New Bounds on the (n, k, d) Storage Systems with Exact Repair

Soheil Mohajer
Department of Electrical and Computer Engineering
University of Minnesota
Minneapolis, MN 55404
Email: soheil@umn.edu

Ravi Tandon
Discovery Analytics Center
Department of Computer Science
Virginia Tech, Blacksburg, VA 24060
Email: tandonr@vt.edu

***Abstract*—The exact-repair problem for distributed storage systems is considered. Characterizing the optimal storage-vs-repair bandwidth tradeoff for such systems remains an open problem for more than four storage nodes. A new family of information theoretic bounds is provided for the storage-vs-repair bandwidth tradeoff for all (n, k, d) systems. The proposed bound readily recovers Tian's result for the $(4, 3, 3)$ system, and hence suffices for exact characterization for this system. In addition, the bound improves upon the existing bounds for the $(5, 4, 4)$ system. More generally, it is shown that this bound characterizes the optimal boundary of the exact repair tradeoff for all distributed storage systems, with $(n, k, d) = (n, n-1, n-1)$ when $\beta \leq 2\alpha/k$.**

***Index Terms*—Distributed storage system, Exact repair, New outer bounds**

I. Introduction

Contemporary distributed storage systems store massive amounts of data over a set of distributed nodes. Besides the traditional goals of achieving reliability by introducing redundancy, new aspects such as efficient repair of failed storage nodes are becoming increasingly important. To address these issues, the concept of regenerating codes for distributed storage systems (DSS) was introduced by Dimakis *et al.* [1]. A DSS consists of n storage nodes each with a storage capacity of α units, such that the entire file of size F can be recovered by accessing any $k < n$ nodes. This is called as the reconstruction property of the DSS. Whenever a node fails, d nodes (where $k \leq d \leq n-1$) participate in the repair process by sending β units of data each. This procedure is termed as the regeneration of a failed node and β is referred to as the per-node repair bandwidth. In [1], it was shown that the maximum amount of data, F, that any regenerating code can store satisfies

$$F \leq \sum_{i=0}^{k-1} \min\left(\alpha, (d-i)\beta\right). \tag{1}$$

Thus, in order to store data of size F, there exists a fundamental tradeoff between α (storage) and $d\beta$ (total repair bandwidth). It was also shown in [1] that the above tradeoff is achievable for functional repair, which does not require the contents of the repaired node to be the same as the original node. In contrast to functional repair, exact repair requires that the contents of the failed node must match with those stored in the original node. Exact repair is a practically appealing property specially when it is desirable that the stored contents remain intact over time. Furthermore, the file recovery process is also easier in this case as the reconstruction procedure need not change whenever a failed node is replaced. While characterizing the storage-vs-bandwidth tradeoff for the case of exact repair remains a challenging open problem in general, two extreme points of this tradeoff namely, the minimum storage regenerating case (MSR) and the minimum bandwidth regenerating (MBR) case have been studied extensively (see [3], [4] and references therein). Other notable works on code constructions beyond MSR and MBR points include [8], [9].

Tian has recently characterized the exact repair tradeoff for the $(4, 3, 3)$-DSS [5]. This result, which is based on a novel computer-aided approach showed that functional and exact repair problems are fundamentally different. Despite its originality, the solution involved solving an optimization problem with a large number of variables and constraints. More importantly, the number of variables/constraints grow (at least) exponentially, and hence, it is not clear whether this approach can be generalized for larger system parameters. Moreover, such a computer-aided approach does not necessarily lead to intuition and insights which could be used to understand the exact repair problem for a general set of parameters. Notably, Sasidharan et.al in [7] brought some intuition in this regard and presented a simpler proof for the $(4, 3, 3)$ problem and also presented new bounds for the $(5, 4, 4)$-DSS.

In this paper, we present a new and general approach for obtaining information theoretic upper bounds on F for the exact repair problem. This approach is used to develop a family of bounds which hold for any (n, k, d)-DSS. Using these bounds, together with the code constructions in [9], we characterize the partial boundary of the optimal exact repair tradeoff for $(n, n-1, n-1)$-DSS in the regime when $\beta \leq 2\alpha/k$. We also show that the proposed bound yields a new and simple proof for the $(4, 3, 3)$-DSS. For the $(5, 4, 4)$-DSS, our bounds improve upon the ones obtain in [7].

II. Problem Statement and Result

Notation: We use $[i : j] = \{i, i+1, \ldots, j\}$ to denote the set of positive integers between (and including) i and j. If $i = 1$, we drop it, and simply use $[j]$ to denote set $\{1, 2, \ldots, j\}$, hence $[n] = \{1, 2, \ldots, n\}$ denotes the set of all node indices. We use W_i to denote the content stored in node i, and extend this definition to $W_A = \{W_i; i \in A\}$ for any $A \subseteq [n]$. In the rest of this paper, unless otherwise mentioned, we focus on a subset of the nodes indexed by $N = \{1, 2, \dots, d+1\}$. Note that any upper bound for this sub-system of $(d+1)$ nodes holds for the original system with n nodes as well.

In this sub-system, the repair data from i to j is denoted by S_i^j. Note that since $|N| = d+1$, there is a unique way of choosing d helper nodes to repair any failed node within N. Therefore, the dependence of S_i^j on the remaining $(d-1)$ helper nodes, that is $N \setminus \{i, j\}$, is clear due to their uniqueness and is hence dropped from the notation for simplicity. We also set S_i^i, to be a dummy variable with zero entropy, for consistency. Moreover, $S_A^B = \{S_i^j : i \in A, j \in B\}$.

Next we describe the exact repair problem and the associated constraints. An exact repair distributed storage system with parameters (n, k, d) and (α, β) is defined as follows. A DSS consists of n storage devices, each with capacity α, which is used to store some Data in a distributed fashion, such that the following properties hold:

- **MDS Property (data recovery):** Data can be recovered from the content of any k nodes: $H(\mathsf{Data}|W_A) = 0$ for any $A \subseteq N$ satisfying $|A| \geq k$.
- **Repairability Requirements:** The content of any failed node can be exactly recovered (repaired) by receiving no more that β units of repair data from any other d nodes, that is, $H(W_i|S_A^i) = 0$ for any $A \subseteq N \setminus \{i\}$, with $|A| \geq d$, where $H(S_i^j) \leq \beta$ and $H(S_i^j|W_i) = 0$.

We next present the main result of this paper which is a new set of lower bounds on the exact repair tradeoff for the (n, k, d) distributed storage system.

Theorem 1. *The exact repair capacity of an (n, k, d) distributed storage system with per node storage α and total repair bandwidth $d\beta$ is upper bounded by a family of bounds, namely,*

$$3F \leq (3k - 2m)\alpha + \frac{m(2d - 2k + m + 1)}{2}\beta + (d - k + 1)\min(\alpha, k\beta),$$

for $m = 0, 1, \dots, k$.

The following corollary is an immediate consequence of this theorem together with the code construction in [9].

Corollary 1. *The exact repair capacity of an $(n, k, d) = (n, n-1, n-1)$ DSS for $\beta \leq 2\alpha/k$ is given by*

$$F \leq \min\left\{\frac{k+1}{3}\alpha + \frac{k(k+1)}{6}\beta, \frac{k(k+1)}{2}\beta\right\}. \quad (2)$$

Proof of Corollary 1. The first bound in the minimum above follows by setting $d = m = k$ in Theorem 1, while the second one, i.e., $F \leq k(k+1)\beta/2$ is simply the cut-set bound. Moreover, achievability of the MBR point $(\alpha, \beta) = \left(\frac{2F}{k+1}, \frac{2F}{k(k+1)}\right)$ is given in [10].

Finally, the other extreme point of this region is $(\alpha, \beta) = \left(\frac{3F}{2(k+1)}, \frac{3F}{k(k+1)}\right)$, which is shown to be achievable by the code construction in [9, Theorem 1 for $\hat{k} = 2$] for every k. $\square$

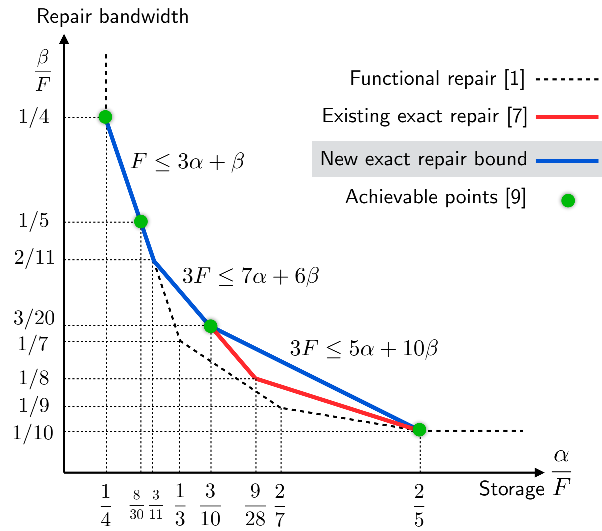

Fig. 1. Existing and new results for $(5, 4, 4)$ DSS.

Remark 1. *For the $(4, 3, 3)$-DSS, setting $m = d = k = 3$, we obtain $3F \leq 4\alpha + 6\beta$, which is precisely the new converse bound obtained by Tian [5] through a novel computer aided approach. This bound together with the cut-set bound and the achievability in [5] suffices to characterize the exact repair tradeoff for $(4, 3, 3)$-DSS.*

Remark 2. *For the $(5, 4, 4)$-DSS, Theorem 1 leads to the following set of new bounds which improve upon the cut-set bound:*

1) $3F \leq 5\alpha + 10\beta$ *(setting $m = 4$)*
2) $3F \leq 7\alpha + 6\beta$ *(setting $m = 3$)*

It is interesting to note that the bound $3F \leq 7\alpha + 6\beta$ was also obtained in [7] through a different set of arguments. Moreover, the other bound $3F \leq 5\alpha + 10\beta$ (corresponding[1] to $m = 4$) gives the optimal characterization of the exact repair tradeoff for the regime in which $\beta \leq 2\alpha/k$ (see Corollary 1). These bounds together with the cut-set bound and the best known code-constructions are shown in Fig. 1.

III. Proof of Theorem 1

For the sake of brevity and simplicity, we focus on the tradeoff of the *symmetric*[2] exact-repair regeneration codes for DSSs, in which the information-theoretical quantities are invariant under any relabeling of the nodes. We adopt the notation in [5] in order to formally define this symmetry:

Definition 1. *A* permutation *π is given by a one-to-one mapping $\pi : [n] \to [n]$. We denote the set of all permutations by Π.*

Then a symmetric DSS can be defined as the following.

[1]This specific bound for $(5, 4, 4)$ first appeared in our prior work [11]. In contrast to [11], the bounding technique of this paper is general and applicable to any (n, k, d) DSS.

[2]Note that the symmetry assumption is made without any loss in generality, as any asymmetric code can be symmetrized by augmenting its $n!$ copies, each copy corresponding to a permutation of the node labels. The resulting symmetric code and the original asymmetric code achieve the same (F, α, β) upto the scaling factor of $n!$.

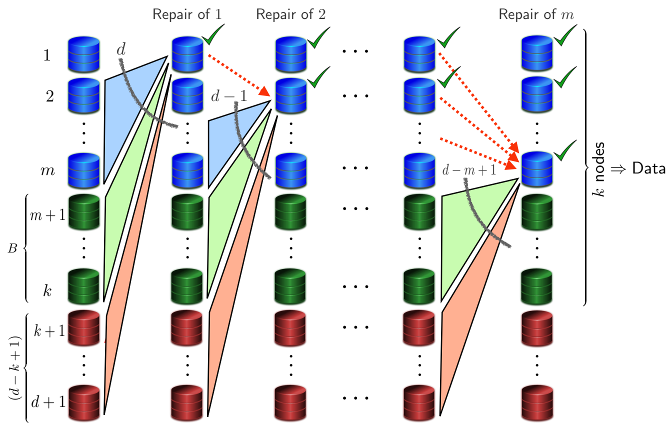

Fig. 2. Pictorial illustration of Lemma 1. Starting from node 1, we can repair nodes in a serial fashion, and then use their outgoing repair data.

Definition 2. *An (n,k,d) exact-repair regeneration is called symmetric if for any subset of node $A \subseteq W_{[n]}$ and repair data $B \subseteq \{S_i^j : i,j \in [n]\}$ and permutation $\pi \in \Pi$,*

$$H(A,B) = H(\pi(A),\pi(B)).$$

In the following we focus on a subset of nodes in the DSS. Let $N = \{1,2,\dots,d+1\} \subseteq \{1,2,\dots,n\}$. Both the data-recovery and node-repairability property should also hold from nodes in N. Moreover, any outer bound derived for the nodes in N will also be a valid bound for the entire set of nodes. The main advantage of restriction to nodes in N is the fact that there is only one possibility for the repair of each node within N, which further simplifies our notation.

We next present three key lemmas, which play a central role in the proofs of the outer bounds. The proofs of these lemma are presented in Appendix. A.

Lemma 1. *Let $B = \{m+1, m+3, \dots, k\}$ be a subset of nodes for some $m \leq k$. Then,*

$$\sum_{i=1}^{m} H\left(S_i^{[i-1]}\middle|W_B\right) + (d+1-k)H\left(S_{k+1}^{[k]}\middle|W_B\right) \geq F - |B|\alpha. \quad (3)$$

In spite of its complicated statement, Lemma 1 is just a simple cut-set bound. As shown in Figure 2, the repair data on the LHS of (3) (shown by solid arrows) suffice to recover W_1, which further determines outgoing repair data from W_1 (shown in dashed arrows). Then W_2 can be recovered, and the procedure continues until we repair k nodes, which suffice to recover the entire data.

Lemma 2. *For any pair of disjoints sets $A,B \subseteq N$ with $|A|+|B| \leq d$, and $i \notin A \cup B$, we have*

$$H(S_A^i|W_B) \geq \frac{|A|}{d-|B|} H(S_N^i|W_B). \quad (4)$$

Lemma 3. *For any subsets of nodes $A,B,C \subseteq N$, we have*

$$H(S_N^{A\cup B}|W_C) + H(S_A^B, S_B^A|W_C) \leq H(S_N^A|W_C) + H(S_N^B|W_C). \quad (5)$$

Having these lemmas, we are ready to present the proof of the main theorem. Consider an arbitrary integer $1 \leq m \leq k$, and two disjoint sets $P = \{1,2,\dots,m\}$ and $Q = \{m+1, m+2, \dots, k\}$. Then, since $|P \cup Q| = k$, the entire data can be recovered from disks in $P \cup Q$. Hence,

$$\begin{aligned}
F &= H(\mathsf{Data}) = H(W_{P\cup Q}) = H(W_Q) + H(W_P|W_Q) \\
&= H(W_Q) + \sum_{i=1}^{m} H(W_i|W_{[i-1]}, W_Q) \\
&= H(W_Q) + \sum_{i=1}^{m} [H(W_i|W_Q) - I(W_i; W_{[i-1]}|W_Q)] \\
&\leq H(W_Q) + \sum_{i=1}^{m} H(W_i|W_Q) - \sum_{i=1}^{m} I(W_i; W_{[i-1]}|W_Q) \\
&\leq (k-m)\alpha + m\alpha - \sum_{i=1}^{m} I(W_i; W_{[i-1]}|W_Q). \\
&= k\alpha - \sum_{i=1}^{m} I(W_i; W_{[i-1]}|W_Q). \quad (6)
\end{aligned}$$

Next, note that the repair data $S_i^{[i-1]}$ (which is sent by node i) is a function of W_i. Similarly, $S_{[i-1]}^i$ is a function of $W_{[i-1]}$. Hence we can write

$$\begin{aligned}
&\sum_{i=1}^{m} I(W_i; W_{[i-1]}|W_Q) \geq \sum_{i=1}^{m} I\left(S_i^{[i-1]}; S_{[i-1]}^i|W_Q\right) \\
&= \sum_{i=1}^{m} \left[H\left(S_i^{[i-1]}|W_Q\right) + H\left(S_{[i-1]}^i|W_Q\right) - H\left(S_i^{[i-1]}, S_{[i-1]}^i|W_Q\right)\right] \\
&= \underbrace{\sum_{i=1}^{m} H\left(S_i^{[i-1]}|W_Q\right)}_{\mathsf{Term}_1} + \underbrace{\sum_{i=1}^{m} H\left(S_{[i-1]}^i|W_Q\right)}_{\mathsf{Term}_2} \\
&\quad - \underbrace{\sum_{i=1}^{m} H\left(S_i^{[i-1]}, S_{[i-1]}^i|W_Q\right)}_{\mathsf{Term}_3}, \quad (7)
\end{aligned}$$

which together with (6) implies that

$$F \leq k\alpha - [\mathsf{Term}_1 + \mathsf{Term}_2 - \mathsf{Term}_3]. \quad (8)$$

Our next goal is lower bounding Term_1 and Term_2, and upper bounding Term_3.

A. Lower Bounding Term_1

First we use Lemma 1 for $B = Q$ to get

$$\sum_{i=1}^{m} H\left(S_i^{[i-1]}|W_Q\right) + (d+1-k)H(S_{k+1}^{[k]}|W_Q) \geq F - |Q|\alpha.$$

Hence,

$$\begin{aligned}
\mathsf{Term}_1 &= \sum_{i=1}^{m} H\left(S_i^{[i-1]}\middle|W_Q\right) \\
&\geq F - (k-m)\alpha - (d+1-k)H\left(S_{k+1}^{[k]}\middle|W_Q\right). \quad (9)
\end{aligned}$$

B. Lower Bounding Term_2

Next, we use Lemma 2 to lower bound each individual conditional entropy in the summation in Term_2. Evaluating Lemma 2 for $A = [i-1]$ and $B = Q$, we get

$$H\left(S^i_{[i-1]}|W_Q\right) \geq \frac{|[i-1]|}{d-|Q|} H(S^i_N|W_Q) = \frac{i-1}{d-(k-m)} H(S^1_N|W_Q), \quad (10)$$

where in the last equality we used the symmetry property implying that $H(S^i_N|W_Q) = H(S^1_N|W_Q)$. Summing up (10) for $i = 1, 2, \ldots, m$, we get

$$\mathsf{Term}_2 = \sum_{i=1}^{m} H\left(S^i_{[i-1]}|W_Q\right) \geq \sum_{i=1}^{m} \frac{i-1}{d-(k-m)} H(S^1_N|W_Q) = \frac{m(m-1)}{2(d-(k-m))} H(S^1_N|W_Q). \quad (11)$$

C. Upper Bounding Term_3

Finally, in order to bound Term_3 in (7), we apply Lemma 3 with $C = Q$ and $(A, B) = ([i-1], \{i\})$ (so that $A \cup B = [i]$) to get

$$H\left(S^{[i]}_N \middle| W_Q\right) + H\left(S^i_{[i-1]}, S^{[i-1]}_i \middle| W_Q\right) \leq H\left(S^{[i-1]}_N \middle| W_Q\right) + H\left(S^i_N \middle| W_Q\right). \quad (12)$$

Summing up (12) for $i = 1, 2, \ldots, m$, we get

$$H\left(S^{[m]}_N \middle| W_Q\right) + \sum_{i=1}^{m} H\left(S^i_{[i-1]}, S^{[i-1]}_i \middle| W_Q\right) \leq \sum_{i=1}^{m} H\left(S^i_N \middle| W_Q\right). \quad (13)$$

Recall that $P = [m]$, and having the repair data from every node in N to P (i.e., $S^{[m]}_N$), we can recover the contents for every node in P (i.e., W_P). Thus we have

$$\begin{aligned} H\left(S^{[m]}_N \middle| W_Q\right) &\geq H(W_P|W_Q) = H(W_{P\cup Q}|W_Q) \\ &= H(\mathsf{Data}|W_B) = H(\mathsf{Data}) - H(W_B) \\ &\geq F - (k-m)\alpha. \end{aligned} \quad (14)$$

Hence (13) together with (14) imply

$$\begin{aligned} \mathsf{Term}_3 &= \sum_{i=1}^{m} H\left(S^i_{[i-1]}, S^{[i-1]}_i \middle| W_Q\right) \\ &\leq \sum_{i=1}^{m} H\left(S^i_N \middle| W_Q\right) - H\left(S^{[m]}_N \middle| W_Q\right) \\ &\leq \sum_{i=1}^{m} H\left(S^i_N \middle| W_Q\right) - [F - (k-m)\alpha] \\ &= mH\left(S^1_N \middle| W_Q\right) + (k-m)\alpha - F, \end{aligned} \quad (15)$$

where the last equality follows from the symmetry property, that is $H\left(S^i_N \middle| W_Q\right) = H\left(S^1_N \middle| W_Q\right)$ for $i = 1, 2, \ldots, m$.

D. Upper Bounding F

Next, we plug (9), (11) and (15) in (8), to get

$$\begin{aligned} F &\leq k\alpha - \mathsf{Term}_1 - \mathsf{Term}_2 + \mathsf{Term}_3 \\ &\leq k\alpha - \left[F - (k-m)\alpha - (d+1-k)H\left(S^{[k]}_{k+1} \middle| W_Q\right)\right] \\ &\quad - \left[\frac{m(m-1)}{2(d-(k-m))} H(S^1_N|W_Q)\right] \\ &\quad + \left[mH\left(S^1_N \middle| W_Q\right) + (k-m)\alpha - F\right] \\ &= (3k-2m)\alpha + \frac{m[2(d-k)+m+1]}{2((d-k)+m)} H\left(S^1_N \middle| W_Q\right) \\ &\quad + (d+1-k)H\left(S^{[k]}_{k+1} \middle| W_Q\right) - 2F. \end{aligned} \quad (16)$$

Hence, since

$$\begin{aligned} H\left(S^1_N \middle| W_Q\right) &= H\left(S^1_{N\setminus(Q\cup\{1\})} \middle| W_Q\right) \leq (d-|Q|)\beta \\ &= (d-(k-m))\beta \end{aligned}$$

and

$$H\left(S^{[k]}_{k+1}|W_Q\right) \leq \min(\alpha, k\beta), \quad (17)$$

we have

$$\begin{aligned} 3F \leq (3k-2m)\alpha &+ \frac{m[2(d-k)+m+1]}{2}\beta \\ &+ (d+1-k)\min(\alpha, k\beta). \end{aligned} \quad (18)$$

This concludes the proof of Theorem 1.

IV. Conclusion

We studied the exact-repair problem for the (n, k, d)-distributed storage system and obtained new bounds on its optimum tradeoff. Our bounds indicate a gap between the functional and exact-repair tradeoffs for a wide range of parameters. Furthermore, the proposed bound is achievable for $(n, k, d) = (n, n-1, n-1)$-DSS when $\beta \in (\alpha/d, 2\alpha/d]$, and consequently characterizes the optimum tradeoff in this regime.

While our results provide the state-of-the-art bounds for (n, k, d) exact-repair distributed storage systems, and partially characterize their optimum tradeoff, the central contribution of this paper is to introduce a novel bounding mechanism and demonstrate its applicability in finding upper bounds on the optimum tradeoff of exact repair DSS problem for a wide range of system parameters.

Appendix

Proof of Lemma 1. First note that

$$\begin{aligned} \sum_{i=1}^{m} H\left(S^{[i-1]}_i \middle| W_B\right) &\geq H\left(\{S^{[i-1]}_i : i \in [m]\} \middle| W_B\right) \\ &= H\left(\{S^i_{[i+1:m]} : i \in [m]\} \middle| W_B\right) \\ &\overset{(a)}{=} H\left(\{S^i_{[i+1:m]} : i \in [m]\}, \{S^{[m]}_j : j \in [m+1:k]\} \middle| W_B\right) \\ &= H\left(\{S^i_{[i+1:k]} : i \in [m]\} \middle| W_B\right), \end{aligned} \quad (19)$$

where in (a) we used the fact that $S_B^{[m]} = S_{[m+1:k]}^{[m]}$ is a function of W_B. On the other hand, using the symmetry property in Definition 2, we have

$$\begin{aligned}(d-k+1)H\left(S_{k+1}^{[k]}\middle|W_B\right) &= \sum_{i=k+1}^{d+1} H\left(S_i^{[k]}\middle|W_B\right)\\ &\geq H\left(\{S_i^{[k]} : i\in[k+1:d+1]\}\middle|W_B\right)\\ &= H\left(\{S_{[k+1:d+1]}^i : i\in[k]\}\middle|W_B\right). \qquad (20)\end{aligned}$$

Hence, adding (19) and (20) we get

$$\begin{aligned}&\sum_{i=1}^{m} H\left(S_i^{[i-1]}\middle|W_B\right) + (d-k+1)H\left(S_{k+1}^{[k]}\middle|W_B\right)\\ &\quad\geq H\left(\{S_{[i+1:k]}^i : i\in[m]\}\middle|W_B\right)\\ &\qquad+ H\left(\{S_{[k+1:d+1]}^i : i\in[k]\}\middle|W_B\right)\\ &\quad\geq H\left(\{S_{[i+1:d+1]}^i : i\in[k]\}\middle|W_B\right) \qquad (21)\end{aligned}$$

Next note that $S_{[2:d+1]}^1$ in (21) provides enough information to repair W_1, and hence the outgoing repair data from W_1. Once $S_1^{[k]}$ is reconstructed, this together with $S_{[3:d+1]}^2$ suffices to repair W_2, from which W_2 and its outgoing repair data (i.e., $S_2^{[k]}$) can be recovered. Thereafter having $(S_1^{[k]}, S_2^{[k]})$ and $S_{[4:d+1]}^3$ we can recover W_3. A similar line of reasoning shows that $\{S_{[i+1:d+1]}^i : i \in [k]\}$ suffices to recover $(W_1, W_2, \ldots, W_k)$, and hence the entire original data can be recovered by the MDS property. Thus,

$$\begin{aligned}&\sum_{i=1}^{m} H\left(S_i^{[i-1]}\middle|W_B\right) + (d-k+1)H\left(S_{k+1}^{[k]}\middle|W_B\right)\\ &\quad\geq H(\mathsf{Data}|W_B) = H(\mathsf{Data}) - H(W_B) \geq F - |B|\alpha.\end{aligned}$$

This completes the proof of Lemma 1. □

Proof of Lemma 2. Let $C = N \setminus (B \cup \{i\})$. It is clear that $A \subseteq C$, and $|C \cup B| = |N| - 1 = d$. Now consider any arbitrary $A' \subseteq C$ with $|A'| = |A|$. The symmetry property of the code (Definition 2) implies that $H(S_A^i|W_B) = H(S_{A'}^i|W_B)$. Hence, we can write

$$\begin{aligned}\frac{1}{|A|}H(S_A^i|W_B) &= \frac{1}{|A|}\frac{1}{\binom{|C|}{|A|}}\sum_{\substack{A'\subseteq C\\ |A'|=|A|}} H(S_A^i|W_B)\\ &= \frac{1}{|A|\binom{|C|}{|A|}}\sum_{\substack{A'\subseteq C\\ |A'|=|A|}} H(S_{A'}^i|W_B)\\ &\overset{(*)}{\geq} \frac{1}{|C|\binom{|C|}{|C|}}\sum_{\substack{C'\subseteq C\\ |C'|=|C|}} H(S_{C'}^i|W_B)\\ &= \frac{1}{|C|}H(S_C^i|W_B), \qquad (22)\end{aligned}$$

where in $(*)$ we used the conditional version of Han's inequality [6]. Next note that, given W_B, all the repair data outgoing from nodes in B are determined. Moreover, S_i^i is just a dummy variable with zero entropy. Hence,

$$H(S_C^i|W_B) = H(S_C^i, S_B^i, S_i^i|W_B) = H(S_N^i|W_B). \qquad (23)$$

Substituting (23) in (22), and incorporating $|C| = d - |B|$, we get the desired bound. □

Proof of Lemma 3. First note that S_N^A includes S_B^A since $B \subseteq N$. Moreover, S_N^A provides all repair data required to repair nodes in A. Hence W_A can be reconstructed from S_N^A, from which the outgoing repair data S_A^B can be found. Hence

$$H(S_N^A|W_C) = H(S_N^A, S_A^B, S_B^A|W_C), \qquad (24)$$

and similarly

$$H(S_N^B|W_C) = H(S_N^A, S_A^B, S_B^A|W_C). \qquad (25)$$

Therefore, using the inequality

$$H(X,Y|T) + H(X,Z|T) \geq H(X,Y,Z|T) + H(X|T),$$

we get

$$\begin{aligned}&H(S_N^A|W_C) + H(S_N^B|W_C)\\ &\quad= H(S_N^A, S_A^B, S_B^A|W_C) + H(S_N^A, S_A^B, S_B^A|W_C)\\ &\quad\geq H(S_N^{A\cup B}, S_A^B, S_B^A|W_C) + H(S_A^B, S_B^A|W_C)\\ &\quad= H(S_N^{A\cup B}|W_C) + H(S_A^B, S_B^A|W_C), \qquad (26)\end{aligned}$$

which implies the desired inequality. □

REFERENCES

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

[2] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory,* vol. 46, pp. 1204–1216, Jul. 2000.

[3] 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. Inf. Theory,* vol. 58, no. 3, pp. 1837–1852, Mar. 2012.

[4] 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 Inf. Theory,* vol. 59, no. 5, pp. 2974–2987, May. 2013.

[5] C. Tian, "Rate region of the (4,3,3) exact-repair regenerating codes," in *Proc. Intern. Symp. Inf Theory, ISIT*, Istanbul, Turkey, Jun. 2013.

[6] T. M. Cover and J. A. Thomas, "Elements of Information Theory", 1991. New York: Wiley.

[7] B. Sasidharan, K. Senthoor, P. V. Kumar , "An Improved Outer Bound on the Storage-Repair-Bandwidth Tradeoff of Exact-Repair Regenerating Codes", in arXiv:1312.6079, Dec. 2013.

[8] C. Tian, B. Sasidharan, V. Aggarwal, V. A. Vaishampayan, P. V. Kumar, "Layered, Exact-Repair Regenerating Codes Via Embedded Error Correction and Block Designs", in arXiv:1408.0377, Aug. 2014.

[9] S. Goparaju, S. El Rouayheb, R. Calderbank , "New Codes and Inner Bounds for Exact Repair in Distributed Storage Systems", in arXiv:1402.2343, Feb. 2014.

[10] 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," in *IEEE Transactions on Information Theory*, vol. 57, pp. 5227–5239, Aug. 2011.

[11] S. Mohajer and R. Tandon, "Exact Repair for Distributed Storage Systems: Partial Characterization via New Bounds", Information Theory and Applications Workshop (ITA), San Diego, Feb. 2015.