Permutation Decoding the Binary Images of Certain Double-Parity Reed-Solomon Codes

Fabian Lim[1], Marc Fossorier[2], and Aleksandar Kavčić[1]
[1]EE Department, University of Hawaii at Manoa, Honolulu, HI 96822
[2]ETIS ENSEA/UCP/CNRS UMR-8051, 6 avenue du Ponceau, 95014, Cergy Pontoise, France
flim@hawaii.edu, mfossorier@ieee.org, alek@hawaii.edu

***Abstract*—We introduce two permutation decoder designs for the binary images of double-parity $[n, n-2, 3]$ Reed-Solomon (RS) codes over binary extension fields $\mathbb{F}_{2^m}$. The codes considered are limited to have zeros $\{1, \alpha\}$, where α is any primitive element in $\mathbb{F}_{2^m}$. We show that there exists a large set of m binary symbol errors that may be corrected via permutation decoding. The permutation decoders are shown to achieve near maximum-likelihood decoder performance, while only utilizing simple ideas borrowed from well-known reliability-based decoding algorithms.**

I. Introduction

The automorphism group of a code contains all possible permutations (that act on code symbol positions) which send codewords to other codewords. For example, any cyclic permutation is a code automorphism of a cyclic code, and also any permutation of code symbols leaves invariant a single parity check codeword. Another well-known example is the binary Golay code, which has a Mathieu group [1] as its automorphism group. The automorphism group may be utilized in ways to aid decoding of codes, for example in the well-known *error-trapping decoding* of cyclic codes [1], and in Kasami's work on *covering polynomials* [1].

Lacan and Delpeyroux derived an automorphism subgroup for the q-ary images of a family of Reed-Solomon (RS) codes with double parity symbols [2], and proposed a permutation decoding algorithm. Lim et. al. [3] went on to obtain a larger automorphism group for the binary images of this class of codes. There are however no results so far that show how to utilize these automorphisms efficiently in permutation decoders. For example in [2], a brute force approach was used to identify useful permutations for each decoding instance, which very quickly becomes inefficient for large code lengths.

The aim of this paper is to present two low complexity permutation decoding algorithms for the binary image of certain double parity RS codes. We first begin by clarifying the concept of permutation decoding for the RS binary image in Section II. The structure of these codes are next described in Section III. Two permutation decoders A and B are described in Sections IV and V, respectively. We conclude in Section VI.

II. Permutation Decoding

Let $\mathbb{F}_{2^m}$ be the Galois field of size 2^m, and let α be a *fixed* primitive element in the field. Let the codelength be $n = 2^m - 1$. Let $\mathbf{c} = [c_0, c_1, \cdots, c_{n-1}]^T$ denote a RS codeword in vector form. RS codes can be viewed as ideals in the ring $\mathcal{R}_{2^m} = \mathbb{F}_{2^m}[x]/(x^n - 1)$, and we interchangeably refer to codeword vectors $\mathbf{c}$ as polynomials $c(x) = \sum_{j \in \mathbb{Z}_n} c_j x^j$. We consider only *double-parity* $[n, n-2, 3]$ RS codes over $\mathbb{F}_{2^m}$ with zeros $\{1, \alpha\}$. Let $\mathbb{Z}_n$ denote the integers modulo n. Note that $\mathbb{Z}_n$ indexes a codeword in both forms $\mathbf{c}$ and $c(x)$.

This work was supported by the NSF under grant number ECCS07-25649.

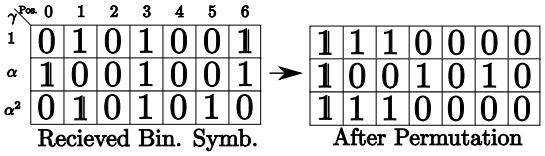

Fig. 1. Example of permutation decoding. Each column represents a $\mathbb{F}_{2^3}$ symbol in binary notation. Erroneous binary symbols are marked in bold.

Definition 1. *Let $\gamma = [\gamma_1, \gamma_2, \cdots, \gamma_m]^T$ be a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. The **binary image** of a $[n, n-2, 3]$ RS code is obtained by representing every codeword $\mathbf{c}$ as a $m \times n$ binary matrix*

$$\mathcal{B}_M(\mathbf{c}) \triangleq \begin{bmatrix} c_{[1,0]} & c_{[1,1]} & c_{[1,2]} & \cdots & c_{[1,n-1]} \\ c_{[2,0]} & c_{[2,1]} & c_{[2,2]} & \cdots & c_{[2,n-1]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{[m,0]} & c_{[m,1]} & c_{[m,2]} & \cdots & c_{[m,n-1]} \end{bmatrix},$$

where $c_j \triangleq \sum_{i=1}^m c_{[i,j]} \cdot \gamma_i$ for all $j \in \mathbb{Z}_n$. Alternatively, we may represent every polynomial form codeword $c(x)$ as a length-m vector

$$\mathcal{B}_P(\mathbf{c}) \triangleq [c^{(1)}(x), c^{(2)}(x), \cdots, c^{(m)}(x)]^T$$

of binary polynomials $c^{(i)}(x) \triangleq \sum_{j \in \mathbb{Z}_n} c_{[i,j]} x^j \in \mathcal{R}_2$.

A permutation ρ acting on the set $\mathbb{Z}_n$ is a bijective mapping $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$. Permutations act on binary polynomials $b(x) = \sum_{j \in \mathbb{Z}_n} b_j x^j \in \mathcal{R}_2$ by acting on the set $\mathbb{Z}_n$. Here we use cycle notation (e.g. the permutation $\rho = (2, 5, 3)$ denotes $\rho(2) = 5$, $\rho(5) = 3$, $\rho(3) = 2$, and $\rho(i) = i$ for $i \notin \{2, 5, 3\}$).

The RS binary image permutation decoder described in [2] is illustrated here using a simple example. Each codeword $\mathbf{c}$ is transmitted over a *binary-input channel* via its binary image $\mathcal{B}_M(\mathbf{c})$. We consider a (double-parity) 1-symbol correcting RS code over $\mathbb{F}_{2^3}$ with zeros $\{1, \alpha\}$ and let α satisfy $\alpha^3 = \alpha + 1$. We choose the basis $\gamma = [1, \alpha, \alpha^2]^T$. Let the RS codeword $\mathbf{c} = [0, 1, 0, \alpha^5, 0, \alpha^2, \alpha]^T$ be transmitted in its (polynomial form) binary image $\mathcal{B}_P(\mathbf{c}) = [x + x^3, x^3 + x^6, x^3 + x^5]^T$ (see Def. 1). A total of 3 bits were received in error and marked in

$\mathbb{F}_{2^m}$	Vector $\mathbf{u}$	Prim. elem. α	Trace dual basis $\gamma^{\perp}$
$\mathbb{F}_{2^3}$	$[2,1,0]^T$	$\alpha^3=\alpha+1$	$[1,\alpha^2,\alpha]^T$
$\mathbb{F}_{2^4}$	$[2,1,0,14]^T$	$\alpha^4=\alpha+1$	$[\alpha^{-1},\alpha^2,\alpha,1]^T$
$\mathbb{F}_{2^5}$	$[30,29,28,27,26]^T$	$\alpha^5=\alpha^2+1$	$[\alpha^{-5},\alpha^{-6},\alpha^{-2},\alpha^{-3},\alpha^{-4}]^T$
$\mathbb{F}_{2^6}$	$[4,3,2,1,0,62]^T$	$\alpha^6=\alpha+1$	$[\alpha^{-1},\alpha^4,\alpha^3,\alpha^2,\alpha^1,1]^T$

TABLE I
$\mathbf{u}$ VECTORS COMPUTED FOR $\gamma=[1,\alpha,\cdots,\alpha^{m-1}]^T$.

bold in Figure 1. Now permute the three elements of $\mathcal{B}_P(\mathbf{c})$ (corresponding to the 3 rows in Fig. 1) by $(0,4,6)(2,5,3)$, and $(1,4,2)(3,5,6)$, and $(0,3,1)(2,4,5)$, respectively. Observe that all the erroneous bits get permuted into the first symbol (see Figure 1). Furthermore, the binary image $\mathcal{B}_P(\mathbf{c})$ is permuted to $\mathcal{B}_P(\mathbf{c}')=[x+x^2,x^3+x^5,x+x^2]^T$, where $\mathbf{c}'=[0,\alpha^6,\alpha^6,\alpha,0,\alpha,0]^T$ can be verified to also have zeros $\{1,\alpha\}$ (and is thus also a codeword). This implies that decoding may be performed in the permuted order, in which all 3 binary errors now appear in the same symbol and are therefore all correctable by a hard decision decoder (HDD).

III. Binary Images of Double-Parity RS Codes

In this section we briefly look at the structure of the double-parity RS $[n,n-2,3]$ binary image parity-check matrix. Our presentation is sparse and further discussions on this topic can be found in [2], [3], [4], [5], [6]. Our aim is to convey the following 2 important facts (regarding the binary image structure): i) The relation to a smaller length-n binary code (denoted here as $\langle\theta_{\check{\alpha}}(x)\rangle$). ii) Parameterization by a special vector $\mathbf{u}\in\mathbb{Z}_n^m$ that depends on α and the basis γ.

For notational convenience, we denote $\check{\alpha}\stackrel{\triangle}{=}\alpha^{-1}$. For all $\beta\in\mathbb{F}_{2^m}$, define the set of conjugates as $\mathcal{C}(\beta)=\{\beta,\beta^2,\cdots,\beta^{|\mathcal{C}(\beta)|-1}\}$. The parity-check matrix of the double-parity RS $[n,n-2,3]$ binary image, is represented[1] by the following $2m\times m$ matrix with entries in $\mathcal{R}_2$ (see [2], [4])

$$\begin{bmatrix} \theta_1(x) & 0 & \cdots & 0 \\ 0 & \theta_1(x) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \theta_1(x) \\ \theta_{\check{\alpha}}(x)x^{u_1} & \theta_{\check{\alpha}}(x)x^{u_2} & \cdots & \theta_{\check{\alpha}}(x)x^{u_m} \\ \vdots & \vdots & & \vdots \\ \theta_{\check{\alpha}}(x)x^{u_1+m-1} & \theta_{\check{\alpha}}(x)x^{u_2+m-1} & \cdots & \theta_{\check{\alpha}}(x)x^{u_m+m-1} \end{bmatrix} \quad (1)$$

where $u_i\in\mathbb{Z}_n$, and $\theta_\beta(x)$ is a polynomial that satisfies

$$\begin{array}{lll} \theta_\beta(x)=1 & \text{for all} & x\in\mathcal{C}(\beta) \\ \theta_\beta(x)=0 & \text{for all} & x\notin\mathcal{C}(\beta) \end{array} \quad (2)$$

In particular, the polynomial $\theta_1(x)$ equals $\theta_1(x)=1+x+x^2+\cdots+x^{n-1}$ [1]. The constants $\mathbf{u}=[u_1,u_2,\cdots,u_m]$ are determined as follows: the polynomial

$$\theta_{\check{\alpha}}(x)\cdot\prod_{\beta\in\mathcal{C}(\check{\alpha})\setminus\check{\alpha}}(x-\beta) \quad (3)$$

is reduced via the trace dual basis [1], [4] of γ (denoted $\gamma^{\perp}$)

$$\theta_{\check{\alpha}}(x)\left(b_1(x)\gamma_1^{\perp}+\cdots+b_m(x)\gamma_m^{\perp}\right), \quad (4)$$

[1]Let the map $\phi:\mathcal{R}_2\to\mathbb{F}_2^n$ satisfy $\phi(b(x))=[b_0,b_1,\cdots,b_{n-1}]^T$. Any binary image codeword $\mathcal{B}_P(\mathbf{c})$ (see Def. 1) satisfies $\sum_{i=1}^m\phi(c^{(i)}(x))^T\phi(b^{(i)}(x))=0$ for any row $[b^{(1)}(x),\cdots,b^{(m)}(x)]$ of (1).

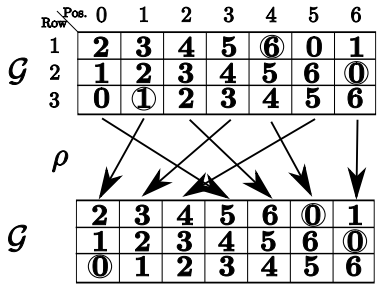

Fig. 2. Automorphism diagram of $g\in\mathcal{P}^{(1)}$ that sends $\mathbf{j}=[6,0,1]^T$ to the 0-th symbol.

where each polynomial $b_i(x)\neq 0$ is binary, and has degree at most $m-1$ [2].

Proposition 1 ([1], Thm. 9, p. 225)**.** *For any primitive $\alpha\in\mathbb{F}_{2^m}$, the polynomial $\theta_{\check{\alpha}}(x)$ generates an ideal in $\mathcal{R}_2$ (therefore a length-n cyclic code) $\langle\theta_\beta(x)\rangle$. The elements in $\langle\theta_{\check{\alpha}}(x)\rangle\setminus\{0\}$ consist of all $n=2^m-1$ cyclic shifts of $\theta_{\check{\alpha}}(x)$*

By Prop. 1 every $\theta_{\check{\alpha}}(x)b_i(x)$ in (4) can be written as $\theta_{\check{\alpha}}(x)b_i(x)=\theta(x)x^{u_i}$ for some $u_i\in\mathbb{Z}_n$. Table I shows the $\mathbf{u}$ vectors computed for various fields $\mathbb{F}_{2^m}$.

IV. Permutation Decoder Algorithm A

In this section, we first show that the code automorphisms found in [3] can be easily described by a matrix $\mathcal{G}$ related to the special vector $\mathbf{u}\in\mathbb{Z}_n^m$ (obtained in the previous section). A permutation on the binary image codeword $\mathcal{B}_M(\mathbf{c})$ acts on the matrix index set $\mathcal{I}\stackrel{\triangle}{=}\{[i,j]:1\le i\le m,j\in\mathbb{Z}_n\}$ (see Def. 1). For the obtained $\mathbf{u}$ (see (1) and Table I), define the $m\times n$ matrix $\mathcal{G}$ that has elements $\mathcal{G}_{[i,j]}=j+u_i\in\mathbb{Z}_n$. Let $Aut\left(\langle\theta_{\check{\alpha}}(x)\rangle\right)$ denote the automorphism group of $\langle\theta_{\check{\alpha}}(x)\rangle$.

Theorem 1 (Lim et. al. [3])**.** *Let $\mathcal{P}^{(1)}$ be a permutation group acting on the index set $\mathcal{I}$. Let every $g\in\mathcal{P}^{(1)}$ be in a one-to-one correspondence with some $\rho\in Aut\left(\langle\theta_{\check{\alpha}}(x)\rangle\right)$. For the correspondence $g\leftrightarrow\rho$, let g act on $\mathcal{B}_M(\mathbf{c})$ by sending*

$$\left[i,\mathcal{G}_{[i,j]}\right]\stackrel{g}{\to}\left[i,\mathcal{G}_{[i,\rho(j)]}\right]. \quad (5)$$

Then $\mathcal{P}^{(1)}$ is a code automorphism subgroup of the RS $[n,n-2,3]$ binary image with zeros $\{1,\alpha\}$, and $|\mathcal{P}^{(1)}|=|Aut\left(\langle\theta_{\check{\alpha}}(x)\rangle\right)|$.

Thm. 1 is modified from Prop. 2 in [3]. Thm. 1 indicates that a code automorphism $g\in\mathcal{P}^{(1)}$ of the double parity RS binary image may be constructed as follows.

Example 1. *Consider the case $\mathbb{F}_{2^3}$, and use $\mathbf{u}=[2,1,0]^T$ from Table I. Construct $\mathcal{G}$ and stack two replicas one on top of the other (see Figure 2). Pick some $\rho\in Aut\left(\langle\theta_{\check{\alpha}}(x)\rangle\right)$ (in Figure 2 we assumed $\rho=(0,3,1)(2,4,5)$). Map the columns of both replicas using the map $\rho:\mathbb{Z}_7\to\mathbb{Z}_7$ (see Figure 2).*

Equation (5) can be easily evaluated as follows. Look into some entry $\mathcal{G}_{[i,j]}$ in the top replica (eg. $\mathcal{G}_{[2,3]}=4$, see Figure 2), follow the arrow to the $\rho(j)$-th column of the bottom replica (eg. $\rho(3)=1$), and finally look into entry $\mathcal{G}_{[i,\rho(j)]}$ (eg. the image of $\mathcal{G}_{[2,3]}=4$ is $\mathcal{G}_{[2,\rho(3)]}=\mathcal{G}_{[2,1]}=2$).

Algorithm A: Permutation Decoder

Input: Observations of channel outputs $\mathbf{y}$. Parameter η. Matrix $\mathbf{S}$ and vector $\mathbf{u}$. Basis γ;
Initialize: Construct set $\mathcal{J}(\mathbf{y}, \eta)$, index grid $\mathcal{G}$, and codeword list $\mathcal{L} := \emptyset$;
Output: Most-likely codeword in list $\mathcal{L}$;

1 Perform *hard decision decoding* (HDD) on[2] $z(\mathbf{y})$;
2 **if** *HDD decoded to some codeword* $\mathbf{c}$ **then** store $\mathbf{c}$ in $\mathcal{L}$;
3 **forall** $\mathbf{j} \in \mathcal{J}(\mathbf{y}, \eta)$ **do**
4 Run Alg. 1 with inputs $\mathbf{S}$, $\mathbf{j} - \mathbf{u}$ and $-\mathbf{u}$;
5 **if** *Alg. 1 returned a permutation* $\rho \in Aut\left(\langle \theta_{\breve{\alpha}}(x) \rangle\right)$ **then**
6 Construct $\mathbf{y}^{(g)}$ by setting $y^{(g)}_{[i,\mathcal{G}_{[i,j]}]} := y_{[i,\mathcal{G}_{[i,\rho(j)]}]}$;
7 Compute $[i_0, \tau_0] = \arg \min_{[i,j] \in \mathcal{I}:\, j>0} |y^{(g)}_{[i,j]}|$;
8 Erase 0-th and τ_0-th symbol, decode $z\left(\mathbf{y}^{(g)}\right)$ to obtain codeword $\mathbf{c}^{(g)}$;
9 Permute $\mathbf{c}^{(g)}$ with g^{-1} and store in $\mathcal{L}$;
10 **end**
11 **end**

Let $\mathbf{S}$ denote a generator matrix of the code $\langle \theta_{\breve{\alpha}}(x) \rangle$ (see Prop. 1) and let $\mathbf{s}[j]$ denote its j-th column. The following first main result says that for certain choices of m binary positions, there exists some $g \in \mathcal{P}^{(1)}$ that permutes all m binary positions into a single $\mathbb{F}_{2^m}$ symbol position.

Theorem 2. *For a vector* $\mathbf{j} \in \mathbb{Z}_n^m$*, if the set of vectors* $\{\mathbf{s}[j_i - u_i] : 1 \leq i \leq m\}$ *are linearly independent, then there exists some* $g \in \mathcal{P}^{(1)}$ *that sends all positions* $[i, j_i] \xrightarrow{g} [i, 0]$ *for all* i*.*

The proof of Thm. 2 is deferred to Subsection IV-A. For any $\mathbf{j} \in \mathbb{Z}_n^m$, the $\rho \in Aut\left(\langle \theta_{\breve{\alpha}}(x) \rangle\right)$ which satisfies $\mathcal{G}_{[i,\rho(j_i)]} = 0$ for all i, may be obtained (if it exists) using only n additions in $\mathbb{F}_2^m$ (see app.). The automorphism $g \in \mathcal{P}^{(1)}$ that satisfies Thm. 2 may be then easily constructed using Thm. 1.

We state permutation decoder Alg. A for the AWGN channel. Let E_b and N_0 denote the energy per information symbol, and (single-sided) AWGN noise variance, respectively. We transmit the binary image codeword $\mathcal{B}_M(\mathbf{c})$ (see Def. 1) and receive the $m \times n$ matrix $\mathbf{y}$ of real-valued channel observations. Let $\eta \geq 1$ denote the algorithm parameter.

Definition 2. *Define the* ***error hypothesis set*** $\mathcal{J}(\mathbf{y}, \eta) \subseteq \mathbb{Z}_n^m$*. For each* $\mathbf{j} = [j_1, j_2, \cdots, j_m]^T \in \mathcal{J}(\mathbf{y}, \eta)$*, each index* $[i, j_i]$ *points to one of the* η*-smallest values in the set* $\{|y_{[i,j]}| : j \in \mathbb{Z}_n\}$*. That is for each* j_i*, there are at least* $n - \eta$ *elements in* $\{|y_{[i,j]}| : j \in \mathbb{Z}_n\}$ *that are greater than* $|y_{[i,j_i]}|$*.*

We now explain the decoding algorithm given in Algorithm A. Note that Alg. A depends on Alg. 1 (see Lines 4-5) given in the appendix. First, the symbol hard decisions[2] $z(\mathbf{y})$ are formed from the channel observations $\mathbf{y}$ and performs hard decision decoding (HDD). Each vector $\mathbf{j} = [j_1, j_2, \cdots, j_m]^T$ in the error hypothesis set $\mathcal{J}(\mathbf{y}, \eta)$ (see Def. 2), points to m binary positions $[i, j_i] \in \mathcal{I}$ that are likely to be in error. For each $\mathbf{j} \in \mathcal{J}(\mathbf{y}, \eta)$, we thus permute all m positions $[i, j_i]$ into the 0-th symbol (which is erased in Line 8). The double-parity RS allows 2 erasures. The second erased symbol is the τ_0-th symbol (see Line 7), which contains the smallest observation (absolute) value in the permuted $\mathbf{y}^{(g)}$. Note we exclude the 0-th symbol when choosing τ_0 to ensure $\tau_0 \neq 0$.

[2]The function z is a map and $z(\mathbf{y}) = [z_0, \cdots, z_{n-1}]^T$ is obtained by $z_j = \sum_{i=1}^m b_{[i,j]} \gamma_i$, where $b_{[i,j]}$ is the binary decision associated with $y_{[i,j]}$.

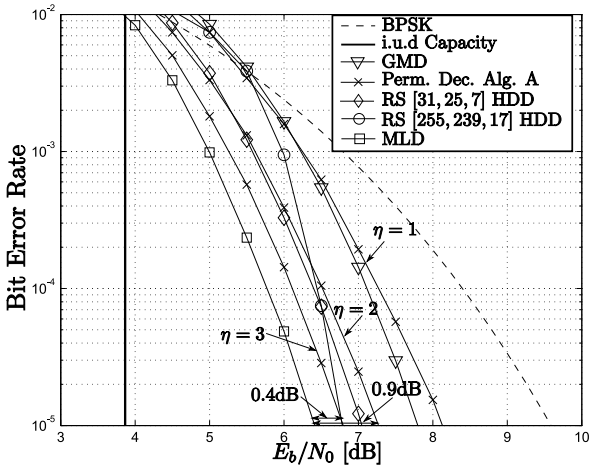

Fig. 3. Algorithm A performance for the RS $[31, 29, 3]$ binary image.

Figure 3 shows the bit error rate (BER) performance of our permutation decoder for the RS $[31, 29, 3]$ binary image, with the parameters $\eta = 1, 2$ and 3. When we choose $\eta = 1$, Algorithm A performs very close to the *generalized minimum-distance decoder* (GMD). When $\eta = 1$, the GMD slightly outperforms Alg. A because if Alg. 1 fails on Line 4, then the erasure decoding in Line 8 is not performed. We observe significant gains when we choose $\eta = 2$ and 3, with the latter case coming within 0.4dB on the maximum likelihood decoder (MLD). We also compare our performance to the HDD of 2 standard RS codes, the RS $[31, 25, 7]$ and the RS $[255, 239, 17]$. The latter code has similar rate ($239/255 \approx 29/31$) to our double-parity RS code $[31, 29, 3]$. We see that our permutation decoder performs very close to the RS $[31, 25, 7]$ HDD when we choose $\eta = 2$, and we outperforms it when we choose $\eta = 3$. Also when we choose $\eta = 3$, we outperform the HDD of the RS $[255, 239, 17]$ for all SNR values less than 6.75 dB.

A. Proof of Theorem 2

We now prove Thm. 2. The result will follow from the fact that $Aut\left(\langle \theta_{\breve{\alpha}}(x) \rangle\right)$ is isomorphic to $GL(m, 2)$, the *general linear group* over $\mathbb{F}_2$ (i.e., $GL(m, 2)$ is the matrix group that contains all $m \times m$ invertible matrices with binary entries [1]).

Proposition 2 ([1] p. 223)**.** *For any primitive* $\alpha \in \mathbb{F}_{2^m}$*, the code* $\langle \theta_{\breve{\alpha}}(x) \rangle$ *is* ***equivalent*** *to the binary* ***simplex*** *code.*

Recall the generator matrix $\mathbf{S}$ of $\langle \theta_{\breve{\alpha}}(x) \rangle$, that contains (by Prop. 2) all non-zero binary m tuples as its columns.

Proposition 3 ([1] p. 232)**.** *There is a one-to-one correspondence between an automorphism of the code generated by* $\mathbf{S}$ *and an element* $\mathbf{K} \in GL(m, 2)$*.*

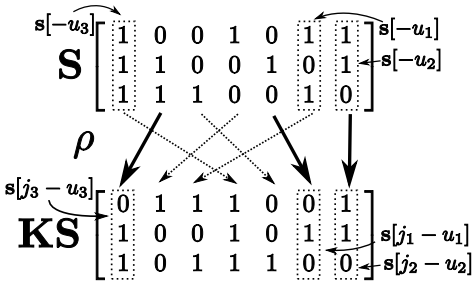

Fig. 4. Simplex automorphism that sends $\ell = [6, 0, 1]^T$ to the first symbol

Prop. 2 and 3 establish the isomorphism between $Aut\left(\langle\theta_{\breve{\alpha}}(x)\rangle\right)$ and $GL(m, 2)$. It can be verified that if $\mathbf{K} \leftrightarrow \rho$ then $\mathbf{Ks}[\rho(j)] = \mathbf{s}[j]$ for all $j \in \mathbb{Z}_n$. We require the following lemma (its proof will appear in a future journal version [7]).

Lemma 1. *Recall* $\mathbf{u}$ *(see Section III). The set of vectors* $\{\mathbf{s}[-u_i] : 1 \le i \le m\}$ *are linearly independent.*

Proof of Thm. 2: For a chosen $\mathbf{j} \in \mathbb{Z}_n^m$*, we want some* $\rho \in Aut\left(\langle\theta_{\breve{\alpha}}(x)\rangle\right)$ *that satisfies* $\rho(j_i - u_i) = -u_i$ *for all* i*, then by Thm. 1 there must exist some* $g \in \mathcal{P}^{(1)}$ *that sends all m binary positions* $[i, j_i] \xrightarrow{g} [i, 0]$*. From Prop. 3, that particular* $\mathbf{K} \in \mathbb{F}_{2^m}$ *corresponding to* ρ *will satisfy* $\mathbf{Ks}[\rho(j_i - u_i)] = \mathbf{s}[j_i - u_i]$ *for all* i*. By substituting* $\rho(j_i - u_i) = -u_i$ *(as required by the permutation* ρ *of interest), we require*

$$\mathbf{Ks}[-u_i] = \mathbf{s}[j_i - u_i] \text{ for } 1 \le i \le m. \tag{6}$$

By Lemma 1, there must exist some $\mathbf{K}$ *that satisfies (6) if* $\{\mathbf{s}[-u_i] : 1 \le i \le m\}$ *are linearly independent.* ∎

Example 2. *We now verify that* $\rho = (0, 3, 1)(2, 4, 5)$ *is indeed in* $Aut\left(\langle\theta_{\breve{\alpha}}(x)\rangle\right)$ *(as assumed in Example 1). Figure 4 shows some chosen* $\mathbf{S}$ *and the columns* $\mathbf{s}[-u_i]$ *are marked (recall* $\mathbf{u} = [2, 1, 0]^T$*). From Example 1 recall that* $\mathbf{j} = [6, 0, 1]^T$*. From Figure 4 we verify that all* $\mathbf{s}[j_i - u_i]$ *are linearly independent. Thus by Thm. 2 we find* $\mathbf{K}$ *that satisfies (6) and obtain the column permuted version* $\mathbf{KS}$ *of* $\mathbf{S}$ *(see Figure 4).*

The size $|Aut\left(\langle\theta_{\breve{\alpha}}(x)\rangle\right)| = |GL(m, 2)| = \prod_{r=0}^{m-1}(2^m - 2^r)$ (follows from counting the number of ways to construct invertible $m \times m$ binary matrices, see [1]). We have $\prod_{r=0}^{m-1}(2^m - 2^r) = (n+1)^m \cdot \prod_{r=1}^{m}(1 - 2^{-r})$. Thus, the fraction of location choices $\mathbf{j} \in \mathbb{Z}_n^m$ (a total of n^m of them) that can be sent to the 0-th symbol, is approximately $\prod_{r=1}^{m}(1 - 2^{-r})$. For large m, the fraction converges to roughly 0.289.

V. Permutation Decoding Algorithm B

In this section we extend Alg. A by selecting from a larger code automorphism subgroup. We show that for some $\mathbf{j} \in \mathbb{Z}_n^m$, there exists a variety of $m!$ automorphisms (in the larger group) that send all $[i, j_i]$ into the 0-th symbol. Define Ω_m to be the group of all permutations on the set $\{1, 2, \cdots, m\}$. We begin with the following result [2], [3].

Theorem 3 (Lacan et. al. [2])**.** *Let* $\mathcal{P}^{(2)}$ *be a permutation group acting on the index set* $\mathcal{I}$*. Let every* $h \in \mathcal{P}^{(2)}$ *be in a one-to-one correspondence with some* $\sigma \in \Omega_m$*. For the correspondence* $h \leftrightarrow \sigma$*, let* h *act on* $\mathcal{B}_M(\mathbf{c})$ *by sending the index* $[i, j] \in \mathcal{I}$ *to* $\left[\sigma(i), j - u_i + u_{\sigma(i)}\right]$*. Then* $\mathcal{P}^{(2)}$ *is a subgroup of code automorphisms of the RS* $[n, n-2, 3]$ *binary image with zeros* $\{1, \alpha\}$*, and* $|\mathcal{P}^{(2)}| = m!$*.*

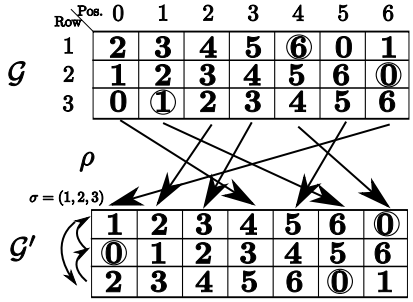

Fig. 5. Automorphism diagram of $gh \in \mathcal{P}^{(1)}\mathcal{P}^{(2)}$ that sends $\mathbf{j} = [6, 0, 1]^T$ to the 0-th symbol.

Let $\mathcal{P}^{(1)}\mathcal{P}^{(2)} \triangleq \{gh | g \in \mathcal{P}^{(1)}, h \in \mathcal{P}^{(2)}\}$ denote the *product group* of $\mathcal{P}^{(1)}$ and $\mathcal{P}^{(2)}$. Define the matrix $\mathcal{G}'$, with entries $\mathcal{G}'_{[i,j]} = \mathcal{G}_{[\sigma(i),j]}$. The following proposition may be easily shown using both Thm. 1 and 3.

Proposition 4. *Let* $gh \in \mathcal{P}^{(1)}\mathcal{P}^{(2)}$ *and* $\sigma \in \Omega_m$ *and* $\rho \in Aut\left(\langle\theta_{\breve{\alpha}}(x)\rangle\right)$ *correspond as* $g \leftrightarrow \rho$ *and* $h \leftrightarrow \sigma$*. Let* $\mathcal{G}$ *denote the index grid. Then* gh *permutes the indicies in* $\mathcal{I}$ *as*

$$\left[i, \mathcal{G}_{[i,j]}\right] \xrightarrow{gh} \left[\sigma(i), \mathcal{G}_{[\sigma(i),\rho(j)]}\right] = \left[\sigma(i), \mathcal{G}'_{[i,\rho(j)]}\right]. \tag{7}$$

Example 3. *Figure 5 shows a different automorphism (than that shown in Example 2 and Figure 2) that sends* $\mathbf{j} = [6, 0, 1]^T$ *to the* 0*-th symbol position. In Figure 5, the automorphism is taken from* $\mathcal{P}^{(1)}\mathcal{P}^{(2)}$*. As it was shown in Example 2, Equation (7) can be similarly evaluated using the diagram in Figure 5.*

Theorem 4. *Assume that the set of columns* $\{\mathbf{s}[j_i - u_i] : 1 \le i \le m\}$ *are linearly independent. Then for any* $h \in \mathcal{P}^{(2)}$*, there exist some* $g \in \mathcal{P}^{(1)}$*, such that* gh *sends the positions* $\mathbf{j}$ *to the* 0*-th symbol position.*

Proof: From (7), the image of $[i, j_i] = \left[i, \mathcal{G}_{[i,j_i-u_i]}\right]$ *under some* $gh \in \mathcal{P}^{(1)}\mathcal{P}^{(2)}$ *equals* $\left[\sigma(i), \mathcal{G}_{[\sigma(i),\rho(j_i-u_i)]}\right]$*, where* ρ *and* σ *correspond to* $g \in \mathcal{P}^{(1)}$ *and* $h \in \mathcal{P}^{(2)}$*, respectively. To send positions* $\mathbf{j}$ *to the* 0*-th symbol position, we require* $\mathcal{G}_{[\sigma(i),\rho(j_i-u_i)]} = 0$ *for all* $i \in \{1, 2, \cdots, m\}$*, or equivalently* $\rho(j_i - u_i) = -u_{\sigma(i)}$ *for all* $i \in \{1, 2, \cdots, m\}$*. Hence we require some* $\rho \in Aut\left(\langle\theta_{\breve{\alpha}}(x)\rangle\right)$ *and a corresponding* $\mathbf{K} \in GL(m, 2)$ *that satisfies*

$$\mathbf{s}[j_i - u_i] = \mathbf{Ks}[\rho(j_i - u_i)] = \mathbf{Ks}[-u_{\sigma(i)}] \tag{8}$$

(the first equality follows because if $\rho \leftrightarrow \mathbf{K}$*, then* $\mathbf{Ks}[\rho(j)] = \mathbf{s}[j]$ *for all* $j \in \mathbb{Z}_n$*). By our assumption that* $\{\mathbf{s}[j_i - u_i] : 1 \le i \le m\}$ *are linearly independent and by Lemma 1, there must exist a* $\mathbf{K}$ *that satisfies (8). Thus we are done* ∎

Corollary 1. *Assume there exists some* $g' \in \mathcal{P}^{(1)}$ *that sends the positions* $\mathbf{j}$ *to the* 0*-th symbol position. Then there exists* $m!$ *unique automorphisms* $gh \in \mathcal{P}^{(1)}\mathcal{P}^{(2)}$ *that send the positions* $\mathbf{j}$ *to the* 0*-th symbol position.*

Alg. B has a new parameter $\kappa \ge 0$ in addition to η (see Alg. A). It can be checked that when $\kappa = 0$ both Alg. A and B are equal. In Lines 7 and 10 the erased

Algorithm B: Permutation Decoder

Input: Param. η and κ. Matricies $\mathbf{y}$ and $\mathbf{S}$. Also $\mathbf{u}$ and γ;
Initialize: Construct $\mathcal{J}(\mathbf{y}, \eta)$, grid $\mathcal{G}$, and $\mathcal{L} := \emptyset$;
Initialize: Collection of sets $\mathcal{T} := \emptyset$;
Output: Most-likely codeword in list $\mathcal{L}$;

1 Perform Lines 1-2 of Alg. A;
2 **forall** $\mathbf{j} \in \mathcal{J}(\mathbf{y}, \eta)$ **do**
3 **forall** $\sigma \in \Omega_m$ **do**
4 Run Alg. 1 with $\mathbf{S}$, $\mathbf{j} - \mathbf{u}$, $-[u_{\sigma(1)}, \cdots, u_{\sigma(m)}]^T$;
5 **if** *Alg. 1 returned invalid perm.* ρ **then break**;
6 Construct $\mathbf{y}^{(gh)}$ as $y^{(gh)}_{[\sigma(i), \mathcal{G}_{\sigma(i),\rho(j)}]} := y_{[i,\mathcal{G}_{i,j}]}$;
7 Compute $[i_0, \tau_0] = \arg \min_{[i,j] \in \mathcal{I}:\, j>0} |y^{(gh)}_{[i,j]}|$;
8 Compute $\tau_1, \cdots, \tau_k$ that satisfy (9);
9 **if** $\{i : 1 \le i \le \kappa, \tau_i = \tau_0\} \notin \mathcal{T}$ **then**
10 Erase 0-th and τ_0-th symbol, decode $z\left(\mathbf{y}^{(gh)}\right)$ to obtain codeword $\mathbf{c}^{(gh)}$;
11 Permute $\mathbf{c}^{(gh)}$ with $h^{-1}g^{-1}$ and store in $\mathcal{L}$;
12 Store $\{i : 1 \le i \le \kappa, \tau_i = \tau_0\}$ in $\mathcal{T}$;
13 **end**
14 **if** $|\mathcal{T}| = 2^\kappa$ **then break**;
15 **end**
16 **end**

symbol positions (0 and τ_0) are the same as those in Alg. A Lines 7-8. However in Line 8, for each $gh \in \mathcal{P}^{(1)}\mathcal{P}^{(2)}$ we obtain κ additional symbol locations $\tau_1, \tau_2, \cdots, \tau_\kappa$ satisfying

$$|y^{(gh)}_{[i_0,\tau_0]}| \le |y^{(gh)}_{[i_1,\tau_1]}| \le \cdots \le |y^{(gh)}_{[i_\kappa,\tau_\kappa]}| \overset{(a)}{\le} |y^{(gh)}_{[i,j]}| \tag{9}$$

where inequality (a) is satisfied for all values (excluding those to the left of (a)) in the set $\{|y^{(gh)}_{[i,j]}| : [i,j] \in \mathcal{I}, j > 0\}$. That is, $[i_0, \tau_0], \cdots, [i_\kappa, \tau_\kappa]$ index the $\kappa + 1$ lowest reliable binary symbols (excluding the 0-th symbol).

In Lines 3-15, we search through the $m!$ permutations that satisfy Cor. 1. The check on Line 9 prevents repetitive decoding. Each set in $\mathcal{T}$ records which combination of κ symbols $[i_1, \tau_1], \cdots, [i_\kappa, \tau_\kappa]$ have been erased together with $[i_0, \tau_0]$. The maximal number of erasure decodings within the loop in Lines 3-15 is limited by the check in Line 14 to 2^κ.

Figure 6 shows the performance of Alg. B for the RS $[63, 61, 3]$ code. Figure 6 suggests that Alg. B with parameters η and κ achieves performance in between that of Alg. A with parameters η and $\eta + 1$. The gain of $\eta = 2, \kappa = 2$ over (Alg. A) $\eta = 2, \kappa = 0$ is approximately 0.15dB at BER=10^{-5}, and the gain of $\eta = 2, \kappa = 2$ over (Alg. A) $\eta = 2, \kappa = 0$ is approximately 0.1dB at BER=10^{-5}.

VI. Conclusion

In this paper, we discussed two permutation decoders for certain double-parity RS binary images with zeros $\{1, \alpha\}$. For these codes over $\mathbb{F}_{2^m}$, we showed there exists at least $\prod_{r=0}^{m-1}(2^m - 2^r)$ number of m binary error patterns, that may be corrected using automorphisms. Simulation results show significant gain over HDD and GMD decoding, and near MLD performance can be achieved. Due to the high-rate of the RS codes, only these three references were considered.

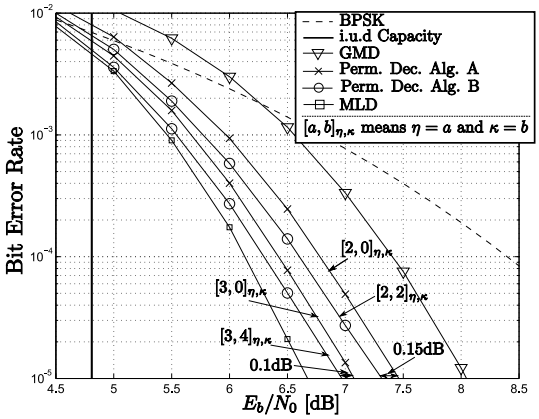

Fig. 6. Performance of Alg. B for the RS $[63, 61, 3]$ binary image.

Appendix

Algorithm 1: Computing a simplex automorphism

Input: Matrix $\mathbf{S}$ and vectors $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_n^m$
Output: The permutation ρ if valid.
Initialize: Set $\rho(j) := -1$ for all $j \in \mathbb{Z}_n$

1 **forall** $i = 1$ **to** m **do**
2 **forall** $j \in \mathbb{Z}_n$ *s.t.* $\rho(j) \neq -1$ **do**
3 **if** $\mathbf{s}[a_i] + \mathbf{s}[j] = \mathbf{0}$ **then quit**;
4 **if** $\mathbf{s}[b_i] + \mathbf{s}[\rho(j)] = \mathbf{0}$ **then quit**;
5 Set $j' := \varphi\left(\mathbf{s}[a_i] + \mathbf{s}[j]\right)$;
6 Set $\rho(j') := \varphi\left(\mathbf{s}[b_i] + \mathbf{s}[\rho(j)]\right)$;
7 **end**
8 Set $\rho(a_i) := b_i$;
9 **end**

Alg. 1 computes $\rho \in Aut\left(\langle \theta_{\check{\alpha}}(x) \rangle\right)$ that sends $\rho(a_i) = b_i$ for all $i \in \{1, 2, \cdots, m\}$. Alg. 1 may return an invalid permutation (i.e. a permutation that maps $\rho(j) = -1$ for some $j \in \mathbb{Z}_n$) if Thm. 2 and 4 are not satisfied. Note that $\varphi : \mathbb{F}_2^m \setminus \{\mathbf{0}\} \mapsto \mathbb{Z}_n$ maps the (unique) columns of $\mathbf{S}$ to their column indexes (i.e. if we have $\mathbf{s}[j] = \nu$, then we have $\varphi(\nu) = j$).

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. Amsterdam, The Netherlands: North-Holland, 1983.

[2] J. Lacan and E. Delpeyroux, "The q-ary image of some q^m-ary cyclic codes: Permutation group and soft-decision decoding," *IEEE Trans. on Inform. Theory*, vol. 48, no. 7, pp. 2069–2078, Jul. 2002.

[3] F. Lim, M. P. Fossorier, and A. Kavčić, "Notes on the automorphism groups of Reed-Solomon binary images," in *Proc. IEEE International Symposium on Inform. Theory (ISIT' 08)*, Toronto, Canada, Jul. 2008, pp. 1813–1817.

[4] G. E. Seguin, "The q-ary image of a q^m-ary cyclic code," *IEEE Trans. on Inform. Theory*, vol. 41, no. 2, pp. 387–399, Mar. 1995.

[5] K. Sakakibara, K. Tokiwa, and M. Kasahara, "Notes on q-ary expanded Reed-Solomon codes over GF(q^m)," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 72, no. 2, pp. 14–23, 1989.

[6] A. Vardy and Y. Be'ery, "Bit level soft-decision decoding of Reed-Solomon codes," *IEEE Trans. on Inform. Theory*, vol. 39, no. 3, pp. 440–444, 1991.

[7] F. Lim, M. P. Fossorier, and A. Kavčić, "Code automorphisms and permutation decoding of certain Reed-Solomon binary images," *Submitted to IEEE Trans. on Inform. Theory*.