# Partition Information and its Transmission over Boolean Multi-Access Channels

Shuhang Wu, Shuangqing Wei, Yue Wang, Ramachandran Vaidyanathan and Jian Yuan

**Abstract**

In this paper, we propose a novel partition reservation system to study the partition information and its transmission over a noise-free Boolean multi-access channel. The objective of transmission is not message restoration, but to partition active users into distinct groups so that they can, subsequently, transmit their messages without collision. We first calculate (by mutual information) the amount of information needed for the partitioning without channel effects, and then propose two different coding schemes to obtain achievable transmission rates over the channel. The first one is the brute force method, where the codebook design is based on centralized source coding. On the other hand, the second method uses random coding where the codebook is generated randomly and MAP decoding is employed to reconstruct the partition. Both methods shed light on the internal structure of the partition problem. A novel hypergraph formulation is proposed for the random coding scheme, which intuitively describes the information in terms of a strong coloring of a hypergraph induced by a sequence of channel operations and interactions between active users. An extended Fibonacci structure is found for a simple, but non-trivial, case with two active users. A comparison between these methods and group testing is conducted to demonstrate the uniqueness of our problem.

**Index Terms**

partitioning information, conflict resolution, Boolean algebra, Fibonacci numbers.

[1]S. Wu, Y. Wang and J. Yuan is with Department of Electronic Engineering, Tsinghua University, Beijing, P. R. China, 100084. (E-mail: wsh05@mails.tsinghua.edu.cn; wangyue, jyuan@mail.tsinghua.edu.cn). S. Wei and R. Vaidyanathan are with the School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803, USA (Email: swei@lsu.edu, vaidy@lsu.edu).

## I. INTRODUCTION

One primary objective of many coordination processes is to order a set of participants. For example, multiaccess can be viewed as (explicitly or implicitly) ordering a set of users for exclusive access to a resource. Information interaction plays a key role in establishing such an order. To formalize this interactive information and derive fundamental limits on its transmission, we propose in this paper a novel partition reservation model over a noise-free Boolean multi-access channel and use an information theoretic approach in its analysis.

For the simplest variant of the problem we study, let $\mathcal{N} = \{1, \ldots, N\}$ be a set of $N$ users and let $\mathcal{G}_{\mathbf{s}} = \{i_1, \ldots, i_K\} \subseteq \mathcal{N}$ be a set of *active* users. These users are connected through a shared Boolean multi-access channel. The channel is slotted and during slot $t$ it provides a Boolean feedback $y_t \in \{0, 1\}$ which is 0 iff no user transmits on the channel during slot $t$. For this simple model, each user can observe $y_t$. The problem is to partition $\mathcal{N}$ into $|\mathcal{G}_{\mathbf{s}}| = K$ groups (or blocks), so that each group has exactly one active user from $\mathcal{G}_{\mathbf{s}}$ and each user $i$ learns the id $z_i \in \mathcal{K} \triangleq \{1, 2, \cdots, K\}$ of the group it belongs to. Suppose that each active user $i$ transmits bit $x_{i,t} \in \{0, 1\}$ during slot $t$. At the end of $T$ slots, the common feedback from the channel (observable by all users) is $\mathbf{y} = [y_1, \ldots, y_T]^\top$, where $y_t = \bigvee_{i \in \mathcal{G}_{\mathbf{s}}} x_{i,t}$, for all $1 \leq t \leq T$. The goal is to schedule the transmissions (through and accessing matrix or codebook $\mathbf{X} \triangleq [x_{i,t}]_{1 \leq i \leq N, 1 \leq t \leq T}$) and a common decoding function $g(\cdot)$ in advance, so that the desired common *partition* $\mathbf{z} = [z_1, \ldots, z_N]^\top = g(\mathbf{y})$ is obtained, here user $i$ belongs to block(or group) $z_i$ of the partition, recall that $z_i \in \mathcal{K}$. The objective is to find an achievable lowerbound on the number of slots $T$, within which there exists a matrix $\mathbf{X}$ so that every possible active set $\mathcal{G}_{\mathbf{s}} \subseteq \mathcal{N}$ can be assigned different groups.

In the problem we consider, we do not seek to restore the states of all users (that is, determine $\mathcal{G}_{\mathbf{s}}$ exactly), but to partition $\mathcal{G}_{\mathbf{s}}$. Thus, a particular partition information that only pertains to the relationship between active users in $\mathcal{G}_{\mathbf{s}}$, is transmitted through the Boolean multi-access channel. We will formalize this partition information, and focus on the achievable bound of its transmission rate over Boolean multi-access channels. This problem plays a significant role in understanding the fundamental limits on the capability of establishment of order in distributed systems.

The proposed problem has a close relationship to a typical slotted conflict resolution problem [2], where each active users must transmit without conflict at least once during $T$ slots, i.e., if

$x_{i,t} = 1$ denotes a trial of transmission for user $i$ at slot $t$, then there exists a $1 \leq t_i \leq T$ such that $x_{i,t_i} = 1$, and for all $j \in \mathcal{G}_{\mathbf{s}} - \{i\}$, we have $x_{j,t_i} = 0$. Hajak proposed that the essence of this problem is to partition active users into different sets of slots during the conflict resolution process [3]. To achieve this goal, mainly two types of systems are studied: direct transmission system and reservation system with group testing [4]. The former focuses on directly designing an accessing matrix $\mathbf{X}$ so that each node finds at least one slot for its exclusive access to the channel. The slot scale is the same as the payload package size, and the partition process is actually mixed with payload transmission. Note that the resulting transmission order for each active node is not known to the user, only its success is ensured. The latter (reservation and group testing) has two stages. In the first reservation stage, an accessing matrix $\mathbf{X}$ and decoding function $g(\cdot)$ are designed such that $\mathcal{G}_{\mathbf{s}}$ is exactly determined by $g(\mathbf{y})$, where $\mathbf{y}$ is the channel feedback. That is, (active or inactive) states of all users are restored and, subsequently, active users can transmit in a predetermined order in a second stage. The reservation stage is also called group testing [5] or compressed sensing [6] in different fields. The two stages can be of different time scales. We can see the payload transmission is separated, but in the reservation stage, $\mathcal{G}_{\mathbf{s}}$ is known to all users, which is more than we need.

Compared with group testing and direct transmission system, our partitioning reservation system provides a new way to individually analyze the process of partitioning, which is the essence of coordination in conflict resolution problems. It can be used as a reservation stage instead of group testing in conflict resolution problems, and holds the possibility of requiring fewer resources, since it seeks only to partition $\mathcal{N}$, rather than restore $\mathcal{G}_{\mathbf{s}}$. (Notice that once $\mathcal{G}_{\mathbf{s}}$ is restored, obtaining a partition is straightforward.) Compared with direct transmission, we observe that usually, the time scale for reservation can be much smaller in partition/reservation than that in payload transmission, thus it is difficult to compare the actual total times of these two approaches. However, since the obtained common partition is known to all active users in the partition reservation system, in addition to conflict resolution, it has more applications in parallel and distributed computation [7–9], such as leader election [10], broadcasting [11]. Our theoretical study will also further the understanding of the limits of partitionability of interacting users in distributed systems.

In this paper, we first use source coding to quantify the partition information. Then two coding schemes for the accessing matrix $\mathbf{X}$, and decoding function $g(\cdot)$ are proposed. The

first uses a brute force method to design $\mathbf{X}$ and $g(\cdot)$ directly by source coding. The second scheme, employing random coding, generates accessing matrix elements $x_{i,t}$ i.i.d. a by Bernoulli distribution, then the partition is recovered by MAP (maximum a posteriori) decoding. The two methods can both work, and provide different views of this problem. In particular, in the brute force method, if $T^{BF} = \frac{K^{K+1}}{K!} f(N)$ and $f(N)$ is an arbitrary function satisfying $\lim_{N\to\infty} f(N) = \infty$, the average error probability $P_e^{(N)} \leq e^{-f(N)} \to 0$, as $N \to \infty$. While for a simple but non-trivial $K = 2$ case, we prove in random coding, if for any $\xi > 0$, $\frac{logN}{T} \leq \max_{0\leq p\leq 1} C(p) - \xi$, where $C(p) = -(1-(1-p)^2)\log\varphi(p) - (1-p)^2\log(1-p)$, $\varphi(p) = \frac{p+\sqrt{4p-3p^2}}{2}$, we have the average error probability $P_e^{(N)} \leq \frac{1}{N^\Delta} \to 0$ for some $\Delta > 0$, i.e., with polynomial speed. The two achievable bounds are shown better than that of group testing.

Moreover, for the random coding approach, we provide a novel framework to solve the problem from the view of strong coloring of hypergraphs, namely, the partition objective can be transformed to the strong coloring problem of a resulting hypergraph, and the effect of channel(s) is reflected by a series of operations on hypergraph edges. Under such a framework, the partition information is represented by types of hypergraphs in which hyper-edges are determined by the interaction among a set of possible active nodes. The joint work between the encoder and decoder is to make sure that the resulting hypergraphs become strong colorable after transmissions by active nodes and intervention by channels. In a simple, but nontrivial, case with $K = 2$ active users for a set of $N$ users, a suboptimal odd cycle based analysis is proposed, and a structure of extended Fibonacci numbers is found, which sheds lights on the inherent structure of the partition information and Boolean channel, and could be further explored for $K > 2$ cases.

As a summary, the contributions of this paper are twofold. First, we formulate a novel partition reservation problem which captures the transmission and restoration of some relationship information among active users. This relationship communication problem is also represented in a novel hypergraph based framework. Secondly, we propose two types of coding approaches, and the corresponding achievable bounds on the communication period, which provides the intuitive examples to study the relationship information transmission over Boolean multi-access channels.

Part of our results has been presented in [1]. In this paper, we provide a more complete and comprehensive solution the formulated problems. In particular, we discuss the source coding problem in Section IV. Then based on source coding, we give a brute force coding method

in Section V to solve the partition problem. In Section VII, a sub-optimal decoding approach for the case of $K = 2$ is provided which requires the resulting graph without odd cycles (i.e. two-colorable). Detailed proofs are then given to both Lemma 2 and Theorem 3, which are not included in [1] due to space limitation.

The rest of this paper is organized as follows: in Section II, we introduce the related work. The problem formulation appears in Section III. In Section IV, the partition information is illustrated by centralized source coding, then a brute force method directly inspired by source coding is proposed in Section V. In Section VI, a random coding method is considered and the problem is reformulated in terms of a hypergraph. Based on this, a simple, but non-trivial, result for $K = 2$ in random coding is analyzed in Section VII. In Section VIII, we compare our results with that of group testing. We summarize our results and make some concluding remarks in Section IX.

## II. Related Work

Although the proposed partition model could be useful in many problem settings, typical applications are in conflict resolution problems. The work on conflict resolution is too wide for a comprehensive survey here, so only work closest to our problem setting are discussed.

To the best of our knowledge, Hajak first expressed the nature of conflict resolution as that of partitioning active users into different groups [3, 12], and derived an achievable bound of partition information, without considering the channel effect. The converse problem (namely, to find bound $T_0$, such that if $T$ is achievable, we must have $T > T_0$) was discussed by Hajek, Körner, Simonyi and Marton [13–15], and is still an open question. The previous work on partition information [3, 13, 14] is actually from the source coding perspective, i.e. representation of users' states using partition information, and is consistent with Section IV of this paper. In contrast, we focus on construction of a partition relationship among active users by their explicit transmission over a collision Boolean multi-access channel. This problem has not been addressed previously, to the best of our knowledge.

On the other hand, there are extensive works on direct transmission and group testing that consider channel effects from the *combinatorics* and *probabilistic* perspectives. Ding-Zhu and Hwang provide in [5] an overview; more specific approaches can be found on superimposed codes for either disjunct or separable purposes [16–20], on selective families [11], on the broadcasting problem [21], and for other methods [19, 22, 23].

It should be noted that recently, group testing has been reformulated using an information theoretic framework to study the limits of restoration of the IDs of all active nodes over Boolean multiple access channels [24]. On the other hand, we address in this paper the transmission of partition information (rather than identification information) over the channel, and it is thus, different from existing work.

## III. System model

### A. Formulation

In this paper, lower-case (resp., upper-case) boldface letters are used for column vectors (resp., matrices). For instance, $x_i$ is used for the $i$-th element of vector $\mathbf{x}$, and $x_{i,t}$ is used for the $(i,j)$-th element of matrix $\mathbf{X}$. Logarithms are always to base 2.

Assume the number of active users $K$ is known to all users. The users are also given a common $N \times T$ accessing matrix (or codebook) $\mathbf{X}$, and a decoding function $g(\cdot)$. We use a Boolean vector $\mathbf{s} = [s_1, \ldots, s_N]^\top$ to represent the active or inactive states of users, where $s_i = 1$ iff user $i$ is active (that is, $i \in \mathcal{G}_\mathbf{s}$). Active users will use $T$ slots to transmit according to codebook $\mathbf{X}$ and observe the feedback $\mathbf{y} = [y_t \ : \ 1 \le t \le T]^\top$ over these $T$ slots. Then users derive the partition $\mathbf{z} = g(\mathbf{y})$. There are two dimensions in this problem, the user dimension of size $N$ and the time dimension of size $T$.

*a) An Example:* Our approach is illustrated by an example in Fig. 1 with four users from $\mathcal{N} = \{1,2,3,4\}$, of which the users of set $\mathcal{G}_\mathbf{s} = \{1,2\}$ are active. The $N \times T$ codebook is

$$\mathbf{X} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

In each slot $1 \le t \le 3 = T$, user $i$ writes to the channel iff $i$ is active and $x_{i,t} = 1$. For example, in slot 1, that has $x_{1,1} = x_{2,1} = 1$ and $x_{3,1} = x_{4,1} = 0$, both active users 1 and 2 write to the channel, resulting in a channel feedback of $y_1 = 1$. In slot 2, $x_{3,2} = 1$, however, since user 3 is not active, there is no write and $y_2 = 0$. In slot 3, users 1 and 3 are called upon to write, but only user 1 writes as user 3 is not active. The channel feedback over the three slots is $\mathbf{y} = [y_1, y_2, y_3]^\top = [1,0,1]^\top$. From this feedback, the knowledge of $K = 2$ and the accessing matrix $\mathbf{X}$, the following conclusions can be drawn.

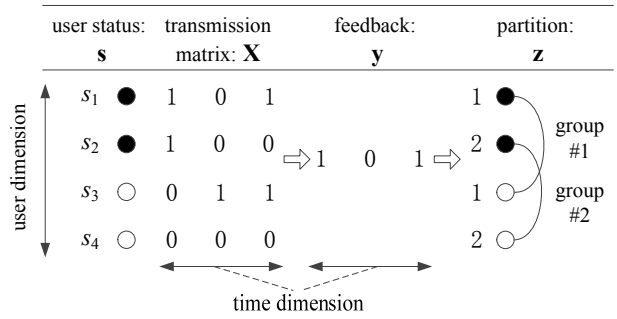


Fig. 1. Example of the formulation. ($N = 4$, $K = 2$, $\mathcal{G} = \{1, 2\}$ indicates that users 1 and 2 are active; the total number of time slots is $T = 3$. )

- Because $x_{3,2} = 1$ and $y_2 = 0$, it can be concluded that user 3 is not active.
- Because $x_{1,3} = x_{3,3} = 1$ and $y_3 = 1$, it can be concluded that user 1 is active (as user 3 is inactive), also $\mathcal{G}_{\mathbf{s}} \nsubseteq \{2, 4\}$.
- The interaction in slot 1 only says that $\mathcal{G}_{\mathbf{s}} \nsubseteq \{3, 4\}$.
- Since $K$ is known to be 2, we conclude that exactly one of users 2 and 4 must be active and the other inactive.
- Thus partition $\{\{1, 3\}, \{2, 4\}\}$ of $\mathcal{N}$ separates active nodes into different groups, and $\mathbf{z} = [1\ 2\ 1\ 2]^\top$ can be selected as the result of decoding $\mathbf{y}$.

Observe that (unlike the restoration of $\mathcal{G}_{\mathbf{s}}$), we do not (and need not) know which among users 2 and 4 is active. Likewise although we happen to know that user 1 is active and user 3 is not, this knowledge is coincidental; the partition approach does not invest resources to seek this knowledge.

To have a more general formulation, the problem can be treated as a coding problem in multi-access channels from the information theoretic view. Consider $N$ users whose active states are given in a vector $\mathbf{s} \in \mathbb{S}_{K;N} \triangleq \{\mathbf{s} \in \{0, 1\}^N : \sum s_i = K\}$. The $i$-th row of $\mathbf{X}$, denoted by $\mathbf{x}_i^\top$ can be viewed as a codeword of user $i$ (note that $\mathbf{x}_i$ is a column vector, we would like to use a row vector $\mathbf{x}_i^\top$ to represent the codeword according to the tradition). It is also easy to see that user $i$ sends $s_i\mathbf{x}_i^\top$ on the channel. The channel feedback is $\mathbf{y} = \bigvee_{i=1}^N s_i\mathbf{x}_i \triangleq [\bigvee_{i=1}^N s_i x_{i,t}]_{t=1}^T$. Then the

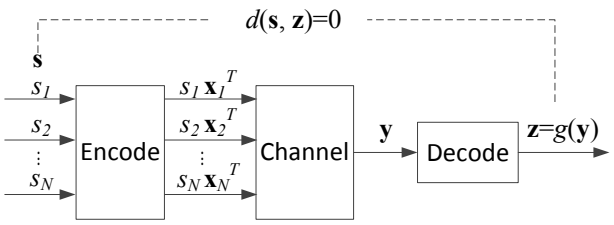


Fig. 2. Encoding-channel-decoding system with distortion criterion

decoded output is a partition[1] $\mathbf{z} \in \mathbb{Z}_{K;N}$, where:

$$\mathbb{Z}_{K;N} = \left\{ \mathbf{z} \in \mathcal{K}^N : \forall 1 \leq k \leq K, \exists z_i = k \right\}.$$

A *distortion function* is defined for any status vector $\mathbf{s} \in \mathbb{S}_{K;N}$ and a partition vector $\mathbf{z} \in \mathbb{Z}_{K;N}$ as follows:

$$d(\mathbf{s}, \mathbf{z}) = \begin{cases} 0, & \text{if } \forall i, j \in \mathcal{G}_{\mathbf{s}}, \quad (i \neq j) \Longrightarrow (z_i \neq z_j) \\ 1, & \text{otherwise} \end{cases}. \tag{1}$$

The objective is to design a proper matrix $\mathbf{X}$ and a corresponding decoding function $\mathbf{z} = g(\mathbf{y})$, so that $d(\mathbf{s}, g(\mathbf{y})) = 0$.

To simplify the notation, we write $\mathbf{y} = \mathbf{X}^\top \otimes \mathbf{s}$, where $\otimes$ denotes Boolean matrix multiplication in which the traditional arithmetic multiplication and addition operations are replaced by logical AND and OR, respectively. For any given $\mathbf{s}$, we denote the set of all possible desired $\mathbf{z}$ as $\mathbb{Z}_{K;N}(\mathbf{s}) = \{\mathbf{z} \in \mathbb{Z}_{K;N} : d(\mathbf{s}, \mathbf{z}) = 0\}$. The set of all possible vectors $\mathbf{s}$ that are compatible with a given $\mathbf{z}$ to produce 0 distortion is denoted by $\mathbb{S}_{K;N}(\mathbf{z}) = \{\mathbf{s} \in \mathbb{S}_{K;N} : d(\mathbf{s}, \mathbf{z}) = 0\}$. In some situations, we will need to know the number of users, $n_k$, in a given group $k \in \mathcal{K}$. The set of all possible $\mathbf{z}$ with group sizes $(n_1, \ldots, n_K)$, where $\sum_{k=1}^{K} n_k = N$, is denoted by:

$$\mathbb{Z}_{K;N}(n_1, \ldots, n_K) \triangleq \left\{ \mathbf{z} \in \mathbb{Z}_{K;N} : \left( \sum_{i=1}^{N} \mathbb{1}(z_i = k) \right) = n_k, 1 \leq k \leq K \right\},$$

here the indicator function $\mathbb{1}(A)$, which accepts a Boolean value $A$ as input, is 1 if $A$ is true, and 0 if $A$ is false.

[1]In the traditional view [25], a $K$ ordered partition of $\mathcal{N}$ is a $K$-tuple of subsets of $\mathcal{N}$, denoted by $(\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_K)$, where $\forall 1 \leq K_1 < K_2 \leq K$, $\mathcal{B}_{K_1} \neq \emptyset$, $\mathcal{B}_{K_1} \cap \mathcal{B}_{K_2} = \emptyset$ and $\bigcup_{k=1}^{K} \mathcal{B}_k = \mathcal{N}$. Our notation here is equivalent. For example, for a partition denoted by $\mathbf{z} = [3\ 1\ 1\ 2\ 2]^\top \in \mathbb{Z}_{3;5}$, it represents a partition $(\{2, 3\}, \{4, 5\}, \{1\})$.

### B. Performance Criteria

In this paper, we consider an average error. Assume each input $\mathbf{s} \in \mathbb{S}_{K;N}$ is with equal probability, i.e., $\mathbf{s} \sim \mathcal{U}(\mathbb{S}_{K;N})$, where $\mathcal{U}(\mathbb{A})$ means the uniform distribution in any set $\mathbb{A}$. Thus $\forall \tilde{\mathbf{s}} \in \mathbb{S}_K$, $p_{\mathbf{s}}(\tilde{\mathbf{s}}) \triangleq \Pr(\mathbf{s} = \tilde{\mathbf{s}}) = 1/\binom{N}{K}$. (For simplifying the notation, sometimes we will use $p_{\mathbf{s}}(\mathbf{s})$ instead of $p_{\mathbf{s}}(\tilde{\mathbf{s}})$, the subscript $\mathbf{s}$ is just used to describe the random vector, $\mathbf{s}$ in brackets is the outcome. We may also drop subscript $\mathbf{s}$ if it is clear). For a given $\mathbf{X}$, the average error probability is defined:

$$\begin{aligned} P_e^{(N)}(\mathbf{X}) &\triangleq \sum_{\mathbf{s}\in\mathbb{S}_{K;N}} p_{\mathbf{s}}(\mathbf{s}) \Pr(d(\mathbf{s}, g(\mathbf{y})) \neq 0 | \mathbf{s}, \mathbf{X}) \\ &= \frac{1}{\binom{N}{K}} \sum_{\mathbf{s}\in\mathbb{S}_{K;N}} \sum_{\mathbf{y}} \mathbb{1}(d(\mathbf{s}, g(\mathbf{y})) \neq 0) \mathbb{1}(\mathbf{y} = \mathbf{X}^\top \otimes \mathbf{s}) \end{aligned} \tag{2}$$

The first term $\mathbb{1}(d(\mathbf{s}, g(\mathbf{y})) \neq 0)$ reveals the effect of decoding, and the second term $\mathbb{1}(\mathbf{y} = \mathbf{X}^\top \otimes \mathbf{s})$ the effect of channel.

We define a number of slots $T_c^{(N)}$ to be achievable, if for any $T > T_c^{(N)}$, there exists a $N \times T$ matrix $\mathbf{X}^{(N)}$ and a decoding function $g^{(N)}(\cdot)$ for a given $N$, such that $\lim_{N\to\infty} P_e^{(N)}(\mathbf{X}^{(N)}) = 0$. The aim is to find $T_c^{(N)}$, when $N \to \infty$.

*Remark:* In group testing, the objective is to restore every user's state, i.e., the output should be $\mathbf{z}_g \in \mathbb{S}_{K;N}$, and correct restoration means $\mathbf{z}_g = \mathbf{s}$. Thus if by the definition of distortion

$$d_g(\mathbf{s}, \mathbf{z}_g) = \mathbb{1}(\mathbf{z}_g = \mathbf{s}), \tag{3}$$

the problem above is exactly a noiseless group testing problem. Thus the main difference between our partition problem and group testing problem lies in the different definitions of distortion functions, more importantly, lies in the different forms of information to transmit. Furthermore, since knowing $\mathcal{G}_{\mathbf{s}}$ will always induce a correct partition of $\mathcal{N}$ by distortion definition (1), the partition problem requires no more information transferred than that in the case of group testing. In the next section, we rigorously analyze the amount of the information used to solve the partition problem.

## IV. Source coding

In this section, we first focus on the inputs and outputs of the system without considering channel effects, i.e., a centralized source coding scheme illustrated as in Fig. 3, to find the amount of information needed for describing the source with the purpose of partition.

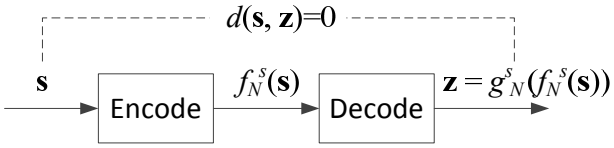


Fig. 3. Source coding part with distortion criterion

For group testing, the objective is to restore all states of users, if we use a *source codebook* $\mathcal{C}_g \triangleq \{\mathbf{s}_1, \ldots, \mathbf{s}_{L^{(N)}}\}$ to represent all $\mathbf{s} \in \mathbb{S}_{K;N}$, the size $L^{(N)}$ should be $|\mathbb{S}_{K;N}| = \binom{N}{K}$. However, in the partition reservation system, for a given $\mathbf{z} \in \mathbb{Z}_{K;N}$, there can be more than one $\mathbf{s}$ so that $d(\mathbf{s}, \mathbf{z}) = 0$. Actually when $\mathbf{z} \in \mathbb{Z}_{K;N}(n_1, \ldots, n_K)$, we have $|\mathbb{S}_{K;N}(\mathbf{z})| = \Pi_{k=1}^{K} n_k$. Thus, we can use codebook with size smaller than $\mathbb{S}_{K;N}$ to represent the inputs. Strictly speaking, for $\mathbf{s} \sim \mathcal{U}(\mathbb{S}_{K;N})$, if there exists a source encoding function:

$$f_N^s : \mathbb{S}_{K;N} \to \{1, 2, \ldots, L^{(N)}\},$$

and a source decoding function:

$$g_N^s : \{1, 2, \ldots, L^{(N)}\} \to \mathbb{Z}_{K;N},$$

so that we can map $\mathbf{s}$ to a decoding output $\mathbf{z} = g_N^s(f_N^s(\mathbf{s}))$, and the average source coding error:

$$P_e^{s,(N)} \triangleq \sum_{\mathbf{s} \in \mathbb{S}_{K;N}} p_{\mathbf{s}}(\mathbf{s}) \mathbb{1}(d(\mathbf{s}, g_N^s(f_N^s(\mathbf{s}))) = 0) \tag{4}$$

approaches 0 when $N \to \infty$, we will call $(L^{(N)}, f_N^s, g_N^s)$ an achievable source code sequence for the uniform source $\mathbf{s} \sim \mathcal{U}(\mathbb{S}_{K;N})$, the range of $g_N^s(\cdot)$ is defined as the source codebook. The minimum of $\log L^{(N)}$ for all achievable source code sequences will be called the partition information for $\mathbf{s} \sim \mathcal{U}(\mathbb{S}_{K;N})$. In this section, we first compute the minimum constrained mutual information $W_N^I$ in Lemma 1, and then prove the existence of an achievable source code sequence $(L^{(N)}, f_N^s, g_N^s)$ for those $L^{(N)} > 2^{W_N^I}$ in Theorem 1.

Constrained mutual information is always related to the rate distortion problem [26, 27]. Thus, we first calculate the constrained minimum mutual information for $\mathbf{s} \sim \mathcal{U}(\mathbb{S}_{K;N})$ and $\mathbf{z}$, i.e.,

$$W_N^I \triangleq \min_{p(\mathbf{z}|\mathbf{s}) \in \mathcal{P}_{z|s}} I(\mathbf{s}, \mathbf{z}) \tag{5}$$

where the constraint is:

$$\mathcal{P}_{z|s} \triangleq \{p(\mathbf{z}|\mathbf{s}) : p(\mathbf{z}|\mathbf{s}) = 0, \text{if } d(\mathbf{s},\mathbf{z}) = 0\}, \tag{6}$$

which means wrong partition $\mathbf{z}$ cannot be chosen for given $\mathbf{s}$. The result is the same as that by Hajak[3].

*Lemma 1:*

$$W_N^I \triangleq \min_{p(\mathbf{z}|\mathbf{s})\in\mathcal{P}_{z|s}} I(\mathbf{s},\mathbf{z}) = \log \frac{\binom{N}{K}}{\prod_{k=1}^{K} n_k^*} \tag{7}$$

*where*

$$(n_1^*,\ldots,n_K^*) = \arg\max_{n_k} \prod_{k=1}^{K} n_k,$$

$$\textit{subject to } \sum_{k=1}^{K} n_k = N, \textit{ and } \forall k \in \mathcal{K}, n_k \geq 1. \tag{8}$$

*$W_N^I$ can be achieved by choosing*

$$\mathbf{z}|\mathbf{s} \sim \mathcal{U}\left(\mathbb{Z}_{K;N}(n_1^*,\ldots,n_K^*) \bigcap \mathbb{Z}_{K;N}(\mathbf{s})\right). \tag{9}$$

Eq. (9) means for any given $\mathbf{s}$, $\mathbf{z}$ should be chosen from the "correct" set $\mathbb{Z}_{K;N}(\mathbf{s})$ since the constraint $\mathcal{P}_{z|s}$, also we require that $\mathbf{z} \in \mathbb{Z}_{K;N}(n_1^*,\ldots,n_K^*)$ to minimize the mutual information, which means there are $n_k^*$ users assigned to the group $k$. The partition $\mathbf{z}$ can be chosen uniformly from the set satisfying these two conditions. The proof is in Appendix A, in which we first partition $\mathbb{Z}_{K;N}$ to $\bigcup_{(n_1,\ldots,n_K)} \mathbb{Z}_{K;N}(n_1,\ldots,n_K)$, and then for each set of partitions, log sum inequality is used to obtain the lower bound. For the achievability, a direct construction of the optimal $p(\mathbf{z}|\mathbf{s})$ is introduced by (9). Denote $L^{(N)}$ as the size of a codebook, we have

*Theorem 1 (Source coding): There exists a codebook $\{\mathbf{z}_\ell\}_{\ell=1}^{L^{(N)}}$ of size $L^{(N)}$, and a source coding sequence $(L^{(N)}, f_N^s, g_N^s)$, so that for all $N$, the average source decoding error probability is bounded by:*

$$P_e^{s,(N)} \leq e^{-2^{\left(\log L^{(N)} - W_N^I\right)}}$$

*Thus, when $\log L^{(N)} > W_N^I$ and $\log L^{(N)} - W_N^I \overset{N\to\infty}{\longrightarrow} \infty$, sequence $(L^{(N)}, f_N^s, g_N^s)$ is achievable.*

The proof is in Appendix B. The core of the proof is to use random coding method to construct the codebook $\{\mathbf{z}_\ell\}_{\ell=1}^{L^{(N)}}$, in particular, choose $\mathbf{z}_\ell$ i.i.d. from $\mathcal{U}\left(\mathbb{Z}_{K;N}(n_1^*,\ldots,n_K^*)\right)$, and show the

average of $P_e^{s,(N)}$ over all possible codebooks satisfying the bound in Theorem 1, thus there must exists at least one codebook satisfying this bound. Then by assigning the source encoding function $f_N^s(\mathbf{s}) = \arg\min_{1\le\ell\le L^{(N)}} d(\mathbf{s}, \mathbf{z}_\ell)$, and the source decoding function $g_N^s(\ell) = \mathbf{z}_\ell$, we will obtain the source coding sequence $(L^{(N)}, f_N^s, g_N^s)$ with the error probability bounded by Theorem 1.

From Theorem 1, we can see $W_N^I$ can be used to measure the amount of asymptotic partition information of the source. And it explicitly shows the partition information, as well as its difference from the required information to restore all states in further remarks.

*Remark 1:* For group testing, if we define $W_{G,N}^I$ as that in (1), obviously we have:

$$W_{G,N}^I = \log \binom{N}{K} \tag{10}$$

Thus $W_N^I = \log \binom{N}{K} - \log \left(\prod_{k=1}^K n_k^*\right)$ of partition problem is smaller by a factor $\log \left(\prod_{k=1}^K n_k^*\right)$ than that of group testing. We next remark on the effect of the order of $K$ as compared with $N$ on the achieved mutual information, as well as the error probability.

*Remark 2:* First, let's show the explicit expression of $W_N^I$. From restriction of $[n_k]_{k=1}^K$ in (8), it is easy to see without requiring $n_k$ to be a integer, then the optimal values of $n_k$ are

$$n_1^* = n_2^* = \ldots = n_K^* = \frac{N}{K}.$$

Thus

$$W_N^I \ge \log \binom{N}{K} - \log \left(\frac{N}{K}\right)^K \tag{11}$$

The equality is achieved when $K$ divides $N$, and it is a good approximation when $N \gg K$. Also, we have the inequalities:

$$\frac{\binom{N}{K}}{\left(\frac{N}{K}\right)^K} \overset{(a)}{\le} \frac{K^K}{K!} \overset{(b)}{\le} e^K, \tag{12}$$

Equality of $(a)$ will be approximately achieved when $K \ll N$, and the equality of $(b)$ requires $1 \ll K \ll N$.

*Remark 3:* When $K = O(N)$, e.g. $K = \eta N$ and $0 < \eta < 1$ is a constant, we have:

$$\lim_{N\to\infty} \frac{1}{N} W_N^I = -(1-\eta)\log(1-\eta) \tag{13}$$

$$\lim_{N\to\infty} \frac{1}{N} W_{G,N}^I = H(\eta) \triangleq -\eta\log\eta - (1-\eta)\log(1-\eta) \tag{14}$$

They are obtained by a tight bound of $\binom{N}{K}$ derived by Wozencraft and Reiffen, see in Section 17.5 in [26]. Thus we can define an achievable source information rate $R_s$ for the partition problem (note the unit of the rate defined here is bits/user), so that for any $R \geq R_s + \xi$, where $\xi > 0$ is any constant, there exists an achievable coding sequence $(L^{(N)} = 2^{NR}, f_N^s, g_N^s)$, and

$$P_e^{s,(N)} \to 0, \text{ when } N \to \infty \tag{15}$$

By Theorem 1 and Eq. (13), we can see that $R_s = \lim_{N\to\infty} \frac{1}{N} W_N^I$, when $K = \eta N$, since we can always construct the achievable coding sequence of $L^{(N)} = 2^{NR}$ that for all $\xi > 0$, and $\forall R \geq R_s + \xi$,

$$P_e^{s,(N)} \leq e^{-2^{N(R-R_s)}} \to 0 \tag{16}$$

Note that the error is doubly exponential. While for group testing, if we define $R_s^g$ similarly to $R_s$, we can see by (13) and (14) that $R_s^g = \lim_{N\to\infty} \frac{1}{N} W_{G,N}^I = R_s + (-\eta \log \eta) > R_s$. Thus, we need higher rate to represent the states of users than to partition them.

*Remark 4:* When $K = o(N)$, e.g. $K$ is a constant, $\lim_{N\to\infty} W_N^I = \log \frac{K^K}{K!}$ is also a constant. we can see the proposed achievable rate $R_s = 0$ by (12), i.e., $\frac{1}{N} W_N^I \leq \frac{K}{N} \log e \to 0$. By Theorem 1, for any $L^{(N)} = f(N)$, where $f(N)$ is a function satisfying $f(N) \overset{N\to\infty}{\longrightarrow} \infty$, we can always construct a source coding sequence with codebook size $L^{(N)} = f(N)$, and

$$P_e^{s,(N)} \leq e^{-2^{\left(\log f(N) - \log \frac{K^K}{K!}\right)}} \to 0, \text{ when } N \to \infty \tag{17}$$

It can be seen that we can choose $L^{(N)}$ to be of any order of $N$ to guarantee the convergence of $P_e^{s,(N)}$, e.g., $L^{(N)} = \log \log N$. While for group testing, we should always need $L^{(N)} = \binom{N}{K}$ to represent the source, which can be much larger than that of partition problem. However, different choices of $f(N)$ will influence the speed of convergence, e.g., if an exponential convergence speed is required, i.e., $P_e^{s,(N)} \leq e^{-\Delta N}$ for some $\Delta > 0$, there should be $L^{(N)} = O(N)$.

## V. The brute force method

Based on centralized source coding, a coding scheme, the brute force method uses the general centralized source coding to design $\mathbf{X}$, then the decoder checks each possible source codeword exhaustedly with the help of Boolean channel.

For a given $L^{(N)}$, we can find a source codebook $\{\mathbf{z}_\ell\}_{\ell=1}^{L^{(N)}}$ to represent the source under error probability $P_e^{s,(N)}$ by Theorem 1. Thus if a matrix $\mathbf{X}$ is designed to check whether $\mathbf{z}_\ell$ is the

correct output one by one, the average error probability $P_e^{(N)}$ will behave the same as $P_e^{s,(N)}$, and thus approaches zero when $\log L^{(N)} > W_N^I$ and $\log L^{(N)} - W_N^I \to \infty$. This is a brute force method, as further described in detail below:

1) Source coding: For $L^{(N)}$, choose the codebook $\{\mathbf{z}_\ell\}_{\ell=1}^{L^{(N)}}$, and the source coding sequence $(L^{(N)}, f_N^s, g_N^s)$ based on Theorem 1.
2) Joint coding: Generate $\mathbf{X}$ by $L$ submatrices of dimension $N \times K$,

$$\mathbf{X} = [\mathbf{X}_1, \ldots, \mathbf{X}_{L^{(N)}}].$$

Thus the dimension of $\mathbf{X}$ is $N \times T$, where $T = KL^{(N)}$. Each $\mathbf{X}_\ell$ is a $N \times K$ matrix, so that $\forall 1 \le i \le N,\ 1 \le k \le K$, the $(i,k)$-th element of $\mathbf{X}_\ell$ satisfies:

$$x_{\ell;i,k} = \begin{cases} 1, & z_{\ell;i} = k; \\ 0, & \text{otherwise} \end{cases}.$$

See Fig. 4 for an example.
3) Decoding: Now the outputs is separated into $L^{(N)}$ parts:

$$\mathbf{y} = [\mathbf{y}_1; \ldots; \mathbf{y}_{L^{(N)}}],$$

and

$$\mathbf{y}_\ell = \mathbf{X}_\ell^\top \otimes \mathbf{s}$$

is a $K \times 1$ column vector. If there exists $\mathbf{y}_\ell = \mathbf{1}_{K\times 1}$, where $\mathbf{1}_{K\times 1}$ is a $K \times 1$ column vector with all components equal to 1, then the joint decoder is $g(\mathbf{y}) = \mathbf{z}_\ell$; if there exist more than one, we can select one of them, e.g., the first one; otherwise there is decoding error.

Note that if $\mathbf{y}_\ell = \mathbf{1}_{K\times 1}$, then there exists at least one active user in each of $k$ groups assigned by $\mathbf{z}_\ell$. And since we know there are exactly $K$ active users, only one active user is assigned in each group. Then definitely $d(\mathbf{s}, \mathbf{z}_\ell) = 0$, i.e., it is based on the following fact:

$$\forall i \ne j \in \mathcal{G}_\mathbf{s}, z_i \ne z_j \iff \bigcup_{i\in\mathcal{G}_\mathbf{s}} \{z_i\} = \mathcal{K}.$$

Obviously in the brute force method the number of channel uses $T^{BF} = KL^{(N)}$. In addition, since in this method if there exists $\mathbf{z}_\ell$ in codebook $\{\mathbf{z}_\ell\}_{\ell=1}^{L^{(N)}}$ so that $d(\mathbf{s}, \mathbf{z}_\ell) = 0$, then definitely

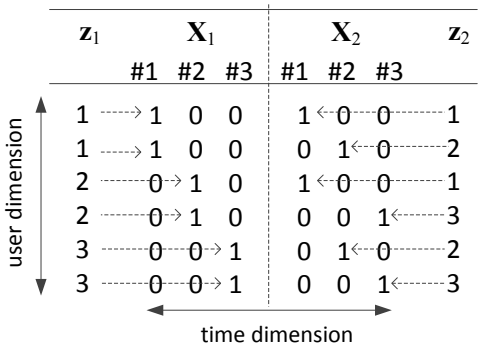


Fig. 4. Example of the generation of $\mathbf{X}$ in brute force method, where $N = 6$, $K = 3$, and source codebook of size $L^{(N)} = 2$ is chosen.

$d(\mathbf{s}, g(\mathbf{y})) = 0$, the average error of the brute force method is the same as centralized source coding. Then based on the analysis of centralized source coding as in Theorem 1, we have

*Theorem 2 (Brute force method): For the brute force method, if the size of centralized source codebook is* $L^{(N)}$, then

$$T_{BF} = KL^{(N)},$$

*and the average error probability is*

$$P_e^{(N)} \leq e^{-\left(\frac{T_{BF}}{K}\middle/ 2^{W_N^I}\right)} = e^{-2^{\left(\log L^{(N)} - W_N^I\right)}}$$

Although the brute force method is very simple and obviously not optimal, it highlights some features of the partition problem. First, if $K$ is a fixed number, then as stated in Remark 4 in the last section, only $T^{BF} = \frac{K^{K+1}}{K!} f(N)$ is needed for the convergence of $P_e^{(N)}$(since $P_e^{(N)} \leq e^{-f(N)}$), where $\frac{K^{K+1}}{K!}$ is a constant and $f(N)$ is any function satisfying $\lim_{N\to\infty} f(N) = \infty$. In this case, the threshold effect of the convergence doesn't exist as that in group testing or compressive sensing [6], and the choice of $f(N)$ is related to the speed of convergence of $P_e^{(N)}$. However, when $K$ is large, e.g. when $1 \ll K \ll N$, $2^{W_N^I} \to e^K$, $T^{BF}$ should be larger than $Ke^K$ to guarantee the convergence of $P_e^{(N)}$, which may be even larger than the time needed for group testing $T_G = O(K \log N)$. It is expected since the brute force method is not optimal. In particular, when $K$ increases, the size of centralized source codebook increases fast, and it becomes so inefficient to check them one by one.

## VI. Random coding and Reformulation as Hypergraph

The brute force method was inspired by a centralized source coding and it works well only for small $K$. To find the achievable bound of $T$ for general case, we design the code from another way by randomly generating $\mathbf{X}$ first and then employing MAP decoding. However, to have a more amiable approach to derive an achievable rate, and to provide more insights on the internal structure of the problem in depth, a new angle from graph theory is proposed in this section, which transforms the effect of channel to a series of operations on hypergraphs. It is shown that seeking an acceptable partition is equivalent to obtaining a common strong colorable hypergraph by all users, and then coloring this hypergraph. Because we are only concerned about an achievable rate, the computational cost associated with the coloring is not counted in our framework.

### *A. Random coding and MAP decoding*

Random coding is frequently used in the proof of achievability in information theory, and has been proven useful for group testing [24]. The binary matrix $\mathbf{X}$ is generated randomly, where each element $x_{i,t} \sim \mathcal{B}(p)$ follows the i.i.d Bernoulli distribution with $p$ parameter (other distributions of $\mathbf{X}$ can also be considered, but that is out of scope of this paper). The probability of $\mathbf{X}$ is denoted by $Q(\mathbf{X})$. Then the average probability of error over the realization of $\mathbf{X}$ is given by:

$$\begin{aligned} P_e^{(N)} &= \sum_{\mathbf{X}} Q(\mathbf{X}) P_e^{(N)}(\mathbf{X}) \\ &= \sum_{\mathbf{X}} Q(\mathbf{X}) \sum_{\mathbf{s}\in\mathbb{S}_{K;N}} \sum_{\mathbf{y}} p_{\mathbf{s}}(\mathbf{s}) p_{y|s;X}(\mathbf{y}|\mathbf{s}) \mathbb{1}(d(\mathbf{s}, g(\mathbf{y})) \neq 0) \\ &\overset{(a)}{=} \sum_{\mathbf{X}} Q(\mathbf{X}) \sum_{\mathbf{y}} p_{y|s;X}(\mathbf{y}|\mathbf{s}_0) \mathbb{1}(d(\mathbf{s}_0, g(\mathbf{y})) \neq 0) \end{aligned} \tag{18}$$

Since we don't consider observation noise in this paper,

$$p_{y|s;X}(\mathbf{y}|\mathbf{s}) = \mathbb{1}\left(\mathbf{y} = \mathbf{X} \otimes \mathbf{s}\right),$$

and equality of $(a)$ above follows from the symmetry of the generation of $\mathbf{X}$, so we can choose any particular $\mathbf{s}_0$ as input to analyze. We will choose $\mathcal{G}_{\mathbf{s}_0} = \{1, 2\}$ in the rest of the paper. Since the derived achievable $T_c^{(N)}$ for random coding is of order $\log N$, we define an achievable rate

$S_c$, so that for any $T$ satisfying $\frac{\log(N)}{T} \leq S_c - \xi$, where $\xi > 0$ is an arbitrary constant, we have $P_e^{(N)} \overset{N\to\infty}{\longrightarrow} 0$. Which also implies there exists a $X^*$ such that $P_e^{(N)}(\mathbf{X}^*) \overset{N\to\infty}{\longrightarrow} 0$. In this section, we will derive such a $S_c$.

The optimal decoding method is MAP decoding, i.e., given feedback $\mathbf{y}$, choose $\mathbf{z}^* = g(\mathbf{y})$ so that $\forall \mathbf{z} \neq \mathbf{z}^* \in \mathbb{Z}_{K;N}$, the following holds

$$p_{z|y;X}(\mathbf{z}^*|\mathbf{y}) \geq p_{z|y;X}(\mathbf{z}|\mathbf{y}),$$

which is equivalent to

$$\sum_{\mathbf{s}\in\mathbb{S}_{K;N}} \mathbb{1}\left(d(\mathbf{s},\mathbf{z}^*)=0\right) p_{y|s;X}(\mathbf{y}|\mathbf{s}) \geq \sum_{\mathbf{s}\in\mathbb{S}_{K;N}} \mathbb{1}\left(d(\mathbf{s},\mathbf{z})=0\right) p_{y|s;X}(\mathbf{y}|\mathbf{s}) \tag{19}$$

If there is more than one $\mathbf{z}^*$ with the maximum value, choose any one. Note that here we search all possible $\mathbf{z}^*$ in all possible $\mathbf{z} \in \mathbb{Z}_{K;N}$; however, considering the source coding results, we can just search $\mathbf{z}^* \in \mathbb{Z}_{K;N}(n_1^*, \ldots, n_K^*)$ without loss of generality.

As seen in the definition of MAP decoding, to find MAP of $\mathbf{z}$, we should count all $\mathbf{s} \in \mathbb{S}(\mathbf{z})$ satisfying $\mathbf{y} = \mathbf{X} \otimes \mathbf{s}$. While many $\mathbf{s} \in \mathbb{S}(\mathbf{z})$ has common active users, so $\mathbb{1}(\mathbf{y} = \mathbf{X} \otimes \mathbf{s})$ are correlated for different $\mathbf{s}$ sharing parts of common active users. Thus, it is extremely difficult to compare the posterior probability of different $\mathbf{z}$. The obstacle arises because in MAP decoding, few inherent structures of the problem are found and utilized. To further reveal this inherent problem structure, a novel formulation from the perspective of hypergraph is proposed in the next section, which proves to be helpful in reducing complexity of performance analysis.

### *B. Reformulation as Hypergraph*

The process of random coding can be illustrated in the upper part of Fig. 5. For an input $\mathbf{s}_0$, the channel output $\mathbf{y} = \bigvee_{i\in\mathcal{G}_{\mathbf{s}_0}} \mathbf{x}_i$ is observed, and then a candidate subset of $\mathbb{S}_{K;N}$ that is capable of generating $\mathbf{y}$ can be inferred:

$$\mathbb{S}_{\mathbf{y}} = \{\mathbf{s} \in \mathbb{S}_{K;N} : \mathbf{y} = \mathbf{X} \otimes \mathbf{s}\}$$

MAP decoder tries to find $\mathbf{z}^*$ such that there is the largest number of $\mathbf{s} \in \mathbb{S}_{\mathbf{y}}$ satisfying $d(\mathbf{z}^*, \mathbf{s}) = 0$.

This process can be illustrated from the perspective of hypergraphs, as shown in Fig. 5.

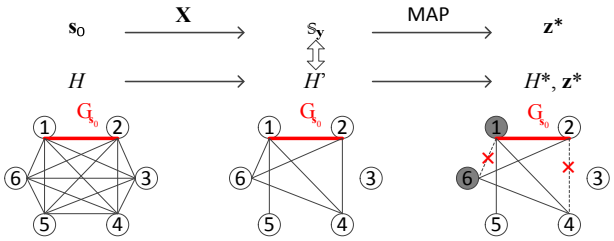


Fig. 5. Reformulation from hypergraph

1) Source: Since all real sources $\mathbf{s}_0 \in \mathbb{S}_{K;N}$ are equiprobable, a complete $K$-uniform hypergraph $H(V(H), E(H))$ can be used to express the knowledge of the source before observation, where the set of nodes $V(H) = \mathcal{N}$ represents $N$ users, and the set of hyper-edges $E(H) = \{e \subseteq V(H) : |e| = K\}$ represents all possible inputs [28, 29]. It means every hyper-edge in $H$ could be $\mathbf{s}_0$. Actually the real input is just an edge $\mathcal{G}_{\mathbf{s}_0} \in E(H)$, the objective of group testing is to find exactly this edge to obtain every user's state; while for partition reservation system, the objective is to separate each vertex of $\mathcal{G}_{\mathbf{s}_0}$.
2) Transmission and observation: the transmission and corresponding observation can be seen as a series of edge deleting operations on the hypergraphs. Because after observing each feedback $y_t$, $1 \leq t \leq T$, some $\mathbf{s}$ could be determined to be not possible, and the candidate set $\mathbb{S}_{\mathbf{y}}$ could shrink. A sub-hypergraph $H'(V(H'), E(H')) \subseteq H(V(H), E(H))$ is used to denote the candidate set $\mathbb{S}_{\mathbf{y}}$ after observing the feedback $\mathbf{y}$. Note that we consider the node set $V(H') = V(H)$ to be invariant, but actually there will be many isolated nodes in $V(H')$ with zero degree. The details of the operations will be shown in next subsection. Note that for the considered noiseless case, we always have $\mathbf{s}_0 \in \mathbb{S}_{\mathbf{y}}$, so $\mathcal{G}_{\mathbf{s}_0} \in H'$.
3) Partition: Finally, the partition $\mathbf{z}^*$ should be decided by observing $H'$. First, we introduce the concept of strong coloring. A strong coloring of a hypergraph $H$ is a map $\Psi : V(H) \to \mathbb{N}^+$, such that for any vertices $u, v \in e$ for some $e \in E(H)$, $\Psi(u) \neq \Psi(v)$. The value of $\Psi(u)$ is called the color of node $u$. In other words, all vertices of any edge should have different colors.The corresponding strong chromatic number $\chi_s(H)$ is the least number of colors so that $H$ has a proper strong coloring [30]. Obviously for a $K$-uniform hypergraph, $\chi_s(H) \geq K$. We called a strong coloring with $K$ colors to be $K$-strong coloring. If $z_i^*$ is viewed as a color of node $i$, actually $\mathbf{z}^* \in \mathbb{Z}_{K;N}$ gives a coloring mapping of $V(H)$ with

$K$ colors.

For MAP decoding in (19), the method of finding $\mathbf{z}^*$ from $\mathbb{S}_{\mathbf{y}}$ is equivalent to finding a hypergraph $H^*(V(H^*), E(H^*)) \subseteq H'(V(H), E(H'))$, such that $\chi_s(H^*) = K$, i.e., $H^*$ is $K$-strong colorable, and the number of deleted edges $|E(H') \setminus E(H^*)|$ is minimum. Then the output $\mathbf{z}^*$ can be any strong coloring of $H^*$.

From the prospective of hypergraph, the process can be represented as $H \to H' \to (H^*, \mathbf{z}^*)$, corresponding to the expression from vectors $\mathbf{s}_0 \to \mathbb{S}_{\mathbf{y}} \to \mathbf{z}^*$. The process is shown in Fig. 5 through an example of $N = 6$, $K = 2$. Note that the hypergraph becomes a graph when $K = 2$. Compared with group testing, whose objective is to obtain $H^* = H'$ with only one edge $\mathcal{G}_{\mathbf{s}_0}$ by deleting edges through transmissions and observations, our partition problem allows $H'$ and $H^*$ to have more edges, so less effort is needed to delete edges, which is translated to higher achievable rate than that of the group testing problem. We can see $\mathbf{z}^*$ is correct iff $\mathcal{G}_{\mathbf{s}_0} \in E(H^*)$ and $H^*$ is $K$-strong colorable, we will use this equivalent condition to judge if the decoding is correct in the analysis. From the view of algorithm, the real process is that all users obtain a common $H^*$ first, and need to choose a common consistent $\mathbf{z}^*$. The computational complexity of $K$-strong coloring of a hypergraph [30] doesn't influence the amount of time used to arrive at a hypergraph $H^*$ that is strong colorable. A better understanding of deleting edges operations is introduced in the next subsection.

### *C. Effect of* $\mathbf{X}$ *on Hypergraph*

The effect of transmissions and observation using matrix $\mathbf{X}$ can be summarized in two operations: deleting vertex and deleting clique. Assume at time $t$, the set of active users transmitting 1 is:

$$\mathcal{G}_{\mathbf{X}}(t) = \{i \in \mathcal{N} : x_{i,t} = 1\}. \tag{20}$$

The operation at time $t$ can be classified based on the feedback $y_t$:

1) If $y_t = 0$, which means any users in $\mathcal{G}_{\mathbf{X}}(t)$ should not be active users, so these vertices should be deleted, i.e., all edges containing these vertices should be deleted.
2) If $y_t = 1$, which means at least one active user is transmitting 1 at time $t$, so any edge completely generated by vertices in $\mathcal{N} \setminus \mathcal{G}_{\mathbf{X}}(t)$ should be deleted. Otherwise if these edges

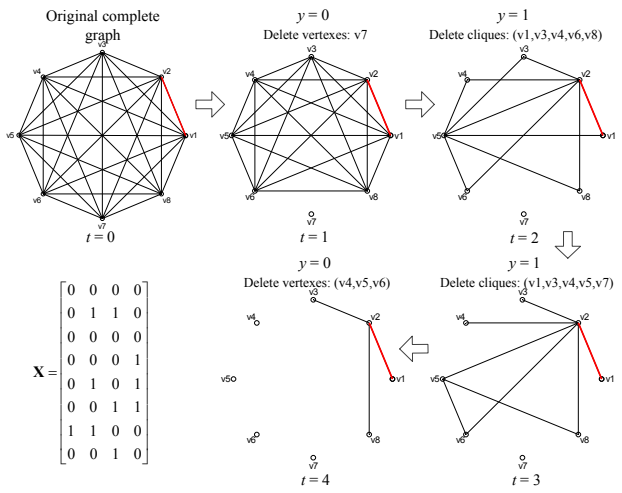


Fig. 6. Example of $\mathbf{X}$ effects on the operations of a graph. (Here $N = 8$, $K = 2$, $T = 4$, and $\mathcal{G}_{\mathbf{s}_0} = \{1, 2\}$)

are actually the $\mathcal{G}_{\mathbf{s}_0}$, there will be no active users in $\mathcal{G}_{\mathbf{X}}(t)$ and $y_t = 0$. In fact, it is equivalent to deleting all $K$ uniform hyper-cliques generated by $\mathcal{N} \setminus \mathcal{G}_{\mathbf{X}}(t)$.

The two effects are illustrated by an example in Fig. 6 using a graph with sequence of nodes removed and clique removing operations. There are $8$ users and $4$ slots are used for transmission. We can see the edges removing process starting from a complete hypergraph at $t = 0$, to a graph of only 3 edges at time $t = 4$. At $t = 1, 4$, $y_t = 0$, the corresponding vertices are removed, while at time $t = 2, 3$ cliques are removed.

Now it is clear that the original problem can be approached by hypergraph $K$-strong coloring and operations designing. In next section, a special case of $K = 2$ is solved. As will be seen, even in this simple case, it is shown how nontrivially the proposed graph operation based approach works, which further provides the insight of the partition problem.

## VII. Random coding of $K = 2$

For $K = 2$, two sub-optimal decoding methods inspired by MAP decoding are proposed to further simplify the calculation.

### A. Two simplified decoding methods

In MAP decoding, the decoder will find a $K$-strong colorable graph $H^*$ from $H'$ by deleting the minimum number of edges, and the decoding result is correct if $\mathcal{G}_{\mathbf{s}_0} \in H^*$. For $K = 2$,

hypergraph $H^*$ being 2-strong colorable is equivalent to $H^*$ being bipartite, or equivalently, not having *no odd cycles*. Further, assume $\mathcal{G}_{\mathbf{s}_0} = \{1, 2\}$, odd cycles can be classified into three kinds:

1) Containing a cycle with vertices 1 and 2, the cycle may or may not containing edge (1,2);
2) Containing one of the vertices 1 and 2;
3) Containing neither vertex 1 or 2.

Denote the odd cycles containing edge $(1, 2)$ by "1-odd cycles". Since $(1, 2)$ always exists in $H'$ due to the noiseless channel, it is easy to see $H'$ contains no first kind of cycles iff $H'$ contains no 1-odd cycles. Thus in the rest of paper, we just consider the existence of 1-odd cycles and the other two kinds of odd cycles (sometimes for simplification of notation, we also call 1-odd cycle *the type-1 odd cycle*). We can assert that if there is no 1-odd cycles in $H'$, the decoding result will be surely correct. The reason is that for MAP decoding, it breaks all odd cycles in $H'$ to get $H^*$ by deleting least edges. If there is no 1-odd cycle in $H'$, set $\mathcal{G}_{\mathbf{s}_0}$ will not be deleted during this process. Thus, $\mathcal{G}_{\mathbf{s}_0} \in H^*$, which implies the correct decoding. Thus, we have

$$P_e^{(N)} \leq P_e^{1-odd} \triangleq \sum_{\mathbf{X}} Q(\mathbf{X}) \Pr(H' \text{ contains 1-odd cycles} | \mathbf{X}, \mathbf{s}_0) \tag{21}$$

$$\leq P_e^{odd} \triangleq \sum_{\mathbf{X}} Q(\mathbf{X}) \Pr(H' \text{ contains odd cycles} | \mathbf{X}, \mathbf{s}_0) \tag{22}$$

In the following, $P_e^{odd}$ and $P_e^{1-odd}$ are both determined, and it is shown they are nearly the same when $N \to \infty$, which points to the possibility of using a suboptimal decoding to advantage: when $H'$ is 2-colorable, find any $\mathbf{z}$ consistent with it; otherwise announce an error. The reason is if MAP coding is used, it is necessary to obtain $H^*$ by deleting minimum edges of $H'$, which is a NP hard problem[31]; however, it is easy to judge whether $H'$ is a bipartite graph in linear steps of $N$. So while the suboptimal decoding method needs more channel use, it is easier to compute.

### *B. Main result: Achievable bound of $T$ for $K = 2$ case*

To upperbound $P_e^{(N)}$ by $P_e^{1-odd}$, denote:

$$C(p) = -(1 - (1 - p)^2) \log \varphi(p) - (1 - p)^2 \log(1 - p) \tag{23}$$

where

$$\varphi(p) = \frac{p + \sqrt{4p - 3p^2}}{2}. \tag{24}$$

We have the following lemma:

*Lemma 2: For $K = 2$ case, if for any constant $\xi > 0$ such that $\frac{\log N}{T} \leq S_c - \xi$, and $S_c \triangleq \max_{0 \leq p \leq 1} C(p)$, we have $P_e^{(N)} \leq P_e^{1-odd} \xrightarrow{N \to \infty} 0$.*

And similarly, by bounding $P_e^{(N)}$ by $P_e^{odd}$, we have the following theorem:

*Theorem 3: For random coding scheme, for any constant $\xi > 0$ that $\frac{\log N}{T} \leq S_c - \xi$, we will have $P_e^{(N)} \leq P_e^{odd} \xrightarrow{N \to \infty} 0$.*

The proofs of Lemma 2 and Theorem 3 are given in Appendix C. Actually if the elements of $\mathbf{X}$ are generated i.i.d. by Bernoulli distribution of parameter $p$, we will have $P_e^{1-odd}$ and $P_e^{odd}$ approaches 0 if $\frac{\log N}{T} \leq C(p) - \xi$, thus $S_c = \max_p C(p)$. We can see the achievable bounds are both $S_c$ for two methods to make $P_e^{(N)} \to 0$. The main idea in the proof is to calculate the probability of existence of a particular odd cycle in $H'$, and the calculation is similar for all three kinds of odd cycles. As a key factor in the result, $\varphi(p)$ in (24) is actually a factor of the solution of the extended Fibonacci numbers, which reveals some interesting structure in the partition problem.

A sketch of the proof of Lemma 2 is given as below, it is the same for Theorem 3:

1) Consider the problem conditioning on $[\mathbf{x}_1, \mathbf{x}_2]$ in a strong typical set $\mathcal{A}_\epsilon^{(T)}$; this will make the algebra easier. Assume the probability of existence of a particular 1-odd cycle of $M$ vertices in $H'$ to be $P_{e;M}$; there are $\binom{N-2}{M-2}(M-2)! \leq N^{M-2}$ such odd cycles and all of them are equiprobable. Thus,

$$P_e^{1-odd} \leq \sum_{M \geq 3, M \text{ is odd}} 2^{(M-2)\log N} P_{e;M} + \Pr([\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) \tag{25}$$

Since $\Pr([\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) \leq 2^{-q(p,\epsilon)T} \xrightarrow{T \to \infty} 0$, where $q(p, \epsilon)$ is some constant, according to the properties of strong typical set[32]. We will show that $P_{e;M} \leq 2^{-(M-2)C(p)T}$. Thus when $\log N < (C(p) - \xi)T$, $2^{(M-2)\log N} \times P_{e;M} \leq 2^{-(M-2)\xi}$, which means the $P_e^{1-odd} \to 0$. Note that we can also see the $P_e^{1-odd}$ goes to 0 with an exponential speed with $T$, and thus, polynomial speed with $N$, i.e., $P_e^{1-odd} \leq 2^{-\Delta_1 T} = \frac{1}{N^{\Delta_2}}$, where $\Delta_1$ and $\Delta_2$ are constant.

2) Divide $T$ slots into four parts $\mathcal{T}_{u,v} = \{t : (x_{1,t}, x_{2,t}) = (u, v)\}$, for four different $(u, v) \in \{0, 1\}^2$, according to the codewords of the real input $[\mathbf{x}_1, \mathbf{x}_2]$. In the strong typical set, we just need to consider when $|\mathcal{T}_{u,v}| \approx p_x(u)p_x(v)T$, where $p_x(u) \triangleq p\mathbb{1}(u = 1) + (1 - p)\mathbb{1}(u = 0)$ is the probability distribution of Bernoulli variable. And due to symmetry and

independence of the generation of $\mathbf{X}$, for any $(u, v)$, we just need to consider any slot $t$ $\mathcal{T}_{u,v}$.

3) At $t \in \mathcal{T}_{u,v}$, denote $\mu_{u,v;M}$ to be the probability that the considered 1-odd cycle of length $M$ won't be deleted by the operations, then

$$P_{e;M} = \Pi_{u,v} \left(\mu_{u,v;M}\right)^{|\mathcal{T}_{u,v}|} \approx \Pi_{u,v} \left(\mu_{u,v;M}\right)^{p_x(u)p_x(v)T} \tag{26}$$

4) We have shown that for all $t$ where $y_t = 0$, i.e., $t \in \bigcup_{(u,v)\neq(0,0)} \mathcal{T}_{u,v}$, $\mu_{u,v;M} = (1-p)^{M-2}$, and the exponent $p_x(0)p_x(0) = (1-p)^2$, thus

$$\left(\mu_{0,0;M}\right)^{p_x(0)p_x(0)T} = (1-p)^{(M-2)(1-p)^2 T} = 2^{(M-2)T(1-p)^2 \log(1-p)} \tag{27}$$

While for $y_t = 1$, i.e., $t \in \mathcal{T}_{u,v}$, $(u, v) \neq (0, 0)$, we have shown $\mu_{u,v;M} = \varphi^{M-2}(p)$, and $\sum_{(u,v)\neq(0,0)} p_x(u)p_x(v) = 1 - (1-p)^2$. Thus,

$$\Pi_{(u,v)\neq 0} \left(\mu_{u,v;M}\right)^{p_x(u)p_x(v)T} = (1-p)^{(M-2)(1-(1-p)^2)T} = 2^{(M-2)T(1-(1-p))^2 \log \varphi(p)} \tag{28}$$

Then, combining (27) and (28), we obtain $P_{e;M} \leq 2^{-(M-2)C(p)T}$, which completes the proof.

We can provide an intuitive explanation. The result in Lemma 2 can be expressed as

$$\forall p,\ T > \frac{\log N^{M-2}}{(M-2)C(p)} \tag{29}$$

Intuitively the problem can be stated as that we have at most $N^{M-2}$ 1-odd cycles of length $M$, and after determining(or eliminating) all of them, the error probability becomes 0. Thus, $\log N^{M-2}$ can be seen as an upperbound on source information, which describes the uncertainty of 1-odd cycles; $(M-2)C(p)$ can be seen as the information transmitting rate of the channel, which represents the speed of eliminating the uncertainty of odd cycles with $M$ vertices.

To further explain the meaning of $(M-2)C(p)$, we should use the effect of $\mathbf{X}$ on hypergraph stated in Section VI-C. If a given 1-odd cycle $H_{e;M}$ of $M$ vertices exists in $H'$, in $1 \leq t \leq T$, none of the $M$ vertices, or the cliques containing the edges of $H_{e;M}$ can be deleted. See an example in Fig. 7, where $H_{e;M}$ is the outer boundary. It won't be removed if all the nodes are maintained; and the cliques to be deleted should not contain the consecutive vertices on the outer boundary.

Since at any test $t$, vertices are deleted if $y_t = 0$; the probability of this happening is $(1-p)^2$. For a particular $t$ when $y_t = 0$, the vertex of an inactive vertex $i$ is deleted only if $x_{i,t} = 1$, so the probability that all $M$ vertices are maintained at time $t$ is $\mu_{0,0;M} = (1-p)^{M-2}$.

On the other hand, all the edges of the odd cycle $H_{e;M}$ can't be deleted by the clique deleting operation. At any slot $t$ so that $y_t = 1$, whose probability is $1-(1-p)^2$, there are 3 different cases $(x_{1,t}, x_{2,t}) = (u, v), (u, v) \neq (0, 0)$, their analysis is similar, let us just consider $(x_{1,t}, x_{2,t}) = (1, 1)$. Assume $H_{e;M} = (1, 2, i_1, \ldots, i_{M-2})$, so at any slot $t$, the probability that $H_{e;M}$ is not removed by deleting cliques can be derived:

$$\begin{aligned}\mu_{1,1;M} =& 1 - \Pr(H_{e;M} \text{ is removed at slot } t | t \in \mathcal{T}_{1,1}) \\ =& 1 - \Pr(\exists w \in \{1, \ldots, M-3\}, (x_{i_w}(t), x_{i_{w+1}}(t)) = (0, 0)) \\ \overset{(a)}{=}& \frac{1}{p} F(M, p) \leq \varphi(p)^{M-2} \end{aligned} \tag{30}$$

The derivation of $(a)$ is seen in Appendix C, and

$$F(k, p) = \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k-1-j}{j} p^{k-1-j} (1-p)^j \tag{31}$$

$$= \frac{\varphi(p)^k - \psi(p)^k}{\varphi(p) - \psi(p)}, \tag{32}$$

$$\textit{where} \qquad \varphi(p) = \frac{p + \sqrt{4p - 3p^2}}{2}; \quad \psi(p) = \frac{p - \sqrt{4p - 3p^2}}{2} \tag{33}$$

is the solution of a generalized Fibonacci sequence [33]. Actually $\frac{1}{p} F(k+2, p)$ is the probability that there are no consecutive 0s in a $p$-Bernoulli sequence of length $k$. This feature of Fibonacci sequences has also been used in generating codes without consecutive 1s, known as Fibonacci coding. The other $\mu_{1,0;M}$ and $\mu_{0,1;M}$ can be derived similarly. Thus, we can see $(M-2)C(p)$ is well explained as the rate of deleting vertices or cliques for an 1-odd cycle with $M$ vertices from above.

Now it is clear that Lemma 1 and Theorem 2 above have revealed the internal structure of the partition problem. The partition information is related to odd cycles, and $\mathbf{X}$ is constructed to destroy the odd cycles by deleting vertices or cliques. The Fibonacci structure emerges since it is related to considering consecutive 0s in Bernoulli sequences, which may be a key factor in partition problem and could be extended to more general cases with $K > 2$. In the next section, the efficiency is compared with random coding based group testing approach.

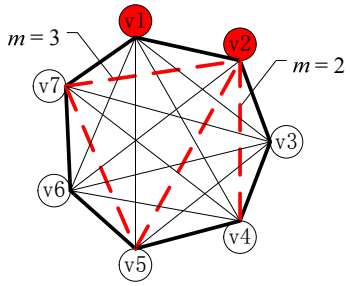


Fig. 7. Random clique deleting while keeping an particular odd cycle at a particular $t$ such that $\mathbf{y}(t) = 1$. (Here the size of the odd cycle is $M = 7$, $K = 2$, only the cliques of size 2 (edge) or 3 (triangle) consisted with non consecutive vertices can be deleted, as shown by $(2, 4)$ and $(2, 5, 7)$ for example.)

## VIII. Comparison

As stated in the introduction, our partition reservation has close relation to direct transmission and group testing. Since the average error considered in direct transmission system is not the same as the definition used in this paper, we just compare with the group testing.

Atia and Saligrama have proved the achievable rate in Theorem III. 1 in [24] for group testing with random coding, which shows that if for any $\xi > 0$ and $\frac{\log N}{T} \leq S_{cg} - \xi$, $S_{cg} \triangleq \max_p C_g(p)$, where

$$C_g(p) = \min\left\{(1-p)H(p), \frac{1}{2}H((1-p)^2)\right\}$$

the average error probability $P_e^{(N)} \to 0$ (Also, $S_{cg}$ is shown to be a capacity in Theorem IV. 1 in [24]). From Fig. 8, we can see $C_g(p) < C(p)$ for any $0 < p < 1$, so $S_{cg} < S_g$, i.e., our achievable rate is always larger than the capacity of group testing with random coding, when using random coding. Further, the diminishing speeds of group testing and partition reservation are both polynomial, i.e., $P_e^{(N)} \leq \frac{1}{N^\Delta}$ for some constant $\Delta > 0$.

Compared with a brute force method, as shown in Section V, when $K = 2$, if $T^{BF} = \frac{K^{K+1}}{K!} f(N)$, where $f(N)$ is an arbitrary function satisfying $f(N) \xrightarrow{N\to\infty} \infty$, we will have $P_e^{(N)} \leq e^{-f(N)} \xrightarrow{N\to\infty} 0$. This means that the threshold effect of the convergence doesn't exist as that in group testing or compressive sensing [6], i.e., $T$ should be of order $\log N$. However, the choice of $f(N)$ will influence the diminishing speed. If we require that the convergence speed of the brute force method to be polynomial, $f(N) = O(\log N)$ and thus $T^{BF} = O(\log N)$, which is of the same order as partition and group testing.

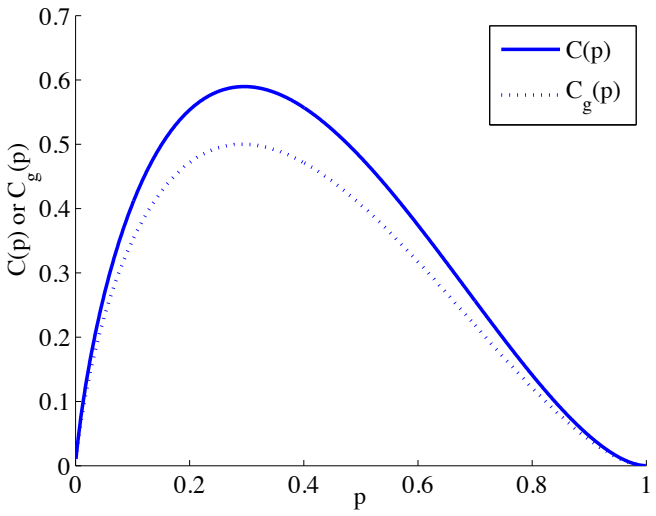


Fig. 8. Compare $C(p)$ with $C_g(p)$.

A random coding method is not as efficient as brute force method when $K = 2$, that is because intuitively, in the brute force approach, we actually encode the coloring information in the codebook, which is not the case for random coding. The main point is if we use the source codebook to construct channel codebook as done in the brute force approach, we have to deliver the associated coloring information. While for the random coding approach, we actually only care about sending information enough for the nodes to form a 2-colorable graph. However, random coding approach shows the internal structure of the problem, and the possibility to attain consistent partition for generalized $K > 2$.

## IX. Conclusion

In this paper, a new partition reservation problem is formulated to focus on the coordination overhead in the conflict resolution multi-access problem. The partition information, which is related to the relationships between active users is calculated, and two codebook design methods, source coding based and random coding are proposed and analyzed to estimate the achievable bound of partitioning overhead in non-adaptive $(0, 1)$-channel. The formulation using hypergraph and its coloring reveals the partition information and fundamental properties of the decentralized Boolean channel, and further uncovers the Fibonacci structure for a non-trivial $K = 2$ case. The comparison with group testing shows the uniqueness of the partitioning problem, and sheds light

on the future designs. In this paper, we just provide achievable rate for simple $K = 2$ cases, the converse bound and more general $K > 2$ cases are our ongoing works. In addition, we are working on cases with noise present in multiple access channels, which requires different machinery in the corresponding achievability analysis for the random coding approach [35].

## APPENDIX A
## PROOF OF LEMMA 1

*Proof:* The following derivation is subject to $p(\mathbf{z}|\mathbf{s}) \in \mathcal{P}_{z|s}$:

$$
\begin{aligned}
I(\mathbf{s};\mathbf{z}_{\mathbf{s}}) =& H(\mathbf{s}) - H(\mathbf{s} \mid \mathbf{z}) \\
=& H(\mathbf{s}) + \sum_{\mathbf{z}\in\mathbb{Z}_{K;N}} \sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \mathbf{s}) p_s(\mathbf{s}) \log \frac{p(\mathbf{z} \mid \mathbf{s}) p_s(\mathbf{s})}{\sum_{\tilde{\mathbf{s}}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \tilde{\mathbf{s}}) p_s(\tilde{\mathbf{s}})} \\
\overset{(a)}{=}& \log \binom{N}{K} + p_s(\mathbf{s}) \sum_{\mathbf{z}\in\mathbb{Z}_{K;N}} \sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \mathbf{s}) \log \frac{p(\mathbf{z} \mid \mathbf{s})}{\sum_{\tilde{\mathbf{s}}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \tilde{\mathbf{s}})} \\
\overset{(b)}{=}& \log \binom{N}{K} + p_s(\mathbf{s}) \sum_{(n_1,\ldots,n_K)} \sum_{\mathbf{z}\in\mathbb{Z}_{K;N}\{n_1,\ldots,n_K\}} \sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \mathbf{s}) \log \frac{p(\mathbf{z} \mid \mathbf{s})}{\sum_{\tilde{\mathbf{s}}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \tilde{\mathbf{s}})} \\
\overset{(c)}{\geq}& \log \binom{N}{K} + p_s(\mathbf{s}) \sum_{(n_1,\ldots,n_K)} \sum_{\mathbf{z}\in\mathbb{Z}_{K;N}\{n_1,\ldots,n_K\}} \left( \sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \mathbf{s}) \right) \times \\
& \log \frac{\left[\sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \mathbf{s})\right]}{\sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} \left[\sum_{\tilde{\mathbf{s}}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \tilde{\mathbf{s}})\right]} \\
=& \log \binom{N}{K} - p_s(\mathbf{s}) \sum_{(n_1,\ldots,n_K)} \sum_{\mathbf{z}\in\mathbb{Z}_{K;N}(n_1,\ldots,n_K)} \left( \sum_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \mathbf{s}) \right) \log |\mathbb{S}_{K;N}(\mathbf{z})| \\
\overset{(d)}{=}& \log \binom{N}{K} - \sum_{(n_1,\ldots,n_K)} \Pr(\mathbb{Z}_{K;N}(n_1,\ldots,n_K)) \log \prod_{k=1}^{K} n_k \\
\overset{(e)}{\geq}& \log \binom{N}{K} - \max_{(n_1,\ldots,n_K)} \log \prod_{k=1}^{K} n_k \qquad (34) \\
\overset{(f)}{\geq}& \log \binom{N}{K} - K \log \left(\frac{N}{K}\right), \qquad (35)
\end{aligned}
$$

where $\Pr(\mathbb{Z}_{K;N}(n_1,\ldots,n_K)) = \sum_{\mathbf{z}\in\mathbb{Z}_{K;N}(n_1,\ldots,n_K)} p_z(\mathbf{z})$ and $p_z(\mathbf{z})$ is the marginal distribution function with $p(\mathbf{z} \mid \mathbf{s}) \in \mathcal{P}_{z|s}$. In the derivation, line $(a)$ is because of $\mathbf{s} \sim \mathcal{U}(\mathbb{S}_{K;N})$; line $(b)$ is because set $\mathbb{Z}_{K;N}$ includes all partition sets $\mathbb{Z}_{K;N}(n_1,\ldots,n_K)$, i.e.,

$\mathbb{Z}_{K;N} = \bigcup_{(n_1,\ldots,n_K)} \mathbb{Z}_{K;N}(n_1,\ldots,n_K)$; Line $(c)$ is derived from the log sum inequality, i.e., for non-negative sequence $a_1,\ldots,a_n$ and $b_1,\ldots,b_n$,

$$\sum_{i=1}^{n} a_i \log \frac{a_i}{b_i} \geq \left(\sum_{i=1}^{n} a_i\right) \log \frac{\sum_{j=1}^{n} a_j}{\sum_{\ell=1}^{n} b_\ell} \tag{36}$$

with equality if and only if $\frac{a_i}{b_i}$ is a constant for all $i$. And here, sequence $[a_i] = [p(\mathbf{z}|\mathbf{s})]_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})}$, $[b_i] = [\sum_{\tilde{\mathbf{s}}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \tilde{\mathbf{s}})]_{\mathbf{s}\in\mathbb{S}_{K;N}(\mathbf{z})}$ is a constant sequence. Line $(d)$ follows for any $\mathbf{z} \in \mathbb{Z}_{K;N}(n_1,\ldots,n_K)$, $|\mathbb{S}_{K;N}(\mathbf{z})| = \prod_{k=1}^{K} n_k$; line (f) is just an application of the inequality of arithmetic and geometric means. For the equality of (34), line $(c)$, $(e)$ should be equalities, which means by $(b)$,

$$\frac{p(\mathbf{z}|\mathbf{s})}{\sum_{\tilde{\mathbf{s}}\in\mathbb{S}_{K;N}(\mathbf{z})} p(\mathbf{z} \mid \tilde{\mathbf{s}})} = p(\mathbf{s}|\mathbf{z}) = \text{const.}, \quad \forall \mathbf{s} \in \mathbb{S}_{K;N}(\mathbf{z}), \tag{37}$$

and by $(e)$,

$$\Pr(\mathbb{Z}_{K;N}(n_1^*,\ldots,n_K^*)) = \begin{cases} \frac{1}{A}, & (n_1^*,\ldots,n_K^*) = \arg\max \prod_{k=1}^{K} n_k \\ 0, & otherwise \end{cases} \tag{38}$$

where $A = \sum \Pr(\mathbb{Z}_{K;N}(n_1^*,\ldots,n_K^*))$ is a normalized factor. We can choose $\mathbf{z}|\mathbf{s} \sim \mathcal{U}(\mathbb{Z}_{K;N}(n_1^*,\ldots,n_K^*) \bigcap \mathbb{Z}_{K;N}(\mathbf{s}))$, and it is easy to see under this condition, both $(b)$ and $(d)$ will be equality, then so is $(e)$. Thus the lower bound (34) is proved to be achieved.

It is worth noting the result won't change with a generalized $\mathbf{z}$. Define $\mathbf{z} \in \{0,1,\ldots,N\}^N$, such that $z_i = 0$ indicates an inactive $i$-th user, and $z_i = k$ indicates that the $i$-th user is assigned into the $k$-th group. The definition of distortion can be generalized as follows:

$$d(\mathbf{s},\mathbf{z}) = \begin{cases} 0, & \forall i,j \in \mathcal{G}_{\mathbf{s}}, i \neq j, \text{ and } z_i, z_j \neq 0, \text{ and } z_i s_i \neq z_j s_j \\ 1, & \text{otherwise} \end{cases}. \tag{39}$$

i.e., active users are assigned different groups, and they cannot be announced as inactive. The definition is consistent with our earlier definition where $\mathbf{z}$ is restricted to $\mathbb{Z}_{K;N}$. From the proof above, it is easy to see with this generalization, the lower bound is the same as in Eq. (34). The equality in line $(e)$ can be achieved by choosing $\mathbf{z}|\mathbf{s}$ uniformly in the same way. ■

## APPENDIX B
## PROOF OF THEOREM 1

First, for $\sum n_k = N$ and $n_k \geq 0$, define

$$\binom{N}{n_1^*, \ldots, n_K^*} = \frac{N!}{\Pi_k n_k!} \tag{40}$$

to be the number of possible partitions in $\mathbb{Z}_{K;N}(n_1^*, \ldots, n_K^*)$.

*Proof:* The proof is based on random coding, i.e., randomly generate the source codebook $\mathcal{C} = \{\mathbf{z}_\ell\}_{\ell=1}^{L^{(N)}}$ from $p_z(\mathbf{z})$, which is the marginal distribution function based on $p(\mathbf{z} \mid \mathbf{s})$ in (9) in Lemma 1 and $p_s(\mathbf{s}) = 1/\binom{N}{K}$, i.e.,

$$p(\mathbf{z} \mid \mathbf{s}) = \frac{1}{K!\binom{N-K}{n_1^*-1, \ldots, n_K^*-1}},\ \mathbf{z} \in \mathbb{Z}_{K;N}(n_1^*, \ldots, n_K^*) \bigcap \mathbb{Z}_{K;N}(\mathbf{s}) \tag{41}$$

$$p(\mathbf{z}) = \frac{1}{\binom{N}{n_1^*, \ldots, n_K^*}},\ \mathbf{z} \in \mathbb{Z}_{K;N}(n_1^*, \ldots, n_K^*) \tag{42}$$

Reveal this codebook to the source encoder and decoder. For any $\mathbf{s} \in \mathbb{S}_{K;N}$, define the source encoding function $f_N^s(\mathbf{s}) = \ell$, such that $\ell = \arg \min_{1 \leq \ell \leq L^{(N)}} d(\mathbf{s}, \mathbf{z}_\ell)$. If there is more than one such $\ell$, choose the least. Then define the source decoding function $g_N^s(\ell) = \mathbf{z}_\ell$. So for any source $\mathbf{s}$, it will be correctly reconstructed if and only if there exists $\ell$ such that $d(\mathbf{s}, \mathbf{z}_\ell) = 0$. The average

error probability over the codebook $\mathcal{C}$ is

$$\begin{aligned}
P_e^{s,(N)} &= \sum_{\mathcal{C}} p(\mathcal{C}) \sum_{\mathbf{s}} p_{\mathbf{s}}(\mathbf{s}) \Pr(\forall \mathbf{z}_\ell \in \mathcal{C}, d(\mathbf{s}, \mathbf{z}_\ell) \neq 0 | \mathcal{C}, \mathbf{s}) \\
&= \sum_{\mathcal{C}} p(\mathcal{C}) \sum_{\mathbf{s}:\forall \mathbf{z}_\ell \in \mathcal{C}, d(\mathbf{s},\mathbf{z}_\ell)\neq 0} p_{\mathbf{s}}(\mathbf{s}) \\
&= \sum_{\mathbf{s}} p_{\mathbf{s}}(\mathbf{s}) \sum_{\mathcal{C}:\forall \mathbf{z}_\ell \in \mathcal{C}, d(\mathbf{z}^\ell,\mathbf{s})\neq 0} p(\mathcal{C}) \\
&\overset{(a)}{=} \sum_{\mathcal{C}:\forall \mathbf{z}_\ell \in \mathcal{C}, d(\mathbf{z}^\ell,\tilde{\mathbf{s}})\neq 0} p(\mathcal{C}) \\
&= \prod_{\ell=1}^{L^{(N)}} \sum_{\mathbf{z}_\ell : d(\mathbf{z}_\ell,\tilde{\mathbf{s}})\neq 0} p(\mathbf{z}_\ell) \\
&= \prod_{\ell=1}^{L^{(N)}} \left(1 - \sum_{\mathbf{z}_\ell : d(\mathbf{z}_\ell,\tilde{\mathbf{s}})= 0} p(\mathbf{z}_\ell)\right) \\
&\overset{(b)}{=} \left(1 - K! \binom{N-K}{n_1^*-1,\ldots,n_K^*-1} \times \frac{1}{\binom{N}{n_1^*,\ldots,n_K^*}}\right)^{L^{(N)}} \\
&= \left(1 - 2^{-W_N^I}\right)^{L^{(N)}}
\end{aligned} \tag{43}$$

The meaning of line $(a)$ is the probability that there are no correct codewords in a random chosen $\mathcal{C}$ for any given $\tilde{\mathbf{s}}$, it is derived by the symmetry of random codebook. Line $(b)$ is derived using the fact that $|\{\mathbf{z}_\ell : d(\mathbf{z}_\ell, \tilde{\mathbf{s}}) = 0\}| = |\mathbb{Z}_{K;N}(n_1^*, \ldots, n_K^*) \bigcap \mathbb{Z}(\tilde{\mathbf{s}})| = K! \binom{N-K}{n_1^*-1,\ldots,n_K^*-1}$. According to the inequality:

$$(1 - xy)^n \leq 1 - x + e^{-yn}, \text{ for } 0 \leq x, y \leq 1, n > 0 \tag{44}$$

We have

$$P_e^{s,(N)} \leq e^{-2^{\left(\log L^{(N)} - W_N^I\right)}} \tag{45}$$

Since this is the average error probability over all possible codebooks $\mathcal{C}$, there must exist a codebook to achieve the error bound above, which completes the proof. ■

## APPENDIX C
## PROOF OF LEMMA 2 AND THEOREM 3

*Proof:* The proofs of Lemma 2 and Theorem 3 are similar, so we put them together. In the proof, we will use the method of strong typical set, definition of which can be found in the book

of Csiszar and Körner [32]. Recall that $T \times 1$ vectors $\mathbf{x}_1$, $\mathbf{x}_2$ represent the codewords of user 1 and 2, let $[\mathbf{x}_1, \mathbf{x}_2]$ denote the $T \times 2$ matrix with $\mathbf{x}_1$ and $\mathbf{x}_2$ as its two columns. A strong typical set $\mathcal{A}_\epsilon^{(T)}$ is proposed at first, which contains almost all $[\mathbf{x}_1, \mathbf{x}_2]$, i.e., $\Pr\left([\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}\right) \xrightarrow{T\to\infty} 1$. In this typical set, the probability of existence of any possible odd cycle (1-odd cycle) is calculated and $P_e$ is bounded by using union bound.

To simplify notation, denote $E^{(w)}$, $w = 1, 2$ as the event that $H'$ contains the 1-odd cycles or odd cycles respectively, and $P_e^{(1)} \triangleq P_e^{1-odd} \triangleq \Pr(E^{(1)})$, $P_e^{(2)} \triangleq P_e^{odd} \triangleq \Pr(E^{(2)})$. Since we have:

$$\begin{aligned} P_e^{(w)} =& \Pr(E^{(w)}[\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) + \Pr(E^{(w)}, [\mathbf{x}_1, \mathbf{x}_2] \notin \mathcal{A}_\epsilon^{(T)}) \\ \leq& \Pr(E^{(w)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) + \Pr([\mathbf{x}_1, \mathbf{x}_2] \notin \mathcal{A}_\epsilon^{(T)}), \end{aligned} \tag{46}$$

it suffices to show that for any $0 < p < 1$, when $\frac{\log N}{T} < C(p)$, both $\Pr([\mathbf{x}_1, \mathbf{x}_2] \notin \mathcal{A}_\epsilon^{(T)})$ and $\Pr(E^{(w)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)})$ approach 0 as $N \to \infty$. While the first one is directly from the feature of strong typical set, the key point is to estimate the probability of $E^{(w)}$ in the typical set $\mathcal{A}_\epsilon^{(T)}$. First, let us define the strong typical set that will simplify the calculation of $\Pr(E^{(w)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)})$.

### *A. Strong typical set*

Note that the input is $\mathcal{G}_{\mathbf{s}_0} = \{1, 2\}$, since the codewords $x_{1,t}$ and $x_{2,t}$ are generated from $\mathcal{B}(p)$, it is very likely that in the set $\{(x_{1,t}, x_{2,t})\}_{t=1}^T$, there are $p_{12}(u, v)T$ pairs $(u, v)$, $\forall u, v \in \{0, 1\}$, where $p_{12}(u, v) \triangleq p_x(u)p_x(v)$, and $p_x(\tilde{x}) \triangleq p\mathbb{1}(\tilde{x} = 1) + (1 - p)\mathbb{1}(\tilde{x} = 0)$ is the pdf of $\mathcal{B}(p)$. Strictly speaking, define $N((u, v)|[\mathbf{x}_1, \mathbf{x}_2])$ as the number of $(u, v)$ in $\{(x_{1,t}, x_{2,t})\}_{t=1}^T$, for any given $\epsilon > 0$, define the strong typical set:

$$\mathcal{A}_\epsilon^{(T)} = \left\{ [\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2] \in \{0, 1\}^{2T} : \left| \frac{1}{T} N((u, v)|[\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2]) - p_{12}(u, v) \right| < \frac{\epsilon}{4}, \forall u, v \in \{0, 1\} \right\} \tag{47}$$

The parameter $\epsilon$ will be chosen at beginning to guarantee some good features of the set $\mathcal{A}_\epsilon^{(T)}$, we will provide such requirements on $\epsilon$ during the proof, and summarize them at the end of the proof. The first requirement is that

$$\epsilon/4 < \max_{u,v} \left( \max(p_{12}(u, v), 1 - p_{12}(u, v)) \right), \tag{48}$$

so that $1 > p_{12}(u, v) \pm \epsilon/4 > 0$. For strong typical set, $\forall \epsilon > 0$, $\Pr(\mathbf{X} \notin \mathcal{A}_\epsilon^{(T)}) \to 0$, as $T \to \infty$, thus let us consider the case that $\Pr(E^{(w)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) \to 0$ in the following parts.

*B. Odd cycles for given $\mathcal{A}_\epsilon^{(T)}$*

Consider $\Pr(E^{(w)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)})$. For simplicity, assume $N$ is an odd number. Denote $A_M^{(g)}, g \in \{1,2,3\}$ to be the event of existence of the type-$g$ odd cycles with size $M$, thus:

$$E^{(1)} = \bigcup_{m=1}^{(N-1)/2} A_{2m+1}^{(1)} \tag{49}$$

$$E^{(2)} = \bigcup_{m=1}^{(N-1)/2} \bigcup_{g=1,2,3} A_{2m+1}^{(g)} \tag{50}$$

For any given particular $[\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}$, denote

$$P_{2m+1|[\mathbf{x}_1,\mathbf{x}_2]}^{(g)} \triangleq \Pr\left(A_{2m+1}^{(g)} \middle| [\mathbf{x}_1, \mathbf{x}_2]\right), \tag{51}$$

as the probability that the $g$-th kind of odd cycle of length $2m+1$ exists in $H'$ for given $[\mathbf{x}_1, \mathbf{x}_2]$. Then by union bound, we have:

$$\begin{aligned}\Pr(E^{(1)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) &\leq \sum_{[\mathbf{x}_1,\mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}} \sum_{M=3,5,\ldots,N} P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(1)} Q_{1,2}(\mathbf{x}_1, \mathbf{x}_2) \\ &\leq \sum_{M=3,5,\ldots,N} \max_{[\mathbf{x}_1,\mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}} P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(1)} \end{aligned} \tag{52}$$

where $Q_{1,2}(\mathbf{x}_1, \mathbf{x}_2)$ is the probability that the first two codewords take values $\mathbf{x}_1, \mathbf{x}_2$. Similarly,

$$\Pr(E^{(2)}, [\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}) \leq \sum_{M=3,5,\ldots,N} \sum_{g=1,2,3} \max_{[\mathbf{x}_1,\mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}} P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(g)} \tag{53}$$

Thus, the key point is to calculate $P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(g)}$ for any given $[\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}$ and upper bound it.

*C. The probability of existence of 1-odd cycles of length $M$: $P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(1)}$*

Consider any particular 1-odd cycle of length $M$, denoted by $H_{e;M}^{(1)} = (1, 2, i_1, \ldots, i_{M-2})$, there are at most $\binom{N-2}{M-2}(M-2)!$ such odd cycles out of $N$ nodes, and because of symmetry, the existence of any of them is equiprobable. Let us see for a given $[\mathbf{x}_1, \mathbf{x}_2]$, what values should the codewords $\{\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_{M-2}}\}$ of other $M-2$ vertices be to guarantee $H_{e;M}^{(1)} \subseteq H'$.

Note $H'$ is obtained by a series of operations on graph, and the order of operations is not important. Let us calculate the probability that $H_{e;M}^{(1)}$ is not deleted at any slot $1 \leq t \leq T$. By the symmetry of the generation of codewords, this probability only depends on the values of $(x_{1,t}, x_{2,t})$. Given $[\mathbf{x}_1, \mathbf{x}_2]$, let $\mathcal{T}_{u,v} = \{t : (x_{1,t}, x_{2,t}) = (u, v)\}$, and $T_{u,v} \triangleq |\mathcal{T}_{u,v}| = N((u,v)|[\mathbf{x}_1, \mathbf{x}_2])$. Thus

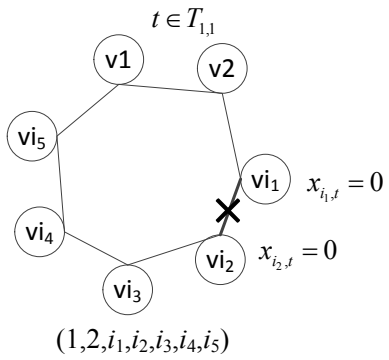


Fig. 9. Example that odd cycle is destroyed by edge $(i_1, i_2)$ deleted.

we just need to consider four situations $t \in \mathcal{T}_{u,v}$. Denote the probability that $H_{e;M}^{(1)}$ is not deleted at $t \in \mathcal{T}_{u,v}$ as $\mu_{u,v;M}^{(1)}$, so by union bound of all possible $H_{e;M}^{(1)}$, we have for all $[\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}_\epsilon^{(T)}$:

$$\begin{aligned} P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(1)} \leq & \binom{N-2}{M-2}(M-2)!\Pi_{u,v}\left(\mu_{u,v;M}^{(1)}\right)^{T_{u,v}} \\ \leq & N^{M-2}\Pi_{u,v}\left(\mu_{u,v;M}^{(1)}\right)^{(p_{12}(u,v)-\epsilon/4)T} \end{aligned} \tag{54}$$

Now $\mu_{u,v;M}^{(1)}$ is determined separately for cases of different $(u, v)$ as follows:

1) The case that $t \in \mathcal{T}_{0,0}$

   For $t \in \mathcal{T}_{0,0}$, $y_t = 0$, the operation is to delete vertices. Then all of the codewords of other $M-2$ vertices should be 0, otherwise these vertices would be deleted, thus

$$\mu_{0,0;M}^{(1)} = \Pr(x_{i_w,t} = 0, \forall w \in \{1, \ldots, M-2\}) = (1-p)^{M-2} \tag{55}$$

2) The case that $t \in \mathcal{T}_{1,1}$

   In these slots $y_t = 1$, the operation of deleting clique is done in $H'$. At any slot $t$, $H_{e;M}^{(1)}$ will be broken up if the edges of it are deleted, which is equivalent to the existence of codewords of two consecutive vertices from $\{1, 2, i_1, \ldots, i_{M-2}, 1\}$ to be both 0 at those $t \in \mathcal{T}_{1,1}$, as shown in Fig. 9. So we have:

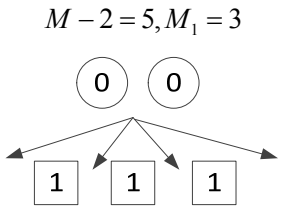


Fig. 10. Example of counting number of sequence $\{x_{i_1,t},\ldots,x_{i_{M-2},t}\}$ with $M_1$ ones, here $M-2=5$, $M_1=3$.

$$\begin{aligned}
\mu^{(1)}_{1,1;M} \triangleq & 1-\Pr\left(\exists(i,j)\in\{(1,2),(2,i_1),\ldots,(i_{M-3},i_{M-2}),(i_{M-2},1)\},x_{i,t}=x_{j,t}=0\right)\\
\overset{(a)}{=} & 1-\Pr\left(\exists w\in\{1,\ldots,M-3\},x_{i_w,t}=x_{i_{w+1},t}=0\right)\\
\overset{(b)}{=} & 1-\sum_{M_1=\frac{M-3}{2}}^{M-2}\Pr\left(\sum_{w=1}^{M-2}x_{i_w,t}=M_1,\exists w\in\{1,\ldots,M-3\},x_{i_w,t}=x_{i_{w+1},t}=0\right)\\
\overset{(c)}{=} & \sum_{M_1=\frac{M-3}{2}}^{M-2}\binom{M_1+1}{M-2-M_1}p^{M_1}(1-p)^{M-2-M_1}.
\end{aligned}\tag{56}$$

Line $(a)$ is because now $x_{1,t}=x_{2,t}=1$. For line $(b)$, we change the sum by grouping items with different $M_1$, where $M_1$ is the number of values of $1\le w\le M-2$ for which $x_{i_w,t}=1$. It is easy to see there must be $M_1\ge\lfloor\frac{M-2}{2}\rfloor=\frac{M-2}{2}$, otherwise there must exists a $w$ such that $x_{i_w,t}=x_{i_{w+1},t}=0$. In line $(c)$, the sum of probability of the items with $M_1$ is calculated out, since the probability of each item is $p^{M_1}(1-p)^{M-2-M_1}$, the key point is to count the number of sequences $(x_{i_1,t},\ldots,x_{i_{M-2},t})$ with $M_1$ ones and $M-2-M_1$ zeros. The counting method is to fix $M_1$ ones, then count how many combinations to put $M-2-M_1$ zeros into $M_1+1$ spots, as shown in Fig. 10.

For a better statement in the rest of the paper, define a function $J_M(p)$ which calculates the probability of a $M$ length random Bernoulli sequence $(x_1,\ldots,x_M)$, $x_w\sim\mathcal{B}(p)$ without consecutive zeros, i.e.,

$$\begin{aligned}
J_M(p) =& 1-\Pr\left(\exists w\in\{1,\ldots,M-1\},x_w=x_{w+1}=0\right)\\
=& \sum_{M_1=\lfloor\frac{M}{2}\rfloor}^{M}\binom{M_1+1}{M-M_1}p^{M_1}(1-p)^{M-M_1}.
\end{aligned}\tag{57}$$

Thus, we can see $\mu^{(1)}_{1,1;M} = J_{M-2}(p)$.

3) The cases that $t \in \mathcal{T}_{1,0}$ or $t \in \mathcal{T}_{0,1}$

The two cases are symmetric, let's consider $t \in \mathcal{T}_{1,0}$ first. It is similar as the case that $t \in \mathcal{T}_{1,1}$, but since now $x_{2,t} = 0$, the codeword of vertex that connected to vertex 2 (i.e., vertex $i_1$), should be $x_{i_1,t} = 1$. For other $M-3$ vertices, it is required codewords of any two consecutive vertices from $\{i_2, \ldots, i_{M-2}\}$ at those $t \in \mathcal{T}_{1,0}$ should not be both 0. Thus,

$$\begin{aligned}\mu^{(1)}_{1,0;M} =& \Pr(x_{i_1 t} = 1)\left(1 - \Pr\left(\exists w \in \{1, \ldots, M-1\}, x_w = x_{w+1} = 0\right)\right)\\ =& pJ_{M-3}(p)\end{aligned} \tag{58}$$

Similarly, for $t \in \mathcal{T}_{0,1}$, we have $\mu^{(1)}_{1,0;M} = J_{M-3}(p)$.

Then $P^{(1)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}$ can be bounded by (54).

### *D. The probability of existence of type-2 and type-3 cycles of length $M$: $P^{(2)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}$ and $P^{(3)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}$*

For the type-2 odd cycles, either 1 or 2 nodes are included. Denote $H^{(2),h}$ to be a second kind odd cycle containing vertex $h \in \{1, 2\}$. We can choose a particular odd cycle $H^{(2),1}_{e;M} = (1, i_1, \ldots, i_{M-1})$, $H^{(2),2}_{e;M} = (2, i_1, \ldots, i_{M-1})$, and a particular type-3 odd cycle $H^{(3)}_{e;M} = (i_1, \ldots, i_M)$. There are $\binom{N-2}{M-1}\frac{(M-1)!}{2}$ such $H^{(2),h}_{e;M}$, and $\binom{N-2}{M}\frac{(M-1)!}{2}$ such $H^{(3)}_{e;M}$. Then following the same analysis as for $P^{(1)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}$, we have for all $[\mathbf{x}_1, \mathbf{x}_2] \in \mathcal{A}^{(T)}_\epsilon$,

$$\begin{aligned}P^{(2)}_{M|[\mathbf{x}_1,\mathbf{x}_2]} \leq& \sum_{h=1,2}\binom{N-2}{M-1}\frac{(M-1)!}{2}\Pi_{u,v}\left(\mu^{(2),h}_{u,v;M}\right)^{T_{u,v}}\\ \leq& \frac{1}{2}N^{M-1}\sum_{h=1,2}\Pi_{u,v}\left(\mu^{(2),h}_{u,v;M}\right)^{(p_{12}(u,v)-\epsilon/4)T},\end{aligned} \tag{59}$$

$$\begin{aligned}P^{(3)}_{M|[\mathbf{x}_1,\mathbf{x}_2]} \leq& \binom{N-2}{M}\frac{(M-1)!}{2}\Pi_{u,v}\left(\mu^{(3)}_{u,v;M}\right)^{T_{u,v}}\\ \leq& N^M\Pi_{u,v}\left(\mu^{(3)}_{u,v;M}\right)^{(p_{12}(u,v)-\epsilon/4)T},\end{aligned} \tag{60}$$

where $\mu^{(g),h}_{u,v;M}$ is the probability that $H^{(g),h}_{e;M}$ won't be deleted at $t \in \mathcal{T}_{u,v}$. Then similarly, we have:

1) For $t \in \mathcal{T}_{0,0}$, $y_t = 0$, every vertex cannot be deleted, thus:

$$\mu^{(2),h}_{0,0;M} = (1-p)^{M-1}; \quad \mu^{(3)}_{0,0;M} = (1-p)^M \tag{61}$$

2) For $g=2$, let's consider $H_{e;M}^{(2),1}$ first, when $t\in\mathcal{T}_{1,1}$ or $t\in\mathcal{T}_{1,0}$, $x_{1,t}=1$, thus:

$$\mu_{1,0;M}^{(2),1}=\mu_{1,1;M}^{(2),1}=1-\Pr\left(\exists w\in\{1,\ldots,M-2\},x_{i_w,t}=x_{i_{w+1},t}=0\right)=J_{M-1}(p) \quad (62)$$

When $t\in\mathcal{T}_{0,1}$, $x_{1,t}=0$, thus, the codewords of vertexs $i_1$ and $i_{M-1}$ which are connected to 1 should be 1, i.e.,

$$\begin{aligned}\mu_{0,1;M}^{(2),1}=&\Pr(x_{i_1,t}=x_{i_{M-1},t}=1)\left(1-\Pr\left(\exists w\in\{2,\ldots,M-1\},x_{i_w,t}=x_{i_{w+1},t}=0\right)\right)\\=&p^2J_{M-3}(p)\end{aligned} \quad (63)$$

For $H_{e;M}^{(2),2}$, due to symmetry, the result is easy to derive:

$$\mu_{1,1;M}^{(2),2}=\mu_{0,1;M}^{(2),2}=J_{M-1}(p);\quad \mu_{1,0;M}^{(2),2}=p^2J_{M-3}(p) \quad (64)$$

3) For $g=3$, for $t\notin\mathcal{T}_{0,0}$, $y_t=1$. Since neither vertices 1 nor 2 are in $H_{e;M}^{(3)}$, $\mu_{u,v;M}^{(3)}$ are the same for any $(u,v)\neq(0,0)$. Now we have:

$$\begin{aligned}\mu_{u,v;M}^{(3)}=&1-\Pr\left(\exists(i,j)\in\{(i_1,i_2),\ldots,(i_{M-1},i_M),(i_M,i_1)\},x_{i,t}=x_{j,t}=0\right)\\=&1-\Pr\left(\exists w\in\{1,\ldots,M-1\},x_{i_w,t}=x_{i_{w+1},t}=0\right)\\&-\Pr\left((x_{i_1,t},x_{i_M,t})=(0,0);\nexists w\in\{1,\ldots,M-1\},x_{i_w,t}=x_{i_{w+1},t}=0\right)\\=&J_M(p)-\Pr((x_{i_1,t},x_{i_M,t})=(0,0),x_{i_2,t}=1,x_{i_{M-1},t}=1)\times\\&\left(1-\Pr\left(w\in\{3,\ldots,M-3\},x_{i_w,t}=x_{i_{w+1},t}=0\right)\right)\\=&J_M(p)-p^2(1-p)^2J_{M-4}(p)\end{aligned} \quad (65)$$

Now we can bound $P_{M|[\mathbf{x}_1,\mathbf{x}_2]}^{(g)}$. In the next subsection, we will get explicit expressions for $J_M(p)$, then $\mu_{u,v;M}^{(g)}$. We can see they have a close relationship to extended Fibonacci numbers.

### *E. Explicit expressions for $J_M(p)$ and extended Fibonacci numbers*

We will show that expression for $J_M(p)$ has a close relation to a certain extended Fibonacci numbers. It is not surprising since Fibonacci numbers can be used for determining the numbers of consecutive 0s in Bernoulli sequence [34].

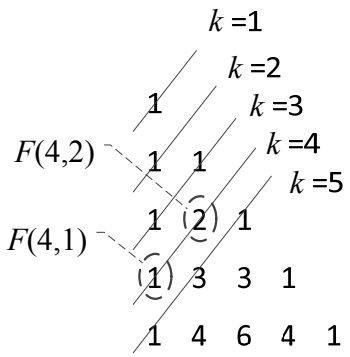


Fig. 11. $F(k,j)$ in the Pascal triangle.

Define extended Fibonacci numbers as:

$$F(k,p) = \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} F(k,j) p^{k-1-j}(1-p)^j \tag{66}$$

$$F(k,j) = \begin{cases} \binom{k-1-j}{j}, & 0 \le j \le \lfloor \frac{k-1}{2} \rfloor \\ 0, & otherwise \end{cases} \tag{67}$$

The meaning of $F(k,j)$ can be seen directly from the Pascal triangle, as shown in Fig. 11, and $F(k,p)$ is a weighted sum of $F(k,j)$ with the weight $p^{k-1-j}(1-p)^j$. From Fig. 11 it is shown:

$$F(k,j) = F(k-1,j) + F(k-1,j-1), \tag{68}$$

so that

$$\begin{aligned} F(k,p) &= \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} \left( F(k-1,j) + F(k-1,j-1) \right) p^{k-1-j}(1-p)^j \\ &= pF(k-1,p) + p(1-p)F(k-2,p). \end{aligned} \tag{69}$$

Then we can get the general terms of $F(k,p)$ by solving the corresponding difference equation, which gives us:

$$F(k,p) = \frac{\varphi(p)^k - \psi(p)^k}{\varphi(p) - \psi(p)}, \tag{70}$$

where

$$\varphi(p) = \frac{p + \sqrt{4p - 3p^2}}{2}; \quad \psi(p) = \frac{p - \sqrt{4p - 3p^2}}{2} \tag{71}$$

It is not difficult to see

$$1 \geq \varphi(p) \geq 0 \geq \psi(p) \geq -1, \ |\varphi(p)| \geq |\psi(p)| \tag{72}$$

Given $F(k,p)$ defined in (70), it is straightforward to see:

$$J(M,p) = \frac{1}{p}F(M+2,p) = \frac{1}{p}\frac{\varphi(p)^{M+2} - \psi(p)^{M+2}}{\varphi(p) - \psi(p)} \tag{73}$$

Which further enables us to determine $\mu^{(g)}_{u,v;M}$ and upperbound $P^{(g)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}$.

### *F. Bounds of* $P^{(g)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}$

By Eq. (54), (59), (60), now we have for any $[\mathbf{x}_1,\mathbf{x}_2] \in \mathcal{A}^{(T)}_\epsilon$,

$$P^{(g)}_{M|[\mathbf{x}_1,\mathbf{x}_2]} \leq 2^{-(M-3+g)T\left(\left(h^{(g)} - ((1-p)^2 - \frac{\epsilon}{4})\log(1-p)\right) - \frac{\log N}{T}\right)} \tag{74}$$

where

$$h^{(1)} \triangleq -\frac{1}{M-2}\left((p^2 - \frac{\epsilon}{4})\log J_{M-2}(p) + (2p(1-p) - \frac{\epsilon}{2})\log pJ_{M-3}(p)\right) \tag{75}$$

$$h^{(2)} \triangleq -\frac{1}{M-1}\left((p - \frac{\epsilon}{2})\log J_{M-1}(p) + (p(1-p) - \frac{\epsilon}{4})\log p^2 J_{M-3}(p)\right) \tag{76}$$

$$h^{(3)} \triangleq -\frac{1}{M}\left(1 - (1-p)^2 - \frac{3\epsilon}{4}\right)\log\left(J_M(p) - p^2(1-p)^2 J_{M-4}(p)\right) \tag{77}$$

Next we will give a concise lower bound of $h^{(g)}$, which can be obtained by the monotonicity and concavity of $\log(\cdot)$.

(1) Bound of $h^{(1)}$

Define a normalizing factor

$$W = (p^2 - \frac{\epsilon}{4}) + (2p(1-p) - \frac{\epsilon}{2}) = 1 - (1-p)^2 - \frac{3\epsilon}{4}. \tag{78}$$

If we choose $\epsilon$ so that

$$W - \varphi(p)^2 = \frac{p}{2}\left((2-p) - \sqrt{(2-p)^2 - 4(1-p)^2}\right) - \frac{3\epsilon}{4} > 0. \tag{79}$$

then when $M$ is an odd number,

$$\begin{aligned}
-h^{(1)} \overset{(a)}{\leq} & W\log\left(\frac{p^2-\epsilon/4}{W}J_{M-2}(p)+\frac{2p(1-p)-\epsilon/2}{W}pJ_{M-3}(p)\right)\\
\overset{(b)}{\leq} & W\log\left(\frac{p^2J_{M-2}(p)+2p^2(1-p)J_{M-3}(p)}{W}\right) \qquad (80)\\
= & W\log\left(\frac{p\sqrt{4-3p}}{W(\varphi(p)-\psi(p))}\left(\frac{\sqrt{4-3p}+\sqrt{p}}{2}\varphi(p)^{M-1}-\frac{\sqrt{4-3p}-\sqrt{p}}{2}\psi(p)^{M-1}\right)\right)\\
\overset{(c)}{\leq} & W\log\left(\frac{p}{W(\varphi(p)-\psi(p))}\frac{\sqrt{4-3p}(\sqrt{4-3p}+\sqrt{p})}{2}\varphi(p)^{M-1}\right)\\
= & W\log\left(\frac{\varphi(p)^M}{W}\right) \qquad (81)\\
= & W\log\left(\varphi(p)^{M-2}\right)+W\log\left(\frac{\varphi(p)^2}{W}\right)\\
\leq & W\log\left(\varphi(p)^{M-2}\right) \qquad (82)
\end{aligned}$$

Where line $(a)$ is because of the concavity of $\log(\cdot)$; inequalities $(b)$ and $(c)$ are because of the increasing monotonicity of $\log(\cdot)$. Then

$$h^{(1)}-((1-p)^2-\frac{\epsilon}{4})\log(1-p)\geq C(p)-g_1(p)\epsilon \qquad (83)$$

where $g_1(p)\triangleq-\frac{1}{4}\left(3\log(\varphi(p))+\log(1-p)\right)>0$, and

$$C(p)\triangleq-(1-(1-p)^2)\log\varphi(p)-(1-p)^2\log(1-p). \qquad (84)$$

(2) Bound of $h^{(2)}$

Similarly, if $\epsilon$ satisfies (48) and (79), we have

$$\begin{aligned}
-h_2 \overset{(a)}{\leq} & W\log\left(\frac{p-\epsilon/2}{W}J_{M-1}(p)+\frac{p(1-p)-\epsilon/4}{W}pJ_{M-3}(p)\right)+(p(1-p)-\epsilon/4)\log p\\
\overset{(b)}{\leq} & W\log\left(\frac{p}{W}J_{M-1}(p)+\frac{p(1-p)}{W}pJ_{M-3}(p)\right)+(p(1-p)-\epsilon/4)\log p\\
\overset{(c)}{\leq} & W\log\left(\frac{\varphi(p)^M}{W}\right)+(p(1-p)-\epsilon/4)\log p\\
= & W\log\left(\varphi(p)^{M-1}\right)+W\log\left(\frac{\varphi(p)}{W}\right)+(p(1-p)-\epsilon/4)\log p\\
\overset{(d)}{\leq} & W\log\left(\varphi(p)^{M-1}\right)-\frac{\epsilon}{4}\log p \qquad (85)
\end{aligned}$$

where inequalities $(a)$ and $(b)$ are because of the concavity and monotonicity of $\log(\cdot)$; line $(c)$ is because that $\frac{p}{W}J_{M-1}(p)+\frac{p(1-p)}{W}pJ_{M-3}(p)=\frac{p^2J_{M-2}(p)+2p^2(1-p)J_{M-3}(p)}{W}$, and then is the same with (80) and (81); line $(d)$ is derived from Eq. (79), and:

$$\begin{aligned}
&W\log\left(\frac{\varphi(p)}{W}\right)+(p(1-p)-\epsilon/4)\log p\\
=&\left(\frac{W}{2}\log(\varphi(p)^2/W)-(2p-p^2)\log\sqrt{2p-p^2}+p(1-p)\log p\right)\\
&+\left(\frac{3\epsilon}{8}\log(1-(1-p)^2)+\frac{W}{2}\log\left(1-\frac{3\epsilon}{4(2p-p^2)}\right)-\frac{\epsilon}{4}\log p\right)\\
\leq&\left(-(2p-p^2)\log\sqrt{2p-p^2}+p(1-p)\log p\right)-\frac{\epsilon}{4}\log p\\
=&-p(1-H(p/2))-\frac{\epsilon}{4}\log p\\
\leq&-\frac{\epsilon}{4}\log p
\end{aligned}\tag{86}$$

and thus,

$$\begin{aligned}
h_2-((1-p)^2-\frac{\epsilon}{4})\geq&-W\log\varphi(p)-((1-p)^2-\frac{\epsilon}{4})\log(1-p)+\frac{\epsilon\log p}{4(M-1)}\\
=&C(p)+(3\log(\varphi(p))+\log(1-p))\frac{\epsilon}{4}+\frac{\epsilon\log p}{4(M-1)}\\
\geq&C(p)-g_2(p)\epsilon,
\end{aligned}\tag{87}$$

where $g_2(p)=g_1(p)-\log p/8>0$.

(3) Bound of $h^{(3)}$

Similarly, we can bound $h_3$ if $\epsilon$ satisfies (48) and (79), and $M$ is odd number,

$$\begin{aligned}
&h_3-((1-p)^2-\frac{\epsilon}{4})\log(1-p)\\
\geq&-\frac{1}{M}\left(1-(1-p)^2-\frac{3\epsilon}{4}\right)\log(\varphi(p)^M+\psi(p)^M)-((1-p)^2-\frac{\epsilon}{4})\log(1-p)\\
\overset{(a)}{\geq}&\frac{1}{M}\left(1-(1-p)^2-\frac{3\epsilon}{4}\right)\log(\varphi(p)^M)-((1-p)^2-\frac{\epsilon}{4})\log(1-p)\\
=&C(p)-g_1(p)\epsilon
\end{aligned}\tag{88}$$

where line $(a)$ is because $\psi(p)<0$ and $M$ is odd number.

As determined above, since $g_2(p)>g_1(p)$, we can summarize the results that when $\epsilon$ satisfies (48) and (79), we have:

$$h^{(g)}-((1-p)^2-\frac{\epsilon}{4})\log(1-p)\geq C(p)-g_2(p)\epsilon\tag{89}$$

and thus from Eq. (74), we have

$$\max_{[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)}} P^{(g)}_{M|[\mathbf{x}_1,\mathbf{x}_2]} \leq 2^{-(M-3+g)T\left(C(p)-g_2(p)\epsilon-\frac{\log N}{T}\right)}. \tag{90}$$

### *G. Completing the proof*

If $\frac{\log N}{T} \leq C(p)-\xi$ for any constant $\xi > 0$, we can always choose $\epsilon$ satisfying (48) and (79), and

$$\epsilon < (C(p)-\delta)/g_2(p) \tag{91}$$

so that $C(p)-\frac{\log N}{T}-g_2(p)\epsilon \geq C(p)-\delta-g_2(p)\epsilon \triangleq \Delta > 0$, where $\Delta$ is a predetermined constant. Then by Eq. (52), (53) and (90), we have:

$$\begin{aligned}\Pr(E^{(1)},[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)}) \leq & \sum_{M=3,5,\ldots,N}\max_{[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)}} P^{(1)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}\\ \leq & \sum_{M=3,5,\ldots,N} 2^{-(M-2)\Delta T}\\ \leq & \frac{2^{-\Delta T}}{1-2^{-2\Delta T}}\end{aligned} \tag{92}$$

and

$$\begin{aligned}\Pr(E^{(2)},[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)}) \leq & \sum_{g=1,2,3}\sum_{M=3,5,\ldots,N}\max_{[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)}} P^{(g)}_{M|[\mathbf{x}_1,\mathbf{x}_2]}\\ \leq & \sum_{g=1,2,3}\sum_{M=3,5,\ldots,N} 2^{-(M-3+g)\Delta T}\\ \leq & 3\times\frac{2^{-\Delta T}}{1-2^{-2\Delta T}}\end{aligned} \tag{93}$$

Thus, when $N\to\infty$, which also means $T\to\infty$, we can see $\Pr(E^{(w)},[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)})$ approaches 0, $\forall w = 1,2$. Since $\Pr(E^{(w)},[\mathbf{x}_1,\mathbf{x}_2]\in\mathcal{A}_\epsilon^{(T)})\to 0$ as well, we have $P_e^{(w)}\to 0$ when $\frac{\log N}{T} < C(p)-\xi$, which completes the proof. ■

## REFERENCES

[1] S. Wu, S. Wei, Y. Wang, R. Vaidy, J. Yuan, "Transmission of partitioning information over non-adaptive multi-access boolean channel," to appear in the Proceedings of 48th Conference on Information Sciences and Systems, Princeton, NJ, March 2014.

[2] R. Gallager, "A perspective on multiaccess channels," *Information Theory, IEEE Transactions on*, vol. 31, no. 2, pp. 124–142, 1985.

[3] B. Hajek, "Information of partitions with applications to random access communications," *Information Theory, IEEE Transactions on*, vol. 28, no. 5, pp. 691–701, 1982.

[4] T. Berger, N. Mehravari, D. Towsley, and J. Wolf, "Random multiple-access communication and group testing," *Communications, IEEE Transactions on*, vol. 32, no. 7, pp. 769–779, 1984.

[5] D. Ding-Zhu and F. K. Hwang, "Combinatorial group testing and its applications," 2000.

[6] M. Malyutov, "Search for sparse active inputs: a review," in *Information Theory, Combinatorics, and Search Theory*. Springer, pp. 609–647, 2013.

[7] N. A. Lynch, *Distributed algorithms*. Morgan Kaufmann, 1996.

[8] C. Xavier and S. S. Iyengar, *Introduction to parallel algorithms*. Wiley. com, 1998.

[9] H. Attiya and J. Welch, *Distributed computing: fundamentals, simulations, and advanced topics*. Wiley. com, 2004.

[10] J. Hromkovic, *Dissemination of information in communication networks: broadcasting, gossiping, leader election, and fault-tolerance*. Springer, 2005.

[11] D. R. Kowalski, "On selection problem in radio networks," in *Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing*. ACM, pp. 158–166, 2005.

[12] N. Pippenger, "Bounds on the performance of protocols for a multiple-access broadcast channel," *Information Theory, IEEE Transactions on*, vol. 27, no. 2, pp. 145–151, 1981.

[13] B. Hajek, "A conjectured generalized permanent inequality and a multiaccess problem," in *Open Problems in Communication and Computation*. Springer, pp. 127–129, 1987.

[14] J. Körner and G. Simonyi, "Separating partition systems and locally different sequences," *SIAM journal on discrete mathematics*, vol. 1, no. 3, pp. 355–359, 1988.

[15] J. Korner and K. Marton, "Random access communication and graph entropy," *Information Theory, IEEE Transactions on*, vol. 34, no. 2, pp. 312–314, 1988.

[16] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *Information Theory, IEEE Transactions on*, vol. 10, no. 4, pp. 363–377, 1964.

[17] A. Dyachkov and V. Rykov, "A survey of superimposed code theory," *Problems of Control and Information Theory*, vol. 12, no. 4, pp. 1–13, 1983.

[18] A. De Bonis and U. Vaccaro, "Constructions of generalized superimposed codes with applications to group testing and conflict resolution in multiple access channels," *Theoretical Computer Science*, vol. 306, no. 1, pp. 223–243, 2003.

[19] A. Sebő, "On two random search problems," *Journal of Statistical Planning and Inference*, vol. 11, no. 1, pp. 23–31, 1985.

[20] H.-B. Chen, F. K. Hwang *et al.*, "Exploring the missing link among d-separable,-separable and d-disjunct matrices," *Discrete applied mathematics*, vol. 155, no. 5, pp. 662–664, 2007.

[21] A. E. Clementi, A. Monti, and R. Silvestri, "Selective families, superimposed codes, and broadcasting on unknown radio networks," in *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, pp. 709–718, 2001.

[22] J. Capetanakis, "Generalized tdma: The multi-accessing tree protocol," *Communications, IEEE Transactions on*, vol. 27, no. 10, pp. 1476–1484, 1979.

[23] J. Komlos and A. G. Greenberg, "An asymptotically fast nonadaptive algorithm for conflict resolution in multiple-access channels," *Information Theory, IEEE Transactions on*, vol. 31, no. 2, pp. 302–306, 1985.

[24] G. K. Atia and V. Saligrama, "Boolean compressed sensing and noisy group testing," *Information Theory, IEEE Transactions on*, vol. 58, no. 3, pp. 1880–1901, 2012.

[25] M. C. Jordan and R. Vaidyanathan, "Mu-decoders: A class of fast and efficient configurable decoders," in *Parallel & Distributed Processing, Workshops and Phd Forum (IPDPSW), 2010 IEEE International Symposium on*. IEEE, 2010.

[26] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[27] R. G. Gallager, "Information theory and reliable communication," 1968.

[28] D. B. West *et al.*, *Introduction to graph theory*. Prentice hall Englewood Cliffs, 2001.

[29] C. Berge and E. Minieka, *Graphs and hypergraphs*. North-Holland publishing company Amsterdam, 1973.

[30] G. Agnarsson and M. M. Halldórsson, "Strong colorings of hypergraphs," in *Approximation and Online Algorithms*. Springer, pp. 253–266, 2005.

[31] M. Yannakakis, "Node-and edge-deletion np-complete problems," in *Proceedings of the tenth annual ACM symposium on Theory of computing*. ACM, pp. 253–264, 1978.

[32] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[33] H. D. NGUYEN, "Generalized binomial expansions and bernoulli polynomials," 2012.

[34] T. Koshy, *Fibonacci and Lucas numbers with applications*. Wiley. com, 2011.

[35] S. Wu, S. Wei, Y. Wang, R. Vaidyanathan and J. Yuan, "Achievable Partition Information Rate over Noisy Multi-Access Boolean Channel", Submitted to IEEE International Symposium on Information Theory, Jan. 2014.