we will use (46) to choose a good tuple (i_0, j_0, π_1) for which $\tilde{\Pi}$ also achieves success probability at least $1/2 + \epsilon_2$, for all $n > \max\left\{n_0, 2^{(7/(\epsilon_1 - \epsilon_2))^{1/\beta_2}}\right\}$. For each tuple (i_0, j_0, π_1), we have constructed above a protocol $\tilde{\Pi}$ for $(r-2)$-PV, with communication at most $n/\log^{\beta_1} n \leq n/\log^{\beta_2} n$, and where Alice and Bob use $(r+1)/2$ rounds of communication. If moreover (i_0, j_0, π_1) is good, then the distribution of $(I_1, J_1, \Sigma_2, \ldots, \Sigma_{r-1})$ under $\tilde{D}_{i_0, j_0, \pi_1}$ belongs to $\mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$.

Now suppose for the purpose of contradiction that the probability of success of all $((r+1)/2, n/\log^{\beta_2} n)$ protocols on any distribution $\tilde{D} \in \mathcal{D}_{\mathrm{PV}}^{\mathrm{Mix}}(r-2, n, 1/\log^{\beta_2} n, n/\log^{\beta_2} n)$ were at most $1/2 + \epsilon_2$. In particular, for any good tuple (i_0, j_0, π_1), the probability of success of $\tilde{\Pi}$ on the distribution $\tilde{D}_{\pi_1, i_0, j_0}$ is at most $1/2 + \epsilon_2$. Then by (46) and since $n \geq n_0$, the probability of success of Π would be at most

$$7/\log^{\beta_2} n + (1 - 7/\log^{\beta_2} n) \cdot (1/2 + \epsilon_2) \leq 1/2 + 7/\log^{\beta_2} n + \epsilon_2.$$

Since we also have $n > 2^{(7/(\epsilon_1 - \epsilon_2))^{1/\beta_2}}$, it follows that

$$\epsilon_2 + 7/\log^{\beta_2} n < \epsilon_1,$$

which is a contradiction and thus completes the proof of Lemma 4.17.

□

5 Rounds-Communication Tradeoffs in Amortized Setting

In this section, our main goal is to prove the following theorem stating, roughly, that for the source $\mu_{r,n,\ell}$, there is an efficient protocol (i.e., one with little communication) for CRG and SKG with many rounds, but that there is no efficient protocol with few rounds.

Theorem 5.1. *For each $r \in \mathbb{N}, \gamma \in (0,1)$, there is a constant $c_0 > 0$ such that for $n \geq c_0$, there is a source $\mu_{r,n,\ell}$, such that:*

1. *The tuple $((r+2)\lceil \log n \rceil, \ell)$ is $(r+2)$-achievable for SKG (and thus CRG) from $\mu_{r,n,\ell}$.*
2. *Set $\ell = n$. For any $C, L \in \mathbb{R}$ with $C \leq n/\log^{c_0} n$ and $L > \gamma\ell$, the tuple (C, L) is not $\lfloor (r+1)/2 \rfloor$-achievable for CRG (and thus for SKG) from $\mu_{r,n,n}$.*
3. *Again set $\ell = n$. For any $C, L \in \mathbb{R}$ with $C \leq \sqrt{n}/\log^{c_0} n$ and $L > \gamma\ell$, the tuple (C, L) is not r-achievable for CRG (and thus for SKG) from $\mu_{r,n,n}$.*

5.1 Using the Compression of Information to Communication

We will prove Theorem 5.1 by reducing to the non-amortized setting; in particular, we will use Theorems 4.6 and 4.7 as a black-box. A crucial technical ingredient in doing so is the use of an "compression of internal information cost to communication" result for bounded round protocols, saying that for any protocol with a fixed number r of rounds and internal information cost I, there is another protocol with the same number r of rounds and communication cost not much larger than I. As we discussed in Section 2, these types of theorems were originally proved in order to establish direct sum and direct product results for communication complexity. Our use of these compression results may be interpreted as a roughly analogous approach for the setting of amortized CRG and SKG, which can be thought of as the "direct sum version of non-amortized CRG and SKG".

Theorem 5.2 (Lemma 3.4, [JPY12])**.** *Suppose that $(X,Y) \sim \nu$ are inputs to an r-round communication protocol Π with public randomness $R_{\mathtt{Pub}}$ (and which may use private coins as well. Then for every $\epsilon > 0$, there is a public coin protocol L with r rounds and communication at most $\frac{\mathrm{IC}_\mu^{\mathrm{int}}(\Pi)+5r}{\epsilon} + O(r\log(1/\epsilon))$ such that at the end of the protocol each party possesses a random variable $(\hat{\Pi}_1,\ldots,\hat{\Pi}_r)$ representing a transcript for Π, which satisfies*

$$\Delta((R_{\mathtt{Pub}},X,Y,\Pi_1,\ldots,\Pi_r),(R_{\mathtt{Pub}},X,Y,\hat{\Pi}_1,\ldots,\hat{\Pi}_r)) \le 6\epsilon r.$$

Our first lemma, Lemma 5.3, uses Theorem 5.2 to show that for any protocol Π which satisfies $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) \gg \mathrm{IC}_\mu^{\mathrm{int}}(\Pi)$ then there exists another protocol Π with communication cost not much greater than $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi)$ and which satisfies some additional properties:

Lemma 5.3. *Fix any $r,n,\ell \in \mathbb{N}$, and let $\mu = \mu_{r,n,\ell}$. Suppose $\rho \in \mathbb{N}$ and $C,L \in \mathbb{R}_+$. Suppose Π is a ρ-round protocol with $\mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) = L$ and $\mathrm{IC}_\mu^{\mathrm{int}}(\Pi) = C$ and public randomness $R_{\mathtt{Pub}}$ (and which may use private randomness as well). Then for every $\epsilon > 0$ there is some ρ-round protocol Π' with inputs $(X,Y) \sim \mu$, public randomness $R_{\mathtt{Pub}}$, with communication at most $\frac{C+5\rho}{\epsilon} + O(\rho \log 1/\epsilon)$ and which outputs keys K'_A, K'_B, such that*

1. *$\mathbb{P}_\mu[K'_A = K'_B] = 1$.*
2. *When inputs (X,Y) are drawn from μ, $I(K'_A; B_{I_r}) = I(K'_A; A_{I_r}) \ge L - (C+1+2\log n + 36\epsilon\rho\ell)$.*
3. *When inputs (X,Y) are drawn from $\mu_X \otimes \mu_Y$,*

$$I_{\mu_X\otimes\mu_Y}(K'_A, R_{\mathtt{Pub}}, (\Pi')^\rho; B_1,\ldots,B_n) \le \frac{C+5\rho}{\epsilon} + O(\rho\log 1/\epsilon) \tag{47}$$

and

$$I_{\mu_X\otimes\mu_Y}(K'_B, R_{\mathtt{Pub}}, (\Pi')^\rho; A_1,\ldots,A_n) \le \frac{C+5\rho}{\epsilon} + O(\rho\log 1/\epsilon). \tag{48}$$

Proof. Let Π' be the protocol given by Theorem 5.2 for the protocol Π and the given ϵ. Then the communication of Π' is at most $\frac{C+5\rho}{\epsilon} + O(\rho\log 1/\epsilon))$. At the end of Π', Alice and Bob each possess a random variable $(\hat{\Pi}_1,\ldots,\hat{\Pi}_\rho)$, such that, when $(X,Y) \sim \mu$,

$$\Delta((R_{\mathtt{Pub}},X,Y,\hat{\Pi}_1,\ldots,\hat{\Pi}_\rho),(R_{\mathtt{Pub}},X,Y,\Pi_1,\ldots,\Pi_\rho)) \le 6\epsilon\rho. \tag{49}$$

(Notice that $\hat{\Pi}^\rho = (\hat{\Pi}_1,\ldots,\hat{\Pi}_\rho)$ is different from the transcript $(\Pi')^\rho = (\Pi'_1,\ldots,\Pi'_\rho)$ of Π'.) Now set $K'_{\mathtt{A}} = K'_{\mathtt{B}} = (\hat{\Pi}_1,\ldots,\hat{\Pi}_\rho)$, which immediately establishes item (1) of the lemma.

To establish point (2), we will first argue that it holds for Π; in particular we show that when $(X,Y) \sim \mu$,

$$H(B_{I_r}|\Pi^\rho) \le \ell + C - L + 2\log n. \tag{50}$$

(Since $H(B_{i_r}) = \ell$ it will follow from (50) that $I_\mu(\Pi^\rho; B_{I_r}) \ge L - C - 2\log n$, though we will not use this directly.) To see this, first notice that[10]

$$\begin{aligned} I(X;Y|\Pi^\rho) &= I(Y;X,\Pi^\rho) - I(\Pi^\rho;Y) \\ &= I(X;Y) + I(\Pi^\rho;Y|X) + I(\Pi^\rho;X|Y) - I(\Pi^\rho;X,Y) \\ &= I(X;Y) + \mathrm{IC}_\mu^{\mathrm{int}}(\Pi) - \mathrm{IC}_\mu^{\mathrm{ext}}(\Pi) \\ &\le \ell + C - L. \end{aligned} \tag{51}$$

Recalling the notation $I_r = \Sigma_r \circ \cdots \circ \Sigma_1(I_0)$, we observe by Lemma 6.2 and the data processing inequality that

$$\begin{aligned} I(X;Y|\Pi^\rho) &\ge I(X;Y|\Pi^\rho, I_r) - \log n \\ &\ge I(A_{I_r}; B_{I_r}|\Pi^\rho, I_r) - \log n \\ &\ge I(A_{I_r}; B_{I_r}|\Pi^\rho) - 2\log n \\ &= H(A_{I_r}|\Pi^\rho) - 2\log n = H(B_{I_r}|\Pi^\rho) - 2\log n, \end{aligned}$$

since $H(A_{I_r}|B_{I_r}, \Pi^\rho) = H(A_{I_r}|B_{I_r}) = 0$ as $A_{I_r} = B_{I_r}$ for all inputs in the support of μ. It then follows that $H(B_{I_r}|\Pi^\rho, R_{\mathtt{Pub}}) \le \ell + C - L + 2\log n$, establishing (50).

Next, (49) and the data processing inequality give us that $\Delta((R_{\mathtt{Pub}}, B_{I_r}, \Pi^\rho), (R_{\mathtt{Pub}}, B_{I_r}, \hat{\Pi}^\rho)) \le 6\epsilon\rho$. Corollary 6.6 and (50) then give that

$$H(B_{I_r}|\hat{\Pi}^\rho, R_{\mathtt{Pub}}) \le H(B_{I_r}|\hat{\Pi}^\rho) \le \ell + C - L + 2\log n + 36\epsilon\rho\ell + 1.$$

Since $K'_{\mathtt{A}} = \hat{\Pi}^\rho$, we get that

$$I(B_{I_r}; K'_{\mathtt{A}}) \ge L - (C + 1 + 2\log n + 36\epsilon\rho\ell),$$

which establishes point (2).

Finally, to establish point (3), first notice that some inputs $(X,Y) \sim \mu_X \otimes \mu_Y$ may not be in the support of μ. We may extend the protocol Π' to be defined for all pairs of inputs $(X,Y) \in \mathcal{X} \times \mathcal{Y}$, by choosing an arbitrary behavior (e.g., terminating immediately) whenever there is a partial transcript $(\Pi')^{t-1}$ for which the distribution of the next message Π'_t has not been defined.

Recall that $(\Pi'_1, \ldots, \Pi'_\rho)$ denotes the transcript of communication of Π' and $R_{\mathtt{Pub}}$ is the public randomness of Π', so that when $(X,Y) \sim \mu_X \otimes \mu_Y$,

$$I_{\mu_X\otimes\mu_Y}((\Pi')^\rho, X, R_{\mathtt{Pub}}; Y) = I_{\mu_X\otimes\mu_Y}((\Pi')^\rho; Y|X, R_{\mathtt{Pub}}) \le H_{\mu_X\otimes\mu_Y}((\Pi')^\rho) \le \frac{C + 5\rho}{\epsilon} + O(\rho \log 1/\epsilon).$$

Recalling that $K'_{\mathtt{A}} = \hat{\Pi}^\rho$, by construction of Π' (and $\hat{\Pi}$) from Theorem 5.2, it follows that

$$(K'_{\mathtt{A}}, R_{\mathtt{Pub}}, (\Pi')^\rho) - (X, (\Pi')^\rho, R_{\mathtt{Pub}}) - Y$$

[10] We remark that the equality of $I(X;Y|\Pi^\rho)$ to (51) also played a crucial role in [LCV17] which derived a characterization of the achievable rate region in terms of the convex envelope of a functional on source distributions.

is a Markov chain. It then follows from the data processing inequality that

$$I_{\mu_X\otimes\mu_Y}(K'_{\mathtt{A}}, R_{\mathtt{Pub}}, (\Pi')^\rho; B_1, \ldots, B_n) \le I_{\mu_X\otimes\mu_Y}(\hat{K}_{\mathtt{A}}{}', R_{\mathtt{Pub}}, (\Pi')^\rho; Y) \le \frac{C+5\rho}{\epsilon} + O(\rho \log 1/\epsilon),$$

which gives (47); (48) follows in a similar manner. □

Roughly speaking, the next lemma, Lemma 5.4, shows how the protocol Π' constructed in Lemma 5.3 can use the properties (2) and (3) of Lemma 5.3 to distinguish between the distributions μ (ν_1 in the below statement) and $\mu_X \otimes \mu_Y$ (ν_2 in the below statement). This, in combination with the result from Theorem 4.7 stating that μ and $\mu_X \otimes \mu_Y$ are indistinguishable to protocols with little communication, will ultimately complete the proof of Theorem 5.1.

Lemma 5.4. *Suppose ν_1, ν_2 are distributions over tuples of random variables $(Z_1, \ldots, Z_n, I, K, \tilde{K})$, where $Z_1, \ldots, Z_n \in \{0,1\}^\ell$, $I \in [n]$, and $K \in \mathcal{K}$, where $\mathcal{K}$ is a finite set. Suppose that the marginal distribution of $Z_1, \ldots, Z_n, I$ over each of ν_1, ν_2 is uniform over $\{0,1\}^{n\ell} \times [n]$. Finally suppose that $0 < \xi < 1$ and C satisfy $\log n \le C \le \frac{(1-\xi)^3\ell}{1620}$ as well as:*

1. *$I_{\nu_1}(K; Z_1, \ldots, Z_n) \le C$.*
2. *$I_{\nu_2}(K; Z_I) \ge \ell(1-\xi)$.*
3. *$\mathbb{P}_{\nu_2}[K = \tilde{K}] = 1$, and $\mathbb{P}_{\nu_1}[K = \tilde{K}] \ge 1 - (1-\xi)^2/36$.*

Then there is some function $f : \mathcal{K} \times \{0,1\}^{n\ell} \to \{0,1\}$ such that

$$\left|\mathbb{E}_{\nu_1}[f(\tilde{K}, Z_1, \ldots, Z_n)] - \mathbb{E}_{\nu_2}[f(\tilde{K}, Z_1, \ldots, Z_n)]\right| \ge p/2,$$

where $p = (1-\xi)^2/18$.

We first establish some basic lemmas before proving Lemma 5.4.

Lemma 5.5. *Suppose $W \in \{0,1\}^\ell$ is a random varaible, and $H(W) = c$. For any $\delta \in (0,1]$ there is some set $\mathcal{S} \subset \{0,1\}^\ell$ such that $|\mathcal{S}| \le 2^{c/\delta}$ and $\mathbb{P}[W \notin \mathcal{S}] \le \delta$.*

Proof. Set

$$\mathcal{S} = \{w \in \{0,1\}^\ell : \mathbb{P}[W = w] \ge 2^{-c/\delta}\}.$$

We know that $c = H(W) = \mathbb{E}_{w\sim W}[\log(1/\mathbb{P}[W = w])]$, so the probability that $\mathbb{P}[W = w] < 2^{-c/\delta}$, i.e. that $\log(1/\mathbb{P}[W = w]) > c/\delta$, over $w \sim W$ is at most δ. Thus $\mathbb{P}[W \notin \mathcal{S}] \le \delta$. Clearly, by the definition of $\mathcal{S}$, we have that $|\mathcal{S}| \le 2^{c/\delta}$. □

Lemma 5.6. *Suppose that random variables $I, Z_1, \ldots, Z_n$ are distributed jointly so that the marginal of $Z_1, \ldots, Z_n \in \{0,1\}^\ell$ is uniform on $\{0,1\}^{n\ell}$. Then $H(Z_I) \ge \ell - \log n$.*

Proof. Notice that

$$\begin{aligned} H(Z_I, Z_{I+1}, \ldots, Z_{I+n-1}) &\ge H(Z_I, \ldots, Z_{I+n-1}|I) \\ &= \mathbb{E}_{i\sim I}\left[H(Z_i, \ldots, Z_{i+n-1}|I = i)\right] \\ &= \mathbb{E}_{i\sim I}\left[H(Z_1, \ldots, Z_n|I = i)\right] \\ &= H(Z_1, \ldots, Z_n|I) \\ &\ge \ell n - \log n, \end{aligned} \tag{52}$$

where addition of subscripts is taken modulo n. Since $(Z_{I+1}, \ldots, Z_{I+n-1}) \in \{0,1\}^{\ell n - \ell}$, we get that

$$H(Z_I) \geq H(Z_I | Z_{I+1}, \ldots, Z_{I+n-1}) \geq H(Z_I, \ldots, Z_{I+n-1}) - (\ell n - \ell) \geq \ell - \log n,$$

as desired. □

Lemma 5.7. *Suppose that $W \in \{0,1\}^\ell$ is a random variable with $H(W) = h \leq \ell$. Let $\mathcal{S} \subset \{0,1\}^\ell$ be a subset with size $|\mathcal{S}| \leq 2^c$, for some $c < \ell$. Then $\mathbb{P}[W \in \mathcal{S}] \leq \frac{\ell+1-h}{\ell-c}$.*

Proof. Write $p = \mathbb{P}[W \in \mathcal{S}]$. Let $J = \mathbb{1}[W \in \mathcal{S}]$. Then $pc + (1-p)\ell \geq pc + (1-p)\log(2^\ell - 2^c) \geq H(W|J) \geq H(W) - 1 = h - 1$. Hence $p(c-\ell) \geq h - 1 - \ell$, so $p \leq \frac{\ell+1-h}{\ell-c}$. □

Now we prove Lemma 5.4.

Proof of Lemma 5.4. We will first define f and determine a lower bound on $\mathbb{E}_{\nu_2}[f(K, Z_1, \ldots, Z_n)]$. By assumption, $H_{\nu_2}(Z_I) = \ell$, so $H_{\nu_2}(Z_I|K) \leq \xi\ell$. For each $k \in \mathcal{K}$, let $\gamma_k = H(Z_I|K=k)/\ell$, so that $\mathbb{E}_{k\sim K}[\gamma_k] \leq \xi$. Pick some $\eta > 1, \zeta > 1$ to be specified later. By Lemma 5.5, for each $k \in \mathcal{K}$, there is a set $\mathcal{T}_k \subset \{0,1\}^\ell$ of size at most $2^{\eta\gamma_k\ell}$ such that $\mathbb{P}_{\nu_2}[Z_I \notin \mathcal{T}_k | K = k] \leq 1/\eta$. Next, set $\mathcal{S} = \{k \in \mathcal{K} : \gamma_k \leq \zeta\xi\}$. By Markov's inequality, $\mathbb{P}_{\nu_2}[K \in \mathcal{S}] \geq 1 - 1/\zeta$. Thus $\mathbb{P}_{\nu_2}[K \in \mathcal{S}] \cdot \mathbb{P}_{\nu_2}[Z_I \in T_K | K \in \mathcal{S}] \geq (1-1/\zeta)\cdot(1-1/\eta)$, and for all $k \in \mathcal{S}$, $|\mathcal{T}_k| \leq 2^{\eta\zeta\xi\ell} < 2^{\eta\zeta\ell}$.

We now set

$$f(K, Z_1, \ldots, Z_n) = \begin{cases} \bigvee_{i\in[n]} \mathbb{1}[Z_i \in \mathcal{T}_K] & : \quad K \in \mathcal{S} \\ 0 & : \quad \text{else.} \end{cases}$$

Since $\mathbb{P}[K \in \mathcal{S}] \cdot \mathbb{P}[Z_I \in \mathcal{T}_K | K \in \mathcal{S}] \leq \mathbb{E}\left[\vee_{i\in[n]} \mathbb{1}[Z_i \in \mathcal{T}_K]\right]$,

$$\mathbb{E}_{\nu_2}[f(K, Z_1, \ldots, Z_n)] \geq (1-1/\eta)\cdot(1-1/\zeta).$$

Next we determine an upper bound on $\mathbb{E}_{\nu_1}[f(K, Z_1, \ldots, Z_n)]$. Define a random variable $\hat{I} = \hat{I}(Z_1, \ldots, Z_n, K)$, by $\hat{I} = \min\{i \ : \ Z_i \in \mathcal{T}_K\}$, if the set $\{i \ : \ Z_i \in \mathcal{T}_K\}$ is nonempty, else $\hat{I} = 1$. Thus $H(\hat{I}) \leq \log n$. Consider the random variable $Z_{\hat{I}} \in \{0,1\}^\ell$. It follows that $f(K, Z_1, \ldots, Z_n) \leq \mathbb{1}[Z_{\hat{I}} \in \mathcal{T}_K]$. By Lemma 6.2 and the data processing inequality, we have that

$$I_{\nu_1}(K; Z_{\hat{I}}) - \log n \leq I_{\nu_1}(K; Z_{\hat{I}} | \hat{I}) \leq I_{\nu_1}(K; Z_1, \ldots, Z_n | \hat{I}) \leq I_{\nu_1}(K; Z_1, \ldots, Z_n) + \log n \leq C + \log n.$$

Lemma 5.6 gives that $H_{\nu_1}(Z_{\hat{I}}) \geq \ell - \log n$, so $H_{\nu_1}(Z_{\hat{I}}|K) \geq \ell - C - 3\log n$. For each $k \in \mathcal{K}$, let $h_k = H_{\nu_1}(Z_{\hat{I}} | K = k)$, so that $\mathbb{E}_{\nu_1}[h_K] \geq \ell - C - 3\log n$. By Lemma 5.7, for each $k \in \mathcal{K}$ with $\eta\gamma_k < 1$, $\mathbb{P}[Z_{\hat{I}} \in \mathcal{T}_K | K = k] \leq \frac{\ell+1-h_k}{\ell(1-\eta\gamma_k)}$, by our upper bound $|\mathcal{T}_k| \leq 2^{\eta\gamma_k\ell}$.

Recall that $\mathbb{E}_{\nu_2}[\gamma_k] \leq \xi$. For $i \in \{1,2\}$, let K_{ν_i} be the marginal distribution of K according to ν_i. We must have that $\Delta(K_{\nu_2}, K_{\nu_1}) < p$, else we could choose f to be a function of only K and would get that $|\mathbb{E}_{\nu_1}[f] - \mathbb{E}_{\nu_2}[f]| \geq p$. Thus $1 - 1/\zeta - p \leq \mathbb{P}_{\nu_1}[K \in \mathcal{S}] \leq 1$. Next notice that $\mathbb{E}_{\nu_1}[\ell - h_K] \leq C + 3\log n$, and that $\ell - h_K \geq 0$ with probability 1. Therefore, $\mathbb{E}_{\nu_1}[\ell - h_K | K \in \mathcal{S}] \leq \frac{C+3\log n}{1-1/\zeta-p}$. Since $\gamma_k \leq \zeta\xi$ for all $k \in \mathcal{S}$, it follows that

$$\begin{aligned} \mathbb{E}_{\nu_1}[f(K, Z_1, \ldots, Z_n)] &\leq \mathbb{E}_{\nu_1}[f(K, Z_1, \ldots, Z_n) | K \in \mathcal{S}] \\ &\leq \mathbb{P}_{\nu_1}[Z_{\hat{I}} \in \mathcal{T}_K | K \in \mathcal{S}] \\ &\leq \frac{1 + \frac{C+3\log n}{1-1/\zeta-p}}{\ell(1-\eta\zeta\xi)}. \end{aligned}$$

Thus

$$\mathbb{E}_{\nu_2}[f(K,Z_1,\ldots,Z_n)] - \mathbb{E}_{\nu_1}[f(K,Z_1,\ldots,Z_n)] \geq (1-1/\zeta)\cdot\left((1-1/\eta) - \frac{1}{1-1/\zeta}\cdot\frac{1+\frac{C+3\log n}{1-1/\zeta-p}}{\ell(1-\eta\zeta\xi)}\right).$$

Now, choose $\eta=\zeta=\xi^{-1/3}$, and let $\xi'=1-\xi$, so that $p\leq \xi'/6 \leq \frac{1-(1-\xi')^{1/3}}{2} = \frac{1-1/\zeta}{2}$. Using the inequality $ax \leq 1-(1-x)^a \leq x$ for $0<a<1$, $x\in[0,1]$ and $C\geq \log n$ gives

$$\begin{aligned}
\mathbb{E}_{\nu_2}[f(K,Z_1,\ldots,Z_n)] - \mathbb{E}_{\nu_1}[f(K,Z_1,\ldots,Z_n)] &\geq \xi'/3\cdot\left(\xi'/3 - \frac{1}{(1-1/\zeta)(1-1/\zeta-p)}\cdot\frac{15C}{\xi'\ell}\right)\\
&\geq \xi'/3\cdot\left(\xi'/3 - \frac{270C}{(\xi')^2\ell}\right)\\
&\geq (\xi')^2/18 = p,
\end{aligned}$$

where the last inequality follows from $C\leq\frac{(\xi')^3\ell}{1620}$.

Since $K=\tilde{K}$ over ν_2 and are only nonequal with probability at most $p/2$ over ν_1, it follows that

$$\mathbb{E}_{\nu_2}[f(\tilde{K},Z_1,\ldots,Z_n)] - \mathbb{E}_{\nu_1}[f(\tilde{K},Z_1,\ldots,Z_n)] \geq p/2,$$

as desired. □

5.2 Proof of Theorem 5.1

Using Lemmas 5.3, 5.4, and Theorem 3.4, we now may prove Theorem 5.1:

Proof of Theorem 5.1. The first part of Theorem 5.1 follows directly from Lemma 4.4.

To prove the second part of Theorem 5.1, first suppose r is odd. We take $\mu=\mu_{r,n,\ell}$ and set $\epsilon=\gamma/(54(r+1))$.

We argue by contradiction. Suppose the theorem statement is false: namely, that for some $C\leq n/\log^{c_0} n$ and $L>\gamma\ell$, the tuple (C,L) is $\lfloor(r+1)/2\rfloor$-achievable from μ. We can assume without loss of generality that $L<\ell$. By Theorem 3.4 (and in particular, Corollary 3.5), since $I_\mu(X;Y)=\ell>L$, there is a $\lfloor(r+1)/2\rfloor$-round protocol Π such that $\mathrm{IC}^{\mathrm{int}}_\mu(\Pi)\leq C$ and $\mathrm{IC}^{\mathrm{ext}}_\mu(\Pi)\geq L$.

By Lemma 5.3, there is an $\lfloor(r+1)/2\rfloor$-round public-coin protocol Π' with inputs $(X,Y)\sim\mu$ and communication at most $\frac{C+3+5r/2}{\epsilon}+O(r\log 1/\epsilon)$ such that at the end of Π' with inputs $(X,Y)\sim\mu$, Alice and Bob output keys $K'_{\mathtt{A}}=K'_{\mathtt{B}}$, respectively, which satisfy $I_\mu(K'_{\mathtt{B}};B_{I_r})\geq L-(C+1+2\log n+18\epsilon(r+1)\ell)$. Moreover, when $(X,Y)\sim\mu_X\otimes\mu_Y$,

$$\max\{I_{\mu_X\otimes\mu_Y}(K'_{\mathtt{A}};B_1,\ldots,B_n), I_{\mu_X\otimes\mu_Y}(K'_{\mathtt{B}};A_1,\ldots,A_n)\}\leq\frac{C+3+5r/2}{\epsilon}+O(r\log 1/\epsilon).$$

Next, let Π'' be the protocol where the parties run Π', and the last party (suppose it is Alice, for concreteness) to speak in Π' sends over a random hash $h(K'_{\mathtt{A}})$ of length $O(\log 1/\gamma)$, so that for any $K'_{\mathtt{A}}\neq K'_{\mathtt{B}}$, $\mathbb{P}_h[h(K'_{\mathtt{A}})=h(K'_{\mathtt{B}})]\leq\gamma^2/648$, and the other party, Bob, outputs a final bit equal to $\mathbb{1}[h(K'_{\mathtt{A}})=h(K'_{\mathtt{B}})]$. For sufficiently large n, we have that

$$\mathrm{CC}(\Pi'')\leq\frac{C+3+5r/2}{\epsilon}+O(r\log 1/\epsilon)+O(\log 1/\gamma)\leq n/\log^{(c_0-1)} n. \tag{53}$$

Claim 5.8. *Π'' distinguishes μ and $\mu_X \otimes \mu_Y$ with advantage at least $\gamma^2/324$.*

Proof. To prove Claim 5.8, we consider two cases.

The first case is that $\mathbb{P}_{\mu_X \otimes \mu_Y}[K'_{\mathtt{A}} \neq K'_{\mathtt{B}}] \geq \gamma^2/324$. In this case, the last bit output by Bob will be 0 with probability at least $\gamma^2/648$ when $(X, Y) \sim \mu_X \otimes \mu_Y$. Since $K'_{\mathtt{A}} = K'_{\mathtt{B}}$ with probability 1 when $(X, Y) \sim \mu$, it follows that Π'' distinguishes between the two distributions with advantage at least $\gamma^2/648$ in this case.

The second case is that $\mathbb{P}_{\mu_X \otimes \mu_Y}[K'_{\mathtt{A}} \neq K'_{\mathtt{B}}] \leq \gamma^2/324$. Here we will use Lemma 5.4. Since $18\epsilon(r+1) \leq \gamma/3$, and since for sufficiently large n, $C + 1 + 2\log n \leq \gamma n/3 = \gamma\ell/3$, we see that $I_\mu(K'_{\mathtt{B}}; B_{I_r}) \geq \gamma\ell - 2\gamma\ell/3 = \gamma\ell/3$.

We apply Lemma 5.4, with $(Z_1, \ldots, Z_n) = (B_1, \ldots, B_n), I = I_r, K = K'_{\mathtt{A}}, \tilde{K} = K'_{\mathtt{B}}, \nu_1 = \mu_X \otimes \mu_Y, \nu_2 = \mu$, $\xi = 1 - \gamma/3$ and $L = n/\log^{(c_0-1)} n$. Here we use that $n/\log^{(c_0-1)} n \leq \frac{(\gamma/3)^3 n}{1620}$ for sufficiently large n (depending on γ), as well as $\mathbb{P}_{\mu_X \otimes \mu_Y}[K'_{\mathtt{A}} \neq K'_{\mathtt{B}}] \leq \gamma^2/324 = (1-\xi)^2/36$. Then Lemma 5.4 gives that Bob can output a bit as a deterministic function of $K'_{\mathtt{B}}, B_1, \ldots, B_n$ (all of which Bob holds at the conclusion of Π'), that distinguishes μ and $\mu_X \otimes \mu_Y$ with advantage at least $\gamma^2/324$. □

By Theorem 4.6, with $\epsilon = \gamma^2/324$, and as long as c_0 is large enough so that the right-hand side of (53) holds for $n \geq c_0$, and such that $c_0 - 1 \geq \beta$ (where β is chosen from Theorem 4.6, given $\epsilon = \gamma^2/325$), we arrive at a contradiction.

For even r, we use the distribution $\mu = \mu_{r-1,n,\ell}$. Part (1) of the theorem still follows from Lemma 4.4 (in fact, we even have $(r+1)$-achievability). For part (2), the argument above applies, except now the lower bound on round complexity is $\lceil((r-1)+1)/2\rceil = \lceil r/2\rceil = r/2$.

Finally, to prove part (3) of Theorem 5.1, an argument virtually identical to the one for part (2) applies, except that the protocols Π and Π' have r rounds, the protocol Π'' has $r+1$ rounds, and the upper bound in (53) is $\sqrt{n}/\log^{(c_0-1)} n$, which needs to be less than $\frac{(\gamma/3)^3 n}{1620} = \frac{(\gamma/3)^3 \ell}{1620}$ (which it is, for sufficiently large n. In the last step fo the proof, we use Theorem 4.7 (instead of Theorem 4.6), which establishes that μ and $\mu_X \otimes \mu_Y$ are $(\epsilon, r+1, \sqrt{n}/\operatorname{poly}\log n)$-indistinguishable for any constant $\epsilon > 0$. □

5.3 Separations in MIMK, CBIB, and KBIB

In this section we use Theorem 5.1 and the results of Section 2.3 to derive separations in the MIMK for the pointer chasing source $\mu_{r,n,\ell}$. The below Theorem 5.9 generalizes a result of Tyagi [Tya13], which established a constant-factor separation in the MIMK for 2-round and 1-round protocols for a certain source.

Theorem 5.9. *For each $r \in \mathbb{N}$, there is a c_0 such that for each $n \geq c_0$, the pointer chasing source $\mu_{r,n,n}$ satisfies:*

1. $\mathscr{I}_{r+2}(X; Y) \leq (r+2)\lceil \log n \rceil$.
2. $\mathscr{I}_{\lfloor (r+1)/2 \rfloor}(X; Y) > n/\log^{c_0} n$.
3. $\mathscr{I}_r(X; Y) > \sqrt{n}/\log^{c_0} n$.

Proof. Let the constant c_0 be that given by Theorem 5.1 for an arbitrary γ.

The first item follows from the definition of $\mathscr{I}_r(X;Y)$ in Definition 2.8, the fact that $I_{\mu_{r,n,n}}(X;Y) = n$ (Lemma 4.3), and the first item of Theorem 5.1 stating that the tuple $((r+2)\lceil \log n \rceil, n)$ is $(r+2)$-achievable for SKG from the source $\mu_{r,n,n}$.

To see the second item, suppose that $\mathscr{I}_{\lfloor (r+1)/2 \rfloor}(X;Y) \leq n/\log^{c_0} n$. Then the tuple $(n/\log^{c_0} n, \ell)$ is $\lfloor (r+1)/2 \rfloor$-achievable from the source $\mu_{r,n,n}$, contradicting the second item of Theorem 5.1.

Similarly, for the third item, if $\mathscr{I}_r(X;Y) \leq \sqrt{n}/\log^{c_0} n$, then the tuple $(\sqrt{n}/\log^{c_0} n, \ell)$ would be r-achievable from the source $\mu_{r,n,n}$, contradicting the third item of Theorem 5.1. □

Using Theorem 3.9, Theorem 5.9 immediately gives an analogous round separation for $\lim_{\lambda \downarrow 0} \frac{\omega_\rho^\lambda(\mu_{r,n,n})}{\lambda}$, between $\rho = r+2$ and $\rho = r$ (or $\rho = \lfloor (r+1)/2 \rfloor$). We can, however, use the stronger nature of Theorem 5.1 to obtain some information about $\omega_\rho^\lambda(\mu_{r,n,n})$, for all λ that are bounded away from 1:

Corollary 5.10. *Fix any $r \in \mathbb{N}, \gamma \in (0,1)$. Then:*

1. *For all $\lambda \in (0,1)$, $n \in \mathbb{N}$, $\omega_{r+2}^\lambda(\mu_{r,n,n}) \geq \lambda H(X,Y) - \lambda n + (r+2)\lceil \log n \rceil$.*
2. *Let c_0 be the constant from Theorem 5.1 for $\gamma = 1/2$. Then for all $\lambda \in (0, 1 - 2/\log^{c_0} n)$ and $n \geq c_0$,*

$$\omega_{\lfloor (r+1)/2 \rfloor}^\lambda(\mu_{r,n,n}) \leq \lambda H(X,Y) - \lambda n - n/\log^{c_0} n. \tag{54}$$

Thus, in particular,

$$\omega_{\lfloor (r+1)/2 \rfloor}^\lambda(\mu_{r,n,n}) \leq \omega_r^\lambda(\mu_{r,n,n}) - n/\log^{c_0} n + O(\log n).$$

Proof. The first part follows immediately from Theorem 3.7 and the fact that $((r+2)\lceil \log n \rceil, \ell) \in \mathcal{T}_{r+2}(X,Y)$.

For the second part, fix $\lambda \in (0,1)$, and let c_0 be the constant from Theorem 5.1 given the value $\gamma = 1/2$. Suppose for the sake of contradiction that (54) does not hold. Then by Theorem 3.7, for some $(C,L) \in \mathcal{T}_r(X,Y)$, we have

$$L(1-\lambda) - C \geq n - \lambda n - n/\log^{c_0} n. \tag{55}$$

We may assume without loss of generality that $L \leq I(X;Y) = n$, since for any $\alpha > 0$ such that $L - \alpha \geq I(X;Y)$, $(C-\alpha, L-\alpha) \in \mathcal{T}_r(X,Y)$ as well.

But (55) gives $L \geq n - \frac{n/\log^{c_0} n}{1-\lambda} \geq n/2$. By Theorem 5.1, it follows that $C > n/\log^{c_0} n$, which contradicts (55) since $L \leq n$. □

Next we would like to derive similar separations for the r-round interactive CBIB (Definition 2.5) and KBIB (Definition 2.6). Notice that from the first item of Theorem 5.1 we have immediately that $\Gamma_{r+2}^{\mathtt{cr}}(X,Y) \geq \frac{n}{(r+2)\lceil \log n \rceil}$. We might hope to use Theorem 2.3 as well as the second and third items of Theorem 5.1 to derive upper bounds on $\Gamma_{\lfloor (r+1)/2 \rfloor}^{\mathtt{cr}}(X,Y)$ and $\Gamma_r^{\mathtt{cr}}(X,Y)$ that grow as $\log^{c_0} n$ and $\sqrt{n}\log^{c_0} n$, respectively. However, such upper bounds do not immediately follow from Theorem 5.1 since Theorem 5.1 requires a lower bound on L in order to show that certain tuples (C,L) are not achievable. In particular, Theorem 5.1 leaves open the possibility that tuples such as $(\log n, \sqrt{n})$, or even $(2^{-n}, 1)$ are $\lfloor (r+1)/2 \rfloor$-achievable for CRG from $\mu_{r,n,n}$. This limitation of Theorem 5.1 results from the fact that Lemmas 5.3 and 5.4 give vacuous bounds on the disintuishability of $\mu = \mu_{r,n,n}$ and $\mu_X \otimes \mu_Y$ when the tuple (C,L) is such that L is small compared to n. We leave the problem of remedying this issue for future work:

Problem 5.1. For each $r \in \mathbb{N}$, show (perhaps using Theorem 5.1) that there is a c_0, such that for each $n \geq c_0$, the pointer chasing source $(X, Y) \sim \mu_{r,n,n}$ satisfies:

1. $\Gamma^{\mathtt{cr}}_{\lfloor (r+1)/2 \rfloor}(X, Y) \leq \log^{c_0} n$.
2. $\Gamma^{\mathtt{cr}}_{r}(X, Y) \leq \sqrt{n} \log^{c_0} n$.

It seems that in fact the even stronger result $\Gamma^{\mathtt{cr}}_{r+1}(X, Y) \leq O(1)$ holds.

A proof of the last sentence of Problem 5.1 would imply a corresponding separation between the $(r+2)$-round and $(r+1)$-round strong data processing constants for the source $\mu_{r,n,n}$: while trivially we have $s^*_{r+2}(X, Y) \geq 1 - \tilde{O}(1/n)$, $\Gamma^{\mathtt{cr}}_{r+1}(X, Y) \leq O(1)$ is equivalent to $s^*_{r+1}(X, Y) \leq 1 - c$ for some constant c. In view of Theorem 2.3, an answer to Problem 5.1 would imply similar types of separations for the concave enelopes ω^{λ}_{ρ} as well.

6 Information Theoretic Lemmas

In this section we collect several information theoretic lemmas which are used throughout the paper.

The data processing inequality states that if X, Y are jointly distributed random variables, and then we compute some randomized function Z of Y (i.e., we "process Y"), then the mutual information between X and Z can be no greater than the mutual information between X and Y.

Proposition 6.1 (Data processing inequality)**.** *If $X - Y - Z$ is a Markov chain, then $I(X; Z) \leq I(X; Y)$.*

Lemma 6.2 ([HMO+18], Lemma 2.9)**.** *For random variables X, Y, Z, W, we have that*

$$I(X; W|Y, Z) \geq I(X; Y|W, Z) - I(X; Y|Z) \geq -I(X; W|Z).$$

In particular,

$$H(W) \geq I(X; Y|W, Z) - I(X; Y|Z) \geq -H(W).$$

Proof. Using the definition of mutual information, we observe

$$\begin{aligned} & I(X; W|Y, Z) - I(X; W|Z) \\ = \; & H(X|Y, Z) - H(X|W, Y, Z) - H(X|Z) + H(X|W, Z) \\ = \; & I(X; Y|W, Z) - I(X; Y|Z). \end{aligned}$$

The claimed equalities hold by non-negativity of the mutual information. □

Pinsker's inequality gives an upper bound on total variation distance in terms of the KL divergence between two distributions.

Proposition 6.3 (Pinsker's inequality)**.** *Let μ, ν be two distributions supported on a set $\mathcal{X}$. Then*

$$\Delta(\mu, \nu) \leq \sqrt{\frac{\mathrm{KL}(\mu||\nu)}{2}}.$$

The following lemma implies that the entropy functional $H(\cdot)$ is continuous on the set of distributions on a finite $\mathcal{X}$ set with respect to the topology induced by total variation distance.

Lemma 6.4 ([HY10], Theorem 6)**.** *Suppose X_1, X_2 are random variables whose distributions are supported on a set $\mathcal{X}$, and let $\delta = \Delta(X_1, X_2)$. If $0 \le \delta \le \frac{|\mathcal{X}|-1}{|\mathcal{X}|}$, then*

$$|H(X_1) - H(X_2)| \le h(\delta) + \delta \log(|\mathcal{X}| - 1).$$

Remark 6.1. When X_1 is uniform, $H(X_1) - H(X_2) = \log|\mathcal{X}| - H(X_2)$ is equal to the KL divergence $\mathrm{KL}(X||U_{\mathcal{X}})$ between X and the uniform distribution $U_{\mathcal{X}}$ on $\mathcal{X}$. In this regime, Lemma 6.4 can be interpreted as a reverse Pinsker inequality. This interpretation is particularly useful in Section 4.

The following theorem is a slightly weaker version of Lemma 6.4.

Theorem 6.5 ([CT12], Theorem 17.3.3)**.** *Suppose that μ, ν are distributions on $[m]$ and $\Delta(\mu, \nu) \le \epsilon \le 1/2$. Then, letting $X \sim \mu, Y \sim \nu$,*

$$|H(X) - H(Y)| \le \epsilon \cdot \log\left(\frac{m}{\epsilon}\right).$$

Corollary 6.6 derives a conditional version of Lemma 6.4.

Corollary 6.6. *Suppose that X_1, X_2 are random variables whose distributions are supported on a set $\mathcal{X}$, and that Y_1, Y_2 are random variables whose distributions are supported on a set $\mathcal{Y}$. Let $\delta = \Delta(X_1Y_1, X_2Y_2)$. Then*

$$|H(X_1|Y_1) - H(X_2|Y_2)| \le 1 + 6\delta \log|\mathcal{X}|.$$

Proof. For $x \in \mathcal{X}, y \in \mathcal{Y}$, write $p_{X_1Y_1}(x, y)$ for the probability of the event $\{X_1 = x, Y_1 = y\}$, and similarly $p_{X_2Y_2}(x, y), p_{Y_1}(y), p_{Y_2}(y), p_{X_1|Y_1}(x|y), p_{X_2|Y_2}(x|y)$, and so on. For any y not in the support of Y_2, and any $x \in \mathcal{X}$, let $p_{X_2|Y_2}(x|y) = 0$ (and similarly for $p_{X_1|Y_1}(x|y)$ for y not in the support of Y_1). Choose an arbitrary element $* \in \mathcal{X}$, and define a random variable $\tilde{X}_2$ with support in $\mathcal{X}$ that is jointly distributed with Y_1 as follows. For y in the support of Y_2, let $p_{\tilde{X}_2|Y_1}(x|y) = p_{X_2|Y_2}(x|y)$, for $x \in \mathcal{X}$. For y not in the support of Y_2, let $p_{\tilde{X}_2|Y_1}(\cdot|y)$ have all its mass on $* \in \mathcal{X}$.

By the data processing inequality, $\Delta(Y_1, Y_2) \le \delta$, so

$$\begin{aligned}
\Delta(X_1Y_1, X_2Y_2) &= \frac{1}{2} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} |p_{X_1Y_1}(x, y) - p_{X_2Y_2}(x, y)| \\
&= \frac{1}{2} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} |p_{X_1|Y_1}(x|y) p_{Y_1}(y) - p_{X_2|Y_2}(x|y) p_{Y_2}(y)| \\
&\ge -\delta + \frac{1}{2} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p_{Y_1}(y) \cdot |p_{X_1|Y_1}(x|y) - p_{\tilde{X}_2|Y_1}(x|y)|.
\end{aligned}$$

For $y \in \mathcal{Y}$, write $\delta_y = \frac{1}{2} \sum_{x \in \mathcal{X}} |p_{X_1|Y_1}(x|y) - p_{\tilde{X}_2|Y_1}(x|y)|$, so that the above gives $\mathbb{E}_{y \sim Y_1}[\delta_y] \le 2\delta$.

Write $\mathrm{supp}(Z)$ for the support of a (discrete) random variable Z. Next, notice that by Hölder's

inequality,

$$\begin{aligned}
|H(X_1|Y_1) - H(X_2|Y_2)| &= |\mathbb{E}_{y_1\sim Y_1}[H(X_1|Y_1=y_1)] - \mathbb{E}_{y_2\sim Y_2}[H(X_2|Y_2=y_2)]| \\
&\leq \left| \sum_{y_1 \in \mathrm{supp}(Y_1)\cap\mathrm{supp}(Y_2)} p_{Y_1}(y_1)\left(H(X_1|Y_1=y_1) - H(X_2|Y_2=y_1)\right)\right| + 2\delta\cdot\log|\mathcal{X}| \\
&= \left| \sum_{y_1 \in \mathrm{supp}(Y_1)} p_{Y_1}(y_1)(H(X_1|Y_1=y_1) - H(\tilde{X}_2|Y_1=y_1))\right| + 2\delta\cdot\log|\mathcal{X}| \\
&\leq \mathbb{E}_{y_1\sim Y_1}\left[\left|H(X_1|Y_1=y_1) - H(\tilde{X}_2|Y_1=y_1)\right|\right].
\end{aligned}$$

For each $y \in \mathrm{supp}(Y_1)$, we have from Lemma 6.4 that $|H(X_1|Y_1=y) - H(\tilde{X}_2|Y_1=y)| \leq h(\delta_y) + \delta_y \log|\mathcal{X}|$ as long as $\delta_y \leq \frac{|\mathcal{X}|-1}{|\mathcal{X}|}$, which happens with probability at least $1-4\delta$ by Markov's inequality. Thus,

$$\begin{aligned}
|H(X_1|Y_1) - H(X_2|Y_2)| &\leq \mathbb{E}_{y\sim Y_1}\left[h(\delta_y) + \delta_y\log|\mathcal{X}|\right] + 4\delta\log|\mathcal{X}| \\
&\leq 1 + 6\delta\log|\mathcal{X}|.
\end{aligned}$$

□

References

[AC93] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography. part i: secret sharing. *IEEE Transactions on Information Theory*, 39(4), 1993.

[AC98] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography. ii. cr capacity. *Information Theory, IEEE Transactions on*, 44(1):225–240, 1998.

[AD89a] R. Ahlswede and G. Dueck. Identification in the presence of feedback-a discovery of new capacity formulas. *IEEE Transactions on Information Theory*, 35(1):30–36, January 1989.

[AD89b] R. Ahlswede and G. Dueck. Identification via channels. *IEEE Transactions on Information Theory*, 35(1):15–29, January 1989.

[AG76] Rudolf Ahlswede and Peter Gács. Spreading of sets in product spaces and hypercontraction of the markov operator. *The annals of probability*, pages 925–939, 1976.

[AGKN13] Venkat Anantharam, Amin Gohari, Sudeep Kamath, and Chandra Nair. On maximal correlation, hypercontractivity, and the data processing inequality studied by Erkip and Cover. *arXiv preprint arXiv:1304.6133*, 2013.

[BBB+92] Charles H Bennett, Franqois Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:26, 1992.

[BBCR13] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. *SIAM Journal on Computing*, 42(3):1327–1363, 2013.

[BBT60] David Blackwell, Leo Breiman, and A. J. Thomasian. The Capacities of Certain Channel Classes Under Random Coding. *Ann. Math. Statist.*, 31(3):558–567, September 1960.

[BGGS19] Mitali Bafna, Badih Ghazi, Noah Golowich, and Madhu Sudan. Communications-rounds tradeoffs for common randomness and secret key generation. In *2019 Symposium on Discrete Algorithms*. ACM-SIAM, 2019.

[BGI14] Mohammad Bavarian, Dmitry Gavinsky, and Tsuyoshi Ito. On the role of shared randomness in simultaneous communication. In *Automata, Languages, and Programming*, pages 150–162. Springer, 2014.

[BGKR18] Mark Braverman, Anat Ganor, Gillat Kol, and Ran Raz. A Candidate for a Strong Separation of Information and Communication. In *Innovations in Theoretical Computer Science*, 2018.

[BGPW13] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein. From Information to Exact Communication. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 151–160, New York, NY, USA, 2013. ACM.

[BM11] Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *Information Theory, IEEE Transactions on*, 57(10):6351–6355, 2011.

[BR11] Mark Braverman and Anup Rao. Information equals amortized communication. In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, pages 748–757. IEEE, 2011.

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

[BRWY13] Mark Braverman, Anup Rao, Omri Weinstein, and Amir Yehudayoff. Direct product via round-preserving compression. *Automata, Languages, and Programming*, 7965:232–243, 2013.

[CCM16] Amit Chakrabarti, Graham Cormode, and Andrew McGregor. Robust Lower Bounds for Communication and Stream Computation. *Theory of Computing*, 12:1–35, August 2016.

[CGMS17] Clément L Canonne, Venkatesan Guruswami, Raghu Meka, and Madhu Sudan. Communication with imperfectly shared randomness. *IEEE Transactions on Information Theory*, 63(10):6799–6818, 2017.

[CK81] Imre Csiszár and János Körner. *Information theory: coding theorems for discrete memoryless systems*. Academic Press, 1981.

[CMN14] Siu On Chan, Elchanan Mossel, and Joe Neeman. On extracting common random bits from correlated sources on large alphabets. *Information Theory, IEEE Transactions on*, 60(3):1630–1637, 2014.

[CN91] I. Csiszar and P. Narayan. Capacity of the Gaussian arbitrarily varying channel. *IEEE Transactions on Information Theory*, 37(1):18–26, January 1991.

[CN00] Imre Csiszár and Prakash Narayan. Common randomness and secret key generation with a helper. *Information Theory, IEEE Transactions on*, 46(2):344–366, 2000.

[CN04] Imre Csiszár and Prakash Narayan. Secrecy capacities for multiple terminals. *IEEE Transactions on Information Theory*, 50(12):3047–3061, 2004.

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

[CT12] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[DGS84] Pavol Duris, Zvi Galil, and Georg Schnitger. Lower Bounds on Communication Complexity. In *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing*, STOC '84, pages 81–91, New York, NY, USA, 1984. ACM.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[DJS96] Carsten Damm, Stasys Jukna, and Jirí Sgall. Some Bounds on Multiparty Communication Complexity of Pointer Jumping. *Computational Complexity*, 7:643–654, 1996.

[FNKN95] Tomas Feder, Moni Naor, Eyal Kushilevitz, and Noam Nisan. Amortized Communication Complexity. *SIAM Journal on Computing*, 24(4):736–750, 1995.

[GA10a] A. A. Gohari and V. Anantharam. Information-Theoretic Key Agreement of Multiple Terminals—Part I. *IEEE Transactions on Information Theory*, 56(8):3973–3996, August 2010.

[GA10b] Amin Aminzadeh Gohari and Venkat Anantharam. Information-theoretic Key Agreement of Multiple Terminal: Part II: Channel Model. *IEEE Trans. Inf. Theor.*, 56(8):3997–4010, August 2010.

[GJ18] Badih Ghazi and TS Jayram. Resource-efficient common randomness and secret-key schemes. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1834–1853. Society for Industrial and Applied Mathematics, 2018.

[GK73] Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973.

[GKR14] Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of information and communication. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 176–185. IEEE, 2014.

[GKR16] Anat Ganor, Gillat Kol, and Ran Raz. Exponential separation of communication and external information. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing - STOC 2016*, pages 977–986, Cambridge, MA, USA, 2016. ACM Press.

[GKS15] Badih Ghazi, Pritish Kamath, and Madhu Sudan. Communication Complexity of Permutation-Invariant Functions. *arXiv:1506.00273 [cs, math]*, May 2015. arXiv: 1506.00273.

[GM08] Sudipto Guha and Andrew McGregor. Tight Lower Bounds for Multi-pass Stream Computation Via Pass Elimination. In *Automata, Languages and Programming*, volume 5125, pages 760–772. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[GM09] Sudipto Guha and Andrew McGregor. Stream Order and Order Statistics: Quantile Estimation in Random-Order Streams. *SIAM Journal on Computing*, 38(5):2044–2059, January 2009.

[GO16] Venkatesan Guruswami and Krzysztof Onak. Superlinear Lower Bounds for Multipass Graph Processing. *Algorithmica*, 76(3):654–683, November 2016.

[GR16] Venkatesan Guruswami and Jaikumar Radhakrishnan. Tight bounds for communication-assisted agreement distillation. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 6:1–6:17, 2016.

[GS17] Badih Ghazi and Madhu Sudan. The Power of Shared Randomness in Uncertain Communication. *arXiv:1705.01082*, May 2017.

[HAD+95] Richard J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. Quantum Cryptography. *Contemporary Physics*, 36(3), April 1995.

[Han03] Te Sun Han. *Information-Spectrum Methods in Information Theory*. Stochastic Modelling and Applied Probability. Springer-Verlag, Berlin Heidelberg, 2003.

[HJMR07] Prahladh Harsha, Rahul Jain, David McAllester, and Jaikumar Radhakrishnan. The Communication Complexity of Correlation. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 10–23, San Diego, CA, June 2007. IEEE.

[HMO+18] Iftach Haitner, Noam Mazor, Rotem Oshman, Omer Reingold, and Amir Yehudayoff. On the Communication Complexity of Key-Agreement Protocols. In *Innovations in Theoretical Computer Science*, 2018.

[HY10] S. W. Ho and R. W. Yeung. The Interplay Between Entropy and Variational Distance. *IEEE Transactions on Information Theory*, 56(12):5906–5929, December 2010.

[JPY12] Rahul Jain, Attile Pereszlenyi, and Penghui Yao. A direct product theorem for bounded-round public-coin randomized communication complexity. In *2012 IEE Symposium on Foundations of Computer Science*. IEEE, 2012.

[JRS03] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A Direct Sum Theorem in Communication Complexity via Message Compression. In Jos C. M. Baeten, Jan Karel Lenstra, Joachim Parrow, and Gerhard J. Woeginger, editors, *Automata, Languages and Programming*, Lecture Notes in Computer Science, pages 300–315. Springer Berlin Heidelberg, 2003.

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

[KRW95] Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3-4):191–204, September 1995.

[LCV15] Jingbo Liu, Paul Cuff, and Sergio Verdú. Secret key generation with one communicator and a one-shot converse via hypercontractivity. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 710–714. IEEE, 2015.

[LCV17] Jingbo Liu, Paul W. Cuff, and Sergio Verdú. Secret key generation with limited interaction. *IEEE Transactions on Information Theory*, 63, 2017.

[Liu16] Jingbo Liu. Rate region for interactive key generation and common randomness generation. *Manuscript*, 2016.

[Mau91] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing - STOC '91*, pages 561–571, New Orleans, Louisiana, United States, 1991. ACM Press.

[Mau92] UeliM. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1), 1992.

[Mau93] Ueli M Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[MO05] Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005.

[MOR+06] Elchanan Mossel, Ryan O'Donnell, Oded Regev, Jeffrey E Steif, and Benny Sudakov. Non-interactive correlation distillation, inhomogeneous markov chains, and the reverse bonami-beckner inequality. *Israel Journal of Mathematics*, 154(1):299–336, 2006.

[MW99] U.M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, March 1999.

[MW00] Ueli Maurer and Stefan Wolf. Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free. In *Advances in Cryptology — EUROCRYPT 2000*, volume 1807, pages 351–368. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

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

[Orl90] A. Orlitsky. Worst-case interactive communication. I. Two messages are almost optimal. *IEEE Transactions on Information Theory*, 36(5):1111–1126, September 1990.

[Orl91] A. Orlitsky. Worst-case interactive communication. II. Two messages are not optimal. *IEEE Transactions on Information Theory*, 37(4):995–1005, July 1991.

[PRV01] Stephen J. Ponzio, Jaikumar Radhakrishnan, and S. Venkatesh. The Communication Complexity of Pointer Chasing. *Journal of Computer and System Sciences*, 62(2):323–355, March 2001.

[PS82] Christos H. Papadimitriou and Michael Sipser. Communication Complexity. In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, pages 196–200, New York, NY, USA, 1982. ACM. event-place: San Francisco, California, USA.

[Raz92] Alexander A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

[RS18] Anup Rao and Makrand Sinha. Simplified Separation of Information and Communication. *Theory of Computing*, 14:29, 2018.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[SCP16] E. C. Song, P. Cuff, and H. V. Poor. The Likelihood Encoder for Lossy Compression. *IEEE Transactions on Information Theory*, 62(4):1836–1849, April 2016.

[Sho97] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. arXiv: quant-ph/9508027.

[STW19] Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for Generating Correlation. *In preparation*, 2019.

[Tya13] Himanshu Tyagi. Common information and secret key capacity. *IEEE Transactions on Information Theory*, 59(9):5627–5640, 2013.

[Wit75] Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975.

[Wyn75] Aaron D. Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975.

[Yan07] Ke Yang. On the (im)possibility of non-interactive correlation distillation. *Theoretical Computer Science*, 382(2):157–166, August 2007.

[Yao79] Andrew Chi-Chih Yao. Some Complexity Questions Related to Distributive Computing(Preliminary Report). In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 209–213, New York, NY, USA, 1979. ACM.

[Ye05] Chunxuan Ye. *Information Theoretic Generation of Multiple Secret Keys*. PhD thesis, University of Maryland, 2005.

[Yeh16] Amir Yehudayoff. Pointer chasing via triangular discrimination. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:151, 2016.

[ZC11] Lei Zhao and Yeow-Kiang Chia. The efficiency of common randomness generation. In *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2011.

A Alternate Definitions of Rate Regions

In this section we discussed the atlernate (though equivalent) definitions of rate regions for amortized and non-amortized CRG mentioned in Section 2.

A.1 Amortized CRG

The below definition was introduced in [AC93] for the case of 1-round and 2-round protocols, and the straightforward extension to r-round protocols has been referenced in several places, such as [GJ18]:

Definition A.1 (Amortized CRG (alternate definition to Definition 2.1))**.** A tuple (C, L) is *r-quasi-achievable for CRG* for a distribution ν if for each $N \in \mathbb{N}$, there is some $\epsilon_N \in \mathbb{R}$ with $\lim_{N\to\infty} \epsilon_N \to 0$, a key set $\mathcal{K}_N$, and an r-round private coin protocol $\Pi = \Pi(N) = (\Pi(N)_1, \ldots, \Pi(N)_r) \in (\{0,1\}^*)^r$ that takes as input $(X^N, Y^N) \sim \nu^{\otimes N}$, with output keys $K_{\mathtt{A}} = K_{\mathtt{A}}(N), K_{\mathtt{B}} = K_{\mathtt{B}}(N) \in \mathcal{K}_N$, such that

1. $\limsup_{N\to\infty} \frac{1}{N} \cdot \mathrm{CC}(\Pi(N)) \leq C$.
2. $\liminf_{N\to\infty} \frac{1}{N} \cdot \min\{H(K_{\mathtt{A}}(N)), H(K_{\mathtt{B}}(N))\} \geq L$.
3. $\log |\mathcal{K}_N| \leq cN$, for some absolute constant c that is independent of N (but which may depend on C, L).
4. $\mathbb{P}[K_{\mathtt{A}}(N) \neq K_{\mathtt{B}}(N)] \leq \epsilon_N$.

We denote the set of pairs (C, L) that are r-quasi-achievable from $(X, Y) \sim \nu$ by $\tilde{\mathcal{T}}_r(X, Y)$.

We remark that it is immediate that r-quasi-achievability (i.e., as in Definition A.1), at least for $c = L$, is stronger than r-achievability (i.e., as in Definition 2.1) in that any family of protocols Π satisfying the conditions of Definition A.1 and attaining a tuple (C, L) attains the same tuple and satisfies the conditions of Definition 2.1:

Proposition A.1. *Suppose Π r-quasi-achieves a tuple (C, L) according to Definition A.1 with $c = L$. Then it r-achieves the same tuple according to Definition 2.1.*

Proof. For any $N \in \mathbb{N}$, consider the r-round protocol from Definition A.1. Then condition (1) of that definition is the same as condition (1) of Definition 2.1, for the same ϵ_N. Since $K_{\mathtt{A}} \in \mathcal{K}_N$,

condition (2) of Definition A.1 gives $\liminf_{N\to\infty} \log|\mathcal{K}_N| \geq \liminf_{N\to\infty} H(K_{\mathtt{A}}) \geq L$ (in fact equality holds since $c = L$), thus verifying condition (2) of Definition 2.1. Pinsker's inequality now gives

$$\Delta(KK, K_{\mathtt{A}}K_{\mathtt{B}}) \leq \mathbb{P}[K_{\mathtt{A}} \neq K_{\mathtt{B}}] + \Delta(K, K_{\mathtt{A}}) \leq \epsilon_N + \sqrt{\mathrm{KL}(K||K_{\mathtt{A}})/2} = \epsilon_N + \sqrt{(L - H(K_{\mathtt{A}}))/2},$$

which tends to 0 as $N \to \infty$ by condition (2) of Definition A.1.

□

In fact, it turns out that the rate regions $\mathcal{T}_r(X,Y)$ and $\tilde{\mathcal{T}}_r(X,Y)$, for any source $(X,Y) \sim \nu$, are equal:

Theorem A.2 ([LCV17])**.** *For any source $(X,Y) \sim \nu$, $\mathcal{T}_r(X,Y) = \tilde{\mathcal{T}}_r(X,Y)$.*

In light of Theorem A.2, we will simply refer to tuples $(C,L) \in \mathcal{T}_r(X,Y) = \tilde{\mathcal{T}}_r(X,Y)$ as *r-achievable*, and will always use $\mathcal{T}_r(X,Y)$ to denote this region.

A.2 Amortized SKG

We can also use the conditions of Definiton A.1 instead of those of Definiiton 2.1 in the definition of r-achievability for SKG:

Definition A.2 (Amortized SKG (alternate definition to Definition 2.2))**.** A tuple (C,L) is *r-quasi-achievable for SKG* for a distribution ν if there is some choice of a sequence $\epsilon_N \to 0$ such that the following holds: for each $N \in \mathbb{N}$, there is some choice of private-coin protocol Π such that, first, conditions (1) – (3) of Definition A.1 are satisfied for these ϵ_N, Π, N, and, second,

$$\Delta(K_{\mathtt{A}}K_{\mathtt{B}}\Pi^r, K_{\mathtt{A}}K_{\mathtt{B}} \otimes \Pi^r) \leq \epsilon_N. \tag{56}$$

We denote the set of pairs (C,L) that are r-quasi-achievable for SKG from ν by $\tilde{\mathcal{S}}_r(X,Y)$.

As with CRG, quasi-achievability (i.e., Definition A.2) is equivalent to achievability (i.e., Definition 2.2), and we will never use the prefix "quasi" nor the tilde $\tilde{\mathcal{S}}_r(\cdot,\cdot)$ in the rate regions:

Theorem A.3 ([LCV17])**.** *For any source $(X,Y) \sim \nu$, $\mathcal{S}_r(X,Y) = \tilde{\mathcal{S}}_r(X,Y)$.*

A.3 Non-amortized CRG

As opposed to Definition 2.3, much of the literature on the non-amortized CRG problem [BM11, CGMS17, GR16, GJ18] has used the following definition, which only guarantees that the agreed-upon key is "close to uniform over a set of size 2^L", in the sense that it has min-entropy at least L:

Definition A.3 (Non-amortized CRG (alternate definition to Definition 2.3))**.** For $r, C \in \mathbb{N}$, and $L, \epsilon \in \mathbb{R}_{\geq 0}$, we say that *the tuple (C,L,ϵ) is r-quasi-achievable from the source ν (for CRG)* if there is some $N \in \mathbb{N}$ and an r-round protocol Π with private randomness that takes as input $(X^N, Y^N) \sim \nu^{\otimes N}$, such that at the end of Π, Alice and Bob output keys $K_{\mathtt{A}}, K_{\mathtt{B}} \in \mathcal{K}$, given by deterministic functions $K_{\mathtt{A}} = K_{\mathtt{A}}(X^N, R_{\mathtt{A}}, \Pi^r)$, $K_{\mathtt{B}} = K_{\mathtt{B}}(Y^N, R_{\mathtt{B}}, \Pi^r)$, such that:

1. $\mathrm{CC}(\Pi) \leq C$.
2. $\min\{H_\infty(K_{\mathtt{A}}), H_\infty(K_{\mathtt{B}})\} \geq L$.

3. $\mathbb{P}_\nu[K_{\mathtt{A}} = K_{\mathtt{B}}] \geq 1 - \epsilon$.

It is instructive to consider what would result if we were to change the second item in Definition A.3 to the requirement that $\min\{H(K_{\mathtt{A}}), H(K_{\mathtt{B}})\} \geq L$: for any $L, \epsilon > 0$ and any source μ, the tuple $(1, L, \epsilon)$ would be 1-achievable from the source μ. In other words, under this alternative definition, Alice and Bob would be able to generate arbitrarily large amounts of common randomness with only 1 bit of communication. To see this claim, consider the protocol where Alice uses private randomness to generate a random bit $B \in \{0, 1\}$ that is 1 with probability ϵ, and 0 otherwise. Alice then sends B to Bob. Then the keys, which are elements of $\mathcal{K} := \{0, 1\}^{\lceil L/\epsilon \rceil}$, are given as follows: if $B = 0$, then Alice and Bob both output the string of all 0s as the key. If $B = 1$, then Alice and Bob each use private randomness to choose a random element of $\mathcal{K}$, and output their respective elements as $K_{\mathtt{A}}, K_{\mathtt{B}}$, respectively. The probability of agreement is at least $1 - \epsilon$ (as Alice and Bob agree whenever $B = 0$), and the entropy of each of $K_{\mathtt{A}}, K_{\mathtt{B}}$ is at least $\epsilon \cdot \lceil L/\epsilon \rceil \geq L$.

Next we verify the simple fact that Definitions 2.3 and A.3 are essentially equivalent:

Proposition A.4. *The following two statements hold:*

- *Suppose that Π is an r-round protocol that achieves the tuple (C, L, ϵ) according to Definition 2.3, for some r, C, L, ϵ. Then there is an r-round protocol Π' that quasi-achieves the tuple $(C, L, 3\epsilon)$ in the sense of Definition A.3.*
- *Suppose that Π is an r-round protocol that quasi-achieves the tuple (C, L, ϵ) according to Definition A.3, for some r, C, L, ϵ. Then for any $\delta > 0$, there is an r-round protocol Π' that achieves the tuple $(C, \lfloor L - 2\log 1/\delta \rfloor, \epsilon + \delta)$ in the sen of Definition 2.3.*

Proof. First suppose that Π is an r-round protocol achieving the tuple (C, L, ϵ) in the sense of Definition 2.3. Definition 2.3 gives that if $K_{\mathtt{A}}, K_{\mathtt{B}}$ denote the parties' keys from the protocol Π, and if K denotes a uniformly distributed key on $\mathcal{K}$, a set of size at least 2^L, then $\Delta(K_{\mathtt{A}}, K) \leq \epsilon$ and $\Delta(K_{\mathtt{B}}, K) \leq \epsilon$. Therefore, there are randomized functions $g_{\mathtt{A}} : \mathcal{K} \to \mathcal{K}$ and $g_{\mathtt{B}} : \mathcal{K} \to \mathcal{K}$ such that $g_{\mathtt{A}}(K_{\mathtt{A}})$ and $g_{\mathtt{B}}(K_{\mathtt{B}})$ are distributed uniformly on $\mathcal{K}$, and such that $\mathbb{P}[K_{\mathtt{A}} \neq g_{\mathtt{A}}(K_{\mathtt{A}})] \leq \epsilon$ and $\mathbb{P}[K_{\mathtt{B}} \neq g_{\mathtt{B}}(K_{\mathtt{B}})] \leq \epsilon$. By the union bound, it follows that $\mathbb{P}[g_{\mathtt{A}}(K_{\mathtt{A}}) \neq g_{\mathtt{B}}(K_{\mathtt{B}})] \leq 3\epsilon$. Certainly $H_\infty(g_{\mathtt{A}}(K_{\mathtt{A}})) = H_\infty(g_{\mathtt{B}}(K_{\mathtt{B}})) = L$. Therefore, the protocol Π' in which Alice and Bob run Π but then output $g_{\mathtt{A}}(K_{\mathtt{A}}), g_{\mathtt{B}}(K_{\mathtt{B}})$ as their keys, respectively, quasi-achieves the tuple $(C, L, 3\epsilon)$ in the sense of Definition A.3.

Next suppose that Π is an r-round protocol that quasi-achieves the tuple (C, L, ϵ) in the sense of Definition A.3. Letting $K_{\mathtt{A}}, K_{\mathtt{B}}$ be Alice's and Bob's keys at the conclusion of Π, we have that $\min\{H_\infty(K_{\mathtt{A}}), H_\infty(K_{\mathtt{B}})\} \geq L$. We need the below lemma before continuing:

Lemma A.5. *Suppose $L > 0$ and $0 < \delta < 1$. Suppose a random variable K is distributed on a set $\mathcal{K}$ so that $H_\infty(K) \geq L$. Let $\mathcal{K}'$ be a set of size $\lfloor 2^{L - \log 1/\delta} \rfloor = \lfloor \delta 2^L \rfloor$. Then there is a deterministic function $f : \mathcal{K} \to \mathcal{K}'$ such that $H(f(K)) \geq H_\infty(f(K)) \geq (\log |\mathcal{K}'|) - \delta$.*

Proof. Pick some ordering on $\mathcal{K}$, and for each $k \in \mathcal{K}$ according to this ordering, set $f(k)$ to be the element in $\mathcal{K}'$ which has minimal probability mass assigned to it already under the distribution of $f(K)$. After this procedure, let $k'_* \in \mathcal{K}'$ have maximum probability under the distribution of $f(K)$, and suppose the last $k \in \mathcal{K}$ for which we set $f(k) = k'$ is denoted k_*. It must be the case that $\mathbb{P}[K \in \{k \in \mathcal{K} : k \neq k_*, f(k) = k'_*\}] \leq 1/|\mathcal{K}'|$ since before setting $f(k) = k'_*$ we had that k'_* had minimal probability mass under all $k' \in \mathcal{K}'$. Since $\mathbb{P}[K = k_*] \leq 2^{-L} \leq \delta/|\mathcal{K}'|$, it follows that $\mathbb{P}[f(K) = k'_*] \leq (1 + \delta)/|\mathcal{K}'|$, and so $H_\infty(f(K)) \geq (\log |\mathcal{K}'|) - \log(1 + \delta) \geq (\log |\mathcal{K}'|) - \delta$. □

Let $\mathcal{K}'$ be a set of size $\lfloor 2^{L-\log 1/\delta} \rfloor$, as in Lemma A.5. Notice that $|\mathcal{K}'| \geq 2^{\lfloor L-\log 1/\delta \rfloor}$. By Lemma A.5, there is a deterministic function, $f_{\mathtt{A}} : \mathcal{K} \to \mathcal{K}'$ such that $H(f_{\mathtt{A}}(K_{\mathtt{A}})) \geq |\mathcal{K}'| - \delta$. By Pinsker's inequality, it follows that if K' denotes the random variable that is uniformly distributed on $\mathcal{K}'$, then $\Delta(K', f_{\mathtt{A}}(K_{\mathtt{A}})) \leq \sqrt{\delta/2}$. In particular, there is a coupling of $K', f_{\mathtt{A}}(K_{\mathtt{A}})$ such that $\mathbb{P}[K' \neq f_{\mathtt{A}}(K_{\mathtt{A}})] \leq \sqrt{\delta/2}$. Now, the protocol Π' proceeds as follows: Alice and Bob first simulate Π, and then output $f_{\mathtt{A}}(K_{\mathtt{A}})$ and $f_{\mathtt{A}}(K_{\mathtt{B}})$ as their keys, respectively. Since $\mathbb{P}[K_{\mathtt{A}} \neq K_{\mathtt{B}}] \leq \epsilon$, we have $\mathbb{P}[f_{\mathtt{A}}(K_{\mathtt{A}}) \neq f_{\mathtt{A}}(K_{\mathtt{B}})] \leq \epsilon$ and $\mathbb{P}[K' \neq f_{\mathtt{A}}(K_{\mathtt{A}})] \leq \sqrt{\delta/2}$, it follows by the union bound that $\mathbb{P}[f_{\mathtt{A}}(K_{\mathtt{A}}) = f_{\mathtt{A}}(K_{\mathtt{B}}) = K'] \geq 1-\epsilon-\sqrt{\delta/2}$. It follows that Π' achieves the tuple $(C, \lfloor L-\log 1/\delta \rfloor, \sqrt{\delta})$ in the sense of Definition 2.3; the statement of the proposition then follows by replacing δ with δ^2. □