ACKNOWLEDGMENT

The authors wish to thank Prof. J. Ferrar of the Department of Mathematics, The Ohio State University, for his useful discussions and the referees for the suggestions.

REFERENCES

[1] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasitwisted codes and new linear codes," *Des., Codes Cryptogr.*, vol. 23, no. 3, pp. 313–326, December 2001.
[2] A. E. Brouwer. Linear code bounds. [Online]. Available: http://www.win.tue.nl/aeb/voorlincod.html
[3] A. R. Calderbank and G. McGuire, "Construction of a $(64, 2^{37}, 12)$ code via Galois rings," *Des. Codes Cryptogr.*, vol. 10, no. 2, pp. 157–165, 1997.
[4] Z. Chen, "Six new binary quasicyclic codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1666–1667, Sept. 1994.
[5] R. N. Daskalov, T. A. Gulliver, and E. Metodieva, "New good quasicyclic ternary and quaternary linear codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1647–1650, Sept. 1997.
[6] ——, "New ternary linear codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1687–1688, July 1999.
[7] P. P. Greenough and R. Hill, "Optimal ternary quasicyclic codes," *Des. Codes, Cryptogr.*, vol. 2, pp. 81–91, 1992.
[8] M. Greferath and E. Viterbo, "On $\mathbb{Z}_4$- and $\mathbb{Z}_9$-linear lifts of the Golay code," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2524–2527, Nov. 1999.
[9] T. A. Gulliver and V. K. Bhargava, "Nine good rate $(m-1)/pm$ quasicyclic codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1366–1369, July 1992.
[10] ——, "New good rate $(m-1)/pm$ ternary and quaternary quasicyclic codes," *Des., Codes Cryptogr.*, vol. 7, pp. 223–233, 1996.
[11] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preperata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.
[12] K. Lally and P. Fitzpatrick, "Construction and classification of quasicyclic codes," in *Proc. Workshop on Coding and Cryptography (WCC 99)*, Paris, France, Jan. 11–14, 1999.
[13] S. Litsyn. Table of nonlinear binary codes. [Online]. Available: http://www.eng.tau.ac.il/litysn/tableand/index.html
[14] V. S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594–1600, Sept. 1996.
[15] G. E. Séguin and G. Drolet, "The theory of 1-generator quasicyclic codes," preprint, 1990.
[16] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, "New ternary quasicyclic codes with better minimum distances," *IEEE Trans. Inform. Theory*, vol. 46, pp. 1554–1558, July 2000.
[17] J. H. van Lint, *Introduction to Coding Theory*. Berlin, Germany: Springer-Verlag, 1999.
[18] Z. X. Wan, *Quaternary Codes*. Singapore: World Scientific, 1997.
[19] J. Wolfmann, "Negacyclic and cyclic codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2527–2532, Nov. 1999.
[20] M. Yamada, "Distance-regular graphs of girth 4 over an extension ring of Z/4Z," *Graphs Comb.*, vol. 6, pp. 381–394, 1990.

The q-ary Image of Some q^m-ary Cyclic Codes: Permutation Group and Soft-Decision Decoding

Jérôme Lacan and Emmanuelle Delpeyroux

***Abstract*—Using a particular construction of generator matrices of the q-ary image of q^m-ary cyclic codes, it is proved that some of these codes are invariant under the action of particular permutation groups. The equivalence of such codes with some two-dimensional (2-D) Abelian codes and cyclic codes is deduced from this property. These permutations are also used in the area of the soft-decision decoding of some expanded Reed–Solomon (RS) codes to improve the performance of generalized minimum-distance decoding.**

***Index Terms*—Permutation groups, q-ary image of q^m-ary cyclic codes, soft-decision decoding.**

I. INTRODUCTION

One important area in coding theory is concerned with codes which are invariant under a set of permutations.

For example, any linear code of length n over $\mathbb{F}_{q^r}$ (i.e., vector subspace of $(\mathbb{F}_{q^r})^n$) which has the property of being invariant under the cyclic permutation (shift) is called a cyclic code. This property allows us to consider such a code as a principal ideal in the algebra $\mathbb{F}_{q^r}[z]/(z^n-1)$. Let (i, j) denote the greatest common divisor of two integers i and j. When $(n, q) = 1$, a cyclic code is entirely defined by the set of its nonzeros, i.e., the nth roots of unity such that at least one codeword polynomial $c(x)$ does not evaluate to zero in this point. The parameters of such a code are usually denoted by $[n, k]$, where k is the dimension of the code considered as a $\mathbb{F}_{q^r}$-vector subspace. Note that k is also the number of nonzeros. In order to distinguish different codes of the same dimension, we denote a code by $[n, NZ]_{q^r}$, where NZ is the set of nonzeros. A generator polynomial $g(z)$ of such a code is a polynomial codeword such that each codeword $c(z)$ can be expressed as a product $c(z) = g(z) \times u(z)$ where $u(z)$ is a polynomial of degree less than k. From such a generator polynomial, we can obtain a generator matrix G of this code defined as follows:

$$G^T = \left[g(z)\, zg(z)\, \cdots\, z^{k-1}g(z)\right]$$

where G^T denotes the transpose of G.

An Abelian code over $\mathbb{F}_{q^r}$ is a vector subspace of $(\mathbb{F}_{q^r})^{mn}$ invariant under the shift of the rows and the columns where we consider each codeword as an $m \times n$-matrix [6]. Many researchers have worked on codes which are invariant under particular groups of permutations such as, for example, the general linear group [1]–[3] or the Mathieu group [5, Ch. 20]. The first problem we address in this correspondence is that of determining a group of permutations under whose action the q-ary image of some q^m-ary cyclic codes is invariant. This property is used to obtain new results on these codes such as the invariance under particular permutations or the equivalence with cyclic and two-dimensional (2-D) Abelian codes.

Permutations that fix a code have an interesting application in the area of soft-decision decoding of the q-ary image (the so-called expanded image) of the Reed–Solomon (RS) codes. For these codes,

Manuscript received September 5, 2000; revised September 7, 2001.
J. Lacan is with the Département de Mathématiques Appliquées et d'Informatique, ENSICA, 31056 Toulouse, France (e-mail: jerome.lacan@ensica.fr).
E. Delpeyroux is with the Département d'Informatique, ICAM, 31300 Toulouse, France (e-mail: emmanuelle.delpeyroux@icam.fr).
Communicated by R. Koetter, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(02)05155-6.

the use of soft-decision decoding can significantly improve the performance. In practice, in most cases, q^m is equal to 2^m, but the codewords are transmitted in their expanded binary form and the available soft information is relative to the binary symbols. However, soft-decoding algorithms, like the generalized minimum distance decoding (GMD) of Forney [10] or the Chase algorithm [11], make use of soft-decision information on the symbol level. In [9], it is stated that "the major drawback with RS codes (for satellite use) is that the present generation of decoders does not make full use of bit-based soft decision information." The permutations introduced in this correspondence can be used for this purpose.

This correspondence is divided into five sections. In Section II, we give a construction of a $\mathbb{F}_q$-generator matrix of the q-ary image of q^m-ary cyclic codes. A similar construction is found in [8], but here we completely characterize each block as a generator matrix of a cyclic code over $\mathbb{F}_q$. This characterization is necessary to prove the invariance of the q-ary image under the action of permutation groups.

In Section III, we define special sets of permutations, and we prove that they form a group. Then we determine cyclic codes whose q-ary image is invariant under the action of these permutations.

In Section IV, we present some consequences of these results. We prove that if a cyclic code over $\mathbb{F}_{q^m}$ is such that its q-ary image is invariant under the action of some of these groups then this q-ary image is equivalent to a 2-D Abelian code. When $(n,\ m) = 1$, the q-ary image is equivalent to a cyclic code.

Section V presents an application of these permutations and shows how to use them to improve the performance of the soft-decision decoding of RS codes. The algorithm is worked out in detail and some simulation results are presented.

II. Generator Matrix of the q-ary Image of a q^m-ary Cyclic Code

Let NZ be a subset of $\mathbb{F}_{q^m}\backslash\{0\}$ and let C be the code equal to $[n = q^m - 1,\ NZ]_{q^m}$. In this section, we present a construction of a $\mathbb{F}_q$-generator matrix of the q-ary image of C. The generator matrix is obtained as a block matrix where each block is a generator matrix of a cyclic code of length n over $\mathbb{F}_q$.

A. Definitions and Preliminaries

We start by defining the q^s-ary image of a q^r-ary cyclic code, where $\mathbb{F}_{q^s}$ is a subfield of $\mathbb{F}_{q^r}$. Let

$$a(z) = \sum_{j=0}^{n-1} a_j z^j$$

be an element of $\mathbb{F}_{q^r}[z]/(z^n - 1)$. Let $\underline{\alpha} = \{\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{\frac{r}{s}-1}\}$ be a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_{q^s}$. Using $\underline{\alpha}$, the polynomial $a(z)$ may be written as

$$\sum_{j=0}^{n-1}\sum_{i=0}^{\frac{r}{s}-1} a_{i,j}\alpha_i z^j$$

where $a_{i,j} \in \mathbb{F}_{q^s}$ and

$$\sum_{i=0}^{\frac{r}{s}-1} a_{i,j}\alpha_i = a_j.$$

We define the q^s-ary image of $a(z)$ with respect to the basis $\underline{\alpha}$ by the bijective module homomorphism

$$\begin{array}{rcl} \mathcal{D}_{\underline{\alpha}}:\ \mathbb{F}_{q^r}[z]/(z^n-1) & \longrightarrow & (\mathbb{F}_{q^s}[x]/(x^n-1))^{\frac{r}{s}} \\ a(z) & \longrightarrow & \left(a_0(x),\ a_1(x),\ \ldots,\ a_{\frac{r}{s}-1}(x)\right) \end{array}$$

where

$$a_i(x) = \sum_{j=0}^{n-1} a_{i,j}x^j.$$

The q^s-ary image of $[n,\ NZ]_{q^r}$ with respect to the basis $\underline{\alpha}$ is denoted by $\mathcal{D}_{\underline{\alpha}}([n,\ NZ]_{q^r})$, and we have

$$\mathcal{D}_{\underline{\alpha}}([n,\ NZ]_{q^r}) = \{\mathcal{D}_{\underline{\alpha}}(c(z))|c(z) \in [n,\ NZ]_{q^r}\}.$$

Then $\mathcal{D}_{\underline{\alpha}}([n,\ NZ]_{q^r})$ is a submodule of dimension $\frac{r}{s}k$ of the $\mathbb{F}_{q^s}[x]/(x^n-1)$-module $(\mathbb{F}_{q^s}[x]/(x^n-1))^{\frac{r}{s}}$.

Let

$$\left\{(c_0^{(i)}(x),\ c_1^{(i)}(x),\ \ldots,\ c_{\frac{r}{s}-1}^{(i)}(x)),\ \text{for } i = 0,\ \ldots,\ \frac{r}{s}k - 1\right\}$$

be an $\mathbb{F}_{q^s}$-basis of $\mathcal{D}_{\underline{\alpha}}([n,\ NZ]_{q^r})$. An $\mathbb{F}_{q^s}$-generator matrix for $\mathcal{D}_{\underline{\alpha}}([n,\ NZ]_{q^r})$ is given as

$$\begin{bmatrix} c_0^{(0)}(x) & \cdots & c_{\frac{r}{s}-1}^{(0)}(x) \\ & \cdots & \\ c_0^{(\frac{r}{s}k-1)}(x) & \cdots & c_{\frac{r}{s}-1}^{(\frac{r}{s}k-1)}(x) \end{bmatrix}.$$

We define the set of conjugates of an element β of $\mathbb{F}_{q^r}$ with respect to $\mathbb{F}_{q^s}$ as the set of elements $\beta,\ \beta^{q^s},\ \ldots,\ \beta^{q^{s(\frac{r}{s}-1)}}$ [4, Ch. 2, Definition 2.17]. This set is denoted by $\mathcal{C}_{q^s}(\beta)$.

In order to construct the $\mathbb{F}_q$-generator matrix of the q-ary image of C, we need to split NZ (the set of nonzeros of C), into full sets of conjugates with respect to subfields of $\mathbb{F}_{q^m}$. Let $\mathbb{F}_{q^{r_1}}, \mathbb{F}_{q^{r_2}},\ \ldots,\ \mathbb{F}_{q^{r_t}}$ be the subfields of $\mathbb{F}_{q^m}$ such that $r_1 < r_2 < \cdots < r_t$. Note that $r_1 = 1$ and $r_t = m$. Let NZ_1 denote the union of full sets of conjugates with respect to $\mathbb{F}_{q^{r_1}}$ that are contained in NZ. The set NZ_2 is defined as the union of full sets of conjugates with respect to $\mathbb{F}_{q^{r_2}}$ that are contained in $NZ\backslash NZ_1$. Similarly, for $i = 3,\ \ldots,\ t$, NZ_i is defined as the union of full sets of conjugates with respect to $\mathbb{F}_{q^{r_i}}$ that are contained in $NZ\backslash\{NZ_1 \cup \cdots \cup NZ_{i-1}\}$.

For $i = 1,\ \ldots,\ t$, we denote by C_i the subfield subcode of C defined by $[n,\ NZ_i]_{q^{r_i}}$.

Example 1: Let α be a primitive element of $\mathbb{F}_{2^4}$ such that $\alpha^4 + \alpha + 1 = 0$. Let us define the RS code $C = [15,\ NZ]_{16}$ (presented in [8]) such that $NZ = \{\alpha^7,\ \alpha^8,\ \ldots,\ \alpha^{14},\ \alpha^0\}$. For this set of nonzeros, we have $r_1 = 1$, $NZ_1 = \mathcal{C}_{2^1}(\alpha^0) \cup \mathcal{C}_{2^1}(\alpha^7)$, $r_2 = 2$, $NZ_2 = \mathcal{C}_{2^2}(\alpha^{10})$, and $r_3 = 4$, $NZ_3 = \mathcal{C}_{2^4}(\alpha^8) \cup \mathcal{C}_{2^4}(\alpha^9) \cup \mathcal{C}_{2^4}(\alpha^{12})$. We obtain then the subfield subcodes $C_1 = [15,\ NZ_1]_2$, $C_2 = [15,\ NZ_2]_{2^2}$, and $C_3 = [15,\ NZ_3]_{2^4}$. ◇

For each $i = 1,\ \ldots,\ t$, we construct a particular $\mathbb{F}_q$-generator matrix of the q-ary image of C_i in Section II-B. Section II-C extends this construction to the construction of a particular $\mathbb{F}_{q^{r_i}}$-generator matrix of the q^{r_i}-ary image of the code $[n,\ NZ_i]_{q^m}$. Finally, in Section II-D, the fact that C is equal to $\bigoplus_{i=1}^{t}[n,\ NZ_i]_{q^m}$ is used to construct an $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}([n,\ NZ_i]_{q^m})$ and thus a $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$.

B. Generator Matrix of the q-ary Image of C_i

For each $i = 1,\ \ldots,\ t$, consider the subfield subcode C_i. The subset NZ_i is a union of full sets of conjugates with respect to $\mathbb{F}_{q^{r_i}}$

$$NZ_i = \bigcup_{j=1}^{t_i} \mathcal{C}_{q^{r_i}}(\beta_{i,j}), \qquad \text{where } \beta_{i,j} \in NZ_i.$$

Let $C_{i,j}$ be the code $[n, \mathcal{C}_{q^{r_i}}(\beta_{i,j})]_{q^{r_i}}$. Clearly, $C_i = \bigoplus_{j=1}^{t_i} C_{i,j}$. Let $\theta_{i,j}(z)$ be the primitive idempotent of $[n, \mathcal{C}_q(\beta_{i,j})]_q$. A generator of $C_{i,j}$ may be expressed as

$$g_{i,j}(z) = \theta_{i,j}(z) \prod_{b \in \mathcal{C}_q(\beta_{i,j}) \setminus \mathcal{C}_{q^{r_i}}(\beta_{i,j})} (z - b). \tag{1}$$

Let $\underline{\delta} = \{\delta_0, \ldots, \delta_{r_i-1}\}$ be a basis of $\mathbb{F}_{q^{r_i}}$ over $\mathbb{F}_q$. Then the generator $g_{i,j}(z)$ may also be expressed as

$$g_{i,j}(z) = \theta_{i,j}(z) \left[b_{i,j}^{(0)}(z)\delta_0 + b_{i,j}^{(1)}(z)\delta_1 + \cdots + b_{i,j}^{(r_i-1)}(z)\delta_{r_i-1} \right] \tag{2}$$

where each $b_{i,j}^{(l)}(z)$ has its coefficients in $\mathbb{F}_q$.

Example 2: By considering the code C defined in Example 1, C_1 is equal to $C_{1,1} \oplus C_{1,2}$, C_2 is equal to $C_{2,1}$, and C_3 is equal to $C_{3,1} \oplus C_{3,2} \oplus C_{3,3}$. Let us compute, for example, $g_{2,1}(z)$ and $g_{3,2}(z)$. Note that the basis $\underline{\alpha}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ (here $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$) must be, for each $\mathbb{F}_{q^{r_i}}$, a direct product between a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_{q^{r_i}}$ and a basis of $\mathbb{F}_{q^{r_i}}$ over $\mathbb{F}_q$ (see [12]). Hence, $\underline{\alpha}$ must be a direct product between a basis of $\mathbb{F}_{2^4}$ over $\mathbb{F}_2^2$ (we take the basis $\{1, \alpha\}$) and a basis of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$ (we take the basis $\{1, \alpha^5\}$).

Following (1), a generator of $C_{2,1}$ is $g_{2,1}(z) = \theta_{2,1}(z)(z - \alpha^5)$. As $\{1, \alpha^5\}$ is a basis of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$, then $g_{2,1}(z)$ may be expressed as $\theta_{2,1}(z)(z.1 + 1 \cdot \alpha^5)$ (see (2)). A generator of $C_{3,1}$ is

$$\theta_{3,1}(z)(z - \alpha)(z - \alpha^2)(z - \alpha^4).$$

By developing the coefficients in basis $\underline{\alpha}$, we obtain the polynomial

$$g_{3,1}(z) = \theta_{3,1}(z)((z^3 + z^2 + 1) \cdot 1 + (z^2 + 1) \cdot \alpha^5 + (z^2 + z) \cdot \alpha + 1 \cdot \alpha^6)$$

which respects the form defined by (2). ◇

Proposition 1: For $j = 1, \ldots, t_i$, let $B_{i,j}$ be the $|\mathcal{C}_q(\beta_{i,j})| \times r_i$ matrix whose entries are

$$x^u \theta_{i,j}(x) b_{i,j}^{(l)}(x)$$

for $u = 0, \ldots, |\mathcal{C}_q(\beta_{i,j})| - 1$ and $l = 0, \ldots, r_i - 1$.

Then $B_{i,j}$ is a $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\delta}}(C_{i,j})$.

Proof: The first row of $B_{i,j}$ is equal to $\mathcal{D}_{\underline{\delta}}(g_{i,j}(z))$. Thus, each row of $B_{i,j}$ is in $\mathcal{D}_{\underline{\delta}}(C_{i,j})$.

Let us prove that these $|\mathcal{C}_q(\beta_{i,j})|$ rows are linearly independent. Clearly, there is at least one $\theta_{i,j}(x) b_{i,j}^{(l_0)}(x)$ not equal to 0. On the other hand, the code $[n, \mathcal{C}_q(\beta_{i,j})]_q$ (generated, for example, by $\theta_{i,j}(x)$) is irreducible (see [6, Ch. 5]), it follows that it is also generated by $\theta_{i,j}(x) b_{i,j}^{(l_0)}(x)$, and $\{x^u \theta_{i,j}(x) b_{i,j}^{(l_0)}(x), u = 0, \ldots, |\mathcal{C}_q(\beta_{i,j})| - 1\}$ is an $\mathbb{F}_q$-basis of $[n, \mathcal{C}_q(\beta_{i,j})]_q$. This proves that the $|\mathcal{C}_q(\beta_{i,j})|$ rows are linearly independent.

Moreover

$$\begin{aligned} \dim_{\mathbb{F}_q} \mathcal{D}_{\underline{\delta}}(C_{i,j}) &= r_i \times \dim_{\mathbb{F}_{q^{r_i}}} C_{i,j} \\ &= r_i \times \dim_{\mathbb{F}_{q^{r_i}}} [n, \mathcal{C}_{q^{r_i}}(\beta_{i,j})]_{q^{r_i}} \\ &= r_i \times |\mathcal{C}_{q^{r_i}}(\beta_{i,j})| \\ &= |\mathcal{C}_q(\beta_{i,j})| \\ &= \dim_{\mathbb{F}_q} [n, \mathcal{C}_q(\beta_{i,j})]_q. \end{aligned}$$

This completes the proof. □

Example 3: Let us develop matrices $B_{2,1}$ and $B_{3,1}$ related to codes $C_{2,1}$ and $C_{3,1}$ (see Example 2). The polynomial $\theta_{2,1}(z)$ is equal to

$$z + z^2 + z^4 + z^5 + z^7 + z^8 + z^{10} + z^{11} + z^{13} + z^{14}.$$

Then, from $g_{1,2}(z)$, we obtain

$$B_{2,1} = \begin{bmatrix} 101101101101101 & 011011011011011 \\ 110110110110110 & 101101101101101 \end{bmatrix}.$$

Similarly, from $g_{3,1}(z)$ and $\theta_{3,1}(z)$ which is equal to

$$z + z^2 + z^3 + z^4 + z^6 + z^8 + z^9 + z^{12}$$

we obtain $B_{3,1}$ equal to the matrix shown at the bottom of the page. ◇

As $C_i = \bigoplus_{j=1}^{t_i} C_{i,j}$, an $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\delta}}(C_i)$ may be expressed as

$$M_i = \begin{bmatrix} B_{i,1} \\ \cdots \\ B_{i,t_i} \end{bmatrix} = \begin{bmatrix} b_{i,1}^{(0)}(x) M_{i,1} & \cdots & b_{i,1}^{(r_i-1)}(x) M_{i,1} \\ & \cdots & \\ b_{i,t_i}^{(0)}(x) M_{i,t_i} & \cdots & b_{i,t_i}^{(r_i-1)}(x) M_{i,t_i} \end{bmatrix}$$

where $M_{i,j}$ is the following particular generator matrix of $[n, \mathcal{C}_q(\beta_{i,j})]_q$:

$$\begin{bmatrix} \theta_{i,j}(x) \\ x\theta_{i,j}(x) \\ \cdots \\ x^{|\mathcal{C}_q(\beta_i,j)|-1}\theta_{i,j}(x) \end{bmatrix}.$$

When $b_{i,j}^{(l)}(x)$ is not equal to 0, since $[n, \mathcal{C}_q(\beta_{i,j})]_q$ is irreducible, the matrix $b_{i,j}^{(l)}(x) M_{i,j}$ is also a generator matrix of $[n, \mathcal{C}_q(\beta_{i,j})]_q$.

Thus, M_i is composed of block matrices generating cyclic codes over $\mathbb{F}_q$.

C. Generator Matrix of the q^{r_i}-ary Image of $[n, NZ_i]_{q^m}$

For each $i = 1, \ldots, t$, let $\underline{\gamma} = \{\gamma_0, \gamma_1, \ldots, \gamma_{\frac{m}{r_i}-1}\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_{q^{r_i}}$, and let $\{g_0(z), \ldots, g_{|NZ_i|-1}(z)\}$ be a basis of C_i over $\mathbb{F}_{q^{r_i}}$.

For $j = 0, \ldots, \frac{m}{r_i}-1$, we define by $\gamma_j C_i$ the set $\{\gamma_j c(z) : c(z) \in C_i\}$. Clearly, for $j = 0, \ldots, \frac{m}{r_i} - 1$, $\gamma_j C_i$ is a subcode of C and $\{\gamma_j g_u(z) : u = 0, \ldots, |NZ_i| - 1\}$ is a basis of $\gamma_j C_i$.

Then the $|NZ_i| \times \frac{m}{r_i}$ elements of

$$\bigcup_{j=0}^{\frac{m}{r_i}-1} \{\mathcal{D}_{\underline{\gamma}}(\gamma_j g_u(z)) : u = 0, \ldots, |NZ_i| - 1\}$$

may be considered as the rows of a $\mathbb{F}_{q^{r_i}}$-generator matrix of $\mathcal{D}_{\underline{\gamma}}([n, NZ_i]_{q^m})$. These rows form a block matrix

$$\mathcal{T}_i = \begin{bmatrix} \mathcal{M}_i & 0 & \ldots & 0 \\ 0 & \mathcal{M}_i & \ldots & 0 \\ & \cdots & \cdots & \\ 0 & 0 & \ldots & \mathcal{M}_i \end{bmatrix},$$

where $\mathcal{M}_i$ is a generator matrix of C_i over $\mathbb{F}_{q^{r_i}}$.

Example 4: As an illustration of this part, we may express the matrix $\mathcal{T}_2$ of code C (see Example 1) as

$$\mathcal{T}_2 = \begin{bmatrix} \mathcal{M}_2 & 0 \\ 0 & \mathcal{M}_2 \end{bmatrix}$$

where $\mathcal{M}_2$ is a generator matrix of C_2 over $\mathbb{F}_{2^2}$. ◇

$$\begin{bmatrix} 111010110010001 & 011001000111101 & 01000111101011 & 11110101100100 \\ 111101011001000 & 101100100011110 & 10100011110101 & 01111010110010 \\ 011110101100100 & 010110010001111 & 11010001111010 & 00111101011001 \\ 001111010110010 & 101011001000111 & 01101000111101 & 10011110101100 \end{bmatrix}.$$

D. Construction of the $\mathbb{F}_q$-Generator Matrix of $\mathcal{D}_{\underline{\alpha}}(C)$

Now, using the two previous sections, we can construct an $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$.

Let the basis $\underline{\alpha}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ be chosen such that $\underline{\alpha}$ is the direct product of a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_{q^{r_i}}$ with a basis of $\mathbb{F}_{q^{r_i}}$ over $\mathbb{F}_q$ for every subfield $\mathbb{F}_{q^{r_i}}$ of $\mathbb{F}_{q^m}$. Such a basis always exists (see [12]). In other words, for each i, we choose the bases used in Sections II-B and II-C such that their direct product is equal to $\underline{\alpha}$.

Finally, in order to obtain an $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}([n, NZ_i]_{q^m})$ it is sufficient to replace $\mathcal{M}_i$ (Section II-C) by M_i (Section II-B) in $\mathcal{T}_i$. We call the obtained matrix T_i. If $r_1 = 1$, we have $\mathcal{M}_1 = M_1$ and $\mathcal{T}_1 = T_1$. If $r_t = m$, then $T_t = M_t$ holds.

Since C is the direct sum of the codes $[n, NZ_i]_{q^m}$ (for $i = 1, \ldots, t$), an $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C)$ is given, in transposed form, as

$$[\,T_1 \quad T_2 \quad \cdots \quad T_t\,].$$

This matrix generates $\mathcal{D}_{\underline{\alpha}}(C)$ and it is composed of block matrices generating cyclic codes over $\mathbb{F}_q$ (see Section II-B).

Example 5: As an illustration, we construct two submatrices of the $\mathbb{F}_2$-generator matrix of code $\mathcal{C}$ defined in Example 1. The first one is related to nonzero α^{10}, i.e., to subfield subcode C_2. The code C_2 (over $\mathbb{F}_{2^2}$) is equal to $C_{1,2}$. Therefore, M_2 is equal to $B_{2,1}$ which is developed in Example 3. Then, we can deduce the corresponding submatrix T_2 of the generator matrix of C shown in the first matrix at the bottom of the page.

The second submatrix is related to the nonzero α^8. This submatrix is a part of T_3 (see previous notations). As $r_3 = 4$ is equal to m, $T_3 = M_3$, and M_3 is the concatenation of $B_{3,1}$, $B_{3,2}$, and $B_{3,3}$. The submatrix corresponding to α^8 is shown in the second matrix at the bottom of the page.

Note that this example illustrates the difference between our construction and the construction of [8]. Indeed, in [8], the submatrix corresponding to α^8 is not factorized into explicit block matrices. ◇

III. Groups of Permutations of the q-ary Image of Some q^m-ary Cyclic Codes

A. Groups of Permutations

Now, let us introduce the following sets of permutations.

Definition 1: Let $\mathbb{Z}/(n)$ be the ring of integers modulo n. Let $(w_0, w_1, \ldots, w_{m-1})$ be some m-tuple, such that each w_i is in $\mathbb{Z}/(n)$. We denote by (l, σ, a) the permutation of $\{0, 1, \ldots, m-1\} \times \mathbb{Z}/(n)$ which sends (i, j) to $(\sigma(i), (j + s_i^{(l,\sigma)})q^l + a)$, where

1) $\sigma \in S_m$ (where S_m is the group of permutations of $\{0, 1, \ldots, m-1\}$);
2) $a \in \mathbb{Z}/(n)$ and $l \in \{0, 1, \ldots, m-1\}$;
3) $s_i^{(l,\sigma)} = q^{-l} w_{\sigma(i)} - w_i$, for $i = 0, 1, \ldots, m-1$.

Let us denote by $\mathcal{P}$ the set

$$\{(l, \sigma, a),\ l = 0, 1, \ldots, m-1,\ \sigma \in S_m \text{ and } a \in \mathbb{Z}/(n)\}.$$

Proposition 2: Let us denote the law of composition by $\circ$. Then

1) $(\mathcal{P}, \circ)$ is a group;
2) the generators of this group are $(0, id, 1), (1, id, 0)$, and the set of $(0, \sigma, 0)$ for σ in the set of the generators of S_m;
3) $|\mathcal{P}| = m \times m! \times n$.

Proof:

1) Clearly, $(l_1, \sigma_1, a_1) \circ (l_2, \sigma_2, a_2)$ is equal to
$$(l_1 + l_2,\ \sigma_1 \circ \sigma_2,\ a_1 + a_2 q^{l_1})$$
which is also an element of $\mathcal{P}$. Moreover, for all $(l, \sigma, a) \in \mathcal{P}$, we have the following two equalities:
— $(l, \sigma, a) \circ (0, id, 0) = (0, id, 0) \circ (l, \sigma, a) = (l, \sigma, a)$
— $(l, \sigma, a) \circ (-l, \sigma^{-1}, -q^{-l}a) = (0, id, 0)$.
So, $\mathcal{P}$ is a group under composition.
2) Direct.
3) It is sufficient to show that all these permutations are different. Let (l_1, σ_1, a_1) and (l_2, σ_2, a_2) be two permutations. Let us assume that, for any pair (i, j), we have
$$(\sigma_1(i), (j + s_i^{(l_1,\sigma_1)})q^{l_1} + a_1) = (\sigma_2(i), (j + s_i^{(l_2,\sigma_2)})q^{l_2} + a_2).$$
Then $\sigma_1 = \sigma_2$. Thus, for $\sigma_1 = \sigma_2 = \sigma$ and for any pair (i, j), we have
$$\left(j + q^{m-l_1} w_{\sigma(i)} - w_i\right) q^{l_1} + a_1 \equiv \left(j + q^{m-l_2} w_{\sigma(i)} - w_i\right) q^{l_2} + a_2 \text{ modulo } n.$$
So, for any pair (i, j), we have
$$q^{l_1} j - w_i q^{l_1} + a_1 \equiv q^{l_2} j - w_i q^{l_2} + a_2 \text{ modulo } n$$
i.e.,
$$(j - w_i)\left(q^{l_1} - q^{l_2}\right) + a_1 - a_2 \equiv 0 \text{ modulo } n.$$
Since there is a pair (i, j) such that $j - w_i \equiv 0$ modulo n, we have $a_1 \equiv a_2$ modulo n.

Moreover, there is a pair (i, j) such that $(j - w_i, n) = 1$. Thus, $q^{l_1} - q^{l_2} \equiv 0$ modulo n and hence $l_1 = l_2$. □

The action of a permutation (l, σ, a) of $\mathcal{P}$ on an element of $(\mathbb{F}_q[x]/(x^n - 1))^m$ is defined as follows.

Definition 2: Let $c(x)$ and $c'(x)$ be two elements of $(\mathbb{F}_q[x]/(x^n - 1))^m$. Let $c(x)$ be equal to $(c_0(x), c_1(x), \ldots, c_{m-1}(x))$ and $c'(x)$ to $(c'_0(x), c'_1(x), \ldots, c'_{m-1}(x))$, where

$$c_i(x) = \sum_{j=0}^{n-1} c_{i,j} x^j \quad \text{and} \quad c'_i(x) = \sum_{j=0}^{n-1} c'_{i,j} x^j.$$

$$\begin{bmatrix} 101101101101101 & 011011011011011 & 0 & 0 \\ 110110110110110 & 101101101101101 & 0 & 0 \\ 0 & 0 & 101101101101101 & 011011011011011 \\ 0 & 0 & 110110110110110 & 101101101101101 \end{bmatrix}.$$

$$\begin{bmatrix} 111010110010001 & 011001000111101 & 01000111101011 & 11110101100100 \\ 111101011001000 & 101100100011110 & 10100011110101 & 01111010110010 \\ 011110101100100 & 010110010001111 & 11010001111010 & 00111101011001 \\ 001111010110010 & 101011001000111 & 01101000111101 & 10011110101100 \end{bmatrix}.$$

For each permutation $(l,\ \sigma,\ a)$ of $\mathcal{P}$, we define the map $\overline{(l,\ \sigma,\ a)}$ of $(\mathbb{F}_q[x]/(x^n-1))^m$ which sends $c(x)$ onto $c'(x)$ if $c'_{i,\,j}=c_{u,\,t}$, where $(u,\ t)=(l,\ \sigma,\ a)^{-1}(i,\ j)$, for $i=0,\ 1,\ \ldots,\ m-1$ and $j\in\mathbb{Z}/(n)$.

The element $\overline{(l,\ \sigma,\ a)}(c(x))$ is called the image of $c(x)$ by the permutation $\overline{(l,\ \sigma,\ a)}$.

Clearly, for a fixed permutation, the images of two different elements of $(\mathbb{F}_q[x]/(x^n-1))^m$ are different.

B. Invariant Codes Under the Action of Some Groups of Permutations

Let $\underline{\alpha}=\{\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{m-1}\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We consider the code $C_1=[n,\ \{\beta\}]_{q^m}$, where β is a primitive element of $\mathbb{F}_{q^m}$. Then the construction of the $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_1)$ implies no condition on basis $\underline{\alpha}$ because there is no subfield subcode (see Section II-D). Moreover, a generator of C_1 is (see Section II-B)

$$\theta(z)\prod_{b\in\mathcal{C}_q(\beta)\setminus\mathcal{C}_{q^m}(\beta)}(z-b)$$

where $\theta(z)$ is the primitive idempotent of $[n,\ \mathcal{C}_q(\beta)]_q$. In basis $\underline{\alpha}$, this polynomial may be expressed as

$$\theta(z)(b_0(z)\alpha_0+\cdots+b_{m-1}(z)\alpha_{m-1})$$

where $b_i(z)$ is some polynomial over $\mathbb{F}_q$ $(i=0,\ \ldots,\ m-1)$. Then the $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_1)$ has the following form (see Proposition 1):

$$\begin{bmatrix}\theta(x)b_0(x) & \cdots & \theta(x)b_{m-1}(x)\\ x\theta(x)b_0(x) & \cdots & x\theta(x)b_{m-1}(x)\\ \cdots & \cdots & \cdots\\ x^{m-1}\theta(x)b_0(x) & \cdots & x^{m-1}\theta(x)b_{m-1}(x)\end{bmatrix}.$$

Let us denote the first row of this matrix by $G_1^{\underline{\alpha}}(x)$. As this matrix is entirely defined by its first row, $G_1^{\underline{\alpha}}(x)$ may be considered as a generator of $\mathcal{D}_{\underline{\alpha}}(C_1)$. For this particular construction of the $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_1)$ and for the fixed basis $\underline{\alpha}$, $G_1^{\underline{\alpha}}(x)$ is unique. Thus, from now on, $G_1^{\underline{\alpha}}(x)$ will be called *the* generator of $\mathcal{D}_{\underline{\alpha}}(C_1)$.

Remark 1: In order to prove the following propositions, we define a mapping ψ as

$$\begin{aligned}\psi:\ \mathbb{F}_{q^m}=\mathbb{F}_q(\beta)\quad&\longrightarrow\quad[n,\ \mathcal{C}_q(\beta)]_q\\ \sum_{i=0}^{m-1}e_i\beta^i\quad&\longrightarrow\quad\theta(x)\sum_{i=0}^{m-1}e_ix^i.\end{aligned}$$

The mapping ψ is a ring isomorphism (see [5, Ch. 8]).

Proposition 3: Let C_1 be equal to $[n,\ \{\beta\}]_{q^m}$, where β is a primitive element of $\mathbb{F}_{q^m}$. Let $G_1^{\underline{\alpha}}(x)$ be equal to

$$(\theta(x)b_0(x),\ \ldots,\ \theta(x)b_{m-1}(x)).$$

Then

1) $G_1^{\underline{\alpha}}(x)$ can be expressed as $(\theta(x)x^{u_0},\ \ldots,\ \theta(x)x^{u_{m-1}})$;
2) $\mathcal{D}_{\underline{\alpha}}(C_1)=\{(\theta(x)x^{u_0+r},\ \ldots,\ \theta(x)x^{u_{m-1}+r})$, for $r=0,\ \ldots,\ q^m-2\}\cup\{(0,\ \ldots,\ 0)\}$.

Proof:

1) First, let us prove that $\theta(x)b_i(x)\neq 0$, for all $i=0,\ \ldots,\ m-1$. If there exists an integer i_0 such that $\theta(x)b_{i_0}(x)$ is equal to zero then all codewords of C_1 have the form

$$\sum_{j=0}^{n-1}\sum_{i=0}^{m-1}c_{i,\,j}\alpha_iz^j,\qquad\text{with } c_{i_0,\,j}=0,\ \forall j.$$

This is clearly impossible. Thus, $\theta(x)b_i(x)\neq 0$, for all $i=0,\ \ldots,\ m-1$.

Second, the nonzero β of C_1 is a primitive element of $\mathbb{F}_{q^m}$. Remark 1 implies that $[n,\ \mathcal{C}_q(\beta)]_q$ is equal to

$$\{\theta(x)x^r,\ r=0,\ \ldots,\ n-1\}\cup\{0\}$$

and then all the $\theta(x)b_i(x)$ may be expressed as $\theta(x)x^{u_i}$.

2) Follows from 1) and Remark 1. □

Example 6: In order to illustrate Proposition 3, we consider the code $C_1=[n,\ \{\alpha^8\}]_{2^4}$ where α is a primitive element of $\mathbb{F}_{2^4}$ such that $\alpha^4+\alpha+1=0$. A generator polynomial of this code is the polynomial $g_{3,\,1}(z)$ given in Example 2

$$\theta(z)(1\cdot(z^3+z^2+1)+\alpha^5\cdot(z^2+1)+\alpha\cdot(z^2+z)+\alpha^6\cdot 1).$$

Using this polynomial, we can deduce *the* generator polynomial in the basis $\underline{\alpha}=\{1,\ \alpha^5,\ \alpha,\ \alpha^6\}$. This generator $G_1^{\underline{\alpha}}(x)$ is equal to

$$(\theta(x)(x^3+x^2+1),\ \theta(x)(x^2+1),\ \theta(x)(x^2+x),\ \theta(x)).$$

Following Proposition 3, the generator polynomial can be expressed as $G_1^{\underline{\alpha}}(x)=(\theta(x)x^{13},\theta(x)x^8,\ \theta(x)x^5,\ \theta(x))$. ◇

Now, the expression of $G_1^{\underline{\alpha}}(x)$ leads us to define a group of permutations such that $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of these permutations. All these permutations depend on the m-tuple $(u_0,\ \ldots,\ u_{m-1})$ defined by $G_1^{\underline{\alpha}}(x)$ (see Proposition 3), so they depend on the basis $\underline{\alpha}$ and on the code C_1.

Definition 3: Let C_1 be equal to $[n,\ \{\beta\}]_{q^m}$, where β is a primitive element of $\mathbb{F}_{q^m}$. Let $G_1^{\underline{\alpha}}(x)$ be equal to $(\theta(x)x^{u_0},\ \ldots,\ \theta(x)x^{u_{m-1}})$. We define $\mathcal{P}_1^{\underline{\alpha}}$ as the group of permutations for which the m-tuple $(w_0,\ \ldots,\ w_{m-1})$ is equal to $(u_0,\ \ldots,\ u_{m-1})$ (see Definition 1).

Proposition 4: $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of each permutation in $\mathcal{P}_1^{\underline{\alpha}}$.

Proof: In order to prove this proposition, it is sufficient to prove that the image of any codeword $(\theta(x)x^{r+u_0},\ \ldots,\ \theta(x)x^{r+u_{m-1}})$ of $\mathcal{D}_{\underline{\alpha}}(C_1)$ by any permutation in $\mathcal{P}_1^{\underline{\alpha}}$ is also a codeword of $\mathcal{D}_{\underline{\alpha}}(C_1)$. Let us express $\theta(x)$ as $\sum_{j=0}^{n-1}\theta_jx^j$. Then we have

$$\begin{aligned}&\left(\theta(x)x^{r+u_0},\ \ldots,\ \theta(x)x^{r+u_{m-1}}\right)\\&\qquad=\left(\sum_{j=0}^{n-1}\theta_{j-u_0-r}x^j,\ \ldots,\ \sum_{j=0}^{n-1}\theta_{j-u_{m-1}-r}x^j\right)\end{aligned}$$

and by using Definition 2 its image by the permutation $(l,\ \sigma,\ a)$ is equal to

$$\left(\sum_{j=0}^{n-1}\theta_{(j-a)q^{-l}-q^{-l}u_0-r}x^j,\ \ldots,\ \sum_{j=0}^{n-1}\theta_{(j-a)q^{-l}-q^{-l}u_{m-1}-r}x^j\right).$$

Since $(\theta(x))^{q^l}=\theta(x)$ (by definition, $\theta(x)$ is an idempotent), this element is also equal to $(\theta(x)x^{rq^l+a+u_0},\ \ldots,\theta(x)x^{rq^l+a+u_{m-1}})$. □

Example 7: Let us consider the group of permutations $\mathcal{P}_1^{\underline{\alpha}}$ of code C_1 defined in Example 6. This group is constructed from the 4-tuple $(13,\ 8,\ 5,\ 0)$. Let us consider some permutation of $\mathcal{P}_1^{\underline{\alpha}}$, for example, $(l,\ \sigma,\ a)=(3,\ s,\ 4)$ where s is the cyclic permutation modulo 4. It may be verified that the corresponding map $\overline{(3,\ s,\ 4)}$ (see Definition 2) sends any codeword of C_1 onto another codeword of C_1. For example, $x^4G_1^{\underline{\alpha}}(x)$ is sent onto $x^{10}G_1^{\underline{\alpha}}(x)$. ◇

Now, we prove that for other codes C in $\mathbb{F}_{q^m}[z]/(z^n-1)$, $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of any group $\mathcal{P}$ (defined in Definition 1).

Proposition 5: Let C_0 be equal to $[n,\ V]_{q^m}$, where V is some union of full sets of conjugates with respect to $\mathbb{F}_q$. Then $\mathcal{D}_{\underline{\alpha}}(C_0)$ is invariant under the action of any $\mathcal{P}$.

Proof: Let us denote by C_0' the code $[n,\ V]_q$. The particular form of the $\mathbb{F}_q$-generator matrix of $\mathcal{D}_{\underline{\alpha}}(C_0)$ (see Section II) implies that C_0 may be expressed as $\{(c_0(x),\ \ldots,\ c_{m-1}(x))\colon c_i(x)\in C_0'\}$.

The action of the permutations of $\mathcal{P}$ over $\mathcal{D}_{\underline{\alpha}}(C_0)$ may be split into two parts:

— the permutation of the different polynomials $c_i(x)$ by the elements of S_m (the group of permutations of $\{0, 1, \ldots, m-1\}$);
— some cyclic shifts and some exponentiations by q^l of the codewords of C_0'.

It can easily be proved that $_{\mathcal{D}}\underline{\alpha}(C_0)$ is invariant under the action of these two kinds of operations. Thus, $\mathcal{D}_{\underline{\alpha}}(C_0)$ is invariant under the action of all the permutations. □

Proposition 6: Let C be equal to $[n, \{\beta\} \cup V]_{q^m}$, where β is a primitive element of $\mathbb{F}_{q^m}$, and V is some union of full sets of conjugates with respect to $\mathbb{F}_q$. Let C_1 be equal to $[n, \{\beta\}]_{q^m}$, and let $G_1^{\underline{\alpha}}(x)$ be equal to $(\theta(x)x^{u_0}, \ldots, \theta(x)x^{u_{m-1}})$.

The code $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$.

Proof: As C is equal to $C_0 \oplus C_1$ where $C_0 = [n, V]_{q^m}$, the proof is direct from Propositions 4 and 5. □

Another way to increase the number of codes which are invariant under the action of any group $\mathcal{P}$ is to consider the dual codes.

Definition 4: Let Tr be the trace function of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ defined by

$$Tr(\gamma) = \sum_{i=0}^{m-1} \gamma^{q^i}.$$

The trace-dual basis of $\underline{\alpha} = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ is defined as the unique basis $\underline{\alpha}^{\perp} = \{\alpha_0', \alpha_1', \ldots, \alpha_{m-1}'\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that

$$Tr(\alpha_i \alpha_j') = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases}$$

Let $C^{\perp}$ be the dual code of C.

Proposition 7: Let C be a code in $\mathbb{F}_{q^m}[z]/(z^n - 1)$ such that $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of $\mathcal{P}$. Then $\mathcal{D}_{\underline{\alpha}^{\perp}}(C^{\perp})$ is also invariant under the action of $\mathcal{P}$.

Proof: Clearly $\mathcal{D}_{\underline{\alpha}}(C)^{\perp}$ is invariant under the action of $\mathcal{P}$. Moreover, it is known [7, Lemma 6] that $\mathcal{D}_{\underline{\alpha}}(C)^{\perp} = \mathcal{D}_{\underline{\alpha}^{\perp}}(C^{\perp})$. Thus, $\mathcal{D}_{\underline{\alpha}^{\perp}}(C^{\perp})$ is invariant under the action of $\mathcal{P}$. □

Propositions 6 and 7 allow us to determine codes which are invariant under the action of some $\mathcal{P}$. Several RS codes satisfy the conditions given by these propositions. For example, it can be verified that for all $k = 1, \ldots, 7$, there is a $[7, k, 8-k]_8$ RS code (i.e., a RS code of length 7, dimension k, and minimum distance $8-k$ over $\mathbb{F}_8$) whose binary image is invariant under the action of a $\mathcal{P}\underline{\alpha}$. This is also the case for the $[8, k, 9-k]_9$ RS codes (for $k = 1, \ldots, 8$) whose ternary image has the same property.

Some infinite families of RS codes also satisfy this property. All the RS codes $[q^m - 1, \{1, \alpha\}, q^m - 2]_{q^m}$, where α is a primitive element of $\mathbb{F}_{q^m}$, are such that their q-ary image is invariant under the action of a group $\mathcal{P}$. The duals of these codes in the trace-dual basis, i.e., $[q^m - 1, q^m - 3, 3]_{q^m}$ RS codes, also have the same property.

Note that the list of RS codes given here is not exhaustive. Several other RS codes can be found satisfying the conditions given by Propositions 6 and 7.

IV. Theoretical Consequences

In this section, it will prove that the invariance of some expanded codes under the action of the permutations allows us to determine some new properties of these codes. We start by determining the conditions under which the group of permutations contains the permutation τ of $\{0, 1, \ldots, m-1\} \times \mathbb{Z}/(n)$ which sends (i, j) to $(i+1, j)$ if $i < m-1$ and to $(0, j+1)$ otherwise (see [7]). In a second part, it will be proved that all expanded codes which are invariant under a group $\mathcal{P}$ are necessarily equivalent to a 2-D Abelian code, and sometimes to a cyclic code.

Let us fix some notations for this section: C_1 will represent the code $[n, \{\beta\}]_{q^m}$ where β is a primitive element of $\mathbb{F}_{q^m}$, its generator $G_1^{\underline{\alpha}}$ is equal to $(\theta(x)x^{u_0}, \ldots, \theta(x)x^{u_{m-1}})$, C_0 will represent the code $[n, V]_{q^m}$, where V is some union of full sets of conjugates with respect to $\mathbb{F}_q$.

A. Invariance Under the Cyclic Permutation

A well-known problem in the area of q-ary images of q^m-ary cyclic codes is to determine under what conditions the q-ary image is invariant under the action of a cyclic permutation, i.e., the mapping which sends a codeword $(c_0(x), \ldots, c_{m-1}(x))$ to the codeword $(xc_{m-1}(x), c_0(x), \ldots, c_{m-2}(x))$.

Clearly, this mapping corresponds to the permutation τ defined previously.

In order to make the connection between τ and the group of permutations $\mathcal{P}$, we give the following three lemmas.

Lemma 1: Let

$$G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \ldots, \theta(x)x^{u_{m-1}})$$

be the generator of the code $C_1 = [n, \{\beta\}]_m$, where β is a primitive element of $\mathbb{F}_{q^m}$. We consider an m-tuple $(v_0, \ldots, v_{m-1})$. There is a basis $\underline{\gamma}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that $G_1^{\underline{\gamma}}(x)$ is equal to $(\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}})$ if and only if $\{\beta^{v_0}, \ldots, \beta^{v_{m-1}}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Proof: First, let us give a preliminary result. Let $\underline{\alpha}$ and $\underline{\gamma}$ be two bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let P be the change of basis such that $\underline{\alpha}^t = P\underline{\gamma}^t$. Let us assume that $G_1^{\underline{\alpha}}(x)$ is equal to $(\theta(x)x^{u_0}, \ldots, \theta(x)x^{u_{m-1}})$ and $G_1^{\underline{\gamma}}(x)$ is equal to $(\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}})$. By using the definition of $G_1^{\underline{\alpha}}(x)$ (and $G_1^{\underline{\gamma}}(x)$) given at the beginning of the Section III-B, it is clear that we have $G_1^{\underline{\gamma}}(x)^t = P^t G_1^{\underline{\alpha}}(x)^t$.

1) Suppose that there exists a basis $\underline{\gamma}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that

$$G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}}).$$

Suppose that there are some scalars a_i, not all equal to zero (we take, for example, $a_0 \neq 0$), such that $\sum_{i=0}^{m-1} a_i \beta^{v_i} = 0$. It follows that $\theta(x)\sum_{i=0}^{m-1} a_i x^{v_i} = 0$ holds (use Remark 1). Let $\underline{\gamma}$ be equal to $\{\gamma_0, \ldots, \gamma_{m-1}\}$ and let us consider the basis $\underline{\delta}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ equal to $\{\gamma_0, \gamma_1 - \gamma_0 \frac{a_1}{a_0}, \ldots, \gamma_{m-1} - \gamma_0 \frac{a_{m-1}}{a_0}\}$. Using the preliminary result, $G_1^{\underline{\delta}}(x)$ is equal to $(0, \theta(x)x^{v_1}, \ldots, \theta(x)x^{v_{m-1}})$. Because of the proof of Proposition 3, this is impossible.

2) Conversely, suppose that $\{\beta^{v_0}, \ldots, \beta^{v_{m-1}}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $\{\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}}\}$ is a basis of $[n, \mathcal{C}_q(\beta)]_q$ (see Remark 1). On the other hand, $\{\beta^{u_0}, \ldots, \beta^{u_{m-1}}\}$ is also a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ (see previous point) and the same argument as above shows that $\{\theta(x)x^{u_0}, \ldots, \theta(x)x^{u_{m-1}}\}$ is also a basis of $[n, \mathcal{C}_q(\beta)]_q$. Then there exists an invertible matrix P' such that

$$(\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}})^t = P'(\theta(x)x^{u_0}, \ldots, \theta(x)x^{u_{m-1}})^t.$$

Now, we consider the set $\underline{\gamma}$ such that $\underline{\alpha} = P'^t\underline{\gamma}^t$. Since P' is invertible, $\underline{\gamma}$ is also a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and the preliminary result implies that

$$G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}}).$$ □

Lemma 2: Let

$$G_1^{\underline{\alpha}}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}}).$$

Then for any integer t, there exists a basis $\underline{\gamma}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that

$$G_1^{\underline{\gamma}}(x) = (\theta(x)x^{u_0+t}, \ldots, \theta(x)x^{u_{m-1}+t})$$

and we have $\mathcal{D}_{\underline{\alpha}}(C_1) = \mathcal{D}_{\underline{\gamma}}(C_1)$.

Proof: Lemma 1 proves that $\{\beta^{u_0}, \ldots, \beta^{u_{m-1}}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Thus, $\{\beta^{u_0+t}, \ldots, \beta^{u_{m-1}+t}\}$ is also a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. On the other hand, it proves that there is a basis $\underline{\gamma}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that

$$G_1^{\underline{\gamma}}(x) = (\theta(x)x^{u_0+t}, \ldots, \theta(x)x^{u_{m-1}+t}).$$

The dimensions of $\mathcal{D}_{\underline{\alpha}}(C_1)$ and $\mathcal{D}_{\underline{\gamma}}(C_1)$ and Proposition 3 prove the last assertion. □

In Proposition 4, it is proved that $\mathcal{D}_{\underline{\alpha}}(C_1)$ is invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$. Lemma 2 proved that there are other bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, called, for example, $\underline{\gamma}$, such that $\mathcal{D}_{\underline{\gamma}}(C_1)$ is also invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$.

Lemma 3: For any integer t, there exists a basis $\underline{\gamma}$ such that

$$G_1^{\underline{\gamma}}(x) = (\theta(x)x^t, \theta(x)x^{-b+t}, \ldots, \theta(x)x^{-(m-1)b+t})$$

where b is invertible in $\mathbb{Z}/(n)$.

Proof: Clearly, $\{1, \beta^{-b}, \ldots, \beta^{-(m-1)b}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ because β is a primitive element of $\mathbb{F}_{q^m}$ and b is invertible in $\mathbb{Z}/(n)$. Lemma 1 proves that there exists a basis $\underline{\gamma}'$ such that

$$G_1^{\underline{\gamma}'}(x) = (\theta(x)x^{u_0}, \theta(x)x^{u_1}, \ldots, \theta(x)x^{u_{m-1}}).$$

The final result is obtained using Lemma 2 for this polynomial. □

Proposition 8: There exists a basis $\underline{\gamma}$ such that τ is in $\mathcal{P}_1^{\underline{\gamma}}$ if and only if $(n, m) = 1$. When such a basis exists, we have

1) $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_0-a}, \ldots, \theta(x)x^{v_0-(m-1)a})$, where a is the inverse of m in $\mathbb{Z}/(n)$, and v_0 is an integer.
2) $\tau = (0, \sigma, a)$, where σ is the permutation of S_m defined by $\sigma(i) \equiv i + 1$ modulo m and a is the inverse of m in $\mathbb{Z}/(n)$.

Proof: Let us suppose that there is a basis $\underline{\gamma}$ such that τ is in $\mathcal{P}_1^{\underline{\gamma}}$ and that $G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \ldots, \theta(x)x^{v_{m-1}})$. Then, by considering the image of the different pairs (i, j) by τ, for all j in $\mathbb{Z}/(n)$, we have

$$(i+1, j) = (\sigma(i), jq^l + v_{\sigma(i)} - q^l v_i + a), \qquad \text{if } i < m-1$$

and

$$(0, j+1) = (\sigma(m-1), jq^l + v_{\sigma(m-1)} - q^l v_{m-1} + a), \qquad \text{if } i = m-1.$$

Therefore, σ is necessarily the permutation of S_m defined by $\sigma(i) \equiv i + 1$ modulo m, and for $j = 0$: $v_{i+1} - q^l v_i + a \equiv 0$ modulo n if $i < m-1$, and $v_0 - q^l v_{m-1} + a \equiv 1$ modulo n otherwise.

Thus, for any j in $\mathbb{Z}/(n)$, $q^l j \equiv j$ modulo n, and necessarily $l = 0$. Thus, we have $v_{i+1} - v_i \equiv -a$ modulo n if $i < m-1$, and $v_0 - v_{m-1} \equiv 1 - a$ modulo n. Hence, $1 - am \equiv 0$ modulo n, and $(n, m) = 1$ holds.

Clearly, $\tau = (0, \sigma, a)$, where σ is the permutation of S_m defined by $\sigma(i) \equiv i+1$ modulo m and a is the inverse of m in $\mathbb{Z}/(n)$. Moreover, $v_i = v_0 - ia$, for all $i = 1, \ldots, m-1$.

Conversely, suppose that $(n, m) = 1$. Let a be the inverse of m in $\mathbb{Z}/(n)$. Then there is a basis $\underline{\gamma}$ such that

$$G_1^{\underline{\gamma}}(x) = (\theta(x)x^{v_0}, \theta(x)x^{v_0-a}, \ldots, \theta(x)x^{v_0-(m-1)a})$$

for some integer v_0 (see Lemma 3). Let us consider $\mathcal{P}_1^{\underline{\gamma}}$, and the particular permutation $(0, \sigma, a)$, where σ is the permutation of S_m defined by $\sigma(i) \equiv i + 1$ modulo m. This permutation is equal to τ, and hence, it is in $\mathcal{P}_1^{\underline{\gamma}}$. □

Corollary 1: Let C be equal to $C_0 \oplus C_1$. If $(n, m) = 1$ then there exists a basis $\underline{\gamma}$ such that $\mathcal{D}_{\underline{\gamma}}(C_1)$, $\mathcal{D}_{\underline{\gamma}}(C_0)$, and $\mathcal{D}_{\underline{\gamma}}(C)$ are invariant under the action of τ.

Also, in the basis $\underline{\gamma}^{\perp}$, their dual codes are invariant under the action of τ.

Proof: Use Propositions 4, 5, 7, and 8. □

This result is another proof of a part of the results given in [7].

B. Equivalence With Cyclic and 2-D Abelian Codes

In [7], Seguin presents an open question which is "when does a q^m-ary cyclic code have a q-ary image which is equivalent to a cyclic code?" The following proposition partly solves this problem.

Proposition 9: Let C be a code in $\mathbb{F}_{q^m}[z]/(z^n - 1)$ which is invariant under the action of a group $\mathcal{P}$. Then, the following two statements are true.

1) $\mathcal{D}_{\underline{\alpha}}(C)$ is equivalent to a 2-D Abelian code.
2) If $(m, n) = 1$, then $\mathcal{D}_{\underline{\alpha}}(C)$ is equivalent to a cyclic code.

Proof:

1) Recall that a set of matrices can be considered as a 2-D Abelian code if it is a vector space which is invariant under the cyclic shifts of the rows and the columns. Here, it will be proved that it is possible to define a permutation P which sends the set of codewords of $\mathcal{D}_{\underline{\alpha}}(C)$ onto a set of $m \times n$-matrices that satisfies the required property.

Let P be the permutation of $\{0, 1, \ldots, m-1\} \times \mathbb{Z}/(n)$ which sends (i, j) onto $(i, w_0 - w_i + j)$ where $(w_0, \ldots, w_{m-1})$ is defined by $\mathcal{P}$ (see Definition 1). Let $c(x)$ be an element of $\mathcal{D}_{\underline{\alpha}}(C)$ equal to $(c_0(x), \ldots, c_{m-1}(x))$, where

$$c_i(x) = \sum_{j=0}^{n-1} c_{i,j} x^j.$$

Let $c'(x)$ be equal to $(c'_0(x), \ldots, c'_{m-1}(x))$, where

$$c'_i(x) = \sum_{j=0}^{n-1} c'_{i,j} x^j.$$

The action of P on $c(x)$ is defined by $c'_{i,j} = c_{u,t}$, where $(u, t) = P^{-1}(i, j)$ for $i = 0, 1, \ldots, m-1$, and $j \in \mathbb{Z}/(n)$. We call $c'(x)$ the image of $c(x)$ by P. Let us denote by $P(\mathcal{D}_{\underline{\alpha}}(C))$ the set of the images of the codewords of $\mathcal{D}_{\underline{\alpha}}(C)$ under P.

Now, let p be a permutation of $\mathcal{P}$. Since $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of p, then $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the action of $P \circ p \circ P^{-1}$.

Let σ be the permutation of S_m defined by $\sigma(i) \equiv i + 1$ modulo m. We consider the action of $P \circ (0, \sigma, 0) \circ P^{-1}$ over $P(\mathcal{D}_{\underline{\alpha}}(C))$. Clearly we have

$$P \circ (0, \sigma, 0) \circ P^{-1}(i, j) = (i + 1, j).$$

Thus, this permutation acts on $P(\mathcal{D}_{\underline{\alpha}}(C))$ as the shift of each column and $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the action of this permutation.

Finally, let us consider the action of $P \circ (0, Id, 1) \circ P^{-1}$ over $P(\mathcal{D}_{\underline{\alpha}}(C))$. We have

$$P \circ (0, Id, 1) \circ P^{-1}(i, j) = (i, j + 1).$$

So this permutation acts on $P(\mathcal{D}_{\underline{\alpha}}(C))$ as the shift of each row and $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the action of this permutation. Then, $P(\mathcal{D}_{\underline{\alpha}}(C))$ is invariant under the shift of the rows and the columns. Since it is the image of a vector space ($\mathcal{D}_{\underline{\alpha}}(C)$) under a permutation, $P(\mathcal{D}_{\underline{\alpha}}(C))$ is also a vector space. Thus, $\mathcal{D}_{\underline{\alpha}}(C)$ is equivalent to a 2-D Abelian code.

2) It is well known that a 2-D Abelian code of length $n_1 \times n_2$ is equivalent to a cyclic code if $(n_1, n_2) = 1$, [6, Ch. 5]. □

V. Application to the Soft-Decision Decoding of Binary Image of Some RS Codes

In practical applications, the q-ary image of some q^m-ary cyclic codes is often used in concatenated schemes. For example, the binary image of some RS codes over $\mathbb{F}_{2^m}$ is used for satellite transmissions [9].

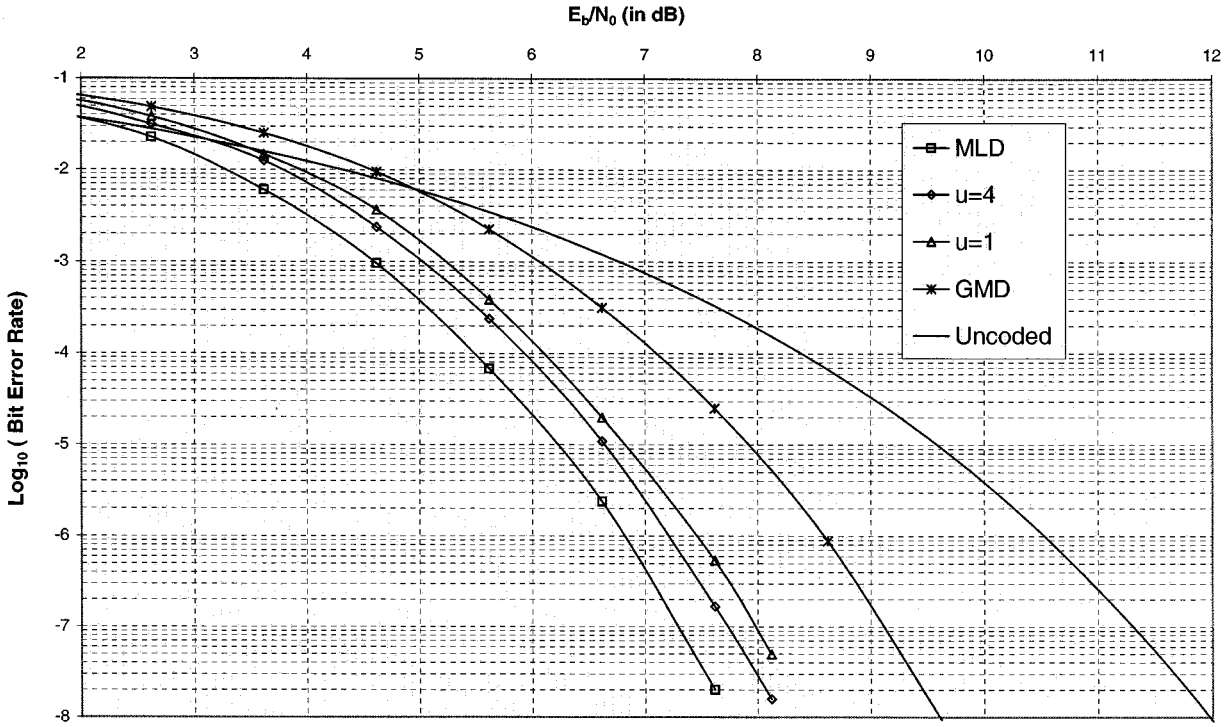

Fig. 1. Performance comparison for the $[7, 4, 4]$ RS code.

In many applications, soft-decision decoding holds the promise of substantial performance gains for this kind of codes. Nevertheless, classical soft-decision decoding algorithms of RS codes use soft information on symbol level and then they do not make full use of bit-based soft-decision information [9].

We propose an approach to this problem based on the use of permutations in conjunction with a GMD algorithm [10]. We also present the results of some simulations of this new decoding algorithm applied to two RS codes.

A. Decoding Algorithm

The main problem in order to use soft-decision decoding of the binary image of the RS code may be summarized as follows. The available soft information is relative to binary symbols (q-ary image). However, some of the main soft-decision decoding algorithms of the RS codes (GMD, Chase algorithm) operate with soft information for byte (q^m-ary symbols). In other words, we have to compute symbol level soft information from the bit-based soft coefficients without losing too much information.

The soft-decision decoding algorithm of RS codes considered here is GMD decoding [10]. The GMD algorithm consists of determining the $d-1$ least reliable bytes (i.e., with the worst soft coefficients) and applying successive erasure decodings by varying the number of erasures. In this way, a list of tentative codewords is obtained. The codeword on this list that is nearest to the received word is considered as the decoded codeword.

In order to improve the performance of this decoding, the permutations introduced in Section III may be used as follows. The received binary word is permuted in order to "group" the unreliable bits within the same bytes. These bytes are then considered as the least reliable for the soft-decision decoding. After a successful GMD decoding of this word, the binary form of the corrected word is permuted by the inverse permutation to obtain a tentative codeword. This operation is performed repeatedly for several permutations. The final decoded output is the best (the nearest to the binary received word) of the codewords proposed by the different decodings.

In order to choose the permutations used for each received codeword, we represent a codeword as an $m \times n$ array over $\mathbb{F}_2$, each column representing the binary image of a byte-symbol.

Clearly, for a given word, the permutations (l, σ, a) and (l, σ, b) compose the same columns. So, for the decoding, the only considered permutations are $(l, \sigma, 0)$, for $l = 0, \ldots, m-1$ and $\sigma \in S_m$. The number of such permutations is $m \times m!$.

From the definition of the permutations, it can be deduced that two distinct positions can be grouped onto the same column only if they belong to distinct rows. This property implies that each row can be considered independently for the choice of permutations. For each of the m rows, the permutations are sorted according to their capability to group bad positions with the *worst* position of the considered row. Then, the selected permutations are the best u permutations for each row, where u is a parameter which determines the number of used permutations ($u \times m$) (and hence, a level of correction).

In order to estimate the complexity of this approach, the two steps of the algorithm must be considered. The first step sorts the permutations to determine the u best ones for each row. The required complexity, counted as the number of multiplications and comparisons in the field of concern, is of order $O(m^2 \times m! \times u)$. The second part of the algorithm concerns the $u \times m$ independent GMD decodings of a word. As the complexity of the computation of GMD decoding is $O(n \times d)$ (see [14] or [15]), the complexity of this step is $O(n \times d \times u \times m)$. Note that these $u \times m$ GMD decodings can be implemented in parallel.

The complexity of the first step can be reduced by considering a subset of the permutations and by only sorting the elements of this subset. If the size of this subset is a power of m, the complexity of the algorithm is bounded by a polynomial in n. Furthermore, the error performance is not significantly degraded. It can be noted that the complexity of different soft-decision decoding algorithms of RS codes with comparable performance [8], [16], [17] contain an exponential factor.

In the next subsection, simulation results for this decoding algorithm are presented for two codes and two values of u.

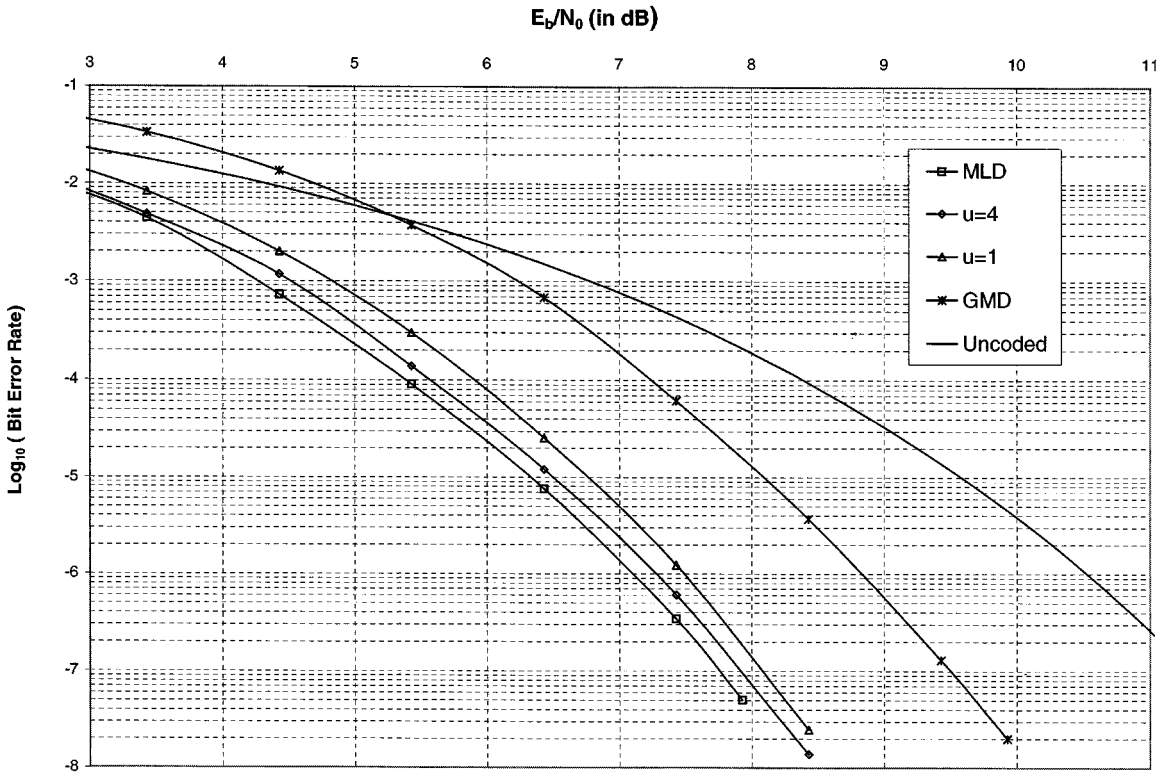

Fig. 2. Performance comparison for the $[15,\ 13,\ 3]$ RS code.

B. Simulation Results

The first code is $C = [7,\ \{\beta^6,\ \beta,\ \beta^3,\ \beta^5\}]_8$, where β is such that $\beta^3 + \beta^2 + 1 = 0$. This code, whose parameters are $[7,\ 4,\ 4]$, is able to correct one byte error and one byte erasure or three byte erasures.

Let us consider $\mathcal{D}_{\underline{\alpha}}(C)$, the binary image of C with respect to the basis $\underline{\alpha}$ equal to $\{1,\ \alpha,\ \alpha^2\}$, where $\alpha = \beta^3$. Then

$$G_1^{\underline{\alpha}}(x) = (\theta(x),\ \theta(x)x^5,\ \theta(x)x^2)$$

where $\theta(x)$ is the primitive idempotent of $[7,\ \{\beta,\ \beta^2,\ \beta^4\}]_2$. As the set of nonzeros can be split into $\{\beta\} \cup \{\beta^3,\ \beta^6,\ \beta^5\}$, $\mathcal{D}_{\underline{\alpha}}(C)$ is invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$ (see Proposition 6).

In our simulations, we have added white Gaussian noise (AWGN) to the binary form of the codewords. For each bit, the associated soft information is computed and quantized into 32 possible values.

In order to evaluate the bit-error rate (BER) performance of our algorithm for several values of u ($u = 1$ and $u = 4$), we have implemented other classical algorithms: maximum-likelihood decoding (MLD) and Forney's GMD decoding [10]. Note that the implemented version of GMD decoding is the one presented in [14].

The results of our simulations are presented in Fig. 1.

The second code is a $[15,\ 13,\ 3]$ RS code over $\mathbb{F}_{16}$ defined as follows. Let β be a primitive element of $\mathbb{F}_{16}$ such that $\beta^4 + \beta + 1 = 0$. Let us define the basis $\underline{\alpha} = \{1,\ \beta,\ \beta^2,\ \beta^3\}$ of $\mathbb{F}_{16}$ over $\mathbb{F}_2$. Proposition 6 proves that $\mathcal{D}_{\underline{\alpha}}([15,\ \{1,\ \beta\}]_{16})$ is invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$ and Proposition 7 proves that the dual code of $[15,\ \{1,\ \beta\}]_{16}$ expanded in the dual basis of $\underline{\alpha}$ is also invariant under the action of $\mathcal{P}_1^{\underline{\alpha}}$.

This dual code is the $[15,\ 13,\ 3]$ RS code considered here. The simulated performance of the decoding algorithm for $u = 1$ and $u = 4$ is presented in Fig. 2.

The two simulations clearly show the benefit of using the permutations for improving the performance of GMD decoding. Indeed, at BER $= 10^{-7}$, the difference in performance between GMD decoding and the new algorithm for $u = 1$ is about 1.4 dB for the $[7,\ 4,\ 4]$ RS code and about 1.2 dB for the $[15,\ 13,\ 3]$ RS code.

For $u = 4$, in comparison with GMD, the gain is about 1.6 dB for the $[7,\ 4,\ 4]$ RS code and about 1.4 dB for the $[15,\ 13,\ 3]$ RS code at BER $= 10^{-7}$. It may also be observed that these performances are close to the MLD, i.e., less than 0.2 dB for the $[7,\ 4,\ 4]$ RS code and about 0.4 dB for the $[15,\ 13,\ 3]$ RS code at BER $= 10^{-7}$.

ACKNOWLEDGMENT

The authors wish to acknowledge the two reviewers for several constructive remarks, A. Poli for the software of simulation SECC, and H. Tang, Y. Liu, M. Fossorier, and S. Lin for the preprint of their paper [16]. The authors also wish to thank R. Koetter for his helpful comments on the drafting of this correspondence.

REFERENCES

[1] T. P. Berger and P. Charpin, "The permutation group of affine-invariant extended cyclic codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2194–2209, Nov. 1996.

[2] P. Delsarte, "On cyclic codes that are invariant under the general linear group," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 760–769, Nov. 1970.

[3] T. Kasami, S. Lin, and W. W. Peterson, "Polynomial codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 807–814, Nov. 1968.

[4] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983.

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

[6] A. Poli and Ll. Huguet, *Error Correcting Codes: Theory and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1992.

[7] G. E. Seguin, "The q-ary image of q^m-ary cyclic code," *IEEE Trans. Inform. Theory*, vol. 41, pp. 387–399, Mar. 1995.

[8] A. Vardy and Y. Be'ery, "Bit-level soft-decision decoding of Reed–Solomon codes," *IEEE Trans. Commun.*, vol. 39, pp. 440–444, Mar. 1991.

[9] E. R. Berlekamp, R. E. Peile, and S. P. Pope, "The application of error control to communications," *IEEE Commun. Mag.*, vol. 25, pp. 44–57, 1987.

[10] G. D. Forney, Jr., "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. IT-12, pp. 125–131, Apr. 1966.
[11] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 170–181, Jan. 1972.
[12] J. Lacan and E. Delpeyroux, "Permutation group of the q-ary image of some q^m-ary cyclic codes," in *Finite Field: Theory, Applications and Algorithms*. Providence, RI: Amer. Math. Soc., 1999, Contemporary Mathematics, 225.
[13] O. Papini and J. Wolfmann, *Algèbre Discrète et Codes Correcteurs (Collections Mathématiques et Applications)*. Berlin, Germany: Springer-Verlag, 1995, vol. 20, .
[14] D. J. Taipale and M. J. Seo, "An efficient soft-decision Reed–Solomon decoding algorithm," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1130–1139, July 1994.
[15] R. Kötter, "Fast generalized minimum-distance decoding of algebraic-geometry and Reed–Solomon codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 721–737, May 1996.
[16] H. Tang, Y. Liu, M. Fossorier, and S. Lin, "On combining chase-2 and GMD decoding algorithms for nonbinary block codes," *IEEE Commun. Lett.*, vol. 5, pp. 209–211, May 2001.
[17] B. Vucetic, V. Ponnampalam, and J. Vuckovic, "Low complexity soft decision algorithms for Reed–Solomon codes," *IECE Trans. Commun.*, vol. E84-B, no. 3, pp. 392–399, Mar. 2001.

Variance of the Turbo Code Performance Bound Over the Interleavers

Atousa H. S. Mohammadi, *Member, IEEE,* and Weihua Zhuang, *Senior Member, IEEE*

***Abstract*—In this correspondence, we evaluate the variance of the union performance bound for a rate-$1/3$ turbo code over all possible interleavers of length N, under the assumption of a maximum-likelihood (ML) decoder. Theoretical and simulation results for turbo codes with two-memory component codes indicate that the coefficient of variation of the bound increases with the signal-to-noise ratio and decreases with the interleaver length. Theoretical analysis for large interleaver lengths shows that the coefficient of variation asymptotically approaches a constant value. The results also demonstrate that the majority of the interleavers have performance bounds very close to the average value of the bound. This phenomenon is more palpable for larger interleaver lengths.**

***Index Terms*—Channel coding, concatenated codes, turbo codes, union performance bound.**

I. Introduction

Turbo codes, introduced in 1993 [1], are composed of the parallel concatenation of two (or more) recursive systematic convolutional (RSC) component codes, connected through an interleaver(s). The interleaver, which reorders the input block of data given to the second encoder, plays a key role in the pseudorandom nature and, consequently, the high performance of turbo codes. Thus, the study and design of the interleaver has been an attractive subject for many researchers in this area.

In [2], an interleaver design technique is proposed which searches for a random interleaver resulting in the fewest output sequences with low weights corresponding to input weights of 2 or 3. The authors then use simulation results to show that for short frame transmission systems and bit error rates (BERs) of around 10^{-3}, a block interleaver outperforms the best such found pseudorandom interleaver, and the overall effect of the interleaver is not significant in this range [3]. In [4], however, it is shown that, for turbo codes of large interleaver lengths, pseudorandom interleavers outperform block interleavers significantly, e.g., 2.7 dB at BER of 10^{-5}. Recently, a systematic approach for the design of the interleaver has been proposed in [5]. The method is based on recursively minimizing a cost function to find an interleaver which best breaks a set of *a priori* chosen error patterns. The weight distribution of a turbo code employing the best such found interleaver of length 100 shows 0.5- to 0.9-dB improvement over a randomly selected interleaver of the same length. In [6], a deterministic interleaver design algorithm is proposed based on linear recursion to produce an initial interleaver which is subsequently optimized by pairwise exchange of its elements. These optimized interleavers show more than 0.5-dB improvement over a randomly selected interleaver and about 0.2-dB improvement over an S-random interleaver for BERs of less than 10^{-5} and block length 576. In [7], a mathematical structure is developed for turbo-code interleaver design at low BERs, which achieves more than 0.5-dB improvement over random interleavers for interleaver length 1176. In [8], high-spread interleavers have been designed for specific short interleaver lengths. These interleavers are shown to significantly lower the error floor occurring at high signal-to-noise ratios. Other works related to the design of the interleaver include [9]–[13].

Although the above works implicitly suggest some conclusions regarding the effect of different choices of interleavers on the performance of turbo codes, they are mainly focused on either search algorithms for the best (or at least *good*) interleaver(s) or explaining the behavior of these codes in general. So far, the only statistical study of the turbo code behavior with respect to interleavers considers the upper bound on the maximum-likelihood (ML) performance of the turbo code, averaged over all possible interleavers (e.g., [14]).

If higher order statistical averages of the turbo code performance with respect to the interleaver are known, it will be possible to have a more accurate estimate of the distribution of the performance bound with respect to the interleaver. As a first step, in this correspondence, we study the effect of the interleaver by looking at the variance of the turbo-code performance with respect to all possible interleavers of the same length, under the assumption of an ML decoder. Note that, in practice, turbo codes are decoded iteratively using a non-ML decoder, however, it is a widely accepted conjecture that the performance of the suboptimum iterative decoding converges toward the ML performance. This study tackles the question brought up in [14, Question 3] to give more insight regarding what performance to expect from a turbo code with fixed component codes and interleaver length. It also provides an estimate of how well a particular interleaver performs among the range of all possible interleavers and helps to evaluate the performance of an interleaver search algorithm.

The correspondence is organized as follows. In Section II, a brief review of the turbo-code average performance bound [14] is given and following that, the mathematical formulations for the second moment

Manuscript received June 17, 1999; revised January 21, 2002. This work was supported by Communications and Information Technology Ontario (CITO) and by the Natural Sciences and Engineering Research Council (NSERC) of Canada. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory (ISIT'98), Cambridge, MA, August 1998 and in part at the IEEE Vehicular Technology Conference (VTC'99), Houston, TX, May 1999.

A. H. S. Mohammadi is with LSI Logic Inc., Mailstop AH340, Milpitas, CA 95035 USA (e-mail: atousa@lsil.com).

W. Zhuang is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: wzhuang@bbcr.uwaterloo.ca).

Communicated by F. R. Kschischang, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(02)05159-3.