Constructions of Abelian Codes multiplying dimension of cyclic codes

José Joaquín Bernal*, Diana H. Bueno-Carreño† and Juan Jacobo Simón*.
*Departamento de Matemáticas
Universidad de Murcia, 30100 Murcia, Spain.
Email: {josejoaquin.bernal, jsimon}@um.es
†Departamento de Ciencias Naturales y Matemáticas
Pontificia Universidad Javeriana, Cali, Colombia
Email: dhbueno@javerianacali.edu.co

Abstract

In this note, we apply some techniques developed in [1]–[3] to give a particular construction of bivariate Abelian Codes from cyclic codes, multiplying their dimension and preserving their apparent distance. We show that, in the case of cyclic codes whose maximum BCH bound equals its minimum distance the obtained abelian code verifies the same property; that is, the strong apparent distance and the minimum distance coincide. We finally use this construction to multiply Reed-Solomon codes to abelian codes.

I. Introduction

In [1], we improve the notion and computation of the apparent distance for abelian codes given in [4] and [9] by means of the q-orbit structure of defining sets of abelian codes. These results allows us to design, based on a suitable election of q-orbits, abelian codes having nice bounds and parameters. In this note, we apply those techniques to construct bivariate BCH codes from cyclic codes, in such a way that we preserve apparent distance but multiplying their dimension. We show that, in the case of cyclic codes whose maximum BCH bound equals its minimum distance the obtained abelian code verifies the same property; that is, the strong apparent distance and the minimum distance coincide; in particular, this drives us to multiply dimension Reed-Solomon codes to abelian codes preserving the true minimum distance. **As it happens with others families of abelian codes, there are alternative constructions to get this one (see, for example [6]). We know that each alternative construction shows different structural properties that allows us to see easily, some specific qualities or parameters; as it happens in our case with the apparent distance and the true minimum distance.**

II. Notation and preliminaries

In this section, we introduce the basic concepts and preliminary results. We shall restrict all notions to the bivariate abelian codes; so throughout this paper, Abelian Code will be an ideal in group algebras $\mathbb{F}_qG$, where $\mathbb{F}_q$ denotes the field with q elements with q a power of a prime p and G is an abelian group with a decomposition $G \simeq C_{r_1} \times C_{r_2}$, where C_{r_i} the cyclic group of order r_i, for $i = 1, 2$. It is well-known that this decomposition induces a canonical isomorphism of $\mathbb{F}_q$-algebras from $\mathbb{F}_qG$ to

$$\mathbb{F}_q[X, Y]/\left\langle X^{r_1} - 1, Y^{r_2} - 1\right\rangle.$$

We denote this quotient algebra by $\mathbb{F}_q(r_1, r_2)$. So, we identify the codewords with polynomials $f = f(X, Y)$ such that every monomial satisfy that the degree of the indeterminate X belongs to $\mathbb{Z}_{r_1}$ and the degree of Y belongs to $\mathbb{Z}_{r_2}$, where $\mathbb{Z}_{r_i}$ is the ring of integers modulo r_i, for $i = 1, 2$, that we always write as canonical representatives; so that, for any $a \in \mathbb{Z}$ we denote the canonical representative by $\overline{a}$ if it is possible that $a \notin \{0, \ldots, r_i - 1\}$, otherwise we only write $\overline{a} = a$. We deal with abelian codes in the semisimple case; that is, we always assume that $\gcd(r_i, q) = 1$ for $i = 1, 2$.

We denote $I = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ and for $i = 1, 2$, we denote by U_{r_i} the set of all r_i-th primitive roots of unity and define $U = U_{r_1} \times U_{r_2}$. It is a known fact that, for a fixed $\hat{\alpha} = (\alpha, \beta) \in U$, any abelian code C is determined by its defining set, with respect to $\hat{\alpha}$, which is defined as

$$\mathcal{D}_{\hat{\alpha}}(C) = \left\{(a, b) \in I \ : \ c(\alpha^a, \beta^b) = 0, \ \forall c \in C\right\}.$$

We note that, for any element $f \in \mathbb{F}_q(r_1, r_2)$, viewed as a polynomial, we may also define its defining set as $\mathcal{D}_{\hat{\alpha}}(f) = \{(a, b) \in I \ : \ f(\alpha^a, \beta^b) = 0\}$.

This work was partially supported by MINECO, project MTM2016-77445-P, and Fundación Séneca of Murcia, project 19880/GERM/15. The second author has been supported by Departamento Administrativo de Ciencia, Tecnología e Innovación de la República de Colombia.

Given an element $\mathbf{a} = (a, b) \in I$, we define its q-orbit modulo (r_1, r_2) as the set

$$Q(\mathbf{a}) = \left\{ \left(\overline{a \cdot q^i}, \overline{b \cdot q^i} \right) \in I \ : \ i \in \mathbb{N} \right\}.$$

In our case, it is known that the defining set $\mathcal{D}_{\hat{\alpha}}(C)$ is a disjoint union of q-orbits modulo (r_1, r_2). Conversely, every union of q-orbits modulo (r_1, r_2) determines a bivariate abelian code (see [1], [4] or [5] for details). We recall that the notion of defining set in the case of cyclic codes corresponds to the notion of q-cyclotomic coset of a positive integer a modulo n.

Let $\mathbb{L}|\mathbb{F}_q$ be an extension field containing U_{r_i}, for $i = 1, 2$. The discrete Fourier transform of a polynomial $f \in \mathbb{F}_q(r_1, r_2)$ with respect to $\hat{\alpha} = (\alpha, \beta) \in U$ (also called Mattson-Solomon polynomial in [9]) is the polynomial $\varphi_{\hat{\alpha},f} = \varphi_{\hat{\alpha},f}(X, Y) = \sum_{(i,j)\in I} f(\alpha^i, \beta^j) X^i Y^j \in \mathbb{L}(r_1, r_2)$.

It is known that the discrete Fourier transform may be viewed as an isomorphism of algebras $\varphi_{\hat{\alpha}} : \mathbb{L}(r_1, r_2) \longrightarrow (\mathbb{L}^{|I|}, \star)$, where the multiplication "$\star$" in $\mathbb{L}^{|I|}$ is defined coordinatewise. Thus, we may see $\varphi_{\hat{\alpha},f}$ as a vector in $\mathbb{L}^{|I|}$ or as a polynomial in $\mathbb{L}(r_1, r_2)$ (see [4, Section 2.2]).

As it is usual, we denote by $M = (a_{ij})_I$ the matrix indexed by I (or the I-matrix) with entries in a ring R, and write $a_{ij} = M(i, j)$; in the case of vectors we write $v = (a_i)_{\mathbb{Z}_r}$. For an easy identification of the reader to the results in [1], we denote the i-th row of M as $H_M(1, i)$ and the j-th column of M as $H_M(2, j)$.

In [1], the following definition is used to compute the apparent distance of an abelian code. Let $D \subseteq I$. The matrix afforded by D is defined as $M = (a_{ij})_I$ where $a_{ij} = 1$ if $(i, j) \notin D$ and $a_{ij} = 0$ otherwise. When D is an union of q-orbits we say that M is a q-orbit matrix, and it will be denoted by $M = M(D)$. For any I-matrix M with entries in a ring, we define the support of M as the set $supp(M) = \{(i, j) \in I \ : \ a_{ij} \neq 0\}$, whose complement with respect to I will be denoted by $\mathcal{D}(M)$. Note that, if D is a union of q-orbits then the q-orbit matrix afforded by D verifies that $\mathcal{D}(M(D)) = D$. Finally, we denote the matrix of coefficients of a polynomial $f \in \mathbb{F}(r_1, r_2)$ by $M(f)$.

Let $\mathcal{Q}$ be the set of all the q-orbits in I. We define a partial ordering over the set of q-orbits matrices $\{M(D) \ : \ D = \cup Q, \text{ for some } Q \in \mathcal{Q}$ as follows:

$$M(D) \leq M(D') \Leftrightarrow supp\left(M(D)\right) \subseteq supp\left(M(D')\right). \tag{II.1}$$

Clearly, this condition is equivalent to $D' \subseteq D$.

III. The strong apparent distance and multivariate BCH codes

In [1], we introduced the notion of strong apparent distance of polynomials and hypermatrices and we applied it to define and study a notion of multivariate BCH bound and BCH abelian codes. As it was pointed out in the mentioned paper, the notion of strong apparent distance was based in the ideas and results in [4] and [9]. In this section, we recall some notions and results in [1] restricted to matrices; that is, the bivariate case, because these are the only results that we will use, and it is much simpler to expose.

For a positive integer r, we say that a list of canonical representatives $b_0, \ldots, b_l$ in $\mathbb{Z}_r$ is a list of consecutive integers modulo r, if for each $0 \leq k < l$ we have that $b_{k+1} = \overline{b_k + 1}$ in $\mathbb{Z}_r$ and so $b_k = \overline{b_{k+1} - 1}$. If $b = b_k$ (resp. $b = b_{k+1}$) we denote $b^+ = b_{k+1}$ (resp. $b^- = b_k$).

Definition III.1. Let M be a matrix over $\mathbb{F}_q$. For any $k \in \{1, 2\}$ and $b \in \mathbb{Z}_{r_k}$, the set of zero rows (if $k = 1$) or columns (if $k = 2$) of M associated to the pair (k, b) is the set

$$CH_M(k, b) = \{H_M(k, b_0), \ldots, H_M(k, b_l)\} \quad \text{with } b = b_0,$$

such that $H_M(k, b_j) = 0$ for all $j \in \{0, \ldots, l\}$, $b_0, \ldots, b_l$ is a list of consecutive integers modulo r_k and $H_M(k, b_l^+) \neq 0$. We denote by $\omega_M(k, b)$ the value $|CH_M(k, b)|$; in the case of vectors we write $\omega_M(b) = \omega_M(1, b)$.

We define $\omega_M(k, b) = 0$ if $H_M(k, b) \neq 0$.

Definition III.2. Let q, r_1, r_2 and I be as above and let M be a matrix over $\mathbb{F}_q$. The strong apparent distance of M, denoted by $sd^*(M)$, is defined as follows

1) $sd^*(0) = 0$.
2) The strong apparent distance of a vector $M = v$ is

$$sd^*(v) = \max\{\omega_v(b) + 1 \ : \ b \in \mathbb{Z}_r\}.$$

3) In the case of matrices, we proceed as follows, for $k \in \{1, 2\}$:

$$\begin{aligned} \epsilon_M(k) &= \max\{sd^*(H_M(k, b)) \ : \ b \in \mathbb{Z}_{r_k}\}; \\ \omega_M(k) &= \max\{\omega_M(k, b) \ : \ b \in \mathbb{Z}_{r_k}\}. \end{aligned}$$

Then

3.1) The strong apparent distance of M with respect to the k-th variable is $sd_k^*(M) = \epsilon_M(k) \cdot (\omega_M(k) + 1)$ and

3.2) the strong apparent distance of M is $sd^*(M) = \max_{1\leq k\leq 2}\{sd_k^*(M)\}$.

Now we recall the definition of strong apparent distance of an abelian code in [1] in the bivariate case.

Definition III.3. Let C be a code in $\mathbb{F}_q(r_1, r_2)$. The strong apparent distance of C, with respect to $\hat{\alpha} \in U$, is $sd^*_{\hat{\alpha}}(C) = \min\left\{sd^*\left(M(\varphi_{\hat{\alpha},e})\right) \ : \ 0 \neq e^2 = e \in C\right\}$. The strong apparent distance of C is $sd^*(C) = \max\left\{sd^*_{\hat{\beta}}(C) \ : \ \hat{\beta} \in U\right\}$.

We also define the set of optimized roots of C as $\mathcal{R}(C) = \{\hat{\beta} \in U \ : \ sd^*(C) = sd^*_{\hat{\beta}}(C)\}$.

In [1] it is proved that, for any $f \in C$ and $\hat{\alpha} \in U$, $sd^*_{\hat{\alpha}}(C) = \min\{sd^*(M(\varphi_{\hat{\alpha},c})) \ : \ c \in C\}$ and the weight of f verifies $\omega(f) \geq sd^*(M(\varphi_{\hat{\alpha},f}))$ (see also [4], [9]); so that, the strong apparent distance of an abelian code is a lower bound for the minimum distance; in fact, the strong apparent distance of any cyclic code, in the obvious sense, is exactly the maximum of all its BCH bounds (what P. Camion calls the BCH bound of an abelian code) [4, pp. 21-22]. Indeed, the following result is proved.

Theorem III.4. *[1, Theorem 16] For any abelian code C in $\mathbb{F}_q(r_1, r_2)$ the inequality $sd^*(C) \leq d(C)$ holds.*

In [1], q-orbit matrices and coefficient matrices of the images of the discrete Fourier transform of idempotent elements in $\mathbb{F}(r_1, r_2)$ are related, for a fixed $\hat{\alpha} = (\alpha, \beta)$, as follows. For any idempotent $e \in \mathbb{F}_q(r_1, r_2)$, let E by its generated ideal. Then $M(\varphi_{\hat{\alpha},e}) = M(\mathcal{D}_{\hat{\alpha}}(E))$. Conversely, any q-orbit matrix corresponds with an idempotent; that is, if $P \leq M(\mathcal{D}_{\hat{\alpha}}(E))$ [see (II.1)] then there exists an idempotent $e' \in E$ such that $P = M(\varphi_{\hat{\alpha},e'})$. So it is concluded that the apparent distance of an abelian code C with $M = M(\mathcal{D}_{\hat{\alpha}}(C))$ may be computed by means of q-orbits matrices $P \leq M(\varphi_{\hat{\alpha},e})$; that is $\min\{sd^*(P) \ : \ P \leq M\} = \min\{sd^*(M(\varphi_{\hat{\alpha},e})) \ : \ e^2 = e \in C\}$. This fact drives us to the following definition.

Definition III.5. In the setting described above, for a q-orbits matrix M, the minimum strong apparent distance is

$$msd(M) = \min\{sd^*(P) \ : \ P \leq M\}.$$

Finally, one has [1, Theorem 18] that for any abelian code C in $\mathbb{F}_q(r_1, r_2)$ with generating idempotent e it happens $sd^*_{\alpha}(C) = msd\left(M(\varphi_{\alpha,e})\right)$ ($\alpha \in U$). Therefore,

$$sd^*(C) = \max\{msd\left(M(\varphi_{\hat{\alpha},e})\right) : \hat{\alpha} \in U\}. \tag{III.1}$$

In [1, Section IV] it is presented an algorithm to find, for any abelian code, a list of matrices (or hypermatrices in case of more than 2 variables) representing some of its idempotents whose strong apparent distances go decreasing until the minimum value is reached. It is a kind of "suitable idempotents chase through hypermatrices" [1, p. 2]. This algorithm is based on certain manipulations of the q-orbit matrix afforded by the defining set of the abelian code. We recall a result of this section that we use repeatedly.

Proposition III.6. *[1, Proposition 23] Let D be a union of q-orbits and $M = M(D) \neq 0$. For $1 \leq k \leq 2$ and $b \in \mathbb{Z}_{r_k}$, let $H_M(k, b)$ be a row or column such that $sd^*(M) = (\omega_M(k) + 1)sd^*(H_M(k, b))$; that is, involved row or column in the computation of the strong apparent distance. If $sd^*(H_M(k, b)) = 1$ then $msd(M) = sd^*(M)$.*

Now we recall the definition of multivariate BCH code in the two-dimensional case.

Definition III.7. [1, Definition 33] Let q, r_1, r_2 and I be as above. Let $\gamma \subseteq \{1, 2\}$ and $\delta = \{r_k \geq \delta_k \geq 2 \ : \ k \in \gamma\}$. An abelian code C in $\mathbb{F}_q(r_1, r_2)$ is a bivariate BCH code of designed distance δ if there exists a list of positive integers $b = \{b_k \ : \ k \in \gamma\}$ such that

$$\mathcal{D}_{\hat{\alpha}}(C) = \bigcup_{k\in\gamma} \bigcup_{l=0}^{\delta_k-2} \bigcup_{\mathbf{i}\in I(k,\overline{b_k+l})} Q(\mathbf{i})$$

for some $\hat{\alpha} \in U$, where $\{\overline{b_k}, \ldots, \overline{b_k + \delta_k - 2}\}$ is a list of consecutive integers modulo r_k and $I\left(k, \overline{b_k + l}\right) = \left\{\mathbf{i} \in I \ : \ \mathbf{i}(k) = \overline{b_k + l}\right\}$.

We denote $C = B_q(\alpha, \gamma, \delta, b)$, as usual.

As a direct consequence of [1, Theorem 30] we have $sd^*\left(B_q(\hat{\alpha}, \gamma, \delta, b)\right) \geq \prod_{k\in\gamma} \delta_k$; also, from [1, Theorem 36], we have that

$$\dim_{\mathbb{F}_q} B_q(\hat{\alpha}, \gamma, \delta, b) \geq r_1 r_2 - \operatorname{lcm}\left\{\mathcal{O}_{r_1}(q), \mathcal{O}_{r_2}(q)\right\} \left(\sum_{k\in\gamma} (\delta_k - 1) \prod_{\substack{j\in\{1,2\}\\ j\neq k}} r_j\right),$$

where $\mathcal{O}_{r_k}(q)$ denotes the multiplicative order of q modulo r_k. In fact, $B_q(\alpha, \gamma, \delta, b)$ is the abelian code with highest dimension over $\mathbb{F}_q$, whose defining set contains $\cup_{k=1}^{2}\{\overline{b_k}, \ldots, \overline{b_k + \delta_k - 2}\}$, of the sets described above, as it happens with the (cyclic) BCH codes [1, Corollary 35].

Example III.8. Let C_1 and C_2 be abelian codes in $\mathbb{F}_{2^2}(7, 9)$ with defining sets $\mathcal{D}(C_1) = Q(0, 0) \cup Q(1, 0) \cup Q(3, 0) \cup \left(\cup_{t=0}^{6} Q(t, 1)\right)$ and $\mathcal{D}(C_2) = \mathcal{D}(C_1) \cup Q(0, 2) \cup Q(0, 3) \cup Q(0, 6)$. Then one may check that $C_1 = B_{2^2}\left(\hat{\alpha}, \{2\}, \{3\}, \{0\}\right)$ and $C_2 = B_{2^2}\left(\hat{\alpha}, \{1, 2\}, \{2, 3\}, \{0, 0\}\right)$.

IV. Multiplying dimension in abelian codes

We shall construct abelian codes starting from BCH (univariate) codes with designed distance $\delta \in \mathbb{N}$. We keep all notation from the preceding sections.

Lemma IV.1. *Let D be a union of q-orbits modulo (r_1, r_2) and consider the q-orbits matrix $M = M(D)$. The following conditions on M are equivalent:*

1) *Each column $H_M(2, j)$ verifies that either $H_M(2, j) = 0$ or all of its entries have constant value 1.*
2) *For all $(i, j) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$, it happens that $(i, j) \in D$ if and only if $(x, j) \in D$ for all $x \in \mathbb{Z}_{r_1}$.*

Proof. The result comes immediately from the definition of (hyper)matrix afforded by D; that is, for any $a_{ij} \in M$, $a_{ij} = 0$ if and only if $(i, j) \in D$ and, otherwise, $a_{ij} = 1$. □

As the reader may see, an analogous result may be obtained by replacing r_2 by r_1. For our next theorem we recall the definition of the set of optimized roots of C as $\mathcal{R}(C) = \{\beta \in U \ : \ sd^*(C) = sd^*_\beta(C)\}$.

Theorem IV.2. *Let n and r be positive integers such that $\gcd(q, nr) = 1$. Let C be a nonzero cyclic code in $\mathbb{F}_q(r)$ with $sd^*(C) = \delta > 1$ and $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_n \times \mathcal{R}(C)$. Then, the abelian code C_n in $\mathbb{F}_q(n, r)$ with defining set $\mathcal{D}_{\hat{\alpha}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\alpha_2}(C)$ verifies that $sd^*(C_n) = \delta$ and $\dim_{\mathbb{F}_q}(C_n) = n \dim_{\mathbb{F}_q}(C)$.*

Proof. Consider any $\hat{\beta} = (\beta_1, \beta_2) \in U_n \times U_r$ and let C_n be the abelian code such that $\mathcal{D}_{\hat{\beta}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\beta_2}(C)$. It is clear that $\mathcal{D}_{\hat{\beta}}(C_n)$ satisfies the condition *(2)* of Lemma IV.1; so, the q-orbits matrix afforded by $\mathcal{D}_{\hat{\beta}}(C_n)$, say $M = M(\mathcal{D}_{\hat{\beta}}(C_n))$, verifies the condition *(1)* of that lemma. Clearly, since $C \neq 0$ there is at least one nonzero column. If $N = (a_j)_{j \in \mathbb{Z}_r}$ is the q-orbit vector afforded by $\mathcal{D}_{\beta_2}(C)$ then $H_M(2, j) = 0$ if and only if $a_j = 0$. (We only focus in $k = 2$ on view of Proposition III.6.)

So, $\omega_M(2, b) = \omega_N(1, b)$ for all $b \in \mathbb{Z}_r$ and hence $\omega_M(2) = sd^*(N) \leq \delta$, and the equality is reached when $\beta_2 \in \mathcal{R}(C)$. On the other hand, we have that $sd^*(H_M(2, b)) = 1$, for any nonzero column; so that, $\epsilon_M(2) = 1$, and this happens for any element of U_n. Hence $sd^*(M) \leq \delta$. Now, by Proposition III.6, $sd^*_{\hat{\beta}}(C_n) = msd(M) = sd^*(M) \leq \delta$, and the equality is reached if $\beta_2 \in \mathcal{R}(C)$; so that $sd^*(C_n) = \delta$.

Finally, since $\dim_{\mathbb{F}_q}(C_n) = |supp(M)|$, we have that $\dim_{\mathbb{F}_q}(C_n) = n \dim_{\mathbb{F}_q}(C)$. □

Now we shall see that this multiplying dimensions technique extends BCH (cyclic) codes to multivariate BCH abelian codes.

Corollary IV.3. *In the setting of theorem above, if C is a BCH code $C = B_q(\alpha_2, \delta, b)$ then $C_n = B_q\left((\alpha_1, \alpha_2), \{2\}, \{\delta\}, \{b\}\right)$*

Proof. Immediate from Definition III.7 and the theorem above. □

Example IV.4. Set $q = 2$, $r = 55$, $n = 3$, $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_3 \times U_{55}$ and let C be the cyclic code in $\mathbb{F}_2(55)$ with defining set with respect to α_2, $D = \mathcal{D}_{\alpha_2}(C) = C_2(1) \cup C_2(5)$. Set $M = M(D)$. A simple inspection on M shows us that C is a BCH code with parameters $C = B_2(\alpha_2, 7, 13)$ and dimension 25. By the corollary above, we may construct the new bivariate code C_3 with defining set $\mathcal{D}_{\hat{\alpha}}(C_3) = \mathbb{Z}_3 \times D$. So that $C_3 = B_2(\hat{\alpha}, \{2\}, \{7\}, \{13\})$ in $\mathbb{F}_2(3, 55)$, $sd^*(C_3) = 7$ and $\dim_{\mathbb{F}_2}(C_3) = 75$.

In [3] we determine some types of abelian codes whose minimum distance equals their strong apparent distance. We now apply these techniques to go further and construct multiplied dimensional abelian codes with the same property.

Proposition IV.5. *Let n and r be positive integers with $\gcd(q, nr) = 1$ and let C be a nonzero cyclic code in $\mathbb{F}_q(r)$ such that $sd^*(C) = d(C)$. Then there exists $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_n \times \mathcal{R}(C)$ such that the abelian code C_n in $\mathbb{F}_q(n, r)$ with defining set $\mathcal{D}_{\hat{\alpha}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\alpha_2}(C)$ verifies the equality $d(C_n) = d(C)$.*

Proof. Since $sd^*(C) = d(C)$ then, by [2, Theorem 1] there exists $b' \in \mathbb{L}(r)$ and $h \in \mathbb{Z}_r$ such that $Y^h b' \mid Y^r - 1$ and there exists $\alpha_2 \in U_r$ such that $\varphi^{-1}_{\alpha_2, b'} \in C$. Set $b = Y^h b'$. On the other hand, setting $a = \sum_{i=0}^{n-1} X^i$, we have that, $a \mid X^n - 1$ and that $\varphi^{-1}_{\alpha_1, a} \in \mathbb{F}_q(n)$, for any $\alpha_1 \in U_n$. Now, a direct aplication of [3, Theorem 36] gives us that $sd^*(C_n) = d(C_n)$ and hence by the theorem above $d(C_n) = d(C)$. □

Combinning this proposition with the construction techniques in [2] we may find a number of examples of Abelian Codes C, satisfying the equality $sd^*(C) = d(C)$. For example, from [2, Corollary 7], we know that in the case $r = 2^m - 1$, for any $m \in \mathbb{N}$, for each $n \in \mathbb{N}$ there are at least $\frac{\phi(r)}{m}$ binary multiplied-dimension abelian codes C_n such that $sd^*(C_n) = d(C_n)$.

Let us multiply dimension of some famous BCH codes. It is known (see [8]) for any $h, m \in \mathbb{N}$, if C is a BCH code of length $r = q^m - 1$ and designed distance $\delta = q^h - 1$ over $\mathbb{F}_q$ then $d(C) = \Delta(C)$. As a direct consequence we have

Corollary IV.6. *Let $h, m \in \mathbb{N}$. If C is a BCH code of length $r = q^m - 1$ and designed distance $\delta = q^h - 1$ over $\mathbb{F}_q$ then $d(C_n) = sd^*(C_n)$, for any $n \in \mathbb{N}$, with $gcd(n, q) = 1$.*

In order to multiply dimension from multivariate Reed Solomon codes we have the following result that we present in the multivariate case instead of bivariate case.

Proposition IV.7. *Let $B_q(\hat{\alpha}, \gamma, \delta, b)$ be a multivariate BCH code with $\gamma = \{k\}$, $\delta = \{\delta_k\}$ and $b = \{b_k\}$, for some $k \in \{1, \ldots, s\}$. If $r_k = q - 1$ then we have $sd^*_{\hat{\alpha}}(B_q(\hat{\alpha}, \gamma, \delta, b)) = \delta_k$ and $\dim_{\mathbb{F}_q}(B_q(\hat{\alpha}, \gamma, \delta, b)) = (r_k - \delta_k + 1)\prod_{\substack{j=1 \\ j \neq k}}^{s} r_j$.*

Proof. Set $C = B_q(\hat{\alpha}, \gamma, \delta, b)$ and suppose that $C \neq 0$. Since $r_k = q - 1$ we have that $lq \equiv l \mod r_k$, for all $l \in \mathbb{Z}_{r_k}$; hence $Q(\mathbf{i}) \subseteq I(k, l)$ for all $\mathbf{i} \in I(k, l)$. So,

$$\mathcal{D}_{\hat{\alpha}}(C) = \bigcup_{l=\overline{b_k}}^{\overline{b_k+\delta_k-2}} I(k, l).$$

Since $\dim_{\mathbb{F}_q}(C) = \prod_{j=1}^{s} r_j - |\mathcal{D}_{\hat{\alpha}}(C)|$ we have that $\dim_{\mathbb{F}_q}(C) = (r_k - \delta_k + 1)\prod_{\substack{j=1 \\ j \neq k}}^{s} r_j$. Note that if $M = M(\mathcal{D}_{\hat{\alpha}}(C))$ and $l \in \{\overline{b_k}, \ldots, \overline{b_k + \delta_k - 2}\}$ then $H_M(k, l) = 0$ and all nonzero hypercolumns have entries with constant value 1. Therefore, $\omega_M(k, \overline{b_k}) = \delta_k - 1$ and $\epsilon_M(k) = 1$, which give us $sd^*_k(M) = \delta_k$.

Moreover, following the terminology of Proposition III.6, every nonzero hypercolumn $H_M(k, t)$ is an involved hypercolumn and have entries with constant value 1, so that by such proposition $msd(M) = sd^*(M) = \delta_k$. Therefore, $sd^*_{\hat{\alpha}}(B_q(\hat{\alpha}, \gamma, \delta, b)) = \delta_k$. □

The proposition above is applicable to codes that we obtain by using the construction given in Theorem IV.2, when we start from Reed-Solomon codes. The following proposition allows us to compute dimension and true minimum distance.

Corollary IV.8. *Let $R = B_q(\alpha, \delta, b)$ be a Reed-Solomon code of length r. Then, for each positive integer n and any $\alpha' \in U_n$, there exists a multivariate BCH code, $C = B_q((\alpha', \alpha), \{2\}, \{\delta\}, \{b\})$, such that $\dim(C) = (r - \delta + 1)\, n = n \cdot \dim_{\mathbb{F}_q}(R)$ and $d(C) = sd^*_{\hat{\alpha}}(C) = \delta$.*

Proof. Apply [3, Section 5.2] to results above. □

As a direct consequence of the corollary above, we may conclude that abelian codes that are multiplied Reed-Solomon codes are never MDS codes. In fact, we do not know MDS abelian codes having minimum distance greater than 1.

Example IV.9. A popular Reed Solomon code is the $RS(255, 223)$ (see [7]), in our notation $R = B_{2^8}(\alpha, 33, 0)$. By multiplying its dimension by 5, we get $C_5 = B_{2^8}((\alpha', \alpha), \{2\}, \{33\}, \{0\})$, such that $\dim(C_5) = 1115$ and $d(C_5) = 33$.

An interesting task would be to find decoding methods for these kinds of codes.

V. Conclusion

In this note, we gave a particular construction of bivariate Abelian Codes from cyclic codes, multiplying their dimension and preserving their apparent distance. In the case of cyclic codes whose maximum BCH bound equals its minimum distance the obtained abelian code verifies the same property; that is, the strong apparent distance and the minimum distance coincide. This construction may be used to multiply Reed-Solomon codes to abelian codes.

References

[1] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, *Apparent distance and a notion of BCH multivariate codes*. IEEE Trans. Inform. Theory, **62**(2), 2016, 655-668.

[2] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, Cyclic and BCH Codes whose Minimum Distance Equals their Maximum BCH bound, Adv Math Comm, 10 (2016), 459-474.

[3] J. J. Bernal, M. Guerreiro, J. J. Simón, From ds-bounds for cyclic codes to true minimum distance for abelian codes. To appear. IEEE Trans. Inform. Theory. DOI: 10.1109/TIT.2018.2868446

[4] P. Camion, *Abelian Codes*, MRC Tech. Sum. Rep. # 1059, University of Wisconsin, 1971.

[5] H. Imai, *A theory of two-dimensional cyclic codes*. Information and Control **34**(1) (1977) 1-21.

[6] J. M. Jensen, The concatenated structure of cyclic and abelian codes, IEEE Trans. Inform. Theory, vol. IT-31, pp. 788-793, 1985.

[7] Y. Laijin, L. Ming, Design and implementation of RS(255,223) decoder on FPGA. In *High Density Microsystem Design and Packaging and Component Failure Analysis, 2004. HDP '04. Proceeding of the Sixth IEEE CPMT Conference on*, Shanghai, China, 30 June-3 July 2004.

[8] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[9] R. Evans Sabin, *On Minimum Distance Bounds for Abelian Codes*, Applicable Algebra in Engineering Communication and Computing, Springer-Verlag, 1992.