From ds-bounds for cyclic codes to true minimum distance for abelian codes.

J.J. Bernal, M. Guerreiro* and J. J. Simón †‡

Abstract

In this paper we develop a technique to extend any bound for the minimum distance of cyclic codes constructed from its defining sets (ds-bounds) to abelian (or multivariate) codes through the notion of $\mathbb{B}$-apparent distance. We also study conditions for an abelian code to verify that its $\mathbb{B}$-apparent distance reaches its (true) minimum distance. Then we construct some codes as an application.

Keywords: Abelian code, bounds for minimum distance, true minimum distance, algorithm.

1 Introduction

The study of abelian codes is an important topic in Coding Theory, having an extensive literature, because they have good algebraic properties that allow one to construct good codes with efficient encoding and decoding algorithms. More precisely, regarding decoding, the two most known general techniques are permutation decoding [2] and the so-called locator decoding [6] that uses the Berlekamp-Massey algorithm [21] (see also [16]).

Even though the mentioned decoding methods require to know the minimum distance, or a bound for it, there are not much literature or studies on its computation and properties, or it does exist only for specific families of abelian codes (see [6]). Concerning BCH bound, in [10], P. Camion introduces an extension from cyclic to abelian codes which is computed through the apparent distance of such codes. Since then there have appeared some papers improving the original computation and giving a notion of multivariate BCH bound and codes (see, for example, [3, 20]).

*M. Guerreiro is with Departamento de Matemática, Universidade Federal de Viçosa, 36570-900 Viçosa-MG, Brazil. Supported by CNPq-Brazil, Processo PDE 233497/2014-5. E-mail: marines@ufv.br

†J. J. Bernal and J. J. Simón are with the Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain. Partially supported by MINECO project MTM2016-77445-P and Fundación Séneca of Murcia. E-mail: {josejoaquin.bernal, jsimon}@um.es

‡This work was partially presented at the ISITA 2016, Monterey, CA, USA.

These advances lead us to some natural questions about the extension to the multivariate case of all generalizations and improvements of the BCH bound known for cyclic codes; specifically, those bounds on the minimum distance for cyclic codes which are defined from defining sets.

There are dozens of papers on this topic regarding approaches from matrix methods ([5, 24]) through split codes techniques ([12, 15]) until arriving at the most classical generalizations based on computations over the defining set, as the Hartmann-Tzeng (HT) bound [13], the Ross (R) bound [19] and the improvements by Van Lint and Wilson, as the shifting bound (SB) [22].

Having so many references on the subject, it seems very necessary to find a general method that allows one to extend any bound for the minimum distance of cyclic codes based on the defining set to the multivariate case. This is our first goal. We shall show a method to extend to the multivariate case any bound of the mentioned type via associating an apparent distance to such bound.

The second target of our study is to improve the searching for new bounds for abelian codes. At this point, we must honestly say that these searches may only have interest for codes whose minimum distances are not known (in fact, if one knows the minimum distance of a code one does not need a bound for it), so that, our examples consider codes of lengths necessarily large. In our opinion, long abelian codes are not so bad (see [1]) in terms of performance.

As we work with long codes, certainly it seems impossible at the moment to compute their minimum distance, and so, it is natural to ask for conditions on them to ensure that a founded bound is in fact the minimum distance. This is the last goal of this paper. We found conditions for a bivariate abelian code to reach the mentioned equality and we write these conditions in terms of its defining set from the notion of composed polynomial matrices (CP-matrices, for short). We comment the extension of these results to several variables. We illustrate with some examples (of large codes) how this technique works.

In order to achieve our goals, we give in Section 3 a notion of defining set bound (ds-bound) for the minimum distance of cyclic codes. In Section 4, we revisit the relation between the weight of codewords of abelian codes and the apparent distance of their discrete Fourier transforms. Then we mention how this technique works, as in [3], to define and compute the apparent distance of an abelian code with respect to a set of ds-bounds (see also [4]). Finally, we study the abelian codes which verify the equality between its BCH bound and its minimum distance. For two variables, we find some sufficient conditions that are easy to extend to several variables.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements, with q a power of a prime p, r_i be positive integers, for all $i \in \{1, \dots, s\}$, and $n = r_1 \cdots r_s$. We denote by $\mathbb{Z}_{r_i}$ the ring of integers modulo r_i and we shall always write its elements as canonical representatives. We also denote by π_i the projection of a direct product of sets onto the i-th factor set.

An **abelian code** of length n is an ideal in the algebra $\mathbb{F}_q(r_1,\dots,r_s) = \mathbb{F}_q[X_1,\dots,X_s]/\langle X_1^{r_1}-1,\dots,X_s^{r_s}-1\rangle$ and throughout this work we assume that this algebra is semisimple; that is, $\gcd(r_i,q)=1$, for all $i\in\{1,\dots,s\}$. Abelian codes are also called multidimensional cyclic codes (see, for example, [14]).

The codewords are identified with polynomials $f(X_1,\dots,X_s)$ in which, for each monomial, the degree of the indeterminate X_k belongs to $\mathbb{Z}_{r_k}$. The weight of a codeword c, is denoted by $\omega(c)$. We denote by I the set $\mathbb{Z}_{r_1}\times\cdots\times\mathbb{Z}_{r_s}$ and we write the elements $f\in\mathbb{F}_q(r_1,\dots,r_s)$ as $f=f(X_1,\dots,X_s)=\sum a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$, where $\mathbf{i}=(i_1,\dots,i_s)\in I$ and $\mathbf{X}^{\mathbf{i}}=X_1^{i_1}\cdots X_s^{i_s}$. Given a polynomial $f\in\mathbb{F}_q[X_1,\dots,X_s]$ we denote by $\overline{f}$ its image under the canonical projection onto $\mathbb{F}_q(r_1,\dots,r_s)$.

For each $i\in\{1,\dots,s\}$, we denote by R_{r_i} (resp. U_{r_i}) the set of all r_i-th roots of unity (resp. all r_i-th primitive roots of unity) and define $R=\prod_{i=1}^s R_{r_i}$ ($U=\prod_{i=1}^s U_{r_i}$).

For $f=f(X_1,\dots,X_s)\in\mathbb{F}_q[X_1,\dots,X_s]$ and $\bar\alpha\in R$, we write $f(\bar\alpha)=f(\alpha_1,\dots,\alpha_s)$. For $\mathbf{i}=(i_1,\dots,i_s)\in I$, we write $\bar\alpha^{\mathbf{i}}=(\alpha_1^{i_1},\dots,\alpha_s^{i_s})$.

It is a known fact that every abelian code C in $\mathbb{F}_q(r_1,\dots,r_s)$ is totally determined by its **root set** or **set of zeros**, namely

$$Z(C)=\{\bar\alpha\in R \mid f(\bar\alpha)=0,\quad \text{for all } \ f\in C\}.$$

The set of non zeros is denoted by $\overline{Z(C)}=R\setminus Z(C)$. For a fixed $\bar\alpha\in U$, the code C is determined by its **defining set**, with respect to $\bar\alpha$, which is defined as

$$\mathcal{D}_{\bar\alpha}(C)=\left\{\mathbf{i}\in I \mid f(\bar\alpha^{\mathbf{i}})=0,\ \text{for all } f\in C\right\}.$$

Given an element $a=(a_1,\dots,a_s)\in I$, we shall define its **q-orbit** modulo $(r_1,\dots,r_s)$ as $Q(a)=\left\{\left(a_1\cdot q^i,\dots,a_s\cdot q^i\right)\in I \mid i\in\mathbb{N}\right\}$. In the case of a semisimple algebra, it is known that any defining set $\mathcal{D}_{\bar\alpha}(C)$ is a disjoint union of q-orbits modulo $(r_1,\dots,r_s)$. Conversely, every union of q-orbits modulo $(r_1,\dots,r_s)$ determines an abelian code (an ideal) in $\mathbb{F}_q(r_1,\dots,r_s)$ (see, for example, [3] for details). We note that the notions of root set and defining set also apply to polynomials; so that, for $f\in\mathbb{F}_q(r_1,\dots,r_n)$ we also define $Z(f)$, $\overline{Z(f)}$ and $\mathcal{D}_{\bar\alpha}(f)$ in the obvious way. Moreover, if C is the ideal generated by the polynomial f in $\mathbb{F}_q(r_1,\dots,r_n)$, then $\mathcal{D}_{\bar\alpha}(C)=\mathcal{D}_{\bar\alpha}(f)$.

We recall that the notion of defining set also applies to cyclic codes. For $s=1$ and $r_1=n$, a q-orbit is called a **q-cyclotomic coset** of a positive integer b modulo n and it is the set $C_q(b)=\{b\cdot q^i\in\mathbb{Z}_n \mid i\in\mathbb{N}\}$, keeping the traditional notation.

Throughout this paper, we fix the notation $\mathbb{L}|\mathbb{F}_q$ for an extension field containing U_{r_i}, for all $i\in\{1,\dots,s\}$. The **discrete Fourier transform of a polynomial** $f\in\mathbb{F}_q(r_1,\dots,r_s)$ **with respect to** $\bar\alpha\in U$ (also called Mattson-Solomon polynomial in [20]) is the polynomial $\varphi_{\bar\alpha,f}(\mathbf{X})=\sum_{\mathbf{j}\in I}f(\bar\alpha^{\mathbf{j}})\mathbf{X}^{\mathbf{j}}\in\mathbb{L}(r_1,\dots,r_s)$. It is known that the discrete Fourier transform may be viewed as an isomorphism of algebras $\varphi_{\bar{\alpha}} : \mathbb{L}(r_1, \ldots, r_s) \longrightarrow (\mathbb{L}^{|I|}, \star)$, where the multiplication "$\star$" in $\mathbb{L}^{|I|}$ is defined coordinatewise. Thus, we may see $\varphi_{\bar{\alpha},f}$ as a vector in $\mathbb{L}^{|I|}$ or as a polynomial in $\mathbb{L}(r_1, \ldots, r_s)$ (see [10, Section 2.2]). The inverse of the discrete Fourier transform is $\varphi^{-1}_{\bar{\alpha},g}(\mathbf{X}) = \frac{1}{r_1 r_2 \cdots r_s} \sum_{\mathbf{j}\in I} g(\bar{\alpha}^{-\mathbf{j}})\mathbf{X}^{\mathbf{j}}$.

3 Defining set bounds for cyclic codes

In this section we deal with cyclic codes; that is, $r_1 = n$. By $\mathcal{P}(\mathbb{Z}_n)$ we denote the power set of $\mathbb{Z}_n$. We take an arbitrary $\alpha \in U_n$.

Definition 1 *A* ***defining set bound*** *(or* ***ds-bound****, for short) for the minimum distance of cyclic codes is a family of relations $\delta = \{\delta_n\}_{n\in\mathbb{N}}$ such that, for each $n \in \mathbb{N}$, $\delta_n \subseteq \mathcal{P}(\mathbb{Z}_n) \times \mathbb{N}$ and it satisfies the following conditions:*

1. *If C is a cyclic code in $\mathbb{F}(n)$ such that $C \neq (0), \mathbb{F}_q(n)$ and $N \subseteq \mathcal{D}_\alpha(C)$, then $1 \leq a \leq d(C)$, for all $(N, a) \in \delta_n$.*
2. *If $N \subseteq M$ are subsets of $\mathbb{Z}_n$ then $(N, a) \in \delta_n$ implies $(M, a) \in \delta_n$.*
3. *For all $N \in \mathcal{P}(\mathbb{Z}_n)$, $(N, 1) \in \delta_n$.*

From now on, sometimes we write simply δ to denote a ds-bound or any of its elements independently on the length n of the code. It will be clear from the context which one is being used.

Remarks 2 **(1)** For example, the BCH bound states that, for any cyclic code in $\mathbb{F}_q(n)$ which in its set of zeros has a string of $t-1$ consecutive powers of some $\alpha \in U_n$, the minimum distance of the code is at least t [17, Theorem 7.8].

Now, define $\delta \subset \mathcal{P}(\mathbb{Z}_n) \times \mathbb{N}$ as follows: for any $a \geq 2$, $(N, a) \in \delta$ if and only if there exist $i_0, i_1, \ldots, i_{a-2}$ in N which are consecutive integers modulo n. Then the BCH bound says that δ is a ds-bound for any cyclic code (we only have to state Condition 3 as a convention; so that $(\emptyset, 1) \in \delta_{BCH}$).

(2) It is easy to check that all extensions of the BCH bound, all new bounds from the defining set of a cyclic code as in [5, 13, 18, 19, 24] and the new bounds and improvements arising from Corollary 1, Theorem 5 and results in Section 4 and Section 5 in [22], also verify Definition 1.

In general, for any bound for the minimum distance of a cyclic code, say b, we denote the corresponding ds-bound by δ_b. In order to relate the idea of ds-bound with the Camion's apparent distance, which will be defined later, we consider the following family of maps.

Definition 3 *Let δ be a ds-bound for the minimum distance of cyclic codes. The* ***optimal ds-bound associated to*** *δ is the family $\overline{\delta} = \{\overline{\delta}_n\}_{n\in\mathbb{N}}$ of maps $\overline{\delta}_n : \mathcal{P}(\mathbb{Z}_n) \longrightarrow \mathbb{N}$ defined as $\overline{\delta}_n(N) = \max\{b \in \mathbb{N} \mid (N, b) \in \delta_n\}$.*

The following result is immediate.

Lemma 4 *Let δ be a ds-bound for the minimum distance of cyclic codes. Then, for each $n \in \mathbb{Z}$:*

1. *If C is a cyclic code in $\mathbb{F}(n)$ such that $N \subseteq \mathcal{D}_\alpha(C)$, then $1 \leq \overline{\delta}_n(N) \leq d(C)$.*
2. *If $N \subseteq M \subseteq \mathbb{Z}_n$, then $\overline{\delta}_n(N) \leq \overline{\delta}_n(M)$.*

As we noted above, we may omit the index of the map $\overline{\delta}_n$, because it will be clear from the context for which value it is being taken.

4 Apparent distance

We begin this section recalling the notion and notation of a hypermatrix that will be used hereby, as it is described in [3]. For any $\mathbf{i} \in I = \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$, we write its k-th coordinate as $\mathbf{i}(k)$. A **hypermatrix with entries in a field S indexed by I (or an I-hypermatrix over S)** is an s-dimensional I-array, denoted by $M = (a_{\mathbf{i}})_{\mathbf{i}\in I}$, with $a_{\mathbf{i}} \in S$ [23]. The set of indices, the dimension and the ground field will be omitted if they are clear from the context. For $s = 2$, M is a matrix and when $s = 1$, M is a vector. We write $M = 0$ when all its entries are zero and $M \neq 0$, otherwise. As usual, a **hypercolumn** is defined as $H_M(j,k) = \{a_{\mathbf{i}} \in M \mid \mathbf{i}(j) = k\}$, with $1 \leq j \leq s$ and $0 \leq k < r_j$, where $a_{\mathbf{i}} \in M$ means that $a_{\mathbf{i}}$ is an entry of M. A hypercolumn can be seen as an $(s-1)$-dimensional hypermatrix. In the case $s = 2$, we refer to hypercolumns as rows or columns and, when $s = 1$, we say entries.

For any I-hypermatrix M with entries in a field, we define the support of M as the set $\operatorname{supp}(M) = \{\mathbf{i} \in I \mid a_{\mathbf{i}} \neq 0\}$. Its complement with respect to I will be denoted by $\mathcal{D}(M)$. When $\mathcal{D}(M)$ (or $\operatorname{supp}(M)$) is an union of q-orbits we say that M is a **q-orbit hypermatrix**. Let $D \subseteq I$. The **hypermatrix afforded by** D is defined as $M = (a_{\mathbf{i}})_{\mathbf{i}\in I}$, where $a_{\mathbf{i}} = 1$ if $\mathbf{i} \notin D$ and $a_{\mathbf{i}} = 0$ otherwise; it will be denoted by $M = M(D)$. Note that if D is union of q-orbits then $M(D)$ is a q-orbit hypermatrix. To define and compute the apparent distance of an abelian code we will use the hypermatrix afforded by its defining set, with respect to $\bar{\alpha} \in U$.

We define a partial ordering on the set $\{M(D) \mid D \text{ is union of } q\text{-orbits in } I\}$ as follows:

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

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

We begin with the apparent distance of a vector in $\mathbb{L}^n$.

Definition 5 *Let δ be a ds-bound for the minimum distance of cyclic codes and $v \in \mathbb{L}^n$ a vector. The **apparent distance of** v **with respect to** δ (or δ-**apparent distance of** v, for short), denoted by $\delta^*(v)$, is defined as*

1. *If $v = 0$, then $\delta^*(v) = 0$.*

2. *If* $v \neq 0$*, then* $\delta^*(v) = \overline{\delta}(\mathbb{Z}_n \setminus \mathrm{supp}(v))$.

From now on we denote by $\mathbb{B}$ a set of ds-bounds which are used to proceed a computation of the apparent distances of matrices, hypermatrices or abelian codes.

Definition 6 *Let* $v \in \mathbb{L}^n$*. The* ***apparent distance of*** v ***with respect to*** $\mathbb{B}$ *denoted by* $\Delta_{\mathbb{B}}(v)$*, is:*

1. *If* $v = 0$*, then* $\Delta_{\mathbb{B}}(v) = 0$.
2. *If* $v \neq 0$*, then* $\Delta_{\mathbb{B}}(v) = \max\{\delta^*(v) \mid \delta \in \mathbb{B}\}$.

Remarks 7 *The following properties arise straightforward from the definition above, for any* $v \in \mathbb{L}^n$*.*

1. *If* $v \neq 0$ *then* $\Delta_{\mathbb{B}}(v) \geq 1$.
2. *If* $\mathrm{supp}(v) \subseteq \mathrm{supp}(w)$ *then* $\Delta_{\mathbb{B}}(v) \geq \Delta_{\mathbb{B}}(w)$.

Proposition 8 *Let* $f \in \mathbb{L}(n)$ *and* v *be the vector of its coefficients. Fix any* $\alpha \in U_n$*. Then* $\Delta_{\mathbb{B}}(v) \leq \omega(\varphi_{\alpha,f}^{-1}) = |\overline{Z(f)}|$.

Proof. Set $N = \mathbb{Z}_n \setminus \mathrm{supp}(v)$ and let C be the abelian code generated by $\varphi_{\alpha,f}^{-1}$ in $\mathbb{L}(n)$. Then $d(C) \leq \omega(\varphi_{\alpha,f}^{-1})$. By properties of the discrete Fourier transform, we have $N = \mathcal{D}_\alpha(\varphi_{\alpha,f}^{-1}) = \mathcal{D}_\alpha(C)$ hence, by Lemma 4 and the definition of apparent distance, $\Delta_{\mathbb{B}}(v) \leq d(C)$. This gives the desired inequality. The last equality is obviuos. ■

The notion of apparent distance appeared for the first time in [10] and originally it was defined for polynomials. Its computation reflects a bound of the nonzeros (in the sense given in the preliminaries) of a *multivariate* polynomial. The aim of the apparent distance was to extend the notion of BCH bound, from cyclic to abelian codes as we will comment in the following paragraphs. The first algorithm for its computation was made in terms of coefficients of polynomials. Later, in [20], R. E. Sabin gave an algorithm in terms of matrices. The notion of strong apparent distance, that appeared in [3], is a slight but powerful modification of the original one, defined for multivariate polynomials and hypermatrices, and it is the predecessor of the current apparent distance defined with respect to a list of ds-bounds.

Remark 9 To identify notations from previous works with the ones used here, given a polynomial $f \in \mathbb{F}_q(r_1, \ldots, r_s)$, if we denote by $M(f)$ its hypermatrix of coefficients (in the obvious sense), then the strong apparent distance of f in [3] is $sd^*(f) = \Delta_{\delta_{BCH}}(M(f))$; that is, $\mathbb{B} = \{\delta_{BCH}\}$, together with $\overline{\delta}_{BCH}(\emptyset) = 1$.

Now let us show how the notion of apparent distance for abelian codes works as the BCH bound for cyclic codes. All results in the following corollary are proved in [10] and [20].

Corollary 10 *Let C be a cyclic code in $\mathbb{F}_q(n)$ and $\alpha \in U_n$. Then*

1. *If $g, e \in C$ are the generating polynomial and the idempotent generator of C, respectively, then $\Delta_{\mathbb{B}}\left[M\left(\varphi_{\alpha,g}\right)\right] = \Delta_{\mathbb{B}}\left[M\left(\varphi_{\alpha,e}\right)\right] \leq \Delta_{\mathbb{B}}\left[M\left(\varphi_{\alpha,c}\right)\right]$, for all $c \in C$.*

2. *If $c \in C$ is a codeword with $\varphi_{\alpha,c} = f \in \mathbb{L}(n)$, then $\omega(c) \geq \Delta_{\mathbb{B}}(M(f))$ and consequently*

3. *$\Delta_{\mathbb{B}}\left[M\left(\varphi_{\alpha,g}\right)\right] = \Delta_{\mathbb{B}}\left[M\left(\varphi_{\alpha,e}\right)\right] = \min\left\{\Delta_{\mathbb{B}}\left[M\left(\varphi_{\alpha,c}\right)\right] \mid c \in C\right\} \leq d(C)$.*

The number on the left of the last inequality is known as the ***apparent distance of the cyclic code*** C ***with respect to the set*** $\mathbb{B}$ ***and*** $\alpha \in U_n$ *or the $\mathbb{B}$-apparent distance of C with respect to $\alpha \in U_n$.*

Proof. *(1)* comes from the fact that, for all $c \in C$, we have $\operatorname{supp}\left(M\left(\varphi_{\alpha,c}\right)\right) \subseteq \operatorname{supp}\left(M\left(\varphi_{\alpha,g}\right)\right) = \operatorname{supp}\left(M\left(\varphi_{\alpha,e}\right)\right)$, together with Remark 7. *(2)* is Proposition 8. *(3)* is immediate from *(1)* and *(2)*. ■

Now we shall define the apparent distance of matrices and hypermatrices with respect to a set $\mathbb{B}$ of ds-bounds.

Definition 11 *Let M be an s-dimensional I-hypermatrix over a field $\mathbb{L}$. The* ***apparent distance of*** M ***with respect to*** $\mathbb{B}$*, denoted by $\Delta_{\mathbb{B}}(M)$, is defined as follows:*

1. *$\Delta_{\mathbb{B}}(0) = 0$ and, for $s = 1$, Definition 6 applies.*

2. *For $s = 2$ and a nonzero matrix M, note that $H_M(1,i)$ is the i-th row and $H_M(2,j)$ is the j-th column of M. Define the* ***row support of*** M *as $\operatorname{supp}_1(M) = \{i \in \{0, \dots r_1 - 1\} \mid H_M(1,i) \neq 0\}$ and the* ***column support of*** M *as $\operatorname{supp}_2(M) = \{k \in \{0, \dots r_2 - 1\} \mid H_M(2,k) \neq 0\}$.*

   Then put

$$\begin{aligned} \omega_1(M) &= \max\{\overline{\delta}(\mathbb{Z}_{r_1} \setminus \operatorname{supp}_1(M)) \mid \delta \in \mathbb{B}\}, \\ \epsilon_1(M) &= \max\{\Delta_{\mathbb{B}}(H_M(1,j)) \mid j \in \operatorname{supp}_1(M)\} \end{aligned}$$

   and set $\Delta_1(M) = \omega_1(M) \cdot \epsilon_1(M)$.

   Analogously, we compute the apparent distance $\Delta_2(M)$ for the other variable and finally we define the ***apparent distance of*** M ***with respect to*** $\mathbb{B}$ *by*

$$\Delta_{\mathbb{B}}(M) = \max\{\Delta_1(M), \Delta_2(M)\}.$$

3. *For $s > 2$, proceed as follows: suppose that one knows how to compute the apparent distance $\Delta_{\mathbb{B}}(N)$, for all non zero hypermatrices N of dimension $s-1$. Then first compute the "hypermatrix support" of $M \neq 0$ with respect to the j-th hypercolumn, that is,*

$$\operatorname{supp}_j(M) = \{i \in \{0, \dots r_j - 1\} \mid H_M(j,i) \neq 0\}.$$

Now put

$$\begin{aligned}\omega_j(M) &= \max\{\overline{\delta}(\mathbb{Z}_{r_j} \setminus \mathrm{supp}_j(M)) \mid \delta \in \mathbb{B}\},\\ \epsilon_j(M) &= \max\{\Delta_{\mathbb{B}}(H_M(j,k)) \,|\, k \in \mathrm{supp}_j(M)\}\end{aligned}$$

and set $\Delta_j(M) = \omega_j(M) \cdot \epsilon_j(M)$.

Finally, define the ***apparent distance of*** M ***with respect to*** $\mathbb{B}$ *(or the* $\mathbb{B}$*-apparent distance) as:*

$$\Delta_{\mathbb{B}}(M) = \max\left\{\Delta_j(M) \;\mid\; j \in \{1, \ldots, s\}\right\}.$$

As we have already commented in Remark 9, by taking $\mathbb{B} = \{\delta_{BCH}\}$, $\Delta_{\mathbb{B}}(M)$ is the strong apparent distance in [3].

For each multivariate polynomial $f = \sum_{\mathbf{i}\in I} a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$, the hypermatrix of the coefficients of f is denoted by $M(f) = (a_{\mathbf{i}})_{\mathbf{i}\in I}$. In [3], the apparent distance is related to the weight of codewords. By analogous arguments to [3, Theorem 8] and [3, Lemma 14] the reader may see that for any polynomial $f \in \mathbb{L}(r_1, \ldots, r_s)$ we have

$$\Delta_{\mathbb{B}}(M(f)) \leq \omega\left(\varphi^{-1}_{\overline{\alpha},f}\right) = |\overline{Z(f)}| \tag{2}$$

Example 12 Set $n = 96 = 4 \times 24$ and $q = 5$. Fix $\alpha_1 \in U_4$ and $\alpha_2 \in U_{24}$ and consider the 5-orbits matrix M afforded by $D = Q(0,0) \cup Q(0,1) \cup Q(0,2) \cup Q(0,3) \cup Q(0,6) \cup Q(0,7) \cup Q(0,9) \cup Q(1,1) \cup Q(1,2) \cup Q(1,3) \cup Q(2,1) \cup Q(2,2) \cup Q(3,6)$. Choose $\mathbb{B} = \{\delta_{BS}, \delta_{BCH}\}$, where δ_{BS} is the Betti-Sala bound in [5]. One may check that $\Delta_{\{\delta_{BS},\delta_{BCH}\}}(M) = 8$.

As it is mentioned in [3], the computation of the apparent distance in several variables is a natural extension of that of one variable, and, moreover, the relationship between apparent distance and weight of a codeword is essentially the same in any case. However, condition (2) of Remark 7*(2)* does not necessarily hold in two or more variables and so we cannot extend directly the results of Corollary 10.

Definition 13 *Let* C *be an abelian code in* $\mathbb{F}_q(r_1, \ldots, r_s)$*.*

1) The ***apparent distance of*** C ***with respect to*** $\bar{\alpha} \in U$ ***and*** $\mathbb{B}$ *(or the* $(\mathbb{B}, \bar{\alpha})$*-apparent distance) is*

$$\Delta_{\mathbb{B},\overline{\alpha}}(C) = \min\{\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},c})) \,|\, c \in C\}.$$

2) The ***apparent distance of*** C ***with respect to*** $\mathbb{B}$ *is*

$$\Delta_{\mathbb{B}}(C) = \max\{\Delta_{\mathbb{B},\bar{\alpha}}(C) \,|\, \bar{\alpha} \in U\}.$$

As above, with minor changes in the proofs of [3, Theorem 16] one may see that, for any abelian code C in $\mathbb{F}_q(r_1, \ldots, r_s)$ and any $\mathbb{B}$

$$\Delta_{\mathbb{B}}(C) \leq d(C). \tag{3}$$

It is certain that to compute the apparent distance for each element of a code in order to obtain its apparent distance can be as hard work as to compute the minimum distance of such a code. It is explained in [3, p. 660] how one may get the following equation that improves the efficiency of computation

$$\Delta_{\mathbb{B},\bar{\alpha}}(C) = \min\{\Delta_{\mathbb{B}}\left(M(\varphi_{\bar{\alpha},e})\right) \mid e^2 = e \in C\}. \quad (4)$$

Remarks 14 1. Let $e \in \mathbb{F}_q(r_1, \ldots, r_s)$ be an idempotent and E be the ideal generated by e. Then $\varphi_{\bar{\alpha},e} \star \varphi_{\bar{\alpha},e} = \varphi_{\bar{\alpha},e}$, for any $\bar{\alpha} \in U$ and thus, if $\varphi_{\bar{\alpha},e} = \sum_{\mathbf{i}\in I} a_{\mathbf{i}} X^{\mathbf{i}}$, we have $a_{\mathbf{i}} \in \{1, 0\} \subseteq \mathbb{F}_q$ and $a_{\mathbf{i}} = 0$ if and only if $\mathbf{i} \in \mathcal{D}_{\bar{\alpha}}(E)$. Hence $M(\varphi_{\bar{\alpha},e}) = M(\mathcal{D}_{\bar{\alpha}}(E))$. Conversely, let M be a hypermatrix afforded by a set D which is a union of q-orbits. We know that D determines a unique ideal C in $\mathbb{F}_q(r_1, \ldots, r_s)$ such that $\mathcal{D}_{\bar{\alpha}}(C) = D$. Let $e \in C$ be its generating idempotent. Clearly, $M(\varphi_{\bar{\alpha},e}) = M(D)$.

2. Now let C be an abelian code, $\bar{\alpha} \in U$ and let M be the hypermatrix afforded by $\mathcal{D}_{\bar{\alpha}}(C)$. For any q-orbit hypermatrix $P \leq M$ [see Equation 1] there exists a unique idempotent $e' \in C$ such that $P = M(\varphi_{\bar{\alpha},e'})$ and, for any codeword $f \in C$, there is a unique idempotent $e(f)$ such that $\Delta_{\mathbb{B}}\left(M(\varphi_{\bar{\alpha},f})\right) = \Delta_{\mathbb{B}}\left(M(\varphi_{\bar{\alpha},e(f)})\right)$.

By the remarks above we have therefore,

$$\min\{\Delta_{\mathbb{B}}(P) \mid 0 \neq P \leq M\} = \min\{\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},e})) \mid 0 \neq e^2 = e \in C\} = \Delta_{\mathbb{B},\bar{\alpha}}(C).$$

These facts drives us to give the following definition.

Definition 15 *For a q-orbit hypermatrix M, its* ***minimum $\mathbb{B}$-apparent distance*** *is*

$$\mathbb{B}\text{−mad}(M) = \min\{\Delta_{\mathbb{B}}(P) \mid 0 \neq P \leq M\}.$$

Finally, in the next theorem we set the relationship between the apparent distance of an abelian code and the minimum apparent distance of hypermatrices. The proof follows directly from the preceding paragraphs.

Theorem 16 *Let C be an abelian code in $\mathbb{F}_q(r_1, \ldots, r_s)$ and let e be its generating idempotent. For any $\bar{\alpha} \in U$, we have $\Delta_{\mathbb{B},\bar{\alpha}}(C) = \mathbb{B}\text{−mad}\left(M(\varphi_{\bar{\alpha},e})\right)$. Therefore, $\Delta_{\mathbb{B}}(C) = \max\{\mathbb{B}\text{−mad}\left(M(\varphi_{\bar{\alpha},e})\right) \mid \bar{\alpha} \in U\}$.*

In [3] 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 apparent distances based on the BCH bound (called the strong apparent distance) go decreasing until the minimum value is reached. It is a kind of "suitable idempotents chase through hypermatrices" [3, p. 2]. This algorithm is based on certain manipulations of the (q-orbit) hypermatrix afforded by the defining set of the abelian code. It is not so hard to see that it is possible to obtain an analogous algorithm in our case. The reader may check the new algorithm and some tables of examples in [4]; specially Example 23, where it is shown an abelian code with the largest known bound to the minimum distance among the linear codes with the same length and dimension.

5 True minimum distance in abelian codes

In this section we study the problem of finding abelian codes such that its apparent distance or its multivariate BCH bound reaches its minimum distance. We keep all the notation from the preceding sections. In [8, 9] it is presented a characterization of cyclic and BCH codes whose apparent distance reaches their minimum distance. Our aim is to extend those results for multivariate codes.

Theorem 17 *Let C be an abelian code in $\mathbb{F}_q(r_1,\ldots,r_s)$. The following conditions are equivalent:*

1. $\Delta_{\mathbb{B}}(C) = d(C)$.
2. *There exist an element $\overline{\alpha}\in U$ and a codeword $c\in C$ such that its image under the discrete Fourier transform, $g=\varphi_{\overline{\alpha},c}$, verifies:*
   (a) $\Delta_{\mathbb{B}}\left(M(g)\right) = \Delta_{\mathbb{B},\overline{\alpha}}(C) = \min\left\{\Delta_{\mathbb{B}}\left(M(\varphi_{\overline{\alpha},v})\right) \mid v\in C\right\}$.
   (b) $\Delta_{\mathbb{B}}\left(M(g)\right) = \left|\overline{Z(g)}\right|$.

Proof. [1 ⇒ 2] Let $c\in C$ a be codeword with $\omega(c)=d(C)$ and $\overline{\alpha}\in U$ such that $\Delta_{\mathbb{B},\overline{\alpha}}(C)=\Delta_{\mathbb{B}}(C)$. Set $g=\varphi_{\overline{\alpha},c}$. Then

$$d(C) = \Delta_{\mathbb{B}}(C) = \Delta_{\mathbb{B},\overline{\alpha}}(C) \le \Delta_{\mathbb{B}}\left(M(g)\right) \le \left|\overline{Z(g)}\right| = \omega(c) = d(C),$$

where the first equality is given by hypothesis. Thus, the inequality becomes equality.

[2 ⇒ 1] Suppose that there is a codeword $c\in C$ satisfying the hypotheses. Then

$$d(C) \le \omega(c) = \left|\overline{Z(g)}\right| = \Delta_{\mathbb{B}}\left(M(g)\right) = \Delta_{\mathbb{B},\overline{\alpha}}(C) \le \Delta_{\mathbb{B}}(C) \le d(C)$$

and, again, equalities hold. ∎

Remarks 18 The conditions in statement *(2)* of Theorem 17 refers only to a single element in U. This is an important reduction that will be very useful later. On the other hand, we recall that if M is the hypermatrix afforded by $\mathcal{D}_{\overline{\alpha}}(C)$ then $\Delta_{\mathbb{B},\overline{\alpha}}(C) = \mathbb{B}-\mathrm{mad}(M)$.

For a given abelian code, the problem of finding, if any, a codeword verifying Condition *(2)* of Theorem 17 is in general difficult to solve. In the case that the codeword is an idempotent we will be able to find it *through the computation of the minimum apparent distance* (see [3, Proposition 25] or [4]). So far we only know an actual way to find the desired idempotent codeword of the mentioned theorem and it is given in the following result.

Proposition 19 *Let C be a code in $\mathbb{F}_q(r_1,\ldots,r_s)$, $\overline{\alpha}\in U$ and M the matrix afforded by its defining set $\mathcal{D}_{\overline{\alpha}}(C)$. Let $P\le M$ be a q-orbit matrix and $g\in\mathbb{L}(r_1,\ldots,r_s)$ be such that $P=M(g)$. If P verifies*

1. $\Delta_{\mathbb{B}}(P)=\mathbb{B}-\mathrm{mad}(M)$ *and*
2. $\Delta_{\mathbb{B}}(P)=\left|\overline{Z(e)}\right|$.

Then $d(C)=\mathbb{B}-\mathrm{mad}(M)=\Delta_{\mathbb{B}}(C)$.

Proof. Since $P\leq M$, then $\varphi_{\overline{\alpha},g}^{-1}\in C$ (see Remark 14), hence $\omega(\varphi_{\overline{\alpha},g}^{-1})\geq d(C)\geq\Delta_{\mathbb{B}}(C)$. On the other hand, by the hypothesis *(2)*,

$$\omega(\varphi_{\overline{\alpha},g}^{-1})=\Delta_{\mathbb{B}}(P)=\mathbb{B}-\mathrm{mad}(M)\leq\Delta_{\mathbb{B}}(C)\leq d(C).$$

Therefore, $d(C)=\mathbb{B}-\mathrm{mad}(M)=\Delta_{\mathbb{B}}(C)$. ∎

So, for a given code C with afforded matrix M, if we want to know whether $d(C)=\Delta_{\mathbb{B}}(C)$ by using Proposition 19, in the case that the requested codeword is an idempotent, we have to analyze all (q-orbit) matrices $P\leq M$. If $\left|\overline{\mathcal{D}_{\overline{\alpha}}(C)}\right|=t$ and such idempotent exists, we have to do at most 2^tsteps (computations of apparent distance). This is a search on the set of idempotents of C. The reader may note that the original computation of the apparent distance in [10] and [20] requires to compute the apparent distance of *exactly* the same set of q-orbit matrices. This might be an important reduction in some cases.

We wonder if it is possible to simplify the procedure to find a q-orbit matrix P, as in Proposition 19, by analyzing the sequence of matrices in the algorithm for the computation of the minimum apparent distance of the matrix M afforded by $\mathcal{D}_{\overline{\alpha}}(C)$; i.e. the computation of $\mathbb{B}-\mathrm{mad}(M)$. The algorithm gives us an interesting reduction.

For example, in the case $s=2$, the algorithm for the computation of the strong apparent distance as in [3, Proposition 25] or [4, Theorem 20] considers the sequence of matrices

$$M=M_0>M_1>\cdots>M_{j_0-1}>M_{j_0}>\cdots>M_\ell>0 \tag{5}$$

where j_0 is the first index such that $\Delta_{\mathbb{B}}\left(M_{j_0}\right)=m_\ell=\mathbb{B}-\mathrm{mad}(M)$. If $m_0=\Delta_{\mathbb{B}}(M)$ equals m_ℓ, then $P=M$ and we do not have any reduction. However, if $m_0>m_\ell$, then $\Delta_{\mathbb{B}}(P)=m_\ell<m_{j_0-1}$ which implies $P\leq M_{j_0}$, hence we can start our search from M_{j_0}; that is, we have to check only at most 2^{t-j_0} matrices in order to find the hypothetical matrix of Theorem 17.

We wonder if the existence of a matrix $P\leq M$ satisfying the conditions of Proposition 19 implies the existence of a matrix in the sequence (5) also satisfying those conditions. The answer is negative, as the following very simple example shows.

Example 20 *Set* $\Delta=\Delta_{\mathbb{B}}$, *with* $\mathbb{B}=\{\delta_{BCH}\}$. *There exists an abelian code* C, *with matrix* M *afforded by* $\mathcal{D}_{\overline{\alpha}}(C)$ *with respect to* $\overline{\alpha}\in U$ *such that:*

1. *For every* q*-orbit matrix in the sequence* $M=M_0>\cdots>0$ *we have* $\Delta(M_j)\neq\left|\overline{Z(e_j)}\right|$, *where* $e_j\in\mathbb{L}(r_1,r_2)$ *is the idempotent that verifies* $M_j=M(e_j)$.

2. $d(C) = \Delta(C)$

Proof. Set $q = 2$ and $r_1 = r_2 = 7$. Let C be the code such that $\mathcal{D}_{\overline{\alpha}}(C) = Q(0,3) \cup Q(1,3) \cup Q(1,5) \cup Q(1,6) \cup Q(3,0) \cup (3,2) \cup Q(3,3) \cup Q(3,4) \cup Q(3,5) \cup Q(3,6)$ with respect to $\overline{\alpha} \in U$.

Let $a(X_1) = (1 + X_1)(1 + X_1^2 + X_1^3)$, $b(X_2) = (1 + X_2)(1 + X_2^2 + X_2^3)$. If $e \in C$ is the idempotent generator then $\varphi_{\overline{\alpha},e}(X_1, X_2) = a(X_1)\, b(X_2) + X_1^3 X_2 + X_1^6 X_2^2 + X_1^5 X_2^4$. One may compute $\left|\overline{Z(\varphi_{\overline{\alpha},e})}\right| = 25$, by using GAP.

On the other hand, computing $\mathbb{B}-\mathrm{mad}(M)$, we obtain the chain $M_0 > 0$ and $\Delta(M) = \mathbb{B}-\mathrm{mad}(M) = 9$. Now consider the q-orbit matrix $0 < P = M\,(ab) < M$. Note that P does not belong to the sequence $M_0 > 0$. However, as we will see below $g_1 = ab$ satisfies the hypothesis of Proposition 27 which means that C satisfies the condition *(2b)* of Theorem 17. Now, as $\Delta(P) = 9$ then condition *(2a)* of the same theorem is satisfied and thus $d(C) = \Delta(C)$. ■

As we have seen, although Proposition 19 gives us a sufficient condition, it does not guarantee that we can find the desired codeword if it is not an idempotent, not even by using the algorithm. Now, in order to construct codes C satisfying $d(C) = \Delta_{\mathbb{B}}(C)$, we try to move forward into a different direction: we firstly characterize those polynomials that verify *(2b)*; that is, $\Delta_{\mathbb{B}}\left(M(g)\right) = |\overline{Z(g)}|$. In the univariate case, those polynomials were characterized in [9]. Before to extend the results to multivariate polynomials, we need to put some restrictions on the election of ds-bounds that we may use. In the case of polynomials in one variable, one may see that the condition *(2b)* in Theorem 17 forces us to use exclusively the BCH bound as, to the best of our knowledge, the computation of $|\overline{Z(g)}|$ is only known to be obtained in terms of the degree of $\overline{X^h g}$ (viewed as a polynomial); that is, a list of consecutive exponents of the monomials with coefficient zero of the highest degrees.

In the rest of this section we shall find some sufficient conditions in the case of two variables. We consider $\mathbb{B} = \{\delta_{BCH}\}$ and denote $\Delta = \Delta_{\{\delta_{BCH}\}}$, for the sake of simplicity. Let us recall some facts from univariate polynomials that will be used herein. For $0 \neq g \in \mathbb{L}(n)$, let $m_g = \gcd(X^n - 1, X^h g)$, which does not depend on $h \in \mathbb{N}$. As we pointed out in Remark 9 about notation, $sd^* = \Delta_{\{\delta_{BCH}\}} = \Delta$. The proof of the following result is essentially the same as [9, Proposition 1]; so we ommit it. Let us introduce some notation about polynomials in two variables. Consider the bivariate polynomial $f = \sum_{(i,j)\in\mathbb{Z}_{r_1}\times\mathbb{Z}_{r_2}} f_{i,j} X_1^i X_2^j$. For any $l \in \{1,2\}$, we write $f = \left[f(X_{l'})\right](X_j) = \sum_{k=0}^{r_l - 1} f_{l,k} X_l^k$, where $f_{l,k} = f_{l,k}(X_{l'})$, with $l' \neq l$. Note that $M\left(f_{l,k}\right) = H_{M(f)}(l,k)$.

Proposition 21 *Let $g \in \mathbb{L}(n)$. Then*
$\Delta(M(g)) = \left|\overline{Z(g)}\right|$ *if and only if* $\overline{X^h g} \mid X^n - 1$, *for some* $h \in \mathbb{N}$.

Consider $g = g(X_1, X_2) \in \mathbb{L}(r_1, r_2)$ and write $M = M(g)$. In general, as we have seen in Equation 2, $\Delta(M(g)) \leq \left|\overline{Z(g)}\right|$. We want to describe the polynomials g in $\mathbb{L}(r_1, r_2)$ such that $\Delta(M(g)) = \left|\overline{Z(g)}\right|$ so we assume that the equality holds; moreover, we impose the following condition

$$\Delta_1(M) = \Delta_2(M) = \Delta(M) = \left|\overline{Z(g)}\right|. \tag{6}$$

where, as in Definition 11, $\Delta_i(M) = \omega_i(M) \cdot \epsilon_i(M)$, for $i \in \{1, 2\}$.

We also write, following the notation above,

$$g = [g(X_1)](X_2) = \sum_{k=0}^{r_2-1} g_{2,k} X_2^k, \quad g = [g(X_2)](X_1) = \sum_{k=0}^{r_1-1} g_{1,k} X_1^k. \tag{7}$$

For all $u \in \mathbb{L}$, the polynomials of the form $g(u, X_2)$ and $g(X_1, u)$ have the obvious meaning. For each $j \in \{1, 2\}$, we set $M_j = \{k \in \{0, \ldots, r_i - 1\} \mid (j, k) \in I_p(M)\}$ (see [3, Definition 12] or [4, Definition 18] for the definition of $I_p(M)$); that is, $\Delta(M(g_{j,k})) = \varepsilon_j$, for any $k \in M_j$. Note that $I_p(M) = (1, M_1) \cup (2, M_2)$.

Now, for each $k \in M_1$, define

$$D_{1,k} = \left\{(u, v) \in R \mid v \in \overline{Z(g_{1,k})} \text{ and } u \in \overline{Z\left(g(X_1, v)\right)}\right\}$$

and analogously, for each $k \in M_2$, define

$$D_{2,k} = \left\{(u, v) \in R \mid u \in \overline{Z(g_{2,k})} \text{ and } v \in \overline{Z\left(g(u, X_2)\right)}\right\}.$$

So, if we set, for $j \in \{1, 2\}$, $\min(j, k) = \min\left\{\left|\overline{Z(g(u, X_j))}\right| \mid u \in \overline{Z(g_{j,k})}\right\}$ then $\left|\overline{Z(g_{j,k})}\right| \cdot \min(j, k) \le |D_{j,k}|$.

We know that, for each $k \in M_1$, it happens $\varepsilon_1(M) = \Delta(M(g_{1,k})) \le \left|\overline{Z(g_{1,k})}\right|$ and for each $v \in \overline{Z(g_{1,k})}$, we have $\omega_1(M) \le \Delta(M(g(X_1, v)))$ and so $\omega_1(M) \le \min(j, k)$, hence $\varepsilon_1(M)\omega_1(M) \le |D_{1,k}|$. However, by the condition (6), $\varepsilon_1(M)\omega_1(M) = \Delta_1(M) = \left|\overline{Z(g)}\right|$ and, by definition, $|D_{1,k}| \le \left|\overline{Z(g)}\right|$. Therefore, for all $k \in M_1$,

$$\left|\overline{Z(g)}\right| = \varepsilon_1(M)\omega_1(M) = |D_{1,k}| \quad \text{and so} \quad D_{1,k} = \overline{Z(g)}. \tag{8}$$

Analogously, $D_{2,k} = \overline{Z(g)}$, for $k \in M_2$.

In fact, for $j \in \{1, 2\}$ and any $k \in M_j$, we have $\left|\overline{Z(g_{j,k})}\right| \cdot \min(j, k) = |D_{j,k}|$, hence

$$\varepsilon_1(M) = \Delta(M(g_{1,k})) = \left|\overline{Z(g_{1,k})}\right| \text{ and } \omega_1(M) = \min(j, k). \tag{9}$$

Keeping in mind the equalities obtained in the previous paragraphs, we get the following two results.

Lemma 22 *Let $g = g(X_1, X_2) \in \mathbb{L}(r_1, r_2)$ be a polynomial such that $M = M(g)$ satisfies the condition* (6)*. Then:*

1. *For each* $k \in M_1$, $\Delta\left(M(g_{1,k})\right) = \left|\overline{Z\left(g_{1,k}\right)}\right| = \left|\pi_2\left(\overline{Z(g)}\right)\right|$ *and* $\Delta(M(g(X_1,v))) = \left|\overline{Z\left(g(X_1,v)\right)}\right|$, *for any* $v \in \overline{Z\left(g_{1,k}\right)}$.

2. *For each* $k \in M_2$, $\Delta\left(M(g_{2,k})\right) = \left|\overline{Z\left(g_{2,k}\right)}\right| = \left|\pi_1\left(\overline{Z(g)}\right)\right|$ *and* $\Delta(M(g(u,X_2))) = \left|\overline{Z\left(g(u,X_2)\right)}\right|$, *for any* $u \in \overline{Z\left(g_{2,k}\right)}$.

Proof. We prove *(1.)* as the the proof of *(2.)* is entirely analogous. As we have already seen, if condition (6) is satisfied then (8) and (9) also hold; so that, $\varepsilon_1(M) = \Delta\left(M(g_{1,k})\right) = \left|\overline{Z\left(g_{1,k}\right)}\right|$.

Once we have the first equality, if $\omega_1(M) = \Delta\left(M(g(X_1,v))\right) < \left|\overline{Z\left(g(X_1,v)\right)}\right|$, for some $v \in \overline{Z\left(g_{1,k}\right)}$, then it must happen $\varepsilon_1(M)\omega_1(M) < |D_{1,j}|$, a contradiction. Finally, if $v \in \overline{Z_2}$, then there exists $u \in R_{r_1}$ such that $(u,v) \in \overline{Z(g)} = D_{1,k}$, hence $u \in \overline{Z\left(g_{1,k}\right)}$. This proves the other equalities of this lemma. ■

Proposition 23 *Let* $g = g(X_1,X_2) \in \mathbb{L}(r_1,r_2)$ *be a polynomial such that* $M = M(g)$ *satisfies the condition* (6). *Then there exist* $a = a(X_1) \in \mathbb{L}(r_1)$, $b = b(X_2) \in \mathbb{L}(r_2)$ *and* $F = F(X_1,X_2) \in \mathbb{L}(r_1,r_2)$ *such that* $g = abF$ *and*

1. $\overline{X_1^{h_1} a} \mid (X_1^{r_1} - 1)$, *for some* $h_1 \in \mathbb{Z}_1$, *with* $\Delta(M(a)) = \varepsilon_2(M)$.

2. $\overline{X_2^{h_2} b} \mid (X_2^{r_2} - 1)$, *for some* $h_2 \in \mathbb{Z}_2$, *with* $\Delta(M(b)) = \varepsilon_1(M)$.

Proof. By Lemma 22.1 and by Proposition 21, for each $k \in M_2$, if we denote $m_k = \gcd\left(g_{2,k}, X_1^{r_1} - 1\right)$, then

$$\begin{aligned}\Delta(M(m_k)) &= \left|\overline{Z(m_k)}\right| = r_1 - |Z(m_k)| = r_1 - \left|Z\left(g_{2,k}\right)\right| = \\ &= \left|\overline{Z\left(g_{2,k}\right)}\right| = \Delta\left(M(g_{2,k})\right).\end{aligned}$$

By [9, Definition 1] (see Remark 9), $\Delta\left(M(g_{2,k})\right) = r_1 - \deg(\overline{X_1^{k'} g_{2,k}})$, for some $k' \in \mathbb{N}$. As $\Delta(M(m_k)) = \Delta\left(M(g_{2,k})\right)$ and, by [9, Lemma 2], $\Delta(M(m_k)) = r_1 - \deg m_k$, then $\overline{X_1^{k'} g_{2,k}}$ and m_k are associated.

Now we claim that $m_k \mid g_{2,j}$, for all $j \in \{0,\ldots,r_2-1\}$. Indeed, for a fixed $k \in M_2$, by (8), we have $D_{2,k} = \overline{Z(g)}$ which implies $\overline{Z\left(g_{2,j}\right)} \subseteq \overline{Z\left(g_{2,k}\right)}$ or rather $Z\left(g_{2,k}\right) \subseteq Z\left(g_{2,j}\right)$. Hence, $m_k \mid g_{2,j}$, for all $j \in \{0,\ldots,r_2-1\}$.

Denoting by $g'_{2,j} = \frac{g_{2,j}}{m_k}$, for all $j \in \{0,\ldots,r_2-1\}$ and $a(X_1) = m_k$, we may write

$$g(X_1)(X_2) = a(X_1)\sum_{j=0}^{r_2-1} g'_{2,j} X_2^j, \tag{10}$$

with $\Delta(M(a(X_1))) = \varepsilon_2(M)$.

Analogously, we get

$$g(X_2)(X_1) = b(X_2) \sum_{i=0}^{r_1-1} g'_{1,i} X_1^i, \tag{11}$$

with $\Delta(M(b(X_2))) = \varepsilon_1(M)$ and $b(X_2)g'_{1,i} = g_{1,i}$, for any $i \in \{0, \dots, r_1 - 1\}$.

It is important to note that $1 = \gcd\left(X_1^{r_1} - 1, g'_{2,0}, \dots, g'_{2,r_2-1}\right)$ and $1 = \gcd\left(X_2^{r_2} - 1, g'_{1,0}, \dots, g'_{1,r_1-1}\right)$.

Now by writing

$$f(X_1, X_2) = \sum_{j=0}^{r_2-1} g'_{2,j} X_2^j \quad \text{and} \quad h(X_1, X_2) = \sum_{i=0}^{r_1-1} g'_{1,i} X_1^i,$$

we get $g(X_1, X_2) = a(X_1)f(X_1, X_2) = b(X_2)h(X_1, X_2)$.

First note that if $v \in \pi_2\left(\overline{Z(g)}\right)$, then there exists $u \in \pi_1\left(\overline{Z(g)}\right)$ such that $(u, v) \in \overline{Z(g)}$. This implies $(u, v) \in D_{1,k}$, for $k \in M_1$, hence $v \in \overline{Z(g_{1,k})} = \overline{Z(b)}$. Therefore, $\pi_2\left(\overline{Z(g)}\right) \subseteq \overline{Z(b)}$ and, by Lemma 22.1, $\pi_2\left(\overline{Z(g)}\right) = \overline{Z(b)}$.

Consider $g(X_1, v) = b(v)\, h(X_1, v) = b(v) \sum_{i=0}^{r_1-1} g'_{1,i}(v) X_1^i$, for any $v \in R_{r_2}$. If $b(v) \neq 0$, then $g(X_1, v) \neq 0$, otherwise all $g'_{1,i}$ would have a common zero, which is not possible. Conversely, if $g(X_1, v) \neq 0$, then $b(v) \neq 0$. This proves that $v \in \overline{Z(b)} = \pi_2\left(\overline{Z(g)}\right)$ if and only if $g(X_1, v) \neq 0$.

Obviously $g(X_1, v) = 0$ also implies $b(v) = 0$, hence $v \in \pi_2\left(Z(g)\right)$, as $Z(b)\pi_2\left(Z(g)\right)$. Now let us write

$$f(X_1, X_2) = \sum_{i=0}^{r_1-1} f_{1,i} X_1^i \quad \text{and} \quad h(X_1, X_2) = \sum_{j=0}^{r_2-1} h_{2,j} X_2^j.$$

If $v \in Z(b)$, then $g(X_1, v) = 0$ and we have $f(X_1, v) = 0$. Since $a(X_1) \neq 0$ we must have $f_{1,i}(v) = 0$, for all $i \in \{0, \dots, r_1 - 1\}$. Hence $b(X_2) \mid f_{1,i}$, for all $i \in \{0, \dots, r_1 - 1\}$. Now if $f_{1,i}(v) = 0$, for all $i \in \{0, \dots, r_1 - 1\}$, then $f(X_1, v) = 0$ and $g(X_1, v) = 0$, which implies $v \in Z(b)$, as we have seen before. Hence $b(X_2) = \gcd(X_2^{r_2} - 1, f_{1,i})$, for all $i \in \{0, \dots, r_1 - 1\}$. Therefore, $f(X_1, X_2) = b(X_2)f'(X_1, X_2)$ and

$$g(X_1, X_2) = a(X_1)b(X_2)f'(X_1, X_2). \tag{12}$$

Analogously, one may prove that $a(X_1) \mid h_{2,j}$, for all $j \in \{0, \dots, r_2 - 1\}$, and get $h(X_1, X_2) = a(X_1)h'(X_1, X_2)$, hence

$$g(X_1, X_2) = a(X_1)b(X_2)h'(X_1, X_2). \tag{13}$$

Finally, note that the decompositions $g = abf'$ and $g = abh'$ from (12) and (13), has been done in $\mathbb{L}[X_1, X_2]$, which is a domain, and so, we have

$f'(X_1,X_2) = h'(X_1,X_2)$. By writing $F(X_1,X_2) = f'(X_1,X_2) = h'(X_1,X_2)$, we get

$$g(X_1,X_2) = a(X_1)\, b(X_2)\, F(X_1,X_2).$$

■

Remark 24 From the proof of the proposition above one may see that the decomposition $g = abF$ is unique in the sense that $a = \gcd(g_{2,0},\ldots,g_{2,r_2-1},X_1^{r_1}-1)$ and $b = \gcd(g_{1,0},\ldots,g_{1,r_1-1},X_2^{r_2}-1)$; that is, a is the factor of g such that $a(u)=0$ if and only if $\{(u,x)\in Z(g) \mid x\in\mathbb{Z}_{r_2}\}$ and similarly for b.

It is clear that the condition (6) plays an important role in all the previous proofs. Recall that a polynomial $g\in\mathbb{L}(r_1,r_2)$, with coefficient matrix $M = M(g)$, satisfies such condition if

$$\Delta_1(M) = \Delta_2(M) = \Delta(M) = \left|\overline{Z(g)}\right|.$$

For those polynomials, we have obtained a factorization $g = abF$, which describes them, where $\Delta(M(a)) = \varepsilon_2(M)$ and $\Delta(M(b)) = \varepsilon_1(M)$.

At this point, two questions arise for an abelian code satisfying Theorem 17 with a codeword image $g = \varphi_{\overline{\alpha},c}$ as in such theorem.

1. Is it always true that g satisfies also condition (6)?
2. Suppose a polynomial $g\in\mathbb{L}(r_1,r_2)$ already satisfies condition (6) and so we have a decomposition $g = abF$. Is it true that $\Delta(M(a))\cdot\Delta(M(b)) = \Delta(M(g))$? And, moreover, is $\Delta(M(F)) = 1$?

We shall answer all these questions in the following examples.

Example 25 *There exists an abelian code C generated by an idempotent $e\in\mathbb{F}_q(r_1,r_2)$, with image $g = \varphi_{\overline{\alpha},e}$, satisfying the following properties.*

1. $\Delta_1(M(g)) < \Delta_2(M(g))$ *(so the condition (6) is not fully satisfied)*
2. $\Delta(M(g)) = \left|\overline{Z(g)}\right|$.
3. $d(C) = \Delta(C)$.

Proof. Set $q=2$, $r_1=5$, $r_2=9$ and C be the code with $\overline{D(C)} = Q(1,3)$, a minimal code with generator idempotent $e(X_1,X_2) = X_1^4X_2^7 + X_1^3X_2^8 + X_1^4X_2^6 + X_1^2X_2^8 + X_1^3X_2^6 + X_1^4X_2^4 + X_1^3X_2^5 + X_1^2X_2^6 + X_1X_2^7 + X_1^4X_2^3 + X_1^2X_2^5 + X_1X_2^6 + X_1^3X_2^3 + X_1^4X_2 + X_1^3X_2^2 + X_1^2X_2^3 + X_1X_2^4 + X_1^4 + X_1^2X_2^2 + X_1X_2^3 + X_1^3 + X_1^2 + X_1X_2 + X_1$. Using the program GAP, we computed $d(C) = 24$. One may check that $\varphi_{\alpha,e} = g(X_1,X_2) = X_1X_2^3 + X_1^4X_2^3 + X_1^2X_2^6 + X_1^3X_2^6$. Some direct computations yield $\Delta_1(M(g)) = 18$ and $\Delta(M(g)) = 24$, so assertion *(1)* of this example is satisfied. As $\omega(e) = 24$ we also get assertion *(2)*. Since C is minimal, we have, $24 = \Delta(M(g)) = \mathbb{B}-\mathrm{mad}(M(g))$. On the other hand

$\Delta(M(g)) \leq \Delta(C) \leq d(C) = 24$. Thus $d(C) = \Delta(C)$ and we get assertion *(3)*. ■

The previous example gives a negative answer to question 1. The following example answers question 2.

Example 26 *Under the same notation of Proposition 23, there exists an abelian code C generated by an idempotent $e \in \mathbb{F}_q(r_1, r_2)$, with image $g = \varphi_{\overline{\alpha},e}$, such that the following properties hold.*

1. *$M(g)$ satisfies the condition* (6) *and then $g = abF$ as in the mentioned proposition (see paragraph prior to Example 25).*
2. *$d(C) = \Delta(C)$.*
3. *$F(X_1, X_2)$ is not a monomial and $\Delta(M(F)) \neq 1$.*
4. *$\Delta(M(a))\Delta(M(b)) \neq \Delta(M(g))$*
5. *$\overline{Z(g)} \neq \overline{Z_1} \times \overline{Z_2}$*

Proof. Let $q = 2$, $r_1 = r_2 = 5$ and C be the code with $\overline{D(C)} = Q(1,1) \cup Q(1,3)$. In this case, $g(X_1, X_2) = X_1^4 X_2^4 + X_1^3 X_2^4 + X_1^4 X_2^2 + X_1^3 X_2^3 + X_1^2 X_2^2 + X_1 X_2^3 + X_1^2 X_2 + X_1 X_2$ and $\varphi_{\alpha,g}^{-1} = X_1^3 X_2^4 + X_1^4 X_2^2 + X_1^4 X_2 + X_1^3 X_2^2 + X_1^2 X_2^3 + X_1 X_2^4 + X_1 X_2^3 + X_1^2 X_2$, so that $|\overline{Z(g)}| = 8$.

By using GAP, we computed $d(C) = 8$ and one may check that $\Delta_1(M(g)) = \Delta_2(M(g)) = \Delta(M(g)) = 8$; so that *(1.)* and *(2.)* hold.

Now one may check that the factorization $g = abF$ gives $a = 1 + X_1$, $b = 1 + X_2$ and $F = X_1 X_2 + X_1 X_2^2 + X_1^2 X_2^2 + X_1^3 X_2^2 + X_1^3 X_2^3$. Then $\Delta(M(F)) = 15$ and we have *(3.)*

Now, one may easily check that $\Delta(M(a)) = \Delta(M(b)) = 4$, hence $\Delta(M(a)) \cdot \Delta(M(b)) \neq \Delta(M(g))$. This gives us *(4)*.

Finally, by using GAP we compute $\overline{Z(g)} = Q(1,3) \cup Q(1,4)$ and clearly $\overline{Z(g)} \neq \overline{Z_1} \times \overline{Z_2}$. ■

To finish our argumentation from Theorem 17 we prove that a polynomial that satisfies condition (6), and so factorizes $g = abF$ with $F(X_1, X_2)$ a monomial in $\mathbb{L}(r_1, r_2)$, verifies that its image under the discrete Fourier transform satisfy condition *(2)* of the mentioned theorem.

Proposition 27 *Suppose $g \in \mathbb{L}(r_1, r_2)$ is such that $g(X_1, X_2) = a(X_1)\, b(X_2)$, where a and b satisfy Proposition 21. Set $M = M(g)$. Then*

1. *$\overline{Z(g)} = \overline{Z_1} \times \overline{Z_2}$*
2. *$\Delta(M) = \Delta(M(a)) \cdot \Delta(M(b)) = \left|\overline{Z(g)}\right|$.*
3. *$\Delta_1(M) = \Delta_2(M) = \Delta(M) = \left|\overline{Z(g)}\right|$ (the condition* (6)*).*

4. $\Delta(M(a)) = \varepsilon_2(M) = \omega_1(M)$ *and*

5. $\Delta(M(b)) = \varepsilon_1(M) = \omega_2(M)$.

Proof. Assertion *(1)* and the equality $\Delta(M(a)) \cdot \Delta(M(b)) = \left|\overline{Z(g)}\right|$ come directly from the decomposition of g together with the hypothesis that a and b satisfy Proposition 21.

Now set $M = M(g)$. Since $g = ab$ then $H_M(2, j) = M(a)$, for all $j \in \operatorname{supp}_2(M)$ and $\operatorname{supp}_2(M) = \operatorname{supp}(M(b))$; so that $\varepsilon_2(M) = \Delta(M(a))$ and $\omega_2(M) = \Delta(M(b))$. Analogously, $\varepsilon_1(M) = \Delta(M(a))$ and $\omega_1(M) = \Delta(M(b))$. From this, we get all assertions. ■

To sum up, from Proposition 23 we have obtained what kind of polynomials we have to use to reach condition (6). This will be the main idea in order to construct abelian codes C, with $d(C) = \Delta(C)$. We address this problem in the following section.

5.1 Application 1: construction of abelian codes for which its multivariate BCH bound, apparent distance and minimum distance coincide.

In this section, we continue considering $\mathbb{B} = \{\delta_{BCH}\}$ and denoting $\Delta = \Delta_{\delta_{BCH}}$, for the sake of simplicity by the same reasons given in the paragraphs prior Proposition 21. Bearing in mind Proposition 27 and Proposition 19, we introduce the following definition.

Definition 28 *A matrix P of order $r_1 \times r_2$, with entries in $\mathbb{L}$ is called a* ***composed polynomial matrix (CP-matrix****, for short) if there exist polynomials $a = a(X_1) \in \mathbb{L}(r_1)$ and $b = b(X_2) \in \mathbb{L}(r_2)$ such that $P = M(ab)$, where $ab \in \mathbb{L}(r_1, r_2)$.*

Note that, for a CP-matrix P, its support is a direct product $\operatorname{supp}(P) = \operatorname{supp}(a(X_1)) \times \operatorname{supp}(b(X_2))$. The polynomials a and b are called the **polynomial factors of** P. The reader may see that to check if a matrix is a CP-matrix is a trivial task, because it must happen $\pi_1(\operatorname{supp}(P)) = \operatorname{supp}(a) = \operatorname{supp}(M(a))$ and $\pi_2(\operatorname{supp}(P)) = \operatorname{supp}(b) = \operatorname{supp}(M(b))$. The following result is an immediate consequence of Proposition 27.

Corollary 29 *Let $P = M(g)$ be a CP-matrix of order $r_1 \times r_2$ with polynomial factors a and b; that is, $g = ab$. If $\overline{X_1^{h_1} a} \mid X_1^{r_1} - 1$ and $\overline{X_2^{h_2} b} \mid X_2^{r_2} - 1$, for some $h_1, h_2 \in \mathbb{N}$, then*

1. $\overline{Z(ab)} = \overline{Z(a)} \times \overline{Z(b)}$.

2. $\Delta(P) = \Delta(M(a)) \cdot \Delta(M(b)) = \left|\overline{Z(g)}\right|$.

3. $\Delta_1(P) = \Delta_2(P) = \Delta(P) = \left|\overline{Z(g)}\right|$ *(the condition* (6)*).*

4. $\Delta(M(a)) = \varepsilon_2(P) = \omega_1(P)$ *and*

5. $\Delta(M(b)) = \varepsilon_1(P) = \omega_2(P)$.

The next example shows that the hypothesis on the polynomials a and b of Corollary 29 are not superfluous.

Example 30 Set $q = 2$, $r_1 = 5$ and $r_2 = 7$; so that $n = 35$. Let P be the CP-matrix with factors $a = X_1 + X_1^2 + X_1^3 + X_1^4$ and $b = X_2 + X_2^2 + X_2^4$. In this case, $\overline{X_1^{h_1} a} \nmid X_1^5 - 1$, for all $h_1 \in \mathbb{Z}_5$. On the other hand $\overline{X_2^6 b} \mid X_2^7 - 1$. Now $\Delta(M(a)) = 2$, $\Delta(M(b)) = 4$. Although $\Delta_1(P) = \Delta_2(P) = \Delta(P) = 8$, one may check that $\left|\overline{Z(ab)}\right| = 16$.

Now we give a method for constructing the desired abelian codes. First, a technical lemma.

Lemma 31 *Let $D \subset \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ be union of q-orbits and $M = M(D)$, the matrix afforded by D. If $\operatorname{supp}(M) = \pi_1(\operatorname{supp}(M)) \times \pi_2(\operatorname{supp}(M))$ then $\mathbb{B}-\mathrm{mad} = \Delta_{\mathbb{B}}(M)$, where $\mathbb{B}$ is any set of ds-bounds.*

In the case $\mathbb{B} = \{\delta_{BCH}\}$, the above equality coincides with the multivariate BCH bound in [3, Theorem 30].

Proof. Clearly, in this case all rows (columns) have the same support and so if one row or column is involved then all of them are too. The last assertion comes directly from the computation of the multivariate BCH bound. ∎

Remark 32 We have already mentioned that for any CP-matrix, M, one has $\operatorname{supp}(M) = \pi_1(\operatorname{supp}(M)) \times \pi_2(\operatorname{supp}(M))$. The converse is true for those matrices satisfying hypothesis of lemma above; that is, if $D \subset \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ is union of q-orbits and $M = M(D)$ is the matrix afforded by D with $\operatorname{supp}(M) = \pi_1(\operatorname{supp}(M)) \times \pi_2(\operatorname{supp}(M))$ then M is a CP-matrix.

Theorem 33 *Let $a = a(X_1) \in \mathbb{L}(r_1)$ and $b = b(X_2) \in \mathbb{L}(r_2)$ be such that $a \mid X_1^{r_1} - 1$ and $b \mid X_2^{r_2} - 1$. If there exist $(\alpha_1, \alpha_2) \in U$, $h_1 \in \mathbb{Z}_{r_1}$ and $h_2 \in \mathbb{Z}_{r_2}$ for which $\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \in \mathbb{F}_q(r_1)$ and $\varphi^{-1}_{\alpha_2, \overline{X_2^{h_2} b}} \in \mathbb{F}_q(r_2)$, then the abelian code $C = \left(\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \cdot \varphi^{-1}_{\alpha_2, \overline{X_2^{h_2} b}}\right)$ in $\mathbb{F}_q(r_1, r_2)$ verifies $\Delta(M(ab)) = \Delta(C) = d(C)$.*

Moreover, in this case, for any $\beta_1 \in U_{r_1}$ and $\beta_2 \in U_{r_2}$ the abelian code $C_{(\beta_1,\beta_2)} = \left(\varphi^{-1}_{\beta_1, \overline{X_1^{h_1} a}} \cdot \varphi^{-1}_{\beta_2, \overline{X_2^{h_2} b}}\right)$ is an ideal of $\mathbb{F}_q(r_1, r_2)$ and verifies $\Delta(M(ab)) = \Delta(C_{(\beta_1,\beta_2)}) = d(C_{(\beta_1,\beta_2)}) = d(C)$.

Proof. Set $g(X_1, X_2) = \overline{X_1^{h_1} a(X_1) \cdot X_2^{h_2} b(X_2)}$ and $\overline{\alpha} = (\alpha_1, \alpha_2)$. By definition of the discrete Fourier transform, it is easy to see that the particular factorization of g implies that $\varphi^{-1}_{(\alpha_1,\alpha_2),g} = \varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \cdot \varphi^{-1}_{\alpha_2, \overline{X_2^{h_2} b}}$. On the other hand, it is clear that $M(g)$ is a CP-matrix satisfying the hypothesis of Corollary 29. This, in turn, implies that statement *2(b)* of Theorem 17 is satisfied.

Let M be the matrix afforded by $\mathcal{D}_{\overline{\alpha}}(C)$. Since $C = \left(\varphi^{-1}_{\overline{\alpha},g}\right)$ then $\mathrm{supp}(M) = \mathrm{supp}(M(g))$, hence M is also a CP-matrix and $\Delta(M) = \Delta(M(g))$. By Lemma 31, $\mathbb{B}-\mathrm{mad}(M) = \Delta(M)$ and so statement *2(a)* of Theorem 17 is also satisfied. Thus $\Delta(C) = d(C)$. The final assertion is a direct consequence of [9, Remark 2] together with the fact that, under these hypothesis, all afforded matrices are CP-matrices. ■

Now, we may apply all known criteria for univariate polynomials to have inverse of the discrete Fourier transform in an specific quotient ring. The following corollary concretizes the proposed construction. It comes from [9, Remark 2] and the theorem above.

Corollary 34 *Let $a = a(X_1) \in \mathbb{L}(r_1)$ and $b = b(X_2) \in \mathbb{L}(r_2)$ be such that $a \mid X_1^{r_1} - 1$ and $b \mid X_2^{r_2} - 1$. If there exist $(\alpha_1, \alpha_2) \in U$, $h_1 \in \mathbb{Z}_{r_1}$ and $h_2 \in \mathbb{Z}_{r_2}$ for which $\left[\left(\overline{X_1^{h_1} a}\right)(\alpha_1^i)\right]^q = \left(\overline{X_1^{h_1} a}\right)(\alpha_1^i)$, for all $i \in \{0, \ldots, r_1 - 1\}$ and $\left[\left(\overline{X_2^{h_2} b}\right)(\alpha_2^j)\right]^q = \left(\overline{X_2^{h_2} b}\right)(\alpha_2^j)$, for all $j \in \{0, \ldots, r_2 - 1\}$, then the family of abelian codes*

$$\left\{ C_{(\beta_1,\beta_2)} = \left(\varphi^{-1}_{\beta_1, \overline{X_1^{h_1} a}} \cdot \varphi^{-1}_{\beta_2, \overline{X_2^{h_2} b}}\right) \mid \beta_1 \in U_{r_1} \text{ and } \beta_2 \in U_{r_2} \right\}$$

in $\mathbb{F}_q(r_1, r_2)$ verifies $\Delta\left(M(ab)\right) = \Delta(C_{(\beta_1,\beta_2)}) = d(C_{(\beta_1,\beta_2)})$.

The following example shows how to use Corollary 34.

Example 35 Set $q = 2$, $r_1 = 3$ and $r_2 = 45$ (so $n = 135$). Fix $\alpha_1 \in U_3$ and $\alpha_2 \in U_{45}$. Consider the polynomials $a = X + 1$ and $b = Y^{40} + Y^{39} + Y^{38} + Y^{36} + Y^{35} + Y^{32} + Y^{30} + Y^{25} + Y^{24} + Y^{23} + Y^{21} + Y^{20} + Y^{17} + Y^{15} + Y^{10} + Y^9 + Y^8 + Y^6 + Y^5 + Y^2 + 1$. Then $a \mid X^3 - 1$. Note that $\mathrm{supp}\left(X \cdot a(X)\right) = \{1, 2\} = C_2(1)$. By [9, Lemma 1] we have that $h_1 = 1$ works. Now, the polynomial b appears in [9, Example 5] where it was mentioned that $b \mid x^{45} - 1$ in $\mathbb{F}_2[x]$. In that example, it is shown that, for $\alpha_2 \in U_{45}$ (for instance, the one with minimal polynomial $Y^{12} + Y^3 + 1$), since $b(1) = 1$ and $b(\alpha_2^3) = \alpha_2^{30}$, then $(Y^5 b)(1) = 1$, $(Y^5 b)\left(\alpha_2^3\right) = (\alpha_2^3)^5 \alpha_2^{30} = \alpha_2^{45} = 1$. So $h_2 = 5$ will work because $(Y^5 b)\left(\alpha_2^6\right) = (Y^5 b)\left(\alpha_2^{12}\right) = (Y^5 b)\left(\alpha_2^{24}\right) = 1$; note that $C_2(3) = \{3, 6, 12, 24\}$ modulo 45. Now set $C = (\varphi^{-1}_{\alpha_1, Xa} \cdot \varphi^{-1}_{\alpha_2, Y^5 b}) \subset \mathbb{F}_2(r_1, r_2) = \mathbb{F}_2(3, 45)$. Then $D_{(\alpha_1,\alpha_2)}(C) = C_2(1) \times (C_2(1) \cup C_2(3) \cup C_2(9) \cup C_2(21))$.

One may check that $10 = \Delta(M(ab))$; so that $d(C) = 10$ and $\dim_{\mathbb{F}_2}(C) = 87$.

The next example shows that from a code satisfying the conditions of Theorem 17, we can obtain a code with better parameters by making slight modifications on the defining set in such a way that the new code verifies the same conditions, but it has higher dimension, for example.

Example 36 Set $q = 2$, $r_1 = 3$ and $r_2 = 45$. Fix $\alpha_1 \in U_3$ and $\alpha_2 \in U_{45}$. Consider the code C in Example 35; that is $D_{(\alpha_1,\alpha_2)}(C) = C_2(1) \times (C_2(1) \cup C_2(3) \cup C_2(9) \cup C_2(21))$ and set $g = Xa \cdot Y^5 b$. As one may check there are three subsets determining $\Delta(M(g))$; to witt

$$\begin{aligned} S_1 &= \{(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4)\}, \\ S_2 &= \{(1,16), (1,17), (1,18), (1,19), (2,16), (2,17), (2,18), (2,19)\} \text{ and} \\ S_3 &= \{(1,31), (1,32), (1,33), (1,34), (2,31), (2,32), (2,33), (2,34)\}. \end{aligned}$$

If one computes $\Delta(M(g))$ by considering S_1 then clearly $C_2(1) \times C_2(21)$ will have no influence in the computation. Hence one may construct the new code C' for which $D_{(\alpha_1,\alpha_2)}(C') = C_2(1) \times (C_2(1) \cup C_2(3) \cup C_2(9))$ such that $\Delta(C') = \Delta(C) = \Delta(M(g))$.

Note that the matrix afforded by $D = D_{(\alpha_1,\alpha_2)}(C')$ is also a CP-matrix and so $\mathbb{B}-\mathrm{mad}(M(D)) = \Delta(M(D)) = 10$. Since C is a subcode of C' then $c = \varphi^{-1}_{\alpha_1,g} \in C'$ and, clearly, g satisfies conditions *(2a)* and *(2b)* of Theorem 17 for C'; hence $\Delta(C') = \Delta(M(g)) = d(C') = 10 = d(C) = \Delta(C)$. Since $\dim_{\mathbb{F}_2}(C') = 95$ and $\dim_{\mathbb{F}_2}(C) = 87$, C' is a code with better parameters than those of C.

Next application comes from [9, Corollary 6].

Corollary 37 *Let $\mathbb{K}$ be an intermediate field $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \mathbb{L}$ and $a = a(X_1) \in \mathbb{K}(r_1)$ be such that $a \mid X_1^{r_1} - 1$ with $\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \in \mathbb{F}_q(r_1)$, for some $\alpha_1 \in U_{r_1}$ and $h_1 \in \mathbb{Z}_{r_1}$.*

Let g be an irreducible factor of $X_2^{r_2} - 1$ in $\mathbb{K}[X_2]$ with defining set $D_{\alpha_2}(g)$, for some $\alpha_2 \in U_{r_2}$. Set $b = (X_2^n - 1)/g$. If there are positive integers j, t such that $b(\alpha_2^j) = \alpha_2^t$ and $\gcd\left(j, \frac{r_2}{\gcd(q-1, r_2)}\right) \mid t$, then there exists $h_2 \in \mathbb{Z}_{r_2}$ such that the abelian code $C = \left(\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \cdot \varphi^{-1}_{\alpha_2, \overline{X_2^{h_2} b}}\right)$ in $\mathbb{F}_q(r_1, r_2)$ verifies $\Delta(M(ab)) = \Delta(C) = d(C)$.

Our last application of this section is the following result that comes from [9, Corollary 7].

Corollary 38 *Let $a = a(X_1) \in \mathbb{L}(r_1)$ be such that $a \mid X_1^{r_1} - 1$ with $\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \in \mathbb{F}_2(r_1)$, for some $\alpha_1 \in U_{r_1}$ and $h_1 \in \mathbb{Z}_{r_1}$, and suppose $r_2 = 2^m - 1$, for some $m \in \mathbb{N}$. Then there exist at least $\frac{\phi(r_2)}{m}$ binary codes C of length $n = r_1 r_2$ such that $\Delta(M(ab)) = \Delta(C) = d(C)$.*

5.2 Application 2: True distance in BCH multivariate codes

A cyclic code C in $\mathbb{F}_q(r)$, with generator polynomial $f(x)$, is a BCH code of designed distance δ if there exists $\alpha \in U_r$ and $b \in \{0, \dots, n-1\}$ such that $f(x)$ is the polynomial with the lowest degree over $\mathbb{F}_q$ such that $\left\{\alpha^{b+j} \mid j = 0, \dots, \delta - 2\right\} \subseteq$

$Z(C)$ (see [17, p. 202]). Equivalently, C is a BCH code if for any cyclotomic coset $A \subseteq D_\alpha(C)$ we have that $A \cap \{b+j \mid j=0,\ldots,\delta-2\} \neq \emptyset$ (see [9]). We denote such a code by $B_q(\alpha,\delta,b)$. Let us recall this definition focused on the bivariate case.

Definition 39 *Let $\bar{\gamma} \subseteq \{1,2\}$ and $\bar{\delta} = \{\delta_k \mid k \in \bar{\gamma}$ and $2 \leq \delta_k \leq r_k\}$. An abelian code C in $\mathbb{F}_q(r_1,r_2)$ is a* ***bivariate BCH code of designed distance*** *$\bar{\delta}$ if there exists a list of positive integers $\bar{b} = (b_k)_{k\in\bar{\gamma}}$ such that*

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

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

The BCH multivariate codes are denoted $B_q(\overline{\alpha},\bar{\gamma},\bar{\delta},\bar{b})$.

Let C be an abelian code in $\mathbb{F}_q(r_1,r_2)$ with $M = M(\mathcal{D}_{\overline{\alpha}}(C))$ the matrix afforded by its defining set with respect to some $\bar{\alpha} = (\alpha_1,\alpha_2) \in U$. If M satisfies $\operatorname{supp}(M) = \pi_1(\operatorname{supp}(M)) \times \pi_2(\operatorname{supp}(M))$ then $\overline{\mathcal{D}_{\overline{\alpha}}(C)} = \pi_1(\operatorname{supp}(M)) \times \pi_2(\operatorname{supp}(M))$. We set $S_1 = \pi_1(\operatorname{supp}(M))$ and $S_2 = \pi_2(\operatorname{supp}(M))$. Then, one may consider the cyclic codes C_1 and C_2 with defining sets $D_1 = \mathbb{Z}_{r_1} \setminus S_1$ and $D_2 = \mathbb{Z}_{r_2} \setminus S_2$ with respect to α_1 and α_2, respectively (note that $\mathcal{D}_{\overline{\alpha}}(C) \neq D_1 \times D_2$ provided $I \neq \mathcal{D}_{\overline{\alpha}}(C) \neq D_1 \times D_2$).

Now suppose that the code C is an abelian code as described in Theorem 33 keeping the notation for the polynomials a and b and having in mind Remark 32. By the proof of this theorem one also may deduce that viewing $\varphi^{-1}_{\alpha_1,\overline{X_1^{h_1}a}}$ in $\mathbb{F}_q(r_1)$ and $\varphi^{-1}_{\alpha_2,\overline{X_2^{h_2}b}}$ in $\mathbb{F}_q(r_2)$ it happens that $C_1 = \left(\varphi^{-1}_{\alpha_1,\overline{X_1^{h_1}a}}\right) \subseteq \mathbb{F}_q(r_1)$ and $C_2 = \left(\varphi^{-1}_{\alpha_2,\overline{X_2^{h_2}b}}\right) \subseteq \mathbb{F}_q(r_2)$. It is also clear that the cyclic codes C_1 and C_2 verify that their minimum distances equal their respective maximum BCH bounds, as a and b satisfy the conditions in [9, Corollary 5].

Lemma 40 *Under the same notation from previous paragraphs, let C be an abelian code in $\mathbb{F}_q(r_1,r_2)$, with $M = M(\mathcal{D}_{\overline{\alpha}}(C))$ and suppose $\operatorname{supp}(M) = \pi_1(\operatorname{supp}(M)) \times \pi_2(\operatorname{supp}(M))$. Consider $D_1 = \mathbb{Z}_{r_1} \setminus \pi_1(\operatorname{supp}(M))$, $D_2 = \mathbb{Z}_{r_2} \setminus \pi_2(\operatorname{supp}(M))$ and let C_i be the cyclic code with $\mathcal{D}_{\alpha_i}(C_i) = D_i$, for $i \in \{1,2\}$. Then*

1. *For any set $\mathbb{B}$ of ds-bounds, $\Delta_{\mathbb{B},\overline{\alpha}}(C) = \Delta_{\mathbb{B},\alpha_1}(C_1) \cdot \Delta_{\mathbb{B},\alpha_2}(C_2)$.*
2. *C is a nonzero BCH multivariate code if and only if C_1 and C_2 are BCH cyclic codes in the classical sense (see [17]).*

Moreover, if case (2) holds, with $C_i = (\alpha_i,\delta_i,b_i)$, for $i \in \{1,2\}$, then $C = B_q((\alpha_1,\alpha_2),\{1,2\},\{\delta_1,\delta_2\},\{b_1,b_2\})$.

Proof. Assertion *(1)* comes from Corollary 29, having in mind Remark 32.

Now we prove assertion *(2)*. First, suppose that C is a multivariate BCH code. Assume that $1 \in \bar{\gamma}$, and let $B = \{\overline{b_1}, \ldots, \overline{b_1 + \delta_1 - 2}\}$ be its list of consecutive integers modulo r_1. Consider a q-cyclotomic coset $T \subseteq D_1$ and take $t \in T$. Since $t \in D_1$ then the set $(t, \mathbb{Z}_{r_2}) \subseteq \mathcal{D}_{\overline{\alpha}}(C)$ (with the obvious meaning).

If $(t, \mathbb{Z}_{r_2}) \cap Q(\overline{b_1 + l}, \mathbb{Z}_{r_2}) \neq \emptyset$, for some $l \in \{0, \ldots, \delta_1 - 2\}$, then we are done. Otherwise, it must happen $2 \in \bar{\gamma}$ and $(t, \mathbb{Z}_{r_2}) \subset \bigcup_{l=0}^{\delta_2 - 2} Q(\mathbb{Z}_{r_1}, \overline{b_2 + l})$. Since $C \neq 0$ then we may take an element $u \in \mathbb{Z}_{r_2} \setminus \bigcup_{l=0}^{\delta_2-2} C_q(\overline{b_2 + l})$ and clearly $(t, u) \notin \bigcup_{l=0}^{\delta_2-2} Q(\mathbb{Z}_{r_1}, \overline{b_2 + l})$, a contradiction.

The final assertion comes immediately from the fact that M is a CP-matrix. ■

Theorem 41 *Let $\mathbb{K}$ be an intermediate field $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \mathbb{L}$, $a = a(X_1) \in \mathbb{K}(r_1)$ and $b = b(X_2) \in \mathbb{K}(r_2)$ be such that $a \mid X_1^{r_1} - 1$ and $b \mid X_2^{r_2} - 1$. If there exist $(\alpha_1, \alpha_2) \in U$, $h_1 \in \mathbb{Z}_{r_1}$ and $h_2 \in \mathbb{Z}_{r_2}$ for which $\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \in \mathbb{F}_q(r_1)$ and $\varphi^{-1}_{\alpha_2, \overline{X_2^{h_2} b}} \in \mathbb{F}_q(r_2)$, with at least one of them not invertible, then there exists a family of permutation equivalent BCH multivariate codes $\left\{C_{\overline{\beta}} = B_q(\overline{\beta}, \bar{\gamma}, \bar{\delta}, \bar{b}) \mid \overline{\beta} \in U\right\}$ in $\mathbb{F}_q(r_1, r_2)$ such that*

1. *$\bar{\gamma} \subseteq \{1, 2\}$ and*
   (a) *If $\mathrm{supp}(a) = \mathbb{Z}_{r_1}$ then $1 \notin \bar{\gamma}$.*
   (b) *If $\mathrm{supp}(b) = \mathbb{Z}_{r_2}$ then $2 \notin \bar{\gamma}$.*
2. *$\bar{\delta} = \{\delta_k \mid k \in \bar{\gamma}\}$ with $\delta_1 = \Delta(M(a))$ and $\delta_2 = \Delta(M(b))$.*
3. *$\prod_{k \in \bar{\gamma}} \delta_k = \Delta(C_{\overline{\beta}}) = d(C_{\overline{\beta}})$, for each $\bar{\beta} \in U$.*
4. *$\varphi^{-1}_{\beta_1, \overline{X_1^{h_1} a}} \cdot \varphi^{-1}_{\beta_2, \overline{X_2^{h_2} b}} = \varphi^{-1}_{\overline{\beta}, \overline{X_1^{h_1} a X_2^{h_2} b}} \in C_{\overline{\beta}}$, where $\overline{\beta} = (\beta_1, \beta_2)$.*

Proof. Set $\bar{b} = \{b_k \mid k \in \bar{\gamma}\}$. First, suppose $\mathrm{supp}(M(a)) = \mathrm{supp}(a) \neq \mathbb{Z}_{r_1}$ and $\mathrm{supp}(M(b)) = \mathrm{supp}(b) \neq \mathbb{Z}_{r_2}$. Then by [9, Theorem 2], for each $\overline{\beta} \in U$, there exist BCH cyclic codes $B(a) = B_q(\beta_1, \delta_1, b_1)$ and $B(b) = B_q(\beta_2, \delta_2, b_2)$ such that $\delta_1 = \Delta(M(a))$, $\delta_2 = \Delta(M(b))$, $\varphi^{-1}_{\beta_1, \overline{X_1^{h_1} a}} \in B(a)$ and $\varphi^{-1}_{\beta_2, \overline{X_2^{h_2} b}} \in B(b)$. Now let $C = C_{\overline{\beta}}$ be the abelian code with $\overline{\mathcal{D}_{\overline{\beta}}(C)} = \overline{\mathcal{D}_{\beta_1}(B(a))} \times \overline{\mathcal{D}_{\beta_2}(B(b))}$ and set $M = M\left(\mathcal{D}_{\overline{\beta}}(C)\right)$. It is clear that M is a CP-matrix and, moreover, following the notation of Lemma 40, $D_1 = \mathcal{D}_{\beta_1}(B(a))$ and $D_2 = \mathcal{D}_{\beta_2}(B(b))$. Then C is a bivariate BCH code with $\bar{\gamma} = \{1, 2\}$, $\bar{\delta} = \{\delta_1, \delta_2\}$ and $b = \{b_1, b_2\}$. Now by statement *(1)* of Lemma 40, we have $\Delta_{\overline{\beta}}(C) = \delta_1 \delta_2$ and clearly statement *(4)* of this theorem holds by Theorem 33.

It remains to prove the equality $\Delta(C_{\overline{\beta}}) = d(C_{\overline{\beta}})$. On the one hand, we have $\Delta_{\overline{\beta}}(C) = \Delta(M(a))\Delta(M(b)) = \Delta(M(ab))$ and, on the other hand, by hypothesis, $\Delta(M(ab)) = \left|\overline{Z(ab)}\right|$. Hence, by applying Theorem 17, we are done. ∎

We may take, again, advantage from cyclic codes to transform a given abelian code $C = (g)$, with $d(C) = \Delta(C)$ into another abelian code with higher dimension, as in Example 36, until to get a new BCH code.

Example 42 We continue with the code C from Example 35. Recall that $q = 2$, $r_1 = 3$, $r_2 = 45$ and we have fixed $\alpha_1 \in U_3$ and $\alpha_2 \in U_{45}$. We have polynomials $a = X + 1$ and $b = Y^{40} + Y^{39} + Y^{38} + Y^{36} + Y^{35} + Y^{32} + Y^{30} + Y^{25} + Y^{24} + Y^{23} + Y^{21} + Y^{20} + Y^{17} + Y^{15} + Y^{10} + Y^{9} + Y^{8} + Y^{6} + Y^{5} + Y^{2} + 1$ such that $a \mid X_1^3 - 1$ and $h_1 = 1$ works, and $b \mid X_2^{45} - 1$ and $h_2 = 5$ works in the sense of Theorem 41. Hence the hypothesis of this theorem are satisfied.

Now we have to follow the proof to construct our multivariate BCH code. The proof of Theorem 41 uses a construction from [9, Theorem 2]. Clearly $B(a)$ is the BCH code in $\mathbb{F}_2(3)$ with defining set $D_{\alpha_1}(B(a)) = C_2(1)$. On the other hand, by [9, Example 8], the code $B(b)$ has defining set $D_{\alpha_2}(B(b)) = C_2(1) \cup C_2(3)$ so that it is a BCH code. In fact, $B(b) = B_2(\alpha_2, 5, 1)$, following the usual notation for BCH codes.

Thus $C_{(\alpha_1,\alpha_2)} = B_2\left((\alpha_1,\alpha_2), \{1,2\}, \{2,5\}, \{1,1\}\right)$, $d\left(C_{(\alpha_1,\alpha_2)}\right) = 10$ and $\dim_{\mathbb{F}_2}\left(C_{(\alpha_1,\alpha_2)}\right) = 58$. This code has better parameters than the code C from Example 35 and C' from Example 36.

We finish by extending Corollary 37 to bivariate BCH codes.

Corollary 43 *Let $\mathbb{K}$ be an intermediate field $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \mathbb{L}$ and $a = a(X_1) \in \mathbb{L}(r_1)$ be such that $a \mid X_1^{r_1} - 1$, with $\varphi^{-1}_{\alpha_1, \overline{X_1^{h_1} a}} \in \mathbb{F}_q(r_1)$, for some $\alpha_1 \in U_{r_1}$ and $h_1 \in \mathbb{Z}_{r_1}$.*

Let g be an irreducible factor of $X_2^{r_2} - 1$ in $\mathbb{K}[X_2]$ with defining set $D_{\alpha_2}(g)$, for some $\alpha_2 \in U_{r_2}$. Set $b = (X_2^n - 1)/h$. If there are positive integers j, t such that $b(\alpha_2^j) = \alpha_2^t$ and $\gcd\left(j, \frac{r_2}{\gcd(q-1,r_2)}\right) \mid t$ then there exists a bivariate BCH code $C = B_q(\overline{\alpha}, \bar{\gamma}, \bar{\delta}, \bar{b})$ in $\mathbb{F}_q(r_1, r_2)$ verifying $\Delta\left(M(ab)\right) = \Delta(C) = d(C)$, for certain $\overline{\alpha}, \bar{\gamma}, \bar{\delta}, \bar{b}$.

Proof. Comes immediately from Corollary 37 together with Theorem 41. ∎

6 Conclusion

We have developed a technique to extend any bound for the minimum distance of cyclic codes constructed from its defining sets (ds-bounds) to abelian (or multivariate) codes through the notion of $\mathbb{B}$-apparent distance. We used this technique to improve the searching for new bounds for abelian codes having unknown minimum distance. We have also studied conditions for an abelian code to verify that its $\mathbb{B}$-apparent distance reaches its (true) minimum distance and we have constructed some tables of such codes as an application.

References

[1] E.R. Berlekamp and J. Justesen, *Some long cyclic linear binary codes are not so bad*. IEEE Transactions on Information Theory **20** (1974), 351-356.

[2] J.J. Bernal, J.J. Simón, *Partial permutation decoding for abelian codes.* IEEE Transactions on Information Theory **59** (8) (2013), 5152-5170.

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

[4] J.J. Bernal, M. Guerreiro, J.J. Simón, *Ds-bounds for cyclic codes: new bounds for abelian codes*. Proceedings of ISITA 2016, Monterey, CA, USA, 712-716.

[5] E. Betti, M. Sala, *A new bound for the minimum distance of a cyclic code from its defining set*. IEEE Transactions on Information Theory **52** (8) (2006) 3700-3706.

[6] R.E. Blahut, *Decoding of cyclic codes and codes on curves.* In W.C. Huffman and V. Pless (Eds.), *Handbook of Coding Theory.* Vol. II, 1569-1633, 1998.

[7] A. E. Brouwer, T. Verhoeff, *An updated table of the minimum-distance bounds for binary linear codes*. IEEE Transactions on Information Theory **39** (2) (1993) 662–677.

[8] D. H. Bueno-Carreño, J.J. Bernal and J.J. Simón, *A characterization of cyclic codes whose minimum distance equals their maximum BCH bound.* Proceedings ACA 2013, Málaga, 109-113.

[9] D. H. Bueno-Carreño, J.J. Bernal and J.J. Simón, *Cyclic and BCH codes whose minimum distance equals their maximum BCH bound*. Advances in Mathematics of Communications 10 (2016), 459-474.

[10] P. Camion, *Abelian Codes*. MCR Tech. Sum. Rep. 1059, University of Wisconsin, Madison, 1970.

[11] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes.* Online available at http://www.codetables.de.

[12] C.R.P. Hartmann, H. Tai-Yang, *Some results on the weight structure of cyclic codes of composite lenght*. IEEE Transactions on Information Theory **22** (3) (1976) 340-348.

[13] C.R.P. Hartmann, K.K. Tzeng, *Generalizations of the BCH bound.* Information and Control **20** (1972) 489-498.

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

[15] J.M. Jensen, *The concatenated structure of cyclic and abelian codes.* IEEE Transactions on Information Theory **31** (6) (1985) 788-793.

[16] T. Kaida, J. Zhen, *A decoding method up to the Hartmann-Tzeng bound using the DFT for cyclic codes.* In Proceedings of Asia-Pacific Conference on Communications (2007) 409-412.

[17] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes.* Elsevier, Amsterdam, 1977.

[18] C. Roos, *A new lower bound for the minimum distance of a cyclic codes.* IEEE Transactions on Information Theory **29** (3) (1983) 330-332.

[19] C. Roos, *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound.* J. Combinatorial Theory, Series A (1982) 229-232.

[20] R.E. Sabin, *On minimum distance bounds for abelian codes.* Applicable Algebra Eng. Commun. Comput. **3** (3) (1992) 183-197.

[21] S. Sakata, *Decoding binary cyclic 2-D codes by the 2-D Berlekamp-Massey algorithm.* IEEE Transactions on Information Theory **37** (4) (1991) 1200-1203.

[22] J.H. van Lint and R.M. Wilson, *On the minimum distance of cyclic codes.* IEEE Transactions on Information Theory **32** (1) (1986) 23-40.

[23] K.-C. Yamada, *Hypermatrix and its applications.* Hitotsubashi J. Arts Sciences **6**(1) (1965) 34-44.

[24] J. Zhen, T. Kaida, *The designed minimum distance of medium length for binary cyclic codes.* ISITA-2012, Honolulu, Hawaii (2012) 441-445.