Notes on the Automorphism Groups of Reed Solomon Binary Images

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, mfossorier2@yahoo.com, alek@hawaii.edu

***Abstract*—In this paper, a new proof of the work by Lacan et. al is obtained. This approach led to newly discovered connections between the automorphism group of the Reed Solomon (RS) binary image, and elementary group theory. This new development facilitated proving the existence and constructing permutations that have not been previously reported in the literature. Simple special cases are then considered in this work.**

I. Introduction

The automorphism group of a code can be used for many purposes, such as finding the weight distribution of a code [1], decoding [1], [2], etc. Thus, there has been vested interest in understanding the properties of such groups. Cyclic codes, and more particularly Reed-Solomon (RS) codes are widely popular in many applications. Also, the binary-images of RS codes are of particular interest, for transmission over practical communication systems. The structure of the binary-image of a cyclic code has been widely studied [1], [2], [3], [4], and it has been shown that it is possible to derive automorphism groups from these structures [2], [3].

In this paper, we study the automorphism group of binary images of RS codes, and point out some interesting observations. In a particular case previously studied by Lacan et. al. [2], we derive an alternate proof, and establish that the automorphism groups of these particular codes are connected to a set of (properly *conjugated*) permutations belonging to the automorphism group of a related *minimal cyclic code*. It follows from the new proof, that a larger group than what was reported by Lacan et. al [2]. can be easily obtained. Note that we do not attempt to address *cyclic* permutations of the binary images, as was done previously by Seguin [3].

II. Background

We focus on extending the theory developed by Lacan et. al. [2], specifically for RS binary images. The decomposition structure of RS binary images has been formulated in different ways [2], [3], [4], [5], which are essentially alike. We first review the material in [2] before stating our new results. Let $\mathcal{F}(2^m)$ be the binary extension field to the power m, and let α to be a primitive element in the field. Let $\mathcal{N}$ be a set containing the consecutive *non-zeros* of the RS code. For any $\beta \in \mathcal{F}(2^m)$, let $\mathcal{C}(\beta)$ be its cyclotomic coset over the binary field, and we denote $\theta_\beta(x)$ as the related *idempotent* [1]. We restrict the code lengths to be $n = 2^m - 1$.

In [2], Lacan et. al. presented a result for an infinite family of *cyclic* codes (not necessarily RS), whereby the set of non-zeros $\mathcal{N}$ satisfy the form $\mathcal{N} = \mathcal{V} \cup \{\alpha\}$, where $\mathcal{V}$ is defined to be a union of cyclotomic cosets. Their result specializes to an infinite family of RS codes where $\mathcal{N} = \{1\} \cup \{\alpha\}$ (Note: $\mathcal{C}(1) = \{1\}$) [2]. It is well-known that cyclic codes with non-zeros $\mathcal{V}$ (or α) forms a subcode of the code with non-zeros $\mathcal{N} = \mathcal{V} \cup \{\alpha\}$. It is shown in [2] that code automorphisms can be obtained by first analyzing the structures of the *individual* subcodes, or from the code *duals*.

For *each* cyclotomic coset $\mathcal{C}(\beta)$ in $\mathcal{V}$ where β is primitive, the binary image of the $\mathcal{N} = \mathcal{C}(\beta)$ subcode has the $mn \times m^2$ generator matrix

$$\begin{bmatrix} \mathcal{M} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathcal{M} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathcal{M} \end{bmatrix} \tag{1}$$

The $n \times m$ submatrix $\mathcal{M}$ is the generator matrix of a (binary) *minimal cyclic code*, which is generated by the idempotent $\theta_\beta(x)$ [1]. The subcode with the single primitive element $\mathcal{N} = \{\alpha\}$, has a (non-binary) generator polynomial

$$g(x) = \theta_\alpha(x) \prod_{\beta \in \mathcal{C}(\alpha) \setminus \alpha} (x - \beta) \tag{2}$$

Taking the binary image with respect to some basis of $\mathcal{F}(2^m)$ over the binary field, denoted $\{\gamma_0, \gamma_1, \cdots, \gamma_{m-1}\}$, we obtain

$$g(x) = \theta_\alpha(x) \left(b_0(x)\gamma_0 + \cdots + b_{m-1}(x)\gamma_{m-1} \right),$$

where each polynomial $b_i(x)$ is binary, and has degree at most $m-1$ (from (2) and the fact[1] $|\mathcal{C}(\alpha)| = m$). Now, $\theta_\alpha(x)b_0(x)$ belongs to the dimension m minimal cyclic code $\langle \theta_\alpha(x) \rangle$, which is isomorphic to the field $\mathcal{F}(2^m)$ [1]. Thus, there exists $u_i \in \mathbb{Z}/n$, for all $0 \le i \le m-1$ whereby $\theta_\alpha(x)b_i(x) = \theta_\alpha(x)x^{u_i}$. We conclude that the binary image of the $\mathcal{N} = \{\alpha\}$ subcode has the structure

$$\begin{bmatrix} \theta_\alpha(x)x^{u_0} & \cdots & \theta_\alpha(x)x^{u_{m-1}} \\ \vdots & & \vdots \\ \theta_\alpha(x)x^{m+u_0} & \cdots & \theta_\alpha(x)x^{m+u_{m-1}} \end{bmatrix} \tag{3}$$

This work was supported by a grant from the Information Storage Industry Consortium (INSIC).

[1]Equality follows because α is primitive

Authorized licensed use limited to: UNIV OF HAWAII LIBRARY. Downloaded on March 15, 2009 at 23:45 from IEEE Xplore. Restrictions apply.

where from (2) the vector $\mathbf{u} = [u_0, u_1, \cdots, u_{m-1}]$ is determined by the primitive element α. The matrices in (1) and (3) are $m \times m$ matrices, where the ith column of the matrix corresponds to a single basis element γ_i.

In relation to the matrix structures, we define the tuple (i, j) that indexes the ith column and the jth bit within the column. The following definition follows from [2].

Definition 1. *Let σ be a permutation of the indices $\{0, 1, \cdots, m-1\}$, and also $0 \leq l \leq m-1$ and $0 \leq a \leq n-1$. The triple (σ, l, a) describes the permutation*

$$(i, j) \rightarrow (\sigma(i), j2^l - u_i 2^l + u_{\sigma(i)} + a).$$

For now we ignore the symbol level shifts as they are not so interesting. Define id as the identity permutation on m indices. The next proposition is from [2] as well.

Proposition 1. *For any cyclic code with non-zeros $\mathcal{N} = \mathcal{V} \cup \{\alpha\}$, all permutations (σ, l, a) belong to its automorphism group.*

In relation to the matrix structures in (1) and (3), we define

Definition 2. *All permutations of the form $(\sigma, 0, 0)$ are termed column variant, while permutations generated by $(id, 1, 0)$ are termed column invariant.*

The permutations in the column variant category can be generated by all elements $(\sigma, 0, 0)$ corresponding to two column swaps, as defined as

$$\begin{array}{lcll} (i, j) & \rightarrow & (i, j) & \text{for } i \neq i', i'' \\ (i', j) & \rightarrow & (i'', j - u_{i'} + u_{i''}) & \text{for } i = i' \\ (i'', j) & \rightarrow & (i', j - u_{i''} + u_{i'}) & \text{for } i = i'' \end{array}$$

With reference to the subcode $\mathcal{N} = \{\alpha\}$, we choose an arbitrary column $\theta_\alpha(x)x^{u_{i'}+r}$, swap it to the new column $\sigma(i') = i''$, and cyclically shift by multiplying with the term $x^{-u_{i'}+u_{\sigma(i')}}$ to obtain $\theta_\alpha(x)x^{u_{i'}+r}x^{-u_{i'}+u_{\sigma i'}} = \theta_\alpha(x)x^{u_{\sigma(i')}+r}$ Observe that for codes with $\mathcal{N} = \{\alpha\} \cup \{\beta\}$, then both α and β may (very well) each have different values in their corresponding $\mathbf{u}$ vectors, and if this is the case, permutations of this form fail to invariant *both* subcodes.

For the permutations in the column invariant category, the generator $(id, 1, 0)$ is written as

$$(i, j) \rightarrow (i, 2j - u_i).$$

The proof of Proposition 1 is given in [2]. In the next section, we extend these results.

III. Constructing More Permutations for the $\mathcal{N} = \{\alpha\}$ Subcode

Here, we develop ways to construct more column invariant permutations, that also establishes a link with the automorphism group of the minimal cyclic code $\langle\theta_\alpha(x)\rangle$. From (3), each codeword in the $\mathcal{N} = \{\alpha\}$ subcode is some cyclic shift

$$\theta_\alpha(x)x^{u_0+r}, \cdots, \theta_\alpha(x)x^{u_{m-1}+r} \tag{4}$$

where $r \in \mathbb{Z}/n$. Note that $\mathbf{u} = [u_0, u_1, \cdots, u_{m-1}]$ determines the cyclic shift of the $\theta_\alpha(x)x^r$ terms in relation to each other. Define $Aut(C)$ as the automorphism group of the linear code C. For $\rho_i \in Aut(\langle\theta_\alpha(x)\rangle)$ where $0 \leq i \leq m-1$, define $[\rho_0, \rho_1, \cdots, \rho_{m-1}]$ as the *direct product*, which acts on the concatenation of $\theta_\alpha(x)$ terms (e.g. in (4)). Define c as an elementary cyclic shift to the right by one acting on n indices.

Proposition 2. *Set $G = Aut(\langle\theta_\alpha(x)\rangle)$. The binary image of the subcode with $\mathcal{N} = \{\alpha\}$ is invariant under the permutation group $[c^{-u_0}Gc^{u_0}, c^{-u_1}Gc^{u_1}, \cdots, c^{-u_{m-1}}Gc^{u_{m-1}}]$, where $\mathbf{u} = [u_0, u_1, \cdots, u_{m-1}]$ is determined by α.*

Proof: Since $\langle\theta_\alpha(x)\rangle$ is cyclic, then $c^{u_i} \in Aut(\langle\theta_\alpha(x)\rangle)$, and also $c^{-u_i}\rho c^{u_i} \in Aut(\langle\theta_\alpha(x)\rangle) \forall i$. For a given value for r, apply each permutation $c^{-u_i}\rho c^{u_i}$ to each corresponding term $\theta_\alpha(x)x^{u_i+r}$ so that

$$\theta_\alpha(x)x^{u_i+r} \overset{c^{-u_i}}{\rightarrow} \theta_\alpha(x)x^r \overset{\rho}{\rightarrow} \theta_\alpha(x)x^{r'} \overset{c^{u_i}}{\rightarrow} \theta_\alpha(x)x^{u_i+r'}$$

holds $\forall i$, and note that r' is constant for all columns. ∎

Essentially, we apply the same permutation ρ to all $\theta_\alpha(x)x^{u_i+r}$ terms, but *relative* to some u_i bit locations. For the following corollary, note that permuting $\theta(x)x^r$ by $j \rightarrow 2j$ is equivalent[2] to $(\theta(x)x^r)^2 = \theta(x)x^{2r}$. Define such a permutation by e.

Corollary 1. *Our permutation group is a supergroup of the column invariant permutations obtained by Lacan et. al. for the $\mathcal{N} = \{\alpha\}$ subcode.*

Proof: For $\rho = e$, we obtain

$$\theta_\alpha(x)x^{u_i+r} \overset{c^{-u_i}}{\rightarrow} \theta_\alpha(x)x^r \overset{e}{\rightarrow} \theta_\alpha(x)x^{2r} \overset{c^{u_i}}{\rightarrow} \theta_\alpha(x)x^{u_i+2r}.$$

Also, compare

$$j \overset{c^{-u_i}}{\rightarrow} j - u_i \overset{e}{\rightarrow} 2j - 2u_i \overset{c^{u_i}}{\rightarrow} 2j - u_i,$$

with

$$j \overset{e}{\rightarrow} 2j \overset{c^{-u_i}}{\rightarrow} 2j - u_i,$$

to see that the two permutations are the same. ∎

Remark 1. *In group theory terminology, the permutation $c^{-u_i}\rho c^{u_i}$ is a conjugate of ρ.*

Example 1. *Consider $\mathcal{F}(2^3)$, let $\alpha^3 + \alpha + 1 = 0$, and set the basis $\gamma = \{1, \alpha, \alpha^2\}$. If $\mathcal{N} = \{\alpha^6\}$, we get $\theta_{\alpha^6}(x) = x^6 + x^5 + x^3 + 1$ and $\mathbf{u} = [2, 0, 1]$. Using GAP [6], we compute $G = Aut(\langle\theta_{\alpha^6}(x)\rangle)$ of order 168 with the set of generators $\{(0,1)(4,6), (1,2)(3,6), (1,3)(4,5)\}$. Thus $\left[c^{-2}Gc^2, G, c^{-1}Gc\right]$ invariants the $\mathcal{N} = \{\alpha^6\}$ subcode and also has order 168.*

A. Re-visit of the Result by Lacan et. al. for $\mathcal{N} = \mathcal{V} \cup \{\alpha\}$

We try to relate our result to the previous result [2] by Lacan et. al.. As stated before, we define $\mathcal{V} = \bigcup_i \mathcal{C}(\beta_i)$. We note the following proposition.

Proposition 3. *If ρ is also a member of $Aut(\langle\theta_{\beta_i}(x)\rangle) \forall i$, then the binary image of $\mathcal{N} = \mathcal{V} \cup \{\alpha\}$ is invariant under the permutation $[c^{-u_0}\rho c^{u_0}, c^{-u_1}\rho c^{u_1}, \cdots, c^{-u_{m-1}}\rho c^{u_{m-1}}]$.*

[2]Since $\theta(x)$ is an idempotent [1], we have $\theta(x)^2 = \theta(x)$.

Authorized licensed use limited to: UNIV OF HAWAII LIBRARY. Downloaded on March 15, 2009 at 23:45 from IEEE Xplore. Restrictions apply.

If $\mathcal{V} = \{1\}$, then $\langle \theta_1(x) \rangle$ is the *repetition* code, which has the *symmetric group* as its automorphism group. Note that this special case includes the only infinite family of RS codes, for which permutations are known. However, if $\mathcal{V}$ does not consist of the single element 1, we must proceed cautiously.

Example 2. *From the previous example, the group* $\left[c^{-2}Gc^2, G, c^{-1}Gc\right]$ *invariants the binary image of the* [7,2,6] *RS code with* $\mathcal{N} = \{1, \alpha^6\}$*, and its dual, the narrow-sense* [7,5,3] *RS code, imaged under the trace-dual basis* [1].

IV. Notes on Subcodes with $\mathcal{N} = \mathcal{C}(\alpha') \cup \{\alpha\}$.

Following our discussion on Proposition 3, we consider the special case where we limit $\mathcal{V}$ to only contain a single cyclotomic coset $\mathcal{C}(\alpha') \neq \{1\}$, where α' is also primitive. We want to show that without using Proposition 3, we can find more permutations. They key is to consider permutations that permute the codes $\langle \theta_\alpha(x) \rangle$ and $\langle \theta_{\alpha'}(x) \rangle$.

Proposition 4. *For any* $\rho \in Aut\left(\langle \theta_{\alpha'}(x) \rangle\right)$ *that also belongs to* $Aut\left(\langle \theta_\alpha(x) + \theta_{\alpha'}(x) \rangle\right)$*, then* $\left[c^{-u_0}\rho c^{u_0}, c^{-u_1}\rho c^{u_1}, \cdots, c^{-u_{m-1}}\rho c^{u_{m-1}}\right]$ *invariants the subcode* $\mathcal{N} = \mathcal{C}(\alpha') \cup \{\alpha\}$*, where* α *determines* $\mathbf{u}$.

Proof: First, note that the subcode $\mathcal{N} = \mathcal{C}(\alpha')$ is permuted amongst itself. Thus, we only need to analyze what happens to the $\mathcal{N} = \{\alpha\}$ subcode, and only when $\rho \notin Aut\left(\langle \theta_\alpha(x) \rangle\right)$. Then the following might occur:

1) ρ permutes a codeword from $\langle \theta_\alpha(x) \rangle$ into $\langle \theta_{\alpha'}(x) \rangle$.
2) ρ permutes a codeword from $\langle \theta_\alpha(x) \rangle$ into a cyclic shift of the form $\theta_\alpha(x) + \theta_{\alpha'}(x)x^d$.

If 1) occurs, it simply means we permute into the $\mathcal{N} = \mathcal{C}(\alpha')$ subcode. If 2) occurs, then we note that

$$\begin{aligned}\theta_\alpha(x)x^{u_i+r} &\overset{c^{-u_i}}{\rightarrow} \theta_\alpha(x)x^r \overset{\rho}{\rightarrow} \theta_\alpha(x)x^{r'} + \theta_{\alpha'}(x)x^{r'+d} \\ &\overset{c^{u_i}}{\rightarrow} \theta_\alpha(x)x^{u_i+r'} + \theta_{\alpha'}(x)x^{u_i+r'+d}\end{aligned}$$

We are only concerned about the $\theta_\alpha(x)x^{u_i+r'}$ terms, and we conclude similarly as in the proof of Proposition 2. ∎

It is generally difficult to find a permutation ρ satisfying the conditions of Proposition 4. However, for codes over $\mathcal{F}(2^3)$, it is relatively easy.

Proposition 5. *For* $\alpha, \alpha' \in \mathcal{F}(2^3)$*,* $Aut\left(\langle \theta_\alpha(x) + \theta_{\alpha'}(x) \rangle\right)$ *is the symmetric group.*

Proof: This follows since $\langle \theta_\alpha(x) + \theta_{\alpha'}(x) \rangle$ is a cyclic code with a single zero $\{1\}$. ∎

Example 3. *The* $\mathcal{N} = \{\alpha^3\}$ *subcode has corresponding* $\mathbf{u} = [2, 5, 0]$*. The [7,4,4] RS code with* $\mathcal{N} = \{\alpha, \alpha^2, \alpha^3, \alpha^4\} = \mathcal{C}(\alpha) \cup \{\alpha^3\}$*, is invariant under the actions of the group* $[c^{-2}G'c^2, c^{-5}G'c^5, G']$*, where* $G' = Aut\left(\langle \theta_\alpha(x) \rangle\right)$.

V. Notes on RS Codes with $\mathcal{N} = \{\alpha, \alpha'\}$.

In this section, we consider the case with two *primitive* elements. We also restrict α and α' to be from the same coset, i.e., $\mathcal{C}(\alpha) = \mathcal{C}(\alpha')$. From the previous discussion, we know that α and α' each determine different $\mathbf{u}$ vectors, however, since α and α' are from the same coset, they correspond to the *same* minimal cyclic code.

Consider some $\rho \in Aut\left(\langle \theta_\alpha(x) \rangle\right)$ that *centralizes* c, then with reference to Proposition 2, we see that $[c^{-u_0}\rho c^{u_0}, c^{-u_1}\rho c^{u_1}, \cdots, c^{-u_{m-1}}\rho c^{u_{m-1}}] = [\rho, \rho, \cdots, \rho]$. Such permutations do not depend on $\mathbf{u}$.

Example 4. *The centralizers of* c *for* α *in* $\mathcal{F}(2^3)$*,* $\mathcal{F}(2^4)$ *and* $\mathcal{F}(2^5)$ *are simply the cyclic group* $\langle c \rangle$*. These permutations are not so interesting as they only result in symbol shifts.*

The permutations derived in [2] depend on $\mathbf{u}$, and thus do not apply to the subcode $\mathcal{N} = \{\alpha, \alpha'\}$. If we change the *basis* of the subcode $\mathcal{N} = \{\alpha, \alpha'\}$, then we obtain some new insight. First, we denote the vectors $\mathbf{u}$, and $\mathbf{u}'$, that correspond to the subcodes $\mathcal{N} = \{\alpha\}$, and $\mathcal{N} = \{\alpha'\}$, respectively. We know they have codewords of the type

$$\begin{aligned}&[\theta_\alpha(x)x^{u_0}, \cdots, \theta_\alpha(x)x^{u_{m-1}}] \\ &\qquad + x^d[\theta_\alpha(x)x^{u'_0}, \cdots, \theta_\alpha(x)x^{u'_{m-1}}] \\ &= [\theta_\alpha(x)x^{u_0+Z(u'_0-u_0+d)}, \cdots, \theta_\alpha(x)x^{u_0+Z(u'_{m-1}-u_{m-1}+d)}]\end{aligned}$$

for all $d \in \mathbb{Z}/n$, and the function $Z(x)$, known as *Zech's logarithm*, obeys $1 + \alpha^x = \alpha^{Z(x)}$. Now, we choose m values for d, exactly $d_i = -(u'_i - u_i) = -\mu_i$ for all $0 \leq i \leq m-1$. Thus, we obtain m vectors, which are placed in the matrix shown (page bottom) in (4). Now we claim the following.

Proposition 6. *Any 2 rows of the matrix in (4), and their relevant cyclic shifts, are a basis for the subcode* $\mathcal{N} = \{\alpha, \alpha'\}$.

Proof: Any cyclic shifts of any two arbitrary rows have $\mathbf{0}$ elements in different columns, thus they are linearly independent. Also similarly to (3), the first m cyclic shifts of each row are linearly independent. Thus, the matrix rank is at least $2m$, but the dimension of the $\mathcal{N} = \{\alpha, \alpha'\}$ subcode is $2m$. ∎

A. Column Variant Permutations: $\mathcal{F}(2^3)$

The dual of the $\mathcal{N} = \{\alpha, \alpha'\}$ subcode has non-zeros in the form $\mathcal{N} = \beta \cup \mathcal{C}(\beta')$ code. for some $\beta, \beta' \in \mathcal{F}(2^3)$. Thus the discussions in Section IV apply. However, here we present a direct proof. To reduce notation, let us define $\lambda_i(j) = u_i +$

$$\begin{bmatrix} \mathbf{0} & \theta_\alpha(x)x^{u_1+Z(\mu_1-\mu_0)} & \cdots & \theta_\alpha(x)x^{u_{m-1}+Z(\mu_{m-1}-\mu_0)} \\ \theta_\alpha(x)x^{u_0+Z(\mu_0-\mu_1)} & \mathbf{0} & \cdots & \theta_\alpha(x)x^{u_{m-1}+Z(\mu_{m-1}-\mu_1)} \\ \vdots & \vdots & \vdots & \vdots \\ \theta_\alpha(x)x^{u_0+Z(\mu_0-\mu_{m-1})} & \theta_\alpha(x)x^{u_1+Z(\mu_1-\mu_{m-1})} & \cdots & \mathbf{0} \end{bmatrix} \tag{4}$$

Authorized licensed use limited to: UNIV OF HAWAII LIBRARY. Downloaded on March 15, 2009 at 23:45 from IEEE Xplore. Restrictions apply.

$Z(\mu_i - \mu_j)$. The matrix in (4) reduces to

$$\begin{bmatrix} \mathbf{0} & \theta_\alpha(x)x^{\lambda_1(0)} & \theta_\alpha(x)x^{\lambda_2(0)} \\ \theta_\alpha(x)x^{\lambda_0(1)} & \mathbf{0} & \theta_\alpha(x)x^{\lambda_2(1)} \\ \theta_\alpha(x)x^{\lambda_0(2)} & \theta_\alpha(x)x^{\lambda_1(2)} & \mathbf{0} \end{bmatrix} \quad (5)$$

To proceed further, we need the following two lemmas.

Lemma 1. *For $a \neq b$, we have the identity $\lambda_a(b) - \lambda_b(a) = u'_a - u'_b$.*

Proof: This can be shown using an identity of Zech's logarithm, which is given as $Z(x-y) - Z(y-x) = x - y$. ■

Lemma 2. *The following identity is satisfied for any arbitrary indices i, j and k, where $i \neq j \neq k$.*

$$\lambda_i(k) + \lambda_j(i) + \lambda_k(j) = \lambda_i(j) + \lambda_j(k) + \lambda_k(i)$$

Proof: This is shown using Lemma 1 and the Zech's logarithm identity $Z(x) - x = Z(-x)$.

$$\begin{aligned} &\lambda_i(k) - \lambda_i(j) + \lambda_k(j) - \lambda_k(i) + \lambda_j(i) \\ &= (\lambda_i(k) - \lambda_k(i)) + (\lambda_j(i) - \lambda_i(j)) + \lambda_k(j) \\ &= u'_i - u'_k + u'_j - u'_i + u_k + Z(\mu_k - \mu_j) \\ &= u'_j - (u_j) - (u'_k - u_k) + (u_j) + Z(\mu_k - \mu_j) \\ &= (u_j) + \mu_j - \mu_k + Z(\mu_k - \mu_j) \\ &= u_j + Z(\mu_j - \mu_k) = \lambda_j(k) \end{aligned}$$ ■

We now define our permutation as follows.

Definition 3. *We define the permutation, which swaps the first and second columns, by performing operations as follows:*

1) *Cyclic shift the first column by $c^{-\lambda_0(2)+\lambda_1(2)}$, and the second column by $c^{-\lambda_1(2)+\lambda_0(2)}$.*
2) *Proceed to swap the first and second columns.*

Since any two arbitrary rows span the whole $\mathcal{N} = \{\alpha, \alpha'\}$ subcode, it is sufficient to prove the next lemma.

Lemma 3. *Any cyclic shift of the first row will be permuted to some cyclic shift of the second row, and vice-versa.*

Proof: Apply the permutation given in Definition 3 to some cyclic shift of the first row. Referring to (5), we see that it now becomes $[\theta_\alpha(x)x^{\lambda_1(0)-\lambda_1(2)+\lambda_0(2)+r}, \mathbf{0}, \theta_\alpha(x)x^{\lambda_2(0)+r}]$. Now we need to check whether this new vector is some cyclic shift of the second row. If this holds, then we have

$$\lambda_1(0) - \lambda_1(2) + \lambda_0(2) - \lambda_0(1) = \lambda_2(0) - \lambda_2(1),$$

but this is proven in Lemma 2, for the case $i = 0, j = 1$, and $k = 2$. Proving this also holds for the second row is similar, and thus omitted. ■

We have proved and constructed a single permutation that permutes the first and second column. We now state our main result in the following proposition.

Proposition 7. *There exists permutations that swap any pair of columns for the binary image of the RS code over $\mathcal{F}(2^3)$.*

Proof: Choose any permutation σ over 3 indices, and permute both the rows and columns of the matrix in (5) with σ. Thus, we get an *equivalent* code, but with the same structure as (5). Apply the permutation in Definition 3 to the equivalent code (which invariants it), and permute the columns back with σ^{-1} to obtain the original code. In this way, we apply all permutations of the form $\sigma(0,1)\sigma^{-1}$, which is exactly the *conjugacy class* of $(0,1)$, that contains the permutations $\{(0,1),(1,2),(0,2)\}$. Also, note that these permutations generate all $3! = 6$ column invariant permutations. ■

Example 5. *Define the permutation map by $\sigma(i) = j$, and the inverse map by $\sigma^{-1}(j) = i$.*

1) *Form the equivalent matrix of (5) using σ.*
2) *$\sigma^{-1}(0)$th column: $c^{-\lambda_{\sigma^{-1}(0)}(\sigma^{-1}(2))+\lambda_{\sigma^{-1}(1)}(\sigma^{-1}(2))}$*
3) *$\sigma^{-1}(1)$th column: $c^{-\lambda_{\sigma^{-1}(1)}(\sigma^{-1}(2))+\lambda_{\sigma^{-1}(0)}(\sigma^{-1}(2))}$*
4) *Swap the $\sigma^{-1}(1)$th and $\sigma^{-1}(2)$th columns.*
5) *Restore the original code using σ^{-1}.*

B. Column Variant Permutations for RS over $\mathcal{F}(2^4)$

For RS codes over $\mathcal{F}(2^4)$, swapping two columns becomes too restrictive. When $m = 4$, the first two rows of (4) are

$$\begin{bmatrix} \mathbf{0} & \theta_\alpha(x)x^{\lambda_1(0)} & \theta_\alpha(x)x^{\lambda_2(0)} & \theta_\alpha(x)x^{\lambda_3(0)} \\ \theta_\alpha(x)x^{\lambda_0(1)} & \mathbf{0} & \theta_\alpha(x)x^{\lambda_2(1)} & \theta_\alpha(x)x^{\lambda_3(1)} \end{bmatrix} \quad (6)$$

Define the following constant

$$\delta \quad = \quad \lambda_2(1) - \lambda_2(0) + \lambda_3(1) - \lambda_3(0). \quad (7)$$

Consider applying the following permutation, to cyclically shifted versions (by r and r', respectively) of the two rows the matrix in (6).

Definition 4. *We define the permutation, which swaps the first and second columns, by performing operations as follows:*

1) *Cyclic shift the first column by $c^{-\lambda_0(1)+\lambda_1(0)+\delta}$, and the second column by $c^{-\lambda_1(0)+\lambda_0(1)}$.*
2) *Proceed to swap the first and second columns.*

We obtain the following (concatenated in matrix form)

$$\begin{bmatrix} \theta_\alpha(x)x^{\lambda_0(1)+r} & \mathbf{0} & \theta_\alpha(x)x^{\lambda_2(0)+r} & \theta_\alpha(x)x^{\lambda_3(0)+r} \\ \mathbf{0} & \theta_\alpha(x)x^{\lambda_1(0)+\delta+r'} & \theta_\alpha(x)x^{\lambda_2(1)+r'} & \theta_\alpha(x)x^{\lambda_3(1)+r'} \end{bmatrix} \quad (8)$$

Next, consider swapping columns 3 and 4.

Definition 5. *We define the permutation, which swaps the columns 3 and 4, as follows:*

1) *Cyclic shift the third column by $c^{-\lambda_2(0)+\lambda_3(1)}$, and the fourth column by $c^{-\lambda_3(0)+\lambda_2(1)}$.*
2) *Swap the third and fourth columns.*

Proposition 8. *The overall permutation obtained by performing the one given in Definition 4, followed by the one in Definition 5, invariants the $\mathcal{N} = \{\alpha, \alpha'\}$ subcode over $\mathcal{F}(2^4)$.*

Proof: With these column shifts, it is clear that for any cylic shift r, the first row of (8) permutes to some cyclic shift of the second row of (8). As for the second row, we observe that the third column permutes to

$$\theta_\alpha(x)x^{\lambda_2(1)-\lambda_2(0)+\lambda_3(1)+r'} \quad = \quad \theta_\alpha(x)x^{\lambda_3(0)+\delta+r'},$$

Authorized licensed use limited to: UNIV OF HAWAII LIBRARY. Downloaded on March 15, 2009 at 23:45 from IEEE Xplore. Restrictions apply.

Field	Dim.	$s^\dagger$	$\mathcal{N}$	$\mathcal{N}_d^\P$	Theory§				GAP [6] Computations
					Old CV	Old CI	New CV	New CI	
$\mathcal{F}(2^3)$	1	$1 \sim 6$	α^s	-	2×3	3×7	2×3	$\mathbf{2^3\times3\times7}$	$2^{10}\times3^8\times7$
	2	$0,\ 6$	$1, \alpha^s$	-	2×3	3×7	2×3	$\mathbf{2^3\times3\times7}$	$2^4\times3^2\times7$
	2	1	α, α^2	$1, \mathcal{C}(\alpha), \alpha^3$	2×3	3×7	$\mathbf{2\times3}^\ddagger$	$\mathbf{2^3\times3\times7}$	$2^4\times3^2\times7$
	2	$2 \sim 4$	α^s, α^{s+1}	-	-	7	-	7	$7 \sim 2\times7$
	2	5	α^5, α^6	$1, \mathcal{C}(\alpha^3), \alpha^4$	2×3	3×7	$\mathbf{2\times3}^\ddagger$	$\mathbf{2^3\times3\times7}$	$2^4\times3^2\times7$
	3	0	$1, \alpha, \alpha^2$	$\mathcal{C}(\alpha), \alpha^3$	2×3	3×7	$\mathbf{2\times3}^\ddagger$	$\mathbf{2^3\times3\times7}$	$2^4\times3^2\times7$
	3	$1 \sim 4,\ 6$	$\alpha^s, \alpha^{s+1}, \alpha^{s+2}$	-	-	7	-	7	$7 \sim 2\times7$
	3	5	$1, \alpha^5, \alpha^6$	$\mathcal{C}(\alpha^3), \alpha^4$	2×3	3×7	$\mathbf{2\times3}^\ddagger$	$\mathbf{2^3\times3\times7}$	$2^4\times3^2\times7$
$\mathcal{F}(2^4)$	1	*s.t.* $\gcd(15, s) = 1$	α^s	-	$2^3\times3$	$2^2\times3\times5$	$2^3\times3$	$\mathbf{2^6\times3^2\times5\times7}$	$2^{51}\times3^{17}\times5\times7$
	2	0	$1, \alpha$	-	$2^3\times3$	$2^2\times3\times5$	$2^3\times3$	$\mathbf{2^6\times3^2\times5\times7}$	$2^9\times3^3\times5\times7$
	2	$1, 13$	α^s, α^{s+1}	-	-	3×5	$\mathbf{2^2}$	3×5	$2^3\times3\times5$
	3	$0, 13$	$1, \alpha, \alpha^2$	-	-	3×5	$\mathbf{2^2}$	3×5	$2^3\times3\times5$
	3	$1 \sim 12, 14$	$\alpha^s, \alpha^{s+1}, \alpha^{s+2}$	-	-	3×5	-	3×5	3×5
$\mathcal{F}(2^5)$	1	$1 \sim 30$	α^s	-	$2^3\times3\times5$	5×31	$2^3\times3\times5$	$\mathbf{2^{10}\times3^2\times5\times7\times31}$	-
	2	0	$1, \alpha$	-	$2^3\times3\times5$	5×31	$2^3\times3\times5$	$\mathbf{2^{10}\times3^2\times5\times7\times31}$	$2^{13}\times3^3\times5^2\times7\times31$
	2	$1 \sim 30$	α^s, α^{s+1}	-	-	31	-	31	$31 \sim 2^2\times31$
	3	$0 \sim 30$	$\alpha^s, \alpha^{s+1}, \alpha^{s+2}$	-	-	31	-	31	$31 \sim 2^2\times31$

TABLE I
KNOWN AUTOMORPHISM GROUP SIZES FOR VARIOUS RS CODES OVER $\mathcal{F}(2^3)$, $\mathcal{F}(2^4)$ AND $\mathcal{F}(2^5)$.

$^\dagger s$ is the starting power of α in the consecutive non-zeros of the code.
¶When theory only applies to the dual code, $\mathcal{N}_d$ is the set of non-zeros.
§CV and CI stand for column variant, and invariant, respectively.
‡New direct proof derived.

and the fourth column permutes to

$$\theta_\alpha(x)x^{\lambda_3(1)-\lambda_3(0)+\lambda_2(1)+r'} = \theta_\alpha(x)x^{\lambda_2(0)+\delta+r'}. \quad \blacksquare$$

Proposition 9. *For the $\mathcal{N} = \{\alpha, \alpha'\}$ subcode over $\mathcal{F}(2^4)$, there exists 4 permutations column variant permutations.*

Proof: Similarly to the case for $\mathcal{F}(2^3)$, we pick σ to form an equivalent code. The conjugacy class of $\sigma(0,1)(2,3)\sigma^{-1}$ contains 3 permutations $\{(0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$ and generates a group of order 4. $\blacksquare$

Example 6. *Continuing from step* 1) of Example 5

2) Compute $\delta = \lambda_{\sigma^{-1}(2)}\left(\sigma^{-1}(1)\right) - \lambda_{\sigma^{-1}(2)}\left(\sigma^{-1}(0)\right) + \lambda_{\sigma^{-1}(3)}\left(\sigma^{-1}(1)\right) - \lambda_{\sigma^{-1}(3)}\left(\sigma^{-1}(0)\right)$.
3) $\sigma^{-1}(0)$th column: $c^{-\lambda_{\sigma^{-1}(0)}\left(\sigma^{-1}(1)\right)+\lambda_{\sigma^{-1}(1)}\left(\sigma^{-1}(0)\right)+\delta}$
4) $\sigma^{-1}(1)$th column: $c^{-\lambda_{\sigma^{-1}(1)}\left(\sigma^{-1}(0)\right)+\lambda_{\sigma^{-1}(0)}\left(\sigma^{-1}(1)\right)}$
5) Swap the $\sigma^{-1}(0)$th and $\sigma^{-1}(1)$th columns.
6) $\sigma^{-1}(2)$th column: $c^{-\lambda_{\sigma^{-1}(2)}\left(\sigma^{-1}(0)\right)+\lambda_{\sigma^{-1}(3)}\left(\sigma^{-1}(1)\right)}$
7) $\sigma^{-1}(3)$th column: $c^{-\lambda_{\sigma^{-1}(3)}\left(\sigma^{-1}(0)\right)+\lambda_{\sigma^{-1}(2)}\left(\sigma^{-1}(1)\right)}$
8) Swap the $\sigma^{-1}(2)$th and $\sigma^{-1}(3)$th columns.
9) Restore original code using σ^{-1}.

VI. COMPUTATIONAL RESULTS

Table I shows the sizes of automorphism groups computed for various RS codes over $\mathcal{F}(2^3)$, $\mathcal{F}(2^4)$ and $\mathcal{F}(2^5)$. The Groups, Algorithms, Programming (GAP) software [6] is used to obtain all computational results, and the new results are highlighted in bold. For RS codes over $\mathcal{F}(2^3)$, with the exception of five dimension 3 codes (and their duals), every RS code in this family have its automorphisms groups characterized by theory. However, the limitation of the current theory is obvious for codes of dimension-3 over fields $\mathcal{F}(2^4)$ and larger. Note that all dimension-1 codes have very large automorphism groups, as their groups are not limited by the column variant and invariant structure. Finally, we observe a drastic decrease in automorphism group sizes as the dimension increases, which incidently correlates to the increase in difficulty to obtain theoretical results.

VII. CONCLUSION

In this paper, we obtained a direct proof of a previous result by Lacan et. al, which led to theoretical connections to the automorphism groups of RS codes, with elementary group theory. Further investigation led to new theoretical results on the existence of permutations for previously studied codes, as well as some new codes.

ACKNOWLEDGMENT

The authors would like to acknowledge the GAP software, and the Partition Backtrack algorithm [7] by J. S. Leon (`ftp://ftp.math.uic.edu/pub/leon/partn`), which were used to perform group computations in this work.

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, 2002.
[3] 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.
[4] 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.
[5] 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.
[6] *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, The GAP Group, 2007. [Online]. Available: http://www.gap-system.org
[7] J. S. Leon, "Computing automorphism groups of error-correcting codes," *IEEE Trans. on Inform. Theory*, vol. 28, no. 3, pp. 496–511, May 1982.

Authorized licensed use limited to: UNIV OF HAWAII LIBRARY. Downloaded on March 15, 2009 at 23:45 from IEEE Xplore. Restrictions apply.