Optimal Communication Rates and Combinatorial Properties for Common Randomness Generation

Yanjun Han*, Kedar Tatwawadi*, Gowtham R. Kurri†, Zhengqing Zhou*, Vinod M. Prabhakaran‡, Tsachy Weissman*
*Stanford University, USA ({yjhan, kedart, zqzhou, tsachy}@stanford.edu)
†Arizona State University, USA (gowthamkurri@gmail.com)
‡Tata Institute of Fundamental Research, India (vinodmp@tifr.res.in)

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9518090

***Abstract*—We study the distributed simulation problem where n players aim to generate *same* sequences of random coin flips, and some subsets of the players share an independent common coin which can be tossed multiple times. The players communicate with each other via a publicly seen blackboard. We provide a tight representation of the optimal communication rates via linear programming, and more importantly, propose explicit algorithms for the optimal distributed simulation for a wide class of hypergraphs. In particular, the optimal communication rate in complete hypergraphs is still achievable in sparser hypergraphs containing a path-connected cycle-free cluster of topologically connected components. Some key steps in analyzing the upper bounds rely on two different definitions of connectivity in hypergraphs, which may be of independent interest.**

I. Introduction

Public randomness, or shared randomness, refers to some external randomness known to all agents which enables them to take coordinated actions. The most classical application of public randomness is the generation of the secret public key in cryptography [1]. This is also a valuable resource which aids diverse applications including developing randomized algorithms [2], reducing the communication complexity in distributed computing [3], reducing the sample complexity in distributed inference [4], coordination among players in game theory [5], and quantum mechanics [6]. In these applications, generating public randomness is of the utmost importance.

In many scenarios, there is shared randomness within certain subsets of the agents, and sound communication strategies are necessary to generate public randomness for all agents. Consider the following simple example: Alice shares independent randomness with Bob and Carlo respectively, and Alice aims to broadcast as few messages as possible to Bob and Carlo so that they have access to some public randomness. The simplest strategy for Alice is to broadcast any random bit R_0, then they generate 1 bit of public randomness with 1 bit of communication. However, if Alice broadcasts $R_1 \oplus R_2$ where the bits R_1 and R_2 come from the shared randomness with Bob and Carlo, respectively, then they successfully generate 2 bits of public randomness still with 1 bit of communication. Hence, the communication resources may be saved under better strategies.

In this paper, we consider a natural generalization of the above scenario: we are given a hypergraph $G = (V, E)$, where the vertex set $V = [n]$ is the set of n players, and the edge set $E = \{e_1, \cdots, e_m\}$ consists of hyperedges $e_i \subseteq V$ representing the subsets of players sharing a common fair coin. We assume that the coins for different hyperedges are mutually independent. The players can toss the shared coins multiple times as a part of the communication strategy. We also assume that the players may communicate with each other via a blackboard communication protocol [7], i.e., each player may write some messages on a publicly seen blackboard based on his shared coins and all current messages on the blackboard. The blackboard communication protocol allows for interactive strategies and is stronger than both the *simultaneous message passing* (SMP) protocol where each player writes messages on the blackboard independently of each other, and the sequential message passing protocol where players write messages sequentially but in a fixed order. The objective of the players is to generate the *same* random variable (or vector) X following a given target discrete distribution while minimizing the communication cost, i.e., the entropy of the message M written on the blackboard. We define the communication rate as the ratio $H(M)/H(X)$, where $H(\cdot)$ denotes the Shannon entropy of discrete random variables. We provide a tight representation of the optimal communication rates via linear programming (see Theorem 1 and the discussion following it). More importantly, we also propose explicit algorithms for the optimal distributed simulation for a wide class of hypergraphs (Theorem 2).

A. Related works

The role of public randomness has been given considerable attention in information theory literature starting from Wyner [8] who characterized the minimum rate of public randomness required for two processors to produce (approximatley) independent copies of random variables (X, Y). Public randomness was used for encoding and decoding in arbitrary varying channels by Ahlswede [9], and Csiszár and Narayan [10]. Generation of public randomness between two players which is hidden from an eavesdropper was studied in secret key (SK) agreement by Maurer [11], and Ahlswede and

Y. Han and K. Tatwawadi contribute equally to this paper. GK and VP were supported by the Department of Atomic Energy, Government of India, under project no. RTI4001. This work was done while G. R. Kurri was at the Tata Institute of Fundamental Research.

Csiszár [1]. Secret key agreement between multiple players was studied by Csiszár and Narayan [12]. This is closely related to communication for omnicience [13], [14]. The minimum communication rate required to generate secret key between two players was studied by Tyagi [15], and Ghazi and Jayram [16]. Building on this, Mukherjee et al. [17] derived a lower bound on this communication rate for SK agreement in the multiterminal source model.

A special source model, i.e., the *hypergraphical source model*, where clusters of players share independent randomness, has received attention in various works [17]–[20]. SK capacity as a function of the total communication was studied by Courtade and Halford [18], Chan [19], and Zhou and Chan [20], where [18] focussed on the non-asymptotic version. Our work is also on the hypergraphical source model, but differs from the previous works in that we exploit the combinatorial nature of general hypergraphs. We remark that the hypergraph theory plays an important role in Theorem 2. Specifically, the two different notions of hypergraph connectivity presented in Theorem 2 aim to generalize the following folklore in different ways (see Lemmas 1 and 3):

Folklore. *A tree on n vertices has exactly $n-1$ edges.*

The work by Mukherjee et al. [17] deserves special mention. Specifically, it showed that if the k-uniform hypergraph, or in general any multiterminal source model, is *of type* $\mathcal{S}$ (a notion introduced in [17]), then there is a strategy achieving the optimal communication rate $\frac{n-k}{n-1}$ and outputting each hyperedge (from a multi-hypergraph) exactly once. The main differences between our work and [17] are as follows. First, our achievability scheme is one-shot (i.e. no blocklengths required) and combinatorial, while the scheme in [17] potentially requires large blocklengths and is more information-theoretic. Second, although the type $\mathcal{S}$ condition is a nice "if and only if" result and could be checked efficiently in polynomial time for a given hypergraph (see also [21]), a rich combinatorial characterization about which family of hypergraphs are of type $\mathcal{S}$ remains unclear. Our work aims to provide a partial answer to this combinatorial problem, and based on the fundamental notions of connectivity, proposes rich families of hypergraphs that achieve the optimal $\frac{n-k}{n-1}$ communication rate. Although our families of hypergraphs must be of type $\mathcal{S}$, it is worth noting that so far we do not have a direct argument to connect them. Thus, our work presents an alternative approach which sheds more lights on the combinatorial perspective.

Notation: We denote by $\oplus$ the logical XOR operator. For a set A and $k \in \mathbb{N}$, let $\binom{A}{k}$ be the collection of all size-k subsets of A. Consequently, a k-uniform hypergraph $G = (V, E)$ is complete if $E = \binom{V}{k}$.

II. Main Results

The first theorem presents a general lower bound of the communication rate for any hypergraph.

Theorem 1. *Let $G = (V, E)$ be any hypergraph. Let X be the discrete random variable outputted by each vertex through a blackboard communication protocol, and M be the message written on the blackboard. Then $H(M)/H(X) \geq t(G)$, where $t(G)$ is the solution to the following linear program:*

$$t(G) = \begin{cases} \min & \sum_{v\in V} r_v, \\ \text{subject to} & \sum_{v\in U} r_v \geq \sum_{e\in E: e\subseteq U} s_e, \quad \forall U \subsetneq V, \\ & \sum_{e\in E} s_e \geq 1, \\ & r_v, s_e \geq 0, \quad \forall v \in V, e \in E. \end{cases}$$

A detailed proof is in an extended draft [22, Appendix B]. The linear program in Theorem 1 can be seen as a special case of a linear program [19, Corollary 2] in a related problem of secret-key agreement where it is also shown to be solvable in polynomial time[1]. Intuitively, the quantity r_v denotes the length of the messages sent by player v, and s_e denotes the number of random bits extracted from the hyperedge e to generate the common output X. Therefore, the first inequality constraints require that for any graph cut $U \subsetneq V$, the amount of information communicated from the players in U should at least cover the amount of randomness extracted out of hyperedges totally contained in U.

Although Theorem 1 (together with the asymptotic upper bounds) provides a tight characterization of the optimal communication rates of distributed simulation, the picture is still incomplete due to the following reasons. First, the existential proof of the network coding approach in [22, Appendix B] does not give an explicit communication strategy, and the result is asymptotic in the sense that large blocklengths are required and the communication rate only approaches but may never reach $t(G)$. Second, the linear program tells little about the combinatorial properties of the hypergraphs where a small communication rate is possible. For example, which hypergraphs are as good as the complete graphs?

To answer these questions, in this paper we propose explicit algorithms of communication strategies and investigate the combinatorial properties of hypergraphs which lead to a small communication rate, at the expense of losing certain generalities. Specifically, we will investigate the hypergraph structures which perform equally well as the complete k-uniform hypergraphs. Note that a hypergraph $G = (V, E)$ is called k-uniform if for all hyperedges $e \in E$ we have $|e| = k$. The following corollary follows immmediately from Theorem 1, which itself is a standard result (e.g. it is exactly the definition of type $\mathcal{S}$ in [17] for uniform hypergraphs).

Corollary 1. *Under the notations of Theorem 1, if $G = (V, E)$ is a k-uniform hypergraph, then*

$$\frac{H(M)}{H(X)} \geq \frac{n-k}{n-1}.$$

By Corollary 1, it remains to find hypergraph structures and explicit communication strategies where the optimal rate $\frac{n-k}{n-1}$ is achievable. The case $k = 2$ is easy and analyzed in [22,

[1]A version of extended draft [22] (arXiv:1904.03271v2) with Theorem 1 appears slightly earlier than [19] (arXiv:1910.01894v1) but without the observation of polynomial time solvability.

Appendix A], where a simple strategy achieves the optimal rate $\frac{n-2}{n-1}$ whenever the graph G is connected. However, this result does not generalize to any k-uniform hypergraphs with $k \geq 3$ under the usual notion of path connectivity for graphs, and a number of path-connected hypergraphs are too sparse to achieve a small communication rate. It also becomes challenging to propose an achievability scheme even if $k = 3$. The following theorem shows that under the correct definitions of connectivity, the optimal rate of communication is attainable.

Theorem 2. *Let $G = (V, E)$ be a k-uniform hypergraph, with $1 \leq k \leq n$. If G is a path-connected cycle-free cluster (cf. Definition 6) of topologically connected components (cf. Definition 1), then there exists an explicit communication strategy under the simultaneous message passing protocol such that for some $m \in \mathbb{N}$, each vertex can output the same random vector $X \sim \mathsf{Unif}(\{0,1\}^m)$ while the message M written on the blackboard satisfies*

$$\frac{H(M)}{H(X)} = \frac{n-k}{n-1}.$$

Remark 1. *Although Theorem 2 restricts the output X to be an independent and identically distributed (i.i.d.) Bernoulli random vector, the same communication rate can also be generalized to any i.i.d. random vectors, for $H(X)$ fair coin flips on average suffice to generate the distribution of a random variable X [8], [23].*

A detailed proof is deferred to Sections III and IV. Theorem 2 shows that the optimal rate $(n-k)/(n-1)$ is attainable non-asymptotically when the underlying hypergraph satisfies suitable connectivity conditions, which are generalizations of the classical connectivity for $k = 2$ from two different angles. We remark that a path-connected cycle-free cluster of topologically connected components differs significantly from the usual notion of path connectivity in hypergraphs, where the topological connectivity, the central concept in Theorem 2 and a stronger notion than path connectivity, views the hypergraph as a simplicial complex in the context of algebraic topology. For example, when $k = 3$ and $n = 4$, the hyperedges may be viewed as surfaces of a pyramid; two surfaces suffice to make the hypergraph path-connected, while three surfaces are necessary to make it topologically connected. We leave more discussions to the related works on hypergraph theory and formal definitions in Section III.

The new notion of connectivity contains a rich family of hypergraphs which suggests that Theorem 2 covers all hypergraphs for which the rate $(n-k)/(n-1)$ is achievable. Surprisingly, there are indeed richer families of hypergraphs which do not follow the previous connectivity notion but still achieve the optimal communication rate. We discuss these examples in [22, Section IV-C], where we characterize the complete class of optimal hypergraphs in certain cases such as $k = 2$, and $k = 3$ *star-shaped* hypergraphs, which are discussed in [22, Appendix F]. It is an outstanding open problem to figure out the complete class of optimal hypergraphs.

III. Achievability: Topological Connectivity

In this section we provide an achievability scheme for general topologically k-connected hypergraphs (cf. Definition 1). Later we generalize this scheme to incorporate cluster of topologically connected components (cf. Definition 6) in Section IV. We introduce the definition and properties of topological connectivity in Section III-A and the corresponding achievability strategy in Section III-B.

A. Topological connectivity

In [22, Appendix A], general achievability schemes have been proposed for all connected simple graphs when $k = 2$. A natural conjecture would be that similar ideas should also work for general "connected" k-uniform hypergraphs. We will show that this conjecture is true, while we need the correct definition of connectivity for k-uniform hypergraphs.

In our paper, we adopt the tree definition in [24] and reinterpret it as *topological connectivity*:

Definition 1 (Topologically k-connected hypergraph)**.** *For any k-uniform hypergraph $G = (V, E)$ with $k \geq 2$, define the following* generation step*: for hyperedges $e_1, \cdots, e_m \in E$ and any hyperedge $e \notin E$, if all $(k-1)$-tuples in $\binom{V}{k-1}$ appearing in $e_1, \cdots, e_m, e$ appear an even number of times, we may add the hyperedge e to the hypergraph. We call G is* topologically k-connected *if G becomes a complete k-uniform hypergraph after a finite number of generation steps.*

Definition 2 (Minimal topologically k-connected hypergraph)**.** *For $k \geq 2$, a k-uniform hypergraph G is called* minimal topologically k-connected *if G is topologically k-connected and removing any hyperedge of G makes it become not topologically k-connected.*

The main property for minimally topologically k-connected hypergraphs is summarized in the following lemma. We remark that this property is implicitly implied by the main theorem in [24].

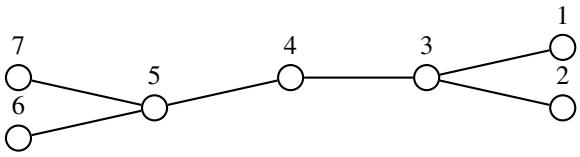
Lemma 1. *Any minimal topological k-connected hypergraph with n vertices has exactly $\binom{n-1}{k-1}$ hyperedges.*

The proofs of this lemma and the subsequent lemmas can be found in [22, Appendix E]. When $k = 2$, Lemma 1 generalizes the fact that a tree on n vertices has exactly $n-1$ edges.

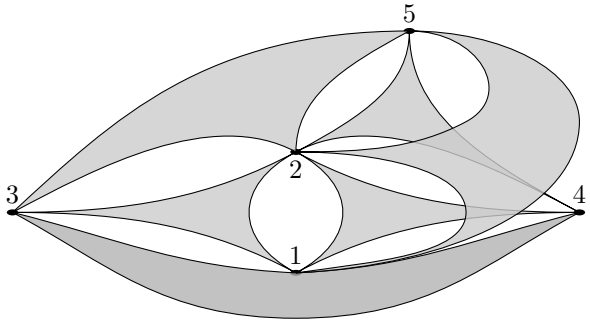
B. Achievability scheme

In this subsection we propose the achievability scheme for general topologically k-connected hypergraph G. We assume that G is minimal topologically k-connected. For each $i \in [n]$, we define the induced hypergraph G_i from G as follows: the vertex set of G_i is $V_i = [n] \backslash \{i\}$, and the edge set of G_i is $E_i = \{e \backslash \{i\} : i \in e \in E\}$. Hence, the induced hypergraph G_i is $(k-1)$-uniform, and e is a hyperedge of G_i if and only if $e \cup \{i\} \in E$. We have the following lemma.

Lemma 2. *For $k \geq 3$, if G is topologically k-connected, then all induced hypergraphs G_i are topologically $(k-1)$-connected.*



(a) A minimal topologically 2-connected hypergraph on 7 vertices with 6 edges, or equivalently, a spanning tree.



(b) A minimal topologically 3-connected hypergraph on 5 vertices with 6 hyperedges.

Fig. 1: Examples of minimal topologically k-connected hypergraphs with $k = 2, 3$.

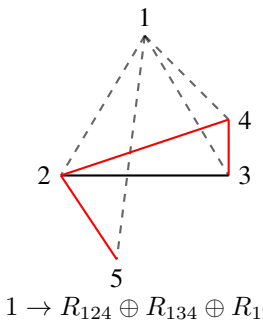
We propose the following communication strategy for topologically k-connected hypergraphs. For each edge $e \in E$, we define an independent random variable $R_e \sim \mathsf{Unif}(\{0,1\})$ by tossing the associated common coin.

Definition 3 (Communication strategy for k-connected hypergraphs)**.** *For a minimal topologically k-connected hypergraph G with $k \geq 3$, the communication strategy is as follows: for each $i \in [n]$,*

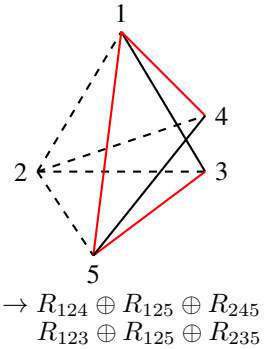
1) *Player i constructs the induced hypergraph G_i, and choose an arbitrary minimal topologically $(k-1)$-connected subgraph $G_i^\star \subseteq G_i$ (existence of $G_i^\star$ is ensured by Lemma 2);*
2) *For each hyperedge e of G_i which is not in $G_i^\star$, let e be generated by $e_1, \cdots, e_m$ in $G_i^\star$ (cf. Definition 1). Player i then writes $R_{e\cup\{i\}} \oplus R_{e_1\cup\{i\}} \oplus \cdots \oplus R_{e_m\cup\{i\}}$ on the blackboard.*

Although the previous scheme is defined for $k \geq 3$, it is straightforward to see that it reduces exactly to the achievability scheme in [22, Appendix A] when $k = 2$ (by adapting the definition of topologically 1-connected graph appropriately). Moreover, this strategy can be implemented under the simultaneous message passing model. We refer to Figure 2 for an example.

Assuming for a moment that every player may decode the random vector $X = (R_e : e \in E)$, we show that the communication rate of this strategy is optimal. Firstly, by Lemma 1 and the minimality of G, $H(X) = |E| = \binom{n-1}{k-1}$. Moreover, the number of bits player i writes on the blackboard is $|M_i| = |\{e \in E : i \in e\}| - \binom{n-2}{k-2}$, where Lemma 1 again shows that each $G_i^\star$ has $\binom{n-2}{k-2}$ hyperedges. As a result, the



(a) Induced graph G_1 (solid lines) and $G_1^\star$ (red lines).



(b) Induced graph G_2 (solid lines) and $G_2^\star$ (red lines).

Fig. 2: The communication strategy on the minimally topologically connected 3-uniform hypergraph in Figure 1(b), which achieves the optimal communication rate $1/2$.

total length of the message M is

$$|M| = \sum_{i=1}^{n} |M_i| = \sum_{i=1}^{n} \left(|\{e \in E : i \in e\}| - \binom{n-2}{k-2} \right)$$
$$= k|E| - n\binom{n-2}{k-2} = \binom{n-2}{k-1}.$$

Hence, the communication rate can be upper bounded as

$$\frac{H(M)}{H(X)} \leq \frac{|M|}{H(X)} = \frac{\binom{n-2}{k-1}}{\binom{n-1}{k-1}} = \frac{n-k}{n-1},$$

which is optimal by Corollary 1. Therefore it remains to prove the following theorem.

Theorem 3. *Let $G = (V, E)$ be a topologically k-connected hypergraph. Then under the communication strategy in Definition 3, every player may decode the random vector X.*

The proof of Theorem 3 requires delicate algebraic and combinatorial arguments for topological connectivity, which is deferred to [22, Appendix C].

IV. Generalization: Clusters of Connected Components

In this section, we generalize the achievability scheme in Section III to incorporate the cases where the hypergraph is not topologically connected but consists of topologically connected components.

A. Path connectivity

First we review the notion of path connectivity in general (and not necessarily uniform) hypergraphs. Recall that a general hypergraph $G = (V, E)$ consists of a finite vertex set V and a finite hyperedge set $E = \{A_1, \cdots, A_m\}$, where $A_i \subseteq V$ are non-empty subsets of V. Path connectivity in hypergraphs is defined as follows.

Definition 4 (Path and path connectivity)**.** *In a hypergraph $G = (V, E)$ and vertices $u, v \in V$, a* simple path *from u*

to v is a sequence of distinct vertices $v_0, v_1, \cdots, v_k \in V$ and distinct hyperedges $A_1, \cdots, A_k \in E$ such that $v_0 = u, v_k = v$, and $v_{i-1}, v_i \in A_i$ for any $i \in [k]$. The hypergraph G is path-connected *iff a simple path from u to v exists for any $u, v \in V$.*

We also need the notion of cycle-free hypergraphs.

Definition 5 (Simple cycle and cycle-free hypergraph)**.** *In a hypergraph $G = (V, E)$, a* simple cycle *is a sequence of distinct vertices $v_0, v_1, \cdots, v_{k-1} \in V$ and distinct hyperedges $A_1, \cdots, A_k \in E$ such that $v_{i-1}, v_i \in A_i$ for any $i \in [k]$, where $v_k = v_0$. The hypergraph G is* cycle-free *iff there is no simple cycle in G.*

Note that a path-connected cycle-free 2-uniform hypergraph is a tree. The next lemma is another generalization of the fact that a tree on n vertices has exactly $n-1$ edges. Recall that for each $v \in V$, the degree of v is defined as $\deg(v) = |\{A \in E : v \in A\}|$.

Lemma 3. *Let $G = (V, E)$ be a path-connected cycle-free hypergraph. Then $\sum_{A \in E} (|A| - 1) = |V| - 1$, and $\sum_{v \in V} (\deg(v) - 1) = |E| - 1$.*

B. Achievability scheme

In this section we formally define the cluster of connected components, and present a communication strategy achieving the upper bound in Theorem 2 under the simultaneous message passing procotol.

Definition 6. *Let $G = (V, E)$ be a k-uniform hypergraph. We call G is a* cluster of connected components *if and only if there is another hypergraph (not necessarily k-uniform) $G_c = (V, \{A_1, \cdots, A_m\})$ such that (where the subscript c stands for "cluster"):*

1) *the hypergraph G_c is path-connected and cycle-free;*
2) *for each $i \in [m]$, the restriction of G on the vertices in A_i is topologically k-connected.*

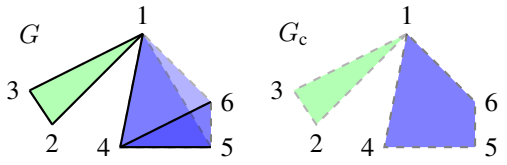


Fig. 3: An example of a cluster of connected components.

Definition 6 essentially says that to form a cluster, the topologically k-connected components of G should be path-connected without cycles in terms of components. Figure 3 illustrates an example of such a cluster, where

$$G = ([6], \{\{1,2,3\}, \{1,4,5\}, \{1,4,6\}, \{4,5,6\}\}),$$
$$G_c = ([6], \{\{1,2,3\}, \{1,4,5,6\}\}).$$

Next we define the communication strategy for clusters of connected components.

Definition 7 (Communication strategy for clusters of connected components)**.** *Let the k-uniform hypergraph $G = (V, E)$ be a cluster of connected components, with the corresponding cluster hypergraph $G_c = (V, \{A_1, \cdots, A_m\})$. The communication strategy is as follows:*

1) *For each $i \in [m]$, remove edges so that the restriction of G on A_i is minimally topologically k-connected;*
2) *Messages within components: for each $i \in [m]$, repeat (for different realizations of coin tosses) the strategy in Definition 3 for M_i times in the restricted graph on A_i, where M_i is chosen so that*

$$M_i \cdot \binom{|A_i| - 2}{k - 2} = C \tag{1}$$

for some common constant $C > 0$. We choose C large enough so that each M_i is an integer;
3) *Messages across components: for each $v \in V$ belonging to at least two connected components $A_{i_1}, \cdots, A_{i_\ell}$ (i.e., $\ell = \deg_{G_c}(v) \geq 2$) and $j \in [\ell]$, let $G_j^\star$ be the minimal topologically $(k-1)$-connected subgraph of v-induced hypergraph in the connected component A_{i_j} (cf. Definition 3) used in the previous step. Let $R_j \in \mathbb{F}_2^C$ be the binary vector consisting of the outcomes of coin tosses corresponding to every hyperedge in $G_j^\star$ repeated M_{i_j} times[2], in an arbitrary order. Then vertex v writes*

$$M_v = (R_1 \oplus R_2, R_1 \oplus R_3, \cdots, R_1 \oplus R_\ell)$$

on the blackboard.

For example, for the previous hypergraph in Figure 3, we have $|A_1| = 3, |A_2| = 4$. Consequently, we may choose $M_1 = 2, M_2 = 1$ and $C = 2$. Let R_{123}, R'_{123} be independent outcomes of the common coin shared among $\{1,2,3\}$ (i.e., toss coin twice), then the message within components (broadcast by player 4) is $R_{145} \oplus R_{146} \oplus R_{456}$, and the messages across components (broadcast by player 1) are $R_{123} \oplus R_{145}, R'_{123} \oplus R_{146}$. It is straightforward to see that each player may decode the random vector $(R_{123}, R'_{123}, R_{145}, R_{146}, R_{456})$, and thus the previous strategy achieves the optimal communication rate $3/5$ in this example.

The following theorem (proved in [22, Appendix D]) states that for general clusters of connected components, the strategy in Definition 7 achieves the optimal communication rate, thereby completing the proof of Theorem 2. Let X be the binary vector consisting of all coin tossing outcomes during the strategy in Definition 7.

Theorem 4. *For any k-uniform hypergraph $G = (V, E)$ which is a path-connected cycle-free cluster of topologically connected components, every player may decode the entire outcome vector X under the strategy in Definition 7, with communication rate $H(M)/H(X) = (n-k)/(n-1)$.*

[2]Note that $G_j^\star$ has exactly $\binom{|A_{i_j}| - 2}{k-2}$ hyperedges by Lemma 1, the choice of M_{i_j} in (1) ensures that the dimension of the vector R_j is exactly C.

REFERENCES

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[2] M. Mitzenmacher and E. Upfal, *Probability and computing: Randomized algorithms and probabilistic analysis*. Cambridge University Press, 2005.

[3] E. Kushilevitz and N. Nisan, "Communication complexity," 1996.

[4] J. Acharya, C. L. Canonne, Y. Han, Z. Sun, and H. Tyagi, "Domain compression and its application to randomness-optimal distributed goodness-of-fit," *arXiv preprint arXiv:1907.08743*, 2019.

[5] V. Anantharam and V. S. Borkar, "Common randomness and distributed control: A counterexample," *Systems & Control Letters*, vol. 56, pp. 568–572, 2007.

[6] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Transactions on Information Theory*, vol. 48, no. 10, pp. 2637–2655, 2002.

[7] E. Kushilevitz, "Communication complexity," in *Advances in Computers*. Elsevier, 1997, vol. 44, pp. 331–360.

[8] A. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, 1975.

[9] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[10] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Transactions on Information Theory*, vol. 34, no. 2, pp. 181–193, 1988.

[11] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[12] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[13] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy, and steiner tree packing," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6490–6500, 2010.

[14] N. Ding, C. Chan, Q. Zhou, R. A. Kennedy, and P. Sadeghi, "Determining optimal rates for communication for omniscience," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1919–1944, 2018.

[15] H. Tyagi, "Common information and secret key capacity," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5627–5640, 2013.

[16] B. Ghazi and T. Jayram, "Resource-efficient common randomness and secret-key schemes," in *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, 2018, pp. 1834–1853.

[17] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam, "On the public communication needed to achieve sk capacity in the multiterminal source model," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3811–3830, 2016.

[18] T. A. Courtade and T. R. Halford, "Coded cooperative data exchange for a secret key," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3785–3795, 2016.

[19] C. Chan, "Secret key agreement for hypergraphical sources with limited total discussion," *arXiv preprint arXiv:1910.01894v1*, 2019.

[20] Q. Zhou and C. Chan, "Secret key generation for minimally connected hypergraphical sources," *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4226–4244, 2020.

[21] C. Chan, A. Al-Bashabsheh, J. B. Ebrahimi, T. Kaced, and T. Liu, "Multivariate mutual information inspired by secret-key agreement," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1883–1913, 2015.

[22] Y. Han, K. Tatwawadi, G. R. Kurri, Z. Zhou, V. M. Prabhakaran, and T. Weissman, "Optimal communication rates and combinatorial properties for distributed simulation," *arXiv preprint arXiv:1904.03271v3*, 2020.

[23] D. Knuth and A. Yao, "The complexity of nonuniform random number generation," *Algorithm and Complexity, New Directions and Results*, pp. 357–428, 1976.

[24] G. Kalai, "Enumeration of Q-acyclic simplicial complexes," *Israel Journal of Mathematics*, vol. 45, no. 4, pp. 337–351, Dec 1983. [Online]. Available: https://doi.org/10.1007/BF02804017