

Characterizing the Rate Region of the $(4, 3, 3)$ Exact-Repair Regenerating Codes

Chao Tian, *Senior Member, IEEE*

Abstract—Exact-repair regenerating codes are considered for the case $(n, k, d) = (4, 3, 3)$, for which a complete characterization of the rate region is provided. This characterization answers in the affirmative the open question whether there exists a non-vanishing gap between the optimal bandwidth-storage tradeoff of the functional-repair regenerating codes (*i.e.*, the cut-set bound) and that of the exact-repair regenerating codes. To obtain an explicit information theoretic converse, a computer-aided proof (CAP) approach based on primal and dual relation is developed. This CAP approach extends Yeung’s linear programming (LP) method, which was previously only used on information theoretic problems with a few random variables due to the exponential growth of the number of variables in the corresponding LP problem. The symmetry in the exact-repair regenerating code problem allows an effective reduction of the number of variables, and together with several other problem-specific reductions, the LP problem is reduced to a manageable scale. For the achievability, only one non-trivial corner point of the rate region needs to be addressed in this case, for which an explicit binary code construction is given.

I. INTRODUCTION

Erasure codes can be used in data storage systems that encode and disperse information to multiple storage nodes in the network (or multiple disks inside a large data center), such that a user can retrieve it by accessing only a subset of them. This kind of systems is able to provide superior availability and durability in the event of disk corruption or network congestion, at a fraction of the cost of the current state of art storage systems based on simple data replication. When data is coded by an erasure code, data repair becomes more involved, because the information stored at a given node may not be directly available from any one of the remaining storage nodes. One key issue that affects the overall system performance is the total amount of information that the remaining nodes needs to transmit to the new node.

Dimakis *et al.* [1] proposed the framework of regenerating codes to address the tradeoff between the storage and repair bandwidth in erasure-coded distributed storage systems. In this framework, the overall system consists of n storage nodes situated in different network locations, each with α units of data, and the content is coded in such a way that by accessing any k of these n storage nodes, the full data content of B units can be completely recovered. When a node fails, a new node may access any d remaining nodes for β units of data each, in order to regenerate a new data node.

The main result in [1] is for the so-called functional-repair case, where the regenerating process does not need to exactly replicate the original data stored on the failed node, but only

needs to guarantee that the regenerated node can serve the same purpose as the lost node, *i.e.*, data reconstruction using any k nodes, and being able to help regenerate new data nodes to replace subsequently failed nodes. It was shown that this problem can be cleverly converted to a network multicast problem, and the celebrated result on network coding [2] can be applied directly to provide a complete characterization of the optimal bandwidth-storage tradeoff. Furthermore, linear network codes [3] are sufficient to achieve this optimal performance.

The decoding and repair rules for functional-repair regenerating codes may evolve as nodes are repaired, which increases the overhead of the system. Moreover, functional-repair does not guarantee systematic format storage, which is an important requirement in practice. For these reasons, exact-repair regenerating codes have received considerable attention recently [4]–[7], where the regenerated data need to be exactly the same as that stored in the failed node.

The optimal bandwidth-storage tradeoff for the functional-repair case can clearly serve as an outer bound for the exact-repair case. There also exist code constructions for the two extreme cases, *i.e.*, the minimum storage regenerating (MSR) point [5]–[7], or the minimum bandwidth regenerating (MBR) point [4], [6], and the aforementioned outer bound is in fact achievable at these two extreme points. The achievability of these two extreme points immediately implies that for the cases $k \leq 2$, the functional-repair outer bound is tight for the exact repair case. Also relevant is the fact that symbol extensions are necessary for linear codes to achieve the MSR point for some parameter range [5], however the MSR point can indeed be asymptotically (in B) achieved by linear codes for all the parameter range [7]. It was also shown in [4] that when $k > 2$, other than the two extreme points and a segment close to the MSR point, the majority the functional repair outer bound is in fact not strictly achievable by exact-repair regenerating codes.

The non-achievability result reported in [4] was proved by contradiction, *i.e.*, a contradiction will occur if one supposes that an exact-repair code operates *strictly* on the optimal functional-repair tradeoff curve. However, it is not clear whether this contradiction is caused by the functional-repair outer bound being only asymptotically achievable, or caused by the existence of a non-vanishing gap between the optimal tradeoff of exact-repair codes and the functional-repair outer bound. In fact, the necessity of symbol extension proved in [5] and the asymptotically optimal construction given in [7] may be interpreted as suggesting that the former is true.

In this work, we focus on the simplest case of exact-

repair regenerating codes, *i.e.*, when $(n, k, d) = (4, 3, 3)$, for which the rate region has not been completely characterized previously. A complete characterization of the rate region is provided for this case, which shows that indeed there exists a non-vanishing gap between the optimal tradeoff of the exact-repair codes and that of the functional-repair codes. The achievability part of this result shows that there exist exact-repair regenerating codes that are better than simply time-sharing between the MSR point and the MBR point.

As in many open information theoretical problems, the difficulty lies in finding good outer bounds, particularly in this problem with a large number of regenerating and reconstruction requirements. We rely on a computer-aided proof (CAP) approach and take advantage of the symmetry and other problem-specific structure to reduce the number of variables in the optimization problem. This approach builds upon Yeung's linear programming (LP) framework [8]. As of our knowledge, this is the first time that the LP framework is meaningfully applied to a non-trivial engineering problem, which leads to a complete solution. More importantly, instead of only machine-proving whether an information theoretic bound is true or not as in [8], we further develop a secondary optimization procedure to find an *explicit information theoretic proof*. By solving the primary LP optimization problem, the tradeoff curve between the storage and repair bandwidth can be traced out numerically, which leads to the hypotheses of the bounding planes for the rate region. A secondary optimization procedure, which essentially solves the dual problem for these candidate bounding planes, directly yields an explicit information theoretic proof. Due to the duality structure in the LP problem, the optimization criterion in the secondary optimization problem can be selected arbitrarily, thus we can choose one that leads to the solution that we most desire. For this purpose, the ℓ_1 norm is chosen that approximates the solution under the ℓ_0 norm, the latter of which gives the sparsest solution and translates roughly to a converse proof with the least number of steps.

The rest of the paper is organized as follows. In Section II, we provide a formal definition of the problem and review briefly the functional-repair outer bound. The characterization of the rate region is given in Section III, together with the forward and converse proof. Section IV provides details on the computer-aid proof approach, and Section V concludes the paper.

II. PROBLEM DEFINITION

In this section we first give a formal definition of the regenerating code problem for the case $(n, k, d) = (4, 3, 3)$, and then introduce some notation useful for the converse proof. Somewhat surprisingly, we were not able to find such a formal definition in the existing literature, and thus believe it is beneficial to include one here (which can be generalized to other parameters). The functional-repair outer bound is briefly reviewed and specialized to the case under consideration.

A. Exact-Repair Regenerating Codes

A $(4, 3, 3)$ exact-repair regenerating code is formally defined as follows, where the notation I_n is used to denote the set

$\{1, 2, \dots, n\}$, and $|A|$ is used to denote the cardinality of a set A .

Definition 1: An (N, K_d, K) exact-repair regenerating code for the $(4, 3, 3)$ case consists of 4 encoding functions $f_i^E(\cdot)$, 4 decoding functions $f_A^D(\cdot, \cdot, \cdot)$, 12 repair encoding functions $F_{i,j}^E(\cdot)$, and 4 repair decoding functions $F_i^D(\cdot, \cdot, \cdot)$, where

$$f_i^E : I_N \rightarrow I_{K_d}, \quad i \in I_4,$$

each of which maps the message $m \in I_N$ to one piece of coded information,

$$f_A^D : I_{K_d} \times I_{K_d} \times I_{K_d} \rightarrow I_N, \quad A \subset I_4 \quad \text{and} \quad |A|=3,$$

each of which maps 3 pieces of coded information stored on a set A of nodes to the original message,

$$F_{i,j}^E : I_{K_d} \rightarrow I_K, \quad j \in I_4, \quad \text{and} \quad i \in I_4 \setminus \{j\},$$

each of which maps a piece of coded information at node i to an index that will be made available to reconstruct the data at node j , and

$$F_j^D : I_K \times I_K \times I_K \rightarrow I_{K_d}, \quad j \in I_4,$$

each of which maps 3 such indices from the helper nodes to reconstruct the information stored at the failed node. The functions must satisfy the data reconstruction conditions

$$f_A^D \left(\prod_{i \in A} f_i^E(m) \right) = m, \quad m \in I_N, \quad A \subset I_4 \quad \text{and} \quad |A|=3, \quad (1)$$

and the repair conditions

$$F_j^D \left(\prod_{i \in I_4 \setminus \{j\}} F_{i,j}^E(f_i^E(m)) \right) = f_j^E(m), \quad m \in I_N, \quad j \in I_4. \quad (2)$$

In the above definition, N is the cardinality of the message set, and $\log N$ is essentially B . Similarly $\log K_d$ is essentially α and $\log K$ is β . To include the case when the storage-bandwidth tradeoff may be approached asymptotically, *e.g.*, the codes considered in [7], the following definition which utilized a normalized version of α and β is further introduced.

Definition 2: A normalized bandwidth-storage pair $(\bar{\alpha}, \bar{\beta})$ is said to be $(4, 3, 3)$ exact-repair achievable if for any $\epsilon > 0$ there exists an (N, K_d, K) exact-repair regenerating code such that

$$\bar{\alpha} + \epsilon \geq \frac{\log K_d}{\log N}, \quad \bar{\beta} + \epsilon \geq \frac{\log K}{\log N}. \quad (3)$$

The collection of all the achievable $(\bar{\alpha}, \bar{\beta})$ pairs is the achievable region \mathcal{R} of the $(4, 3, 3)$ exact-repair regenerating codes.

The reconstruction condition (1) requires that there is no decoding error, *i.e.*, the zero-error requirement is adopted. An alternative definition is to require instead the probability of decoding error to be asymptotically zero as $N \rightarrow \infty$. It will become clear from the rate region characterization given in the sequel that this does not cause any essential difference, and thus we do not give this alternative definition to avoid

repetition.

B. Some Further Notation

In order to derive the outer bound, it is convenient to write the reconstruction and regenerating conditions in the form of entropy constraints. For this purpose, some further notation is introduced here, which is largely borrowed from [4].

Let us denote the message random variable as M , which is uniformly distributed in the set I_N . Define

$$W_i = f_i^E(M), \quad S_{i,j} = F_{i,j}^E(f_i^E(M)). \quad (4)$$

Thus we have the following random variables in the set $\mathcal{W} \cup \mathcal{S}$

$$\mathcal{W} = \{W_1, W_2, W_3, W_4\}, \quad (5)$$

$$\mathcal{S} = \{S_{1,2}, S_{1,3}, S_{1,4}, S_{2,1}, S_{2,3}, S_{2,4}, S_{3,1}, S_{3,2}, S_{3,4}, S_{4,1}, S_{4,2}, S_{4,3}\}. \quad (6)$$

The reconstruction requirement thus implies that

$$H(\mathcal{W} \cup \mathcal{S} | \mathcal{A}) = 0, \quad \text{any } \mathcal{A} \subseteq \mathcal{W} : |\mathcal{A}| = 3. \quad (7)$$

The regenerating requirement implies that

$$H(S_{i,j} | W_i) = 0, \quad j \in I_4, \quad i \in I_4 \setminus \{j\}, \quad (8)$$

and

$$H(W_j | \{S_{i,j} \in \mathcal{S} : i \in I_n \setminus \{j\}\}) = 0, \quad \text{any } j \in I_4. \quad (9)$$

Because the message M has a uniform distribution, we also have that

$$H(\mathcal{W} \cup \mathcal{S}) = H(M) = \log N \triangleq B, \quad (10)$$

which is strictly larger than zero. Note that together with (7), this implies that

$$H(\mathcal{A}) = B, \quad \text{any } \mathcal{A} \text{ such that } |\mathcal{A} \cap \mathcal{W}| \geq 3. \quad (11)$$

The symmetric storage requirement can be written as

$$H(W_i) \leq \log K_d \triangleq \alpha, \quad W_i \in \mathcal{W}, \quad (12)$$

and the regenerating bandwidth constraint can be written as

$$H(S_{i,j}) \leq \log K \triangleq \beta, \quad S_{i,j} \in \mathcal{S}. \quad (13)$$

The above constraints (7)-(13) are the constraints that need to be satisfied by any exact-repair regenerating codes. These constraints will be used later in the converse proof.

C. Review of Functional-Repair Outer Bound

The optimal tradeoff for functional-repair regenerating codes was given by Dimakis *et al.* [1], which provides an outer bound for the exact-repair case. The bound has the following form in our notation for the $(4, 3, 3)$ case (see Fig. 1)

$$\sum_{i=0}^2 \min(\bar{\alpha}, (3-i)\bar{\beta}) \geq 1. \quad (14)$$

It is not difficult to show that it can be rewritten as the following four simultaneous linear bounds

$$3\bar{\alpha} \geq 1, \quad 2\bar{\alpha} + \bar{\beta} \geq 1, \quad \bar{\alpha} + 3\bar{\beta} \geq 1, \quad 6\bar{\beta} \geq 1. \quad (15)$$

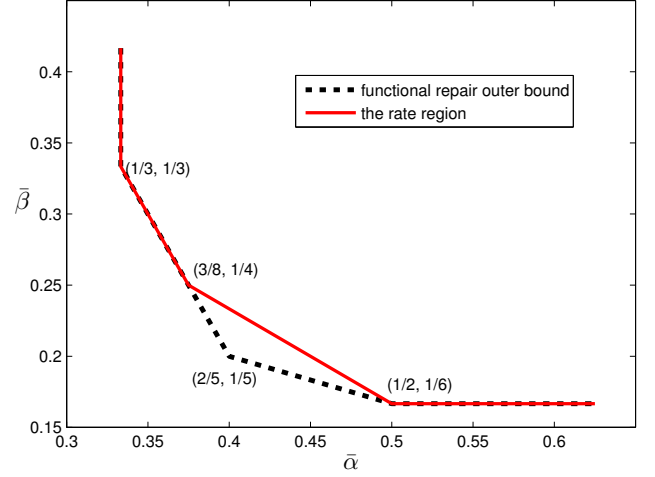


Fig. 1. The functional-repair outer bound and the rate-region \mathcal{R} .

The MSR point for this case is $(\bar{\alpha}, \bar{\beta}) = (\frac{1}{3}, \frac{1}{3})$, and the MBR point is $(\bar{\alpha}, \bar{\beta}) = (\frac{1}{2}, \frac{1}{6})$.

III. THE RATE REGION OF $(4, 3, 3)$ REGENERATING CODES

The following theorem provides a complete characterization of the rate region of the $(4, 3, 3)$ exact-repair regenerating codes.

Theorem 1: The rate region \mathcal{R} of the $(n, k, d) = (4, 3, 3)$ exact-repair regenerating codes is given by the collection of (α, β) pairs that satisfy the following constraints

$$3\bar{\alpha} \geq 1, \quad 2\bar{\alpha} + \bar{\beta} \geq 1, \quad 4\bar{\alpha} + 6\bar{\beta} \geq 3, \quad 6\bar{\beta} \geq 1.$$

This rate region is also depicted in Fig. 1, together with the functional-repair outer bound. It is clear that there is a gap between them, and thus the functional-repair outer bound cannot be asymptotically achievable under the exact-repair requirement. Note that the only difference between the region given in Theorem 1 and that in (15) is the third bounding plane.

A. The Achievability Proof

The rate region \mathcal{R} has three corner points, and thus we only need to show that these three points are all achievable. The MSR point $(\bar{\alpha}, \bar{\beta}) = (\frac{1}{3}, \frac{1}{3})$ is simply achieved by any $(4, 3)$ MDS code, such as the binary systematic code with a single parity check bit. The MBR point $(\bar{\alpha}, \bar{\beta}) = (\frac{1}{2}, \frac{1}{6})$ is also easily obtained by using the repair-by-transfer code construction in [4], which in this case reduces to a simple replication coding. It thus only remains to show that the point $(\bar{\alpha}, \bar{\beta}) = (\frac{3}{8}, \frac{1}{4})$ is also achievable.

Next we shall give a construction for a binary $(4, 3, 3)$ code with $\alpha = 3$, $\beta = 2$ and $B = 8$, which indeed achieves this operating point. The code is illustrated in Table I, where (and in the remainder of this section) the addition $+$ is in the binary field. Here x_i, y_i, z_i, t_i are the systematic bits, $i = 1, 2$, and the remaining bits are the parity bits.

First note that the construction is circularly symmetric, and thus without loss of generality, we only need to consider the

TABLE I
A (4, 3, 3) CODE FOR $(\bar{\alpha}, \bar{\beta}) = (\frac{3}{8}, \frac{1}{4})$.

	first bit	second bit	third bit
node 1	x_1	x_2	$y_1 + z_2 + t_1 + t_2$
node 2	y_1	y_2	$z_1 + t_2 + x_1 + x_2$
node 3	z_1	z_2	$t_1 + x_2 + y_1 + y_2$
node 4	t_1	t_2	$x_1 + y_2 + z_1 + z_2$

TABLE II
REPAIR CONTRIBUTIONS WHEN NODE 1 FAILS.

	first bit	second bit
node 2	y_1	$z_1 + t_2 + x_1 + x_2 + y_1 + y_2$
node 3	z_2	$t_1 + x_2 + y_1 + y_2 + z_1 + z_2$
node 4	$t_1 + t_2$	$x_1 + y_2 + z_1 + z_2 + t_2$

case when node 1 fails. If it can be shown that when node 2, 3, 4 each contribute two bits, node 1 can be reconstructed, which also implies that the complete data can be recovered using only node 2, 3 and 4, then the proof is complete. This can indeed be done using the combination shown in Table II.

Upon receiving these six bits in Table II, the new node can form the following combinations

$$\begin{aligned}
 x_1 + x_2 &+ y_1 + y_2 + z_1 + \mathbf{z_2} + t_2 \\
 x_2 &+ y_1 + y_2 + z_1 + z_2 + t_1 + \mathbf{t_1} + t_2 \\
 x_1 &+ \mathbf{y_1} + y_2 + z_1 + z_2 + t_2,
 \end{aligned}$$

where the first combination is formed by using the second bit from node 2 and the first bit from node 3 (shown in bold), and the other combinations can be formed similarly. In the binary field, this is equivalent to having

$$x_1 + x_2 + y_1 + y_2 + z_1 + z_2 + t_2 \quad (16)$$

$$x_2 + y_1 + y_2 + z_1 + z_2 + t_2 \quad (17)$$

$$x_1 + y_1 + y_2 + z_1 + z_2 + t_2, \quad (18)$$

and it is seen that x_1 can be recovered by simply taking the difference between (16) and (17), and similarly x_2 can be recovered by taking the difference between (16) and (18). Note further that the third bit stored in node 1 is simply the summation of the first bits contributed from node 2, 3, and 4 in Table II. The proof is thus complete.

The hand-crafted code presented above is specific for the (4, 3, 3) case. However, in a recent work, Sasidharan and Kumar [9] discovered a class of codes that is optimal for the $(n, n-1, n-1)$ case at operating points other than MSR or MBR, and specializing it to the (4, 3, 3) case achieves the same performance as the code above; see also [10] for a closely related code construction.

B. The Converse Proof

It is clear that we only need to prove the following bound

$$4\bar{\alpha} + 6\bar{\beta} \geq 3, \quad (19)$$

because the other bounds in the main theorem can be obtained from the outer bound (15). We first give an instrumental result regarding the symmetry of the optimal solution.

Definition 3: A permutation π on the set I_4 is a one-to-one mapping $\pi : I_4 \rightarrow I_4$. The collections of all permutations is denoted as Π .

Any given permutation π correspondingly maps a random variable W_i to $W_{\pi(i)}$. Any subset of \mathcal{W} , e.g., $\mathcal{A} \subseteq \mathcal{W}$, is thus mapped to another set of random variables, denoted as $\pi(\mathcal{A})$. For example, the permutation $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$ and $\pi(4) = 4$ will map the set of random variables $\mathcal{A} = \{W_1, W_4\}$ to $\pi(\mathcal{A}) = \{W_2, W_4\}$. Similarly a random variable $S_{i,j}$ will be mapped to $S_{\pi(i), \pi(j)}$, and for any subset of \mathcal{S} , we use a similar notation as for the case of \mathcal{W} .

Definition 4: An (N, K_d, K) exact-repair regenerating code is said to induce a symmetric entropic vector if for any sets $\mathcal{A} \subseteq \mathcal{S}$ and $\mathcal{B} \subseteq \mathcal{W}$ and any permutation $\pi \in \Pi$,

$$H(\mathcal{A}, \mathcal{B}) = H(\pi(\mathcal{A}), \pi(\mathcal{B})). \quad (20)$$

Definition 5: A normalized bandwidth-storage pair $(\bar{\alpha}, \bar{\beta})$ is said to be symmetrically (4, 3, 3) exact-repair achievable if for any $\epsilon > 0$ there exists an (N, K_d, K) exact-repair regenerating code which induces a symmetric entropic vector such that

$$\bar{\alpha} + \epsilon \geq \frac{\log K_d}{\log N}, \quad \bar{\beta} + \epsilon \geq \frac{\log K}{\log N}. \quad (21)$$

The collection of all such $(\bar{\alpha}, \bar{\beta})$ pairs is the entropy-symmetrical achievable region \mathcal{R}^* of the (4, 3, 3) exact-repair regenerating codes.

With the above definition, it is not difficult to see that the following proposition is true.

Proposition 1: For $(n, k, d) = (4, 3, 3)$ exact-repair regenerating codes $\mathcal{R} = \mathcal{R}^*$.

Clearly the inclusion $\mathcal{R}^* \subseteq \mathcal{R}$ is true. For the other direction, we can invoke a time-sharing (or more precisely here, space-sharing) argument among all possible permutations; the proof is given in the appendix for completeness. We are now ready to prove the converse of Theorem 1.

Converse Proof of Theorem 1: Because of the equivalence in Proposition 1, without loss of generality we only need to prove that the given outer bound holds for the region \mathcal{R}^* , i.e., consider only codes that induce symmetrical entropy vectors.

We first write¹

$$\begin{aligned}
 4\alpha + 6\beta &\geq 4H(W_1) + 6H(S_{2,4}) \\
 &= 4H(W_1) + 3H(S_{2,4}) + 3H(S_{3,4}) \\
 &\geq H(W_1) + 3H(W_1 S_{2,4} S_{3,4})
 \end{aligned} \quad (22)$$

where the first inequality is by (12) and (13), the equality is by the symmetry of the solution

$$H(S_{2,4}) = H(S_{3,4}), \quad (23)$$

and the second inequality is because summation of individual entropy is greater than or equal to the joint entropy.

¹The proof presented here is different from the one given in the preliminary conference version for the same result [11]. The proof here is more concise because further reduction has been applied in the secondary LP problem discussed in the next section.

For notational simplicity, from here on we shall write (s), (7), (8), (9) and (11) on top of the equalities in the derivation to signal the reasons for the equalities, *i.e.*, by the symmetry of the entropy vectors, or by equations (7), (8), (9) and (11), respectively. We next write the following chain of inequalities

$$\begin{aligned}
& 2H(W_1 S_{2,4} S_{3,4}) \\
& \stackrel{(8)}{=} 2H(W_1 S_{1,4} S_{2,4} S_{3,4}) \\
& \stackrel{(9)}{=} 2H(W_1 W_4 S_{1,4} S_{2,4} S_{3,4}) \\
& \stackrel{(8)}{=} 2H(W_1 W_4 S_{2,4} S_{3,4}) \\
& \geq H(W_1 W_4 S_{2,4}) + H(W_1 W_4 S_{2,4} S_{3,4}) \\
& \stackrel{(s)}{=} H(W_2 W_4 S_{1,2}) + H(W_1 W_4 S_{2,4} S_{3,4}) \\
& \stackrel{(8)}{=} H(W_2 W_4 S_{1,2} S_{2,4}) + H(W_1 W_4 S_{1,2} S_{2,4} S_{3,4}) \\
& = H(W_2 | W_4 S_{1,2} S_{2,4}) + H(W_1 S_{3,4} | W_4 S_{1,2} S_{2,4}) \\
& \quad + 2H(W_4 S_{1,2} S_{2,4}) \\
& \geq H(W_1 W_2 S_{3,4} | W_4 S_{1,2} S_{2,4}) + 2H(W_4 S_{1,2} S_{2,4}) \\
& = H(W_1 W_2 W_4 S_{1,2} S_{2,4} S_{3,4}) + H(W_4 S_{1,2} S_{2,4}) \\
& \stackrel{(11)}{=} B + H(W_4 S_{1,2} S_{2,4}). \tag{24}
\end{aligned}$$

It follows that

$$\begin{aligned}
& 4\alpha + 6\beta \\
& \geq B + H(W_1) + H(W_1 S_{2,4} S_{3,4}) + H(W_4 S_{1,2} S_{2,4}). \tag{25}
\end{aligned}$$

However, notice that

$$\begin{aligned}
& H(W_1 S_{2,4} S_{3,4}) + H(W_4 S_{1,2} S_{2,4}) \\
& \stackrel{(8)}{=} H(W_1 S_{1,4} S_{2,4} S_{3,4}) + H(W_4 S_{1,2} S_{2,4}) \\
& \stackrel{(9)}{=} H(W_1 W_4 S_{1,4} S_{2,4} S_{3,4}) + H(W_4 S_{1,2} S_{2,4}) \\
& \stackrel{(s)}{=} H(W_1 W_4 S_{1,4} S_{2,4} S_{3,4}) + H(W_4 S_{3,2} S_{2,4}) \\
& = H(W_1 S_{1,4} S_{3,4} | W_4 S_{2,4}) + H(S_{3,2} | W_4 S_{2,4}) \\
& \quad + 2H(W_4 S_{2,4}) \\
& \geq H(W_1 S_{1,4} S_{3,2} S_{3,4} | W_4 S_{2,4}) + 2H(W_4 S_{2,4}) \\
& = H(W_1 W_4 S_{1,4} S_{2,4} S_{3,2} S_{3,4}) + H(W_4 S_{2,4}) \\
& \stackrel{(8)}{=} H(W_1 W_4 S_{1,2} S_{3,2} S_{4,2} S_{1,4} S_{2,4} S_{3,4}) + H(W_4 S_{2,4}) \\
& \stackrel{(9)}{=} H(W_1 W_2 W_4 S_{1,2} S_{3,2} S_{4,2} S_{1,4} S_{2,4} S_{3,4}) + H(W_4 S_{2,4}) \\
& \stackrel{(11)}{=} B + H(W_4 S_{2,4}). \tag{26}
\end{aligned}$$

This implies that

$$\begin{aligned}
& 4\alpha + 6\beta \\
& \geq 2B + H(W_1) + H(W_4 S_{2,4}) \\
& \stackrel{(s)}{=} 2B + H(W_2) + H(W_4 S_{2,4}) \\
& = 2B + H(W_2) + H(S_{3,1}) + H(W_4 S_{2,4}) - H(S_{3,1}) \\
& \geq 2B + H(W_2 S_{3,1}) + H(W_4 S_{2,4}) - H(S_{3,1}) \\
& \stackrel{(8)}{=} 2B + H(W_2 S_{2,4} S_{3,1}) + H(W_4 S_{2,4}) - H(S_{3,1}) \\
& \stackrel{(s)}{=} 2B + H(W_2 S_{2,4} S_{3,1}) + H(W_4 S_{2,4}) - H(S_{2,4})
\end{aligned}$$

$$\begin{aligned}
& = 2B + H(W_2 S_{3,1} | S_{2,4}) + H(W_4 | S_{2,4}) + H(S_{2,4}) \\
& \geq 2B + H(W_2 W_4 S_{3,1} | S_{2,4}) + H(S_{2,4}) \\
& = 2B + H(W_2 W_4 S_{3,1} S_{2,4}) \\
& \stackrel{(8)}{=} 2B + H(W_2 W_4 S_{2,1} S_{3,1} S_{4,1} S_{2,4}) \\
& \stackrel{(9)}{=} 2B + H(W_1 W_2 W_4 S_{2,1} S_{3,1} S_{4,1} S_{2,4}) \\
& \stackrel{(11)}{=} 3B, \tag{27}
\end{aligned}$$

and the proof is thus complete. ■

It can be seen that the rate region given here remains the same if the codes are required only to have asymptotic zero error probability as B approaches infinity, instead of the more stringent zero-error requirement. We only need to replace the steps where (11) was applied in the above proof to a slightly different version based on Fano's inequality [12], and the details are thus omitted.

IV. THE COMPUTER-AIDED PROOF APPROACH

It should be clear at this point that the converse proof given above is difficult to find manually, in which several rather unconventional steps, such as the adding and subtracting of the same term in the third step of (27), are used. These steps arise from the complex symmetry and dependence structure in the random variables. In fact, the author's own extensive attempt to find such a converse proof manually was utterly unsuccessful, which motivated the investigation of the computer-aided proof (CAP) approach, via which the proof was obtained. In this section, we provide details on our approach used to obtain this converse, which may prove useful for future research.

A. The Basic Primal Linear Program

Yeung provided a linear programming framework to prove Shannon-type information inequalities [8]. The basic framework can be roughly described as follows in the context of the problem being considered.

There are a total number of $2^{16} - 1 = 65535$ joint entropy terms, each of which corresponds to a non-empty subset of the set of 16 random variables in the problem being considered [see (5) and (6)]. Note that every information measure (entropy, conditional entropy, mutual information and conditional mutual information) can be represented as a linear combination of these joint entropies. These joint entropy terms can be viewed as the variables in an optimization problem, and they must satisfy the constraints imposed by the problem, as well as the more general non-problem-specific constraints.

One particular set of general constraints on joint entropies are those imposed by the non-negativity of Shannon's information measures, which are collectively called Shannon-type inequalities [8]. It was shown that without loss of generality, this set of constraints can be represented by the following minimal set of constraints for a collection of random variables $\mathcal{X} = \{X_1, X_2, \dots, X_n\}$:

$$\begin{aligned}
& H(X_i | \{X_k, k \neq i\}) \geq 0, \quad i \in I_n \tag{28} \\
& I(X_i; X_j | \{X_k, k \in K\}) \geq 0, \text{ where } k \in I_n - \{i, j\}, i \neq j. \tag{29}
\end{aligned}$$

Note that in our problem $\mathcal{X} = \mathcal{S} \cup \mathcal{W}$. It can be seen that there are a total of $16 + \binom{16}{2} 2^{14} = 1966096$ constraints in the problem being considered.

Since all the constraints are linear, without loss of generality, we can set $B = 1$. When sweeping through α , for each instance we shall fix $\alpha = \alpha_0 \in [\frac{3}{8}, \frac{1}{2}]$, and seek to find the minimum value of β without violating these constraints, *i.e.*, a lower bound for β when $\alpha = \alpha_0$ and $B = 1$. In addition to the 65535 variables representing the joint entropy terms, an auxiliary variable β is also introduced in the linear program, which will be the objective function subject to minimization. More precisely, we shall consider the following basic optimization problem:

$$\begin{aligned} & \text{minimize: } \beta \\ & \text{subject to: } B = 1 \\ & \quad \alpha = \alpha_0 \\ & \quad \text{constraints (28)-(29)} \\ & \quad \text{constraints (7)-(9), (10)-(13).} \end{aligned} \quad (30)$$

Note that (11) are redundant constraints given (7) and (10) and the Shannon-type inequalities, and thus it is not included in the minimization problem. In this optimization problem, there are a total $1966096 + 4 + 12 = 1966112$ inequality constraints from the Shannon-type inequalities and the constraints (12)-(13), as well as $4 + 12 + 4 + 1 = 21$ equality constraints from (7)-(9) and (10), after substituting the values of B and α into the constraints. It is worth noting that the solution for the above optimization problem is potentially only an outer bound for the rate region, since it does not take into account of non-Shannon type inequalities; nevertheless, it turns out for this problem Shannon-type inequalities are in fact sufficient.

This optimization problem in its basic form is too large for the existing software packages using Yeung's LP framework, *i.e.*, Information Theoretic Inequality Prover (ITIP or XITIP) [13] [14]. In fact, LP problems at this scale in general, with the large total number of constraints in this problem in particular, are on the border of the problems that modern commercial optimization solvers are able to handle. Depending on the software library being used, it may take a few hundred hours without converging. For example, when the popular Cplex optimization library [15] is used, running the solver for 48 hours (2-thread mode on a multi-core Linux server of CPU frequency at 2.66GHz) does not yield a solution for the problem in the basic form, and for any practical purpose it is safe to deem the problem in this form too complex for the solver.

B. Dimension Reduction in the Primal Linear Program

To reduce the dimension of the LP problem, we take advantage of the symmetry and other problem specific structure, as detailed in the sequel.

Firstly, by the existence of the optimal symmetric solution (*i.e.*, with a symmetric entropic vector), the number of variables in the LP problem can be reduced. For example, the variable representing the entropy term $H(W_1, S_{2,3})$ has the same value as any variables representing the entropy terms of

the form $H(W_i, S_{j,k})$, where i, j, k are distinct elements of I_4 . Thus these variables in the LP problem can be eliminated except one arbitrary member of them. In the above example, if a variable representing a joint entropy of the form $H(W_i, S_{j,k})$ appears in any equality or inequality constraints, it can be replaced by the variable representing $H(W_1, S_{2,3})$.

Secondly, recall the equality (11), which is implied by (7) and (10) through the application of the Shannon-type inequalities in (29) and (28). This implies that the variables in the LP problem representing any joint entropy $H(\mathcal{A})$ such that $|\mathcal{A} \cap \mathcal{W}| \geq 3$ is of value B . More generally, consider the following set growth procedure for a set of random variables $\mathcal{A} \subseteq \mathcal{S} \cup \mathcal{W}$:

- 1) Initialize $\text{gr}(\mathcal{A}) = \mathcal{A}$;
- 2) For $i = 1, 2, 3, 4$: if $W_i \in \text{gr}(\mathcal{A})$, let $\text{gr}(\mathcal{A}) = \text{gr}(\mathcal{A}) \cup \{S_{i,j}, S_{i,k}, S_{i,t}\}$ where j, k, t are distinct elements of I_4 and not equal to i ;
- 3) For $i = 1, 2, 3, 4$: if $\{S_{j,i}, S_{k,i}, S_{t,i}\} \subseteq \text{gr}(\mathcal{A})$, let $\text{gr}(\mathcal{A}) = \text{gr}(\mathcal{A}) \cup \{W_i\}$, where j, k, t are distinct elements of I_4 and not equal to i ;
- 4) If the set $\text{gr}(\mathcal{A})$ did not grow in the previous two steps, exit; otherwise, return to step (2).

It is clear that if the resultant set $\text{gr}(\mathcal{A})$ satisfies $|\text{gr}(\mathcal{A}) \cap \mathcal{W}| \geq 3$, then $H(\mathcal{A})$ is also of value B . Thus the corresponding variables in the LP problem can be eliminated.

Moreover, it is clear that if any two subsets of $\mathcal{S} \cup \mathcal{W}$, denoted as \mathcal{A} and \mathcal{B} , satisfy $\text{gr}(\mathcal{A}) = \text{gr}(\mathcal{B})$, then $H(\mathcal{A}) = H(\mathcal{B})$. In other words, these subsets form an equivalent class, and the variables representing them in the LP problem can be eliminated except a single arbitrary member of them. Furthermore, after utilizing the equivalent class relation, the equality constraints (7)-(9) and (10) can now be completely eliminated.

Without loss of optimality, the inequality (12) can be taken to be equality, and thus the variables corresponding to $H(W_i)$ can be eliminated; similarly the inequality (13) can also be taken to be equality, and thus the variable corresponds to $H(S_{i,j})$ can also be eliminated and replaced by β .

Lastly, with the above reductions of variables in the LP problem, many inequality constraints become degenerate (*i.e.*, in the form of $0 \geq 0$) or repetition of others, and they can be removed from the set of constraints.

After the above steps, there remain in the LP problem only a total of 176 variables, and a total of 6152 inequality constraints, which (*i.e.*, each instance with a fixed α_0 value) can be solved in less than 0.1 second using the Cplex solver under the same setup as previously mentioned.

C. The Secondary LP

The reduced primal LP problem allows us to trace out a lower bound for the exact-repair regenerating code rate region *numerically*. There are two concerns for this numeric approach: it is not clear how many values of α we should choose to accurately trace out the rate region, and the solution is numerical which implies that the bound such obtained is only accurate within numerical precision.

There are various methods to address these concerns, however, we wish to find an explicit information theoretic proof (algebraic proof) for its obvious conceptual advantage. Let us consider a hypothetical bound that

$$\gamma_\alpha \alpha + \gamma_\beta \beta \geq \gamma_B B, \quad (31)$$

and moreover, the coefficients $(\gamma_\alpha, \gamma_\beta, \gamma_B)$ are chosen such that there exists (α, β, B) triples that satisfy it with equality under the constraints in the primal problem given in the previous sub-section. This assumption is equivalent to saying that this bound is the tightest outer bound that can be obtained under these constraints.

Recall that the reduced primal LP problem has 176 variables, and 6152 constraints. Let us consider an expanded version of the optimization problem where:

- α and B are also variables;
- The objective function subject to minimization is $\gamma_\alpha \alpha + \gamma_\beta \beta - \gamma_B B$;
- The constraint $B = 1$ is rewritten as follows (as the first two constraints when the optimization problem is written in a matrix form)

$$B \leq 1, \quad -B \leq -1; \quad (32)$$

- The constraint $\alpha = \alpha_0$ is removed.

Under the assumption aforementioned, this minimization problem specified above has a solution of zero. The reason to let $B = 1$ is to avoid the optimal but less meaningful all-zero solution, and we wrote it as two inequalities such that the minimization problem has the following standard LP form, where (B, α, β) correspond to variables (x_1, x_2, x_3) and the 175 entropies terms (in the reduced primal LP problem) correspond to the variables x_4, x_5, \dots, x_{178} :

$$\begin{aligned} &\text{minimize: } c^t x \\ &\text{subject to: } Ax \leq b, \end{aligned} \quad (33)$$

where b and c are both column vectors given as

$$\begin{aligned} b &= [1, -1, 0, 0, \dots, 0]^t \\ c &= [-\gamma_B, \gamma_\alpha, \gamma_\beta, 0, 0, \dots, 0]^t. \end{aligned} \quad (34)$$

The standard dual problem is thus given by (see [16])

$$\begin{aligned} &\text{maximize: } -b^t \lambda \\ &\text{subject to: } A^t \lambda + c = 0 \end{aligned} \quad (35)$$

$$\lambda \geq 0. \quad (36)$$

Note here λ is a vector of length 6152. Clearly the primal LP problem has a trivial solution that all joint entropy terms are equal to B_0 , and thus it is feasible. This fact further implies that the stronger duality holds in this case, and there is no duality gap between the primal and dual problem [16]. The solution for the dual problem is not unique, but because the primal LP problem has solution zero, any such solution must satisfy

$$-b^t \lambda = 0, \quad (37)$$

which implies that $\lambda_1 = \lambda_2$. From (35), it is seen then that $(\lambda_3, \lambda_4, \dots, \lambda_{6152})$ in any optimal solution for the dual problem

TABLE III
THE NON-ZERO TERMS IN THE SECONDARY LP SOLUTION.

y_1	$H(W_i S_{j,i})$
y_2	$H(W_i S_{j,k})$
y_3	$H(W_i S_{j,i} S_{k,i})$
y_4	$H(W_i S_{j,i} S_{k,j})$
y_5	$H(W_i S_{j,k} S_{t,k})$
y_6	$H(W_i S_{j,i} S_{j,k} S_{k,i})$
y_7	$H(W_i W_j)$
y_8	$H(W_i W_j S_{k,i})$

leads to an explicit proof of the inequality $\gamma_\alpha \alpha + \gamma_\beta \beta \geq \gamma_B B$. This is because each column of the matrix A^t is a known information inequality, *i.e.*, either a Shannon-type inequality, or an inequality implied by the combination of Shannon-type inequalities and certain problem-specific constraints; therefore, any non-negative linear combination is a valid information inequality, where the linear coefficients gives an explicit proof of the resultant inequality.

Let A_o be the submatrix of A which does not include the first two rows, *i.e.*, removing the constraints corresponding to $B = 1$. The above discussion essentially states that there exists a vector λ_o such that $A_o^t \lambda_o + c = 0$ for any bound that satisfy the tightness assumption, and it gives an explicit information theoretic proof; in other words, using λ_o as the weights in the linear combination of the known information inequalities, we obtain the desired inequality.

Clearly from the procedure discussed in the previous section, we wish to prove $4\alpha + 6\beta \geq 3B$, and for this purpose, we only need to solve the equality $A_o^t \lambda_o + c = 0$, where

$$c = [-3, 4, 6, 0, 0, \dots, 0]^t, \quad (38)$$

and the solution must exists if $4\alpha + 6\beta \geq 3B$ is the tightest bound under the primal LP constraints.

The solution for this set of equations is not unique, and here we wish to find one that has the fewest non-zero elements (*i.e.*, sparsest solution of λ_o), which roughly translates to a converse proof with the fewest derivation steps. This ℓ_0 optimization problem is however NP-hard, but it is well known that the ℓ_1 norm can be used to approximate the ℓ_0 norm, and thus we can solve the alternative optimization problem:

$$\begin{aligned} &\text{maximize: } \sum \lambda_i \\ &\text{subject to: } A_o^t \lambda_o + c = 0 \\ &\lambda \geq 0. \end{aligned}$$

This problem is an LP problem, and by solving this secondary LP problem, we directly obtain an explicit information theoretic solution. It should be emphasized that the approximation is in the sense that the solution thus obtained is not the sparsest solution that we desired, but not that the proof is of an approximate nature: any solution of the equalities $A_o^t \lambda_o + c = 0$ is a valid explicit information theoretic converse proof, even if it is not the sparsest.

Only a small subset of the joint entropy terms are in the solution of this secondary LP problem, as listed in Table III where we also given them labels y_1, y_2, \dots, y_8 to facilitate

TABLE IV
THE SOLUTION FOR THE DUAL PROBLEM

B	α	β	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8
	7	7		-7						
	-3			6			-3			
	1	-1	1						-1	
-1	-1			1					1	
-1						-1	1			1
-1					-1		1	1		
			-1		1	1		-1		
							1			-1
-3	4	6								

TABLE V
REWRITING THE SOLUTION FOR THE DUAL PROBLEM

Coefficients	Inequalities
7	$I(S_{i,j}; W_k) \geq 0$
3	$I(S_{k,j}; S_{t,j} W_i) \geq 0$
1	$I(W_i; W_j S_{i,j}) \geq 0$
1	$I(W_i; S_{t,k} W_j) \geq 0$
1	$I(W_i; W_j, S_{k,t} S_{i,t}, S_{j,i}, W_t) \geq 0$
1	$I(W_i; S_{k,t} S_{k,j}, S_{t,j}, W_j) \geq 0$
1	$I(S_{k,i}; S_{k,j} S_{j,i}, W_i) \geq 0$
1	$H(S_{t,i} S_{k,i}, W_i, W_j) \geq 0$

subsequent discussion. Here the letters i, j, k, t are used to denote four distinct indices in the set I_4 , because by the symmetry, they may assume any order.

We can now tabulate the solution of the secondary LP problem, as given in Table. IV, one row corresponding to one row in A_o , i.e., one basic information inequality as shown in Table V. The last line in Table. IV is the row summation which is indeed $4\alpha + 6\beta \geq 3B$. Note that the last inequality of Table V is also a basic information inequality, but it is not in the form of (29) because some problem specific reduction discussed in the previous sub-section has been incorporated. Though this is already a valid proof, we can manually combine several inequalities to simplify the proof, and the converse proof given in the previous section is the result after such further manual simplifications.

In [8], Yeung showed that all unconstrained Shannon-type inequalities are linear combinations of elemental Shannon-type inequalities, i.e., (28) and (29). The approach we have discussed above can be viewed as a generalization of this result under additional problem-specific constraints. However, the introduction of the ℓ_1 norm objective function to approximately find the sparsest linear combination has not been used previously to investigate information inequalities, and thus it is a novel ingredient. Moreover, the proof given in [8] relies on the fact that all joint entropies can be represented by a linear combinations of the elementary forms of Shannon's information measures, which are the left hand sides of (28) and (29). Since our result is regarding the *tightest* bounds that can be obtained using the LP approach, the proof directly follows from the strong duality without relying on the completeness of the elementary forms of Shannon's information measures.

V. CONCLUSION

A complete characterization is provided for the rate region of the $(4, 3, 3)$ exact-repair regenerating codes, which shows that the cut-set outer bound [1] is in general not (even asymptotically) tight for exact-repair. An explicit binary code construction is provided to show that the given rate region is achievable. One main novelty of the work is that a computer-aided proof approach is developed by extending Yeung's linear programming framework, and an explicit information theoretic proof is directly obtained using this approach. We believe customizing the LP approach to other communication problems based on similar reduction techniques can be a rather fruitful path, which appears particularly suitable for research on storage systems, and thus have presented some related details in this work.

Although sparsity is used approximately as an objective in the secondary LP problem, this sparsity is only with respect to the elementary Shannon-type inequalities (28)-(29), and thus including more redundant basic Shannon-type inequalities may lead to even sparser solution. This is already evident in the algebraic proof given where manual simplification was taken and some basic inequalities not in (28)-(29) were used. Including these basic inequalities in the secondary LP will clearly yield a more sparser solution. It should also be noted that sparsity only translates roughly to a small number of proof steps, but does not necessarily lead to a structured proof that can be extended to general parameter settings.

The result presented in this work revealed that the cut-set outer bound is in general not tight for exact-repair. Though a complete solution for the special case of $(4, 3, 3)$ is given, the rate region characterization problem under general parameters is still open. Readers may wonder if the procedure given in Section IV can be used on the general problem, if it fundamentally alters the complexity order of the primal optimization problem. Unfortunately, although a few more cases with small (n, k, d) values can be tackled this way, the complexity is still too high for larger parameter values, and the list of information inequalities involved in the proof is quite large. In fact, running only the set growth and symmetry determination procedures alone for each variable is of exponential order in the total number of random variables. As an on-going work, we are investigating whether low complexity procedures exist that can further take into account the symmetry. Through such a general study, we hope to discover more structure in the converse proof which may lead to the complete solution of general (n, k, d) exact-repair regenerating codes.

APPENDIX

Proof of Proposition 1: For any $(\bar{\alpha}, \bar{\beta})$ that is $(4, 3, 3)$ exact-repair achievable, there exists for any $\epsilon > 0$, an (N, K_d, K) exact-repair regenerating code such that

$$\bar{\alpha} + \epsilon \geq \frac{\log K_d}{\log N}, \quad \bar{\beta} + \epsilon \geq \frac{\log K}{\log N}. \quad (39)$$

Let us for now fix a value $\epsilon > 0$, and consider an (N, K_d, K) exact-repair regenerating code satisfy the above conditions, which may or may not induce a symmetric entropy vector.

Let the encoding and decoding functions be denoted as: $f_i^E(\cdot)$, $f_A^D(\cdot, \cdot, \cdot)$, $F_{i,j}^E(\cdot)$, $F_i^D(\cdot, \cdot, \cdot)$, as given in Definition 1. We shall show that it can be used to construct an $(N', K'_d, K') = (N^{24}, K_d^{24}, K^{24})$ code that induces a symmetric distortion vector, which clearly satisfies (39), and the proof will be completed by making ϵ arbitrarily small.

Let the 24 distinct permutations of I_4 be $\pi_1, \pi_2, \dots, \pi_{24}$, and let their inverse function be $\pi_1^{-1}, \pi_2^{-1}, \dots, \pi_{24}^{-1}$. The new encoding and decoding functions can be written as

$$\begin{aligned} \hat{f}_i^E(x^{(1)}, x^{(2)}, \dots, x^{(24)}) &= \prod_{k=1}^{24} f_{\pi_k^{-1}(i)}^E(x^{(k)}), \\ \hat{f}_A^D((x_1^{(1)}, x_2^{(1)}, x_3^{(1)}), \dots, (x_1^{(24)}, x_2^{(24)}, x_3^{(24)})) \\ &= \prod_{k=1}^{24} f_{\pi_k^{-1}A}^D(x_1^{(k)}, x_2^{(k)}, x_3^{(k)}), \\ \hat{F}_{i,j}^E(x^{(1)}, x^{(2)}, \dots, x^{(24)}) &= \prod_{k=1}^{24} F_{\pi_k^{-1}(i), \pi^{-1}(j)}^E(x^{(k)}), \\ \hat{F}_i^D((x_1^{(1)}, x_2^{(1)}, x_3^{(1)}), \dots, (x_1^{(24)}, x_2^{(24)}, x_3^{(24)})) \\ &= \prod_{k=1}^{24} F_{\pi_k^{-1}(i)}^D(x_1^{(k)}, x_2^{(k)}, x_3^{(k)}). \quad (40) \end{aligned}$$

Because of the symmetry of the new encoding and decoding functions, it is clear by utilizing (4) that they indeed induce a symmetric entropy vector, according to Definition 4. The zero-error decoding and repair requirements are satisfied because the original code is able to accomplish them. The proof is thus complete. ■

ACKNOWLEDGMENT

The author wishes to thank Dr. Dahai Xu at AT&T Labs-Research for introducing him to the Cplex optimization software package.

REFERENCES

- [1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. Wainwright and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Information Theory*, vol. 56, no. 9, pp. 4539-4551, Sep. 2010.
- [2] R. Ahlswede, Ning Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Information Theory*, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.
- [3] S. Y. R. Li, R. W. Yeung, and Ning Cai, "Linear network coding," *IEEE Trans. Information Theory*, vol. 49, no. 2, pp. 371-381, Feb. 2003.
- [4] N. B. Shah, K. V. Rashmi, P. V. Kumar and K. Ramchandran, "Distributed storage codes with repair-by-transfer and non-achievability of interior points on the storage-bandwidth tradeoff," *IEEE Trans on Information Theory*, vol. 58, no. 3, pp. 1837-1852, Mar. 2012.
- [5] N. B. Shah, K. V. Rashmi, P. V. Kumar and K. Ramchandran, "Interference alignment in regenerating codes for distributed storage: necessity and code constructions," *IEEE Trans on Information Theory*, vol. 58, no. 4, pp. 2134-2158, Apr. 2012.
- [6] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction," *IEEE Trans on Information Theory*, vol. 57, no. 8, pp. 5227-5239, Aug. 2011.
- [7] V. Cadambe, S. Jafar, H. Maleki, K. Ramchandran and C. Suh, "Asymptotic interference alignment for optimal repair of MDS codes in distributed storage," *IEEE Trans on Information Theory*, vol. 59, no. 5, pp. 2974 -2987, May 2013.
- [8] R. Yeung, *A First Course in Information Theory*, Kluwer Academic Publishers, New York, 2002.
- [9] B. Sasidharan and P. V. Kumar, "High-rate regenerating codes through layering," arXiv:1301.6157
- [10] C. Tian, V. Aggarwal, V. Vaishampayan, "Exact-repair regenerating codes via layered erasure correction and block designs," arXiv:1302.4670
- [11] C. Tian, "Rate region of the $(4, 3, 3)$ exact-repair regenerating codes," in *Proceeds, IEEE International Symposium on Information Theory*, Istanbul, Turkey, Jul. 2013.
- [12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, New York: Wiley, 1991.
- [13] ITIP software package, http://user_www.ie.cuhk.edu.hk/~ITIP/
- [14] Xitip software package, <http://xitip.epfl.ch/>
- [15] IBM ILOG CPLEX Optimizer, http://www-01.ibm.com/software/integration/optimization/cplex_optimizer/
- [16] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.