Outer bounds on the storage-repair bandwidth trade-off of exact-repair regenerating codes

Birenjith Sasidharan

Department of ECE,
Indian Institute of Science,
Bangalore 560012, India
Email: biren@ece.iisc.ernet.in

N. Prakash

Massachusetts Institute of Technology,
Research Laboratory of Electronics,
Room 36-512, 77 Massachusetts Avenue,
Cambridge, MA 02139, USA
Email: prakashn@mit.edu

M. Nikhil Krishnan and Myna Vajha

Department of ECE,
Indian Institute of Science,
Bangalore 560012, India
Email: nikhilkm@ece.iisc.ernet.in
Email: myna@ece.iisc.ernet.in

Kaushik Senthoor

Department of Electrical Engineering,
Indian Institute of Technology Madras,
Chennai, India
Email: kaushik.sr@ece.iisc.ernet.in

P. Vijay Kumar*

Department of ECE,
Indian Institute of Science,
Bangalore 560012, India
Email: vijay@ece.iisc.ernet.in
*Corresponding author

Abstract: In this paper, three outer bounds on the normalised storage-repair bandwidth trade-off of regenerating codes having parameter set $\{(n, k, d), (\alpha, \beta)\}$ under the exact-repair (ER) setting are presented. The first outer bound, termed as the *repair-matrix bound*, is applicable for every parameter set (n, k, d), and in conjunction with a code construction known as *improved* *layered codes*, it characterises the normalised ER trade-off for the case $(n, k = 3, d = n - 1)$. The bound shows that a non-vanishing gap exists between the ER and functional-repair (FR) trade-offs for every (n, k, d). The second bound, termed as the *improved Mohajer-Tandon bound*, is an improvement upon an existing bound due to Mohajer et al. and performs better in a region away from the minimum-storage-regenerating (MSR) point. However, in the vicinity of the MSR point, the repair-matrix bound outperforms the improved Mohajer-Tandon bound. The third bound is applicable to linear codes for the case $k = d$. In conjunction with the class of layered codes, the third outer bound characterises the normalised ER trade-off in the case of linear codes when $k = d = n - 1$.

Keywords: distributed storage; exact-repair; outer bounds; regenerating codes; storage-repair bandwidth trade-off; trade-off characterisation.

Reference to this paper should be made as follows: Sasidharan, B., Prakash, N. Nikhil Krishnan, M., Vajha, M., Senthoor, K. and Vijay Kumar, P. (2016) 'Outer bounds on the storage-repair bandwidth trade-off of exact-repair regenerating codes', *Int. J. Information and Coding Theory*, Vol. 3, No. 4, pp.255–298.

Biographical notes: Birenjith Sasidharan received BTech in Electronics and Communication Engineering from College of Engineering, Trivandrum and MSc(Engg.) from Indian Institute of Science, Bangalore in 2008. During 2008–2011, he was on the faculty of Electronics and Communication Engineering at Govt. Engineering Colleges in Kerala. Since 2011, he has been a PhD student at the Department of Electrical Communication Engineering in Indian Institute of Science, Bangalore. His current research interests include information-theoretic limits and code constructions for distributed storage.

N. Prakash received BTech in Electronics and Communication Engineering, from College of Engineering, Thiruvananthrapuram, in 2004, and MTech in Communication Engineering from the Indian Institute of Technology, Madras, in 2006 and PhD from the Indian Institute of Science, Bangalore in 2015. He is currently a postdoctoral research associate at the Massachusetts Institute of Technology, Cambridge, MA, USA. His current research focusses on various aspects of distributed data storage systems, including designing new erasure codes for practical data storage, efficient schemes for file synchronisation in coded systems, incorporating erasure codes to improve performance of distributed algorithms for asynchronous data storage systems having consistency requirements, and test-bed implementations of storage systems. His past research work includes problems in distributed function computation and hands-on experience in physical layer algorithms for wireless communication systems.

M. Nikhil Krishnan received BTech in Electronics and Communication Engineering from Amrita School of Engineering, Kollam, in 2011 and ME in Telecommunication from the Indian Institute of Science (IISc), Bangalore, in 2013. He is currently a PhD Student at IISc. He is a recipient of the Visvesvaraya Fellowship awarded by the Department of Electronics and Information Technology (DeitY), Government of India. His research currently deals with the application of coding theory in distributed storage systems.

Myna Vajha is currently pursuing PhD at Indian Institute of Science. She received Master's from University of Southern California and BTech from IIT Kharagpur. She has previously worked with Ericsson, San Jose as a systems architect in the areas of computer networks, systems and security. Her current research interests include coding theory and information theory. She is currently supported by Visvesvaraya PhD Scheme for Electronics & IT awarded by the Department of Electronics and Information Technology, Government of India.

Kaushik Senthoor received BTech from Amrita School of Engineering, Coimbatore in 2012 and ME in Telecommunication Engineering from Indian Institute of Science, Bangalore, in 2014. He is currently a PhD Student in Indian Institute of Technology, Madras. Prior to this, he was working as a Project Associate in Indian Institute of Science, Bangalore.

P. Vijay Kumar (S'80-M'82-SM'01-F'02) received PhD from USC in 1983 in Electrical Engg. From 1983 to 2003, he was being the Faculty of EE-Systems Department at USC. Since 2003, he has been on the Faculty of IISc, Bengaluru. He also holds the position of Adjunct Research Professor at USC. He is an ISI highly cited author and a Fellow of the Indian National Academy of Engg. He is also a co-recipient of the 1995 IEEE Information Theory Society Prize-Paper award and the IEEE Data Storage Best-Paper Award of 2011/2012. A pseudorandom sequence family designed in a 1996 paper co-authored by him now forms the short scrambling code of the 3G WCDMA cellular standard. He received the USC School of Engineering Senior Research Award in 1994. He was on the Board of Governors of the IEEE Information Theory Society from 2013 to 2015.

This paper is a revised and expanded version of a paper entitled 'An improved outer bound on the storage-repair-bandwidth tradeoff of exact-repair regenerating codes', presented at *ISIT 2014, Honolulu and 'The storage-repair-bandwidth tradeoff of exact repair linear regenerating codes for the case* $d = k = n - 1$' presented at *ISIT 2015*, Hong Kong.

1 Introduction

1.1 Regenerating codes

In the regenerating-code framework Dimakis et al. (2010), all symbols are drawn from a fixed finite field $\mathbb{F}$ whose size is the power of a prime. The size of the field does not play an important role in the present paper, and for this reason, this does not appear in our notation for the field. Data pertaining to a file comprised of B symbols is encoded into a set of $n\alpha$ coded symbols and then stored across n nodes in the network with each node storing α coded symbols. A data collector should be able to retrieve the file downloading entire data from any k nodes. Furthermore, k is the minimum such number that allows reconstruction of the file. In the event of a node failure[1], node repair is accomplished by having the replacement node connect to any d nodes and download $\beta \leq \alpha$ symbols from each node with $\alpha \leq d\beta < B$. These d nodes are referred to as helper nodes. From the minimality of k, it can be shown that d must lie in the range

$$k \leq d \leq n - 1.$$

The quantity $d\beta$ is called as the repair bandwidth. Here one makes a distinction between functional and exact repair. By functional repair (FR), it is meant that a failed node will be replaced by a new node such that the resulting network continues to satisfy the data collection and node-repair properties defining a regenerating code. An alternative to functional repair is *exact repair* (ER) under which one demands that the replacement node stores precisely the same content as the failed node. From a practical perspective, ER is preferred at least for two reasons. First, the algorithms pertaining to data collection and node repair remain static for the ER case. Second if the ER code is linear, then it permits the storage of data in systematic form, which facilitates operations under paradigms such as MapReduce Dean and Ghemawat (2008). We will use $\mathcal{P}_{\rm f}$ to denote the *full parameter set* $\mathcal{P}_{\rm f} = \{(n, k, d), (\alpha, \beta)\}$ of a regenerating code and use $\mathcal{P}$ when we wish to refer to only the parameters (n, k, d).

Figure 1 Data collection (see online version for colours)

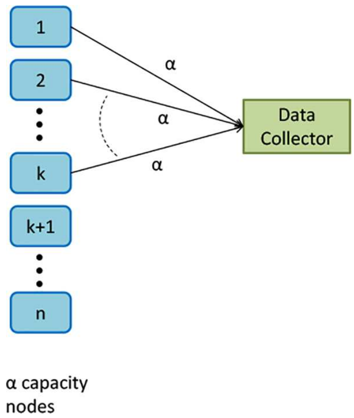
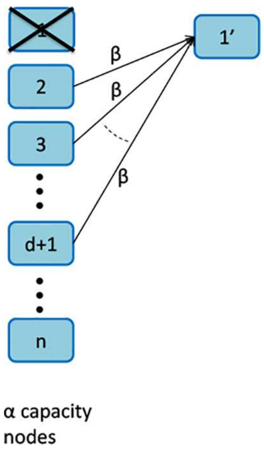


Figure 2 Node repair (see online version for colours)



1.2 The storage-repair bandwidth trade-off

A cut-set bound based on network-coding concepts tells us that given a code parameter set $\mathcal{P}_{\mathrm{f}}$, the maximum possible size B of a regenerating code is upper bounded as Dimakis et al. (2010),

$$B \leq \sum_{\ell=0}^{k-1} \min\{\alpha, (d-\ell)\beta\}. \tag{1}$$

The derivation of the bound in (1) makes use of only FR constraints, and therefore it is valid for both FR and ER codes. An FR code $\hat{\mathcal{C}}$ is said to be optimal if the file size $\hat{B}$ of $\hat{\mathcal{C}}$ achieves the cut-set bound in (1) with equality, and further, that if either α or β is reduced, equality fails to hold in (1). The existence of such codes has been shown in Dimakis et al. (2010), using network-coding arguments related to multicasting Wu (2010). In general, we will use $\hat{\mathcal{C}}$, $\hat{B}$ etc to denote symbols relating to an optimal FR code while reserving $\mathcal{C}$, B etc. to denote symbols relating to an ER code.

Given $\mathcal{P}$ and B, there are multiple pairs (α, β) that satisfy (1). It is desirable to minimise both α as well as β, since minimising α reduces storage requirements, while minimising β results in a storage solution that minimises repair bandwidth. It is not possible to minimise both α and β simultaneously, and thus there is a trade-off between choices of the parameters α and β. This trade-off will be referred to as storage-repair bandwidth (S-RB) trade-off under functional repair. Since much of the emphasis of the current paper is upon the distinction between the S-RB trade-offs under functional and exact repair, we will use FR trade-off and ER trade-off to refer, respectively, to the two trade-offs. The two extreme points in the FR trade-off are termed the *minimum storage regeneration* (MSR) and *minimum bandwidth regeneration* (MBR) points, respectively. The parameters α and β for the MSR point on the trade-off can be obtained by first minimising α and then minimising β to yield

$$B = k\alpha, \;\; \alpha = (d-k+1)\beta. \tag{2}$$

Reversing the order leads to the MBR point which thus corresponds to

$$B = \left(dk - \binom{k}{2}\right)\beta, \;\; \alpha = d\beta. \tag{3}$$

The remaining points on the trade-off will be referred to as *interior points*. As the trade-off is piecewise linear, there are k points of slope discontinuity, corresponding to

$$\alpha = (d-\mu)\beta, \;\; \mu \in \{0, \cdots k-1\}.$$

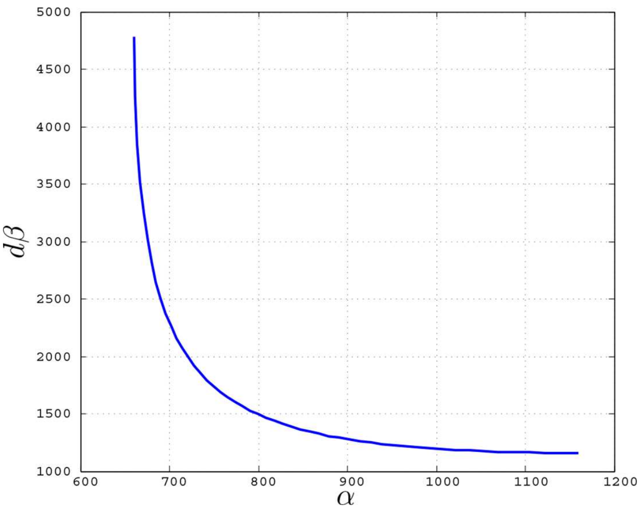
Setting $\mu = k-1$ and 0, respectively, yields the MSR and MBR points. The remaining values of $\mu \in \{1, \cdots k-2\}$ correspond to interior points with slope discontinuity. Interior points where there is no slope discontinuity can be specified by setting,

$$\begin{aligned} \alpha &= (d-\mu)\beta - \theta, \; \theta \in [0, \beta) \\ &= (d-\mu)\beta - \nu\beta, \; \nu \in [0, 1), \end{aligned} \tag{4}$$

with $\mu \in \{0, 1, \ldots, k-2\}$. When $\mu = k-1$, we always set $\nu = 0$. We will refer to the pair (α, β) as an *operating point* of the regenerating code. The trade-off between α and $d\beta$ is plotted in Figure 3 for $(n = 131, k = 120, d = 130)$ and file size $B = 725360$.

The results in the present paper pertain to the ER trade-off. Several ER code constructions Rashmi, Shah and Kumar (2011); Cadambe et al. (2013); Papailiopoulos, Dimakis and Cadambe (2013); Suh and Ramchandran (2011); Shah et al. (2012b,a); Tamo, Wang and Bruck (2013) are now available that correspond to the MSR and the MBR points of the FR trade-off. Thus, the end points of the ER trade-off coincide with those of the FR trade-off. However, characterisation of the interior points of the ER trade-off remains an open problem in general.

Figure 3 FR Trade-off. Here $(n = 60, k = 51, d = 58, B = 33660)$ (see online version for colours)



1.3 The normalised ER trade-off and ER-code symmetry

For a given parameter set $\mathcal{P} = (n, k, d)$, there are several known constructions for an ER code, each of which is valid only for a restricted set of file sizes. Since the ER trade-off for a fixed (n, k, d) varies with file size B, comparison across code constructions is difficult. For this reason, we normalise (α, β) by the file size B. The trade-off between $\bar{\alpha} = \frac{\alpha}{B}$ and $\bar{\beta} = \frac{\beta}{B}$, thus obtained for a fixed value of (n, k, d), will be referred to here as the *normalised ER trade-off*. The tuple $(\bar{\alpha}, \bar{\beta})$ is referred to as the *normalised operating point* of a regenerating code. Throughout the remainder of this paper, we will work only with the normalised version of the ER trade-off.

Given a regenerating code $\mathcal{C}$ associated to parameter set $\mathcal{P}$ and file size B, the parameters of the code are clearly invariant to coordinate (i.e., node) permutation. Given an ER code $\mathcal{C}$, we can vertically stack the $n!$ codewords obtained by encoding independent files using all possible node permutations of $\mathcal{C}$. The resultant stack of $n!$ codewords may be regarded as a single new ER regenerating code $\mathcal{C}'$, where the parameters (n, k, d) remain the same, but where the parameters (α, β) and B are each scaled up multiplicatively, by a factor of $n!$. It is clear that $\mathcal{C}'$ is symmetric in the sense that the amount of information contained in a subset $A \subset [n]$ of nodes depends only upon the size $|A|$ of A and not upon the particular choice of nodes lying in A. This symmetry carries over even in the case of repair data transferred by a collection D of $d = |D|$ nodes for the replacement of a fixed node. Such codes will be referred to as *symmetric* ER codes. Since the normalised values $(\bar{\alpha}, \bar{\beta})$ of $\mathcal{C}'$ remain the same as that of $\mathcal{C}$, there is no change in operating point on the normalised ER trade-off in going from $\mathcal{C}$ to $\mathcal{C}'$. Thus, given our focus on the normalised trade-off, it is sufficient to consider *symmetric* ER codes. This observation was first made by Tian (2014).

1.4 Results

Although the complete characterisation of normalised ER trade-off for every parameter set remains an open problem, much progress has been made. It was shown in Shah et al. (2012a), that apart from the MBR point and a small region adjacent to the MSR point, there do not exist ER codes whose $(\alpha, d\beta)$ values correspond to coordinates of an interior point on the FR trade-off. However, the authors of Shah et al. (2012a) did not rule out the possibility of approaching the FR trade-off asymptotically, i.e., as the file size $B \to \infty$. It was first shown by Tian (2014) that the ER trade-off lies strictly away from the FR trade-off. This was accomplished using an information theory inequality prover ITIP (2016) to characterise the normalised ER trade-off for the particular case of $(n, k, d) = (4, 3, 3)$ and showing it to be distinct from the FR trade-off. The results in the Tian (2014) were, however, restricted to the particular case $(n, k, d) = (4, 3, 3)$.

That the ER trade-off lies strictly above the FR trade-off for *any* value of the parameter set (n, k, d), which was first shown in Sasidharan, Senthoor and Kumar (2014). The first result in the present paper is to show an outer bound on the normalised ER trade-off for every parameter set (n, k, d) and is stated in Theorem 3.4. We refer to this outer bound as the *repair-matrix bound*. This outer bound in conjunction with a code construction appearing in Senthoor, Sasidharan and Kumar (2015) characterises the normalised ER trade-off for the parameter set (n, k, d) for $k = 3$, $d = n - 1$ and any $n \geq 4$.

Two outer bounds on the normalised ER trade-off appeared subsequently in Duursma (2014) and Duursma (2015). In Duursma (2014), the author presents two bounds on the ER file size. In the first bound, he builds on top of the techniques presented in Tian (2014) and derives a bound that applies to a larger set of parameters. The second bound is obtained by taking a similar approach as in Sasidharan, Senthoor and Kumar (2014) and is shown to improve upon the one given in Sasidharan, Senthoor and Kumar (2014). In Duursma (2015), the author provides an upper bound on ER file size, that is non-explicit in general. However for the case of linear codes, the bound can be computed to obtain an explicit expression for any parameter set (n, k, d). A second paper by Tian (2015) characterises the ER trade-off for $(n = 5, k = 4, d = 4)$ with the help of a class of codes known as the *layered codes* introduced in Tian et al. (2015). A different approach adopted to derive an outer bound on the normalised ER trade-off is presented in Mohajer and Tandon (2015). In Mohajer and Tandon (2015), Mohajer et al. derived an outer bound for general (n, k, d) that turns out to be optimal for the special case of $(n, k = n - 1, d = n - 1)$ in a limited region of $\bar{\beta} \leq \frac{2\bar{\alpha}}{k}$ close to the MBR point. Optimality follows from the fact that a code construction due to Goparaju, El Rouayheb and Calderbank (2014) meets their outer bound in the region $\bar{\beta} \leq \frac{2\bar{\alpha}}{k}$. We will refer to this outer bound in Mohajer and Tandon (2015) as the *Mohajer–Tandon bound*.

The second result of the present paper is an improvement upon the Mohajer–Tandon bound for the case $k < d$. We make use of similar techniques introduced in Mohajer and Tandon (2015) to arrive at this improved bound. This bound is stated in Theorem 5.1, and we refer to it as the *improved Mohajer–Tandon bound*. While the improved Mohajer–Tandon bound performs better whenever $k < d$, it coincides with the Mohajer–Tandon bound when $k = d$. The repair-matrix bound still performs better than the improved

Mohajer–Tandon bound in a region close to the MSR point. The theorem below essentially combines the repair-matrix bound and the improved Mohajer–Tandon bound.

Theorem 1.1: *Let*

$$B_1 = \sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\} - \delta,$$

where δ is as defined in (29)*, and it corresponds to the repair-matrix bound. Let B_2 be the expression on the RHS in* (43)*, corresponding to the improved Mohajer–Tandon bound. Then the ER file size B is bounded by,*

$$B \leq \min\{B_1, B_2\}.$$

The final result presented in this paper is under the restricted setting of linear codes. For the case of $(n \geq 4, k = n-1, d = n-1)$, we characterise the normalised ER trade-off under this setting. This is done by deriving an explicit upper bound on the file size B of a ER linear regenerating code for the case $k = d = n-1, n \geq 4$. The outer bound remains valid for the general case $k = d$ even when $d < n-1$. For the case of $(n, k = n-1, d = n-1)$, the outer bound matches with the region achieved by the layered codes. This result, which first appeared in Prakash and Krishnan (2015), is stated below:

Theorem 1.2: *Consider an exact repair linear regenerating code, having parameters $(n, k = n-1, d = n-1), (\alpha, \beta), n \geq 4$. Then, the file size B of the code is upper bounded by*

$$B \leq \begin{cases} \left\lfloor \frac{r(r-1)n\alpha + n(n-1)\beta}{r^2+r} \right\rfloor, & \frac{d\beta}{r} \leq \alpha \leq \frac{d\beta}{r-1}, \quad 2 \leq r \leq n-2 \\ (n-2)\alpha + \beta, & \frac{d\beta}{n-1} \leq \alpha \leq \frac{d\beta}{n-2}. \end{cases} \tag{5}$$

We remark that there are no known instances of non-linear codes that violate the above outer bound derived under the linear setting. In an independent work Elyasi, Mohajer and Tandon (2015), the authors also derive the normalised linear ER trade-off for the case $(n, k = n-1, d = n-1)$, but the trade-off is expressed in an implicit manner as the solution to an optimisation problem.

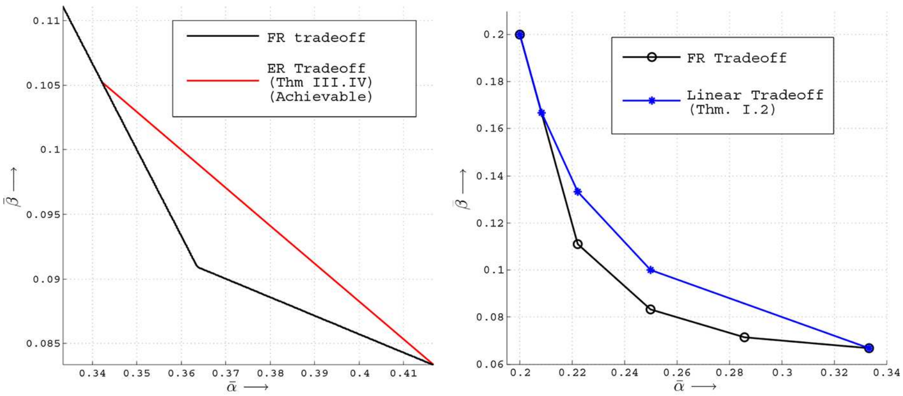
In Figure 4, we plot the cases in which our outer bounds characterise the normalised ER trade-off. In Figure 5, we do a performance comparison of various known bounds.

1.5 Our approach

The present paper derives outer bounds on the normalised ER trade-off of a regenerating code with full parameter set $\mathcal{P}_f = \{(n, k, d), (\alpha, \beta)\}$. Since every ER code is an FR code, it is clear that the normalised ER trade-off lies on or above and to the right of the normalised FR trade-off in the $(\bar{\alpha}, \bar{\beta})$-plane. When we say that the normalised ER trade-off *lies above* the normalised FR trade-off, we imply that, for given (n, k, d), there is at least one value of normalised parameter $\bar{\beta}_0$ such that the corresponding normalised values $\bar{\alpha}_{\text{ER}}$ and $\bar{\alpha}_{\text{FR}}$ satisfy $\bar{\alpha}_{\text{ER}} > \bar{\alpha}_{\text{FR}}$. An equivalent definition in terms of the file size B is given as follows. For given (n, k, d), let $\hat{B}_0 := \hat{B}_{\text{opt}}(\alpha_0, \beta_0)$ denote the optimal FR file size at an operating point (α_0, β_0) with $\alpha_0 = (d - \mu)\beta_0 - \nu\beta_0$ as in (4). Thus $\left(\frac{\alpha_0}{\hat{B}_0}, \frac{\beta_0}{\hat{B}_0}\right)$ is a point lying on the normalised FR trade-off. Suppose that the maximum file size of an ER code as a function of (α, β) is

$$B(\alpha, \beta) = \hat{B}(\alpha, \beta) - \epsilon(\alpha, \beta)$$

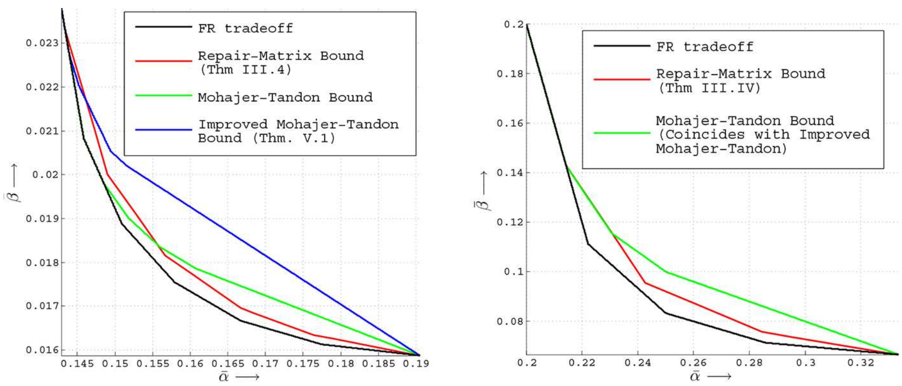
Figure 4 Characterisation of normalised ER Trade-off (see online version for colours)



(a) For $k = 3$, $d = n - 1$, codes in [17] achieves our repair-matrix bound. The example here is $(n = 6, k = 3, d = 5)$.

(b) For $k = d = n - 1$, our outer bound matches the achievable region of layered codes, thus characterizing the tradeoff under linear setting. The example here is $(n = 6, k = 5, d = 5)$.

Figure 5 Performance comparison of various outer bounds (see online version for colours)



(a) The example here is $(n = 13, k = 7, d = 12)$. The combination of repair-matrix bound and improved Mohajer-Tandon bound performs better than other bounds given in the plot.

(b) Example here is $(n = 6, k = d = 5)$. When $k = d$, both Mohajer-Tandon and the improved Mohajer-Tandon bounds coincide.

for some non-negative function $\epsilon(\alpha, \beta)$. Let $\epsilon_0 = \epsilon(\alpha_0, \beta_0)$. Then the normalised operating points $(\bar{\alpha}_{\text{ER}}, \bar{\beta}_{\text{ER}})$ for an optimal ER code as given by

$$\bar{\beta}_{\text{ER}} = \frac{\beta_0}{B(\alpha_0, \beta_0)} = \frac{1}{\frac{\hat{B}_0}{\beta_0} - \frac{\epsilon_0}{\beta_0}}$$

$$\bar{\alpha}_{\text{ER}} = \frac{\alpha_0}{B(\alpha_0, \beta_0)} = \frac{1}{\frac{\hat{B}_0}{\alpha_0} - \frac{\epsilon_0}{\alpha_0}} = \frac{1}{\frac{\hat{B}_0}{\alpha_0} - \frac{\epsilon_0}{\beta_0}\frac{1}{(d-\mu-\nu)}}$$

will be bounded away from $\left(\frac{\alpha_0}{\hat{B}_0}, \frac{\beta_0}{\hat{B}_0}\right)$ if $\left(\frac{\epsilon_0}{\beta_0}\right)$ does not vanish to zero. It follows that an upper bound on the file size B of an ER code

$$B \leq B_{\text{upper}}(\alpha, \beta),$$

such that

$$\lim_{\beta \to \infty} \frac{\hat{B}(\alpha, \beta) - B_{\text{upper}}(\alpha, \beta)}{\beta} > 0 \tag{6}$$

for some (μ, ν) will equivalently define a bound on the normalised ER trade-off that lie strictly above the normalised FR trade-off. Throughout the paper, our approach therefore will be to derive upper bounds on ER file size that satisfy the criterion in (6).

If the full parameter set of a regenerating code has $n > (d+1)$, then by restricting attention to a set of $(d+1)$ nodes, one obtains a regenerating code with $n = (d+1)$ with all other parameters remaining unchanged. It follows from this that any upper bound on the size B corresponding to full parameter set $\{(n = (d+1), k, d), (\alpha, \beta)\}$ continues to holds for the case $n > (d+1)$ with the remaining parameters left unchanged. Keeping this in mind, we will assume throughout that $n = (d+1)$.

A key technique used in the paper is to lower bound the difference $\epsilon = \hat{B}_{\text{opt}}(\alpha, \beta) - B(\alpha, \beta)$ between the file size of an optimal FR code and an ER code. The total information content in a regenerating code can be accumulated from a set $\{1, 2, \ldots, k\}$ of k nodes. The conditional entropy of the $(i+1)$-th node data conditioned on the data accumulated from previous $i, 0 \leq i \leq k-1$ nodes is compared against the corresponding value of an optimal FR code, and the difference is defined to be ω_i. It follows that ϵ is the sum of all $\{\omega_i\}_{i=0}^{k-1}$. Our approach is to relate $\{\omega_i\}_{i=0}^{k-1}$ in terms of entropy of certain collections of repair data and to eventually find an estimate on ϵ. Along the way, we construct a *repair matrix* as an arrangement of random variables corresponding to repair data in a $((d+1) \times (d+1))$-sized matrix. Many properties pertaining to the inherent symmetry of regenerating code become clear from the repair-matrix perspective, and we use it as a tool in our proofs.

A different approach is used in deriving an upper bound on the ER file size of a linear regenerating code. Here we focus on a parity-check matrix H of a linear ER code and construct an augmented parity-check matrix H_{repair} of size $(n\alpha \times n\alpha)$ that captures the exact-repair properties. A block-matrix structure is associated to H_{repair}, and thereby we identify n thick columns $\{H_1, H_2, \ldots H_n\}$ of H_{repair} with H_i associated to the node i. Here, we mean by a thick column a collection of α columns. Let us denote by δ_i the incremental rank added by H_i to the collection of $(i-1)\alpha$ vectors in $\{H_j \mid 1 \leq j < i\}$. We estimate lower bounds on $\{\delta_i\}_{i=1}^{n}$ that will eventually lead to a lower bound on the rank of H. It is clear that the file size B is the dimension of the code, and therefore a lower bound on the rank of H results in an upper bound on the file size.

1.6 Organisation of the paper

In Section 2, we describe the result of Shah et al. showing the non-existence of ER codes operating on the FR trade-off. In Section 3.3, we present an upper bound on the ER file size. In Section 4, we review the various upper bounds on ER file size that are known in the literature. In Section 5, we develop on the existing Mohajer–Tandon bound and make an improvement upon that to get a better bound when $d > k$. In Sections 6,7,8, we focus on upper bounds on file size under linear setting. We characterise the normalised ER trade-off for the case $(n, k = n-1, d = n-1)$ in Section 8, while the proof techniques are illustrated for a particular case of $(n = 5, k = 4, d = 4)$ in Section 7. In Section 9, we discuss the achievability of the outer bounds on normalised ER trade-off derived at earlier sections.

2 The non-existence of ER codes achieving FR trade-off

As mentioned in Section 1.4, it was shown in Shah et al. (2012a) that apart from the MBR point and a small region adjacent to the MSR point, there do not exist ER codes whose $(\alpha, d\beta)$ values correspond to coordinates of an interior point on the FR trade-off. The theorem in Shah et al. (2012a) due to Shah et al. is stated below.

Theorem 2.1 (Theorem 7 in Shah et al. (2012a)): *For any given values of $(n, k \geq 3, d)$, ER codes do not exist for the parameters (α, β, B) lying at an interior point on the FR trade-off except possibly for the case*

$$(d-k+1)\beta \leq \alpha \leq \left[(d-k+2) - \frac{d-k+1}{d-k+2}\right]\beta. \tag{7}$$

The region

$$\left\{(\alpha, \beta) \mid (d-k+1)\beta \leq \alpha \leq \left[(d-k+2) - \frac{d-k+1}{d-k+2}\right]\beta\right\}$$

on which the theorem does not claim the non-existence of ER codes is referred to as the *near-MSR region*. The Theorem 2.1 however did not rule out the possibility of approaching the FR trade-off asymptotically, i.e., as the file size $B \to \infty$. As mentioned earlier, this question was answered by Tian in the negative manner in Tian (2014) for the specific case when $(n, k, d) = (4, 3, 3)$.

In this section, we will describe the approach taken by Shah et al. in proving Theorem 2.1 in terms of the notation to be used in the present paper. We begin with some notation and definitions. Let $\mathcal{C}$ be an ER regenerating code over $\mathbb{F}$ having file size B and full parameter set $\mathcal{P}_f = \{(n, k, d), (\alpha, \beta)\}$. We regard the message symbols as a collection of B random variables taking on values in $\mathbb{F}$ and use M to denote the $(1 \times B)$ random vector whose components are the B message symbols. We use $p_M(\cdot)$ to denote the joint probability distribution of the M random variables. All other random variables pertaining to the regenerating code are functions of the components of M and satisfy probability distributions that are induced by p_M.

We will use $[i], 1 \leq i \leq n$ to denote the set $\{1, 2, \ldots, i\}$ and define [0] to be the empty set ϕ. For $1 \leq i \leq j \leq n$, we use $[i\ j]$ to denote the set $\{i, i+1, \ldots, j\}$. Whenever we write $[i\ j]$ with $i > j$, it will be assumed to be the empty set. On occasion, we will run into a set of random variables of the form W_A where A is the empty set, W_A should again be interpreted as the empty set.

2.1 The repair matrix and the constraints imposed by exact-repair

As made clear in Section 1.5, we assume that $n = d + 1$ without loss of generality. Let $W_x, 1 \leq x \leq n$ denote the random variable corresponding to the contents of a node x. Given a subset $A \subseteq [n]$, we use

$$W_A = \{W_x \mid x \in A\}$$

to denote the contents of nodes indexed by A. Clearly,

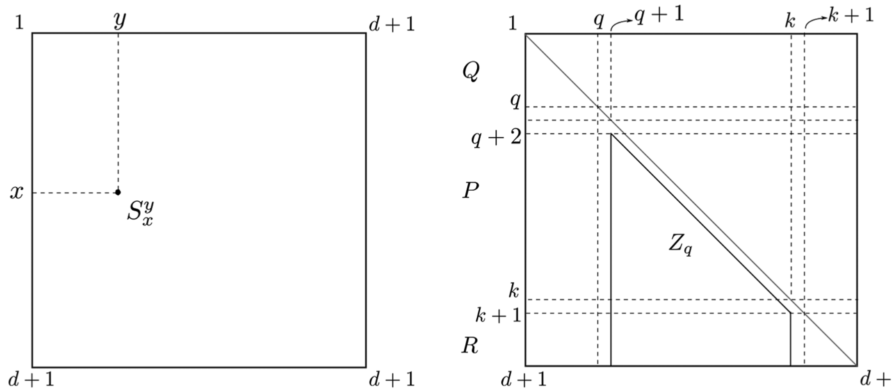
$$H(W_x) \leq \alpha. \tag{8}$$

Let $S_x^y, x, y \in [n], x \neq y$ denote the random variables corresponding to the helper data sent by the helper node x to the replacement of a failed node y. This is well defined because under the assumption $n = (d + 1)$, there is just one set of d helper nodes for any failed node. Given a pair of subsets $X, Y \subseteq [n]$, we define $S_X^Y = \{S_x^y \mid x \in X, y \in Y, x \neq y\}$. We use the short-hand notation S_X to indicate S_X^X. From the definition of regenerating codes, it follows that

$$H(S_x^y) \leq \beta. \tag{9}$$

In (8, 9), information is measured in units of $\log_2(|\mathbb{F}|)$ bits. The collection of random variables $\{S_x^y \mid x \in [d + 1], y \in [d + 1], x \neq y\}$ can schematically be represented using a $(d + 1) \times (d + 1)$ matrix $\mathcal{S}$ with empty cells along the diagonal as shown in Figure 6(a). The rows in this matrix correspond to the helper nodes and the columns to nodes undergoing repair. The (x, y)th entry of this matrix, thus corresponds to S_x^y. We will refer to $\mathcal{S}$ as the *repair matrix*. The subset of $\mathcal{R}$ appearing below the diagonal and above the diagonal are denoted by $\mathcal{R}_L$ and $\mathcal{R}_U$, respectively.

Figure 6 The repair matrix and the trapezoidal configuration



(a) Illustration of the repair matrix. (b) The trapezoidal configuration

Apart from the constraints given in (8), (9), the requirements of data reconstruction and exact-repair impose further constraints. The constraint due to data reconstruction is given by either of the following two equivalent statements:

$$H(W_A) = B, \ |A| \geq k, \tag{10}$$

$$H(M \mid W_A) = 0, \ |A| \geq k. \tag{11}$$

For every $i \in [n]$, the exact-repair condition imposes the constraint

$$H(W_i \mid S^i_{\mathcal{D}}) = 0,\ |\mathcal{D}| = d,\ i \notin \mathcal{D}. \tag{12}$$

2.2 *Trapezoidal configurations in the repair matrix*

Throughout the discussion taking place in Sections up to 3, we will assume that there is a fixed numbering of the $n = (d + 1)$ nodes in the network. In (10), the file size B is expressed as the joint entropy of a collection k random variables $\{W_1, W_2, \ldots, W_k\}$. It is possible to express B as the joint entropy of other subsets of random variables, in particular those involved in node repair. An example, important for the discussion to follow, appears below. Let q be an integer lying in the range $0 \le q \le k$ and set

$$\begin{aligned} Q &= \{1, 2, \cdots, q\} \\ P &= \{q + 1, q + 2, \cdots, k\} \\ R &= \{k + 1, k + 2, \cdots (d + 1)\}. \end{aligned}$$

Note that Q, P, R are all functions of the integer q. When $q = 0$, we will set Q to be the empty set ϕ. Note that $P = [k] \setminus Q$ and $R = [k + 1\ d + 1]$. We define:

$$Z_q = \mathcal{R}_L \cap S^P_{[d+1]} \tag{13}$$

$$X_q = \mathcal{R}_L \cap S_P. \tag{14}$$

Then we can write B as:

$$\begin{aligned} B &= H(W_Q, W_P) \\ &= H(W_Q, W_P, Z_q) \\ &= H(W_Q, Z_q) + H(W_P \mid W_Q, Z_q) \\ &= H(W_Q, Z_q) \end{aligned}$$

where (15) follows from the exact-repair condition (12). The collection Z_q of random variables forms a trapezoidal region within the repair matrix as shown in Figure 6(b). We refer to (W_Q, Z_q), $q \in \{0, 1, \ldots, k\}$ as a *trapezoidal configuration*. The set Z_q is said to be the *trapezoid* corresponding to the trapezoidal configuration (W_Q, Z_q). It is clear that $Z_q = X_q \uplus S^P_R$. Next we proceed to define a *sub-trapezoid* of the trapezoid Z_q. Let $T = \{q + 1, q + 3, \ldots, q + t\} \subseteq P$ be a subset of size $0 \le t \le k - q$ of P. Then we define the subset $Z_{q,t}$ of Z_q as:

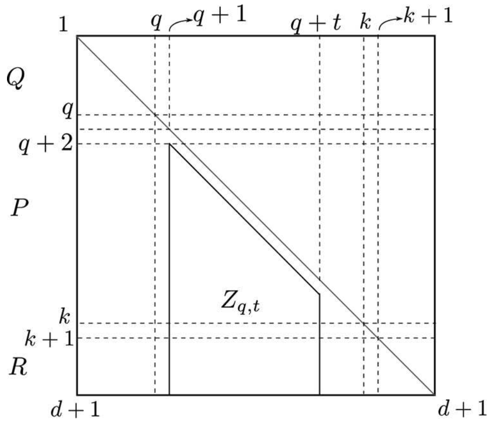
$$Z_{q,t} := \mathcal{R}_L \cap S^T_{[d+1]}.$$

The set $Z_{q,t}$ also forms a trapezoidal region in $\mathcal{R}$ and is called a sub-trapezoid of the trapezoid Z_q. Here again, we define $X_{q,t}$ as:

$$X_{q,t} := S_T \cap Z_{q,t},$$

and it follows that $Z_{q,t} = X_{q,t} \uplus S^T_{R \cup (P \setminus T)}$. A sub-trapezoid is illustrated in Figure 7.

Figure 7 Illustration of the sub-trapezoid $Z_{q,t}$



For every trapezoidal configuration (W_Q, Z_q) indexed by $q = 0, 1, \ldots, k$, we have the identity

$$B = H(W_Q, Z_q), \tag{15}$$

and the corresponding inequality obtained by repeatedly applying the union bound $H(X_1, X_2) \leq H(X_1) + H(X_2)$, i.e.,

$$\begin{aligned} B &\leq H(W_Q) + H(Z_q) \\ &\leq H(W_Q) + H(X_q) + H(S_R^P) \qquad (16) \\ &\leq q\alpha + \binom{k-q}{2}\beta + (d+1-k)(k-q)\beta. \qquad (17) \end{aligned}$$

We define for $q \in \{0, 1, 2 \cdots, k\}$, the quantities:

$$B_q := q\alpha + \binom{k-q}{2}\beta + (d+1-k)(k-q)\beta.$$

2.3 The argument for non-existence

Let us consider an ER code operating at the point (α, β) satisfying $\alpha = (d-\mu)\beta$. For this value of α, as shown below, the FR bound gives us $B_{\mu+1}$ as the upper bound on file size:

$$\begin{aligned} B &\leq \sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\} \\ &= (\mu+1)\alpha \; + \sum_{i=\mu+1}^{k-1} (d-i)\beta \\ &= (\mu+1)\alpha \; + \sum_{j=0}^{k-\mu-2} (d-k+1+j)\beta \end{aligned}$$

$$
\begin{aligned}
&= (\mu+1)\alpha \;+\; (d-k+1)(k-\mu-1)\beta \;+\; \binom{k-\mu-1}{2}\beta \\
&= B_{\mu+1}.
\end{aligned}
$$

Thus if an ER code is optimal with respect to the FR trade-off at the point $\alpha = (d-\mu)\beta$, from Eqs. (15) and (16), with $q = (\mu+1)$, one obtains that such a code must satisfy:

$$
H(Z_{\mu+1} \mid W_{[\mu]}) = H(Z_{\mu+1}) = \binom{k-\mu-1}{2}\beta + (d+1-k)(k-\mu-1)\beta, \quad (18)
$$

i.e., the union bound on $Z_{\mu+1}$ must hold with equality. That means that all the random variables in $Z_{\mu+1}$ are mutually independent. However, it is shown by Shah et al. (2012a) that this is not possible if an ER code lies at an interior point except for the near-MSR region and the MBR point. To prove this result, the authors of Shah et al. (2012a) focus on a subset S_m^L of the repair matrix where $m \in [n]$ and $L \subseteq [n]$ are arbitrarily chosen from $[n]$ while satisfying the conditions $|L| := \ell < k$ and $m \notin L$. The subset S_m^L is of course, the union of helper data sent by a single node m to the nodes in L. We can write

$$
\begin{aligned}
H(S_m^L) &= H(S_m^L \mid W_L) + I(S_m^L : W_L) \\
&\leq H(S_m^L \mid W_L) + I(W_m : W_L). \qquad (19)
\end{aligned}
$$

It can be shown that (see Shah et al. (2012a))

$$
H(S_m^L \mid W_L) = 0, \; \ell \geq \mu+1, \qquad (20)
$$

and that

$$
I(W_m : W_L) = \beta, \; \ell = \mu+1. \qquad (21)
$$

As a consequence, we have that

$$
H(S_m^L) = \beta, \; \ell = \mu+1. \qquad (22)
$$

It follows that

$$
H(S_m^J) \leq \beta, \; \text{for any } J \subseteq [n] \text{ with } \mid J \mid < \mu+1.
$$

In particular this is true of J is of size $|J| = 2$. On the other hand, optimality with respect to the FR bound assumes that each row in the trapezoidal region Z_q has joint entropy equal to the number of repair random variables $S_x^y \in Z_q$ belonging to the row, times β. The bottom row of the trapezoid has $(k-\mu-1)$ entries and thus we clearly have a contradiction whenever $(k-\mu-1) \geq 2$. The argument does not go through when $(k-\mu-1) \leq 1$, i.e., when $\mu \geq k-2$. This necessary condition on μ underlies the fact that the non-existence of ER codes does not hold good in the near-MSR region. The proof given here is for the case when $\alpha = (d-\mu)\beta$ is a multiple of β. This proof can be extended to the general case $\alpha = (d-\mu)\beta - \theta$, for $0 < \theta < \beta$ as well. In the next section, we will exploit this contradiction to derive an upper bound on the file size of an ER code.

3 An upper bound on the ER file size

In this section, we show that for *any* value of the parameter set (n, k, d), the ER trade-off lies strictly above the FR trade-off, a result that was first established in Sasidharan, Senthoor and Kumar (2014). As explained in Section 1.5, we do this by deriving a tighter bound on file size B in the case of ER than is true under FR.

As mentioned in Section 2.3, our approach to bounding the file size B is based on deriving estimates for the joint entropy of subsets of the repair matrix. First, we assume the existence of an ER code having parameters $(n, k, d), (\alpha, \beta)$ whose file size B is of the form $B = \hat{B} - \epsilon$ for some $\epsilon \geq 0$, where $\hat{B}$ is the file size of an optimal FR code having the same parameter set $\mathcal{P}$. Next, we proceed to estimate the joint entropy of the subset Z_q corresponding to a trapezoidal configuration (W_Q, Z_q). We estimate the joint entropy in two different ways and show that the two estimates are in contradiction unless the value of ϵ lies above a threshold value $\epsilon_{\min}$. This allows us to replace $B - \epsilon_{\min}$ as the revised bound on the file size under ER. We will also show that $\epsilon_{\min}$ does not vanish as $\beta \to \infty$.

3.1 Preliminaries

Consider an optimal FR code $\hat{\mathcal{C}}$ possessing the same set of parameters $\mathcal{P}$ as the ER code $\mathcal{C}$. In what follows, given any deterministic or random entity associated with $\mathcal{C}$, we will use a hat to denote the corresponding entity in $\hat{\mathcal{C}}$. For example, $\hat{B}$ denotes the file size of $\hat{\mathcal{C}}$. With this, we can write

$$\begin{aligned}\sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\} = \hat{B} \ &= \ H(\hat{W}_{[k]}) \\ &= \sum_{i=0}^{k-1} H(\hat{W}_{i+1} \mid \hat{W}_{[i]}) \\ &\leq \sum_{i=0}^{k-1} \min\{\alpha, (d-i)\beta\}.\end{aligned}$$

It follows that in an optimal FR code $\hat{\mathcal{C}}$, we must have

$$H(\hat{W}_{i+1} \mid \hat{W}_{[i]}) = \min\{\alpha, (d-i)\beta\}, \ 0 \leq i \leq (k-1).$$

Next, for $0 \leq i \leq k-1$, let us set:

$$\begin{aligned}\gamma_i &= \min\{\alpha, (d-i)\beta\}, \\ \omega_i &= \gamma_i - H(W_{i+1} \mid W_{[i]}),\end{aligned}$$

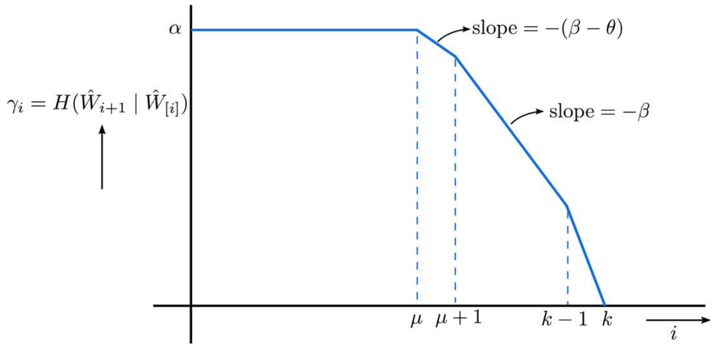
where ω_i measures the drop in the conditional entropy $H(W_{i+1} \mid W_{[i]})$ of an ER code in comparison with its value $H(\hat{W}_{i+1} \mid \hat{W}_{[i]})$ in the case of an optimal FR code. A plot of γ_i as a function of i for a given operating point (α, β) with $\alpha = (d-\mu)\beta - \theta$ appears in Figure 8. We also note the following identities:

$$\epsilon = \sum_{i=0}^{k-1} \omega_i, \tag{23}$$

$$H(W_B \mid W_A) = \sum_{i=a}^{a+b-1} (\gamma_i - \omega_i), \tag{24}$$

where $A = [a]$ and $B = [a+1\ a+b]$ and $0 \leq a \leq a+b \leq k$. The lemma below follows from these identities.

Figure 8 The function γ_i versus i for $\alpha = (d-\mu)\beta - \theta$ (see online version for colours)



Lemma 3.1: *Let (Q, Z_q) be a trapezoidal configuration for some $q \in \{0, 1, \ldots, k\}$, and let $Z_{q,t} \subseteq Z_q$ be a sub-trapezoid with $0 \leq t \leq k-q$. Then*

$$H(Z_{q,t} \mid W_Q) \geq \sum_{i=q}^{q+t-1} (\gamma_i - \omega_i)$$

Proof: By the exact-repair condition, $H(Z_{q,t} \mid W_Q)$ is at least $H(W_{[q+1\ q+t]} \mid W_Q)$ and the result follows from (24). □

3.2 *Upper bounds on joint conditional entropies of repair data*

Let $Q = [q]$ and M, L, be two mutually disjoint subsets of $[d+1] \setminus Q$ with $\ell := |L|$, and $m := |M|$. Then we can write

$$H(S_M^L \mid W_Q) = H(S_M^L \mid W_V, W_Q) + I(S_M^L : W_V \mid W_Q), \tag{25}$$

where in we take $V \supset L$ as a superset of L with $V \cap M = \phi$ and $v := |V|$. Our next objective is to estimate $H(S_M^L \mid W_V, W_Q)$ and $I(S_M^L : W_V \mid W_Q)$ in order to obtain an upper bound on $H(S_M^L \mid W_Q)$.

Lemma 3.2: *Suppose $\alpha = (d-\mu)\beta - \theta$ with $\mu \in \{0, 1, \ldots, k-1\}$ and $\theta \in [0, \beta)$ except when $\mu = k-1$. Then for $2 \leq \ell \leq v < k-q$,*

$$H(S_M^L \mid W_V, W_Q) \leq \begin{cases} \ell\theta + \ell\omega_{v-1+q}, & v = \mu + 1 - q \\ \ell\omega_{v-1+q}, & v > \mu + 1 - q. \end{cases}$$

Proof: Let $\ell_0 \in L$, and by symmetry, $H(S_M^{\ell_0} \mid W_V, W_Q)$ is same for every $\ell_0 \in L$. Define $\tilde{V} = V \setminus \{\ell_0\}$. Then we have

$$\begin{aligned} H(S_M^L \mid W_V, W_Q) &\leq \ell H(S_M^{\ell_0} \mid W_V, W_Q) \\ &= \ell \left\{ H(S_M^{\ell_0}, W_{\ell_0} \mid W_{\tilde{V}}, W_Q) - H(W_{\ell_0} \mid W_{\tilde{V}}, W_Q) \right\} \\ &= \ell \left\{ H(S_M^{\ell_0} \mid W_{\tilde{V}}, W_Q) + H(W_{\ell_0} \mid S_M^{\ell_0}, W_{\tilde{V}}, W_Q) \right. \\ &\quad \left. - H(W_{\ell_0} \mid W_{\tilde{V}}, W_Q) \right\} \end{aligned}$$

By substituting bounds, we obtain for the case $v - 1 + q > \mu$

$$\begin{aligned} H(S_M^L \mid W_V, W_Q) &\leq \ell \{ m\beta + (d - v + 1 - q - m)\beta \\ &\quad -(d - v + 1 - q)\beta + \omega_{v-1+q} \} \\ &= \ell \omega_{v-1+q} , \end{aligned}$$

and for the case $v - 1 + q = \mu$,

$$\begin{aligned} H(S_M^L \mid W_L, W_Q) &\leq \ell \{ m\beta + (d - v + 1 - q - m)\beta - (d - v + 1 - q)\beta \\ &\quad +\theta + \omega_{v-1+q} \} \\ &= \ell\theta + \ell\omega_{v-1+q} . \end{aligned}$$

□

We remark here that in Duursma (2014) the quantity $H(S_M^L)$ is considered for obtaining a bound on ER file size. Our approach here is different in the sense that we estimate $H(S_M^L)$ in terms of $\{\omega_i\}_{i=0}^{k-1}$. The second term in (25) can also be easily estimated in terms of $\{\gamma_i, \omega_i\}_{i=0}^{k-1}$:

$$\begin{aligned} I(S_M^L : W_V \mid W_Q) &\leq I(W_M : W_V \mid W_Q) \\ &= H(W_M \mid W_Q) - H(W_M \mid W_{Q \cup V}) \\ &= \left[\sum_{i=q}^{q+m-1} (\gamma_i - \omega_i) \right] - \left[\sum_{i=q+v}^{q+v+m-1} (\gamma_i - \omega_i) \right] . \end{aligned} \tag{26}$$

The Lemma 3.2 along with (26) allows us to bound $H(S_M^L \mid W_Q)$ from above given an operating point $\alpha = (d - \mu)\beta - \theta$. Calculations for the particular case of $q = 0, m = 1$ taking values for v in $\{\mu + 1, \mu + 2\}$ result in the following corollary.

Corollary 3.3: *Let $\alpha = (d - \mu)\beta - \theta$. Then for $m \notin L$ and $\ell = |L|$, we have*

$$H(S_m^L) \leq \beta + (\ell - 1)\theta + (\ell - 1)\omega_\mu + (\omega_\mu + \omega_{\mu+1}), \quad 2 \leq \ell \leq \mu + 1 \tag{27}$$

$$H(S_m^L) \leq 2\beta - \theta + (\ell - 1)\omega_{\mu+1} + (\omega_{\mu+1+\omega_{\mu+2}}), \quad 2 \leq \ell \leq \mu + 2. \tag{28}$$

3.3 The bound on ER file size

In this section, we make use of Lemma 3.1 and Corollary 3.3 to derive an upper bound on the file size B of an ER code. This will also translate to an outer bound for the ER trade-off.

Theorem 3.4: *Let B denotes the file size of a ER regenerating code with full parameter set $\mathcal{P}_f = \{(n,k,d),(\alpha,\beta)\}$. Let $\alpha = (d-\mu)\beta - \theta$. Then the ER file size B is upper bounded by:*

1 *For $\mu = 0,\ 0 < \theta < \beta$,*

$$B \leq \hat{B} - \epsilon_1$$

2 *For $\mu \in \{1,2,\ldots,k-3\},\ 0 \leq \theta < \beta$,*

$$B \leq \hat{B} - \max\{\epsilon_0, \epsilon_1\}$$

3 *For $\mu = k-2,\ 0 \leq \theta < \left(\frac{d-k+1}{d-k+2}\right)\beta$,*

$$B \leq \hat{B} - \epsilon_0,$$

where ϵ_0 and ϵ_1 are as given in Table 1.

Table 1 Lower Bounds on the quantity $\hat{B} - B$

Regime of (μ,θ)	*Lower bounds* ϵ_0 , ϵ_1 *on* $\epsilon = \hat{B} - B$
	Let $r_0 = \left\lfloor \frac{k-\mu}{\mu+1} \right\rfloor$
$\mu \in \{1,2,\ldots,k-2\}$ for all θ For $\mu = k-2,\ \theta < \frac{d-k+1}{d-k+2}\beta$	$\epsilon_0 = \begin{cases} \frac{(d-k+1)(k-\mu-1)(\beta-\theta)\ -\ \theta}{(d-k+1)(k-\mu)\ +\ 1}, & k-\mu < \mu+1. \\ \frac{\left(d-\frac{(\mu+1)(r_0+3)}{2}+2\right)r_0\mu(\beta-\theta)\ -\ \theta}{\left(d-\frac{(\mu+1)(r_0+3)}{2}+2\right)r_0(\mu+1)\ +\ 1}, & k-\mu \geq \mu+1. \end{cases}$
	Let $r_1 = \left\lfloor \frac{k-\mu-1}{\mu+2} \right\rfloor$
$\mu \in \{0,1,\ldots,k-3\}$ for all θ For $\mu = 0,\ \theta \neq 0$	$\epsilon_1 = \begin{cases} \frac{(d-k+1)[(k-\mu-3)\beta\ +\ \theta]}{(d-k+1)(k-\mu-1)\ +\ 1}, & k-\mu-1 < \mu+2. \\ \frac{\left(d-\frac{(\mu+2)(r_1+3)}{2}+2\right)r_1[\mu\beta\ +\ \theta]}{\left(d-\frac{(\mu+2)(r_1+3)}{2}+2\right)r_1(\mu+2)\ +\ 1}, & k-\mu-1 \geq \mu+2. \end{cases}$

Proof: The proof is relegated to the Appendix. □

Corollary 3.5: *When $k \geq 3$, the normalised ER trade-off is strictly away from the normalised FR trade-off for all normalised operating points $(\bar{\alpha},\bar{\beta})$ with $\bar{\alpha} = (d-\mu)\bar{\beta} - \nu\bar{\beta}$ such that (μ,ν) falls in the range $(\mu = 0,\ 0 < \nu < 1)$, $(\mu \in \{1,2,\ldots,k-3\}, 0 \leq \nu < 1)$ or $(\mu = k-2, 0 \leq \nu < \frac{d-k+1}{d-k+2})$.*

Proof: We will show that the upper bound on the file size given in 3.4 satisfies the criterion in (6). Let

$$\delta = \begin{cases} \epsilon_1 & \mu = 0, \theta \neq 0 \\ \max\{\epsilon_0, \epsilon_1\} & \mu \in \{1, 2, \ldots, k-3\} \\ \epsilon_0 & \mu = k-2, \theta < \frac{d-k+1}{d-k+2}\beta \end{cases} \tag{29}$$

Let α be related to β as $\alpha = (d-\mu)\beta - \theta = (d-\mu)\beta - \nu \cdot \beta, \ \ \nu \in [0, 1)$ by a fixed pair (μ, ν) that falls in the range given. Then for a code with the file size B,

$$\begin{aligned} \frac{\beta}{B} &\geq \frac{\beta}{\hat{B} - \delta}, \quad \text{(using Theorem 3.4)} \\ &= \frac{\beta}{\hat{B}} \cdot \frac{1}{1 - \left(\frac{\delta}{\hat{B}}\right)} \\ &= \frac{\beta}{\hat{B}} \cdot \frac{1}{1 - \left(\frac{\delta}{\beta \sum_{i=0}^{k-1} \min\{(d-\mu)-\nu, (d-i)\}}\right)} \\ &\geq \frac{\beta}{\hat{B}} + \delta_0, \end{aligned}$$

for some $\delta_0 > 0$, determined by the constants $\frac{\epsilon_0}{\beta}$ and $\frac{\epsilon_1}{\beta}$. It can be seen that $\frac{\epsilon_0}{\beta}$ and $\frac{\epsilon_1}{\beta}$ are independent of β, B and dependent only on the fixed values of μ, ν, k and d. This completes the proof. □

4 Discussion on various known upper bounds on ER file size

In this section, we briefly review the results from Tian (2014), Tian (2015), Duursma (2014), Duursma (2015), Mohajer and Tandon (2015), all of them involving upper bounds on the ER file size. While bounds provided in Duursma (2014, 2015) are not explicit, those presented in Tian (2014), Tian (2015), Mohajer and Tandon (2015) have got the form of explicit algebraic expressions.

4.1 Review of the bounds in Tian (2014), Tian (2015)

In Tian (2014), Tian characterised the optimal ER file size for the case of $(n, k, d) = (4, 3, 3)$. This was the first result establishing a non-vanishing gap for ER file size in comparison with the optimal FR file size. For the case of $(n, k, d) = (4, 3, 3)$, there are four bounds

$$B \leq B_q, \ q = 0, 1, 2, 3, \tag{30}$$

that follow from considering all possible trapezoidal configurations. For a given operating point $\alpha = (d-\mu)\beta - \theta$, one of these bounds dominate over the others. By suitably modifying the information theory inequality prover software(see ITIP (2016), Yeung (1997)), Tian was able to characterise a bound

$$3B \leq 4\alpha + 6\beta,$$

that is different from (30). Recently in Tian (2015), Tian made further progress with his computational approach to provide an upper bound on the ER file size for $(n, k, d) = (5, 4, 4)$. In both the cases of $(4, 3, 3)$ and $(5, 4, 4)$, the bounds are achieved using the well-known class of layered codes in Tian et al. (2015). These results are made part of the online collection of "Solutions of Computed Information Theoretic Limits (SCITL)" hosted at SCITL (2016).

4.2 Review of the bound in Duursma (2014)

In the second of two bounds presented in Duursma (2014), Duursma considers the region Z_q in a trapezoidal configuration (Q, Z_q) and tiles the region using rectangular blocks corresponding to random variables S_M^L, with $m := |M|$, $\ell := |L|$. This approach is an extension of the tiling-with-line-segments method, introduced in Sasidharan, Senthoor and Kumar (2014) and used in the present paper in the derivation of Theorem 3.4. Duursma extends the upper bound given in Sasidharan, Senthoor and Kumar (2014) to obtain a bound on $H(S_M^L)$, involving entropy expressions having a negative coefficient. Various carefully chosen alternative bounds on B are used to cancel out these negative terms leading to the improved bound:

$$B + \sum_{(M,L)\in\mathcal{M}} \ell B \leq B_q + \sum_{(M,L)\in\mathcal{M}} (B_{r+m-1} + (\ell - 1)(B_{r+m-2} - \beta)), \tag{31}$$

where $m := |M|$, $\ell := |L|$ and $r \geq \ell$ for every choice of (M, L). In (31), $\mathcal{M}$ denotes a set of possible tilings of the trapezoidal region Z_q using rectangular blocks and B_q remains as defined in Section 2.2. To obtain the best possible explicit bound, one would then proceed to minimise this expression over all possible tilings. It can easily be checked that the bound in (31) is tighter than the one given in (17), by a difference of at most β.

4.3 Review of the bound in Duursma (2015)

In Duursma (2015), Duursma augments the set of node random variables $\{W_i\}_{i=1}^k$ with another set of random variables W'_{k+u} for $1 \leq u \leq \nu$ satisfying

$$H(S_i^j | W'_{k+u}) \leq H(S_i^j | W_{[i+1,k]} W'_{[k+1,k+u-1]}) \text{ for } 1 \leq i < j \leq p, \tag{32}$$

for a given value of p, $0 \leq p \leq k$. The bound on file size B is obtained as

$$(\nu + 1)B \leq (\nu + 1)B_{k-p} + \sum_{u=1}^{\nu} \left(H(W'_{k+u}) - \binom{p}{2}\beta \right),$$

where B_{k-p} is as defined earlier. This results, in general, in an implicit bound as it is not clear how the random variables $\{W'_{k+u}\}_{u=1}^{\nu}$ can be constructed. However, restricting to linear codes, the author is able to construct the $\{W'_{k+u}\}$ resulting in an explicit bound for every parameter set (n, k, d). This bound matches with the one proved in Prakash and Krishnan (2015) for the special case of $(k + 1, k, k)$-linear ER codes.

4.4 Review of the bound in Mohajer and Tandon (2015)

In this section, we give a complete description[2] of the proof of the bound due to Mohajer et al. (2015). We start with recalling the bound given in (15) for a trapezoidal configuration (Q, Z_q),

$$\begin{aligned} B &\leq H(W_Q) + H(Z_q \mid W_Q) \\ &= H(W_Q) + H(X_q, S_R^P \mid W_Q), \end{aligned} \tag{33}$$

where the sets P, Q and R are as defined in Section 2.2. For convenience of notation, we modify the indexing of elements in sets P, Q and R, without making any change in their respective sizes. Thus the sets Q, P, R are defined by the same value of q, and hence the bound in (15) remains unaltered. With respect to the modified indexing, $Q = \{-1, -2, \ldots, -q\}$, $P = \{1, 2, \ldots, p := k - q\}$ and $R = \{k+1, k+2, \ldots, d+1\}$. Continuing from (33), we write

$$\begin{aligned} B &\leq H(W_Q) + H(X_q, S_R^P \mid W_Q) \\ &\leq q\alpha + \underbrace{\sum_{i=1}^{p} H\left(S_i^{[i-1]} \mid W_Q\right)}_{\mathcal{R}(p)} + H\left(S_R^P \mid W_Q\right). \end{aligned} \tag{34}$$

Instead of invoking the union bound as done in (16), the entropic term $\mathcal{R}(p) := \sum_{i=1}^{p} H\left(S_i^{[i-1]} | W_Q\right)$ is canceled out with the help of other expressions for B. In (35) that follows, the authors over-count conditional node entropy $H(W_i \mid W_{[i-1]})$ as α, and later subtract out the error introduced in doing so. This leads to a different expression for B:

$$\begin{aligned} B &= H(W_Q) + \sum_{i=1}^{p} H(W_i \mid W_Q) - \sum_{i=1}^{p} I(W_i; W_{[i-1]} \mid W_Q) \\ &\leq q\alpha + p\alpha - \sum_{i=1}^{p} I(S_i^{[i-1]}; S_{[i-1]}^{i} \mid W_Q) \\ &= k\alpha - \underbrace{\sum_{i=1}^{p} H\left(S_i^{[i-1]} \mid W_Q\right)}_{\mathcal{R}(p)} - \underbrace{\sum_{i=1}^{p} H\left(S_{[i-1]}^{i} \mid W_Q\right)}_{\mathcal{C}(p)} \\ &\quad + \underbrace{\sum_{i=1}^{p} H\left(S_{[i-1]}^{i}, S_i^{[i-1]} \mid W_Q\right)}_{\mathcal{J}(p)}. \end{aligned} \tag{35}$$

While (35) allows cancellation of $\mathcal{R}(p)$ in (34), it introduces new entropic terms $\mathcal{C}(p)$ and $\mathcal{J}(p)$. A third expression for B is obtained by over-counting entropy of columns in the trapezoidal region Z_q using union bound and then subtracting out the error introduced in doing so.

$$B \leq H(W_Q, S_{[d+1]}^{P})$$

$$\leq q\alpha + \sum_{i=1}^{p} H(S^i_{[d+1]}|W_Q) - \sum_{i=1}^{p} I\left(S^i_{[d+1]}; S^{[i-1]}_{[d+1]} \mid W_Q\right)$$
$$\leq q\alpha + \sum_{i=1}^{p} H\left(S^i_{[i-1]} \mid W_Q\right) + \sum_{i=1}^{p} H\left(S^i_{[i+1\ d+1]} \mid W_Q\right)$$
$$- \sum_{i=1}^{p} I\left(S^i_{[d+1]}; S^{[i-1]}_{[d+1]} \mid W_Q\right). \tag{36}$$

The following straightforward lemma is useful in producing a lower bound for $I\left(S^i_{[d+1]}; S^{[i-1]}_{[d+1]} \mid W_Q\right)$.

Lemma 4.1: *Let X, Y, Z, U be random variables such that $Z = f_1(X, U) = f_2(Y, U)$ for some deterministic functions f_1, f_2. Then*

$$I(X : Y \mid U) \geq H(Z \mid U).$$

By invoking Lemma 4.1 along with identifying $Z = \{S^i_{[i-1]}, S^{[i-1]}_i\}$, $X = S^i_{[d+1]}$, $Y = S^{[i-1]}_{[d+1]}$ and $U = W_Q$, it follows that

$$I\left(S^i_{[d+1]}; S^{[i-1]}_{[d+1]}|W_Q\right) \geq H\left(S^i_{[i-1]}, S^{[i-1]}_i|W_Q\right), \tag{37}$$

and substituting (37) back in (36), the authors obtain the bound

$$B \leq q\alpha + \underbrace{\sum_{i=1}^{p} H\left(S^i_{[i-1]} \mid W_Q\right)}_{\mathcal{C}(p)} + \sum_{i=1}^{p} H\left(S^i_{[i+1\ d+1]} \mid W_Q\right)$$
$$\underbrace{- \sum_{i=1}^{p} H\left(S^i_{[i-1]}, S^{[i-1]}_i \mid W_Q\right)}_{\mathcal{J}(p)}. \tag{38}$$

Summation of (34), (35) and (38) eliminates $\mathcal{R}(p), \mathcal{C}(p)$ and $\mathcal{J}(p)$ and results in the bound:

$$3B \leq (3k - 2p)\alpha + \sum_{i=1}^{p} H\left(S^i_{[i+1\ d+1]} \mid W_Q\right) + H\left(S^P_R \mid W_Q\right). \tag{39}$$

By applying union bound, it follows that

$$B \leq \min_{0 \leq p \leq k} \frac{(3k - 2p)\alpha + \frac{p(2(d-k)+p+1)\beta}{2} + (d - k + 1)\min\{\alpha, p\beta\}}{3}. \tag{40}$$

To our knowledge, the bound in (40) due to Mohajer et al. remains the best known upper bound on ER file size in the region away from the MSR point.

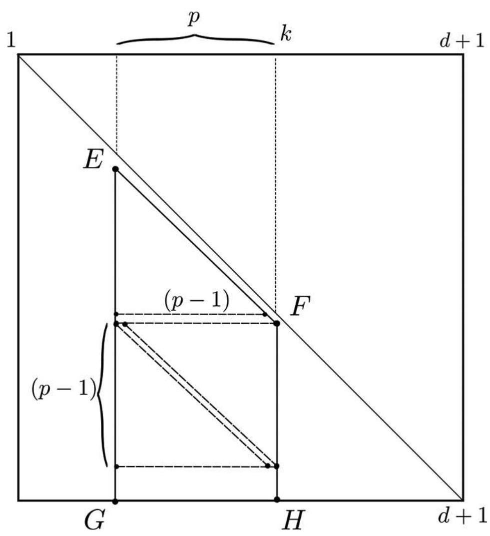
5 An improved upper bound on ER file size

In this section, we first propose an improvement over the bound in Mohajer and Tandon (2015), that is described in Section 4.4. The authors of Mohajer and Tandon (2015) apply union bound on the last two terms in (39) to obtain the final bound. But it is possible to avoid the union bound for the term $H\left(S_R^P \mid W_Q\right)$ when $d >> k$.

Figure 9 illustrates the region S_R^P as it is viewed on the repair matrix. The rectangular region S_R^P, denoted by Γ, is of width p and height $(d-k+1)$. Let us write

$$d-k+1 = a(p-1)+b,\ 0 \le b < (p-1).$$

Figure 9 The splitting up of the region corresponding to S_R^P. In this example, $a = 1, b > 0$



Then Γ can be split into $(a+1)$ sub-rectangles $\Gamma_1, \Gamma_2, \ldots, \Gamma_{a+1}$ of equal width p, and $\Gamma_i, 1 \le i \le a$ have the same height $(p-1)$. The last sub-rectangle Γ_{a+1} is of height b, and it vanishes in the case $b = 0$. Each rectangle $\Gamma_i, 1 \le i \le a$ is further split into two isosceles right triangles Γ_{i1}, Γ_{i2} of base $(p-1)$ as illustrated in Figure 9. By symmetry, we can write

$$\begin{aligned} H(S_P^R|W_Q) &\le aH\left(\Gamma_1|W_Q\right) + H(\Gamma_{a+1}|W_Q) \\ &\le 2aH\left(\Gamma_{11}|W_Q\right) + H(\Gamma_{a+1}|W_Q) \\ &\le 2a\sum_{i=1}^{p} H\left(S_i^{[i-1]}|W_Q\right) + b\min\{\alpha, p\beta\}. \end{aligned} \tag{41}$$

We improve upon the the bound in (34) by substituting (41) and obtain that

$$B \le q\alpha + (1+2a)\sum_{i=1}^{p} H\left(S_i^{[i-1]}|W_Q\right) + b\min\{\alpha, p\beta\}. \tag{42}$$

This modification only affects the coefficient of the term $\mathcal{R}(p)$. The cancellation of the term $\mathcal{R}(p)$ is possible by appropriately scaling the bounds in (35) and (38). This results in an improved bound whenever $a \geq 1$ and is stated in the theorem below. We refer to this bound as the *improved Mohajer–Tandon bound*.

Theorem 5.1: *The ER file size B of regenerating code with full parameter set $\mathcal{P}_f = \{(n,k,d),(\alpha,\beta)\}$ is bounded by*

$$B \leq \min_{0 \leq p \leq k} \frac{\alpha(2(k-p)(1+a)+k(1+2a)) + b\min\{\alpha, p\beta\} + \frac{(1+2a)p(2(d-k)+p+1)\beta}{2}}{3+4a}, \quad (43)$$

where $d-k+1 = a(p-1)+b$ and $0 \leq b < (p-1)$.

We remark that the improved Mohajer-Tandon bound relies upon the same techniques introduced by Mohajer et al. of coming up with various expressions for B allowing one to cancel out entropic terms that are otherwise difficult to estimate. Our incremental contribution is limited to identifying the symmetry in certain entropic terms as seen in the pictorial depiction on a repair matrix, and leveraging upon this symmetry to avoid certain union bounds. When $d > k$, the bound in Theorem 5.1 leads to an outer bound on normalised ER trade-off, that lies above the one due to (40). A principal result of the paper stated in Theorem 1.1 follows by combining both the Theorems 3.4 and 5.1.

6 A dual-code-based approach to bounding the ER file size for linear codes

In this section, we investigate the maximum possible ER file size under the restricted setting of linear regenerating codes. Let $\mathcal{C}_{\text{lin}}$ denotes a linear ER code with full parameter set $\mathcal{P}_f = \{(n,k,d),(\alpha,\beta)\}$. We will continue to use B to denote the file size. By linear, we mean that (a) the encoding mapping that converts the B message symbols to $n\alpha$ coded symbols is linear, (b) the mapping that converts the node data into repair data that is transmitted during the repair of a failed node is linear and furthermore, (c) the mappings that are involved during data collection from a set of k nodes and regeneration of a failed node using repair data from a set of d nodes are linear. A linear regenerating code can be viewed as a linear block-code with length $n\alpha$ over $\mathbb{F}$ such that every set of α symbols (taken in order without loss of generality) are bunched together to correspond to a node.

6.1 The parity-check matrix and its properties

Since $\mathcal{C}_{\text{lin}}$ is a linear code, we can associate a generator matrix to the code. Let G of size $(B \times n\alpha)$ denotes a generator matrix of $\mathcal{C}_{\text{lin}}$. Without loss of generality, we assume that the first α columns of G generate the contents of the first node, the second α columns of G generate the contents of the second node, and so on. The first α columns taken together will be referred to as the first thick column of G. Similarly, the second thick column consists of columns from $\alpha+1$ to 2α, and so on. Overall, we will have n thick columns in G. Let H denotes a parity-check matrix having size $(n\alpha - B) \times n\alpha$. The row-space of H is the dual code of $\mathcal{C}_{\text{lin}}$. The definition of thick columns directly carries over to H. For any set $S \subseteq [n]$, we write $H|_S$ to denote the restriction of H to the thick columns indexed by the set S. From definitions, we have that

$$B = \text{rank}(G) \ = \ n\alpha - \text{rank}(H). \quad (44)$$

By (44), it is sufficient to obtain a lower bound on $rank(H)$ to bound B from above. This is precisely the approach taken here.

In the following two lemmas, we will translate the properties of data collection and exact-repair as properties of the parity-check matrix H. We remark here that these observations are already made in Duursma (2014).

Lemma 6.1 (Data Collection): *Let H be a parity-check matrix of an ER linear regenerating code. Then* $\text{rank}\,(H|_S) = (n-k)\alpha$*, for any $S \subseteq [n]$ such that $|S| = n-k$.*

Proof: This is a restatement of Part (1) of Proposition 2.1 of Duursma (2014) and is equivalent to the data collection property. □

Lemma 6.2 (Exact Repair): *Assume that $d = n-1$. Then the row space of H of an ER linear regenerating code contains a collection of $n\alpha$ vectors that can be arranged as the rows of an $(n\alpha \times n\alpha)$ matrix H_{repair}, which can be written in the block-matrix form:*

$$H_{repair} = \left[\begin{array}{c|c|c|c} A_{1,1} & A_{1,2} & & A_{1,n} \\ \hline A_{2,1} & A_{2,2} & \ldots & A_{2,n} \\ \hline & & \vdots & \\ \hline A_{n,1} & A_{n,2} & & A_{n,n} \end{array}\right], \tag{45}$$

where $A_{i,i}$ is defined to be the identity matrix I_α of size α and $A_{i,j}$ denotes an $\alpha \times \alpha$ matrix such that rank $(A_{i,j}) \leq \beta, 1 \leq i, j \leq n, i \neq j$.

Proof: The first α rows of the form

$$\left[I_\alpha | A_{1,2} | \cdots | A_{1,n} \right]$$

can be obtained by the parity-check equations that are necessitated by the exact-repair requirement of the first node. In a similar manner, there must be parity-check equations that must allow repair of every node. These parity-check equations can be arranged to obtain the matrix H_{repair}. The requirements on the ranks of the sub-matrices A_{ij} follow from the definition of regenerating codes, and the fact that $d = n-1$. In fact, the proof is indicated in Part (2) of Proposition 2.1 of Duursma (2014). □

For the case of $d = k = n-1$, the matrix H_{repair} as given in Lemma 6.2 satisfies the condition given in Lemma 6.1, and therefore H_{repair} by itself defines an $(n, k = n-1, d = n-1)(\alpha, \beta)$ regenerating code. Since $rank(H) \geq rank(H_{\text{repair}})$, and our interest lies in regenerating codes having maximal file size, we will assume that $H = H_{\text{repair}}$ while deriving a lower bound on $rank(H)$ for the case of $d = k = n-1$.

6.2 A proof of FR bound For ER linear codes using dual code

In this section, we will present a simple proof of the FR bound (1) for ER linear regenerating codes. Our proof of Theorem 1.2 will be built up on the proof of (1) that is presented here.

As earlier, let $\mathcal{C}_{\text{lin}}$ denotes an $(n, k, d = n-1)(\alpha, \beta)$ linear regenerating code, and let the matrix H generate the dual code of $\mathcal{C}$. The key idea of the proof is to obtain a lower bound on the column rank of the matrix H. We use the notation $\rho(.)$ to denote the rank of a matrix. Let us define the quantities $\delta_j, 1 \leq j \leq n$ as follows:

$$\delta_1 = \rho(H|_{[1]}), \tag{46}$$
$$\delta_j = \rho(H|_{[j]}) - \rho(H|_{[j-1]}),\ 2 \leq j \leq n. \tag{47}$$

Next, we make the following claims:

$$\delta_j = \rho(A_{j,j}) \tag{48}$$
$$= \alpha,\ \ 1 \leq j \leq n-k \tag{49}$$
$$\delta_j \geq (\alpha - (j-1)\beta)^+,\ n-k+1 \leq j \leq n. \tag{50}$$

Here we have set $a^+ := \max(a, 0)$. The first claim (48) follows from the fact that any $n-k$ thick columns of H has rank given by $(n-k)\alpha$ as required by Lemma 6.1. To show the second claim (50), one needs to first focus on the j^{th} thick row of H_{repair}. By j^{th} thick row, we mean the set of rows starting from $(j-1)\alpha + 1$ and reaching up to $j\alpha$ of H_{repair}. Next observe that

$$\delta_j \geq \left(\rho(A_{j,j}) - \sum_{\ell=1}^{j-1} \rho(A_{j,\ell})\right)^+ \tag{51}$$
$$= \left(\rho(I_\alpha) - \sum_{\ell=1}^{j-1} \rho(A_{j,\ell})\right)^+$$
$$\geq (\alpha - (j-1)\beta)^+,\ n-k+1 \leq j \leq n, \tag{52}$$

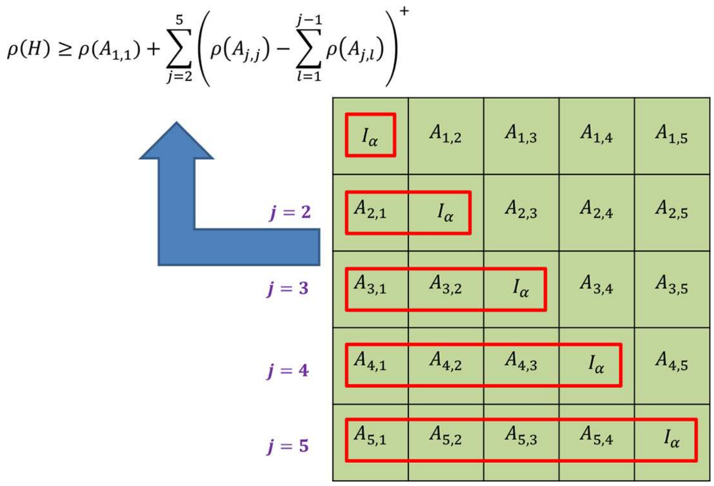
where (52) holds true since $\rho(A_{i,j}) \leq \beta$ by Lemma 6.2. Thus we have shown (50). Next, invoking (48) and (52), we bound the column-rank of H from below as:

$$\text{rank}(H) = \sum_{j=1}^{n} \delta_j \tag{53}$$
$$\geq (n-k)\alpha + \sum_{j=n-k+1}^{n} (\alpha - (j-1)\beta)^+. \tag{54}$$

An illustration of arriving at (51) and (54) is given in Figure 10. Consequently, it follows that

$$B = n\alpha - \rho(H) \tag{55}$$
$$\leq n\alpha - (n-k)\alpha - \sum_{j=n-k+1}^{n} (\alpha - (j-1)\beta)^+ \tag{56}$$
$$= \sum_{j=0}^{k-1} \min(\alpha, (n-1-j)\beta). \tag{57}$$

Figure 10 A lower bound on $\rho(H)$, for the case of $(n = 5, k = 4, d = 4)$. Each term indexed by j in the summation correspond to a lower bound on the incremental rank δ_j. This bound is obtained by looking at the sub-matrices in j^{th} thick row (see online version for colours)



For $d < n - 1$, the proof follows by first puncturing the code on any $(n - d - 1)$ nodes to form a $(n' = d + 1, k, d)$ ER linear regenerating code and then invoking the above analysis on the resultant new code. The way we express incremental ranks $\{\delta_j\}$ in (48) and (51) will turn out to be useful in deriving a strong upper bound on the file size of linear ER codes in Sections 7 and 8.

7 An upper bound on the file size of linear ER codes for the case $(n = 5, k = 4, d = 4)$

In this section, we obtain a new upper bound on the file size of a linear ER code for parameters $(n = 5, k = 4, d = 4)$. Taken along with the achievability using layered codes (see Section 9.2), we characterise the trade-off for this case. As mentioned earlier, our technique is to lower bound the rank of the parity-check matrix H, leading to an upper bound on the file size by (44). The lower bound on $\rho(H)$ that we derive here is in general tighter than what is obtained in (54). The principal result of this section is stated in Theorem 7.1 below. Most of the ideas that are developed in the proof of Theorem 7.1 will later be used in the next section to prove a general result for the case of $(n, k = n - 1, d = n - 1)$.

Theorem 7.1: *Consider an ER linear regenerating code $\mathcal{C}_{lin}$ with full parameter set $\{(n = 5, k = 4, d = 4), (\alpha, \beta)\}$. Let H denotes a parity-check matrix of $\mathcal{C}_{lin}$. Then*

$$\rho(H) \geq \begin{cases} \left\lceil \frac{10(\alpha-\beta)}{3} \right\rceil, \ 2\beta \leq \alpha \leq 4\beta \\ \left\lceil \frac{15\alpha-10\beta}{6} \right\rceil, \ \frac{4}{3}\beta \leq \alpha \leq 2\beta \\ 2\alpha - \beta, \ \beta \leq \alpha \leq \frac{4}{3}\beta \end{cases} \cdot \tag{58}$$

Note that $\alpha = \beta$ and $\alpha = 4\beta$ correspond to the MSR and MBR points, respectively, for the case of $(n = 5, k = 4, d = 4)$. Next, we observe that for a fixed β, the bound given in (58) corresponds to a piecewise linear curve with α on the X-axis and $\rho(H)$ on the Y-axis. Non-linear ceiling operation $\lceil . \rceil$ is used in (58) to enforce integrality requirements on $\rho(H)$. However, it may be removed considering that $\rho(H)$ always takes integer values. We can view (58) as a combination of the following three inequalities without paying attention to the limited range of α:

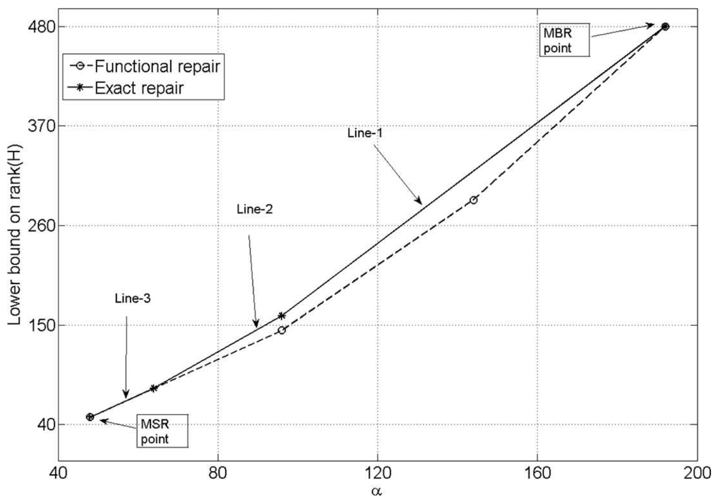
$$\rho(H) \geq \frac{10(\alpha - \beta)}{3} \tag{59}$$

$$\rho(H) \geq \frac{15\alpha - 10\beta}{6} \tag{60}$$

$$\rho(H) \geq 2\alpha - \beta. \tag{61}$$

Here (61) follows from (54) since $\alpha \geq \beta$ and $(\alpha - (j-1)\beta)^+ \geq 0$ for $3 \leq j \leq 5$. Therefore, we need to prove only the remaining two inequalities (59) and (60) to complete the proof of Theorem 7.1. We proceed to prove them by obtaining two lower bounds to the incremental thick-column-rank of H that are stronger than what is given in (52). To make this point clear upfront, a comparison of the bounds in (54) and (58) is shown in Figure 11.

Figure 11 Comparison of the lower bounds on $\rho(H)$ as function of α, for the case of $(n = 5, k = 4, d = 4)$ with $\beta = 48$. The dashed and the solid lines correspond to the cases of functional and exact repairs, respectively. See (54) and (58) for the corresponding equations. Here, lines 1, 2 and 3 are given by (59), (60) and (61), respectively



7.1 *Proof of Theorem 7.1*

We begin with setting up some notation. For any matrix B over $\mathbb{F}$, we denote by $\mathcal{S}(B)$ the column space of B. Note that $\rho(B)$ is the same as the dimension of the vector space $\mathcal{S}(B)$. Next, we define $H^{(5)} = H_{\text{repair}}$, where H_{repair} is as defined in (45). Let the matrix $H_j^{(5)}$

denotes the j^{th} thick column of $H^{(5)}, 1 \leq j \leq 5$, i.e., $H^{(5)} = [H_1^{(5)}\ H_2^{(5)} H_3^{(5)}\ H_4^{(5)}\ H_5^{(5)}]$. Next, we define matrices $H_j^{(4)}, 2 \leq j \leq 5$ such that the columns of $H_j^{(4)}$ form a basis for the vector space $\mathcal{S}\left(H_j^{(5)}\right) \cap \mathcal{S}\left(H^{(5)}|_{[j-1]}\right)$. Next, we define $H^{(4)}$ as

$$H^{(4)} = [H_2^{(4)} H_3^{(4)}\ H_4^{(4)}\ H_5^{(4)}].$$

For convenience of notation, we have used $H_2^{(4)}$ to denote the first thick column of $H^{(4)}$. Similarly, $H^{(3)}$ is obtained from $H^{(4)}$, where columns of $H_j^{(3)}$ form a basis for $\mathcal{S}\left(H_j^{(4)}\right) \cap \mathcal{S}\left(H^{(4)}|_{\{2,\ldots,j-1\}}\right)$:

$$H^{(3)} = [H_3^{(3)}\ H_4^{(3)}\ H_5^{(3)}].$$

Let $A_{i,j}^{(\ell)}$ denotes the i^{th} thick row of $H_j^{(\ell)}$. An illustration of the block-matrix representations of $H^{(5)}, H^{(4)}$ and $H^{(3)}$ is given in Figure 12.

Figure 12 The matrices $H^{(5)}, H^{(4)}$ and $H^{(3)}$, and the associated block submatrix representations for the case $n = 5$. The matrix $H^{(5)} = H_{\text{repair}}$, $H^{(4)}$ is defined based on $H^{(5)}$, and $H^{(3)}$ is defined based on $H^{(4)}$

$$\underbrace{\begin{array}{ccccc} H_1^{(5)} & H_2^{(5)} & H_3^{(5)} & H_4^{(5)} & H_5^{(5)} \\ \left[\begin{array}{c|c|c|c|c} A_{1,1}^{(5)} & A_{1,2}^{(5)} & A_{1,3}^{(5)} & A_{1,4}^{(5)} & A_{1,5}^{(5)} \\ \hline A_{2,1}^{(5)} & A_{2,2}^{(5)} & A_{2,3}^{(5)} & A_{2,4}^{(5)} & A_{2,5}^{(5)} \\ \hline A_{3,1}^{(5)} & A_{3,2}^{(5)} & A_{3,3}^{(5)} & A_{3,4}^{(5)} & A_{3,5}^{(5)} \\ \hline A_{4,1}^{(5)} & A_{4,2}^{(5)} & A_{4,3}^{(5)} & A_{4,4}^{(5)} & A_{4,5}^{(5)} \\ \hline A_{5,1}^{(5)} & A_{5,2}^{(5)} & A_{5,3}^{(5)} & A_{5,4}^{(5)} & A_{5,5}^{(5)} \end{array}\right.\end{array}}_{H^{(5)}} \rightarrow \underbrace{\begin{array}{cccc} H_2^{(4)} & H_3^{(4)} & H_4^{(4)} & H_5^{(4)} \\ \left[\begin{array}{c|c|c|c} A_{1,2}^{(4)} & A_{1,3}^{(4)} & A_{1,4}^{(4)} & A_{1,5}^{(4)} \\ \hline A_{2,2}^{(4)} & A_{2,3}^{(4)} & A_{2,4}^{(4)} & A_{2,5}^{(4)} \\ \hline A_{3,2}^{(4)} & A_{3,3}^{(4)} & A_{3,4}^{(4)} & A_{3,5}^{(4)} \\ \hline A_{4,2}^{(4)} & A_{4,3}^{(4)} & A_{4,4}^{(4)} & A_{4,5}^{(4)} \\ \hline A_{5,2}^{(4)} & A_{5,3}^{(4)} & A_{5,4}^{(4)} & A_{5,5}^{(4)} \end{array}\right]\end{array}}_{H^{(4)}} \rightarrow \underbrace{\begin{array}{ccc} H_3^{(3)} & H_4^{(3)} & H_5^{(3)} \\ \left[\begin{array}{c|c|c} A_{1,3}^{(3)} & A_{1,4}^{(3)} & A_{1,5}^{(3)} \\ \hline A_{2,3}^{(3)} & A_{2,4}^{(3)} & A_{2,5}^{(3)} \\ \hline A_{3,3}^{(3)} & A_{3,4}^{(3)} & A_{3,5}^{(3)} \\ \hline A_{4,3}^{(3)} & A_{4,4}^{(3)} & A_{4,5}^{(3)} \\ \hline A_{5,3}^{(3)} & A_{5,4}^{(3)} & A_{5,5}^{(3)} \end{array}\right]\end{array}}_{H^{(3)}}$$

The key idea in the proof lies on the observation that $\rho(H^{(5)}) \geq \rho(H^{(4)}) \geq \rho(H^{(3)})$. We will show that (59) and (60) are necessary conditions, respectively, for $\rho(H^{(5)}) \geq \rho(H^{(4)})$ and $\rho(H^{(5)}) \geq \rho(H^{(4)}) \geq \rho(H^{(3)})$ to be true. The following remark underlines an important property of $\rho\left(A_{j,j}^{(\ell)}\right)$ preserved in the construction of $H_j^{(\ell)}$.

Remark 1: The sub-matrices $A_{j,j}^{(\ell)}, 3 \leq \ell \leq 5,\ \ 5 - \ell + 1 \leq j \leq 5$ have full column rank, and $\rho\left(A_{j,j}^{(\ell)}\right) = \rho\left(H_j^{(\ell)}\right)$.

7.2 Proof of (59)

We will be using the rank comparison $\rho(H^{(5)}) \geq \rho(H^{(4)})$ to prove (59). It follows from (48), (51) and (53) that

$$\rho\left(H^{(5)}\right) \geq \rho\left(A_{1,1}^{(5)}\right) + \sum_{j=2}^{5}\left\{\left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1}\rho\left(A_{j,\ell}^{(5)}\right)\right)^{+}\right\}. \tag{62}$$

We introduce slack variables $\{\alpha_j, 2 \leq j \leq 5\}$ that take non-negative integer values to convert (51) into equalities, i.e.,

$$\delta_j = \left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1}\rho\left(A_{j,\ell}^{(5)}\right)\right)^{+} + \alpha_j,\ 2 \leq j \leq 5. \tag{63}$$

Hence, using (53) we have:

$$\rho\left(H^{(5)}\right) = \rho\left(A_{1,1}^{(5)}\right) + \sum_{j=2}^{5}\left\{\left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1}\rho\left(A_{j,\ell}^{(5)}\right)\right)^{+} + \alpha_j\right\}. \tag{64}$$

$\rho\left(H^{(4)}\right)$ can be bounded from below quite similar to (62) (see Remark 1 also) to obtain

$$\rho\left(H^{(4)}\right) \geq \rho\left(A_{2,2}^{(4)}\right) + \sum_{j=3}^{5}\left\{\left(\rho\left(A_{j,j}^{(4)}\right) - \sum_{\ell=2}^{j-1}\rho\left(A_{j,\ell}^{(4)}\right)\right)^{+}\right\}. \tag{65}$$

Our aim at first is to find a lower bound for $\sum_{j=2}^{5}\alpha_j$. The analysis in Section 6.2 in fact works with the trivial lower bound $\sum_{j=2}^{5}\alpha_j \geq 0$. But here, we substitute (64) and (65) in

$$\rho(H^{(5)}) \geq \rho(H^{(4)})$$

to obtain a much tighter lower bound for $\sum_{j=2}^{5}\alpha_j$. Using this tighter bound in (64), we will obtain a lower bound for $\rho\left(H^{(5)}\right)$ in terms of $\{\rho\left(A_{i,j}^{(5)}\right), \rho\left(A_{i,j}^{(4)}\right)\}$. We know that the terms $\{\rho\left(A_{i,j}^{(5)}\right)\}$ can be expressed in terms of α and β. In the following Lemma 7.2, we show how $\left\{\rho\left(A_{i,j}^{(4)}\right)\right\}$ can be expressed in terms of $\left\{\rho\left(A_{i,j}^{(5)}\right)\right\}$. Finally, all the terms involve $\{\rho\left(A_{i,j}^{(5)}\right)\}$, and this will lead to the proof of (59).

Lemma 7.2: *The following statements hold:*

a $$\rho\left(A_{j,j}^{(4)}\right) = \rho\left(A_{j,j}^{(5)}\right) - \left\{\left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1}\rho\left(A_{j,\ell}^{(5)}\right)\right)^{+} + \alpha_j\right\},\ 2 \leq j \leq 5. \tag{66}$$

b $$\sum_{\ell=2}^{j-1} \rho\left(A_{j,\ell}^{(4)}\right) \le \sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right) - \rho\left(A_{j,j}^{(4)}\right),\ 3 \le j \le 5. \tag{67}$$

Proof: The proof is relegated to Appendix B. □

By making use of Lemma 7.2, we first obtain a lower bound on $\sum_{j=2}^{5} \alpha_j$, and subsequently a lower bound on $\rho\left(H^{(5)}\right)$ all in terms of $\{\rho\left(A_{i,j}^{(5)}\right)\}$:

$$\begin{aligned}\sum_{j=2}^{5} \alpha_j \ge \frac{1}{3}\Bigg\{ & -\rho\left(A_{1,1}^{(5)}\right) + \rho\left(A_{2,2}^{(5)}\right) + 2\sum_{j=3}^{5} \rho\left(A_{j,j}^{(5)}\right) - \\ & \Bigg[2\left(\rho\left(A_{2,2}^{(5)}\right) - \rho\left(A_{2,1}^{(5)}\right)\right)^{+} + 3\sum_{j=3}^{5}\left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right)\right)^{+} \\ & + \sum_{j=3}^{5}\sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right)\Bigg]\Bigg\} \end{aligned} \tag{68}$$

$$\rho\left(H^{(5)}\right) \ge \frac{1}{3}\left\{2\sum_{j=1}^{5} \rho\left(A_{j,j}^{(5)}\right) - \sum_{j=2}^{5}\sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right)\right\}. \tag{69}$$

Finally, we apply $\rho\left(A_{j,j}^{(5)}\right) = \alpha, 1 \le j \le 5$ and $\rho\left(A_{i,j}^{(5)}\right) \le \beta, 1 \le i, j \le 5,\ i \ne j$ to complete the proof of (59).

7.3 *Proof of* (60)

While proving (59), we leveraged upon the inequality

$$\rho(H^{(5)}) \ge \rho(H^{(4)}).$$

Here, we will make use of the chain

$$\rho(H^{(5)}) \ge \rho(H^{(4)}) \ \ge\ \rho(H^{(3)}),$$

to prove (60). First, we consider $\rho(H^{(4)}) \ge \rho(H^{(3)})$ and obtain a lower bound on $\rho(H^{(4)})$. This is carried out precisely the same way as how we obtained the lower bound (69) on $\rho(H^{(5)})$. The only change required will be to adapt Lemma 7.2 to express $\{A_{i,j}^{(4)}\}$ in terms of $\{A_{i,j}^{(3)}\}$. Thus we obtain that

$$\rho\left(H^{(4)}\right) \ge \frac{1}{3}\left\{2\sum_{j=2}^{5} \rho\left(A_{j,j}^{(4)}\right) - \sum_{j=3}^{5}\sum_{\ell=2}^{j-1} \rho\left(A_{j,\ell}^{(4)}\right)\right\}. \tag{70}$$

Observe that (70) is same as (69) except for that $\{A_{i,j}^{(5)}\}$ are replaced with $\{A_{i,j}^{(4)}\}$. The limits of the summation are also modified accordingly.

We next consider the inequality $\rho(H^{(5)}) \geq \rho(H^{(4)})$ where $\rho(H^{(4)})$ is lower bounded as in (70) and $\rho(H^{(5)})$ is equated using (64). It follows that

$$\begin{aligned} \rho\left(A_{1,1}^{(5)}\right) + \sum_{j=2}^{5} \left\{ \left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right) \right)^{+} + \alpha_j \right\} \\ \geq \frac{1}{3} \left\{ 2\sum_{j=2}^{5} \rho\left(A_{j,j}^{(4)}\right) - \sum_{j=3}^{5}\sum_{\ell=2}^{j-1} \rho\left(A_{j,\ell}^{(4)}\right) \right\}. \end{aligned} \tag{71}$$

After invoking Lemma 7.2, we obtain the lower bound:

$$\begin{aligned} \sum_{j=2}^{5} \alpha_j \geq \frac{1}{6} \Bigg\{ -3\rho\left(A_{1,1}^{(5)}\right) + 3\sum_{j=2}^{5} \rho\left(A_{j,j}^{(5)}\right) - \\ \left[6\sum_{j=2}^{5} \left(\rho\left(A_{j,j}^{(5)}\right) - \sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right) \right)^{+} + \sum_{j=2}^{5}\sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right) \right] \Bigg\}. \end{aligned} \tag{72}$$

Substituting (72) back in (64), we obtain the following lower bound on $\rho(H^{(5)})$:

$$\rho\left(H^{(5)}\right) \geq \frac{1}{6} \left\{ 3\sum_{j=1}^{5} \rho\left(A_{j,j}^{(5)}\right) - \sum_{j=2}^{5}\sum_{\ell=1}^{j-1} \rho\left(A_{j,\ell}^{(5)}\right) \right\}. \tag{73}$$

Finally, we apply $\rho\left(A_{j,j}^{(5)}\right) = \alpha, 1 \leq j \leq 5$ and $\rho\left(A_{i,j}^{(5)}\right) \leq \beta, 1 \leq i, j \leq 5,\ i \neq j$ on (73) to complete the proof of (60).

8 An upper bound on the file size of linear ER codes for general $(n, k = n-1, d = n-1)$

In this section, we generalise the result proved for $(n = 5, k = 4, d = 4)$ in Section 7 to $(n, k = n-1, d = n-1)$. We will only provide a sketch of the proofs, as the techniques remain the same as those presented in Section 7 (see Prakash and Nikhil Krishnan (2015) for details). Again, the upper bound on the file size is a direct corollary of a lower bound on rank(H) and the bound is achievable using layered codes (see Section 9.2). In the following theorem, a lower bound on rank(H) is established.

Theorem 8.1: *Consider an ER linear regenerating code $\mathcal{C}_{lin}$ with full parameter set $\{(n, k = n-1, d = n-1), (\alpha, \beta)\}$ with $n \geq 4$. Let H denotes a parity-check matrix of $\mathcal{C}_{lin}$. Then*

$$rank(H) \geq \begin{cases} \left\lceil \frac{2rn\alpha - n(n-1)\beta}{r^2+r} \right\rceil, & \frac{d\beta}{r} \leq \alpha \leq \frac{d\beta}{r-1},\ \ 2 \leq r \leq n-2 \\ 2\alpha - \beta, & \frac{d\beta}{n-1} \leq \alpha \leq \frac{d\beta}{n-2} \end{cases}. \tag{74}$$

The corresponding Theorem 7.1 for $(n = 5, k = 4, d = 4)$ established that *rank*(H) is lower bounded by a piecewise linear curve determined by 3 inequalities. Here, we show such a behaviour exists in general, i.e., rank(H) can be lower bounded by a piecewise linear curve determined by $(n - 2)$ inequalities. The last inequality

$$\text{rank}(H) \geq 2\alpha - \beta, \tag{75}$$

is already established by (54), since $\alpha \geq \beta$ and $(\alpha - (j-1)\beta)^+ \geq 0$ for $3 \leq j \leq n$. Therefore to complete the proof, it remains to prove the following $(n - 3)$ bounds on *rank*(H), ignoring the range of α:

$$\text{rank}(H) \geq \frac{2rn\alpha - n(n-1)\beta}{r^2 + r}, \tag{76}$$

parameterised by $2 \leq r \leq n - 2$. We will set up some notations, and introduce a key lemma that are essential in describing a sketch of the proof.

8.1 Notations and a key lemma

8.1.1 The matrices $\{H^{(t)},\ 3 \leq t \leq n\}$

For any matrix M over $\mathbb{F}$, we carry over the notation $\rho(M), \mathcal{S}(M)$ from Section 7.1. Quite similar to the definition of $H^{(5)}$ in Section 7.1, we define $H^{(n)} = H_{\text{repair}}$, where H_{repair} is as defined by Lemma 6.2. We denote by $H_j^{(n)}$ the j^{th} thick column of $H^{(n)}, 1 \leq j \leq n$, i.e.,

$$H^{(n)} = [H_1^{(n)}\ H_2^{(n)}\ \ldots\ H_n^{(n)}].$$

Next, we define the matrices $H^{(t)}, 3 \leq t \leq n - 1$ in an iterative manner as follows:

Step 1. Let $t = n - 1$.

Step 2. Define the matrices $H_j^{(t)}, n - t + 1 \leq j \leq n$, such that the columns of $H_j^{(t)}$ form a basis for the vector space
$\mathcal{S}\left(H_j^{(t+1)}\right) \cap \mathcal{S}\left(H^{(t+1)}|_{\{n-t, n-t+1, \ldots, j-1\}}\right)$.

Step 3. Define the matrix $H^{(t)}$ as

$$H^{(t)} = [H_{n-t+1}^{(t)}\ H_{n-t+2}^{(t)}\ \ldots\ H_n^{(t)}]. \tag{77}$$

Step 4. If $t \geq 4$, decrement t by 1 and go back to Step 2.

Clearly, the ranks of the matrices $H^{(t)}, 3 \leq t \leq n$ are ordered as

$$\rho(H^{(t)}) \geq \rho(H^{(t-1)}),\ 4 \leq t \leq n. \tag{78}$$

We use the notation $H_j^{(t)}, n - t + 1 \leq j \leq n$ to refer to the j^{th} thick column of the matrix $H^{(t)}$. While every thick column of $H^{(n)}$ has exactly α thin columns, thick columns of $H^{(t)}, 3 \leq t \leq n - 1$ need not have the same number of thin columns. We point out for clarity that the thick columns of the matrix $H^{(t)}$ are indexed using $\{n - t + 1, \ldots, n\}$. We have avoided $\{1, \ldots, t\}$ for the convenience of notation.

8.1.2 Block matrix representation of the matrix $H^{(t)}$

Since $H^{(n)} = H_{\text{repair}}$, it has a block matrix representation as given in (45). We write in brief

$$H^{(n)} = \left(A_{i,j}^{(n)}, 1 \le i, j \le n \right), \tag{79}$$

where $A_{i,i}^{(n)} = I_\alpha, 1 \le i \le n$. We introduce block matrix representations for $H^{(t)}, 3 \le t \le n-1$ as

$$H^{(t)} = \left(A_{i,j}^{(t)}, 1 \le i \le n, n-t+1 \le j \le n \right), \tag{80}$$

where $A_{i,j}^{(t)}$ is an $\alpha \times \rho(H_j^{(t)})$ matrix over $\mathbb{F}$ such that

$$\mathcal{S}\left(A_{i,j}^{(t)}\right) \subseteq \mathcal{S}\left(A_{i,j}^{(t+1)}\right) \bigcap \sum_{\ell=n-t}^{j-1} \mathcal{S}\left(A_{i,\ell}^{(t+1)}\right). \tag{81}$$

Note that (81) is a direct consequence of our definition of the matrix $H^{(t)}$. Having set up the notation, we introduce the key lemma that establishes the relations among the ranks of the sub-matrices of $\{H^{(t)}\}$. The lemma is similar in spirit to Lemma 7.2, and its proof is omitted here.

Lemma 8.2:

a *For any t, j such that $3 \le t \le n$ and $n-t+1 \le j \le n$, we have*

$$\rho\left(H_j^{(t)}\right) = \rho\left(A_{j,j}^{(t)}\right). \tag{82}$$

b *For any t, j such that $3 \le t \le n-1$ and $n-t+1 \le j \le n$, we have*

$$\begin{aligned}\rho\left(A_{j,j}^{(t)}\right) = \rho\left(A_{j,j}^{(t+1)}\right) - \Big\{\rho\left(H^{(t+1)}|_{\{n-t,\ldots,j\}}\right) \\ -\rho\left(H^{(t+1)}|_{\{n-t,\ldots,j-1\}}\right)\Big\}.\end{aligned} \tag{83}$$

c *For any t, j such that $3 \le t \le n-1$ and $n-t+2 \le j \le n$, we have*

$$\rho\left(A_{j,j}^{(t)}\right) + \sum_{\ell=n-t+1}^{j-1} \rho\left(A_{j,\ell}^{(t)}\right) \le \sum_{\ell=n-t}^{j-1} \rho\left(A_{j,\ell}^{(t+1)}\right). \tag{84}$$

8.2 *On the proof of* (76)

The bounds in (76) is obtained as a necessary condition for satisfying the chain of inequalities given by

$$\rho(H^{(n)}) \geq \rho(H^{(n-1)}) \ \geq \ \cdots \ \geq \ \rho(H^{(n-r+1)}). \tag{85}$$

In the analysis of (85), we consider in the first step, the inequality $\rho(H^{(n-r+2)}) \geq \rho(H^{(n-r+1)})$ and obtain a lower bound on $\rho(H^{(n-r+2)})$. In the second step, we move on to the inequality $\rho(H^{(n-r+3)}) \geq \rho(H^{(n-r+2)})$ and obtain a lower bound on $\rho(H^{(n-r+3)})$. In the second step, we would make use of a lower bound on $\rho(H^{(n-r+2)})$ that was derived in the first step. This procedure is continued iteratively until we arrive at lower bound for $\rho(H^{(n)})$. The following theorem is a key intermediate step in this process.

Theorem 8.3: *For any s such that $1 \leq s \leq n-3$, and any t such that $3+s \leq t \leq n$, the rank of the matrix $H^{(t)}$ is lower bounded by*

$$\begin{aligned}\rho\left(H^{(t)}\right) \geq \frac{2}{(s+1)(s+2)} &\left\{ (s+1) \sum_{j=n-t+1}^{n} \rho\left(A_{j,j}^{(t)}\right) \right. \\ &\left. - \sum_{j=n-t+2}^{n} \sum_{\ell=n-t+1}^{j-1} \rho\left(A_{j,\ell}^{(t)}\right) \right\}.\end{aligned} \tag{86}$$

Proof: The proof is by induction on s, and see Prakash and Nikhil Krishnan (2015) for details. □

One can identify Theorem 8.3 in the context of $(n=5, k=4, d=4)$. The bounds would then be associated with $(s=1, t=5)$, $(s=1, t=4)$ and $(s=2, t=5)$ and are precisely those given in (69), (70) and (73), respectively. To complete the proof of (76), we evaluate the bound in (86) for the $(n-3)$ pairs given by $(s, t=n), 1 \leq s \leq n-3$. By substituting the constraints $\rho\left(A_{j,j}^{(n)}\right) = \alpha, 1 \leq j \leq n$ and $\rho\left(A_{i,j}^{(n)}\right) \leq \beta, 1 \leq i, j \leq n, i \neq j$, we finally obtain that

$$\begin{aligned}\rho\left(H^{(n)}\right) &\geq \frac{2}{(s+1)(s+2)} \left\{ (s+1) \sum_{j=1}^{n} \alpha - \sum_{j=2}^{n} (j-1)\beta \right\} \\ &= \frac{2(s+1)n\alpha - n(n-1)\beta}{(s+1)(s+2)}, \ 1 \leq s \leq n-3.\end{aligned} \tag{87}$$

By choosing $r = s+1$, (76) follows from (87). This completes the proof of (76), and consequently that of the Theorem 8.1.

9 On the achievability of the outer bounds on normalised ER trade-off

The outer bounds presented in the present paper matches with the performance of existing code constructions in certain cases, and we present two such results here.

9.1 *Characterisation of normalised ER trade-off for the case* $k = 3, d = n - 1$

In the case of $k = 3$ and $d = n - 1$, the repair-matrix bound is achieved by a construction that appeared in Senthoor, Sasidharan and Kumar (2015). We will given an example of the repair-matrix bound below:

Example: $(n = 6, k = 3, d = 5)$: Using (29), the bound on the ER file size B can computed as

$$B \leq \frac{10\alpha}{7} + \frac{34\beta}{7}, \;\; 5\beta \geq \alpha > \frac{13\beta}{4}. \tag{88}$$

Based on the bound in (88), an outer bound on the normalised ER trade-off is drawn in Figure 4(a). It is required to have a single code construction $\mathcal{C}_{\text{int}}$ for the normalised operating point $(\bar{\alpha}_0, \bar{\beta}_0) = (\frac{13}{38}, \frac{2}{19})$ to achieve the entire normalised ER trade-off, as the remaining points can be achieved by space sharing of the MSR code $\mathcal{C}_{\text{MSR}}$, the MBR codes $\mathcal{C}_{\text{MBR}}$ and $\mathcal{C}_{\text{int}}$. The construction of $\mathcal{C}_{\text{int}}$ was provided in Senthoor, Sasidharan and Kumar (2015), and thus establishing that the repair-matrix bound is tight in this case.

9.2 *Characterisation of normalised ER trade-off for the case* $(n, k = n - 1, d = n - 1)$ *under the linear setting*

In the case of linear codes, the bound presented in Theorem 1.2 is achieved by canonical layered codes that was introduced in Tian et al. (2015). When specialised to the case of $d = n - 1$, the layered codes achieve points described by

$$(\bar{\alpha}, \bar{\beta}) = \left(\frac{r}{n(r-1)}, \frac{r}{n(n-1)}\right), \;\; 2 \leq r \leq n - 1 \tag{89}$$

on the $(\bar{\alpha}, \bar{\beta})$-plane. If one substitutes $r = 2$ in (89), it corresponds to the MBR point, and the achievable points move closer to the MSR point as r increases. It is also proved that the point corresponding to $r = n - 1$ lies on the FR trade-off in the near-MSR region. An achievable region on the $(\bar{\alpha}, \bar{\beta})$-plane is obtained by space-sharing codes for values of r, $2 \leq r \leq n - 1$ along with an MSR-code. We can write the equation of the line segment obtained by connecting two points $\left(\frac{r}{n(r-1)}, \frac{r}{n(n-1)}\right)$ and $\left(\frac{(r+1)}{n((r+1)-1)}, \frac{(r+1)}{n(n-1)}\right)$, $2 \leq r \leq n - 2$ as

$$r(r-1)n\bar{\alpha} + n(n-1)\bar{\beta} = r^2 + r, \tag{90}$$

and that of the line segment connecting the MSR point and the point corresponding to $r = n - 1$ as

$$(n-2)\bar{\alpha} + \bar{\beta} = 1.$$

This matches with the equations of line segments as given in Theorem 1.2. The normalised linear trade-off for $(n = 6, k = d = 5)$ is given in Figure 4(b).

Acknowledgements

This research is supported in part by the National Science Foundation under Grant 1421848 and in part by an India-Israel UGC-ISF joint research program grant. Birenjith Sasidharan would like to thank the support of TCS Research Scholar Programme Fellowship awarded to him. N. Prakash was a PhD student at IISc, Bangalore and also an Intern at NetApp, Bangalore, during the duration of this work. M. Nikhil Krishnan and Myna Vajha would like to thank the support of Visvesvaraya PhD Scheme for Electronics & IT awarded by the Department of Electronics and Information Technology, Government of India. A portion of the material in this paper was presented in part at the 2014 IEEE International Symposium on Information Theory Sasidharan, Senthoor and Kumar (2014) and in part at the 2015 IEEE International Symposium on Information Theory Prakash and Krishnan (2015).

References

Information theory inequality prover. http://user-www.ie.cuhk.edu.hk/ ITIP/. Accessed: 2016-June-02.

Solutions of computed information theoretic limits (SCITL). http://web.eecs.utk.edu/ ctian1/SCITL.html. Accessed: 2016-April-17.

Cadambe, V., Jafar, S.A., Maleki, H., Ramchandran, K. and Suh, C. (2013) 'Asymptotic interference alignment for optimal repair of MDS codes in distributed storage', *IEEE Transaction on Information Theory*, Vol. 59, No. 5, pp.2974–2987.

Dean, J. and Ghemawat, S. (2008) 'Mapreduce: Simplified data processing on large clusters', *Communications of the ACM*, Vol. 51, No. 1, pp.107–113.

Dimakis, A.G., Godfrey, P.B., Wu, Y., Wainwright, M.J. and Ramchandran, K. (2010) 'Network coding for distributed storage systems', *IEEE Transaction on Information Theory*, Vol. 56, No. 9, pp.4539–4551.

Duursma, I.M. (2014) 'Outer bounds for exact repair codes', *CoRR*, abs/1406.4852.

Duursma, I.M. (2015) 'Shortened regenerating codes', *CoRR*, abs/1505.00178.

Elyasi, M., Mohajer, S. and Tandon, R. (2015) 'Linear exact repair rate region of $(k+1, k, k)$ distributed storage systems: A new approach', *2015 IEEE International Symposium on Information Theory*, June 2015, Hong Kong, pp.2061–2065.

Goparaju, S., El Rouayheb, S. and Calderbank, R. (2014) 'New codes and inner bounds for exact repair in distributed storage systems', *2014 IEEE International Symposium on Information Theory*, June 2014, Honolulu, pp.1036–1040.

Kermarrec, A.M., Le Scouarnec, N. and Straub, G. (2011) 'Repairing multiple failures with coordinated and adaptive regenerating codes', *Proceedings of IEEE International Symposium Network Coding (NetCod)*, Beijing, July 2011, pp.88–93.

Mohajer, S. and Tandon, R. (2015). 'New bounds on the (n, k, d) storage systems with exact repair', *2015 IEEE International Symposium on Information Theory*, June 2015, Hong Kong, pp.2056–2060.

Papailiopoulos, D.S., Dimakis, A.G. and Cadambe, V.R. (2013) 'Repair optimal erasure codes through hadamard designs', *IEEE Transaction on Information Theory*, Vol. 59, No. 5, pp.3021–3037.

Prakash, N. and Krishnan, M.N. (2015) 'The storage-repair-bandwidth trade-off of exact repair linear regenerating codes for the case $d = k = n - 1$', *2015 IEEE International Symposium on Information Theory*, June 2015, Hong Kong, pp.859–863.

Prakash, N. and Nikhil Krishnan, M. (2015) 'The storage-repair-bandwidth trade-off of exact repair linear regenerating codes for the case $d = k = n - 1$', *CoRR*, abs/1501.03983.

Rashmi, K.V., Shah, N.B. and Kumar, P.V. (2011) 'Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction', *IEEE Transactions on Information Theory*, Vol. 57, No. 8, pp.5227–5239.

Sasidharan, B., Senthoor, K. and Kumar, P.V. (2014) 'An improved outer bound on the storage-repair-bandwidth tradeoff of exact-repair regenerating codes', *2014 IEEE International Symposium on Information Theory*, Honolulu, pp.2430–2434.

Senthoor, K., Sasidharan, B. and Kumar, P.V. (2015) 'Improved layered regenerating codes characterising the exa ct-repair storage-repair bandwidth tradeoff for certain parameter sets', *2015 IEEE Information Theory Workshop, Jerusalem*, April 2015, pp.1–5.

Shah, N.B., Rashmi, K.V., Vijay Kumar, P. and Ramchandran, K. (2012a) 'Distributed storage codes with repair-by-transfer and nonachievability of interior points on the storage-bandwidth tradeoff', *IEEE Transactions on Information Theory*, Vol. 58, No. 3, pp.1837–1852.

Shah, N.B., Rashmi, K.V., Vijay Kumar, P. and Ramchandran, K. (2012b) 'Interference alignment in regenerating codes for distributed storage: Necessity and code constructions', *IEEE Transactions on Information Theory*, Vol. 58, No. 4, pp.2134–2158.

Shum, K.W. and Hu, Y. (2013) 'Cooperative regenerating codes', *IEEE Transactions on Information Theory*, Vol. 59, No. 11, pp.7229–7258.

Suh, C. and Ramchandran, K. (2011) 'Exact-repair MDS code construction using interference alignment', *IEEE Transactions on Information Theory*, Vol. 57, No. 3, pp.1425–1442.

Tamo, I., Wang, Z. and Bruck, J. (2013) 'Zigzag codes: MDS array codes with optimal rebuilding', *IEEE Transactions on Information Theory*, Vol. 59, No. (3):1597–1616.

Tian, C. (2014) 'Characterizing the rate region of the (4, 3, 3) exact-repair regenerating codes', *IEEE Journal on Selected Areas in Communications*, Vol. 32, No. 5, pp.967–975.

Tian, C. (2015) 'A note on the rate region of exact-repair regenerating codes', *CoRR*, abs/1503.00011.

Tian, C., Sasidharan, B., Aggarwal, V., Vaishampayan, V.A., Vijay Kumar, P. (2015) 'Layered exact-repair regenerating codes via embedded error correction and block designs', *IEEE Transactions on Information Theory*, Vol. 61, No. 4, pp.1933–1947.

Wu, Y. (2010) 'Existence and construction of capacity-achieving network codes for distributed storage', *IEEE Journal on Selected Areas in Communications*, Vol. 28, No. 2, pp.277–288.

Yeung, R.W. (1997) 'A framework for linear information inequalities', *IEEE Transactions on Information Theory*, Vol. 43, No. 6, pp.1924–1934.

Appendix A

Proof of Theorem 3.4

Two different estimates on the joint entropy of certain repair data, expressed as functions of $\{\omega_i\}_{i=0}^{k-1}$, are used to derive a lower bound on $\epsilon = \hat{B} - B$. The repair data considered differ based on the value of μ.

Case 1: $\mu \in \{1, 2, \ldots, k-2\}$
We set $r_0 = \left\lfloor \frac{k-\mu}{\mu+1} \right\rfloor$. We will have two sub-cases for $r_0 \geq 1$ and $r_0 = 0$.

Case 1(a): $r_0 \geq 1$
We consider the sub-trapezoid $Z_{q,t}$ with parameter $q = \mu$ and $t = r_0(\mu+1)$. Pictorially, it is marked as a trapezium $EFGH$ in the repair matrix shown in Figure 13(a). The set of nodes $T = \{\mu+1, \mu+2, \ldots, (r_0+1)(\mu+1)-1\}$ that are repaired by $Z_{q,t}$ is split into r_0 groups of $(\mu+1)$ nodes in order, and the corresponding subsets of $Z_{q,t}$ are denoted by $\mathcal{E}_i, i = 1, 2, \ldots, r_0$. Pictorially, $\mathcal{E}_1$ is associated with the trapezium EFG_1H_1

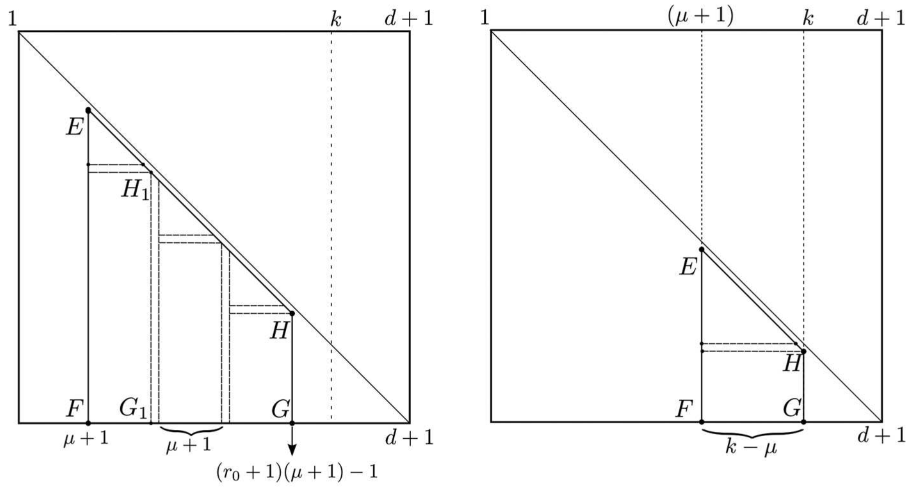
in Figure 13(a). Similarly, every $\mathcal{E}_i$ is associated with a smaller trapezium contained within $EFGH$. The set $\mathcal{E}_i$ can again be viewed as the union of two subsets $\mathcal{V}_i$ and $\mathcal{T}_i$, respectively, associated with the largest rectangle within the trapezium and the remaining triangular region. These sets are formally defined as

$$\mathcal{E}_i = \{S_x^y \mid S_x^y \in Z_{q,t}, (\mu+1)i \leq y \leq (\mu+1)(i+1)-1\}, \ \ i = 1,2,\ldots,r_0$$
$$\mathcal{V}_i = \{S_x^y \mid S_x^y \in \mathcal{E}_i, (\mu+1)(i+1) \leq x \leq d+1\}, \ \ i = 1,2,\ldots,r_0$$
$$\mathcal{T}_i = \{S_x^y \mid S_x^y \in \mathcal{E}_i, (\mu+1)i+1 \leq x \leq (\mu+1)(i+1)-1\}, \ \ i = 1,2,\ldots,r_0.$$

Note that $\mathcal{E}_i = \mathcal{V}_i \cup \mathcal{T}_i$. Next, we bound the joint entropy $H(Z_{q,t})$ as

$$\begin{aligned} H(Z_{q,t}) &\leq \sum_{i=1}^{r_0} H(\mathcal{V}_i) + \sum_{i=1}^{r_0} H(\mathcal{T}_i) \\ &\leq \sum_{i=1}^{r_0} (d-(i+1)(\mu+1)+2)\cdot[\beta+\mu\theta+\mu\omega_\mu+((\omega_\mu+\omega_{\mu+1})] \\ &\quad + \sum_{i=1}^{r_0} \frac{(\mu+1)\mu\beta}{2}. \end{aligned} \tag{91}$$

Figure 13 The illustration of the trapezoid regions considered for Case 1



(a) The sub-trapezoid region considered in Case 1(a) (b) The trapezoid region considered in Case 1(b)

In the second inequality, we use (27) of Corollary 3.3 to obtain the upper bound on $H(\mathcal{V}_i)$. On the other hand, using Lemma 3.1, we also have,

$$\begin{aligned} H(Z_{q,t}) \geq H(Z_{q,t} \mid W_Q) &\geq \sum_{i=\mu}^{(r_0+1)(\mu+1)-2} \min\{\alpha,(d-i)\beta\} - \sum_{i=\mu}^{(r_0+1)(\mu+1)-2} \omega_i \\ &= \left[\sum_{i=\mu}^{(r_0+1)(\mu+1)-2} (d-i)\beta\right] - \theta - \sum_{i=\mu}^{(r_0+1)(\mu+1)-2} \omega_i. \end{aligned} \tag{92}$$

Matching the bounds in (91) and (92) and using the identity (23), we obtain that

$$\epsilon \geq \frac{\left(d - \frac{(\mu+1)(r_0+3)}{2} + 2\right) r_0\mu(\beta - \theta) \ - \ \theta}{\left(d - \frac{(\mu+1)(r_0+3)}{2} + 2\right) r_0(\mu + 1) \ + \ 1}. \tag{93}$$

Case 1(b): $r_0 = 0$

The collection Z_q of repair data considered in this case corresponds to the trapezoid configuration Z_q with $q = \mu$. The set Z_q is written as $Z_q = \mathcal{V} \cup \mathcal{T}$, where

$$\mathcal{V} = \{S_x^y \mid S_x^y \in Z_q, k+1 \leq x \leq d+1\},$$
$$\mathcal{T} = \{S_x^y \mid S_x^y \in Z_q, \mu+2 \leq x \leq k\}$$

Pictorially, Z_q is represented by the trapezium $EFGH$ in Figure 13(b). Quite similar to the *Case 1(a)*, we invoke Corollary 3.3 to bound $H(Z_q)$ as

$$\begin{aligned} H(Z_q) \ \geq \ H(Z_q \mid W_Q) \leq H(\mathcal{V}) + H(\mathcal{T}) \\ \leq (d-k+1) \cdot [\beta + (k-\mu-1)\theta + (k-\mu-1)\omega_\mu \\ +(\omega_\mu + \omega_{\mu+1})] + \frac{(k-\mu-1)(k-\mu)\beta}{2}. \end{aligned} \tag{94}$$

On the other hand, using Lemma 3.1,

$$\begin{aligned} H(Z_q) &\geq \sum_{i=\mu}^{k-1} \min\{\alpha, (d-i)\beta\} - \sum_{i=\mu}^{k-1} \omega_i \\ &= \left[\sum_{i=\mu}^{k-1} (d-i)\beta\right] - \theta - \sum_{i=\mu}^{k-1} \omega_i. \end{aligned} \tag{95}$$

Matching the bounds in (94) and (95) and using the identity (23), we obtain that

$$\epsilon \geq \frac{(d-k+1)(k-\mu-1)(\beta-\theta) \ - \ \theta}{(d-k+1)(k-\mu) \ + \ 1} \tag{96}$$

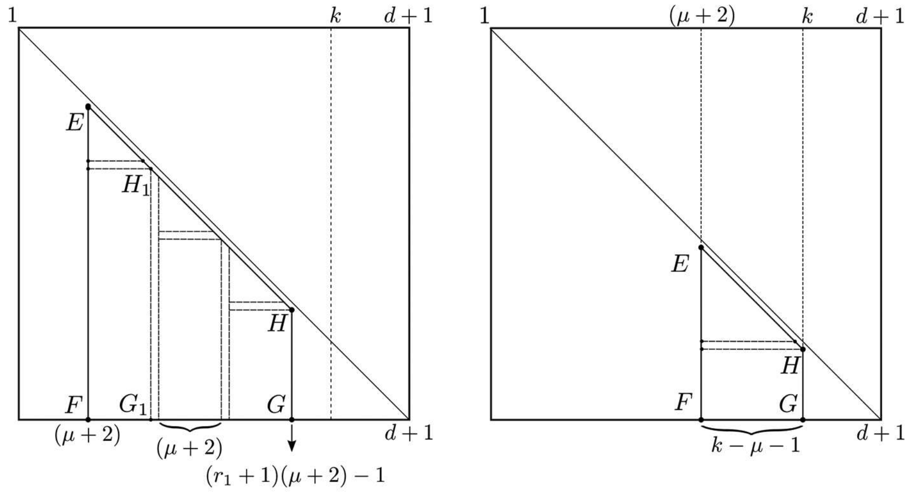
Case 2: $\mu \in \{0, 1, \ldots, k-3\}$

We set $r_1 = \left\lfloor \frac{k-\mu-1}{\mu+2} \right\rfloor$. We will have two sub-cases for $r_1 \geq 1$ and $r_1 = 0$. In contrast with *Case 1*, we consider a different trapezoid configuration (Q, Z_q) with $q = (\mu + 1)$ in *Case 2*. It turns out that this change will help in getting a tighter bound in certain regions of (μ, θ).

Case 2(a): $r_1 \geq 1$

In this case, we consider the set $Z_{q,t}$ with parameter $q = \mu + 1, t = r_1(\mu + 2)$. The set of nodes $T = \{\mu + 2, \mu + 2, \ldots, (r_1 + 1)(\mu + 2) - 1\}$ that are repaired by $Z_{q,t}$ is split into r_1 groups of $(\mu + 2)$ nodes in order, and the corresponding subsets of $Z_{q,t}$ are denoted by $\mathcal{E}_i, i = 1, 2, \ldots, r_1$. A pictorial illustration is given in Figure 14(a). Every $\mathcal{E}_i$ is further viewed as the union of two subsets $\mathcal{V}_i$ and $\mathcal{T}_i$, respectively, associated with the largest

Figure 14 The illustration of the trapezoid regions considered for Case 2



(a) The sub-trapezoid region considered in Case 2(a) (b) The trapezoid region considered in Case 2(b)

rectangle within the trapezium, and the remaining triangular region. The sets of interest are formally defined as

$$\begin{aligned}
\mathcal{E}_i &= \{S_x^y \mid S_x^y \in Z_{q,t}, (\mu+2)i \le y \le (\mu+2)(i+1)-1\}, \;\; i = 1,2,\ldots,r_1 \\
\mathcal{V}_i &= \{S_x^y \mid S_x^y \in \mathcal{E}_i, (\mu+2)(i+1) \le x \le d+1\}, \;\; i = 1,2,\ldots,r_1 \\
\mathcal{T}_i &= \{S_x^y \mid S_x^y \in \mathcal{E}_i, (\mu+2)i+1 \le x \le (\mu+2)(i+1)-1\}, \;\; i = 1,2,\ldots,r_1,
\end{aligned}$$

where $\mathcal{E}_i = \mathcal{V}_i \cup \mathcal{T}_i$. Similar to *Case 1(a)*, we bound the joint entropy $H(Z_{q,t})$ as

$$H(Z_{q,t}) \le \sum_{i=1}^{r_1} H(\mathcal{V}_i) + \sum_{i=1}^{r_1} H(\mathcal{T}_i) \tag{97}$$

$$\begin{aligned}
&\le \sum_{i=1}^{r_1} (d-(i+1)(\mu+2)+2) \cdot [2\beta - \theta + (\mu+1)\omega_{\mu+1} \\
&\quad +(\omega_{\mu+1}+\omega_{\mu+2})] + \sum_{i=1}^{r_1} \frac{(\mu+2)(\mu+1)\beta}{2}.
\end{aligned} \tag{98}$$

In the last inequality, we have used (28) of Corollary 3.3. On the other hand, using Lemma 3.1, we also have

$$\begin{aligned}
H(Z_{q,t}) \ge\; H(Z_{q,t} \mid W_Q) &\ge \sum_{i=\mu+1}^{(r_1+1)(\mu+2)-2} \min\{\alpha, (d-i)\beta\} \\
&\quad - \sum_{i=\mu+1}^{(r_1+1)(\mu+2)-2} \omega_i
\end{aligned} \tag{99}$$

$$= \left[\sum_{i=\mu+1}^{(r_1+1)(\mu+2)-2} (d-i)\beta\right] - \sum_{i=\mu+1}^{(r_1+1)(\mu+2)-2} \omega_i \tag{100}$$

Matching the bounds in (98) and (100) and using the identity (23), we obtain that

$$\epsilon \geq \frac{\left(d - \frac{(\mu+2)(r_1+3)}{2} + 2\right) r_1 \left[\mu\beta \; + \; \theta\right]}{\left(d - \frac{(\mu+2)(r_1+3)}{2} + 2\right) r_1(\mu+2) \; + \; 1} \tag{101}$$

Case 2(b): $r_1 = 0$
The set Z_q with $q = \mu + 1$ is considered in this case. We can write $Z_q = \mathcal{V} \cup \mathcal{T}$, where

$$\mathcal{V} = \{S_x^y \mid S_x^y \in Z_q, k+1 \leq x \leq d+1\},$$
$$\mathcal{T} = \{S_x^y \mid S_x^y \in Z_q, \mu+3 \leq x \leq k\}.$$

A pictorial illustration is given in Figure 14(b). Following the same line of arguments as in *Case 1(a)*, we obtain that

$$H(Z_q) \leq (d-k+1) \cdot [2\beta - \theta + (k-\mu-1)\epsilon] + \frac{(k-\mu-2)(k-\mu-1)\beta}{2}, \tag{102}$$

$$H(Z_q) \geq \left[\sum_{i=\mu+1}^{k-1} (d-i)\beta\right] - \sum_{i=\mu+1}^{k-1} \omega_i. \tag{103}$$

Matching the above two bounds and using the identity (23), we obtain the lower bound for ϵ:

$$\epsilon \geq \frac{(d-k+1)\left[(k-\mu-3)\beta + \theta\right]}{(d-k+1)(k-\mu-1) \; + \; 1} \tag{104}$$

Proof of Lemma 7.2

By definition of δ_j in (47), we have that

$$\delta_j = \rho\left(H^{(5)}|_{[j]}\right) - \rho\left(H^{(5)}|_{[j-1]}\right) \tag{105}$$
$$= \dim\left(\mathcal{S}\left(H^{(5)}|_{[j-1]}\right) + \mathcal{S}\left(H_j^{(5)}\right)\right) - \dim\left(\mathcal{S}\left(H^{(5)}|_{[j-1]}\right)\right) \tag{106}$$
$$= \dim\left(\mathcal{S}\left(H_j^{(5)}\right)\right) - \dim\left(\mathcal{S}\left(H^{(5)}|_{[j-1]}\right) \cap \mathcal{S}\left(H_j^{(5)}\right)\right) \tag{107}$$
$$= \rho\left(H_j^{(5)}\right) - \rho\left(H_j^{(4)}\right) \tag{108}$$
$$= \rho\left(A_{j,j}^{(5)}\right) - \rho\left(A_{j,j}^{(4)}\right), \tag{109}$$

where in (107) we used the identity $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$ for any two subspaces W_1, W_2. While (108) follows from the definition of $H_j^{(4)}$, (109) from Remark 1. The first assertion (66) of the lemma now follows from (109) and (63).

By definition of $H_j^{(4)}$, we have that $\mathcal{S}\left(A_{j,j}^{(4)}\right) \subseteq \sum_{\ell=1}^{j-1} \mathcal{S}\left(A_{j,\ell}^{(5)}\right)$, and it follows that

$$\rho\left(A_{j,j}^{(4)}\right) \leq \dim\left(\sum_{\ell=1}^{j-1} \mathcal{S}\left(A_{j,\ell}^{(5)}\right)\right). \tag{110}$$

The RHS of (110) is further upper bounded as follows:

$$\begin{aligned}
\dim\left(\sum_{\ell=1}^{j-1} \mathcal{S}\left(A_{j,\ell}^{(5)}\right)\right) &= \dim\left(\sum_{\ell=1}^{j-2} \mathcal{S}\left(A_{j,\ell}^{(5)}\right) + \mathcal{S}\left(A_{j,j-1}^{(5)}\right)\right) && (111)\\
&= \dim\left(\sum_{\ell=1}^{j-2} \mathcal{S}\left(A_{j,\ell}^{(5)}\right)\right) + \dim\left(\mathcal{S}\left(A_{j,j-1}^{(5)}\right)\right)\\
&\quad - \dim\left(\sum_{\ell=1}^{j-2} \mathcal{S}\left(A_{j,\ell}^{(5)}\right) \cap \mathcal{S}\left(A_{j,j-1}^{(5)}\right)\right) && (112)\\
&\leq \dim\left(\sum_{\ell=1}^{j-2} \mathcal{S}\left(A_{j,\ell}^{(5)}\right)\right) + \dim\left(\mathcal{S}\left(A_{j,j-1}^{(5)}\right)\right)\\
&\quad - \dim\left(\mathcal{S}\left(A_{j,j-1}^{(4)}\right)\right) && (113)\\
&= \dim\left(\sum_{\ell=1}^{j-2} \mathcal{S}\left(A_{j,\ell}^{(5)}\right)\right) + \rho\left(A_{j,j-1}^{(5)}\right) - \rho\left(A_{j,j-1}^{(4)}\right), && (114)
\end{aligned}$$

where (113) follows from the definition of $H_j^{(4)}$ and $A_{j,j-1}^{(4)}$. If $j = 3$, (114) completes the proof of the second assertion. Else, for the case $j \geq 4$, the term $\dim\left(\sum_{\ell=1}^{j-2} \mathcal{S}\left(A_{j,\ell}^{(4)}\right)\right)$ can further be upper bounded by following a similar sequence of steps as in (111)–(114). This completes the proof.

Notes

[1] Although regenerating codes are defined for the case of single node failures, there are later works that looked into the case of simultaneous failure of multiple nodes and studied cooperative repair in such a situation Shum and Hu (2013); Kermarrec, Le Scouarnec and Straub (2011). However, in this paper, we focus only on single node failures.

[2] We have simplified the proof to some extent, and therefore certain arguments differ from what is presented in Elyasi, Mohajer and Tandon (2015)