A notion of multivariate BCH bounds and codes *

José Joaquín Bernal, Juan Jacobo Simón
Universidad de Murcia, Spain.

Diana H. Bueno-Carreño
Pontificia Universidad Javeriana-Cali, Cali, Colombia

josejoaquin.bernal@um.es, jsimon@um.es,
dhbueno@javerianacali.edu.co

Abstract

In this extended abstract, we use the techniques of computation of the minimum apparent distance of a hypermatrix given in [2] in order to develop a notion of BCH bound and BCH code in the multivariate case. Then we extend the most classical results in BCH codes to the multivariate case and we show how to construct abelian codes with maximum dimension with respect to prefixed bounds for their minimum distance.

Keywords

Minimum apparent distance of a hypermatrix, Apparent distance of an abelian code, Multivariable BCH bound, Multivarible BCH code.

1 Introduction, notation and preliminaries

The oldest lower bound for the minimum distance of a cyclic code is the BCH bound (see [4, p. 151]). Its study and its generalizations are classical topics, which include the study of the very well-known family of BCH codes. In 1970, P. Camion [3] extended the study of the BCH bound to the family of abelian codes by introducing the notion of apparent distance of an abelian code. For cyclic codes, it coincides with *the* BCH bound (see[3, p. 22]).

In [2] we gave an algorithm to compute the minimum apparent distance of a hypermatrix, and thereby to compute the apparent distance of an abelian code, based on hypermatrix manipulations that extends other methods (see [6]). In this extended abstract we use those techniques in [2] to develop a notion of BCH bound and BCH code in the multivariate case. We also extend the most classical results in BCH codes to our case. Finally, we show two different applications. The first one consists of constructing multivariate abelian codes from BCH cyclic codes, multiplying their dimension and preserving their BCH bounds. The second one consists of designing maximum dimensional abelian codes with respect to several bounds.

All throughout, $\mathbb{F}_q$ denotes the field with q elements where q is a power of a prime p. It will be the ground field of the codes. An abelian code is an ideal of a group algebra $\mathbb{F}_q G$, where G is an abelian group. It is well-known that a decomposition $G \simeq C_{r_1} \times \cdots \times C_{r_s}$, with C_{r_k} the cyclic group of order r_k for $k = 1, \ldots, s$, induces a canonical isomorphism of $\mathbb{F}_q$-algebras from $\mathbb{F}_q G$ to $\mathbb{F}_q[x_1, \ldots, x_s]/\langle x_1^{r_1} - 1, \ldots, x_s^{r_s} - 1\rangle$. We denote this quotient algebra by $A_q(r_1, \ldots, r_s)$ and by I the product $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$. So, we identify the codewords with polynomials that we write as $f = f(x_1, \ldots, x_s) = \sum a_{\mathbf{i}} X^{\mathbf{i}}$, where $\mathbf{i} = (i_1, \ldots, i_s) \in I$ and $X^{\mathbf{i}} = x_1^{i_1} \cdots x_s^{i_s}$.

We deal with abelian codes in the semisimple case; that is, we always assume that $\gcd(r_k, q) = 1$ for every $k = 1, \ldots, s$. Let U_{r_i} denotes the set of all r_i-th primitive roots of unity, for each $i = 1, \ldots, s$. We define $U = \{(\alpha_1, \ldots, \alpha_s) \ : \ \alpha_i \in U_{r_i}\}$. Every abelian code C in $A_q(r_1, \ldots, r_s)$ is totally determined by its *root set* $Z(C) = \{\alpha \in U : f(\alpha) = 0 \text{ for all } f \in C\}$. Fixed $\alpha = (\alpha_1, \ldots, \alpha_s) \in U$, C is determined by its *defining set*, $\mathcal{D}_\alpha(C) = \{(a_1, \ldots, a_s) \in I \ : \ f(\alpha_1^{a_1}, \ldots, \alpha_s^{a_s}) = 0 \text{ for all } f \in C\}$.

*This work was partially supported by MINECO (Ministerio de Economía y Competitividad), (Fondo Europeo de Desarrollo Regional) project MTM2012-35240 and Fundación Séneca of Murcia. The second author has been supported by Departamento Administrativo de Ciencia, Tecnología e Innovación de la República de Colombia.

Given an element $a = (a_1, \ldots, a_s) \in I$, we define its q^t-*orbit* modulo $(r_1, \ldots, r_s)$ as $Q_t(a) = \left\{ \left(a_1 \cdot q^i, \ldots, a_s \cdot q^i\right) \mid i \in \mathbb{N} \right\} \subseteq \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$. In the case $t = 1$ we only write $Q(a)$. The parameter $(r_1, \ldots, r_s)$ will be omitted because it will always be clear from the context.

It is easy to see that, in the semisimple case, for every abelian code C in $A_q(r_1, \ldots, r_s)$, $\mathcal{D}_\alpha(C)$ is a disjoint union of q-orbits modulo $(r_1, \ldots, r_s)$. Conversely, every union of q-orbits modulo $(r_1, \ldots, r_s)$ determines an abelian code (an ideal) in $A_q(r_1, \ldots, r_s)$ (see, for example, [1]).

To define and compute the apparent distance of an abelian code, we will associate to its defining set, with respect to $\alpha \in U$, certain hypermatrix that we will call q-orbits hypermatrix. Let $r_1, \ldots, r_s$ be positive integers, and set $I = \prod_{k=1}^{s} \mathbb{Z}_{r_k}$. For any $\mathbf{i} \in I$ we write its k-th coordinate as $\mathbf{i}(k)$. A hypermatrix, with entries in a set R, indexed by I (or an I-hypermatrix over R) is an s-dimensional I-array, that we denote by $M = (a_\mathbf{i})_{\mathbf{i} \in I}$, with $a_\mathbf{i} \in R$ [7]. The set of indices, the dimension and the ground field will be omitted if they are clear by the context. As usual, in case $s = 2$ we will say that M is a matrix, and for $s = 1$ we will call M a vector. We write $M = 0$ when all of its entries are 0; otherwise we may write $M \neq 0$. A hypercolumn is defined as $H_M(k, b) = \{a_\mathbf{i} \in M \ : \ \mathbf{i}(k) = b\}$, with $1 \leq k \leq s$ and $0 \leq b < r_k$, where the expression $a_\mathbf{i} \in M$ means that $a_\mathbf{i}$ is an entry of M. Usually, a hypercolumn will be seen as an $(s-1)$-dimensional hypermatrix. 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. When D is an union of q^t-orbits we will say that M is the hypermatrix of q^t-orbits afforded by D, and it will be denoted by $M = M(D)$. For any I-hypermatrix M with entries in a ring, we define the support of M as the set $supp(M) = \{\mathbf{i} \in I \ : \ a_\mathbf{i} \neq 0\}$; whose complement will be denoted by $\mathcal{D}(M)$. Note that, if D is a union of q^t-orbits, then the q^t-orbits hypermatrix afforded by D verifies that $\mathcal{D}(M(D)) = D$.

Let $\mathcal{Q}_t$ be the set of all q^t-orbits in I, for some $t \in \mathbb{N}$. We define a partial ordering over the set of q^t-orbit hypermatrices $\{M(D) \ : \ D = Q \text{ for some subset } Q \subseteq \mathcal{Q}_t\}$ as follows:

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

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

Let $\mathbb{F}_{q^v}/\mathbb{F}_q$ be an extension field such that $U \subset \mathbb{F}_{q^v}$. The (discrete) Fourier transform of a polynomial $f \in A_q(r_1, \ldots, r_s)$ (also called Mattson-Solomon polynomial [6]), with respect to $\alpha \in U$, that we denote by $\varphi_{\alpha,f}$, is $\varphi_{\alpha,f}(X) = \sum_{\mathbf{j} \in I} f(\alpha^\mathbf{j}) X^\mathbf{j}$. Clearly, $\varphi_{\alpha,f} \in A_{q^v}(r_1, \ldots, r_s)$; moreover, the function Fourier transform may be viewed as an isomorphism of algebras $\varphi_\alpha : A_{q^v}(r_1, \ldots, r_s) \longrightarrow (\mathbb{F}_{q^v}^{\prod_{i=1}^{s} r_i}, \star)$, where the multiplication "$\star$" in $\mathbb{F}_{q^v}^{\prod_{i=1}^{s} r_i}$ is defined coordinatewise. So, we may see $\varphi_{\alpha,f}$ as a vector in $\mathbb{F}_{q^v}^{\prod_{i=1}^{s} r_i}$ or as a polynomial in $A_{q^v}(r_1, \ldots, r_s)$. See [3, Section 2.2] for details.

1.1 Apparent distance of an abelian code

The apparent distance of hypermatrices is a tool used to compute a lower bound for the minimum distance of an abelian code. The notion of apparent distance was originally given for polynomials by P. Camion in [3, p. 21]. In [6, Section 2.3], Sabin computes the apparent distance of polynomials by using matrix methods in the case of two variables. As a generalization of those techniques, we introduce the notion of apparent distance of a hypermatrix (see [2]). 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 module r, if for each $0 \leq k < l$ we have that $b_{k+1} \equiv b_k + 1 \mod r$. If $b = b_k$ (resp. $b = b_{k+1}$) we denote $b^+ = b_{k+1}$ (resp. $b^- = b_k$).

Definition 1. *Let s, q, $r_1, \ldots, r_s$ and I be as above. Let M be a hypermatrix, $k \in \{1, \ldots, s\}$, $b \in \mathbb{Z}_{r_k}$ and $H_M(k, b)$ a nonzero hypercolumn. The set of zero hypercolumns adjacents to $H_M(k, b)$ is the set of hypercolumns $CH_M(k, b) = \{H_M(k, b_0), H_M(k, b_1), \ldots, H_M(k, b_l)\}$ 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, $b^+ = b_0$ and $H_M(k, b_l^+) \neq 0$. In the case $s = 1$ we replace hypercolumns by entries.*

Notation 2. *We denote by $\omega_M(k, b)$ the value $|CH_M(k, b)|$; in the case $s = 1$ we write $\omega_M(b) = \omega_M(1, b)$. Note that for some values k and b it may happen that $\omega_M(k, b) = 0$.*

Definition 3. *Let s, q, $r_1, \ldots, r_s$ and I be as above. Let M be a hypermatrix over $\mathbb{F}_q$ and $k \in \{1, \ldots, s\}$.*

1. *If M is the zero hypermatrix, its apparent distance is $d^*0 = 0$.*
2. *In case $s = 1$, the apparent distance of a vector M is $d^*M = \max_{b \in \mathbb{Z}_{r_1}} \{\omega_M(b) + 1\}$.*

3. *For $s \geq 2$, we give the definition in two steps:*
   (3.1) The apparent distance of M with respect to the k-th face is

$$d_k^* M = \max_{b \in \mathbb{Z}_{r_k}} \{(\omega_M(k,b)+1) \cdot d^* H_M(k,b)\}.$$

   Then

   (3.2) the apparent distance of M is $d^*M = \max_{1 \leq k \leq s}\{d_k^* M\}$.

Theorem 4. *[2, Theorem 7] Let $s, q, r_1, \ldots, r_s$, I and $A_{q^v}(r_1, \ldots, r_s)$ be as above. For a polynomial $f \in A_{q^v}(r_1, \ldots, r_s)$ with coefficient hypermatrix $M(f)$, the equality $d^* f = d^* M(f)$ holds.*

Now, we give an alternative definition of apparent distance of a code, to that given by Camion in [3].

Definition 5. *Let C be a code in $A_q(r_1, \ldots, r_s)$. The apparent distance of C, with respect to $\alpha \in U$, is $d_\alpha^* C = \min\left\{d^* M(\varphi_{\alpha,e}) \ : \ 0 \neq e^2 = e \in C\right\}$, where $\varphi_{\alpha,e}$ denotes the image of e under the discrete Fourier transform, with respect to α, as we denoted in the previous section. The apparent distance of C is $d^*C = \max\left\{d_\beta^* C \ : \ \beta \in U\right\}$. We also define the set of optimized roots of C as $\mathcal{R}(C) = \{\beta \in U \ : \ d^*C = d^* M(\varphi_{\beta,e})\}$.*

Note that, if $e \in A_q(r_1, \ldots, r_s)$ is an idempotent and E is the ideal generated by e then for any $\alpha \in U$ we have that $M(\varphi_{\alpha,e}) = M(\mathcal{D}_\alpha(E))$. Now let C be an abelian code and $M = M(\mathcal{D}_\alpha(C))$. For any q-orbits hypermatrix $P \leq M$ [see (1)] there exists an idempotent $e' \in C$ such that $P = M(\varphi_{e'})$. So we may conclude that $\min\{d^* P \ : \ P \leq M\} = \min\{d^* M(\varphi_{\alpha,e}) \ : \ 0 \neq e^2 = e \in C\}$. This fact drives us to give the following definition.

Definition 6. *In the setting described above, for a q-orbits hypermatrix M, its minimum apparent distance is $mad(M) = \min\{d^* P \ : \ 0 \neq P \leq M\}$.*

The apparent distance is a lower bound for the minimum distance of any abelian code (see [3, Theorem 4.1]). In the next theorem we set the relationship between the apparent distance of an abelian code and the minimum apparent distances of the coefficient hypermatrices of the Fourier transforms of its generating idempotent. It is one of our main results.

Theorem 7. *Let C be an abelian code in $A_q(r_1, \ldots, r_s)$ and let e be its generating idempotent. Then $d_\alpha^* C = mad\,(M(\varphi_{\alpha,e}))$ $(\alpha \in U)$. Therefore, $d^*C = \max\{mad\,(M(\varphi_{\alpha,e})) : \alpha \in U\}$.*

In [2, Theorem 9] we present a technique to compute the minimum apparent distance of a hypermatrix and thereby to compute the apparent distance of an abelian code.

Remark 8. Let us note that the maximum that defines d^*C does not have to be computed over all the elements of U. Indeed, let $Q(a_1), Q(a_2), \ldots, Q(a_h)$ be all different q-orbits modulo $(r_1, \ldots, r_s)$ and fix the representatives $a_1, \ldots, a_h$. Chose $\alpha \in U$ to get a defining set $\mathcal{D}_\alpha(C)$. Let $\beta \in U$. One may see that if $\mathcal{D}_\beta(C) \neq \mathcal{D}_\alpha(C)$ then $\beta^{a_i} = \alpha$ for some $a_i = (a_{i1}, \ldots, a_{is})$ such that $\gcd(a_{ij}, r_j) = 1$ with $j = 1, \ldots, s$. In this case, it is clear that $\mathcal{D}_\beta(C) = a_i \cdot \mathcal{D}_\alpha(C)$, where the multiplication has the obvious meaning.

Then, we denote by $K(r_1, \ldots r_s) = \{a_i = (a_{i1}, \ldots, a_{is}) \ : \ \gcd(a_{ij}, r_j) = 1, j = 1, \ldots, s, i = 1, \ldots, h\}$ and fixed $\alpha \in U$ we define $\mathcal{R}_\alpha = \{\beta \in U \ : \ \beta^{a_i} = \alpha, a_i \in K(r_1, \ldots, r_s)\}$. So, in practice, fixed $\alpha \in U$, $d^*C = \max\left\{d_\beta^* C \ : \ \beta \in \mathcal{R}_\alpha\right\}$.

2 Multivariate BCH bounds and BCH codes

Theorem 9. ***(Multivariate BCH bound)*** *Let s, q, $r_1, \ldots, r_s$ be positive integers, with q a power of a prime number p, such that $p \nmid r_i$, for $i = 1, \ldots s$ and $\alpha \in U$. We set $I = \prod_{j=1}^s \mathbb{Z}_{r_j}$. Let C be a nonzero abelian code in $A_q(r_1, \ldots, r_s)$ with defining set $\mathcal{D}_\alpha(C)$ and M the q-orbits hypermatrix afforded by $\mathcal{D}_\alpha(C)$. Suppose that there exist a subset $\gamma \subseteq \{1, \ldots, s\}$ and a list of integers $\{\delta_k \geq 2 \ : \ k \in \gamma\}$ satisfying the following property: for each $k \in \gamma$, the hypermatrix M has distinct zero hypercolumns $H_M(k, j_{(k,0)}), \ldots, H_M(k, j_{(k,\delta_k-2)})$, where $\{j_{(k,0)}, \ldots, j_{(k,\delta_k-2)}\}$ is a list of consecutive integers modulo r_k (see Section 1.1). Then $d_\alpha^* C \geq \prod_{k \in \gamma} \delta_k$. Hence, $d^*C \geq \prod_{k \in \gamma} \delta_k$.*

Example 10. Set $q=2$, $r_1=5$, $r_2=7$, $D=Q(0,0)\cup Q(0,1)\cup Q(0,3)\cup Q(1,1)$ and $M=M(D)$. Then $H_M(1,0)=0$ and $H_M(2,1)=H_M(2,2)=H_M(2,4)=0$. So we take $\gamma=\{1,2\}$, $\delta_1=2$, $\delta_2=3$, $j_{(1,0)}=0$, $j_{(2,0)}=1$ and $j_{(2,1)}=2$. Then if C is the abelian code with defining set D, with respect to some $\alpha\in U$, we can check that $d^*C\geq 6$. In this case we have that d^*C achieves this bound.

Let us reformulate last theorem in a more traditional way. We recall that for any two integers $b,r\in\mathbb{Z}$ with $r>0$, we denote by $\overline{b}$ the canonical representative of b in $\mathbb{Z}_r$.

Corollary 11. *Let $\gamma\subseteq\{1,\ldots,s\}$ be a set, and let $\delta=\{\delta_k\geq 2\ :\ k\in\gamma\}$ and $b=\{b_k\geq 0\ :\ k\in\gamma\}$ be lists of integers. For each $k\in\gamma$ consider the list of consecutive integers modulo r_k, $J_k=\{\overline{b_k},\ldots,\overline{b_k+\delta_k-2}\}$ and set $A_k=\{\mathbf{i}\in I\ :\ \mathbf{i}(k)\in J_k\}$. If C is a nonzero abelian code satisfying $\cup_{k=1}^s A_k\subseteq\mathcal{D}_\alpha(C)$, for some $\alpha\in U$, then $d^*C\geq\prod_{k\in\gamma}\delta_k$.*

Example 12. Set $q=2$, $r_1=3$, $r_2=r_3=5$, $D=Q(0,0,0)\cup Q(0,0,1)\cup Q(0,1,0)\cup Q(1,0,0)\cup Q(1,0,1)\cup Q(1,0,2)\cup Q(1,1,0)\cup Q(1,2,0)$, $M=M(D)$ and let C be the abelian code with defining set D, with respect to some $\beta\in U$. One may check that $H_M(2,0)=H_M(3,0)=0$; so that, we may take $\gamma=\{1,2\}$, $\delta=\{2,2\}$, $b=\{0,0\}$ and then $d^*C\geq 4$.

Now we present a new notion of multivariate BCH code. We set $I(k,l)=\{\mathbf{i}\in I:\mathbf{i}(k)=l\}$.

Definition 13. ***(Multivariate BCH code)*** *Let $s,q,r_1,\ldots,r_s$, I be as above. Let $\gamma\subseteq\{1,\ldots,s\}$ and $\delta=\{\delta_k\geq 2\ :\ k\in\gamma\}$. An abelian code C in $A_q(r_1,\ldots,r_s)$ is a multivariate BCH code of designed distance δ if there exists a list of positive integers $b=\{b_k\ :\ k\in\gamma\}$ such that $\mathcal{D}_\alpha(C)=\bigcup_{k\in\gamma}\bigcup_{l=0}^{\delta_k-2}\bigcup_{\mathbf{i}\in I(k,\overline{b_k+l})}Q(\mathbf{i})$ for some $\alpha\in U$, where $\{\overline{b_k},\ldots,\overline{b_k+\delta_k-2}\}$ is a list of consecutive integers modulo r_k. We denote $C=B_q(\alpha,\gamma,\delta,b)$, as usual.*

Example 14. *In Example 10 we obtained the multivariate BCH code $B_2(\alpha,\{1,2\},\{2,3\},\{0,1\})$ and the BCH multivariate code in Example 12 is $B_2(\beta,\{2,3\},\{2,2\},\{0,0\})$.*

As a direct consequence of Theroem 9 we have that $d^*B_q(\alpha,\gamma,\delta,b)\geq\prod_{k\in\gamma}\delta_k$. From now on, we shall extend the basic properties of BCH codes to the multivariate case. The following property is immediate.

Corollary 15. *Let $B_q(\alpha,\gamma,\delta,b)$ be a multivariate BCH code. For each $k\in\gamma$, set $J_k=\{\overline{b_k},\ldots,\overline{b_k+\delta_k-2}\}$ and $A_k=\{\mathbf{i}\in I\ :\ \mathbf{i}(k)\in J_k\}$. If C is an abelian code in $A_q(r_1,\ldots,r_s)$ such that $\cup_{k=1}^s A_k\subseteq\mathcal{D}_\alpha(C)$ then $\dim C\leq\dim B_q(\alpha,\gamma,\delta,b)$.*

To see the next property we need additional notation. Let a and b be positive coprime integers. The multiplicative order of a modulo b is the first positive integer m, such that b divides a^m-1. We shall denote it by $\mathcal{O}_b(a)$. It is known (see [5, Theorem 10, p. 203]) that any (univariate) BCH code $B=B_q(\alpha,\delta,b)$ in $\mathbb{F}_q^r$ verifies that $d(B)\geq\delta$ and $\dim(B)\geq r-m(\delta-1)$, where $m=\mathcal{O}_r(q)$. In the multivariate case we have the following result.

Theorem 16. *Let $s,q,r_1,\ldots,r_s$ and I be as above and let $B_q(\alpha,\gamma,\delta,b)$ be a multivariate BCH code with $\delta=\{\delta_k\geq 2\ :\ k\in\gamma\}$ and $b=\{b_k\geq 0\ :\ k\in\gamma\}$. Then $\dim_{\mathbb{F}_q}B_q(\alpha,\gamma,\delta,b)\geq\prod_{j=1}^s r_j-m\left(\sum_{k\in\gamma}\left((\delta_k-1)\prod_{\substack{j=1\\ j\neq k}}^s r_j\right)\right)$, where $m=\operatorname{lcm}\{\mathcal{O}_{r_k}(q)\}_{k\in\gamma}$.*

3 Applications

Application 1. Multiplying dimension in abelian codes. We shall construct abelian codes starting from cyclic codes with apparent distance $\delta\in\mathbb{N}$.

Theorem 17. *Let n and r be positive integers such that $\gcd(q,nr)=1$ and $\alpha=(\alpha_1,\alpha_2)\in U_n\times U_r$. Let C be a cyclic code in $A_q(r)$ with $d^*C=d^*_{\alpha_2}(C)=\delta>1$. Then, the abelian code C_n in $A_q(n,r)$ with defining set $\mathcal{D}_\alpha(C_n)=\mathbb{Z}_n\times\mathcal{D}_{\alpha_2}(C)$ verifies that $d^*C_n=d^*_\alpha(C_n)=\delta$ and $\dim_{\mathbb{F}_q}(C_n)=n\dim_{\mathbb{F}_q}(C)$.*

Example 18. Set $q=2$, $r=55$, $n=3$. Consider $\alpha_2\in U_{35}$ and the code C such that $\mathcal{D}_{\alpha_2}(C)=Q(1)\cup Q(5)$. So C is a BCH code with designed distance $\delta=7$, i.e. $d^*_{\alpha_2}C=\delta=7$, and dimension 25. By applying the theorem above we construct the abelian code C_3 with $\mathcal{D}_{(\alpha_1,\alpha_2)}(C_3)=\mathbb{Z}_3\times\mathcal{D}_{\alpha_2}(C)$, for any $\alpha_1\in U_3$. Note that $\mathcal{D}_{(\alpha_1,\alpha_2)}(C_3)=\mathcal{D}_{(\beta,\alpha_2)}(C_3)$ for all $\beta\in U_3$. Then $d^*_{(\alpha_1,\alpha_2)}C_3=7$, $\dim_{\mathbb{F}_2}(C_3)=75$ and lenght 165. In fact $C_3=B_2((\alpha_1,\alpha_2),\{2\},\{7\},\{13\})$.

Proposition 19. *Let s, q, $r_1, \ldots, r_s$ and I be as above and let $B_q(\alpha, \gamma, \delta, b)$ be a multivariate BCH code with $\gamma = \{k\}$, for some $k \in \{1, \ldots, s\}$. If $r_k = q - 1$ then $d^*_\alpha B_q(\alpha, \gamma, \delta, b) = \delta_k$ and $\dim_{\mathbb{F}_q}(B_q(\alpha, \gamma, \delta, b)) = (r_k - \delta_k + 1) \prod_{\substack{j=1 \\ j \neq k}}^{s} r_j$.*

Application 2. Designing maximum dimensional abelian codes (MD codes) for prescribed apparent distance. We are going to design maximum dimensional abelian codes (MD codes, for short) for prescribed apparent distances in the case $q = 2$ and lenght 45. To do this, we shall apply some of the ideas developed in this extended abstract that allows us to see abelian codes as ideals in univariate, bivariate or multivariate polynomial quotient rings. As the reader will see, our ideas are based in the consideration of the distribution of the q-orbits on the indexes of hypermatrices. We point out that some computations were done with GAP4r7 and with the cooperation of Alexander Konovalov. The authors are indebt to him.

In the case of univariate codes, to be a MD cyclic code implies that it is a BCH code for which its designed distance coincide with its apparent distance (the maximum of its BCH bounds) and with its Bose distance (which is, in fact its apparent distance). One may check that taking α the 45-th primitive root of unity with minimal polynomial $m_\alpha = x^{12} + x^3 + 1$ then $B(\alpha, 4, 15)$, $B(\alpha, 5, 15)$ and $B(\alpha, 7, 15)$ are MD cyclic codes to dimensions 31, 27 and 21, respectively.

Now we consider two variables $r_1 = 5$ and $r_2 = 9$. Following the notation in paragraph bellow Remark 8, we set $a_1 = (0, 0)$, $a_2 = (1, 0)$, $a_3 = (0, 1)$, $a_4 = (1, 1)$, $a_5 = (1, 2)$, $a_6 = (0, 3)$, $a_7 = (1, 3)$ and $a_8 = (1, 6)$ and we fix $\alpha = (\alpha_1, \alpha_2)$, where α_1 is the r_1-th primitive root of unity with minimal polynomial $m_1 = \Phi_5$ and α_2 is the r_2-th primitive root of unity with minimal polynomial $m_2 = x^6 + x^3 + 1$. Then $K(5, 9) = \{a_4, a_5\}$.

Taking into account the distribution of 2-orbits in a 5×9 matrix we begin by considering apparent distance at least 4; $d^* \geq 4$, for short. Let C_1 be the abelian code with $D_\alpha(C_1) = Q(a_2) \cup Q(a_3) = D_1$. One may check that $mad(M(D_1)) = 4$, $a_5 D_1 = D_1$ and $\dim_{\mathbb{F}_2}(C_1) = 35$. A simple inspection shows that C_1 is a MD bivariate code with $d^* C_1 = 4$. Now we consider $d^* \geq 5$. The abelian code C_2 with $D_\alpha(C_2) = Q(a_2) \cup Q(a_4) \cup Q(a_6) = D_2$ verifies that, $a_5 D_2 = Q(a_2) \cup Q(a_5) \cup Q(a_6)$, and one may check that $mad(M(D_2)) = mad(M(a_5 D_2)) = 5$, and that $\dim_{\mathbb{F}_2}(C_2) = 27$. So we have that C_2 is a MD bivariate code with $d^* C_2 = 5$. Finally, for $d^* \geq 6$, we consider the code C_3 with $D_\alpha(C_3) = Q(a_1) \cup D_2$. One may check that C_3 is a MD bivariate code with dimension 26 and apparent distance 6. Observe that, if we consider $r_1 = 3$, $r_2 = 15$ and we fix $\alpha \in U$ then we may choose representatives such that $K(3, 15) = \{(1, 7)\}$. So we can obtain the code C_4 with $D_\alpha(C_4) = Q(0, 0) \cup Q(1, 0) \cup Q(0, 7)$, $d^*(C_4) = 4$ and dimension 38.

By considering the distribution of 2-orbits in a $3 \times 3 \times 5$ hypermatrix, and fixed $\alpha \in U$, we may find the code C_5 with defining set $\mathcal{D}_\alpha(C_5) = Q(0, 0, 1) \cup Q(1, 0, 1) \cup Q(0, 1, 0)$, $d^* C_5 = 4$ and dimension 37. We also find C_6 with $\mathcal{D}_\alpha(C_6) = Q(0, 0, 0) \cup Q(0, 0, 1) \cup Q(1, 0, 1) \cup Q(0, 1, 0) \cup Q(1, 2, 2)$, $d^* C_6 = 6$ and dimension 28. Finally, the code C_7 with $\mathcal{D}_\alpha(C_7) = Q(0, 0, 0) \cup Q(0, 0, 1) \cup Q(1, 0, 1) \cup Q(0, 1, 0) \cup Q(1, 2, 1) \cup Q(1, 0, 2) \cup Q(1, 2, 0)$ has $d^* C_7 = 8$ and dimension 24. This is the code with the largest dimension (even than cyclic codes).

References

[1] J.J. Bernal and J.J. Simón, *Information sets from defining sets in abelian codes*, IEEE Trans. Inform. Theory, vol. 57, no. 12, pp. 7990-7999, 2011.

[2] D. H. Bueno-Carreño, J.J. Bernal and J.J. Simón, *Computing the Camion's multivariate BCH bound*, ITW-Sevilla 2013, pp. 355-359.

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

[4] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge, 2003.

[5] F.J. Macwilliams y N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 1977.

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

[7] K. Yamada, Hypermatrix and its application, Hitotsubashi J= Arts Sci., No. 6, 1965, pp.34–44.