Low bandwidth repair of the RS(10,4) Reed-Solomon code

Iwan Duursma and Hoang Dau
University of Illinois at Urbana-Champaign
{duursma,hoangdau}@illinois.edu

***Abstract*—As an alternative to replication of data blocks, the Hadoop Distributed File System offers the possibility of erasure coding using Reed-Solomon codes. The use of Reed-Solomon codes significantly reduces storage overhead but has more expensive failure recovery. Using the shortened Reed-Solomon code RS(10,4), with 10 data symbols and 4 check symbols, standard erasure repair requires downloading 10 symbols or 80 bits. Known schemes attain a reduced repair bandwidth of 65 or 64 bits. In this paper we present three repair schemes with bandwidth 60, 56 and 54, respectively.**

INTRODUCTION

The HDFS-RAID module for the Hadoop Distributed File System (HDFS) [1] offers different solutions for erasure coding including the use of the code RS(10,4), a shortened version of the double error-correcting Reed-Solomon code of length 255. Codewords have 10 data symbols and 4 check symbols. The code has the property that a codeword can be rebuilt from any subset of ten symbols. To repair a single erased symbol it suffices to first collect any ten other symbols and then use the rebuilding properties of the code. The repair bandwidth for collecting ten symbols is 80 bits. A different approach is to divide an erased symbol into sub-symbols and to collect different sets of repair data at the sub-symbol level. In the sub-symbol setting a helper node will receive multiple sub-symbol requests. A sub-symbol repair scheme lowers the bandwidth by arranging that some of the requests are dependent and can be ignored. The approach was applied previously to the RS(10,4) code in [2], [3], with reductions in bandwidth from 80 to 65 and 64 bits, respectively.

For a linear code, a sub-symbol repair scheme is built from combinations of parity check equations. The parity check equations for the RS(10,4) code use the values of polynomials of degree at most three in $1, \zeta, \ldots, \zeta^{13}$, for $\zeta^{255} = 1$. The larger codes RS(12,2) and RS(11,3) are defined with the same set of elements but use linear and quadratic checks, respectively. We first build a collection of basic parity check combinations for these two codes. We express the reduction in bandwidth geometrically in terms of the cross-ratio of four field elements. We then use the basic combinations to construct three repair schemes for the RS(10,4) code, with bandwidth 60, 56 and 54 bits, respectively. The 54 bit scheme uses a different combination of checks for each position. The checks for the 56 bit scheme all have a common structure. The structure has several benefits for implementations and will be useful for guiding computer searches when building repair schemes for other codes. The 60 bit scheme uses essentially one combination of checks, with a 4-fold symmetry that allows it to correct erasures in any of the 14 positions.

OUTLINE

In Section I we give a formal description of a linear repair scheme and its bandwidth. Section II presents general properties of the scalar restriction of a code and Section III describes erasure repair for the full-length RS-code of rate one-half. Section IV summarizes the construction of low bandwidth repair relations by use of the trace operator. Section V describes the RS(10,4) code and discusses basic repair relations (presented in Tables II, III, IV). In Section VI we construct three different repair schemes for the code RS(10,4), that are of bandwith 60, 56 and 54, respectively (presented in Tables V, VI, VII).

I. BLOCK ERASURES

We describe repair schemes and the notion of repair bandwidth for linear codes with n blocks.

Definition I.1. A repair scheme for a linear code with n blocks is a collection $\{R_j : j \in [n]\}$ of matrices, such that R_j is orthogonal to the code and of the form $(H_1|H_2|\cdots|H_n)$ with H_j a square matrix of full rank.

Lemma I.2. *For a linear code with n blocks and repair scheme $\{R_j : j \in [n]\}$, the parity checks R_j can be used to repair the erasure of the j-th block. The repair requires a bandwidth of $\gamma_j = \sum_{i \neq j} \operatorname{rank} H_i$ symbols.*

$$R_1 = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right] \qquad R_3 = \left[\begin{array}{cc|cc|cc|cc} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$
$$R_2 = \left[\begin{array}{cc|cc|cc|cc} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right] \qquad R_4 = \left[\begin{array}{cc|cc|cc|cc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] \tag{1}$$

Proof. The repair of the $j-$th block in a codeword $(c_1|c_2|\cdots|c_n)$ uses $H_j c_j^T + \sum_{i\neq j} H_i c_i^T = 0$. The vector $H_i c_i^T$ is uniquely determined by a subset of $\operatorname{rank} H_i$ independent symbols. Thus the repair can be completed after collecting a total of γ_j symbols. □

The repair bandwidth γ of a repair scheme $\{R_j : j \in [n]\}$ is defined as the maximum bandwidth used by the scheme to repair any single block, i.e., $\gamma = \max \gamma_j$.

Example I.3. Concatenation of the $[4, 2, 3]$ code

$$C = \left[\begin{array}{cccc} 1 & 0 & b & a \\ 0 & 1 & a & b \end{array}\right],$$

defined over $\mathbb{F}_4 = \{0, 1, a, b\}$, yields a binary code

$$C' = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

The code is equivalent to the extended Hamming code of type $[8, 4, 4]$ and is self-dual. Using either the first two rows or the last two rows, any block can be repaired with bandwidth 4. Equation (1) gives a complete repair scheme with bandwidth 3. The rows used for R_3 and R_4 are both subsets of the rows in C'.

The same steps as in the example will be followed when we consider repair schemes for the code RS(10,4). That code is defined over the field $F = GF(2^8)$. We choose a subfield $L \subset F$ and, after concatenation, we consider the code as a code with coefficients in L. For the code with coefficients in L we then select combinations of checks that yield low bandwidth repair schemes.

II. Restriction of scalars

This section takes the general point of view of representing a linear code that is defined over a field F over one of its subfields L. The part that is used for the RS(10,4) code is summarized in Section IV.

Let C be a F-linear code of type $[n, k]$. Let $L \subset F$ be a subfield such that F is of dimension ℓ as L-vector space and let $A = \{a_1, \ldots, a_\ell\}$ be a basis for F over L. Field elements $x \in F$ can be expressed uniquely as $x = x_1 a_1 + \cdots + x_\ell a_\ell$, with $x_1, \ldots, x_\ell \in L$. The map $\phi(x) = (x_1, \ldots, x_\ell)$ defines an isomorphism of L-vector spaces. For $x, y \in F$ and $c \in L$,

$$\phi(x + y) = \phi(x) + \phi(y), \quad \phi(cx) = c\phi(x). \tag{2}$$

Applying the map ϕ coordinate-wise to every codeword in C yields a L-linear code $\phi(C)$ of type $[n\ell, k\ell]$. The code $\phi(C)$ over the subfield L is called the scalar restriction of C. It is the concatenation of C with a full space outer code.

Let $\{u_h : h \in [k]\} \subset F^n$ be a basis for C as F-linear code. Then $\{a_i u_h : h \in [k], i \in [\ell]\} \subset F^n$ is a basis for C as L-vector space, and $\{\phi(a_i u_h) : h \in [k],\ i \in [\ell]\}$ is a basis for $\phi(C)$ as L-linear code.

Lemma II.1. *Let $(u_{h,i} : h \in [k], i \in [n])$ be a generator matrix for C. Then $(\Phi(u_{h,i}) : h \in [k], i \in [n])$ gives a generator matrix in block form for $\phi(C)$, where*

$$\Phi(x) = \begin{pmatrix} \phi(a_1 x) \\ \vdots \\ \phi(a_\ell x) \end{pmatrix}. \tag{3}$$

Example II.2. For $F = \mathbb{F}_4 = \{0, 1, a, b\}$ and $L = \{0, 1\}$, let $A = \{a, b\}$. Then

$$\Phi(0) = \left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right], \qquad \Phi(a) = \left[\begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array}\right],$$
$$\Phi(1) = \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right], \qquad \Phi(b) = \left[\begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array}\right].$$

With Lemma II.1 we recover the matrix for the code $C' = \phi(C)$ in Example I.3.

Lemma II.3. *For $x, y \in F$,*

$$\phi(x)\Phi(y) = \phi(xy). \tag{4}$$

Proof.

$$\phi(x)\Phi(y) = \phi(\,(\phi(x) \cdot (a_1, \ldots, a_n))y\,) = \phi(xy).$$

□

Lemma II.4. *The map $\Phi : F \to L^{\ell\times\ell}$ in (3) is an L-algebra homomorphism. For $x, y \in F$ and $c \in L$,*

$$\Phi(x + y) = \Phi(x) + \Phi(y),$$
$$\Phi(cx) = c\Phi(x), \text{ and } \Phi(xy) = \Phi(x)\Phi(y).$$

Proof. The first two properties are a direct consequence of (2). For the third property we need that $\phi(a_i x)\Phi(y) = \phi(a_i xy)$, for $i = 1, 2, \ldots, n$.. This follows from the previous lemma after replacing x with $a_i x$. □

Lemma II.5. *The vector $(a_1, \ldots, a_n)^T \in F^n$ is an eigenvector for $\Phi(x)$ with eigenvalue x.*

Proof. By the definition of ϕ, $\phi(a_i x) \cdot (a_1, \ldots, a_n) = a_i x$, and thus

$$\Phi(x)(a_1, \ldots, a_n)^T = (a_1 x, \ldots, a_n x)^T.$$

□

The properties that were established thus far all refer to a basis $a_1, \ldots, a_\ell$ for F over L but did not make use of the Frobenius automorphism σ. For L of size q, and thus F of size q^ℓ, it is defined by $\sigma(x) = x^q$. For $x \in F$, define $\delta(x) = (x, \sigma(x), \ldots, \sigma^{\ell-1}(x))$ and $\Delta(x) = \mathrm{diag}(x, \sigma(x), \ldots, \sigma^{\ell-1}(x))$. Furthermore, let

$$\Sigma(A) = \begin{pmatrix} \delta(a_1) \\ \vdots \\ \delta(a_\ell) \end{pmatrix} = \begin{pmatrix} a_1 & \cdots & \sigma^{\ell-1}(a_1) \\ \vdots & & \vdots \\ a_\ell & \cdots & \sigma^{\ell-1}(a_\ell) \end{pmatrix}$$

The matrix $\Sigma(A)$ is invertible if and only if the elements of A are linearly independent over L.

Lemma II.6. *The eigenvectors and eigenvalues for $\Phi(x)$ are given by*

$$\Phi(x)\Sigma(A) = \Sigma(A)\Delta(x).$$

For the unique basis $B = \{b_1, \ldots, b_\ell\}$ such that $\Sigma(A)\Sigma(B)^T = I$,

$$\Phi(x) = \Sigma(A)\Delta(x)\Sigma(B)^T.$$

Proof. For the first claim apply σ repeatedly to the previous lemma. The second claim is clear. □

The basis B in the lemma is a dual basis for A. For $x \in F$, let $\phi_A(x)$, resp. $\phi_B(x)$, denote the coefficients of x wrt A, resp. wrt B. Let $\mathrm{Tr}(x) = \mathrm{Trace}(\Delta(x)) = \sum_{i=0}^{\ell-1} \sigma^i(x)$ be the trace map from F to L. The second claim in the lemma can be stated as

$$\Phi(x) = (\mathrm{Tr}(a_i b_j x) : i, j \in [\ell]).$$

If we let $e_A = \phi_A(1)$ and $e_B = \phi_B(1)$ then

$$\begin{aligned} \phi_A(x) &= e_A\Phi(x) = e_A(\mathrm{Tr}(abx)) \\ &= (\mathrm{Tr}(b_1 x), \ldots, \mathrm{Tr}(b_\ell x)). \\ \phi_B(y) &= e_B\Phi(y)^T = e_B(\mathrm{Tr}(bay)) \\ &= (\mathrm{Tr}(a_1 y), \ldots, \mathrm{Tr}(a_\ell y)). \end{aligned}$$

Moreover

$$\begin{aligned} \mathrm{Tr}(xy) &= e_A\Phi(xy)e_B^T \\ &= (e_A\Phi(x)) \cdot (e_B\Phi(y)^T) = \phi_A(x) \cdot \phi_B(y). \end{aligned} \quad (5)$$

Lemma II.7. *If C and C' are orthogonal codes (resp. dual codes) over F then $\phi_A(C)$ and $\phi_B(C')$ are orthogonal codes (resp. dual codes) over L.*

Proof. For $c = (c_1, \ldots, c_n) \in C$ and $c' = (c'_1, \ldots, c'_n) \in C'$, so that $c \cdot c' = 0$, we need to show that

$$\sum_{i=1}^{n} \phi_A(c_i) \cdot \phi_B(c'_i) = 0.$$

Using (5), we have

$$\sum_{i=1}^{n} \mathrm{Tr}(c_i c'_i) = \mathrm{Tr}(\sum_{i=1}^{n} c_i c'_i) = \mathrm{Tr}(0) = 0.$$

□

Remark II.8. For a different proof that uses Lemma II.1 and Lemma II.4 note that it suffices to prove

$$\sum_{i=1}^{n} \Phi(c_i)(\Phi(c'_i)^T)^T = 0.$$

Clearly this reduces to

$$\sum_{i=1}^{n} \Phi(c_i)\Phi(c'_i) = \Phi(\sum_{i=1}^{n} c_i c'_i) = \Phi(0) = 0.$$

III. RS-codes in Cauchy form

We describe a special case of a result in [3] for repairing Reed-Solomon codes. It illustrates that standard concatenation as in the previous section does not by itself yield efficient repair schemes over a subfield. The section is independent from the following sections that deal with the code RS(10,4).

Let $F = GF(2^\ell)$ and let $L = \{0, 1\}$ be the binary subfield. Thus $\sigma(x) = x^2$ and $\mathrm{Tr}(x) = \sum_{i=0}^{l-1} \sigma^i(x) = \sum_{i=0}^{l-1} x^{2^i}$. For $x \in F$, either $\mathrm{Tr}(x) = 0$ or $\mathrm{Tr}(x) = 1$. Let $F_0 = \{x \in F : \mathrm{Tr}(x) = 0\}$ and $F_1 = \{x \in F : \mathrm{Tr}(x) = 1\}$. Define a code C over F with length $n = |F|$ and dimension $k = |F_0|$ by the matrix

$$C = (I_k|A), \quad A_{y,z} = \frac{1}{z - y}, \quad (y \in F_0, z \in F_1).$$

The matrix A is a Cauchy matrix and thus the code is MDS. If we label the rows by elements $y \in F_0$ and the columns by elements $z \in F$, with $z \in F_0$ for the first

$$\Phi(x) = \begin{pmatrix} T(a_1b_1x) & T(a_1b_2x) & \cdots & T(a_1b_\ell x) \\ T(a_2b_1x) & T(a_2b_2x) & \cdots & T(a_2b_\ell x) \\ \vdots & & \cdots & \vdots \\ T(a_\ell b_1x) & T(a_\ell b_2x) & \cdots & T(a_\ell b_\ell x) \end{pmatrix} \qquad R(x) = \begin{pmatrix} T(a_1x) \\ T(a_2x) \\ \vdots \\ T(a_\ell x) \end{pmatrix} \begin{pmatrix} T(b_1x^{-1}) \\ T(b_2x^{-1}) \\ \vdots \\ T(b_\ell x^{-1}) \end{pmatrix}^T \tag{6}$$

block and $z \in F_1$ for the second block, then row y of C gives the values in $z \in F$ of the polynomial

$$t_y(x) = \frac{T(x-y)}{x-y}.$$

As y runs through the different elements of F_0, the polynomials $t_y(x)$ span the space of all polyniomials in x of degree less than $2^{\ell-1}$. Thus the code is the Reed-Solomon code of length 2^ℓ and dimension $2^{\ell-1}$. The code is self-dual.

The matrix $\Phi(x) = \Sigma(A)\Delta(x)\Sigma(B)^T$ describes blocks for a generator matrix of $\phi(C)$ (Lemma II.1 and Lemma II.6). Using this format for the code $\phi(C)$ when repairing erasures in the dual code will be inefficient since the blocks $\Phi(x)$ are of full rank when $x \neq 0$. We give a different format for $\phi(C)$ that uses blocks of the form $R(x) = \Sigma(A)J(x)\Sigma(B)$ with $J(x) = \Delta(x)J\Delta(x^{-1})$ and J the all-one matrix of size $\ell \times \ell$. Clearly the blocks $R(x)$ are of rank one. The matrix $J(x)$ has entries, for $x \neq 0$,

$$\sigma^{i-1}(x)/\sigma^{j-1}(x), \quad i \in [\ell], j \in [\ell].$$

For $x \in F$, the polynomial $\sigma^{\ell+i-1}(x)/\sigma^{j-1}(x)$ can be used to compute entries without division and we set $J(0) = I$. The matrix $\Delta(x)$ is what we will call $\sigma-$circulant, every row is obtained by applying σ to a shift of the previous row. As a product of $\sigma-$circulant matrices $J(x)$ is also $\sigma-$circulant. The special case $J(0) = I$ is σ-circulant by direct verification. We have the following relation between rank one matrices J and diagonal matrices Δ.

Lemma III.1. *For $z \in F_1$,*

$$J(z) = \sum_{y \in F_0} J(y)\Delta(\frac{1}{z-y})$$

Proof. The two sides represent $\ell \times \ell$ matrices. Comparing entries in row i and column j yields

$$\frac{\sigma^{i-1}(z)}{\sigma^{j-1}(z)} = \sum_{y \in F_0} \frac{\sigma^{i-1}(y)}{\sigma^{j-1}(y(z-y))}.$$

It suffices to prove equality for entries in the first column $j = 1$. Equality for columns $j > 1$ then follows from the $\sigma-$circulant property on both sides of the equation, i.e., by repeated application of σ. Thus the equality to be proven takes the form

$$\frac{\sigma^{i-1}(z)}{z} = \sum_{y \in F_0} \frac{\sigma^{i-1}(y)}{y} \cdot \frac{1}{z-y}.$$

This is a special case of a partial fraction decomposition. For $f(x)$ with simple roots and for $0 \leq r < \deg f$,

$$\frac{x^r}{f(x)} = \sum_{f(\alpha)=0} \frac{\alpha^r}{f'(\alpha)} \cdot \frac{1}{x-\alpha}.$$

For the special case $f(x) = \mathrm{Tr}(x)$ we have that $f'(x) = 1$ and $f(z) = 1$ for $z \in F_1$. □

Let

$$R(x) = \Sigma(A)J(x)\Sigma(B)^T$$

For $x \neq 0$, the matrix $R(x)$ is of rank one. It has entries $T(a_ix)T(b_jx^{-1}) \in L$, for $i, j \in [l]$. With $J(0) = I$, we have $R(0) = I$.

Proposition III.2. *Let*

$$C = (I_k|A), \quad A_{y,z} = \frac{1}{z-y}, \text{ for } y \in F_0, z \in F_1,$$

The block matrix with block

$$R(z-v)$$

of size $\ell \times \ell$ in row $v \in F_0$ and column $z \in F$ is a generator matrix for $\phi(C)$.

Proof. The generator matrix for the scalar restriction $\phi(C)$ in standard form has blocks indexed by $y \in F_0$ and $z \in F$. The matrix is systematic in the columns $z \in F_0$ and has blocks

$$\Phi(\frac{1}{z-y})$$

in the columns $z \in F_1$. Thus the claim amounts to verifying that, for all $v \in F_0$ and $z \in F_1$,

$$R(z-v) = \sum_{y \in F_0} R(y-v)\Phi(\frac{1}{z-y})$$

Or, equivalently, that

$$J(z-v) = \sum_{y \in F_0} J(y-v)\Delta(\frac{1}{z-y}).$$

$$R_v \;:\; \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} c_v^T = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} c_{v+110}^T + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} c_{v+011}^T + \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} c_{v+101}^T +$$
$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} c_{v+100}^T + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} c_{v+010}^T + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} c_{v+001}^T + \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} c_{v+111}^T. \quad (7)$$

This is Lemma III.1 after the substitution $z \mapsto z - v$, $y \mapsto y - v$. □

Corollary III.3. *For codewords that are orthognal to $\phi(C)$, a block erasure in position $v \in F$ can be repaired using*

$$c_v^T + \sum_{z \in F \setminus v} R(z - v) c_z^T = 0$$

The repair uses one bit each from $|F| - 1$ nodes.

Proof. The proposition gives a generator matrix with blocks $R(z-v)$, $v \in F_0$, $z \in F$, that is sytematic in the positions $z \in F_0$. By symmetry, $\phi(C)$ has a generator matrix with blocks $R(z - v)$, $v \in F_1$, $z \in F$, that is sytematic in the positions $z \in F_1$. Thus, for either $v \in F_0$ or $v \in F_1$, the blocks $R(z - v)$, $z \in F$, form a submatrix of a generator matrix for $\phi(C)$. □

Example III.4. For $F = GF(2^3)$, $\phi(C)$ is the binary Golay code of type [24,12,8]. Codewords in $\phi(C)$ are divided into eight blocks of three bits, labeled as c_z, for $z \in F$. Equation (7) gives the repair equation for a single block erasure using the corollary. The equation uses a binary labeling for the blocks. Thus the Golay code in the given format repairs any one block out of eight blocks of three bits with repair bandwidth seven bits.

IV. Degree two erasure coding

The previous sections showed that while standard concatenation gives generator matrices in a structered block format, with blocks as in Lemma II.1, for efficient repair it is in general necessary to modify this structure and replace the standard blocks with other carefully chosen blocks, such as in Proposition III.2. It is in general difficult to find repair schemes of the form $(H_1|\cdots|H_n)$ in Definition I.1 that have full rank in one block and low rank in the remaining blocks. We consider first repair schemes of degree two, i.e., schemes with blocks H_i of size 2.

For a linear code C of length n with parity check matrix H, a vector $c = (c_1, c_2, \ldots, c_n)$ is a codeword in C if and only if

$$p_1 c_1 + p_2 c_2 + \cdots + p_n c_n = 0 \quad (8)$$

for every vector $p = (p_1, p_2, \ldots, p_n)$ in the row space of H. For correcting a single erasure in a codeword, say in the position i, it suffices to choose a check vector p with $p_i \neq 0$ and to use the interpolation relation (8) to obtain c_i from the remaining codeword symbols. A codeword symbol c_j with $j \neq i$ is needed for interpolation only if $p_j \neq 0$, in other words only if j is in the support of the vector p. Check vectors with small support use fewer computations for the interpolation. A further benefit of a small support is that it reduces repair bandwidth, since there is no need to collect codeword symbols outside the support.

For a field F of size q^2 and a subfield L of size q, the element $x \in F$ has a unique conjugate $\sigma(x) = x^q \in F$ and the trace of x is $T(x) = x + x^q$. The trace map is linear over the subfield, i.e. $T(x + y) = T(x) + T(y)$ and $T(ax) = aT(x)$ for all $x, y \in F$ and $a \in L$. For any two checks $p \cdot c = 0$ and $q \cdot c = 0$ as in (8), and after applying the trace operator to each of them, we have that

$$\begin{cases} T(p_1 c_1) + \cdots + T(p_n c_n) = 0 \\ T(q_1 c_1) + \cdots + T(q_n c_n) = 0 \end{cases}$$

In matrix form

$$\begin{bmatrix} T(p_1 c_1) \\ T(q_1 c_1) \end{bmatrix} + \cdots + \begin{bmatrix} T(p_n c_n) \\ T(q_n c_n) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

After writing out the trace in terms of $\sigma(x) = x^q$ and using that $\sigma(xy) = \sigma(x)\sigma(y)$,

$$\begin{bmatrix} p_1 & \sigma(p_1) \\ q_1 & \sigma(q_1) \end{bmatrix} \begin{bmatrix} c_1 \\ \sigma(c_1) \end{bmatrix} + \quad \cdots \quad +$$
$$+ \begin{bmatrix} p_n & \sigma(p_n) \\ q_n & \sigma(q_n) \end{bmatrix} \begin{bmatrix} c_n \\ \sigma(c_n) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \quad (9)$$

Let

$$P_i = \begin{bmatrix} p_i & \sigma(p_i) \\ q_i & \sigma(q_i) \end{bmatrix}. \quad (10)$$

The interpolation relation (9) is used as before to interpolate c_i. This time the interpolation coefficients are matrices and recovery of c_i from $P_i(c_i, \sigma(c_i))^T$ is possible only if P_i is invertible. A symbol c_j participates in the interpolation only if $P_j \neq 0$. The added feature compared to (8) is that P_j may be nonzero but not of full rank. In that case it suffices to download one subfield symbol, namely $\mathrm{Tr}(p_j c_j)$ or $\mathrm{Tr}(q_j c_j)$.

To pass from the matrices $P_1, \ldots, P_n$ to a repair scheme $(H_1|\cdots|H_n)$ with coefficients in the subfield L, let $\{a_1, a_2\}$ and $\{b_1, b_2\}$ be a pair of dual bases for F as L-vector space, so that

$$\begin{bmatrix} a_1 & \sigma(a_1) \\ a_2 & \sigma(a_2) \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ \sigma(b_1) & \sigma(b_2) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Let

$$H_i = \begin{bmatrix} p_i & \sigma(p_i) \\ q_i & \sigma(q_i) \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ \sigma(a_1) & \sigma(a_2) \end{bmatrix}$$

and

$$\phi(c_i)^T = \begin{bmatrix} b_1 & \sigma(b_1) \\ b_2 & \sigma(b_2) \end{bmatrix} \begin{bmatrix} c_i \\ \sigma(c_i) \end{bmatrix}.$$

Then (9) becomes

$$H_1\phi(c_1)^T + \cdots + H_n\phi(c_n)^T = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \qquad (11)$$

The rank of H_i, which is the relevant property for repair bandwidth, is the same as the L-rank of P_i.

V. The code RS(10,4)

The Hadoop Reed-Solomon code RS(10,4) is defined over the field $F = GF(2^8)$ of 256 elements. The field F is represented as the ring of binary polynomials modulo $x^8+x^4+x^3+x^2+1$. This is the standard choice for Reed-Solomon codes. The polynomial is the lexicographically first polynomial $p(x)$ such that $1, x, x^2, \ldots, x^{254}$ have distinct remainders modulo $p(x)$. The polynomial $x^8 + x^4 + x^3 + x + 1$ is lexicographically earlier and is also irreducible but it divides $x^{51}+1$ so is not primitive which is required for Reed-Solomon codes. The subfields of F that we use are primarily the subfield $L = GF(2^4)$ but also $B = GF(2)$ and $K = GF(2^2)$, such that $B \subset K \subset L \subset F$. We will represent elements of the field L as binary polynomials modulo y^4+y+1 and elements of K as binary polynomials modulo z^2+z+1. The inclusion $K \subset L$ holds for $z = y \cdot y^4 = y^5$ and $L \subset F$ holds for $y = x \cdot x^{16} = x^{17}$. Let $\zeta = x \pmod{x^8+x^4+x^3+x^2+1}$ be a fixed primitive element for $GF(2^8)$.

The code RS(10,4) is the shortening to length 14 of the double error-correcting Reed-Solomon code of length 255. The four checks for the code are therefore

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{12} & \zeta^{13} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{24} & \zeta^{26} \\ 1 & \zeta^3 & \zeta^6 & \cdots & \zeta^{36} & \zeta^{39} \end{pmatrix}$$

The repair properties of the code depend on the choice of primitive element ζ. The choice for ζ such that $\zeta^8 + \zeta^4 + \zeta^3 + \zeta^2 + 1 = 0$ turns out to be a favorable choice, providing us with relations that help to reduce bandwidth. Another useful property of the code is that it is defined with consecutive roots of unity $1, \zeta, \ldots, \zeta^{13}$ which gives two ways to exploit symmetry. First, for any scheme that repairs erasures in ζ^i there is an equivalent reciprocal scheme that repairs erasures in ζ^{13-i}. And second, some repair schemes that repair erasures in ζ^i can be shifted to repair erasures in ζ^{i+1}. The self-reciprocal partition

$$\{0, 3, 5, 8, 10, 13\} \cup \{6, 7\} \cup \{1, 2, 4, 9, 11, 12\}$$

of the positions plays a role in several of the low bandwidth checks that we use in our repair schemes for the RS(10,4) code. Geometrically what helps us to reduce bandwith is that for any subset of four elements in $\{\zeta, \zeta^2, \zeta^4, \zeta^9, \zeta^{11}, \zeta^{12}\}$ the cross-ratio of the four elements lies in the subfield $L = GF(2^4)$. For a different choice of primitive element ζ (other than conjugates and their reciprocals) the size of such a subset among $1, \zeta, \ldots, \zeta^{13}$ would have been at most five.

The codes RS(12,2) and RS(11,3) are defined with the same set of elements but use linear and quadratic checks, respectively. The code RS(12,2) has a self-reciprocal repair scheme that repairs erasures in the first two classes of the partition and reduces bandwith in the last class. The code RS(11,3) has self-reciprocal repair schemes that repair erasures in the first class (resp. last class) and reduce bandwith in the last two classes (resp. first two classes). We rely on the repair schemes for these two codes to construct repair schemes for RS(10,4).

A. Repair relations of type A

For a degree two repair scheme using linear polynomials, a greedy choice is to start with polynomials $p(x) = (x - a)$ and $q(x) = (x - b)$, which guarantees a rank reduction in the matrices P_a and P_b in (9). By using the scaled polynomials $p(x) = (c - b)(x - a)$ and $q(x) = (c - a)(x - b)$ we assure that the L-linear span of $p(x)$ and $q(x)$ contains a polynomial, namely $p(x) - q(x)$, such that $p(c) - q(c) = 0$, raising the

number of positions with bandwidth reduction to three. For a fourth position d to have bandwidth reduction with this choice of $p(x)$ and $q(x)$ it is necessary that $q(d)/p(d) \in L$. The latter quantity is called the cross-ratio of the four elements a, b, c, d.

$$h = \frac{(c-a)(d-b)}{(c-b)(d-a)}. \tag{12}$$

Clearly it satisfies a symmetry property

$$h(a,b,c,d) = h(c,d,a,b) \tag{13}$$

and a transitivity property

$$h(a,b,c,e) = h(a,b,c,d)h(a,b,d,e). \tag{14}$$

The three sets I_1, I_2, I_3 in Table II have the property that, for any four elements chosen from the set, the cross-ratio is in L. Let $\{a,b,c\} = \{\zeta, \zeta^2, \zeta^{11}\}$ and $\{d,e,f\} = \{\zeta^4, \zeta^9, \zeta^{12}\}$ be a partition for I_2. The matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ a & b & c & d & e & f \end{pmatrix}$$

is equivalent to the matrix

$$\begin{pmatrix} (b-c) & (c-a) & (a-b) & & & \\ (b-c)a & (c-a)b & (a-b)c & & & \\ & & & (e-f) & (f-d) & (d-e) \\ & & & (e-f)d & (f-d)e & (d-e)f \end{pmatrix}.$$

The last matrix has all its minors in the subfield $L = GF(2^4)$. This implies that any three of the following polynomials are linearly dependent over L.

$$(b-c)(x-a), (c-a)(x-b), (a-b)(x-c),$$
$$(e-f)(x-d), (f-d)(x-e), (d-e)(x-f).$$

For row A2 in Table II we select $p(x) = \zeta^{11}(x-\zeta^4)$ and $q(x) = (x-\zeta^9)$. Both polynomials are scaled, such that $q(x)$ is monic and such that the leading coefficient of $p(x)$ is among $1, \zeta, \ldots, \zeta^{16}$. Rows A1 and A3 follow by shifting.

B. Repair relations of type B

The relations in Table III arise from four-tuples of quadratic polynomials such that any three are linearly dependent over the subfield $L = GF(2^4)$. For row $B2$ the four polynomials are scaled versions of

$$(x-\zeta)(x-\zeta^{12}), (x-\zeta^2)(x-\zeta^{11}),$$
$$(x-\zeta^4)(x-\zeta^9), (x-\zeta^6)(x-\zeta^7).$$

The polynomials have the same constant terms and are all of the form $(x^2+\zeta^{13}) + \alpha x$. It follows that they can be scaled such that any three become linearly dependent over L if and only if the corresponding linear polynomials $y+\alpha$ have this property, where α is one of

$$a = \zeta + \zeta^{12}, b = \zeta^2 + \zeta^{11}, c = \zeta^4 + \zeta^9, d = \zeta^6 + \zeta^7.$$

The cross-ratio of these four elements is $\zeta^{170} \in L$. The other rows use a similar verification.

C. Repair relations of type C

The relations in Table IV arise from pairs of quadratic polynomials (p,q) that each have five linear combinations $p + \alpha q$ with a zero in $1, \zeta, \ldots, \zeta^{13}$, for a nonzero coefficent $\alpha \in L$. This property can be stated in terms of cross-ratios as follows. Let

$$p(x) = (x-c_1)(x-c_2),\ q(x) = (x-d_1)(x-d_2).$$

The rescaled versions $q(a)p(x)$ and $p(a)q(x)$ have a $L-$linear combination, namely the difference $q(a)p(x) - p(a)q(x)$, that is zero in $x = a$. A $L-$linear combination with a zero in $x = b$ exists if and only if

$$\begin{aligned} \frac{p(a)q(b)}{q(a)p(b)} &= \frac{(a-c_1)(b-d_1)}{(a-d_1)(b-c_1)} \frac{(a-c_2)(b-d_2)}{(a-d_2)(b-c_2)} \\ &= h(c_1,d_1,a,b)h(c_2,d_2,a,b) \\ &= h(a,b,c_1,d_1)h(a,b,c_2,d_2) = h_1 h_2 \in L \end{aligned}$$

In row C2, $p(x)$ has zeros $(c_1,c_2) = (\zeta, \zeta^{11})$ and $q(x)$ has zeros $(d_1,d_2) = (\zeta^6, \zeta^7)$. And $h_1 h_2 \in L$ for any two $a, b \in \{2,4,5,9,12\}$. That this is true for $a, b \in \{2,4,9,12\}$ follows from relation under A2 and B2. For example, for $a = \zeta^2, b = \zeta^4$, using A2 and transitivity shows that

$$\begin{aligned} &h(\zeta^2, \zeta^4, \zeta, \zeta^6)h(\zeta^2, \zeta^4, \zeta^{11}, \zeta^7) \in L \\ &\qquad \Leftrightarrow h(\zeta^2, \zeta^4, \zeta, \zeta^6)h(\zeta^2, \zeta^4, \zeta^{12}, \zeta^7) \in L \end{aligned}$$

and the latter holds by B2. Thus there is strict bandwith increase between the solutions B2 and C2 and it occurs at ζ^5.

D. Degree two relations of other type

There is a modest total number of $17 \cdot (364 \cdot 363)/2$ pairs $(p(x), q(x)\zeta^a)$ where $p(x)$ and $q(x)$ are both monic and each with three zeros in $1, \zeta, \ldots, \zeta^{13}$, and $a = 0, 1, \ldots, 16$ (so that ζ^a represents the cosets of the mutliplicative subgroup L^* in F^*). Using the MAGMA program we found, in a matter of seconds, 100 pairs of polynomials that give a repair scheme with $\sum_j \operatorname{rank} H_j = 68$ and 2375 pairs with next lowest total rank $\sum_j \operatorname{rank} H_j = 72$. Table I gives a breakdown of these pairs according to their rank distributions and includes their mutliplicities (when different pairs span the

same space over L). A similar search in [3] is over pairs of monic polynomials, i.e. the special case $a = 0$. The case $a = 0$ produces five pairs with $\sum_j \operatorname{rank} H_j = 68$ that correct erasures in the positions $2, 3, 4, 8, 11$ with bandwith 60 but not in the other positions.

VI. Repair schemes for RS(10,4)

The repair relations A1–A3 in Table II have $\sum_j \operatorname{rank} H_j = 8 \cdot 8 + 6 \cdot 4 = 88$. They correct erasures for RS(12,2) with bandwith 80. For RS(10,4) we can mutliply the linear polynomials $p(x)$ and $q(x)$ with the same quadratic polynomial $(x - c_1)(x - c_2)$ to reduce the rank in the positions c_1 and c_2. Using A1, A2 and A3 in this way results in a repair scheme for RS(10,4) of bandwidth 64.

The relations B1–B6 in Table III reduce the bandwith to one half in eight positions. The relations have $\sum_j \operatorname{rank} H_j = 6 \cdot 8 + 8 \cdot 4 = 80$. They repair RS(11,3) with bandwith 72. Mutliplication of the quadratic polynomials $p(x)$ and $q(x)$ with the same linear polynomial $x - c$ reduces the rank in the position c. This results in a different repair scheme for RS(10,4) with same bandwith 64.

A. Repair scheme with bandwidth 60

The relations C1–C12 in Table IV reduce the bandwith to one half in nine positions. The relations have $\sum_j \operatorname{rank} H_j = 5 \cdot 8 + 9 \cdot 4 = 76$. After mutliplying the polynomials with a common linear factor the relations repair erasures for RS(10,4) with bandwith 60. A minimal set of such relations is given in Table V. The relations are obtained with C1, C2, C5 and C6 and are such that C1-C2 and C5-C6 are related by shifting and C1-C6 and C2-C5 via reciprocity. Each has full rank in four of the fourteen positions. Together they repair single erasures in any of the fourteen positions.

B. Repair scheme with bandwidth 56

To arrive at bandwidth 56 we use repair schemes of degree four. A single repair relation combines four different checks $p \cdot c = q \cdot c = r \cdot c = s \cdot c = 0$, obtained with four different polynomials $p(x), q(x),\ r(x), s(x)$, all of degree three. The field $F = GF(2^8)$ contains the subfield $K = GF(2^2)$. For $\sigma(x) = x^4$, and for $\operatorname{Tr}(x) = x + \sigma(x) + \sigma^2(x) + \sigma^3(x)$, we have

$$\operatorname{Tr}(p \cdot c) = \operatorname{Tr}(q \cdot c) = \operatorname{Tr}(r \cdot c) = \operatorname{Tr}(s \cdot c) = 0.$$

which may be written as

$$\sum_i P_i \begin{pmatrix} c \\ \sigma(c) \\ \sigma^2(c) \\ \sigma^3(c) \end{pmatrix}^T = 0,$$

for

$$P_i = \begin{pmatrix} p(x_i) & \sigma(p(x_i)) & \sigma^2(p(x_i)) & \sigma^3(p(x_i)) \\ q(x_i) & \sigma(q(x_i)) & \sigma^2(q(x_i)) & \sigma^3(q(x_i)) \\ r(x_i) & \sigma(r(x_i)) & \sigma^2(r(x_i)) & \sigma^3(r(x_i)) \\ s(x_i) & \sigma(s(x_i)) & \sigma^2(s(x_i)) & \sigma^3(s(x_i)) \end{pmatrix}.$$

Rather than searching over all 4-tuples we took a semi-greedy approach and searched over combinations of pairs (p, q) and (r, s) such that each of (p, q) and (r, s) has low (but not necessarilly optimal) bandwidth as degree two repair scheme. Among the various solutions that we found Table VI gives seven repair relations that together repair single erasures in each of the fourteen positions. Each of the seven relations repairs two unique positions. The choices for $p(x), q(x), r(x), s(x)$ are of the special form

$$\begin{aligned} p(x) = f_0(x)g_0(x),\ q(x) = f_0(x)g_1(x), \\ r(x) = f_1(x)g_0(x),\ s(x) = f_1(x)g_1(x), \end{aligned} \quad (15)$$

for linear polynomials $f_0(x), f_1(x)$ and quadratic polynomials $g_0(x), g_1(x)$.

C. Repair scheme with bandwidth 54

Table VII gives individual repair solutions with bandwidth 54 for each of the positions $j = 0, 1, \ldots, 13$. Each individual relation has a certain structure, and this structure was used to search in a non-exhaustive and non-greedy way within the search space of all relations. Solutions are equivalent for each pair of positions j and $13 - j$ through reciprocity. The solutions for positions $2, 5, 8, 11$ are of the special form (15). All solutions are of degree 4 except for the positions $j = 0$ and $j = 13$. Those are of degree 8. They combine two degree 4 solutions of low bandwidth in such a way that the eight polynomials contain a third degree four low bandwidth solution.

References

[1] http://wiki.apache.org/hadoop/HDFS-RAID.

[2] Karthikeyan Shanmugam, Dimitris S Papailiopoulos, Alexandros G Dimakis, and Giuseppe Caire. A repair framework for scalar mds codes. *Selected Areas in Communications, IEEE Journal on*, 32(5):998–1007, 2014.

[3] Venkat Guruswami and Mary Wootters. Repairing Reed-solomon Codes In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC'16, pages 216–226. 2016.

[4] Maheswaran Sathiamoorthy, Megasthenis Asteris, Dimitris Papailiopoulos, Alexandros G Dimakis, Ramkumar Vadali, Scott Chen, and Dhruba Borthakur. Xoring elephants: Novel erasure codes for big data. In *Proceedings of the VLDB Endowment*, volume 6, pages 325–336. 2013.

full	half	zero	total rank	# pairs	# checks
4	9	1	68	90	90
3	11	0	68	10	10
6	6	2	72	1260	84 (15)
5	8	1	72	828	36 (6), 60 (3), 432
4	10	0	72	287	62 (3), 101

TABLE I

COUNTING PAIRS OF DEGREE THREE POLYNOMIALS THAT DEFINE CHECKS FOR RS(14,10) OF TOTAL RANK WEIGHT AT MOST 72 (EQUIVALENT TO 9 FULL SYMBOLS). A STANDARD CHECK USES 11 FULL SYMBOLS. THE LAST COLUMN GIVES THE MULTIPLICITY OF A CHECK (IN PARENTHESES) IF THE SAME CHECK IS DEFINED BY MORE THAN ONE PAIR OF POLYNOMIALS.

A	$p(x)$	$q(x)$	I	J
1	$[3]\zeta^{11}$	$[8]$	$I_1 = \{0,1,3,8,10,11\}$	$J_1 \cup \{5,6\}$
2	$[4]\zeta^{11}$	$[9]$	$I_2 = \{1,2,4,9,11,12\}$	$J_2 \cup \{6,7\}$
3	$[5]\zeta^{11}$	$[10]$	$I_3 = \{2,3,5,10,12,13\}$	$J_3 \cup \{7,8\}$

TABLE II

RS(12,2): PAIRS OF LINEAR POLYNOMIALS, SIX POSITIONS I WHERE THEY REDUCE BANDWIDTH, AND EIGHT POSITIONS J IN WHICH THEY CAN CORRECT SINGLE ERASURES

B	$p(x)$	$q(x)$	I	J
1	[1, 10]	$[5, 6]\zeta^6$	$I_1 \cup \{5,6\}$	$J_1 = \{2,4,7,9,12,13\}$
2	[2, 11]	$[6, 7]\zeta^6$	$I_2 \cup \{6,7\}$	$J_2 = \{3,5,8,10,13,0\}$
3	[3, 12]	$[7, 8]\zeta^6$	$I_3 \cup \{7,8\}$	$J_3 = \{4,6,9,11,0,1\}$
4	[4, 8]	$[0, 12]\zeta^2$	$J_5 \cup \{5,8\}$	$J_4 = \{1,3,6,9,11,13\}$
5	[5, 9]	$[1, 13]\zeta^2$	$J_4 \cup \{5,8\}$	$J_5 = \{0,2,4,7,10,12\}$

TABLE III

RS(11,3): PAIRS OF QUADRATIC POLYNOMIALS, EIGHT POSITIONS I WHERE THEY REDUCE BANDWIDTH, AND SIX POSITIONS J IN WHICH THEY CAN CORRECT SINGLE ERASURES

C	$p(x)$	$q(x)$	I	J
1	[0, 10]	$[5, 6]\zeta^8$	$I_1 \cup \{4,5,6\}$	$J_1 \backslash 4$
2	[1, 11]	$[6, 7]\zeta^8$	$I_2 \cup \{5,6,7\}$	$J_2 \backslash 5$
3	[2, 12]	$[7, 8]\zeta^8$	$I_3 \cup \{6,7,8\}$	$J_3 \backslash 6$
4	[1, 11]	$[5, 6]\zeta^9$	$I_1 \cup \{5,6,7\}$	$J_1 \backslash 7$
5	[2, 12]	$[6, 7]\zeta^9$	$I_2 \cup \{6,7,8\}$	$J_2 \backslash 8$
6	[3, 13]	$[7, 8]\zeta^9$	$I_3 \cup \{7,8,9\}$	$J_3 \backslash 9$
7	[1, 3]	$[5, 6]\zeta^4$	$I_1 \cup \{5,6,12\}$	$J_1 \backslash 12$
8	[2, 4]	$[6, 7]\zeta^4$	$I_2 \cup \{6,7,13\}$	$J_2 \backslash 13$
9	[9, 11]	$[6, 7]\zeta^{11}$	$I_2 \cup \{0,6,7\}$	$J_2 \backslash 0$
10	[10, 12]	$[7, 8]\zeta^{11}$	$I_3 \cup \{1,7,8\}$	$J_3 \backslash 1$
11	[0, 4]	$[12, 8]\zeta^9$	$\{0,\ldots,13\} \backslash J$	$\{2,3,9,10,13\}$
12	[1, 5]	$[13, 9]\zeta^9$	$\{0,\ldots,13\} \backslash J$	$\{0,3,4,10,11\}$

TABLE IV

RS(11,3): PAIRS OF QUADRATIC POLYNOMIALS, NINE POSITIONS I WHERE THEY REDUCE BANDWIDTH, AND FIVE POSITIONS J IN WHICH THEY CAN CORRECT SINGLE ERASURES

$f_0(x)$	$g_0(x)$	$g_1(x)$	J	(g_0, g_1)
[13]	[0, 10]	[5, 6] ζ^8	$J_1 \backslash \{4, 13\}$: $2, 7, 9, 12$	C1
[0]	[1, 11]	[6, 7] ζ^8	$J_2 \backslash \{5, 0\}$: $3, 8, 10, 13$	C2
[13]	[2, 12]	[6, 7] ζ^9	$J_2 \backslash \{8, 13\}$: $3, 5, 10, 0$	C5
[0]	[3, 13]	[7, 8] ζ^9	$J_3 \backslash \{9, 0\}$: $4, 6, 11, 1$	C6

TABLE V
RS(10,4): POLYNOMIALS $f_0 g_0$ AND $f_0 g_1$ REPAIR SINGLE ERASURES IN J WITH BANDWIDTH 60.

$f_0(x)$	$f_1(x)$	$g_0(x)$	$g_1(x)$	J	(g_0, g_1)
[2]	[7] ζ^{57}	[5, 6]	[1, 10] ζ^{28}	4, 12	B1
[4]	[12] ζ^{80}	[5, 6]	[1, 10] ζ^{28}	2, 7	B1
[5]	[8] ζ^{23}	[6, 7]	[2, 11] ζ^{28}	3, 10	B2
[1]	[9] ζ^{82}	[7, 8]	[3, 12] ζ^{28}	6, 11	B3
[6]	[11] ζ^{23}	[7, 8]	[3, 12] ζ^{28}	1, 9	B3
[3]	[13] ζ^{52}	[6, 7]	[1, 11] ζ^{26}	0, 8	C2
[0]	[10] ζ^{23}	[6, 7]	[2, 12] ζ^{25}	5, 13	C5

TABLE VI
RS(10,4): POLYNOMIALS $f_0 g_0, f_0 g_1, f_1 g_0, f_1 g_1$ REPAIR SINGLE ERASURES IN J WITH BANDWIDTH 56.

j	$p(x)$	$q(x)$	$r(x)$	$s(x)$	(p,q)	(r,s)
0	[3, 1, 5]	[3, 9, 13]ζ^{77}	[1, 3, 12]ζ^{253}	[1 ,7, 8]ζ^{140}	C12	B3
	[3, 1, 5]ζ^{85}	[3, 9, 13]ζ^{162}	[9, 3, 12]ζ^{80}	[9, 7, 8]ζ^{52}	C12	B3
1	[3, 4, 8]	[3, 0, 12]ζ^{2}	[0, 3, 12]ζ^{63}	[0, 7, 8]ζ^{35}	B4	B3
2	[12, 5, 9]	[12, 1, 13]ζ^{2}	[4, 5, 9]ζ^{3}	[4, 1, 13]ζ^{5}	B5	B5
3	[11, 1, 5]	[11, 9, 13]ζ^{77}	[13, 1, 11]ζ^{80}	[13, 6, 7]ζ^{139}	C12	C2
4	[10, 1, 5]	[10, 9, 13]ζ^{77}	[9, 3, 12]	[9, 7, 8]ζ^{57}	C12	B3
5	[8, 2, 9]	[8, 1, 12]ζ^{21}	[3, 2, 9]ζ^{62}	[3, 1, 12]ζ^{83}		
6	[4, 10, 12]	[4, 7, 8]ζ^{62}	[2, 4, 12]ζ^{3}	[2, 1, 3]ζ^{80}	C10	
7	[9, 1, 3]	[9, 5, 6]ζ^{55}	[11, 10, 12]ζ^{60}	[11, 1, 9]ζ^{80}	C7	
8	[5, 4, 11]	[5, 1, 12]ζ^{23}	[10, 4, 11]ζ^{57}	[10, 1, 12]ζ^{80}		
9	[3, 0, 4]	[3, 8, 12]ζ^{77}	[4, 1, 10]	[4, 5, 6]ζ^{57}	C11	B1
10	[2, 0, 4]	[2, 8, 12]ζ^{77}	[0, 2, 12]ζ^{80}	[0, 6, 7]ζ^{55}	C11	C5
11	[1, 4, 8]	[1, 0, 12]ζ^{2}	[9, 4, 8]ζ^{80}	[9, 0, 12]ζ^{82}	B4	B4
12	[10, 5, 9]	[10, 1, 13]ζ^{2}	[13, 1, 10]ζ^{63},	[13, 5, 6]ζ^{35}	B5	B1
13	[10, 0, 4]	[10, 8, 12]ζ^{77}	[12, 1, 10]ζ^{252}	[12, 5, 6]ζ^{139}	C11	B1
	[10, 0, 4]ζ^{85}	[10, 8, 12]ζ^{162}	[4, 1, 10]ζ^{87}	[4, 5, 6]ζ^{59}	C11	B1

TABLE VII
RS(10,4): POLYNOMIALS p, q, r, s, REPAIR ERASURES IN j WITH BANDWIDTH 54.