On Secure Exact-Repair Regenerating Codes With a Single Pareto Optimal Point

Fangwei Ye, Member, IEEE, Shiqui Liu, Member, IEEE, Kenneth W. Shum, Senior Member, IEEE, and Raymond W. Yeung, Fellow, IEEE

Abstract—The problem of exact-repair regenerating codes against eavesdropping attack is studied. The eavesdropping model we consider is that the eavesdropper has the capability to observe the data involved in the repair of a subset of \( \ell \) nodes. An \((n, k, d, \ell)\) secure exact-repair regenerating code is an \((n, k, d)\) exact-repair regenerating code that is secure under this eavesdropping model. It has been shown that for some parameters \((n, k, d, \ell)\), the associated optimal storage-bandwidth tradeoff curve, which has one corner point, can be determined. The focus of this paper is on characterizing such parameters. We establish a lower bound \(\ell\) on the number of wiretap nodes, and show that this bound is tight for the case \(k = d = n - 1\).

Index Terms—Secure exact-repair regenerating codes, distributed storage systems, information-theoretic security.

I. INTRODUCTION

Distributed storage systems (DSSs) have been widely researched because of the rapid growth in applications such as data center and cloud network. For data reliability, some redundancy must be added to the system. In the pioneering study [1], Dimakis et al. introduced a new class of codes called regenerating codes, which substantially reduce the amount of data that need to be downloaded during the repair process. In [1], a fundamental tradeoff between the amount of data stored in each node and the repair bandwidth was shown under

Manuscript received May 18, 2018; revised April 29, 2019; accepted August 22, 2019. Date of publication September 19, 2019; date of current version December 23, 2019. This article was presented in part at the On a Simple Characterization of Secure Exact-Repair Regenerating Codes, the IEEE International Symposium on Information Theory, Vail, CO, USA, 2018.

F. Ye was with the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong. He is now with the Department of Electrical and Computer Engineering, Rutgers University—The State University of New Jersey, New Brunswick, NJ 08901-8554 USA (e-mail: fangwei.ye@rutgers.edu).

S. Liu was with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong. She is now with the School of Electronics and Communication Engineering, Sun Yat-sen University, Guangzhou 510006, China (e-mail: liushq27@mail.sysu.edu.cn).

K. W. Shum was with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong. He is now with the School of Science and Engineering, The Chinese University of Hong Kong (Shenzhen), Shenzhen 518172, China (e-mail: wkshum@cuhk.edu.cn).

R. W. Yeung is with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong, and also with the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: whyeung@ie.cuhk.edu.hk).

Communicated by A. Ramamoorthy, Associate Editor for Coding Techniques.

This article has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the authors.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2942315
II. PROBLEM STATEMENT AND KNOWN RESULTS

Following the setting in [1], we assume that there is a secure distributed storage system consisting of $n$ active storage nodes $\mathcal{N} := \{1, 2, \ldots, n\}$ for storing a file $\mathcal{F}$ of $B_i$ message symbols, and each node can store $\alpha$ symbols. When a node fails, a new replacement node with the same storage capacity $\alpha$ connects to any $d \geq k$ nodes chosen from the remaining $n - 1$ nodes and downloads $\beta$ symbols from each of them to regenerate the failed node. Moreover, any legitimate data collector can reconstruct the original file by connecting to any $k$ of the $n$ active nodes. We assume that there exists an eavesdropper Eve who is able to observe the repair data for a subset of nodes with cardinality $\ell (< k)$. It not only can observe the information stored in node $i$ but also all the data transmitted from the other $d$ helper nodes to repair the node $i$ when it fails.

Let $M$ be the uniformly distributed random variable representing the file to be stored in the system. The support set of $M$ is denoted by $\mathcal{M}$, and $B_i = H(M)$. Let $Z$ be a random variable independent on the message variable $M$, called the key, that takes value in an alphabet $\mathcal{Z}$ according to the uniform distribution. As illustrated in Fig. 1, we assume that the message and key are generated at an auxiliary source node and are directly available to all storage nodes in the system. For $i \in \mathcal{N}$, let $W_i$ denote the data stored in the $i$-th node. $S_i^j(D)$ denotes the variable transmitted from node $i$ for repairing the node $j$ for a given set of helper nodes $D \subset \mathcal{N}$, where $|D| = d$ and $i \in D$. $S_i^j(D)$ is defined as a constant for any possible $D$. Denote $\mathcal{W} := \{W_i : i \in \mathcal{N}\}$ and $\mathcal{S} := \{S_i^j(D) : j \in \mathcal{N}, D \subseteq \mathcal{N \setminus \{j\}}, |D| = d, i \in D\}$. Each node has identical storage capacity $\alpha$ and limited transmission bandwidth $\beta$ in repairing any single failure. Thus, assume without loss of generality that each $W_i$ takes value in a common alphabet $\mathcal{W}$ and each $S_i^j(D)$ takes value in a common alphabet $\mathcal{S}$, where $\alpha = \log |\mathcal{W}|$ and $\beta = \log |\mathcal{S}|$. For any set of wiretap nodes $\mathcal{L} \subset \mathcal{N}$ such that $|\mathcal{L}| = \ell$, the information wiretapped by Eve is denoted by $Y_{\mathcal{L}}$, where $Y_{\mathcal{L}}$ is defined as $Y_{\mathcal{L}} := \{S_i^j(D) : j \in \mathcal{L}, D \subseteq \mathcal{N \setminus \{j\}}, |D| = d, i \in D\}$. For any integer $i \leq j \leq n$, denote $[i] := \{1, \ldots, i\}$, and $[i : j] := \{i, \ldots, j\}$.

Next, we formally define a secure distributed storage system based on an exact-repair regenerating code. In the rest of the paper, when we refer to a secure distributed storage system, we always assume that it is based on an exact-repair regenerating code.

**Definition 1.** An $(n, k, d, \ell)$ secure distributed storage system (SDSS) based on an exact-repair regenerating code consists of a set of encoding functions and decoding functions $(F, G, \Phi, \Psi)$, which can be described as follows.

- **Message encoding functions:** $F = \{f_i : i \in \mathcal{N}\}$ is a collection of message encoding functions, where $f_i$ maps the message and key to the information stored in the $i$-th node.
- **Message decoding functions:** $G = \{g_K : K \subset \mathcal{N}, |K| = k\}$ consists of $\binom{n}{k}$ message decoding functions, where $g_K : \mathcal{W}^K \rightarrow \mathcal{M}$

It maps the coded information stored in nodes $i, i \in K$ to the message.

- **Repair encoding functions:** $\Phi = \{\phi_{i,j,D} : j \in \mathcal{N}, i \in D, D \subseteq \mathcal{N \setminus \{j\}}, |D| = d\}$ consists of $n(n-1)\binom{n}{d}$ repair encoding functions, where $\phi_{i,j,D} : \mathcal{W} \rightarrow \mathcal{S}$
maps the coded information in node $i$ to the information transmitted for repairing node $j$ for a given choice of helper nodes set $D$.

- **Repair decoding functions:** $\Psi = \{\psi_{j,D} : j \in \mathcal{N}, D \subseteq \mathcal{N \setminus \{j\}}, |D| = d\}$ consists of $n(n-1)\binom{n-d}{d}$ repair decoding functions, where $\psi_{j,D} : \mathcal{S}^D \rightarrow \mathcal{W}$
maps the information from a set $D$ of help nodes to the information stored in the failed node.

An $(n, k, d, \ell)$ secure distributed storage system is required to satisfy the following criteria:

- **(Reconstruction property)** the file can be retrieved from the contents stored in any $k$ out of $n$ storage nodes:
- $H(M|W_K) = 0, \forall K \subseteq \mathcal{N}, |K| = k$, \hspace{1cm} (1)
where $W_K$ is defined as $W_K := \{W_i : i \in K\}$.

- **(Regeneration property)** any $d$ out of $n-1$ nodes can repair the failed $j$-th node:
- $H\left(W_j|S_i^j(D)\right) = 0, \forall D \subseteq \mathcal{N \setminus \{j\}}, |D| = d, j \in \mathcal{N}$, \hspace{1cm} (2)
where $S_i^j(D) := \{S_i^j(D) : i \in D\}$.

- **(Security condition)**
- $H(M|Y_{\mathcal{L}}) = H(M), \forall \mathcal{L} \subseteq \mathcal{N}, |\mathcal{L}| = \ell$. \hspace{1cm} (3)
Any collection of encoding and decoding functions \(F, G, \Phi, \Psi\) satisfying all these three criteria will naturally induce a secure exact-repair regenerating code associated with the triple \((B_s, \alpha, \beta)\). We can always assume that \(B_s > 0\) because otherwise the code can not be used for storing any information. Under this assumption, we can define the normalized pair \((\tilde{\alpha}, \tilde{\beta})\) by
\[
\tilde{\alpha} := \frac{\alpha}{B_s} \quad \text{and} \quad \tilde{\beta} := \frac{\beta}{B_s}.
\]
A normalized pair \((\tilde{\alpha}, \tilde{\beta})\) is also called an operating point. We may use “the pair” or “the point” interchangeably in the following sections. With the normalized pair \((\tilde{\alpha}, \tilde{\beta})\), we introduce the following definition.

**Definition 2.** A normalized pair \((\tilde{\alpha}, \tilde{\beta})\) is achievable if there exists a secure exact-repair regenerating code that achieves \((\tilde{\alpha}, \tilde{\beta})\). The collection of all achievable pairs \((\tilde{\alpha}, \tilde{\beta})\) is referred to as the zero-error achievable region \(R_{n,k,d,\ell}\).

It follows directly from the definition that if the pair \((\tilde{\alpha}, \tilde{\beta})\) is achievable, then any pair \((\tilde{\alpha}+\delta_1, \tilde{\beta}+\delta_2)\) is also achievable, where \(\delta_1, \delta_2 \geq 0\). Thus, the achievable region can be fully characterized if and only if the boundary is known. To be consistent with the terminology in the literature, we call the collection of points on the boundary the storage-bandwidth tradeoff curve. For a given \(n, k, d, \ell\) secure distributed storage system, its secrecy capacity is defined as the maximum file size \(C_s(\alpha, \beta)\) that can be stored in the system such that \((\alpha/B_s, \beta/B_s)\) is achievable, i.e.,
\[
C_s(\alpha, \beta) := \sup \left\{ B_s : (\alpha/B_s, \beta/B_s) \in R_{n,k,d,\ell} \right\}. \tag{4}
\]

Clearly, determining the secrecy capacity for any given \(\alpha\) and \(\beta\) is equivalent to characterizing the storage-bandwidth tradeoff curve.

In [12], the following point is proved to be achievable for any \((n, k, d, \ell)\)-SDSS:
\[
\left( \frac{d}{\Gamma_{k,d,\ell}}, \frac{1}{\Gamma_{k,d,\ell}} \right) \in R_{n,k,d,\ell}, \tag{5}
\]
where \(\Gamma_{k,d,\ell} := \sum_{i=0}^{k-1} (d-i)\). For notational simplicity, denote
\[
(\hat{\alpha}, \hat{\beta}) := \left( \frac{d}{\Gamma_{k,d,\ell}}, \frac{1}{\Gamma_{k,d,\ell}} \right). \tag{6}
\]

An interesting finding in [17] and [18] is that for some cases, the storage-bandwidth tradeoff curve under the security condition is completely characterized by the single corner point specified in (6), i.e., the achievable rate region is given exactly by
\[
R_{n,k,d,\ell} = \left\{ (\tilde{\alpha}, \tilde{\beta}) : \tilde{\alpha} \geq \hat{\alpha}, \tilde{\beta} \geq \hat{\beta} \right\}. \tag{7}
\]

Subsequently in [19], the first case that the storage-bandwidth tradeoff curve has multiple corner points was found, and a sufficient condition for the number of wiretap nodes was given for the storage-bandwidth tradeoff curve of an SDSS to have a single corner point. In this paper, we will focus on finding parameters \((n, k, d, \ell)\) such that the tradeoff curve has this behavior. Fig. 2 illustrates the optimal storage-bandwidth tradeoff curve for \((7, 6, 6, 1)\) and \((7, 6, 6, 2)\), which has one and two corner points, respectively.

**Remark.** We will prove in Appendix A that the point as defined in (6) must be on the optimal tradeoff curve. Therefore, if the optimal tradeoff curve has only one corner point, then it must be \((\hat{\alpha}, \hat{\beta})\).

In this paper, we focus on the case \(n = d + 1\). After presenting the main results, we will discuss the case \(n > d + 1\) and extend part of the results to the case \(n > d + 1\). We will invoke the setting \(n = d + 1\) from time to time without explicitly mentioning it in the following sections. Under this setting, we can largely simplify the aforementioned notations. When repairing the failed node, all the remaining nodes are helper nodes. Therefore we can drop \(D\) in the notations \(S^j_i(D)\) and \(S^j(D)\). Specifically, we will write \(S^j_i(D)\) as \(S^j_i\) and write \(S^j(D)\) as \(S^j\) because \(D = N \setminus \{j\}\) is implicit. Denote \(S^L := \{S^j : j \in L\}\), and obviously \(S^L\) is identical to \(Y_L\). Then, the regeneration property can be written as
\[
H \left( W_j | S^j \right) = 0, \forall j \in N. \tag{8}
\]

Similarly, we can rewrite the security condition as
\[
H(M | S^L) = H(M), \forall L \subseteq N, |L| = \ell. \tag{9}
\]

We follow the discussion for symmetrical regenerating codes in [3]. A code is said to be a *entropy-symmetrical regenerating code* (or simply symmetrical regenerating code) if for any \(X_A \subseteq W \cup \Phi\) and any permutation \(\pi\) on \(N\), we have \(H(X_A) = H(\pi(X_A))\), where
\[
\pi(X_A) := \{\pi(X_i) : i \in A\}, \quad \pi(X_i) := \begin{cases} W_{\pi(i)}, & \text{if } X_i = W_i, \\ S_{\pi(i)}, & \text{if } X_i = S^j_i. \end{cases}
\]

It has been shown in [18] that assuming that the secure exact-repair regenerating code is symmetrical does not incur any loss of generality when we consider \(R_{n,k,d,\ell}\). Therefore, we
may invoke this symmetrical assumption in our argument without explicitly mentioning it. Under this setting, we can let $H(W_i) = a$ and $H(S_i^j) = \beta$. For notational simplicity, let us define
\[
P := \{ (k, d, \ell) : R_{n,d+1,k,d,\ell} = \{(\bar{a}, \bar{\beta}) : \bar{a} \geq \bar{a}, \bar{\beta} \geq \bar{\beta}\} \}.
\] (10)

Remark. Since $(k, d, \ell = 0) \notin P$ for $k \geq 2$ and $(k = 1, d, \ell = 0) \notin P$ (which can be seen by considering the repetition code), we assume that $\ell \geq 1$ in this paper, so we will invoke the setting $d - 1 \geq k - 1 \geq \ell \geq 1$ from time to time without explicitly mentioning it.

It was first shown that $(k, d, \ell) \in P$ for $d \leq 4$ in [17] and [18]. Subsequently, Shao et al. [19] showed that $(k, d, \ell) \in P$ for $\ell \geq \ell^* := \min\{\ell \geq 1 : \Gamma_{k,d,\ell} \leq d + \sqrt{d\ell}\}$. In this paper, we will give a lower bound $\ell^*$ such that $(k, d, \ell) \in P$ for $\ell \geq \ell^*$, which subsumes all the previous related results [16–19]. Moreover, the given lower bound $\ell^*$ is tight for $k = d$, which means that $(k, d, \ell) \in P$ if and only if $\ell \geq \ell^*$.

III. Main Results

We first present the main results of this paper, and discuss some consequences of the results. The main results of this paper are as follows:

1) For $k = d$, we establish a threshold $\ell^*$ in the following theorem for the number of wiretap nodes for those systems whose optimal tradeoff curve has a single corner.

**Theorem 1.** For any fixed $d$, the triple $(k = d, d, \ell) \in P$ if and only if $\ell \geq \ell^* := \lceil \frac{1}{4}(d - 1) \rceil$.

2) For $k < d$, we obtain a lower bound on the number of wiretap nodes for this single corner point behavior, which is stated in the following theorem.

**Theorem 2.** The triple $(k, d, \ell) \in P$ if $\ell = k - 1$ or
\[
\begin{cases} 
  d(d - \ell - 1) & \geq 0, \quad \ell \leq k - 4, \\
  k \geq \frac{4}{d}(d + 8), & \ell = k - 3, \\
  k \geq \frac{4}{d}(d + 7), & \ell = k - 2. 
\end{cases}
\] (11)

The two theorems are established under the assumption $n = d + 1$. In particular, we can prove the two outer bounds $\bar{a} \geq \bar{a}$ and $\bar{\beta} \geq \bar{\beta}$ for any $(n = d + 1, k, d, \ell)$ such that $(k, d, \ell)$ satisfies the conditions given in two theorems, i.e., $\ell \geq \lceil \frac{1}{4}(d - 1) \rceil$ for $k = d$ or (11) for $k < d$. Now, we claim that these two outer bounds also holds for any $(n, k, d, \ell)$ such that $n > d + 1$ if $(k, d, \ell)$ satisfies the same conditions. The reason is that any $(n, k, d, \ell)$ system contains an $(n' = d + 1, k, d, \ell)$ sub-system, and the sub-system must satisfy the same outer bounds $\bar{a} \geq \bar{a}$ and $\bar{\beta} \geq \bar{\beta}$, which are naturally valid outer bounds for $(n, k, d, \ell)$.

Note that $\hat{a}$ and $\hat{\beta}$ are independent of $n$ (recall that $\hat{a} = d\hat{\beta} = d/\sum_{i=0}^{k}(\ell + 1)(d + 1 - i)$), and we know from [12] that $(\hat{a}, \hat{\beta})$ is achievable for any $(n, k, d, \ell)$. Hence, we know that $R_{n,k,d,\ell} = \{(\bar{a}, \bar{\beta}) : \bar{a} \geq \bar{a}, \bar{\beta} \geq \bar{\beta}\}$ if $(k, d, \ell)$ satisfies the conditions in Theorem 1 or Theorem 2. In other words, if $(k, d, \ell) \in P$, that is the optimal tradeoff curve for $(n' = d + 1, k, d, \ell)$ has a single corner point, then the optimal tradeoff curve for $(n, k, d, \ell)$ also has a single corner point. This is stated in the following corollary.

**Corollary 1.** If $(k, d, \ell) \in P$, then $(n, k, d, \ell) \in P_n$ for any $n \geq d + 1$, where
\[
P_n := \left\{ \left( n, k, d, \ell \right) : R_{n,k,d,\ell} = \left\{ \left( \bar{a}, \bar{\beta} \right) : \bar{a} \geq \bar{a}, \bar{\beta} \geq \bar{\beta} \right\} \right\}.
\]

Before proceeding to the proof, we first discuss some consequences of the theorems, and compare with the best known results in [19].

1) It was shown in [19] that if $\ell \geq \ell^* = \lceil (\sqrt{d} - 1) \rceil$, then $(k = d, d, \ell) \in P$. We can see that when $d$ is large, $\ell^*$ goes to $d$. However, Theorem 1 indicates that the threshold $\ell^*$ is strictly bounded away from $d$, and when $d$ is large, $\ell^* \sim \ell^*/4$. Thus, our bound not only is a significant improvement over the previous bound but also tight.

2) Though the formula in (11) is complicated, we can show that if $(k, d, \ell) \in P$, then $(k, d, \ell + 1) \in P$. In other words, for any fixed $k$ and $d$, there exists a lower bound $\ell^*$ such that $(k, d, \ell) \in P$ for $\ell \geq \ell^*$. Also, we can show that for any $k$ and $d$, the lower bound $\ell^*$ induced from Theorem 2 supersedes the result in [19], that is, $\ell \leq \ell^* = \min\{\ell \geq 1 : \Gamma_{k,d,\ell} \leq d + \sqrt{d\ell}\}$. See details in Appendix B. Instead of presenting details here, we give an example to illustrate the gap between $\ell$ in Theorem 2 and $\ell^*$ in [19].

**Example 1.** Consider the example $d = 32$ and $k = 31$. We can check that the first case in (11) is satisfied for $\ell = 12$, but is not satisfied for $\ell = 11$, so we obtain $\ell = 12$. Also, by substituting by substituting $k = 31$ and $d = 32$ in $\ell^*$, we have
\[
\ell^* = \min\left\{ \ell \geq 1 : \frac{1}{2}(31 - \ell)(34 - \ell) \leq 32 + 32\ell \right\}.
\]

Since the condition $\frac{1}{2}(31 - \ell)(34 - \ell) \leq 32 + 32\ell$ is satisfied for $\ell = 22$ but not for $\ell = 21$, we obtain $\ell^* = 22$. Therefore, we can see that there is a gap between $\ell$ and $\ell^*$, and this gap can be large.

To facilitate our discussion, we have some preparations. First, consider any subset $\mathcal{S}$ of $\mathcal{W} \cup \mathcal{P}$ such that $H(W_k | T) = 0$. Then by the reconstruction property (1) and security constraint (9), we can obtain an upper bound on $B_s$ as follows:
\[
B_s = H(M) - H(M | S^C) - H(M | T, S^C) = I(M; T | S^C) \leq H(T | S^C).
\] (12)

By letting $T = \{ S_j^i : j < i \leq n, 1 \leq j \leq k \}$ and $L = \{1, \ldots, \ell\}$, we can obtain the upper bound in [11]:
\[
B_s \leq \sum_{i=\ell}^{k-1} (d - i)\beta,
\] (13)
which can also be written as $\hat{\beta} \geq \hat{\beta}$. Since $\hat{\beta} \geq \hat{\beta}$ and $(\hat{a}, \hat{\beta}) \in R_{n,k,d,t}$ for any $(n, k, d, \ell)$-SDSS, the triple $(k, d, \ell) \in \mathcal{P}$ if and only if $\hat{a} \geq \hat{a}$, or equivalently
\[
B_s \leq \frac{\Gamma_{k,d,\ell}}{d} a. \quad (14)
\]

Therefore, we will prove that $B_s \leq \frac{\Gamma_{k,d,\ell}}{d} a$ for $\ell \geq \hat{\ell}$ for both theorems to conclude that $(k, d, \ell) \in \mathcal{P}$ for $\ell \geq \hat{\ell}$. On the other hand, to prove the ‘only if’ part of Theorem 1, we will show that if $\ell < \hat{\ell}$, then there exists one achievable point $(\hat{a}, \hat{\beta})$ such that $\hat{a} < \hat{a}$, which implies that $(k, d, \ell) \notin \mathcal{P}$.

Since Han’s inequality together with the symmetry will be invoked in following sections from time to time, we introduce a set of problem-specific inequalities stated in the next lemma by slightly modifying the well-known Han’s inequality in [20] (see also [21, p.47]).

**Lemma 2.** For a subset $\mathcal{R} = \{1, \ldots, r\}$ of $\mathcal{N} = \{1, 2, \ldots, n\}$, let
\[
h_r = \frac{H(S_{\mathcal{R}}^n)}{r}.
\]
Then we have
\[
h_1 \geq h_2 \geq \cdots \geq h_{n-1}.
\]

**Proof.** The lemma can be obtained directly by invoking the symmetry in Han’s inequality as follows:

\[
h_r = \frac{H(S_{\mathcal{R}}^n)}{r} = \begin{cases}
\frac{1}{(r-1)!} \sum_{A \subset \mathcal{R}, |A|=r} H(S_A^n) & \text{if } (a) \\
\frac{1}{(r-1)!} \sum_{B \subset \mathcal{N} \setminus \mathcal{R}, |B|=r-1} H(S_B^n) & \text{if } (b) \\
\end{cases}
\]

where (a) follows because of the symmetry and (b) follows from Han’s inequality.

**Remark.** The lemma still holds if $h_r$ is defined by $\frac{1}{r} H(S_{\mathcal{R}}^n)$, so we may also apply
\[
\frac{H(S_{\mathcal{R}}^n)}{r} \leq \frac{H(S_{\mathcal{R}}^{n-1})}{r-1}
\]
in the following sections. Since the proof is exactly the same, we omit the details here.

**IV. PROOF OF THEOREM 1**

In this section, we will invoke the setting $k = d = n - 1$ from time to time without explicitly mentioning it. Before presenting the details, we first outline the proof.

In Subsection IV-A, we will show that if $\ell < \hat{\ell}$, then there exists one achievable point $(\hat{a}, \hat{\beta})$ such that $\hat{a} < \hat{a}$, which implies that $(k, d, \ell) \notin \mathcal{P}$. The proof of the achievability of this point is largely borrowed from a code construction in [9].

To prove that $(k, d, \ell) \in \mathcal{P}$ for $\ell \geq \hat{\ell}$, we only need to show (14) for $\ell \geq \hat{\ell}$. By letting $T = W[k]$ and $L = \{1, \ldots, \ell\}$ in (12), we see that the secrecy capacity $B_s$ is upper bounded by
\[
B_s \leq H \left( W[k] \mid S[\ell] \right) = H \left( W[\ell+1:k] \mid S[\ell] \right). \quad (15)
\]

Thus, it is sufficient for us to prove that
\[
H \left( W[\ell+1:k] \mid S[\ell] \right) \leq \frac{\Gamma_{k,d,\ell}}{d} a,
\]
for $\ell \geq \hat{\ell}$. This will be proved by induction on $\ell$ in Subsection IV-B.

**A. $\ell < \hat{\ell}$ Imply That $(k, d, \ell) \notin \mathcal{P}$**

We first roughly review the code construction for $(n, k, d, \ell = 0)$ exact-repair regenerating codes with $k = d = n - 1$ in [9], where the code construction is based on duplicated combination block design. Considering a block design over the domain (node index) $\mathcal{N} = \{1, \ldots, n\}$, the design can be viewed as an exhaustive list of all $r$-combinations ($n \geq r$) of $\mathcal{N}$. Each block forms a $(r, r-1)$ erasure code, and symbols in different blocks are independent.

In particular, we consider block size $r = 3$ in this subsection. We have a design $C(r,n) = \{B_1, \ldots, B_n\}$, where each block $B_i$ is a unique $3$-subset of $\mathcal{N}$ and $m = \binom{n}{3}$. For each $3$-subset $B_i = \{b_{i1}, b_{i2}, b_{i3}\}$, let $X_i$ and $Y_i$ be independent random variables uniformly on a sufficient large field $\mathbb{F}$, and we consider a corresponding vector for each $B_i$ such that $b_i = (b_{i1}, b_{i2}, b_{i3})$ where $1 \leq b_{i1} < b_{i2} < b_{i3} \leq n$. Then, the encoding is as the following:

- $X_i$ is stored in node $b_{i1}$;
- $Y_i$ is stored in node $b_{i2}$;
- $X_i + Y_i$ is stored in node $b_{i3}$.

Let $X_i$ and $X_j$ ($Y_i$ and $Y_j$) be independent random variables for $i \neq j$. We can see that in this construction,
\[
\alpha = \binom{n-1}{2}, \quad \beta = n - 2, \quad B_s = 2^{\binom{n-1}{3}},
\]
and hence
\[
(\alpha, \beta) = \left( \binom{n-1}{2}, \binom{n-1}{3}, \binom{n-1}{2} \right) \in \mathcal{R}_{d+1,d,d,0}.
\]

See more details in [9].

Therefore, following the same argument in [22], we know that there exists an $(n, k = n - 1, d = n - 1, \ell)$ secure exact-repair regenerating code with $\alpha = \binom{n-1}{2}$, $\beta = n - 2$ and $B_s = 2^{\binom{n-1}{3}}$ if the field size is large enough, and so
\[
(\hat{a}, \hat{\beta}) = \left( \binom{n-1}{2}, \binom{n-1}{3}, \binom{n-1}{2} \right) \in \mathcal{R}_{d+1,d,d,\ell}.
\]

If an integer $\ell$ satisfying that $\ell < \hat{\ell} = \lceil \frac{1}{4} (d-1) \rceil$, we have $\ell < \frac{1}{4} (d-1) = \frac{1}{4} (n-2)$. As such, we have
\[
\tilde{a} - \hat{a} = \frac{n-1}{2(n-3)} - \frac{n-1}{2(n-2)} = -\frac{4\ell + 2 - n(n-1)}{2(n-\ell)(n-\ell-1)(n-\ell-2)} < 0.
\]
Therefore, we know that if \( \ell < \hat{\ell} \), there exists one achievable point \((\hat{\alpha}, \hat{\beta})\) such that \( \hat{\alpha} - \hat{\alpha} < 0 \), which substantiates that if \( \ell < \hat{\ell} \) then \((k, d, \ell) \not\in \mathcal{P}\).

B. \( \ell \geq \hat{\ell} \) Implies That \((k, d, \ell) \in \mathcal{P}\)

In this subsection, we will show that

\[
H\left(W[\ell+1:k]|S[\ell]\right) \leq \frac{\Gamma_{k,d,\ell}}{d} a,
\]

for \( \ell \geq \hat{\ell} \) by induction. For any subset \( \mathcal{A} \subseteq \mathcal{N} \), denote \( S^\mathcal{A} := \{ S^i : j \in \mathcal{A} \}, i \mathcal{A} := \{ S^i : j \in \mathcal{A} \}, i \mathcal{A} := \{ S^i : i, j \in \mathcal{A} \}, i > j \}.

**Proposition 1.** For \( k = d \), if \( T \subseteq \mathcal{W} \cup \mathcal{Y} \) satisfies 

\[
H\left(W[k]|T\right) = 0,
\]

then 

\[
H(T) = H\left(W[k]\right).
\]

**Proof.** Since \( k = d \), \( W[k] \) can determine any subsets of \( \mathcal{W} \cup \mathcal{Y} \), and so \( H\left(W[k]\right) \geq H(T) \). From \( H\left(W[k]|T\right) = 0 \), we have \( H\left(W[k]\right) \leq H(T) \), and hence \( H(T) = H\left(W[k]\right) \).

The following lemma gives a class of upper bounds on \( H\left(W[\ell+1:k]|S[\ell]\right) \).

**Lemma 3.** For any \((n = d + 1, k = d, d, \ell)\) secure exact-repair regenerating codes, we have

\[
H\left(W[\ell+1:k]|S[\ell]\right) \leq \frac{d + 1 - t}{3} a - \frac{d + 1 - t}{3} H\left(S[\ell]\right) + \frac{d + 1 - t}{6} H\left(S[\ell+1]|S[\ell]\right) - \frac{\ell - 1}{i = t + 1} \sum H\left(S^i|S[i-1]\right),
\]

for any \( t = 0, \ldots, \ell - 1 \).

**Proof.** See Appendix C.

Since \( \ell \geq 1 \), there always exists an upper bound on \( H\left(W[\ell+1:k]|S[\ell]\right) \) for \( t = 0 \). When \( t = 0 \), \( S[\ell] \) is regarded as a constant. For notational simplicity, denote the right-hand side of (17) by \( f(d, \ell, t) \), where \( t = 0, \ldots, \ell - 1 \). Then the following proposition is immediate.

**Proposition 2.** For any \((n = d + 1, k = d, d, \ell)\) secure exact-repair regenerating codes,

\[
H\left(W[\ell+1:k]|S[\ell]\right) \leq \sum_{i = 0}^{\ell - 1} \mu_t f(d, \ell, t),
\]

for any \( \mu_t = (\mu_0, \ldots, \mu_{\ell - 1}) \) such that

\[
\sum_{i = 0}^{\ell - 1} \mu_t = 1,
\]

and 

\[
\mu_t \geq 0, \quad t = 0, \ldots, \ell - 1.
\]

With these preparations, we start to prove that

\[
H\left(W[\ell+1:k]|S[\ell]\right) \leq \frac{\Gamma_{k,d,\ell}}{d} a
\]

for \( \ell \geq \hat{\ell} \) by induction on \( \ell \).

First, for the base case \( \ell = \hat{\ell} \), (19) becomes

\[
H\left(W[\ell+1:k]|S[\ell]\right) \leq \frac{\Gamma_{k,d,\ell}}{d} a.
\]

From Proposition 2, we know that

\[
H\left(W[\ell+1:k]|S[\ell]\right) \leq \sum_{i = 0}^{\ell - 1} \mu_t f(d, \ell, t),
\]

for any \( \mu_t \) satisfying

\[
\sum_{i = 0}^{\ell - 1} \mu_t = 1,
\]

and

\[
\mu_t \geq 0, \quad t = 0, \ldots, \ell - 1.
\]

Clearly, the chosen coefficients should induce the upper bound

\[
\sum_{i = 0}^{\ell - 1} \mu_t f(d, \ell, t) \leq \frac{\Gamma_{k,d,\ell}}{d} a.
\]

Note that since \( f(d, \ell, t) \) is a linear combination of \( \alpha \), \( H(S[i]|S[i-1]) \) and \( \left\{ H(S[i]|S[i-1]) : i = t + 1, \ldots, \ell \right\} \) for each \( t \), the convex combination \( \sum_{i = 0}^{\ell - 1} \mu_t f(d, \ell, t) \) can be written as a linear combination of \( \alpha \), \( \left\{ H(S[i]|S[i-1]) : i = t + 1, \ldots, \ell \right\} \) and \( \left\{ H(S[i]|S[i-1]) : i = 1, \ldots, \ell \right\} \). Roughly speaking, we need to find coefficients \( \mu_t \) such that all terms \( \left\{ H(S[i]|S[i-1]) : i = 1, \ldots, \ell \right\} \) cancel with each other, as the upper bound should only be related to \( \alpha \). In particular, we can let

\[
\mu_t = \left\{ \begin{array}{ll}
\frac{1}{2} \left( n^{\ell - 1} \right), & 1 \leq t \leq \ell - 3, \\
\frac{(n - \ell + 3)}{(n - \ell + 1)} & \ell - 2, \ell - 3, \\
\frac{n - \ell + 1}{n - \ell}, & \ell - 1, \ell - 2,
\end{array} \right.
\]

and

\[
\mu_0 = 1 - \sum_{j = 1}^{\ell - 1} \mu_j.
\]

We first verify that for this choice of \( \mu_t \), both (21) and (22) are satisfied in the following proposition.

**Proposition 3.** \( \mu_t = (\mu_0, \ldots, \mu_{\ell - 1}) \) as defined in (23) and (24) satisfies

\[
\sum_{i = 0}^{\ell - 1} \mu_t = 1,
\]

and

\[
\mu_t \geq 0, \quad t = 0, \ldots, \ell - 1.
\]

**Proof.** See Appendix D-A.

It remains to show that

\[
\sum_{i = 0}^{\ell - 1} \mu_t f(d, \ell, t) \leq \frac{\Gamma_{k,d,\ell}}{d} a.
\]
Towards this end, consider

\begin{equation}
\sum_{i=0}^{t-1} \mu_i f(d, \hat{\ell}, t)
= \sum_{i=0}^{t-1} \mu_i \left( \frac{d + 1 - t}{3} \alpha - \frac{d + 1 - t}{3} H \left( S^{[t]}_n \right) \right)
+ \sum_{i=0}^{t-1} \frac{d + 1 - t}{6} \mu_i H \left( S^{[t]}_n \right)
- \sum_{i=0}^{t-1} \mu_i \sum_{j=0}^{t} H \left( S^{[t+j]}_n \right),
\end{equation}

where in the last step we replace \( i \) by \( t + 1 \) and \( t \) by \( j \).

By letting

\[ b_t = \frac{n - t}{3} \mu_t, \]

and

\[ c_t = \frac{n - t}{6} \mu_t - \sum_{j=0}^{t} \mu_j, \]

we obtain

\begin{equation}
\sum_{i=0}^{t-1} \mu_i f(d, \hat{\ell}, t)
\leq \left( \sum_{i=0}^{t-1} b_t \right) \alpha - \sum_{i=0}^{t-1} b_i H \left( S^{[t]}_n \right) + \sum_{i=0}^{t-1} c_t H \left( S^{[t]}_n \right) + \sum_{i=0}^{t-1} H \left( S^{[t]}_n \right).
\end{equation}

For \( \hat{\ell} \geq 2 \), (25) can be written as

\begin{equation}
\sum_{i=0}^{t-1} \mu_i f(d, \hat{\ell}, t)
\leq \left( \sum_{i=0}^{t-1} b_t \right) \alpha - \sum_{i=0}^{t-1} b_i H \left( S^{[t]}_n \right) + \sum_{i=0}^{t-1} c_t H \left( S^{[t]}_n \right) + \sum_{i=0}^{t-1} H \left( S^{[t]}_n \right).
\end{equation}

Proposition 4. For \( \hat{\ell} \geq 2 \), \( c_t \geq 0 \) for \( t = 0, \ldots, \hat{\ell} - 1 \), and \( c_{\hat{\ell} - 1} = 0 \).

Proof. See Appendix D-B.

Since

\[ H \left( S^{[t]}_n \right) = H \left( \frac{S^{[t+j]}_n}{S^{[t]}_n} \right) \]

\[ \leq \sum_{j=t+2}^{n} H \left( \frac{S^{[t+j]}_n}{S^{[t]}_n} \right) \]

\[ \leq \sum_{j=t+2}^{n} \left( d - t \right) H \left( S^{[t]}_n \right), \]

where (a) follows from the symmetry, we can further bound (26) as follows:

\begin{equation}
\sum_{i=0}^{t-1} \mu_i f(d, \hat{\ell}, t)
\leq \left( \sum_{i=0}^{t-1} b_t \right) \alpha - \sum_{i=0}^{t-1} b_i H \left( S^{[t]}_n \right) + c_t H \left( S^{[t]}_n \right) + \sum_{i=0}^{t-1} H \left( S^{[t]}_n \right).
\end{equation}

We separately discuss the case \( \hat{\ell} = 1 \) here. When \( \hat{\ell} = 1 \), clearly we have \( \mu_0 = 1 \), and then (25) becomes

\[ f(d, \hat{\ell}, t = 0) \leq b_0 \alpha + c_0 H \left( S^{[1]}_n \right) = \frac{n}{3} \alpha + \left( \frac{n - 6}{6} \right) H \left( S^{[1]}_n \right). \]

Since \( \hat{\ell} = \left\lceil \frac{1}{4} (d - 1) \right\rceil = \left\lceil \frac{1}{4} (n - 2) \right\rceil = 1 \), we know that \( n \leq 6 \), and then we have

\[ f(d, \hat{\ell}, t = 0) \geq \frac{n}{3} \alpha + \left( \frac{n - 6}{6} \right) \alpha = \frac{1}{2} (n - 2) \alpha = \Gamma_d, d \geq 1, \]

where (a) follows because \( H(S^{[1]}_n) \geq H(W_1) = \alpha \). We have completed the proof for \( \hat{\ell} = 1 \).
\[ \begin{align*}
&\frac{\hat{c}_{\ell-1}}{d} + \sum_{t=2}^{\ell-1} (c_{t-1}(d-t+1) - c_1(d-t) - b_1) H\left(S_n^1\right) \\
&\leq (b) \left( \sum_{t=0}^{\ell-1} b_t - b_1 \beta + c_0 d \beta - c_1(d-1) \beta \right) \\
&+ \sum_{t=2}^{\ell-1} (c_{t-1}(d-t+1) - c_1(d-t) - b_1) H\left(S_n^1\right),
\end{align*} \]

where \( (a) \) follows from \( \hat{c}_{\ell-1} = 0 \), and \( (b) \) follows because \( c_0 \geq 0 \) and \( H\left(S^1\right) \leq d \beta \). By letting

\[ T_1 = \sum_{t=0}^{\ell-1} b_t, \]
\[ T_2 = b_1 - c_0 d + c_1(d-1), \]

and

\[ \lambda_t = c_{t-1}(d+1-t) - c_1(d-t) - b_t, \quad t = 2, \ldots, \ell - 1, \]
we have

\[ \sum_{t=0}^{\ell-1} \mu_t f(d, \hat{\ell}, t) \leq T_1 \alpha - T_2 \beta - \sum_{t=2}^{\ell-1} \lambda_t H\left(S_n^1\right). \]

**Proposition 5.** For \( \hat{\ell} \geq 3 \), \( \lambda_t = 0 \) for \( t = 2, \ldots, \ell - 1 \).

*Proof.* See Appendix D-C.

From Proposition 5, we obtain

\[ \sum_{t=0}^{\ell-1} \mu_t f(d, \hat{\ell}, t) \leq T_1 \alpha - T_2 \beta. \]

**Proposition 6.** \( T_2 \geq 0 \), \( T_1 - \frac{T_2}{d} = \frac{\Gamma_{k,d}}{d^2} \).

*Proof.* See Appendix D-D.

Finally, we can substitute that

\[ \sum_{t=0}^{\ell-1} \mu_t f(d, \hat{\ell}, t) \leq T_1 \alpha - T_2 \beta \leq T_1 \alpha - \frac{T_2}{d} = \frac{\Gamma_{k,d,\hat{\ell}}}{d^2} \alpha, \]

where \( (a) \) follows from \( \lambda_t \geq \alpha \). Therefore, the base case holds, that is,

\[ H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \leq \frac{\Gamma_{k,d,\hat{\ell}}}{d^2} \alpha. \]

Now, we start the inductive step to show that for any \( \ell \geq \hat{\ell} + 1 \), if \( H\left(W_{[k:k]}|S^{[k-1]}\right) \leq \frac{\Gamma_{k,d,k-1}}{d} \alpha \), then

\[ H\left(W_{[\ell+1:k]}|S^{[\ell-1]}\right) \leq \frac{\Gamma_{k,d,\ell-1}}{d} \alpha. \]

First, assume that

\[ H\left(W_{[\ell:k]}|S^{[\ell-1]}\right) \leq \frac{\Gamma_{k,d,\ell-1}}{d} \alpha, \tag{28} \]

for some \( \ell \geq \hat{\ell} + 1 \).

Then, consider

\[ H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \]
\[ = H\left(W_{[\ell+1:k]}, S^{[\ell]}\right) - H\left(S^{[\ell]}\right) \]
\[ \leq H\left(W_{[\ell:k]}, S^{[\ell-1]}\right) - H\left(S^{[\ell-1]}\right) \]
\[ = H\left(W_{[\ell:k]}|S^{[\ell-1]}\right) - H\left(S^{[\ell]}|S^{[\ell-1]}\right) \]
\[ \leq \frac{\Gamma_{k,d,\ell-1}}{d} \alpha - H\left(S^{[\ell]}|S^{[\ell-1]}\right), \tag{29} \]

where \( (a) \) follows from Proposition 1, and \( (b) \) follows from (28). Also, we have

\[ H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \]
\[ \leq H\left(S^{[\ell+1:k]}|S^{[\ell]}\right) \]
\[ = \sum_{i=\ell+1}^{k} H\left(S_i^{[\ell]}|S_i^{[\ell-1]}\right) \]
\[ \leq \sum_{i=\ell+1}^{k} (n-i) H\left(S_i^{[\ell]}|S_i^{[\ell-1]}\right) \]
\[ = \left( \sum_{i=\ell+1}^{k} H\left(S_i^{[\ell]}\right) \right) - (n-\ell-1) H\left(S_n^{[\ell]}\right), \tag{30} \]

where \( (a) \) follows from (27). Moreover, the following lemma gives another upper bound on \( H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \).

**Lemma 4.** For any \( (n = d + 1, k = d, \ell) \) secure exact-repair regenerating codes, we have

\[ H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \]
\[ \leq \frac{1}{2}(k - \ell + 1) \alpha - \frac{1}{2} \sum_{i=\ell+1}^{k-1} H\left(S_i^{[\ell]}\right) \]
\[ + \frac{1}{4}(k - \ell - 2) H\left(S_n^{[\ell]}\right). \tag{31} \]

*Proof.* The lemma can be proved by modifying the proof of Lemma 3. See details in Appendix E. \( \square \)

Now we have three upper bounds on \( H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \). Similar to what we did in the previous subsection, we will take a particular convex combination of (29), (30) and (31) to obtain the desired upper bound on \( H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \). Denote the coefficients associated with (29), (30) and (31) by \( \nu_1 \), \( \nu_2 \) and \( \nu_3 \).

If \( \ell = k - 1 \), from (30), we obtain

\[ H\left(W_k|S^{[k-1]}\right) \leq H(S_k^{[k]}|S_n^{[k-1]}|S^{[k-1]}) \leq \frac{1}{k} H(S_k^{[k]}) \]
\[ \leq \frac{1}{k} \alpha = \frac{\Gamma_{d,d,d-1}}{d} \alpha. \]

Hence, by letting \( \nu_2 = 1 \) and \( \nu_1 = \nu_3 = 0 \), we obtain that

\[ H\left(W_{[\ell+1:k]}|S^{[\ell]}\right) \leq \frac{\Gamma_{k,d,\ell}}{d} \alpha, \]

for \( \ell = k - 1 \).
For \( \ell \leq k - 2 \), let
\[
\begin{align*}
v_1 &= \frac{(k - \ell - 2)(n - \ell - 1)}{4(n - 1) + (n - \ell + 1)(k - \ell - 2)}, \\
v_2 &= \frac{(n - \ell - 1)}{4(n - 1) + (n - \ell + 1)(k - \ell - 2)}, \\
v_3 &= \frac{4(n - \ell - 1)}{4(n - 1) + (n - \ell + 1)(k - \ell - 2)}.
\end{align*}
\]
and
\[
\begin{align*}
v_1 + v_2 + v_3 &= 1.
\end{align*}
\]
Finally, by substituting \( v_1, v_2 \) and \( v_3 \), we have
\[
\begin{align*}
H \left( W_{(\ell+1):k} | S^{(\ell)} \right)
&\leq v_1 \left( \frac{\Gamma_{k,d\ell-1}}{d} \right) + H \left( S^{(\ell+1)} - H \left( S^{(\ell+1)} \right) \right) + v_2 \left( \sum_{i=\ell+1}^{k} H \left( S^{(i)}_n \right) \right) \\
&\quad - v_2(n - \ell - 1) H \left( S^{(\ell)}_n \right) + \frac{v_3}{2} (k - \ell + 1) \nu
\end{align*}
\]
\[
\begin{align*}
&= v_2 H \left( S^{(k)}_n \right) + \left( v_2 - \frac{v_3}{2} \right) \left( \sum_{i=\ell+1}^{k-1} H \left( S^{(i)}_n \right) \right) \\
&\quad - \left( v_2(n - \ell - 1) + \frac{v_3}{2} \right) H \left( S^{(\ell)}_n \right) - \frac{v_3}{2} H \left( S^{(\ell+1)} \right)
\end{align*}
\]
\[
\begin{align*}
&\leq \left( \frac{k}{\ell} - 1 \right) v_2(n - \ell - 1) + \frac{v_3}{2} - \frac{v_3}{2} \left( \frac{k}{\ell} - 1 \right) H \left( S^{(\ell)}_n \right)
\end{align*}
\]
\[
\begin{align*}
&+ \left( v_2 - \frac{v_3}{2} \right) \sum_{i=\ell+1}^{k-1} \frac{i}{\ell} H \left( S^{(i)}_n \right)
\end{align*}
\]
\[
\begin{align*}
&\leq 0,
\end{align*}
\]
where (a) follows from Lemma 2 and \( v_2 - \frac{v_3}{2} \geq 0 \) for \( \ell \geq 1 \), and (b) can be justified by substituting \( v_2 \) and \( v_3 \).

V. PROOF OF THEOREM 2

A. Our Approach

By letting \( K = [k] \) and \( L = [\ell] \) in (12), we obtain that for any given \( d, k \) and \( \ell \), the secrecy capacity \( B_s \) is upper bounded by
\[
B_s \leq H \left( T | S^{(\ell)} \right),
\]
for any \( T \) such that \( H \left( W_{(k)\mid T} \right) = 0 \).

Similar to what we did in the last section, we will select \( T \) in different ways to obtain a number of upper bounds on \( B_s \), and then take a convex combination of them to derive an upper bound that depends only on \( \alpha \). Consider any set of variables \( T = \{ S^{(\ell)} \} \cup \{ X_y : y = \ell + 1, \ldots, k \} \), where \( X_y \) can either be \( W_y \) or \( S^y \). Then
\[
B_s \leq \sum_{y=\ell+1}^{k} H \left( X_y | S^{(\ell)}, X_{(\ell+1:y-1)} \right). \tag{32}
\]
We can use a \((k-\ell)\)-length binary vector \( q := (q_{\ell+1}, \ldots, q_{k}) \) to represent the choices of \( X_y, \ell + 1 \leq y \leq k \), where
\[
q_y = \begin{cases}
0, & \text{if } X_y = W_y, \\
1, & \text{if } X_y = S^y.
\end{cases} \tag{33}
\]

Clearly, each possible \( q \) induces an upper bound on \( B_s \).

By symmetry we know that \( H \left( X_y | S^{(\ell)}, X_{(\ell+1:y-1)} \right) \) depends on \( \{q_{\ell+1}, \ldots, q_{k}\} \) only through \( q_y \) and \( \sum_{i=\ell+1}^{y-1} q_i \). Hence, we have
\[
H \left( X_y | S^{(\ell)}, X_{(\ell+1:y-1)} \right) = H \left( X_y | S^{(\ell)}, W_{(\ell+1:y-1)} \right), \tag{34}
\]
where
\[
t_y = \ell + \sum_{i=\ell+1}^{y-1} q_i. \tag{35}
\]

The following lemma gives upper bounds on \( H \left( W_{(\ell)\mid \ell+1:y-1} \right) \)
\[H \left( S^y | S^{(\ell)}, W_{(\ell+1:y-1)} \right), \tag{36}\]
for \( t_y = \ell, \ldots, y - 1, \) and
\[
H \left( W_{(\ell)\mid \ell+1:y-1} \right) \leq \frac{d+1-y}{d-t_y} H \left( S^{\ell+1} \right) \tag{37}\]

Proof. See Appendix F. \( \square \)

By combining (32), (34), (36) and (37), we can obtain an upper bound on \( B_s \) for any given \( q \). By examining (36) and (37), we see that the right-hand sides of them may contain the terms \( \alpha, H \left( S^y | S^{(\ell+1)} \right) \) for \( j = \ell, \ldots, k \), and \( H \left( S^{(\ell)}_n \right) \) for \( j = \ell, \ldots, k-1 \). Hence, let us specify the mapping \( f \) from any \((k-\ell)\)-length binary vector to the corresponding upper bound, which can be written as
\[
f \left( q \right) = \left( \sum_{j=\ell}^{k-1} v_j q_j \right) \alpha - \sum_{j=\ell}^{k-1} v_j H \left( S^{(j)}_n \right) + \sum_{j=\ell}^{k-1} \mu_j H \left( S^{(j+1)} \right), \tag{38}\]
where \( v_j \) and \( \mu_j \) can be determined by the given \( q \). Note that from (37) we know that the coefficient of \( \alpha \) can be determined by the sum of the coefficients of \( H \left( S^{(j)}_n \right) \) for \( j = \ell, \ldots, k-1 \).

Furthermore, we consider an \( m \times (k-\ell) \) binary matrix
\[
Q = \begin{bmatrix}
q_1 & q_2 & \cdots & q_{k-1} \\
\vdots & \vdots & \ddots & \vdots \\
q_{m \ell+1} & q_{m \ell+2} & \cdots & q_{m \ell+k}
\end{bmatrix}, \tag{39}
\]
where each \( q_x, 1 \leq x \leq m \) is some binary row vector defined in (33), and the first column of \( Q \) is labeled by the index
\[ f(Q) = \sum_{i=\ell}^{k+1} f(q_i) \]
\[ = \sum_{i=\ell}^{k+1} q_{x,i} \]
\[ + \sum_{i=\ell+1}^{k+1} q_{x,i} \]

\[ \text{For each } q_i, \text{ we can obtain from (38) the upper bound} \]
\[ f(q_i) = \alpha \sum_{j=\ell}^{k-1} q_{x,j} - \sum_{j=\ell}^{k+1} q_{x,j} H \left( S_{n}^{j+1} \right) \]
\[ + \sum_{j=\ell}^{k} \mu_{x,j} H \left( S_{n}^{j+1} \right) \]

\[ \text{With a slight abuse of notations, we write} \]
\[ f(Q) = \sum_{i=\ell}^{k} f(q_i) \]
\[ = \alpha \sum_{j=\ell}^{k} \sum_{i=\ell}^{k} q_{x,j} - \sum_{j=\ell}^{k} \sum_{i=\ell}^{k} q_{x,j} H \left( S_{n}^{j+1} \right) \]
\[ + \sum_{j=\ell}^{k} \mu_{x,j} H \left( S_{n}^{j+1} \right) \]

\[ \text{By denoting } \tilde{v}_j = \frac{1}{m} \sum_{x=1}^{m} q_{x,j} \text{ and } \tilde{\mu}_j = \frac{1}{m} \sum_{x=1}^{m} \tilde{\mu}_{x,j}, \]
\[ \text{we have} \]
\[ f(Q) = \alpha \sum_{j=\ell}^{k} \tilde{v}_j - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]

\[ \text{It is clear that } f(Q) \text{ is an upper bound on } mB_s. \text{ By dividing } m \text{ on both sides of (41), we have} \]
\[ B_s \leq \frac{1}{m} f(Q) \]
\[ = \left( \sum_{j=\ell}^{k} \tilde{v}_j \right) - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]

\[ \text{Clearly, for any } (k, d, \ell), \text{ if there exists a } m \times (k - \ell) \text{ matrix } Q \text{ satisfying } \frac{1}{m} f(Q) \leq \frac{1}{m} f(Q), \text{ then } (k, d, \ell) \in P. \]

\[ \text{Now, we claim that if the following three conditions} \]
\[ \sum_{j=\ell}^{k} \tilde{v}_j = \frac{\Gamma_{k,d,\ell}}{d}, \]
\[ \tilde{\mu}_j \geq 0, j = \ell, \ldots, k, \]
\[ \tilde{\delta}_j \geq 0, j = \ell + 1, \ldots, k \]

\[ \text{are satisfied, where} \]
\[ \tilde{\delta}_j = (d + 1 - j) \tilde{\mu}_j - \sum_{i=j}^{k-1} \tilde{v}_i, j = \ell + 1, \ldots, k, \]

\[ \text{then right hand side of (42) is upper bounded by } \frac{\Gamma_{k,d,\ell}}{d} \alpha. \]

To see this, focus on the right hand side of (42). By recalling from (27) that
\[ H \left( S_{n}^{j+1} \right) \leq (d + 1 - j) H \left( S_{n}^{j+1} \right), \]

we have
\[ \frac{1}{m} f(Q) \]
\[ = \left( \sum_{j=\ell}^{k} \tilde{v}_j \right) - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]

\[ \leq \frac{\Gamma_{k,d,\ell}}{d} \alpha - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]

\[ = \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) \]

\[ \leq \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell+1}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right), \]

where (a) follows from (43) and (b) follows from (44).

Since
\[ \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) \]
\[ = \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell+1}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]

\[ \leq \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) + \sum_{j=\ell+1}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right), \]

where in (c), the indices i and j in the double summation are renamed as j and i, respectively, we obtain
\[ \frac{1}{m} f(Q) \]
\[ \leq \frac{\Gamma_{k,d,\ell}}{d} \alpha - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) \]
\[ + \sum_{j=\ell}^{k} (d + 1 - j) \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]
\[ = \frac{\Gamma_{k,d,\ell}}{d} \alpha - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) \]
\[ + \sum_{j=\ell+1}^{k} \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]
\[ \leq \frac{\Gamma_{k,d,\ell}}{d} \alpha - \sum_{j=\ell}^{k} \tilde{v}_j H \left( S_{n}^{j+1} \right) \]
\[ + \sum_{j=\ell+1}^{k} (d + 1 - j) \tilde{\mu}_j H \left( S_{n}^{j+1} \right) \]

\[ \text{and (d) follows from (44).} \]
where (d) follows from Lemma 2. Since $H(S'_{n} | S_{n}^{j-1}) \leq H(S'_{n} | S_{n}^{j-1})$ for $i \geq j$, we have

$$\frac{1}{m} f(Q) \leq \frac{\Gamma_{k,d,\ell}}{d} \alpha - \left( \frac{\Gamma_{k,d,\ell}}{d} - \frac{d + 1 - \ell}{\ell} \tilde{\mu}_{\ell} \right) H(S'_{n})$$

$$+ \sum_{j=\ell+1}^{k} \delta_{j} H\left(S_{n+1}^{j} | S_{n}^{j-1}\right),$$

(proof continues)

### Proposition 7

$$\frac{\Gamma_{k,d,\ell}}{d} \alpha - \left( \frac{\Gamma_{k,d,\ell}}{d} - \frac{d + 1 - \ell}{\ell} \tilde{\mu}_{\ell} \right) H(S'_{n})$$

$$+ \sum_{j=\ell+1}^{k} \delta_{j} H\left(S_{n+1}^{j} | S_{n}^{j-1}\right)$$

$$= \frac{\Gamma_{k,d,\ell}}{d} \alpha - \left( \frac{\Gamma_{k,d,\ell}}{d} - \frac{d + 1 - \ell}{\ell} \tilde{\mu}_{\ell} - \frac{1}{\ell} \left( \sum_{j=\ell+1}^{k} \delta_{j} \right) \right) H(S'_{n}),$$

(47)

where (e) follows from (45) and (f) follows from Proposition 2.

### Proof

See Appendix G.

We can see easily that $\frac{1}{m} f(Q)$ is upper bounded by $\frac{\Gamma_{k,d,\ell}}{d} \alpha$ from (47) and Proposition 7. Therefore, we have shown that for any $(k, d, \ell)$, if there exists a matrix $Q$ such that $f(Q)$ satisfies (43), (44) and (45), then $(k, d, \ell) \in \mathcal{P}$. 

### B. Specification of the Matrix $Q$

From the previous discussion, we know that for any $(k, d, \ell)$, if there exists a matrix $Q$ such that $f(Q)$ satisfies (43), (44) and (45), then $(k, d, \ell) \in \mathcal{P}$. In this subsection, we will show the existence of a qualified matrix $Q$ for each $(k, d, \ell) \in \mathcal{P}$. In particular, we consider $Q$ satisfying the following conditions:

1) If $q_{x,y} = 0$, then $q_{x',y} = 0$ for all $x' \leq x$;
2) If $q_{x,y} = 0$, then $q_{x',y'} = 0$ for all $y' \leq y$.

These conditions say that the zeros and ones in the matrix $Q$ exhibit an echelon form.

Any matrix satisfying two conditions can be uniquely represented by a set of rational numbers $\left\{ z_{j} : j = \ell + 1, \ldots, k \right\}$ such that $0 \leq z_{j} \leq 1$ and $z_{j} \leq z_{j}$ if $i \geq j$, where $m z_{j}$ corresponds to the number of zeros in the $j$-th column.

Now, for any $(k, d, \ell)$, let

$$z_{j} = \begin{cases} \min \left\{ \frac{\Gamma_{k,d,\ell}}{d} \frac{2d-k-\ell+1}{d}, 1 \right\}, & j = \ell + 1, \\ \frac{2d-k-\ell+1}{2d}, & j = \ell + 2, \ldots, k - 1, \\ \max \left\{ 0, \frac{d-k-\ell+1}{d} \right\}, & j = k \text{ and } \ell + 1 < k. \end{cases}$$

(48)

Note that when $\ell = k - 1$, we have

$$z_{\ell+1} = z_{k} = \min \left\{ \frac{\Gamma_{k,d,\ell}}{d} \frac{2d-k-\ell+1}{d}, 1 \right\} = \frac{\Gamma_{k,d,\ell}}{d},$$

It is easy to see that $0 \leq z_{j} \leq 1$ for all $j$, so we only need to verify that $z_{i} \leq z_{j}$ if $i \geq j$. Obviously, we only need to consider $\ell \leq k - 2$. Then we have

$$\Gamma_{k,d,\ell} = \frac{1}{2} (k - \ell)(2d - k - \ell + 1) \geq 2d - k - \ell + 1.$$  

Next, let us discuss the two cases $2d - k - \ell + 1 \leq d$ and $2d - k - \ell + 1 > d$ as follows.

1) If $2d - k - \ell + 1 \leq d$, (48) can be written as

$$z_{j} = \begin{cases} \frac{2d-k-\ell+1}{2d}, & j = \ell + 1, \\ \frac{2d-k-\ell+1}{2d}, & j = \ell + 2, \ldots, k - 1, \\ 0, & j = k. \end{cases}$$

(50)

Since

$$\frac{2d - k - \ell + 1}{d} \geq \frac{2d - k - \ell + 1}{2d} \geq 0,$$

we see that $z_{i} \leq z_{j}$ if $i \geq j$.

2) If $2d - k - \ell + 1 > d$, (48) can be written as

$$z_{j} = \begin{cases} 1, & j = \ell + 1, \\ \frac{2d-k-\ell+1}{2d}, & j = \ell + 2, \ldots, k - 1, \\ \frac{d-k-\ell+1}{d}, & j = k. \end{cases}$$

(51)

Since

$$1 \geq \frac{2d - k - \ell + 1}{2d} \geq \frac{d - k - \ell + 1}{d},$$

we see that $z_{i} \leq z_{j}$ if $i \geq j$.

Therefore, the matrix specified by $z_{j}$ defined in (48) is admissible.

In the remaining of this subsection, we will verify that for any $(k, d, \ell) \in \mathcal{P}$, $f(Q)$ satisfies the conditions (43), (44) and (45), where $Q$ is determined by (48). First, we need to write $f(Q)$ explicitly. To do this, we divide the matrix $Q$ into three regions, namely $A$, $B$ and $C$ as illustrated in Fig. 3.

1) For the shaded gray region $A = \{q_{x,y} : x \leq s_{y}, \ell + 1 \leq y \leq \ell \}$, we can easily see that $q_{x,y} = 0$ and $t_{x,y} = \ell$.

Then by checking the conditions in (37), we see that only the elements in the first column, i.e., $y = \ell + 1$,
belong to the second case, while all others belong to the first case. Hence, the total contribution of the region $A$ to $f(Q)$ is given by
\[
mz_{\ell+1} \left( a - H(S_n^{[\ell+1]}) \right) - \sum_{j=\ell+2}^{k} mz_{j} \left( H(S_n^{[j-2]}) + H(S_n^{[j-2]}) \right) + \sum_{j=\ell+2}^{k} mz_{j} \left( a + \frac{d + 1 - j}{d + 1 - \ell} H(S_n^{[\ell-1]}) \right). \tag{52}\]

2) For the dotted area $B = \{q_{x,y} : x > mz_{\ell+1}, \ell + 1 \leq y \leq k\}$, we can easily see that $q_{s,y} = 1$ and $t_{s,y} = y - 1$. Hence, we can obtain from (36) that the total contribution of the region $B$ to $f(Q)$ is given by
\[
m(1 - z_{\ell+1}) \sum_{j=\ell+1}^{k} H \left( S_n^{[j-1]} \right). \tag{53}\]

3) For the remaining region $C = \{q_{x,y} : mz_{y} < x \leq mz_{\ell+1}, \ell + 1 \leq y \leq k\}$, we consider its contribution to $f(Q)$ column by column. For the column $j$, let $C_{j} = \{q_{x,y} : mz_{j} < x \leq mz_{\ell+1}\}$, which is illustrated as the vertical stripe in Fig. 3. We further divide $C_{j}$ into $j-\ell$ segments. Let $C_{j}^{i} = \{q_{x,y} : mz_{i+1} < x \leq mz_{j}\}$ for $i = \ell + 1, \ldots, j - 1$, where
\[
\bigcup_{i=\ell+1}^{j-1} C_{j}^{i} = C_{j}.
\]

Note that for a fixed $j$, $C_{j}^{i}$ may be empty for some $i$. Focus on a non-empty $C_{j}^{i}$, which is illustrated as the crosshatched segment in Fig. 3. Then we have $q_{s,y} = 1$ and $t_{s,y} = \ell + j - i - 1$. By invoking (36), we obtain that the contribution of $C_{j}^{i}$ to $f(Q)$ is
\[
m(z_{i} - z_{\ell+1}) \frac{d + 1 - j}{d + 1 - (\ell + j - i)} H(S_n^{[\ell+j-i]}|S_n^{[\ell+j-i]}). \]

It follows that the contribution of $C_{j}^{i}$ to $f(Q)$ is given by
\[
\sum_{i=\ell+1}^{j-1} m(z_{i} - z_{\ell+1})(d + 1 - j) \frac{d + 1 - j}{d + 1 - (\ell + j - i)} H(S_n^{[\ell+j-i]}|S_n^{[\ell+j-i]}),
\]
and the total contribution of the region $C$ to $f(Q)$ is given by
\[
\sum_{j=\ell+1}^{k} \sum_{i=\ell+1}^{j-1} m(z_{i} - z_{\ell+1})(d + 1 - j) \frac{d + 1 - j}{d + 1 - (\ell + j - i)} H(S_n^{[\ell+j-i]}|S_n^{[\ell+j-i]}). \tag{54}\]

For the ease of notation in the remaining parts, let us first simplify (54). Consider
\[
\sum_{j=\ell+1}^{k} \sum_{i=\ell+1}^{j-1} (z_{i} - z_{\ell+1})(d + 1 - j) H(S_n^{[\ell+j-i]}|S_n^{[\ell+j-i]}),
\]
where (a) follows from replacing the indices $p$ and $j$ by $j$ and $i$, respectively.

Let
\[
c_{j} = \sum_{i=\ell+1}^{j-1} (z_{\ell+i-j} - z_{\ell+i-j+1})(d + 1 - i), \quad j = \ell + 1, \ldots, k.
\]

Then we have
\[
\sum_{j=\ell+1}^{k-1} \sum_{i=\ell+1}^{j-1} (z_{\ell+i-j} - z_{\ell+i-j+1})(d + 1 - i) \frac{H(S_n^{[\ell+j-i]}|S_n^{[\ell+j-i]})}{d + 1 - j},
\]
where (b) follows from $c_{k} = 0$ by definition. Hence, (54) can be written as
\[
m \sum_{j=\ell+1}^{k} c_{j} \frac{H(S_n^{[\ell+j-i]}|S_n^{[\ell+j-i]})}{d + 1 - j}. \tag{55}\]

Now, focus on $f(Q)$, which can be obtained by adding (52), (53), and (55) as follows:
\[
f(Q) = mz_{\ell+1} \left( a - H(S_n^{[\ell+1]}) \right)
\]
By dividing $m$ on both sides, we have
\[
\frac{1}{m} f(Q) = z_{\ell+1} \left( \alpha - H(S_n^{(\ell)}) \right)
+ \sum_{j=\ell+2}^{k} \sum_{j=\ell+1}^{k} \left( \frac{d + 1 - j}{d + 1 - \ell} H(S_{n}^{|S_{\ell+1}|}) - H(S_{n}^{|S_{j+1}|}) \right)
+ \frac{1}{d + 1 - \ell} \left( \frac{d + 1 - j}{d + 1 - \ell} \sum_{j=\ell+1}^{k} \left( z_{j + 1} H(S_{n}^{|S_{j+1}|}) - \sum_{j=\ell+1}^{k} \left( z_{j+2} H(S_{n}^{|S_{j+1}|}) \right) \right) \right)
+ \frac{1}{d + 1 - \ell} \sum_{j=\ell+1}^{k} \left( 1 - z_{\ell+1} + \frac{c_j}{d + 1 - j} \right) H(S_{n}^{|S_{j+1}|}) .
\]  
(56)

For notational simplicity, let us separately discuss the case $\ell = k - 1$. For $\ell = k - 1$, (56) can be written as
\[
\frac{1}{m} f(Q) = z_{\ell+1} \alpha - z_{\ell+1} H(S_{n}^{(\ell)}) + (1 - z_{\ell+1}) H(S_{n}^{(\ell+1)}) = \beta_{k,d,k-1} \alpha - \beta_{k,d,k-1} H(S_{n}^{(\ell)})
+ \left( 1 - \beta_{k,d,k-1} \right) H(S_{n}^{(\ell+1)}) ,
\]  
where (c) follows from (49). By comparing the coefficients of $\alpha$, $H(S_{n}^{(\ell)})$ and $H(S_{n}^{(\ell+1)})$ with those in (42), we have $\tilde{\beta}_{k,d,k} = \beta_{k,d,k}$, $\bar{\beta}_{k,d,k} = \beta_{k,d,k-1}$, and we can easily check that these coefficients satisfy (43), (44) and (45), which implies that if $\ell = k - 1$, then $(k, d, \ell) \in \mathcal{P}$. This result has already been obtained in [18] and [19], but the proof here is much shorter (if we confine our discussion to the case $\ell = k - 1$).

For $\ell \leq k - 2$, by collecting the terms in (56), we obtain
\[
\frac{1}{m} f(Q) = \left( \sum_{j=\ell}^{k-1} \tilde{v}_j \right) \alpha - \sum_{j=\ell}^{k-1} \tilde{v}_j H(S_{n}^{(j)})
+ \sum_{j=\ell}^{k} \bar{\mu}_j H(S_{n}^{(j-1)}) ,
\]  
(57)

where
\[
\tilde{v}_j = \begin{cases} 0, & j = k - 1, \\ z_{j+2}, & j = \ell + 1, \ldots, k - 2, \\ z_{\ell+1} + z_{\ell+2}, & j = \ell, \end{cases}
\]  
(58)
\[
\bar{\mu}_j = \begin{cases} \sum_{i=j+1}^{k} \frac{z_{i}(d+j-1)}{d + 1 - j}, & j = \ell, \\ 1 - z_{j+1} - z_{j+1} + \frac{c_j}{d + 1 - j}, & j = \ell + 1, \ldots, k - 1, \\ 1 - z_{\ell+1}, & j = k, \end{cases}
\]  
and
\[
\hat{\delta}_j = \left\{ \begin{array}{ll} \frac{2d - k - \ell + 1}{d} & j = \ell, \\ \frac{2d - k - \ell + 1}{d} & j = \ell + 1, \ldots, k - 2, \\ 0 & j = k - 1. \end{array} \right.
\]  
(60)

Hence we obtain
\[
\sum_{j=\ell}^{k-1} \tilde{v}_j = \sum_{j=\ell+1}^{k} \frac{z_{j}}{d} = \frac{2d - k - \ell + 1}{d} + \sum_{j=\ell+2}^{k-1} \frac{z_{j}}{d}
\]  
(\text{d}) $2d - k - \ell + 1 - \frac{(k - \ell - 2)}{2d}$, where (d) follows from (48).

Now, let us verify the conditions (44) and (45). From (58), we see that $\bar{\mu}_\ell \geq 0$ and $\bar{\mu}_k \geq 0$. Since $\bar{\delta}_k = (d + 1 - k)\bar{\mu}_k$, we have $\bar{\delta}_k \geq 0$, hence, it remains to show that $\bar{\mu}_j \geq 0$ and $\bar{\delta}_j \geq 0$ for $j = \ell + 1, \ldots, k - 1$. We know from (59) that $\bar{\delta}_j \geq 0$ for all $j$, so we have
\[
\tilde{v}_j = (d + 1 - j)\bar{\mu}_j - \sum_{i=\ell}^{k-1} \bar{v}_i \leq (d + 1 - j)\bar{\mu}_j ,
\]  
which implies that if $\bar{\delta}_j \geq 0$, then $\bar{\mu}_j \geq 0$. Therefore, it suffices to prove the following proposition.

**Proposition 8.** For any $(k, d, \ell) \in \mathcal{P}$, where $\ell \leq k - 2$, $\bar{\delta}_j \geq 0$ for $j = \ell + 1, \ldots, k - 1$.

**Proof.** See Appendix H.

### C. Discussion

In this paper, we are interested in the problem of determining parameters whose optimal storage-bandwidth tradeoff curve has a single corner point. However, the approach proposed to solve the problem may also be helpful to the general problem, that is characterizing the tradeoff for any parameters $(n, k, d, \ell)$.

Recall that we upper bounded the secrecy capacity by a linear combination of random variables $\alpha$, $H(S_n^{(\ell)})$ and $H(S_{n}^{(\ell+1)})$, i.e. (cf. (42)),
\[
B_s \leq \left( \sum_{j=\ell}^{k-1} \bar{v}_j \right) \alpha - \sum_{j=\ell}^{k-1} \bar{v}_j H(S_{n}^{(j)}) + \sum_{j=\ell}^{k} \bar{\mu}_j H(S_{n}^{(j-1)}) ,
\]  
where each configuration of $Q$ (cf. (39)) gives a different upper bound on $B_s$. Also, we know that the two entropies $H(S_n^{(\ell)})$ and $H(S_{n}^{(\ell+1)})$ are related by the following inequality:
\[
H(S_{n}^{(|S_{\ell+1}|)}) \leq (n - j)H(S_{n}^{(j)}) - (n - j)H(S_{n}^{(j-1)}) .
\]  
Since our purpose is to bound the secrecy capacity $B_s$ by some $\alpha$, we found some configurations that give coefficients satisfying the conditions in (43), (44) and (45), which guarantee that we can cancel all the $H(S_{n}^{(\ell)})$ and $H(S_{n}^{(\ell+1)})$.
terms (related to $\beta$), and finally can upper bound $B_s$ only by
some $\alpha$.

However, if one’s purpose is not canceling all terms related to $\beta$, one may find some other configurations to make some $H(S_{n+1}^j)$ remain with positive coefficients. Then by the union bound, one can easily obtain an upper bound which is some linear combination of $\alpha$ and $\beta$ and also a valid outer bound for the secrecy capacity region. This is indeed what we did to prove the first case in (62) for $\Gamma_{k,d,\ell} > 0$, i.e.,

$$\tilde{\alpha} + (\Gamma_{k,d,\ell} - d)\tilde{\beta} \geq 1.$$  

(61)

To the best of our knowledge, for those parameters whose tradeoff may have multiple corner points, the cut-set bound is the best known outer bound in general, that is

$$\sum_{i=\ell+1}^{k-1} \min(\tilde{\alpha}, (d+1-i)\beta) \geq 1.$$  

One can easily check that the outer bound in (61) that we have obtained largely improves the cut-set bound in the region where $\tilde{\beta}$ is small (the so-called bandwidth-limited region in [11]).

VI. CONCLUSION

In this paper, we study parameters $(n,k,d,\ell)$ whose optimal storage-bandwidth tradeoff curve has one corner point and can be determined. Toward this end, we obtained a lower bound $\ell$ on the number of wiretap nodes which is tight for $k = d = n - 1$. Whether this bound is tight for other values of $n$, $k$ and $d$ is a problem for future research. Our results subsume all the previous related results [16]–[19].

APPENDIX A

PROOF OF THE OPTIMALITY OF $(\tilde{\alpha}, \tilde{\beta})$

We will prove that $(\tilde{\alpha}, \tilde{\beta})$ is on the optimal tradeoff curve by establishing the following outer bound

$$\begin{cases} 
\tilde{\alpha} + (\Gamma_{k,d,\ell} - d)\tilde{\beta} \geq 1, & \Gamma_{k,d,\ell} > 0, \\
\tilde{\alpha} \geq \tilde{\alpha}, & \Gamma_{k,d,\ell} \leq 0.
\end{cases}$$  

(62)

It has been shown that $\tilde{\beta} \geq \tilde{\beta}$ (cf.(13)). As illustrated in Fig. 4, we can see that the intersection of $\tilde{\beta} \geq \tilde{\beta}$ and (62) is given by $(\tilde{\alpha}, \tilde{\beta})$, no matter whether $\Gamma_{k,d,\ell} > 0$ or $\Gamma_{k,d,\ell} \leq 0$. As $(\tilde{\alpha}, \tilde{\beta})$ is achievable, we can conclude that $(\tilde{\alpha}, \tilde{\beta})$ must be on the tradeoff curve if (62) holds.

We now proceed to (62). By letting $T = \{S^i : i = 1, \ldots, k\}$ and $L = \ell$ in (12), we have

$$B_s \leq H\left(\sum_{i=\ell+1}^{k} S^n_i | S^\ell_i\right)$$

$$= \sum_{i=\ell+1}^{k} H\left(S^n_i | S^{\ell-1}_i\right)$$

where (a) follows from (27), and (b) follows from Lemma 2. Similarly, by letting $T = \{S^i : i = 1, \ldots, k - 1\} \cup \{W_k\}$ and $L = \ell$ in (12), we have

$$B_s \leq H\left(\sum_{i=\ell+1}^{k-1} S^n_i | S^{\ell-1}_i\right) + H\left(W_k | S^{k-1}_i\right)$$

(63)

where (c) follows from (27) and (d) follows from Lemma 2. When $\Gamma_{k,d,\ell} > d$, we know from (64) that

$$B_s \leq \alpha + \frac{\Gamma_{k,d,\ell} - d}{\ell} H\left(S^n_i\right) \leq \alpha + (\Gamma_{k,d,\ell} - d)\beta,$$

which is equivalent to

$$\tilde{\alpha} + (\Gamma_{k,d,\ell} - d)\tilde{\beta} \geq 1,$$

i.e. the first case of (62).

When $\Gamma_{k,d,\ell} \leq d$, by multiplying (63) and (64) by $d - \Gamma_{k,d,\ell}$ and $\Gamma_{k,d,\ell}$ respectively, we have

$$d B_s \leq (d - \Gamma_{k,d,\ell}) \frac{\Gamma_{k,d,\ell}}{\ell} H\left(S^n_i\right)$$

$$+ \Gamma_{k,d,\ell} \left(\alpha + \frac{\Gamma_{k,d,\ell} - d}{\ell} H\left(S^n_i\right)\right)$$

$$= \Gamma_{k,d,\ell} \alpha,$$
which is equivalent to $\tilde{a} \geq \hat{a}$, i.e. the second case of (62). Therefore, we have proved (62).

**Remark.** Shao et al. [19] have proved that $\tilde{a} \geq \hat{a}$ if $\Gamma_{k,d,\ell} \leq d$, i.e. the second case of (62). The proof therein is very lengthy. The proof of (62) here is much simple, and the first case is a new result.

**APPENDIX B**

**CONSEQUENCES OF THEOREM 2**

1) We first justify that there exists a lower bound on $\ell$ by proving the claim: if $\ell$ satisfies (11) then $\ell + 1$ satisfies (11).

Let

$$P_s := \{(k, d, \ell) : \ell = k - 1 \text{ or (11) is satisfied}\},$$

and for fixed $k$ and $d$ define

$$\ell := \min \{\ell \geq 1 : (k, d, \ell) \in P_s\}. \quad (65)$$

Note that $\ell$ is well defined since $(k, d, \ell = k - 1) \in P_s$ for any given $k$ and $d$.

One can easily check that when $k - 4 \leq \ell \leq k - 2$, the claim is true, so it remains to show that if $(k, d, \ell) \in P_s$ for $\ell < k - 4$, then $(k, d, \ell + 1) \in P_s$.

Towards this end, let

$$g(\ell) = d(d - \ell - 1) - \frac{1}{2}(2d - k - \ell + 1)(2d + k - 3\ell - 5)$$

for $1 \leq \ell \leq k - 4$. Clearly $(k, d, \ell) \in P_s$ for $\ell \leq k - 4$ if and only if $g(\ell) \geq 0$. For the quadratic equation $g(\ell) = 0$, the discriminant is $3(d - k)^2 + 12(d - 4) + (k - 8)^2$, which is nonnegative provided that $d \geq 4$. This condition is guaranteed because we have

$$d \geq k \geq \ell + 4 \geq 5,$$

where the second inequality follows from the range of $\ell$ in (66). Let $\ell_1$ and $\ell_2$ be two roots of $g(\ell) = 0$ such that $\ell_1 \leq \ell_2$. Since the leading coefficient of $g(\ell)$ is negative, we see that $g(\ell) \geq 0$ if and only if $\ell_1 \leq \ell \leq \ell_2$.

Consider

$$\ell_2 = \frac{1}{3} \left(3d - k - 1 + \sqrt{3(d - k)^2 + 12(d - 4) + (k - 8)^2}\right)$$

$$\geq \frac{1}{3} \left(3d - k - 1 + k - 8\right)$$

$$\geq k - 3.$$  

Then, if $g(\ell) \geq 0$ for some $\ell < k - 4$, we have

$$\ell + 1 < k - 3 \leq \ell_2,$$

which implies that $g(\ell + 1) \geq 0$, as is to be proved.

2) Second, we claim that Theorem 2 improves the existing result in Shao et al. [19], where they showed that $(k, d, \ell) \in \mathcal{P}$ if

$$\ell \geq \ell^* := \min \left\{\ell' \geq 1 : \Gamma_{k,d,\ell'} \leq d + \sqrt{d\ell'}\right\}. \quad (67)$$

Let

$$\mathcal{P}_r := \{(k, d, \ell) : \ell \geq \ell^*\}.$$

Recall that

$$\Gamma_{k,d,\ell} = \sum_{i=\ell}^{k-1} (d - i) = \frac{1}{2}(k - \ell)(2d - k - \ell + 1).$$

Evidently, $\Gamma_{k,d,\ell}$ is decreasing with $\ell$ while $d + \sqrt{d\ell}$ is increasing with $\ell$, and so we have

$$\mathcal{P}_r = \{(k, d, \ell) : \ell \geq \ell^*\} = \{(k, d, \ell) : \Gamma_{k,d,\ell} \leq d + \sqrt{d\ell}\}. \quad (68)$$

We will justify our claim by first showing that $\mathcal{P}_r \subseteq \mathcal{P}_s$, or equivalently $\ell \leq \ell^*$. For fixed $k$ and $d$, assume that $(k, d, \ell) \in \mathcal{P}_r$, and we will prove that $(k, d, \ell) \in \mathcal{P}_s$. One can easily check that it is true for $\ell \geq k - 3$, so we focus on the case $\ell \leq k - 4$.

Let

$$h(\ell) = d + \sqrt{d\ell} - \Gamma_{k,d,\ell}, \quad 1 \leq \ell \leq k - 4.$$  

Then $(k, d, \ell) \in \mathcal{P}_r$ for some $\ell \leq k - 4$ if and only if $h(\ell) \geq 0$ for some $\ell \leq k - 4$. We claim that if $h(\ell) \geq 0$ for some $\ell \leq k - 4$, then $\ell \geq \ell_0$, where $\ell_0 = \left\lfloor \frac{1}{2}d - 1\right\rfloor$.

This can be substantiated by contradiction. Assume the contrary that $\ell \leq \ell_0 - 1$. Then we have

$$h(\ell) = d + \sqrt{d\ell} - \Gamma_{k,d,\ell} \overset{(a)}{\leq} \frac{\ell - \ell_0}{2}(d - 1) + 1 \overset{(c)}{<} 0,$$

where (a) follows from $k \geq \ell + 4$ and $\frac{1}{2}(k - \ell)(2d - k - \ell + 1)$ is increasing with $k$ when $k \leq d$; (b) follows from the assumption $\ell \leq \ell_0 - 1$; and (c) follows from $1 \leq \ell \leq k - 4 \leq d - 4$. Clearly, (69) contradicts with the assumption that $h(\ell) \geq 0$, and hence we know that if $h(\ell) \geq 0$ for some $\ell \leq k - 4$, then $\ell \geq \ell_0$. Next, we will show that $g(\ell) \geq 0$ for $\ell_0 \leq \ell \leq k - 4$. Consider

$$g(\ell) = d(d - \ell - 1) - \frac{1}{2}(2d - k - \ell + 1)(2d + k - 3\ell - 5) \overset{(d)}{\geq} d(d - \ell - 1) - \frac{1}{2}(2d - 2\ell - 3)(2d - 2\ell - 1) \overset{(e)}{\geq} (d - \ell - 1)(2\ell_0 - d + 2) + \frac{1}{2} \overset{(f)}{\geq} (d - \ell - 1) + \frac{1}{2} \overset{(g)}{\geq} 0,$$

where (d) follows because $\frac{1}{2}(2d - k - \ell + 1)(2d + k - 3\ell - 5)$ is decreasing with $k$ when $k \geq \ell + 4$, (e) follows from $\ell \geq \ell_0$, and (f) follows from $2\ell_0 - d + 2 \geq 1$. Hence, we have shown that $g(\ell) \geq 0$ if $h(\ell) \geq 0$ for some $\ell \leq k - 4$. Therefore we can conclude that $\mathcal{P}_r \subseteq \mathcal{P}_s$, or $\ell \leq \ell^*$. 
APPENDIX C
PROOF OF LEMMA 3

First, for $t = 0, \ldots, k - 2$, we consider

\begin{align}
H(W_{[t+1:k]}|S^{[t]}) &= \sum_{i=t+1}^{k} H\left(W_{i}|W_{[t+1:i-1]}, S^{[t]}\right)
\leq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) - \sum_{i=t+2}^{k} I\left(W_{i}; W_{[t+1:i-1]}|S^{[t]}\right) \\
&\leq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) - \sum_{i=t+2}^{k} I\left(S_{[t+1:i-1]}^{i}; S_{[t+1:i-1]}^{[i]}|S^{[t]}\right),
\end{align}

where (71) is justified because $S_{[t+1:i]}^{i}$ and $S_{[t+1:i-1]}^{i}$ are functions of $W_{i}$ and $W_{[t+1:i-1]}$ respectively.

The second term on the right-hand side of (71) can be further bounded as follows:

\begin{align}
\sum_{i=t+2}^{k} I\left(S_{[t+1:i-1]}^{i}; S_{[t+1:i-1]}^{[i]}|S^{[t]}\right) &= \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) - \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{[i]}|S^{[t]}\right) \\
&\geq \sum_{i=t+2}^{k} \frac{i - 1 - t}{2} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right)
+ \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{[i]}|S^{[t]}\right) \\
&\geq \sum_{i=t+2}^{k} \frac{i - 1 - t}{2} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right)
- \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{[i]}|S^{[t]}\right) \\
&\geq \sum_{i=t+2}^{k} \frac{i - 1 - t}{2} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) \\
&\geq \sum_{i=t+2}^{k} \frac{i - 1 - t}{2} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) \\
&\geq \sum_{i=t+2}^{k} \frac{i - 1 - t}{2} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right)
- \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{[i]}|S^{[t]}\right),
\end{align}

where (a) follows from Lemma 2, and (b) is justified because $\{S_{[t+1:i-1]}^{i}, S_{[t+1:i-1]}^{[i]}\}$ is a function of $S_{[t+1:i-1]}^{[t]}$ and also a function of $S_{[t+1]}^{[t]}$.

By symmetry, we know that

\begin{align}
\sum_{i=t+2}^{k} \frac{i - 1 - t}{2} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right)
&\geq \left(\sum_{i=t+2}^{k} \frac{i - 1 - t}{2} \right) H\left(S_{[t+1]}^{[t]}|S^{[t]}\right),
\end{align}

and

\begin{align}
\sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) &= (k - t) H\left(S_{[t+1]}^{[t]}|S^{[t]}\right).
\end{align}

Hence, (72) can be written as

\begin{align}
\sum_{i=t+2}^{k} &I\left(S_{[t+1:i-1]}^{i}; S_{[t+1:i-1]}^{[i]}|S^{[t]}\right)
\geq \left(\sum_{i=t+2}^{k} \frac{i - 1 - t}{2} \right) H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
+ \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) - (k - t) H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
+ H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right).
\end{align}

By substituting (73) in (71), we have

\begin{align}
H(W_{[t+1:k]}|S^{[t]}&)
\leq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) - \left(\sum_{i=t+2}^{k} \frac{i - 1 - t}{2} \right) H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
- \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right)
+ (k - t) H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
\geq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) + \frac{d - t + 1}{2} H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
- \sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) - H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right),
\end{align}

where (c) follows from $k = d$.

From the union bound, we know that

\begin{align}
\sum_{i=t+2}^{k} H\left(S_{[t+1:i-1]}^{i}|S^{[t]}\right) &\geq H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right),
\end{align}

and then we can further bound (74) as follows:

\begin{align}
H(W_{[t+1:k]}|S^{[t]}&)
\leq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) + \frac{d - t + 1}{2} H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
- \sum_{i=t+2}^{k} H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right)
\geq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) + \frac{d - t + 1}{2} H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
- \sum_{i=t+2}^{k} H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right)
- H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right) - \sum_{i=t+1}^{k} H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right)
+ \sum_{i=t+1}^{k} H\left(S_{[t+1]}^{[t]}|S^{[t]}\right)
+ H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right)
- \sum_{i=t+1}^{k} H\left(S_{[t+1:k]}^{[t]}|S^{[t]}\right).
\end{align}
By re-arranging (75), we have
\[
H(W_{t+1:k}|S^{[t]}) + H(S^{[t+1:k]}|S^{[t]}) + H(S_{t+1:n}|S^{[t]}) \\
\leq \sum_{i=t+1}^{k} H(W_i|S^{[t]}) + \frac{d - t + 1}{2} H(S^{[t+1]}|S^{[t]}) \\
+ H(S_{t+1:n}|S^{[t]}, S_{t+1:k}) \\
\leq k \sum_{i=t+1}^{k} H(W_i|S^{[t]}) + \frac{d - t + 1}{2} H(S^{[t+1]}|S^{[t]}) \\
+ H(W_n|S^{[t]}) \\
\leq k \sum_{i=t+1}^{k} (H(W_i|S^{[t]}) + \frac{d - t + 1}{2} H(S^{[t+1]}|S^{[t]})) \\
+ H(W_n|S^{[t]}) \\
\leq (k - t + 1)H(W_n|S^{[t]}) + \frac{d - t + 1}{2} H(S^{[t+1]}|S^{[t]}) \\
\leq (d - t + 1)\mu - (d - t + 1)H(S^{[t]}|S^{[t]}) \\
+ \frac{d - t + 1}{2} H(S^{[t+1]}|S^{[t]}),
\]
where (d) and (f) follow from \(k = d = n - 1\), and (e) follows from the symmetry.

From Proposition 1, we know that
\[
H(W_{t+1:k}, S^{[t]}) = H(S^{[t+1:k]}, S^{[t]}) \\
= H(S_{t+1:n}, S^{[t]}) = H(W_{t}^{[k]}),
\]
so
\[
H(W_{t+1:k}|S^{[t]}) = H(S^{[t+1:k]}|S^{[t]}) = H(S_{t+1:n}|S^{[t]}).
\]
Hence we have
\[
3 H(W_{t+1:k}|S^{[t]}) \leq (d - t + 1)\alpha - (d - t + 1)H(S^{[t]}|S^{[t]}) \\
+ \frac{d - t + 1}{2} H(S^{[t+1]}|S^{[t]}),
\]
or
\[
H(W_{t+1:k}|S^{[t]}) \leq \frac{d - t + 1}{3} \alpha - \frac{d - t + 1}{3} H(S^{[t]}|S^{[t]}) \\
+ \frac{d - t + 1}{6} H(S^{[t+1]}|S^{[t]}),
\]
for \(t = 0, \ldots, k - 2\).

Now, consider \(H(W_{t+1:k}|S^{[t]})\). For any \(t < \ell\), we have
\[
H(W_{t+1:k}|S^{[t]}) \\
= H(W_{t+1:k}, S^{[t]}) - H(S^{[t]}|S^{[t]}) - H(S^{[t]}|S^{[t]}) \\
\leq H(W_{t+1:k}, S^{[t]}) - H(S^{[t]}|S^{[t]}) - H(S^{[t]}|S^{[t]}) \\
= H(W_{t+1:k}|S^{[t]}) - H(S^{[t]}|S^{[t]}) \\
= H(W_{t+1:k}|S^{[t]}) - \sum_{i=t+1}^{\ell} H(S^{[t]}|S^{[t-1]}),
\]
which completes the proof.

**APPENDIX D**

**PROOF OF PROPOSITIONS IN SUBSECTION IV-B**

**A. Proof of Proposition 3**

Since \(\mu_0 = 1 - \sum_{j=1}^{\ell-1} \mu_j\), it is obvious that
\[
\sum_{i=0}^{\ell-1} \mu_i = 1.
\]
Recall that
\[
\mu_t = \begin{cases} 
\frac{n - \hat{t}}{2} - \frac{n - 2(\hat{t} - 1)}{2}, & 1 \leq t \leq \hat{t} - 3, \\
\frac{n - \hat{t} - 3}{6(n - \hat{t} + 1)(n - \hat{t} + 2)}, & t = \hat{t} - 2, \hat{t} \geq 3, \\
\frac{n - \hat{t} - 1}{6}, & t = \hat{t} - 1, \hat{t} \geq 2.
\end{cases}
\]
Since \(\hat{t} = \left\lfloor \frac{n}{4} - 2 \right\rfloor\), if \(\hat{t} \geq 3\), we have \(n \geq 11\), and hence
\[
n - \hat{t} - 3 = n - \left\lfloor \frac{n}{4} - 2 \right\rfloor - 3 > n - \frac{1}{4}(n - 2) - 4 = \frac{3}{4} \left( n - \frac{14}{3} \right) > 0.
\]
Also, when \(1 \leq t \leq \hat{t} - 3\), we have
\[
n - 2\hat{t} - 1 + t \geq n - 2\hat{t} = n - 2 \left\lfloor \frac{n}{4} - 2 \right\rfloor > \frac{1}{2}n - 1 > 0.
\]
Hence, \(\mu_t \geq 0\) for \(t = 1, \ldots, \hat{t} - 1\) and so it remains to show that \(\mu_0 \geq 0\).
For \(\hat{t} = 1\), this is trivial as \(\mu_0 = 1\). For \(\hat{t} \geq 2\), we claim that
\[
\mu_0 = \frac{(n - \hat{t})(n - \hat{t} - 1)(n + 1 - 4\hat{t})}{(n - 1)(n - 2)(n - 3)}. \tag{78}
\]
To see this, we first separately discuss the cases \( \hat{\ell} = 2 \) and \( \hat{\ell} = 3 \), where \( \mu_t, t = 0, \ldots, \hat{\ell} - 1 \) are as given as follows:

- \( \hat{\ell} = 2 \)
  \[
  \mu_t = \begin{cases} 
  \frac{\hat{\ell}^{-1}}{n-\hat{\ell}+1}, & t = 0, \\
  \frac{\hat{\ell}^{-1}}{n-\hat{\ell}+2}, & t = 1. 
  \end{cases}
  \tag{79}
  \]

- \( \hat{\ell} = 3 \)
  \[
  \mu_t = \begin{cases} 
  \frac{(n-1)(n-4)}{6(n-6)}, & t = 0, \\
  \frac{(n-1)(n-2)}{6(n-2)}, & t = 1, \\
  \frac{6}{n-2}, & t = 2. 
  \end{cases}
  \tag{80}
  \]

Then we can easily verify that (78) holds.

For \( \hat{\ell} \geq 4 \) and any \( j = 1, \ldots, \hat{\ell} - 3 \), we have
\[
\sum_{i=1}^{\hat{\ell} - 3} \mu_i = \sum_{i=1}^{\hat{\ell} - 3} \frac{1}{2} \left( \frac{n - \hat{\ell}}{n - \hat{\ell} - 1} \right) \frac{n - 2\hat{\ell} - 1 + i}{(n-1)^{i-4}} \geq \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(n - 4\hat{\ell} + 1 + 3j)}{(n - j - 1)(n - j - 2)(n - j - 3)} + \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(4\hat{\ell} - n - 1)}{(n - 1)(n - 2)(n - 3)}, \tag{81}
\]
where the above inequality and some other algebraic equalities in the sequel which are marked by an asterisk can be verified by symbolic computation application such as SageMath [23]. The steps are very lengthy and they are omitted here.

By substituting \( j = \hat{\ell} - 3 \), we have
\[
\sum_{i=1}^{\hat{\ell} - 3} \mu_i = \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(4\hat{\ell} - n - 1)}{(n - 1)(n - 2)(n - 3)}, \tag{82}
\]
and
\[
\frac{6(n - \hat{\ell} - 3)}{(n - \hat{\ell} + 1)(n - \hat{\ell} + 2)},
\]
we have
\[
\sum_{i=1}^{\hat{\ell} - 3} \mu_i = 1 + \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(4\hat{\ell} - n - 1)}{(n - 1)(n - 2)(n - 3)} = 1 - \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(n + 1 - 4\hat{\ell})}{(n - 1)(n - 2)(n - 3)},
\]
and so
\[
\mu_0 = \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(n + 1 - 4\hat{\ell})}{(n - 1)(n - 2)(n - 3)}. \tag{83}
\]

Therefore, we obtain
\[
\mu_0 = \begin{cases} 
  \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)(n + 1 - 4\hat{\ell})}{(n - 1)(n - 2)(n - 3)}, & \hat{\ell} \geq 2, \\
  1, & \hat{\ell} = 1. 
  \end{cases}
  \tag{84}
  \]

Since
\[
n + 1 - 4\hat{\ell} = n + 1 - 4 \left( \frac{1}{4}(n - 2) \right) > n + 1 - (n - 2) - 4 = -1,
\]
and \( n + 1 - 4\hat{\ell} \) is an integer, we have
\[
n + 1 - 4\hat{\ell} \geq 0,
\]
and thus \( \mu_0 \geq 0 \) for \( \hat{\ell} \geq 2 \).

B. Proof of Proposition 4

We need to prove that \( c_t \geq 0 \) for \( t = 0, \ldots, \hat{\ell} - 1 \) and \( c_{\hat{\ell} - 1} = 0 \) when \( \hat{\ell} \geq 2 \). Recall that
\[
c_t = \frac{n - t}{6} \mu_t - \sum_{j=0}^{t} \mu_j, \quad t = 0, \ldots, \hat{\ell} - 1.
\]

First, we show that \( c_{\hat{\ell} - 1} = 0 \) for \( \hat{\ell} \geq 2 \) as follows:
\[
c_{\hat{\ell} - 1} = \frac{n - \hat{\ell} + 1}{6} \mu_{\hat{\ell} - 1} - \sum_{j=0}^{\hat{\ell} - 1} \mu_j = 1 - 1 = 0.
\]

For \( t = 0 \), it is easy to see that
\[
c_0 = \frac{n}{6} \mu_0 - \mu_0 = \frac{n - 6}{6} \mu_0 \geq 0,
\]
as \( \hat{\ell} \geq 2 \) implies that \( n \geq 7 \), and we know from Proposition 3 that \( \mu_0 \geq 0 \). Clearly, the proposition is proved for \( \hat{\ell} = 2 \), and it remains to verify that \( c_t \geq 0 \) for \( t = 1, \ldots, \hat{\ell} - 2 \) for \( \hat{\ell} \geq 3 \).

If \( \hat{\ell} = 3 \), we obtain from (80) that
\[
c_1 = \frac{n - 1}{6} \mu_1 - \sum_{j=0}^{1} \mu_j = \frac{n - 6}{n - 2} - \left( 1 - \frac{6}{n - 2} \right) = \frac{2}{n - 2} \geq 0,
\]
which completes the proof for \( \hat{\ell} = 3 \).

For \( \hat{\ell} \geq 4 \) and any \( t = 1, \ldots, \hat{\ell} - 3 \), we have
\[
c_t = \frac{n - t}{6} \mu_t - \sum_{j=0}^{t} \mu_j \geq \frac{2(n - \hat{\ell})(n - \hat{\ell} - 1)(\hat{\ell} - 1 - t)}{(n - t - 1)(n - t - 2)(n - t - 3)}, \tag{84}
\]

It is easy to see that \( c_t \geq 0 \) for any \( t = 1, \ldots, \hat{\ell} - 3 \) from (84).

If \( t = \hat{\ell} - 2 \), we have
\[
c_{\hat{\ell} - 2} = \frac{n - \hat{\ell} + 2}{6} \mu_{\hat{\ell} - 2} - \sum_{j=0}^{\hat{\ell} - 2} \mu_j = \frac{2}{n - \hat{\ell} + 1} > 0.
\]
Hence, we obtain that \( c_t \geq 0, t = 1, \ldots, \hat{\ell} - 2 \) for \( \hat{\ell} \geq 4 \).

In summary, for \( \hat{\ell} \geq 2 \), we have
\[
c_t = \begin{cases} 
  \frac{n - 6}{6} \mu_0, & t = 0, \\
  \frac{2(n - \ell)(n - \ell - 1)(\ell - 1 - t)}{(n - t - 1)(n - t - 2)(n - t - 3)} & 1 \leq t \leq \hat{\ell} - 3, \\
  \frac{2}{n - \hat{\ell} + 1}, & t = \hat{\ell} - 2, \hat{\ell} \geq 3, \\
  0, & t = \hat{\ell} - 1, \tag{85}
  \end{cases}
  \]
which substantiates that \( c_{\hat{\ell} - 1} = 0 \) and \( c_t \geq 0 \) for all possible \( t \) and \( \hat{\ell} \geq 2 \).
C. Proof of Proposition 5

We need to verify that \( \lambda_t = c_{t-1}(d+1-t) - c_t(d-t) - b_t = 0 \) for \( t = 2, \ldots, \hat{\ell} - 1 \) and \( \hat{\ell} \geq 3 \). Recall that (85) and

\[
\begin{align*}
   b_t &= \frac{n-t}{3} \mu_t. \\
   \lambda_t &= c_{t-2}(d + 2 - \hat{\ell}) - c_{t-1}(d - \hat{\ell} + 1) - b_{t-1} \\
   &= 2 - \frac{(n - \hat{\ell} + 1)}{3} \mu_{\hat{\ell} - 1} = 0.
\end{align*}
\]

If \( t = \hat{\ell} - 1 \), we have

\[
\begin{align*}
   \lambda_t &= c_{\hat{\ell} - 2}(d + 2 - \hat{\ell}) - c_{\hat{\ell} - 1}(d - \hat{\ell} + 1) + b_{\hat{\ell} - 1} \\
   &= 4(n - \hat{\ell} - 1) - 2 - \frac{n - \hat{\ell} + 2}{3} \mu_{\hat{\ell} - 2} = 0.
\end{align*}
\]

If \( t = \hat{\ell} - 2 \) (implies that \( \hat{\ell} \geq 4 \)), we have

\[
\begin{align*}
   \lambda_t &= c_{\hat{\ell} - 3}(d + 3 - \hat{\ell}) - c_{\hat{\ell} - 2}(d + 2 - \hat{\ell}) + b_{\hat{\ell} - 2} \\
   &= \frac{2(n - \hat{\ell})(n - \hat{\ell} - 1)(\hat{\ell} - t)}{(n - t - 1)(n - t - 2)} \\
   &\quad - \frac{2(n - \hat{\ell})(n - \hat{\ell} - 1)(\hat{\ell} - 1 - t)}{(n - t - 2)(n - t - 3)} \\
   &\quad - \frac{n - t}{6} \frac{n - 2\hat{\ell} + 1 + t}{2} \frac{(n-t)}{4}.
\end{align*}
\]

Therefore, we conclude that \( \lambda_t = c_{t-1}(d + 1 - t) - c_t(d - t) - b_t = 0 \) for \( t = 2, \ldots, \hat{\ell} - 1 \).

D. Proof of Proposition 6

We first prove that \( T_2 \geq 0 \) as follows:

\[
T_2 = b_1 - c_0 d + c_1(d - 1) = \frac{n - 1}{3} \mu_1 + \frac{(n - 1)(n - 6)}{6} \mu_0
\]

\[
+ \frac{n - 1}{6} (\mu_1 - \mu_0 - \mu_1) (n - 2) = \frac{1}{6} (n - 7)(n - 2) + \frac{1}{3} (n - 1) \mu_1
\]

\[
- \frac{1}{6} (n - 1)(n - 6) + (n - 2) \mu_0
\]

\[
\overset{(a)}{=} \frac{(4\hat{\ell} + 2 - n)(n - \hat{\ell})(n - \hat{\ell} - 1)}{6(n - 2)},
\]

and then we have \( T_2 \geq 0 \) because \( \hat{\ell} = \lceil \frac{1}{4}(n - 2) \rceil \geq \frac{1}{4}(n - 2) \).

Now, we focus on \( T_1 \). For \( \hat{\ell} = 2 \), we have

\[
T_1 = \sum_{t=0}^{\hat{\ell} - 1} \frac{n - t}{3} \mu_t n - 1 \mu_0 + \frac{n - 1}{3} \mu_1 \overset{(a)}{=} \frac{n(n - 7)}{3(n - 1)} + 2
\]

\[
= \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)}{(n - 3)(n - 2)} \left( \frac{n(n + 1 - 4\hat{\ell})}{3(n - 1)} + 2(\hat{\ell} - 1) \right),
\]

where (a) follows from (79). For \( \hat{\ell} = 3 \), we have

\[
T_1 = \sum_{t=0}^{\hat{\ell} - 1} \frac{n - t}{3} \mu_t
\]

\[
= \frac{n}{3} \mu_0 + \frac{n - 1}{3} \mu_1 + \frac{n - 2}{3} \mu_2
\]

\[
\overset{(a)}{=} \frac{n(n - 4)(n - 11)}{3(n - 1)} + \frac{2(n - 6)}{n - 2} + 2
\]

\[
= \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)}{(n - 3)(n - 2)} \left( \frac{n(n + 1 - 4\hat{\ell})}{3(n - 1)} + 2(\hat{\ell} - 1) \right),
\]

where (a) follows from (80). For \( \hat{\ell} \geq 4 \), we have

\[
T_1 = \sum_{t=0}^{\hat{\ell} - 1} \frac{n - t}{3} \mu_t
\]

\[
= \frac{n}{3} \mu_0 + \frac{n - \hat{\ell} + 2}{3} \mu_{\hat{\ell} - 2} + \frac{n - \hat{\ell} + 1}{3} \mu_{\hat{\ell} - 1}
\]

\[
+ \sum_{t=1}^{\hat{\ell} - 3} \frac{n - t}{3} \mu_t
\]

\[
= \frac{n(n - \hat{\ell})(n - \hat{\ell} - 1)(n + 4\hat{\ell})}{3(n - 1)(n - 2)(n - 3)} + \frac{4(n - \hat{\ell} - 1)}{n - \hat{\ell} + 1}
\]

\[
+ \sum_{t=1}^{\hat{\ell} - 3} \frac{2(n - 2\hat{\ell} + 1 + t)(n - \hat{\ell})(n - \hat{\ell} + 1)}{(n - t - 1)(n - t - 2)(n - t - 3)}
\]

\[
\overset{(a)}{=} \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)}{(n - 3)(n - 2)} \left( \frac{n(n + 1 - 4\hat{\ell})}{3(n - 1)} + 2(\hat{\ell} - 1) \right),
\]

Therefore, for \( \hat{\ell} \geq 2 \), we obtain

\[
T_1 = \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)}{(n - 3)(n - 2)} \left( \frac{n(n + 1 - 4\hat{\ell})}{3(n - 1)} + 2(\hat{\ell} - 1) \right),
\]

and we can verify that

\[
T_1 - \frac{T_2}{d} = \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)}{(n - 3)(n - 2)} \left( \frac{n(n + 1 - 4\hat{\ell})}{3(n - 1)} + 2(\hat{\ell} - 1) \right)
\]

\[
- \frac{(4\hat{\ell} + 2 - n)(n - \hat{\ell})(n - \hat{\ell} - 1)}{6(n - 2)(n - 1)}
\]

\[
= \frac{(n - \hat{\ell})(n - \hat{\ell} - 1)}{2(n - 1)}
\]

\[
= \frac{\Gamma_{k,d,\hat{\ell}}}{d},
\]

APPENDIX E

PROOF OF LEMMA 4

From (74), we know that for \( t = 0, \ldots, k - 2 \),

\[
H \left( W_{t+1:k} | S^{(t)} \right)
\]

\[
\leq \sum_{i=t+1}^{k} H \left( W_i | S^{(t)} \right) + \frac{d - t + 1}{2} H \left( S^{(t+1:k)} | S^{(t)} \right)
\]

\[
- \sum_{i=t+2}^{k} H \left( S^{(t+1:k-1)} | S^{(t)} \right) - H \left( S^{(t+1:k)} | S^{(t)} \right).
\]
Then we have
\[
H\left(W_{t+1:k}|S^{[t]}\right) \\
\leq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}\right) + \frac{d-t+1}{2} H\left(S^{[t+1]}|S^{[t]}\right) \\
- \sum_{i=t+2}^{k} H\left(S^{[t+1:i-1]}|S^{[t]}\right) - H\left(S^{[t+1:k]}|S^{[t]}\right) \\
= \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t]}, S^{[t+1:i-1]}\right) \\
+ \frac{d-t+1}{2} H\left(S^{[t+1]}|S^{[t]}\right) - H\left(S^{[t+1:k]}|S^{[t]}\right) \\
\leq \sum_{i=t+1}^{k} H\left(W_{i}|S^{[t-1]}\right) + \frac{d-t+1}{2} H\left(S^{[t+1]}|S^{[t]}\right) \\
- H\left(S^{[t+1:k]}|S^{[t]}\right),
\]
where (a) follows from the symmetry. Therefore, we have
\[
2 \cdot H\left(W_{t+1:k}|S^{[t]}\right) \\
\implies H\left(W_{t+1:k}|S^{[t]}\right) + H\left(S^{[t+1:k]}|S^{[t]}\right) \\
\leq (k-t) \alpha - \sum_{i=t}^{k-1} H\left(S^{[i]}\right) + \frac{d-t+1}{2} H\left(S^{[t+1]}|S^{[t]}\right),
\]
where (b) follows from Proposition 1.

Upon dividing by 2, we obtain
\[
H\left(W_{t+1:k}|S^{[t]}\right) \\
\leq \frac{1}{2} (k-t) \alpha - \frac{1}{2} \sum_{i=t}^{k-1} H\left(S^{[i]}\right) + \frac{1}{4} (d-t+1) H\left(S^{[t+1]}|S^{[t]}\right),
\]
for \(t = 0, \ldots, k-2\).

Since \(t = \ell - 1\) in (89), we have
\[
H\left(W_{\ell:k}|S^{[\ell-1]}\right) \leq \frac{1}{2} (k-\ell+1) \alpha - \frac{1}{2} \sum_{i=\ell+1}^{k-1} H\left(S^{[i]}\right) \\
+ \frac{1}{4} (d-\ell+2) H\left(S^{[\ell]}|S^{[\ell-1]}\right).
\]
Finally, consider
\[
H\left(W_{t+1:k}|S^{[t]}\right) = H\left(W_{t+1:k}, S^{[t]}\right) - H\left(S^{[t]}\right) \\
\overset{(c)}{=} H\left(W_{t+1:k}, S^{[t+1:k]}\right) - H\left(S^{[t]}\right) \\
= H\left(W_{t+1:k}|S^{[t+1:k]}\right) - H\left(S^{[t]}|S^{[t+1:k]}\right),
\]
where (c) follows from Proposition 1. By substituting (90) into (91), we obtain
\[
H\left(W_{t+1:k}|S^{[t]}\right) \\
\leq \frac{1}{2} (k-\ell+1) \alpha - \frac{1}{2} \sum_{i=(\ell+1)}^{k-1} H\left(S^{[i]}\right) \\
+ \frac{1}{4} (d-\ell+2) H\left(S^{[\ell]}|S^{[\ell-1]}\right) - H\left(S^{[\ell]}|S^{[\ell-1]}\right) \\
= \frac{1}{2} (k-\ell+1) \alpha - \frac{1}{2} \sum_{i=(\ell+1)}^{k-1} H\left(S^{[i]}\right) \\
+ \frac{1}{4} (k-\ell+2) H\left(S^{[\ell]}|S^{[\ell-1]}\right),
\]
which completes the proof.

APPENDIX F
PROOF OF LEMMA 5
We first prove (36). For any \(y = \ell + 1, \ldots, k\) and \(\ell \leq t_y \leq y-1\), consider
\[
H\left(S^{[y]}|S^{[t_y]}, W_{[t_y+1:y-1]}\right) \\
= H\left(S^{[y]}|S^{[y-1]}|S^{[t_y]}, W_{[t_y+1:y-1]}\right) \\
= H\left(S^{[y]}|S^{[y-1]}|S^{[t_y]}, W_{[t_y+1:y-1]}\right) \\
\overset{(a)}{=} H\left(S^{[y]}|S^{[y-1]}|S^{[t_y]}, S^{[t_y+1:y-1]}\right) \\
\overset{(b)}{=} \frac{d+1-y}{d-t_y} H\left(S^{[y]}|S^{[y-1]}|S^{[t_y+1:y-1]}\right) \\
\overset{(c)}{=} \frac{d+1-y}{d-t_y} H\left(S^{[y]}|S^{[t_y+1:y-1]}\right),
\]
where (a) follows because \(S^{[t_y+1:y-1]}\) is a function of \(W_{[t_y+1:y-1]}\), (b) follows from Lemma 2, and (c) is justified by invoking the symmetry.

Now, we focus on (37). If \(t_y = y - 1\), we have
\[
H\left(W_{y}|S^{[y]}\right) \leq H\left(W_{[t_y+1:y-1]}\right) \\
\overset{(93)}{=} H\left(W_{y}|S^{[y]}, W_{[t_y+1:y-1]}\right) \\
\overset{(a)}{=} H\left(W_{y}|S^{[y]}, S^{[t_y-1]}, W_{[t_y+1:y-1]}\right) \\
\overset{(b)}{=} H\left(W_{y}|S^{[y]}, S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
= H\left(W_{y}|S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
- I\left(W_{y}; S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
\overset{(c)}{=} H\left(S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
- H\left(W_{y}; S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
- I\left(W_{y}; S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right),
\]
where the last step follows from the symmetry. For \(\ell \leq t_y \leq y-2\), consider
\[
H\left(W_{y}|S^{[t_y]}, W_{[t_y+1:y-1]}\right) \\
\overset{(93)}{=} H\left(W_{y}|S^{[t_y]}, S^{[t_y-1]}, W_{[t_y+1:y-1]}\right) \\
\overset{(a)}{=} H\left(W_{y}|S^{[t_y]}, S^{[t_y-1]}, W_{[t_y+1:y-1]}\right) \\
\overset{(b)}{=} H\left(W_{y}|S^{[t_y]}, S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
= H\left(W_{y}|S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
- I\left(W_{y}; S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
\overset{(c)}{=} H\left(S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
- H\left(W_{y}; S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right) \\
- I\left(W_{y}; S^{[t_y-1]}, W_{t_y}, W_{[t_y+1:y-1]}\right),
\]
where (a) follows because $t_y \geq \ell \geq 1$, so that $S^y$ is well defined, (b) follows because $W_{t_y}$ is a function of $S^y$, (c) follows because $W_y$ is a function of $S^y$, (d) is obtained from the symmetry by interchanging the indices $y$ and $t_y$ in the second term (while keeping the indices $[t_y-1]$ and $[t_y+1 : y-1]$ fixed), and (e) is obtained from the symmetry by replacing the index $t_y$ by $y-1$ and the indices $[t_y+1 : y-1]$ by $[t_y : y-2]$ (while keeping the indices $[t_y-1]$ fixed).

On the right-hand side of (94), we can upper bound the first term as

$$H \left( S^y | S^{[t_y-1]}, W_{[t_y:y-1]} \right) \leq \frac{d + 1 - y}{d + 1 - t_y} H \left( S^y | S^{[t_y-1]} \right);$$

(95)

this can be obtained by following the proof of (92) step-by-step with $t_y$ replaced by $t_y - 1$. For the second term on the right-hand side of (94), we have

$$H \left( S^{y-1} | S^{[t_y-1]}, W_{[t_y:y-2]}, W_{y-1} \right) \tag{d}$$

$$= H \left( S^{y-1} | S^{[t_y-1]}, W_{[t_y:y-2]}, W_{y-1}, S^{[t_y:y-2]}_{y-1} \right)$$

$$\geq H \left( S^{y-1} | S^{[t_y-2]} \right)$$

(96)

Similarly, for $j = \ell, \ldots, k - 1$, let

$$\Lambda_1(j) = \{ (x, y) : q_{x,y} = 1, t_{x,y} = j - 1 \},$$

$$\Lambda_2(j) = \{ (x, y) : q_{x,y} = 0, t_{x,y} = j, y \neq j + 1 \},$$

and

$$\Lambda_3(j) = \{ (x, y) : q_{x,y} = 0, t_{x,y} \neq j, y = j + 1 \}.$$
and
\[
\Delta_2(j) = \{(x, y) : q_{x,y} = 0, t_{x,y} \neq j + 1, y = j + 2\}.
\]
Here, \(\Delta_1(j)\) is the set of all \((x, y)\) that contributes to the coefficient of \(H(S_n^{(j)})\) via the second term in the upper bound in the second line of (37), and \(\Delta_2(j)\) is the set of all \((x, y)\) that contributes to the coefficient of \(H(S_n^{(j)})\) via the second term in the upper bound in the first line of (37). Since \(\Delta_1(j)\) and \(\Delta_2(j)\) are disjoint, for the row \(x\), \(\nu_{x,j}\) is defined by
\[
\nu_{x,j} = \sum_y \left( \bar{1}_{\Delta_1(j)}((x, y)) + \bar{1}_{\Delta_2(j)}((x, y)) \right),
\]
and so we have
\[
\tilde{\nu}_j = \frac{1}{m} \sum_x \nu_{x,j} = \frac{1}{m} \sum_{x,y} \left( \bar{1}_{\Delta_1(j)}((x, y)) + \bar{1}_{\Delta_2(j)}((x, y)) \right).
\]
(98)

Now, consider
\[
\frac{\Gamma_{k,d,t}}{d} - \frac{d + 1 - \ell}{\ell} \mu_t - \frac{1}{\ell} \left( \sum_{j=1+1}^{k} \delta_j \right) = \frac{\Gamma_{k,d,t}}{d} - \frac{1}{\ell} \left( \sum_{j=1}^{k-1} \tilde{\nu}_j \right) - \frac{1}{\ell} \sum_{j=1}^{k-1} (d + 1 - j) \mu_j - \sum_{j=1}^{k-1} \tilde{\nu}_j = \frac{\Gamma_{k,d,t}}{d} - \frac{1}{\ell} \sum_{j=1}^{k-1} \tilde{\nu}_j + \frac{1}{\ell} \sum_{j=1}^{k-1} \sum_{i=j}^{k-1} \tilde{\nu}_i.
\]
(99)

First, focus on \(\sum_{j=1}^{k} (d + 1 - j) \mu_j\). Then we have
\[
\sum_{j=1}^{k} (d + 1 - j) \mu_j = \sum_{j=1}^{k} (d + 1 - j) \frac{1}{m} \sum_{x,y} \bar{1}_{\Delta_1(j)}((x, y)) \frac{d + 1 - y}{d + 1 - j} + \sum_{j=1}^{k} (d + 1 - j) \frac{1}{m} \sum_{x,y} \bar{1}_{\Delta_2(j)}((x, y)) \frac{d + 1 - y}{d + 1 - j} - \sum_{j=1}^{k} (d + 1 - j) \frac{1}{m} \sum_{x,y} \bar{1}_{\Delta_3(j)}((x, y)) + \frac{1}{m} \sum_{j=1}^{k} \sum_{x,y} \bar{1}_{\Delta_1(j)}((x, y)) (d + 1 - y) + \frac{1}{m} \sum_{j=1}^{k} \sum_{x,y} \bar{1}_{\Delta_2(j)}((x, y)) (d + 1 - y) - \frac{1}{m} \sum_{j=1}^{k} \sum_{x,y} \bar{1}_{\Delta_3(j)}((x, y)) (d + 1 - y).
\]
(100)

where (a) follows because for fixed \(x\) and \(y\), \(\bar{1}_{\Delta_3(j)}((x, y)) = 1\) only if \(j = y - 1\).

Since \(\Delta_1(j) \cap \Delta_1(j') = \emptyset\), \(\Delta_2(j) \cap \Delta_2(j') = \emptyset\) and \(\Delta_3(j) \cap \Delta_3(j') = \emptyset\) for \(j \neq j'\), we have
\[
\sum_{j=1}^{k} \bar{1}_{\Delta_1(j)}((x, y)) = \bar{1}_{\cup_j \Delta_1(j)}((x, y)),
\]
\[
\sum_{j=1}^{k} \bar{1}_{\Delta_2(j)}((x, y)) = \bar{1}_{\cup_j \Delta_2(j)}((x, y)),
\]
and
\[
\sum_{j=1}^{k} \bar{1}_{\Delta_3(j)}((x, y)) = \bar{1}_{\cup_j \Delta_3(j)}((x, y)).
\]

By examining the set \(\cup_j \Delta_1(j)\), we have
\[
\bigcup_j \Delta_1(j) = \{(x, y) : q_{x,y} = 1, \ell - 1 \leq t_{x,y} \leq k - 1\},
\]
and hence
\[
\bar{1}_{\cup_j \Delta_1(j)}((x, y)) = \begin{cases} 1, & \text{if } q_{x,y} = 1, \\ 0, & \text{if } q_{x,y} = 0, \end{cases}
\]
(101)

which is equivalent to
\[
\bar{1}_{\cup_j \Delta_1(j)}((x, y)) = q_{x,y}.
\]

Similarly, for the sets \(\cup_j \Delta_2(j)\) and \(\cup_j \Delta_3(j)\), we have
\[
\bigcup_j \Delta_2(j) = \{(x, y) : q_{x,y} = 0, y \neq t_{x,y} + 1\},
\]
and
\[
\bigcup_j \Delta_3(j) = \{(x, y) : q_{x,y} = 0, t_{x,y} \neq y - 1\}.
\]

Note that \(\cup_j \Delta_2(j) = \cup_j \Delta_3(j)\). By letting
\[
\Delta = \bigcup_j \Delta_2(j) = \bigcup_j \Delta_3(j),
\]
(102)
we have
\[ 1_{\cup_j \Delta_2(j)}((x, y)) = 1_{\cup_j \Delta_3(j)}((x, y)) = 1_{\Delta}((x, y)). \] (103)

Hence, (100) can be written as
\[
\begin{align*}
\sum_{j=\ell}^{k} (d + 1 - j)\bar{\nu}_j \\
= \frac{1}{m} \sum_{x, y} (d + 1 - y) 1_{\cup_j \Delta_1(j)}((x, y)) \\
+ \frac{1}{m} \sum_{x, y} (d + 1 - y) 1_{\cup_j \Delta_2(j)}((x, y)) \\
- \frac{1}{m} \sum_{x, y} (d + 2 - y) 1_{\cup_j \Delta_3(j)}((x, y)) \\
= \frac{1}{m} \sum_{x, y} (d + 1 - y) q_{x, y} - 1_{\Delta}((x, y)).
\end{align*}
\] (104)

Now, focus on \( \sum_{j=\ell}^{k} \sum_{i=j}^{k-1} \bar{v}_i \) in (99), and we have
\[
\begin{align*}
\sum_{j=\ell}^{k} \sum_{i=j}^{k-1} \bar{v}_i \\
= \sum_{j=\ell}^{k-1} (j - \ell + 1)\bar{v}_j \\
= \sum_{j=\ell}^{k-1} (j - \ell + 1) \frac{1}{m} \sum_{x, y} (1_{\Delta_1(j)}((x, y)) + 1_{\Delta_2(j)}((x, y))) \\
= \frac{1}{m} \sum_{x, y} \sum_{j=\ell}^{k-1} (j - \ell + 1)1_{\Delta_1(j)}((x, y)) \\
+ \frac{1}{m} \sum_{x, y} \sum_{j=\ell}^{k-1} (j - \ell + 1)1_{\Delta_2(j)}((x, y)) \\
= \frac{1}{m} \sum_{x, y} (y - \ell) \sum_{j=\ell}^{k-1} 1_{\Delta_1(j)}((x, y)) \\
+ \frac{1}{m} \sum_{x, y} (y - \ell) \sum_{j=\ell}^{k-1} 1_{\Delta_2(j)}((x, y))
\end{align*}
\]

where (b) follows because for fixed \( x \) and \( y \), \( 1_{\Delta_1(j)}((x, y)) = 1 \) only if \( y = j + 1 \) and \( 1_{\Delta_2(j)}((x, y)) = 1 \) only if \( y = j + 2 \). Since \( \Delta_1(j) \cap \Delta_1(j') = \emptyset \) and \( \Delta_2(j) \cap \Delta_2(j') = \emptyset \) for \( j \neq j' \), we have
\[
\begin{align*}
\sum_{j=\ell}^{k-1} 1_{\Delta_1(j)}((x, y)) = 1_{\cup_j \Delta_1(j)}((x, y)), \\
\sum_{j=\ell}^{k-1} 1_{\Delta_2(j)}((x, y)) = 1_{\cup_j \Delta_2(j)}((x, y)).
\end{align*}
\]

By examining the sets \( \cup_j \Delta_1(j) \) and \( \cup_j \Delta_2(j) \), we have
\[
\begin{align*}
\bigcup_j \Delta_1(j) &= \{ (x, y) : q_{x, y} = 0, t_{x, y} = y - 1 \}, \\
\bigcup_j \Delta_2(j) &= \{ (x, y) : q_{x, y} = 0, t_{x, y} \neq y - 1, \ell + 2 \leq y \leq k + 1 \}.
\end{align*}
\]

Since \( \ell + 1 \leq y \leq k \), \( \cup_j \Delta_2(j) \) can be written as \( \{ (x, y) : q_{x, y} = 0, t_{x, y} \neq y - 1, y \neq \ell + 1 \} \). Note that if \( y = \ell + 1 \), then \( t_{x, y} = \ell = y - 1 \), so we know that \( t_{x, y} \neq y - 1 \) implies that \( y \neq \ell + 1 \). Hence, \( \cup_j \Delta_2(j) \) can be written as
\[
\bigcup_j \Delta_2(j) = \{ (x, y) : q_{x, y} = 0, t_{x, y} \neq y - 1 \}.
\]

We can easily see that \( \cup_j \Delta_2(j) = \Delta \), where \( \Delta \) is defined in (102).

By letting
\[
\Delta' = \bigcup_j \Delta_1(j),
\]
we have
\[
\begin{align*}
\sum_{j=\ell}^{k-1} 1_{\Delta_1(j)}((x, y)) &= 1_{\cup_j \Delta_1(j)}((x, y)) = 1_{\Delta'}((x, y)).
\end{align*}
\]

Also,
\[
\sum_{j=\ell}^{k-1} 1_{\Delta_2(j)}((x, y)) = 1_{\cup_j \Delta_2(j)}((x, y)) = 1_{\Delta}((x, y)).
\]

Hence, we obtain that
\[
\begin{align*}
\sum_{j=\ell}^{k} \sum_{i=j}^{k-1} \bar{v}_i \\
= \frac{1}{m} \sum_{x, y} (y - \ell) \sum_{j=\ell}^{k-1} 1_{\Delta_1(j)}((x, y)) \\
+ \frac{1}{m} \sum_{x, y} (y - \ell) \sum_{j=\ell}^{k-1} 1_{\Delta_2(j)}((x, y)) \\
= \frac{1}{m} \sum_{x, y} ((y - \ell)1_{\Delta}((x, y)) + (y - \ell - 1)1_{\Delta}((x, y)))
\end{align*}
\] (105)

By substituting (104) and (105) in (99), we obtain
\[
\frac{\Gamma_{k,d,\ell}}{d} - \frac{d + 1 - \ell}{\ell} \bar{\mu}_\ell - \frac{1}{\ell} \left( \sum_{j=\ell+1}^{k} \delta_j \right) \\
= \frac{\Gamma_{k,d,\ell}}{d} - \frac{1}{\ell} \left( \sum_{j=\ell}^{k-1} \bar{v}_j \right) - \frac{1}{\ell} \sum_{j=\ell}^{k} (d + 1 - j)\bar{\mu}_j \\
+ \frac{1}{\ell} \sum_{j=\ell}^{k} \sum_{i=j}^{k-1} \bar{v}_i.
\]
where (c) follows from (104) and (105), and (d) is justified because \( \Delta \) and \( \Delta' \) are disjoint and \( \Delta \cup \Delta' = \{ (x, y) : q_{x,y} = 0 \} \).

Since we know from (37) and (41) that \( m \sum_{j=\ell}^{k-1} \bar{v}_j \) corresponds to the total number of zeros in the matrix \( Q \), we have

\[
m \sum_{j=\ell}^{k-1} \bar{v}_j = \sum_{x,y} (1 - q_{x,y}),
\]

and so

\[
\sum_{x,y} q_{x,y} = m(k - \ell) - m \sum_{j=\ell}^{k-1} \bar{v}_j = m(k - \ell) - m \frac{\Gamma_{k,d,\ell}}{d},
\]

where (e) follows from (43). Finally, we obtain that

\[
\begin{align*}
&= \frac{\Gamma_{k,d,\ell}}{d} - \frac{d+1-\ell}{\ell} \bar{\mu}_\ell - \frac{1}{\ell} \left( \sum_{j=\ell+1}^{k-1} \bar{\delta}_j \right) \\
&= \frac{\Gamma_{k,d,\ell}}{d} - \frac{1}{\ell} \left( \sum_{j=\ell+1}^{k-1} \bar{v}_j \right) - \frac{d+1-\ell}{\ell m} \sum_{x,y} q_{x,y} \\
&\quad + \frac{1}{\ell} \sum_{y=\ell+1}^{k} (y - \ell) \\
&= \frac{1}{\ell} \left( \sum_{i=\ell+1}^{k} (d+1-i) - \sum_{i=\ell+1}^{k} (d+1-\ell) + \sum_{i=\ell+1}^{k} (i - \ell) \right) \\
&= 0,
\end{align*}
\]

which completes the proof.

### Appendix H

**Proof of Proposition 8**

For \( j = \ell + 1, \ldots, k - 1 \), \( \bar{\delta}_j \) can be written as

\[
\bar{\delta}_j = (d+1-j)\bar{\mu}_j - \sum_{i=\ell+1}^{j-1} \bar{v}_i \\
= (d+1-j) \left( 1 - z_{j+1} \right) - (d+1-k)z_{\ell+k-j+1} \\
- \sum_{i=\ell+1}^{j-1} z_i - \sum_{i=\ell+1}^{j} z_i.
\]

Recall that we need to prove that for any \((k,d,\ell) \in P_1\), \( \bar{\delta}_j \geq 0 \) for \( j = \ell + 1, \ldots, k - 1 \). When \( \ell = k-2 \) and \( \ell = k-3 \), we need to verify that \( \bar{\delta}_{\ell+1} \geq 0 \) provided that \( k \geq \frac{1}{4}(d+7) \), and \( \bar{\delta}_{\ell+2} \geq 0 \) provided that \( k \geq \frac{1}{4}(d+8) \), respectively. This can be justified by substituting values in (106), and the verification details are omitted here.

Now, we consider the case \( \ell \leq k-4 \). We need to show that for any given \((k,d,\ell) \), where \( \ell \leq k-4 \), if \( g(\ell) \geq 0 \) (c.f.(66)), then \( \bar{\delta}_j \geq 0 \) for \( j = \ell + 1, \ldots, k - 1 \).

First, we claim that if \( g(\ell) \geq 0 \), then \( \ell \geq d - k + 1 \). To see this, recall that we know from the discussion in Appendix B that \( g(\ell) \geq 0 \) if and only if \( \ell_1 \leq \ell \leq \ell_2 \), where

\[
\ell_1 = \frac{1}{3} \left( 3d-k-1-\sqrt{3(d-k)^2+12(d-k)+(k-8)^2} \right).
\]

Clearly, to justify the claim, we only need to show that \( \ell_1 \geq d - k + 1 \). Consider

\[
\ell_1 = (d-k+1) + \frac{1}{3} \left( \sqrt{(2k-4)^2} - \sqrt{(2k-4)^2+3d-k-4} \right),
\]

and we can see that \( \ell_1 \geq d - k + 1 \) if and only if \( d - 2k + 4 \leq 0 \). Hence, it remains to show that if \( g(\ell) \geq 0 \) for some \( \ell \leq k-4 \), then \( d - 2k + 4 \leq 0 \). Since we know from Appendix B that if \( g(\ell) \geq 0 \) for some \( \ell \leq k-4 \), then \( g(\ell') \geq 0 \) for any \( \ell' \) such that \( \ell \leq \ell' \leq k-4 \). In particular, we have \( g(k-4) \geq 0 \).

Hence, we have

\[
g(k-4) = d(d-k+3) - \frac{1}{2}(2d-2k+5)(2d-2k+7) \\
= (2k-d-6)(d-k+3) + \frac{1}{2} \geq 0,
\]

which implies that \( d - 2k + 4 \leq 0 \) since \( k \) and \( d \) are integers and \( d \geq k \). Thus, we have proved the claim that if \( g(\ell) \geq 0 \), then \( \ell \geq d - k + 1 \).

Under the condition \( \ell \geq d - k + 1 \), (48) can be written as

\[
z_j = \begin{cases} 
\frac{2d-k-\ell+1}{d}, & j = \ell + 1, \\
\frac{2d-k-2\ell+1}{2d-k}, & j = \ell + 2, \ldots, k - 1, \\
0, & j = k.
\end{cases}
\]

Now, we write \( \bar{\delta}_j \) explicitly for all values of \( j \). Recall from (106) that

\[
\bar{\delta}_j = (d+1-j) \left( 1 - z_{j+1} \right) - (d+1-k)z_{\ell+k-j+1} \\
- \sum_{i=\ell+1}^{j-1} z_i - \sum_{i=\ell+1}^{j} z_i.
\]
If \( j = \ell + 1 \), we have
\[
\tilde{\delta}_{\ell+1} = (d - \ell) (1 - z_{\ell+2}) - (d + 1 - k)z_k
- \sum_{i=\ell+1}^{k} z_i - \sum_{i=\ell+1}^{k} z_{i-1}
\geq \frac{g(\ell)}{d}
\geq 0.
\]

If \( j = k - 1 \), we have
\[
\tilde{\delta}_{k-1} = (d - k + 2) (1 - z_k) - (d + 1 - k)z_{\ell+2} - z_{\ell+1}
\geq \frac{(2d - k - \ell + 1)(d - k + 1)}{2d}
\geq 0.
\]

For \( j = \ell + 2, \ldots, k - 2 \), we have
\[
\tilde{\delta}_j = (d + 1 - j) (1 - z_{j+1}) - (d + 1 - k)z_{\ell+1}
- \sum_{i=j+2}^{k} z_i - \sum_{i=\ell+1}^{k} z_{i-1}
= (d + 1 - j) - \frac{(2d + k - 3j + 1)(2d - k - \ell + 1)}{2d}.
\]

One can easily check that
\[
\tilde{\delta}_j = (d + 1 - j) - \frac{(2d + k - 3j + 1)(2d - k - \ell + 1)}{2d} \geq 0
\]
for \( j = \ell + 2, \ldots, k - 2 \).

REFERENCES

[1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” IEEE Trans. Inf. Theory, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[2] K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, “Explicit construction of optimal exact regenerating codes for distributed storage,” in Proc. 47th Annu. Allerton Conf. Commun. Control. Comput., Oct. 2009, pp. 1243–1249.

[3] C. Tian, “Characterizing the rate region of the (4, 3, 3) exact-repair regenerating codes,” IEEE J. Sel. Areas Commun., vol. 32, no. 5, pp. 967–975, May 2014.

[4] B. Sasidharan, K. Senthoor, and P. V. Kumar, “An improved outer bound on the storage-repair-bandwidth tradeoff of exact-repair regenerating codes,” in Proc. IEEE Int. Symp. Inf. Theory, Honolulu, HI, USA, Jun./Jul. 2014, pp. 2430–2434.

[5] I. M. Duursma, “Outer bounds for exact repair codes,” 2014, arXiv:1406.4852. [Online]. Available: https://arxiv.org/abs/1406.4852

[6] S. Mohajer and R. Tandon, “New bounds on the (n, k, d) storage systems with exact repair,” in Proc. IEEE Int. Symp. Inf. Theory, Jun. 2015, pp. 2056–2060.

Fangwei Ye (S’16–M’19) received the B.Eng. degree in Information Engineering from Southeast University, in 2013, and the Ph.D. degree from Department of Information Engineering, The Chinese University of Hong Kong, in 2018. He is currently a Post-Doctoral Associate with Department of Electrical and Computer Engineering, Rutgers University. His research interests include information theory and its applications to security and privacy, and coding opportunities in networking.

Shiqiu Liu (M’19) received the B.Sc and M.Sc degrees in Mathematics and Applied Mathematics from Jilin University in 2010 and 2013, respectively, and the Ph.D degree in Applied Mathematics from Nanyang Technological University, Singapore, in 2016. From 2016 to 2018, she was a Post-doctoral Fellow with the Institute of Network Coding, The Chinese University of Hong Kong. She is currently an Associate Research Fellow with School of Electronics and Communication Engineering, Sun Yat-Sen University. Her research interests include the coding for distributed storage systems and algebraic coding theory.

Kenneth W. Shum (M’00–SM’16) received the B.Eng. degree from the Department of Information Engineering, The Chinese University of Hong Kong in 1993, and the M.Sc. and Ph.D. degrees from the Department of Electrical Engineering, University of Southern California, in 1995 and 2000, respectively. He is currently an Associate Professor with the School of Science and Engineering, The Chinese University of Hong Kong (Shenzhen). His research interests include the coding for distributed storage systems and sequence design for wireless networks.
Raymond W. Yeung (S’85-M’88-SM’92-F’03) was born in Hong Kong on June 3, 1962. He received the B.S., M.Eng., and Ph.D. degrees in electrical engineering from Cornell University, Ithaca, NY, in 1984, 1985, and 1988, respectively.

He was on leave at Ecole Nationale Supérieure des Télécommunications, Paris, France, during fall 1986. He was a Member of Technical Staff of AT&T Bell Laboratories from 1988 to 1991. Since 1991, he has been with The Chinese University of Hong Kong, where he is now Choh-Ming Li Professor of Information Engineering and Co-Director of Institute of Network Coding. He has held visiting positions at Cornell University, Nankai University, the University of Bielefeld, the University of Copenhagen, Tokyo Institute of Technology, Munich University of Technology, and Columbia University. He was a consultant in a project of Jet Propulsion Laboratory, Pasadena, CA, for salvaging the malfunctioning Galileo Spacecraft and a consultant for NEC, USA. His 25-bit synchronization marker was used onboard the Galileo Spacecraft for image synchronization.

His research interests include information theory and network coding. He is the author of the textbooks A First Course in Information Theory (Kluwer Academic/Plenum 2002) and its revision Information Theory and Network Coding (Springer 2008), which have been adopted by over 100 institutions around the world. This book has also been published in Chinese (Higher Education Press 2011, translation by Ning Cai et al.). He also co-authored with Shenghao Yang the monograph BATS Codes: Theory and Applications (Morgan & Claypool Publishers, 2017). In spring 2014, he gave the first MOOC on information theory that reached over 25,000 students. Dr. Yeung was a member of the Board of Governors of the IEEE Information Theory Society from 1999 to 2001. He has served on the committees of a number of information theory symposiums and workshops. He was General Chair of the First and the Fourth Workshops on Network, Coding, and Applications (NetCod 2005 and 2008), a Technical Co-Chair for the 2006 IEEE International Symposium on Information Theory, a Technical Co-Chair for the 2006 IEEE Information Theory Workshop (Chengdu, China), and a General Co-Chair of the 2015 IEEE International Symposium on Information Theory. He currently serves as an Editor-at-Large of Communications in Information and Systems, an Editor of Foundation and Trends in Communications and Information Theory and of Foundation and Trends in Networking, and was an Associate Editor for Shannon Theory of the IEEE Transactions on Information Theory from 2003 to 2005. In 2011-12, he serves as a Distinguished Lecturer of the IEEE Information Theory Society. He was a recipient of the Croucher Foundation Senior Research Fellowship for 2000/2001, the Best Paper Award (Communication Theory) of the 2004 International Conference on Communications, Circuits and System, the 2005 IEEE Information Theory Society Paper Award, the Friedrich Wilhelm Bessel Research Award of the Alexander von Humboldt Foundation in 2007, the 2016 IEEE Eric E. Sumner Award (“for pioneering contributions to the field of network coding”), and the 2018 ACM SIGMOBILE Test-of-Time Paper Award. In 2015, he was named (together with Zhen Zhang) an Outstanding Overseas Chinese Information Theorist by the China Information Theory Society. In 2019, his team won a Gold Medal with Congratulations of the Jury at the 47th International Exhibition of Inventions of Geneva for their invention “BATS: Enabling the Nervous System of Smart Cities.” He is a Fellow of the IEEE, Hong Kong Academy of Engineering Sciences, and Hong Kong Institution of Engineers.