Ds-bounds for cyclic codes: new bounds for abelian codes

Marinês Guerreiro,
marines@ufv.br

Departamento de Matemática
Universidade Federal de Viçosa

Algebra: celebrating Paulo Ribenboim´s 90th Birthday

Joint work with José Joaquín Bernal and Juan Jacobo Simón (Universidad de Murcia).

Research supported by CNPq-Brazil, Processo PDE 233497/2014-5.

Contents of the talk

- Define abelian codes and state some notation.
- Define ds-bound for the minimum distance of cyclic codes.
- Relate the weight of the codewords with the apparent distance of their discrete Fourier transforms.
- Define the apparent distance of abelian codes with respect to a set of ds-bounds.
- Present an algorithm (of linear complexity) to compute the apparent distance.
- Examples.

Abelian Codes

$\mathbb{F}$ a finite field with q elements, with q a power of a prime p
r_i positive integers, for all $i \in \{1, \ldots, s\}$, and $n = r_1 \cdots r_s$
$\mathbb{Z}_{r_i}$ the ring of integers modulo r_i with canonical representatives

An **abelian code** of length n is an ideal in the algebra

$$F(r_1, \ldots, r_s) = \mathbb{F}[X_1, \ldots, X_s]/\langle X_1^{r_1} - 1, \ldots, X_s^{r_s} - 1\rangle$$

and throughout the work we assume that this algebra is semisimple; that is, $\gcd(r_i, q) = 1$, for all $i \in \{1, \ldots, s\}$.

The codewords are identified with multivariable polynomials.
Let $I = \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$. Write $f \in \mathbb{F}(r_1, \ldots, r_s)$ as

$$f = f(X_1, \ldots, X_s) = \sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}},$$

where $\mathbf{i} = (i_1, \ldots, i_s) \in I$ and $\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_s^{i_s}$.

Abelian Codes

Generalized Reed-Muller codes, extended Golay codes and generalized Reed-Solomon codes are examples of non-cyclic abelian codes.

Camion in 1970 introduced an extension of the BCH bound from cyclic to abelian codes via computing the apparent distance of such codes.

There are papers by Sabin (1992) and Bernal et alli (2016) improving the original computation of Camion and giving a notion of multivariate BCH codes and bounds.

We propose a method to extend any bound for the minimum distance of cyclic codes based on the defining set to the multivariate case.

Some known such bounds for cyclic codes - BCH, Hartmann-Tzeng (HT), Roos, van Lint-Wilson (SB), Betti-Sala (BS).

Abelian Codes

Generalized Reed-Muller codes, extended Golay codes and generalized Reed-Solomon codes are examples of non-cyclic abelian codes.

Camion in 1970 introduced an extension of the BCH bound from cyclic to abelian codes via computing the apparent distance of such codes.

There are papers by Sabin (1992) and Bernal et alli (2016) improving the original computation of Camion and giving a notion of multivariate BCH codes and bounds.

We propose a method to extend any bound for the minimum distance of cyclic codes based on the defining set to the multivariate case.

Some known such bounds for cyclic codes - BCH, Hartmann-Tzeng (HT), Roos, van Lint-Wilson (SB), Betti-Sala (BS).

Abelian Codes

Generalized Reed-Muller codes, extended Golay codes and generalized Reed-Solomon codes are examples of non-cyclic abelian codes.

Camion in 1970 introduced an extension of the BCH bound from cyclic to abelian codes via computing the apparent distance of such codes.

There are papers by Sabin (1992) and Bernal et alli (2016) improving the original computation of Camion and giving a notion of multivariate BCH codes and bounds.

We propose a method to extend any bound for the minimum distance of cyclic codes based on the defining set to the multivariate case.

Some known such bounds for cyclic codes - BCH, Hartmann-Tzeng (HT), Roos, van Lint-Wilson (SB), Betti-Sala (BS).

Abelian Codes

Let U_{r_i} be the set of all r_i-th primitive roots of unity, for each $i \in \{1, \ldots, s\}$

$U = \prod_{i=1}^{s} U_{r_i}$.

For a fixed $\bar{\alpha} = (\alpha_1, \ldots, \alpha_s) \in U$, the code C is determined by its **defining set** with respect to $\bar{\alpha}$, which is defined as

$$\mathcal{D}_{\bar{\alpha}}(C) = \{(a_1, \ldots, a_s) \in I \ : \ f(\alpha_1^{a_1}, \ldots, \alpha_s^{a_s}) = 0, \text{ for all } f \in C.\}$$

For $\mathbf{a} = (a_1, \ldots, a_s) \in I$, define its q-**orbit** modulo $(r_1, \ldots, r_s)$ as

$$Q(a) = \left\{ \left(a_1 \cdot q^i, \ldots, a_s \cdot q^i\right) \in I \mid i \in \mathbb{N} \right\}.$$

Known Fact: the defining set $\mathcal{D}_{\bar{\alpha}}(C)$ of a code C is a disjoint union of q-orbits modulo $(r_1, \ldots, r_s)$ and, conversely, every union of q-orbits modulo $(r_1, \ldots, r_s)$ determines an abelian code (an ideal) in $\mathbb{F}(r_1, \ldots, r_s)$ (see [2, 7] or [12] for details).

Abelian Codes

Let U_{r_i} be the set of all r_i-th primitive roots of unity, for each $i \in \{1, \ldots, s\}$

$U = \prod_{i=1}^{s} U_{r_i}$.

For a fixed $\bar{\alpha} = (\alpha_1, \ldots, \alpha_s) \in U$, the code C is determined by its **defining set** with respect to $\bar{\alpha}$, which is defined as

$$\mathcal{D}_{\bar{\alpha}}(C) = \{(a_1, \ldots, a_s) \in I \ : \ f(\alpha_1^{a_1}, \ldots, \alpha_s^{a_s}) = 0, \text{ for all } f \in C.\}$$

For $\mathbf{a} = (a_1, \ldots, a_s) \in I$, define its q-**orbit** modulo $(r_1, \ldots, r_s)$ as

$$Q(a) = \left\{ \left(a_1 \cdot q^i, \ldots, a_s \cdot q^i\right) \in I \mid i \in \mathbb{N} \right\}.$$

Known Fact: the defining set $\mathcal{D}_{\bar{\alpha}}(C)$ of a code C is a disjoint union of q-orbits modulo $(r_1, \ldots, r_s)$ and, conversely, every union of q-orbits modulo $(r_1, \ldots, r_s)$ determines an abelian code (an ideal) in $\mathbb{F}(r_1, \ldots, r_s)$ (see [2, 7] or [12] for details).

Ds-bounds for cyclic codes

Let $r_1 = n$. Denote by $\mathcal{P}(\mathbb{Z}_n)$ the power set of $\mathbb{Z}_n$ and take $\alpha \in U_n$.

Definition

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 $n \in \mathbb{N}$, $\delta_n \subseteq \mathcal{P}(\mathbb{Z}_n) \times \mathbb{N}$ satisfies the following conditions:

1. If C is a cyclic code in $\mathbb{F}(n)$ such that $N \subseteq \mathcal{D}_\alpha(C)$, then $\mathbf{1 \leq a \leq d(C)}$, for all $(N, a) \in \delta_n$.
2. If $\emptyset \neq N \subseteq M$ 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 of the code. It will be clear in the context which one is being used.

Ds-bounds for cyclic codes

(1) BCH bound: for any cyclic code in $\mathbb{F}_q(n)$ having a string of $t-1$ consecutive integers in its defining set with respect to some $\alpha \in U_n$, the minimum distance of the code is at least t [16, Theorem 7.8].

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 (by stating Condition 3 as a convention).

(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 [4, 11, 17, 18, 24] and the new bounds and improvements arising from Corollary 1, Theorem 5 and results in Section 4 and Section 5 in [21], also verify Definition 1.

In order to relate the idea of ds-bound with the Camion's apparent distance (defined later), we consider the following family of maps.

Ds-bounds for cyclic codes

Definition

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 $\overline{\delta}_n(N) = \max\{b \in \mathbb{N} \,|\, (N, b) \in \delta_n\}$.

The following result is immediate.

Lemma

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

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

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

Hypermatrices and multivariate polynomials

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 set R indexed by I** is an s-dimensional I-array, denoted by $M = (a_{\mathbf{i}})_{\mathbf{i} \in I}$, with $a_{\mathbf{i}} \in R$ [22].
For $s = 2$, M is a matrix and when $s = 1$, M is a vector. We write $M = 0$ when all its entries are 0 and $M \neq 0$, otherwise.

For each polynomial $f = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$, consider the **hypermatrix of the coefficients of f**, denoted by $M(f) = (a_{\mathbf{i}})_{\mathbf{i} \in I}$.

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.

For any $j \in \{0, \ldots, s\}$, if we write $f = \sum_{k=0}^{r_j - 1} f_{j,k} X_j^k$, where $f_{j,k} = f_k(\mathbf{X}_j)$ and $\mathbf{X}_j = X_1 \cdots X_{j-1} \cdot X_{j+1} \cdots X_s$, then $M(f_{j,k}) = H_M(j,k)$.

This means that "fixed" the variable X_j in f, for each power k of X_j, the coefficient $f_{j,k}$ is a polynomial in $\mathbf{X}_j$, and $H_M(j,k)$ is the hypermatrix obtained from the coefficients of this $f_{j,k}$.

Hypermatrices and multivariate polynomials

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 set R indexed by I** is an s-dimensional I-array, denoted by $M = (a_{\mathbf{i}})_{\mathbf{i} \in I}$, with $a_{\mathbf{i}} \in R$ [22].
For $s = 2$, M is a matrix and when $s = 1$, M is a vector. We write $M = 0$ when all its entries are 0 and $M \neq 0$, otherwise.

For each polynomial $f = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$, consider the **hypermatrix of the coefficients of f**, denoted by $M(f) = (a_{\mathbf{i}})_{\mathbf{i} \in I}$.

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.

For any $j \in \{0, \ldots, s\}$, if we write $f = \sum_{k=0}^{r_j - 1} f_{j,k} X_j^k$, where $f_{j,k} = f_k(\mathbf{X}_j)$ and $\mathbf{X}_j = X_1 \cdots X_{j-1} \cdot X_{j+1} \cdots X_s$, then $M(f_{j,k}) = H_M(j,k)$.

This means that "fixed" the variable X_j in f, for each power k of X_j, the coefficient $f_{j,k}$ is a polynomial in $\mathbf{X}_j$, and $H_M(j,k)$ is the hypermatrix obtained from the coefficients of this $f_{j,k}$.

Hypermatrices

Let $D \subseteq I$. The **hypermatrix afforded by** D is defined as $M = (a_{\mathbf{i}})_{\mathbf{i} \in \mathbf{I}}$, where $a_{\mathbf{i}} = 1$ if $\mathbf{i} \notin D$ and $a_{\mathbf{i}} = 0$, otherwise.

When D is an union of q-orbits we say that M is a **q-orbits hypermatrix**, and denoted it by $M = M(D)$.

Let $n = 45 = 3 \times 15$ and $q = 5$. Fix $\alpha_1 \in U_3$ and $\alpha_2 \in U_{15}$. Then M is the 2-orbits matrix afforded by $D = Q(0,0) \cup Q(0,1) \cup Q(1,0)$.

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

For any I-hypermatrix M with entries in a ring, we define **the support of** M as the set $\mathrm{supp}(\mathbf{M}) = \{\mathbf{i} \in \mathbf{I} \mid \mathbf{a_i} \neq \mathbf{0}\}$. Its complement with respect to I will be denoted by $\mathcal{D}(M)$.

Hypermatrices

Let $D \subseteq I$. The **hypermatrix afforded by** D is defined as $M = (a_{\mathbf{i}})_{\mathbf{i} \in \mathbf{I}}$, where $a_{\mathbf{i}} = 1$ if $\mathbf{i} \notin D$ and $a_{\mathbf{i}} = 0$, otherwise.

When D is an union of q-orbits we say that M is a **q-orbits hypermatrix**, and denoted it by $M = M(D)$.

Let $n = 45 = 3 \times 15$ and $q = 5$. Fix $\alpha_1 \in U_3$ and $\alpha_2 \in U_{15}$. Then M is the 2-orbits matrix afforded by $D = Q(0,0) \cup Q(0,1) \cup Q(1,0)$.

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

For any I-hypermatrix M with entries in a ring, we define **the support of** M as the set $\mathrm{supp}(\mathbf{M}) = \{\mathbf{i} \in \mathbf{I} \mid \mathbf{a_i} \neq \mathbf{0}\}$. Its complement with respect to I will be denoted by $\mathcal{D}(M)$.

Hypermatrices

To define and compute the apparent distance of an abelian code we will use the hypermatrix afforded by its defining set, with respect to $\bar{\alpha} \in U$. Here we use the discrete Fourier transform of the polynomial.

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

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

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

Example: for $n = 3 \times 7 = 21$.

$$D = Q(0,1) \cup Q(1,1) \cup Q(1,3) \cup Q(0,0) \cup Q(0,3) \quad \supset \quad D' = Q(0,1) \cup Q(1,1) \cup Q(1,3)$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \leq \quad \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Apparent distance for vectors

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

Definition

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 $\delta^*(v) = \overline{\delta}(\mathbb{Z}_n \setminus \mathrm{supp}(v))$.

Let $\mathbb{B}$ a set of ds-bounds.

Definition

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 $\Delta_{\mathbb{B}}(v) = \max\{\delta^*(v) \mid \delta \in \mathbb{B}\}$.

Apparent distance for vectors

Example 1: Let C be a cyclic code of length 24 over $\mathbb{F}_5$, with defining set $D = \{0, 1, 2, 3, 5, 6, 7, 9, 10, 11, 15, 21\}$.

$$v = (0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1)$$

$\delta^*_{BS} = 8$, $\delta^*_{HT} = 5$, $\delta^*_{BCH} = 5$, $\delta^*_{Ross} = 6$

$\mathbb{B} = \{\delta_{BCH}, \delta_{Ross}, \delta_{HT}\} \Longrightarrow \Delta_{\mathbb{B}}(v) = 6.$

$\mathbb{B} = \{\delta_{BS}, \delta_{BCH}, \delta_{Ross}, \delta_{HT}\} \Longrightarrow \Delta_{\mathbb{B}}(v) = 8.$

Apparent distance for vectors

Remark

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* $\Delta_{\mathbb{B}}(v) \geq \Delta_{\mathbb{B}}(w)$. ■

We have examples that show that property (2) is not valid for abelian non-cyclic codes.

Proposition

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

Here φ is the discrete Fourier transform of the polynomial with respect to α.

Apparent distance for hypermatrices

Definition

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

1. $\Delta_{\mathbb{B}}(0) = 0$ and, for $s = 1$, Definition 5 applies.

Apparent distance for hypermatrices

Definition

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 $\mathrm{supp}_1(M) = \{i \in \{0, \ldots r_1 - 1\} \mid H_M(1, i) \neq 0\}$ and the **column support of** M as $\mathrm{supp}_2(M) = \{j \in \{0, \ldots r_2 - 1\} \mid H_M(2, j) \neq 0\}$. Then put

$$\begin{aligned} \omega_2(M) &= \max\{\overline{\delta}(\mathbb{Z}_{r_2} \setminus \mathrm{supp}_2(M)) \mid \delta \in \mathbb{B}\}, \\ \epsilon_2(M) &= \max\{\Delta_{\mathbb{B}}(H_M(2, j)) \mid j \in \mathrm{supp}_2(M)\} \end{aligned}$$

and set $\Delta_2(M) = \omega_2(M) \cdot \epsilon_2(M)$.
Analogously, we compute the apparent distance $\Delta_1(M)$ for the other variable and finally we define the **apparent distance of** M **with respect to** $\mathbb{B}$ by

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

Apparent distance for hypermatrices

Definition

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 of dimension $s-1$. Then first compute the "hypermatrix support" of $M \neq 0$ with respect to the j-th hypercolumn, that is,

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

Now put $\omega_j(M) = \max\{\overline{\delta}(\mathbb{Z}_{r_j} \setminus \mathrm{supp}_j(M)) \mid \delta \in \mathbb{B}\}$ and $\epsilon_j(M) = \max\{\Delta_{\mathbb{B}}(H_M(j,k)) \mid k \in \mathrm{supp}_j(M)\}$ 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:

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

Examples

Example

Set $n = 72 = 3 \times 24$ and $q = 5$. Fix $\alpha_1 \in U_3$ and $\alpha_2 \in U_{24}$ and consider the 5-orbits matrix M afforded by
$D = Q(0,0) \cup Q(0,1) \cup Q(0,2) \cup Q(0,3) \cup Q(0,6) \cup Q(0,7) \cup Q(0,9) \cup Q(1,0) \cup Q(1,1) \cup Q(1,5) \cup Q(1,6)$.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Choose $\mathbb{B} = \{\delta_{HT}, \delta_{BS}\}$. Then $\Delta_{\mathbb{B}}(M) = 8$.
$\mathrm{supp}_1(M) = \{0, 1, 2\}$ (there is no zero line) and $\omega_1(M) = 1$ (as $(\emptyset, 1) \in \delta, \forall \delta$)
$\Delta_{\mathbb{B}}(H_M(1,0)) = 8$, by using δ_{BS} (see [4, Example 4.2]) which is the maximum, hence $\epsilon_1(M) = 8$.
$\Delta_1(M) = \omega_1(M) \cdot \epsilon_1(M) = 1 \cdot 8$

On the other hand, $\mathrm{supp}_2(M) = \mathbb{Z}_{24} \setminus \{0, 1, 5, 6\}$ (the non-zero columns)
and $\omega_2(M) = 4$, by using δ_{HT}
$\epsilon_2(M) = 2$ (in the non-zero columns, the maximum length of strings of zeros is 1)
$\Delta_2(M) = \omega_2(M) \cdot \epsilon_2(M) = 2 \cdot 4 = 8$.

Also $\Delta_{\delta_{HT}}(M) = 8$, because although $\Delta_1(M) = 6$, $\Delta_2(M) = 8$.

Moreover, for $\mathbb{B} = \{\delta_{BCH}\}$, $\Delta_1(M) = 5$ and $\Delta_2(M) = 6$ (because $\omega_2(M) = 3$), hence $\Delta_{\mathbb{B}}(M) = 6$.

Apparent Distance and Weight of Codewords

Now we extend Proposition 6 to several variables.

Theorem

Let $f \in \mathbb{L}(r_1, \ldots, r_n)$ and $M(f)$ be the hypermatrix of its coefficients. Fix any $\bar{\alpha} \in U$. Then $\Delta_{\mathbb{B}}(M(f)) \leq \omega\left(\varphi_{\bar{\alpha},f}^{-1}\right)$.

The apparent distance of $M(f)$ is a lower bound for the weight of the word.

Apparent Distance for Abelian Codes

The following definition changes the usual way to present the apparent distance in [7] and the strong apparent distance in [2] (see also [19])

Definition

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

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

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

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

The following result is consequence of Theorem 11.

Corollary

For any abelian code C in $\mathbb{F}(r_1, \ldots, r_s)$ and any $\mathbb{B}$ as above, $\Delta_{\mathbb{B}}(C) \leq d(C)$.

Apparent Distance for Abelian Codes

To improve the efficiency of the computation the following result tells us that we may restrict our attention to the idempotents of the code.

Proposition

Let C be an abelian code in $\mathbb{F}(r_1, \ldots, r_s)$. The apparent distance of C with respect to $\bar{\alpha} \in U$ and $\mathbb{B}$ verifies the equality

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

If $e \in \mathbb{F}(r_1, \ldots, r_s)$ is an idempotent and E is the ideal generated by e then $\varphi_{\bar{\alpha},e} \star \varphi_{\bar{\alpha},e} = \varphi_{\bar{\alpha},e}$, for any $\bar{\alpha} \in U$.

Thus if $\varphi_{\bar{\alpha},e} = \sum_{\mathbf{i} \in \mathbf{I}} a_{\mathbf{i}} X^{\mathbf{i}}$, we have $a_{\mathbf{i}} \in \{1, 0\} \subseteq \mathbb{F}$ and $a_{\mathbf{i}} = 0$ if and only if $\mathbf{i} \in \mathcal{D}_{\bar{\alpha}}(\mathbf{E})$. Hence $M(\varphi_{\bar{\alpha},e}) = M(\mathcal{D}_{\bar{\alpha}}(E))$.

Apparent Distance for Abelian Codes

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 $\mathbb{F}(r_1, \ldots, r_s)$ such that $\mathcal{D}_{\bar{\alpha}}(C) = D$. Let $e \in C$ be its generating idempotent. One may verify that $M(\varphi_{\bar{\alpha},e}) = M(D)$.

Now let C be an abelian code, $\bar{\alpha} \in U$ and M the hypermatrix afforded by $\mathcal{D}_{\bar{\alpha}}(C)$. For any q-orbits hypermatrix $P \leq M$ [see the ordering (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 $\Delta_{\mathbb{B}}\left(M(\varphi_{\bar{\alpha},f})\right) = \Delta_{\mathbb{B}}\left(M(\varphi_{\bar{\alpha},e(f)})\right)$. So

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

This fact drives us to give the following definition.

Apparent Distance for Abelian Codes

Definition

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

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

The relation between the apparent distance of an abelian code and the minimum apparent distance of hypermatrices is set by:

Theorem

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

Algorithm for Two Variables

Definition

With the notation of the previous section, let D be a union of q-orbits and $M = M(D)$ the hypermatrix afforded by D. We say that $H_M(j,k)$ is an **involved hypercolumn (row or column for two variables) in the computation of $\Delta_{\mathbb{B}}(M)$**, if $\Delta_{\mathbb{B}}(H_M(j,k)) = \epsilon_j(M)$ and $\Delta_j(M) = \Delta_{\mathbb{B}}(M)$.

$I_p(M)$ denotes the set of indices of involved hypercolumns.

The involved hypercolumns are those which contribute in the computation of the $\mathbb{B}$-apparent distance.

The next result is a sufficient condition to get at once the minimum $\mathbb{B}$-apparent distance of a hypermatrix.

Proposition

With the notation as above, let D be a union of q-orbits and $M = M(D)$ the hypermatrix afforded by D. If $\Delta_{\mathbb{B}}(H_M(j,k)) = 1$, for some $H_M(j,k) \in I_p(M)$, then $\mathbb{B}-\mathrm{mad}(M) = \Delta_{\mathbb{B}}(M)$. ■

Algorithm for Two Variables

Theorem

Let $\mathbb{Q}$ be the set of all q-orbits modulo (r_1, r_2), $\mu \in \{1, \ldots, |\mathbb{Q}| - 1\}$ and $\{Q_j\}_{j=1}^{\mu}$ a subset of $\mathbb{Q}$. Set $D = \cup_{j=1}^{\mu} Q_j$ and $M = M(D)$.

Then there exist two sequences: the first one is formed by nonzero q-orbits matrices $M = M_0 > \cdots > M_l \neq 0$ and the second one is formed by positive integers $m_0 \geq \cdots \geq m_l$, with $l \leq \mu$ and $m_i \leq \Delta_{\mathbb{B}}(M_i)$, verifying the following property:

If P is a q-orbits matrix such that $0 \neq P \leq M$, then $\Delta_{\mathbb{B}}(P) \geq m_l$ and if $\Delta_{\mathbb{B}}(P) < m_{i-1}$ then $P \leq M_i$, where $0 < i \leq l$.
Moreover, if $l' \in \{0, \ldots, l\}$ is the first element satisfying $m_{l'} = m_l$ then $\Delta_{\mathbb{B}}(M_{l'}) = \mathbb{B}-\mathrm{mad}(M)$.

Algorithm for Two Variables

Set $I = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$.

Consider the matrix $M = (a_{ij})_{(i,j)\in I}$ and a set $\mathbb{B}$ of ds-bounds.

Step 1. Compute the apparent distance of M with respect to $\mathbb{B}$ and set $m_0 = \Delta_{\mathbb{B}}(M)$.

Step 2.

a) If there exists $H_M(j,k) \in Ip(M)$ (see Definition 17) such that $\Delta_{\mathbb{B}}(H_M(j,k)) = 1$ then we finish giving the sequences $M = M_0$ and $m_0 = \Delta_{\mathbb{B}}(M)$ (because of Proposition 18).

b) If $\Delta_{\mathbb{B}}(H_M(j,k)) \neq 1$, for all $H_M(k,b) \in Ip(M)$, we set $S = \bigcup_{H_M(k,b)\in Ip(M)} supp(H_M(k,b))$ and construct the matrix $M_1 = (a_{ij})_{(i,j)\in I}$ such that

$$a_{ij} = \begin{cases} 0 & \text{if } (i,j) \in \cup\{Q(k,b) \mid (k,b) \in S\} \\ m_{ij} & \text{otherwise.} \end{cases}$$

Algorithm for Two Variables

(In other words, $M_1 < M$ is the matrix with maximum support such that its involved rows and columns are zero. One may prove that if $0 \neq P < M$ and $\Delta_{\mathbb{B}}(P) < m_0$ then $P \leq M_1$.)

Step 3.

a) If $M_1 = 0$ then we finish giving the sequences $M = M_0$ and $m_0 = \Delta_{\mathbb{B}}(M)$.

b) If $M_1 \neq 0$, we set $m_1 = \min\{m_0, \Delta_{\mathbb{B}}(M_1)\}$, and we get the sequences $M = M_0 > M_1$ and $m_0 \geq m_1$. Then, we go back to Step 1 with M_1 in the place of M and m_1 in the place of m_0. ■

Remark

It is worth to note that if a matrix has μ q-orbits the algorithm has at most μ steps. ■

Examples

Tabela: Binary abelian codes with $n = 3 \times r_2$ and big rate

Code	n	dim	$\mathcal{D}(C)$ representatives	$\mathbb{B}$	Δ
C_1	21	16	$(0,1),(1,0)$	δ_{BCH}	3
C_2	45	39	$(0,1),(1,0)$	δ_{BCH}	3
C_3	51	35	$(0,1),(1,3)$	δ_{HT}	3
C_4	69	46	$(0,0),(1,1)$	δ_{SB}, δ_{BCH}	6
C_5	105	93	$(0,5)$, $(0,7)$, $(0,15)$,$(1,0)$	δ_{HT}, δ_{BCH}	4

Conclusion

We have developed a technique to extend any ds-bound for cyclic codes to multivariate codes, which can be applied to codes of arbitrary length, mainly for those whose minimum distance is unknown.

We use this technique to improve the searching of new bounds for abelian codes.

Discrete Fourier Transform

Let $\mathbb{L}|\mathbb{F}$ be an extension field containing U_{r_i}, for all $i \in \{1 \ldots, s\}$.

Definition

The **discrete Fourier transform of a polynomial $f \in \mathbb{F}(r_1, \ldots, r_s)$ with respect to $\bar{\alpha} \in U$** (also called **Mattson-Solomon polynomial** in [19]) is the polynomial

$$\varphi_{\bar{\alpha},f}(\mathbf{X}) = \sum_{\mathbf{j}\in\mathbf{I}} \mathbf{f}(\bar{\alpha}^{\mathbf{j}})\mathbf{X}^{\mathbf{j}} \in \mathbb{L}(\mathbf{r_1}, \ldots, \mathbf{r_s}).$$

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 [7, Section 2.2]).

To know more...


J.J. Bernal, J.J. Simón, *Partial permutation decoding for abelian codes*. IEEE Trans. Inform. Theory, **59** (8) (2013) 5152-5170.


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


F. Bernhardt, P. Landrock, O. Manz, *The extended Golay codes considered as ideals*. J. Comb. Theory Ser. A, **55** (1990) 235-246.


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


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.

To know more...


A. E. Brouwer, T. Verhoeff, *An updated table of the minimum-distance bounds for binary linear codes*. IEEE Trans. Inform. Theory, **39** (2) (1993) 662-677.


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


P. Charpin, *The Reed-Solomon code as ideals of a modular algebra*. C.R. Acad. Sci. Paris Ser. I Math. **294** (1982) 597-600.


M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Available online at http://www.codetables.de.


C.R.P. Hartmann, H. Tai-Yang, *Some results on the weight structure of cyclic codes of composite lenght*. IEEE Trans. Inform. Theory, **IT-22** (3) (1976) 340-348.


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

To know more...

- H. Imai, *A theory of two-dimensional cyclic codes*. Information and Control **34** (1) (1977) 1-21.
- A.V. Keralev, P. Solé, *Error-correcting Codes as Ideals in Group Rings*. Contemporary Mathematics **273** (2001) 11-18.
- 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.
- J.M. Jensen, *The Concatenated Structure of Cyclic and Abelian Codes*. IEEE Trans. Inform. Theory, **IT-31**(6) (1985) 788-793.
- F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, Amsterdam, 1977.
- C. Roos, *A new lower bound for the minimum distance of a cyclic codes*. IEEE Trans. Inform. Theory, **29** (3) (1983) 330-332.

To know more...

- C. Roos, *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*. J. Combinatorial Theory, Series A (1982) 229-232.
- R.E. Sabin, *On minimum distance bounds for Abelian Codes*. Applicable Algebra Eng. Commun. Comput. **3** (3) (1992) 183-197.
- S. Sakata, *Decoding binary cyclic 2-D codes by the 2-D Berlekamp-Massey algorithm*. IEEE Trans. Inform. Theory, **37** (4) (1991) 1200-1203.
- J.H. van Lint and R.M. Wilson, *On the minimum distance of cyclic codes*. IEEE Trans. Inform. Theory, **32** (1) (1986) 23-40.
- K.-C. Yamada, *Hypermatrix and its applications*. Hitotsubashi J. Arts Sciences **6** (1) (1965) 34-44.
- A. Zeh, T. Jerkovits, *Cyclic Codes*. Available online at http://www.boundtables.org.