Minimal weight codewords of affine cartesian codes

Victor Gonzalo Lopez Neumann
Faculdade de Matemática
Universidade Federal de Uberlândia
in joint work with Cícero Carvalho

CIMPA Research School
Algebraic Methods in Coding Theory
Ubatuba, July 13, 2017

Partially supported by FAPEMIG

Generalized Reed-Muller code

Reed-Muller codes appeared in 1954, defined by D.E. Muller, and were given a decoding algorithm by I.S. Reed. They are codes defined over $\mathbb{F}_2$. In 1968 Kasami, Lin and Peterson extended the original definition to $\mathbb{F}_q$, where q is any prime power. These codes are now called Generalized Reed-Muller codes.

Definition

Let $P_1, \ldots, P_{q^n}$ be the points of $\mathbb{F}_q^n$. For a nonnegative integer d write $\mathbb{F}_q[\boldsymbol{X}]_{\leq d}$ for the $\mathbb{F}_q$-vector space formed by the polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$ of degree up to d together with the zero polynomial. Define $\varphi_d : \mathbb{F}_q[\boldsymbol{X}]_{\leq d} \to \mathbb{F}_q^{q^n}$ as the evaluation morphism $\varphi_d(g) = (g(P_1), \ldots, g(P_{q^n}))$. The subspace $\mathrm{Im}\,\varphi_\mathrm{d}$ of $\mathbb{F}_q^{q^n}$ is called the Generalized Reed-Muller code of order d and length q^n, and is denoted by $\mathrm{GRM(n, d)}$.

Generalized Reed-Muller code

The dimension of $\mathrm{GRM(n,d)}$ is well known as well as its minimum distance $\delta(n,d)$.
For a polynomial $g \in \mathbb{F}_q[\boldsymbol{X}]_{\leq d}$ we may define the Hamming weight of its image $\varphi_d(g)$ as $w(\varphi_d(g)) = |\{P \in \mathbb{F}_q^n \mid g(P) \neq 0\}|$. Thus the minimum distance of $\mathrm{GRM(n,d)}$ is

$$\delta(n,d) = \min\left\{w(\varphi_d(g)) \mid g \in \mathbb{F}_q[\boldsymbol{X}]_{\leq d} \text{ and } w(\varphi_d(g)) \neq 0\right\}.$$

If $d \geq n(q-1)$ then $\mathrm{GRM(n,d)} = \mathbb{F}_{\mathrm{q}}^{\mathrm{q^n}}$ and $\delta(n,d) = 1$. To find the minimum distance for $1 \leq d \leq n(q-1)$ write d uniquely as $d = k(q-1) + \ell$ with $0 \leq k < n$, $0 < \ell \leq q-1$ and then $\delta(n,d) = (q-\ell)q^{n-k+1}$.

Generalized Reed-Muller code

In 1970 Delsarte, Goethals and Mac Williams proved a theorem on the generation of the minimal codewords. They proved that the polynomials whose evaluation produces codewords of minimal weight are a special product of degree one polynomials. They wrote “The authors hasten to point out that it would be very desirable to find a more sophisticated and shorter proof”.

In 2012 E. Leducq published a paper with a new and short proof of their theorem. She expounded some geometrical methods used by Delsarte et al. and replaced the codewords by functions.

Generalized Reed-Muller code

Delsarte, Goethals and Mac Williams' theorem on Leducq's paper reads as follows.

Theorem

The minimal weight codewords of $\mathrm{GRM(n,d)}$ *are equivalent, under the action of the affine group, to a codeword of the following form:*

$$\forall x \in \mathbb{F}_q^n, \quad f(x) = c\prod_{i=1}^{k}(x_i^{q-1} - 1)\prod_{j=1}^{s}(x_{k+1} - b_j)$$

where $c \in \mathbb{F}_q^*$ *and* b_j *are distinct elements of* $\mathbb{F}_q$*.*

Affine cartesian code

In 2014 H. López, C. Renteria-Marquez and R. Villarreal introduced a new class of codes which contain the GRM codes.
Let $K_1, \ldots, K_n$ be a collection of non-empty subsets of $\mathbb{F}_q$. Consider an *affine cartesian set*

$$\mathcal{X} := K_1 \times \cdots \times K_n := \{(\alpha_1 : \cdots : \alpha_n) |\, \alpha_i \in K_i \text{ for all } i\} \subset \mathbb{F}_q^n.$$

We denote by d_i the cardinality of K_i, for $i = 1, \ldots, n$. Clearly $|\mathcal{X}| = \Pi_{i=1}^n d_i =: \widetilde{m}$ and let $P_1, \ldots, P_{\widetilde{m}}$ be the points of $\mathcal{X}$.

Affine cartesian code

Define $\psi_d : \mathbb{F}_q[\boldsymbol{X}]_{\leq d} \to \mathbb{F}_q^{\widetilde{m}}$ as the evaluation morphism $\psi_d(g) = (g(P_1), \ldots, g(P_{\widetilde{m}}))$.

Definition

The image $\mathcal{C}_{\mathcal{X}}(d)$ of ψ_d is a vector subspace of $\mathbb{F}_q^{\widetilde{m}}$ called the *affine cartesian code* (of order d) defined over the sets $K_1, \ldots, K_n$.

In the special case where $K_1 = \cdots = K_n = \mathbb{F}_q$ we have the well-known generalized Reed-Muller code of order d. An affine cartesian code is a type of affine variety code, as defined by Fitzgerald (1998). In their work H. López, C. Rentería-Marquez and R. Villarreal proved that we may ignore, in the cartesian product, sets with just one element and moreover may always assume that $2 \leq d_1 \leq \cdots \leq d_n$.

Affine cartesian code

López et al. calculated the parameters of this code. In particular:

Theorem

The minimum distance $\delta_{\mathcal{X}}(d)$ *of* $\mathcal{C}_{\mathcal{X}}(d)$ *is 1, if* $d \geq \sum_{i=1}^{n}(d_i - 1)$*, and for* $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$ *we have*

$$\delta_{\mathcal{X}}(d) = (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$$

where k *and* ℓ *are uniquely defined by* $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ *with* $0 < \ell \leq d_{k+1} - 1$ *(if* $k + 1 = n$ *we understand that* $\prod_{i=k+2}^{n} d_i = 1$*, and if* $d \leq d_1 - 1$ *then we set* $k = 0$ *and* $\ell = d$*).*

Affine cartesian code

In a joint work with Cícero Carvalho we extend the result of Delsarte, Goethals and Mac Williams to affine cartesian codes, in the case where K_i is a field, for all $i = 1, \ldots, n$ and $K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{F}_q$.
To describe the codewords of minimum weight we take yet another approach to $\mathcal{C}_{\mathcal{X}}(d)$, already used by E. Leducq, which we describe now.

The approach via functions

Remember that $\mathcal{X} = \{P_1, \dots, P_{\widetilde{m}}\}$ and $\psi_d : \mathbb{F}_q[\boldsymbol{X}]_{\leq d} \to \mathbb{F}_q^{\widetilde{m}}$ is the evaluation morphism $\psi_d(g) = (g(P_1), \dots, g(P_{\widetilde{m}}))$.
We assume from now on that $K_1, \dots, K_n$ are fields and that $K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{F}_q$. In the case we have

$$\begin{aligned} I_{\mathcal{X}} &= \left\{ f \in \mathbb{F}_q[\boldsymbol{X}] \mid f(P) = 0, \forall P \in \mathcal{X} \right\} \\ &= \left\langle X_1^{d_1} - X_1, \dots, X_n^{d_n} - X_n \right\rangle. \end{aligned}$$

It is easy to see that $\ker \psi_d = \mathbb{F}_q[\boldsymbol{X}]_{\leq d} \cap I_{\mathcal{X}}$ and so $\mathcal{C}_{\mathcal{X}}(d) \cong (\mathbb{F}_q[\boldsymbol{X}]/I_{\mathcal{X}})_{\leq d}$.

The approach via functions

It is well known that, given a subset $Y \subset \mathbb{F}_q^n$, any function $f : Y \to \mathbb{F}_q$ is given by a polynomial $P \in \mathbb{F}_q[\boldsymbol{X}]$. Denoting by $C_{\mathcal{X}}$ the $\mathbb{F}_q$-algebra of functions defined on $\mathcal{X}$ we clearly have an isomorphism $\Phi : \mathbb{F}_q[\boldsymbol{X}]/I_{\mathcal{X}} \to C_{\mathcal{X}}$ hence for each function $f \in C_{\mathcal{X}}$ there exists a unique polynomial $P \in \mathbb{F}_q[\boldsymbol{X}]$ such that the degree of P in the variable X_i is less than d_i for all $i = 1, \ldots, n$, and $\Phi(P + I_{\mathcal{X}}) = f$.

Definition

We say that P is *the reduced polynomial associated to f* and we define the *degree of f* as being the degree of P.

The approach via functions

Definition

We denote by $C_{\mathcal{X}}(d)$ the $\mathbb{F}_q$-vector space formed by functions of degree up to d, together with the zero function. We saw above that $C_{\mathcal{X}}$ is isomorphic to $\mathbb{F}_q[\boldsymbol{X}]/I_{\mathcal{X}}$, and hence to $\mathbb{F}_q^{\widetilde{m}}$, and clearly $C_{\mathcal{X}}(d) \subset C_{\mathcal{X}}$ is isomorphic to the code $\mathcal{C}_{\mathcal{X}}(d) \subset \mathbb{F}_q^{\widetilde{m}}$, so from now on we also call $C_{\mathcal{X}}(d)$ the affine cartesian code of order d.

Definition

We define the support of a function $f \in C_{\mathcal{X}}$ as the set $\{P \in \mathcal{X} \mid f(P) \neq 0\}$ and we write $|f|$ for its cardinality, which, in this approach, is the Hamming weight of f. Thus the minimum distance of $C_{\mathcal{X}}(d)$ is $\delta_{\mathcal{X}}(d) := \min\{|f| \mid f \in C_{\mathcal{X}}(d) \text{ and } f \neq 0\}$.

The approach via functions

Definition

We denote by

$$Z_{\mathcal{X}}(f) := \{P \in \mathcal{X} \mid f(P) = 0\}$$

the set of zeros of $f \in C_{\mathcal{X}}$.

In this way $|f| = |\mathcal{X}| - |Z_{\mathcal{X}}(f)|$, which means that the minimum distance is closely related to the maximum number of points of intersection of $\mathcal{X}$ with a hypersurface of the affine space which does not contain $\mathcal{X}$.

The approach via functions

We write $\mathrm{Aff}(n, \mathbb{F}_q)$ for the affine group in $\mathbb{F}_q^n$, i.e. the transformations of $\mathbb{F}_q^n$ of the type $P \longmapsto AP + Q$, where $A \in GL(n, \mathbb{F}_q)$ and $Q \in \mathbb{F}_q^n$.

Definition

The affine group associated to $\mathcal{X}$ is

$$\mathrm{Aff}(\mathcal{X}) = \{\varphi : \mathcal{X} \to \mathcal{X} \mid \varphi = \psi_{|\mathcal{X}} \text{ with } \psi \in \mathrm{Aff}(n, \mathbb{F}_q) \text{ and } \psi(\mathcal{X}) = \mathcal{X}\}.$$

Definition

We say that $f, g \in C_{\mathcal{X}}$ are $\mathcal{X}$-equivalent if there exists $\varphi \in \mathrm{Aff}(\mathcal{X})$ such that $f = g \circ \varphi$.

In particular, if $f, g \in C_{\mathcal{X}}$ are $\mathcal{X}$-equivalent then $|f| = |g|$.

The approach via functions

Definition

An affine subspace $G \subset \mathbb{F}_q^n$ of dimension r is said to be $\mathcal{X}$-affine if there exists $\psi \in \mathrm{Aff}(n, \mathbb{F}_q)$ and $1 \leq i_1 < \cdots < i_r \leq n$ such that $\psi(\mathcal{X}) = \mathcal{X}$ and $\psi(\langle e_{i_1}, \ldots, e_{i_r} \rangle) = G$, where we write $\{e_1, \ldots, e_n\}$ for the canonical basis of $\mathbb{F}_q^n$. We denote by x_i the coordinate function $x_i(\sum_j a_j e_j) = a_i$ where $\sum_j a_j e_j \in \mathbb{F}_q^n$ (and by abuse of notation we also denote by x_i its restriction to $\mathcal{X}$) for all $i = 1, \ldots, n$.

The approach via functions

For $1 \leq j \leq n$, define

$$\mathcal{X}_{\hat{j}} = K_1 \times \cdots \times K_{j-1} \times K_{j+1} \times \cdots \times K_n$$

and $\delta_{\mathcal{X}_{\hat{j}}}(d)$ the corresponding minimum distance of $C_{\mathcal{X}_{\hat{j}}}(d)$.

Definition

For every $\alpha \in K_j$ we have an evaluation homomorphism of $\mathbb{F}_q$-algebras given by

$$\begin{array}{ccc} C_{\mathcal{X}} & \longrightarrow & C_{\mathcal{X}_{\hat{j}}} \\ f & \longmapsto & f(x_1, \ldots, x_{j-1}, \alpha, x_{j+1}, \ldots, , x_n) =: f_\alpha^{(j)} . \end{array}$$

First results

The central first result we use is the following

Proposition

Let $1 \leq d < \sum_{i=1}^{n}(d_i - 1)$ and write $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ as in Theorem 4. Let $S \subset \mathcal{X}$ be a nonempty set and assume that S has the following properties:

1. $|S| < \left(1 + \dfrac{1}{d_{k+1}}\right)\delta_{\mathcal{X}}(d) = \left(1 + \dfrac{1}{d_{k+1}}\right)(d_{k+1} - \ell)d_{k+2} \cdots d_n.$
2. *For every $\mathcal{X}$-affine subspace $G \subset \mathbb{F}_q^n$ of dimension r, with $r \in \{0, \ldots, n-1\}$, either $S \cap G = \emptyset$ or $|S \cap G| \geq \delta_{\mathcal{X}_G}(d)$.*

Then there exists an affine subspace $H \subset \mathbb{F}_q^n$, of dimension $n - 1$ and a transformation $\psi \in \mathit{Aff}(n, \mathbb{F}_q)$ such that $\psi(\mathcal{X}) = \mathcal{X}$, $\psi(V_{k+1}) = H$ where V_{k+1} is the $\mathbb{F}_q$-vector space generated by $\{e_1, \ldots, e_n\} \setminus \{e_{k+1}\}$ (so, in particular, H is $\mathcal{X}$-affine) and $S \cap H = \emptyset$.

First results

The last result gives a first step in the direction of the main result.

Corollary

Let f be a nonzero function in $C_{\mathcal{X}}(d)$ such that $|f| < \left(1 + \frac{1}{d_{k+1}}\right)\delta_{\mathcal{X}}(d)$, then f is a multiple of a function h of degree 1 which is $\mathcal{X}$-equivalent to x_{k+1}.

Lemma

Let f be a nonzero function in $C_{\mathcal{X}}(d)$, and let $h \in C_{\mathbf{X}}(d)$ be such that $h = x_j \circ \varphi$, where $j \in \{1, \ldots, n\}$ and $\varphi \in \mathit{Aff}(\mathbf{X})$. If m is the number of $\alpha \in K_j$ such that $Z_{\mathcal{X}}(h - \alpha) \subset Z_{\mathcal{X}}(f)$ then $m \leq d$ and $|f| \geq (d_j - m)\delta_{\mathcal{X}_{\hat{j}}}(d - m)$

First results

Proposition

Let $1 \leq d < d_1$*, the minimal weight codewords of* $C_{\mathcal{X}}(d)$ *are* $\mathcal{X}$*-equivalent to the functions*

$$g = \sigma \prod_{i=1}^{\ell} (x_1 - \alpha_i)\,,$$

with $\sigma \in \mathbb{F}_q^*$*,* $\alpha_i \in K_1$ *and* $\alpha_i \neq \alpha_j$ *for* $1 \leq i \neq j \leq \ell$*.*

Main result

Theorem

The minimal weight codewords of $C_{\mathcal{X}}(d)$, for $d = \sum_{i=1}^{k}(d_i - 1) + \ell$, $0 \leq k < n$ and $0 < \ell \leq d_{k+1} - 1$ are $\mathcal{X}$-equivalent to the functions

$$g = \sigma \prod_{i=1, i \neq j}^{k+1} (1 - x_i^{d_i - 1}) \prod_{t=1}^{d_j - (d_{k+1} - \ell)} (x_j - \alpha_t) \ ,$$

for some $1 \leq j \leq k+1$, where $d_{k+1} - \ell \leq d_j$, with $\sigma \in \mathbb{F}_q^*$, $\alpha_t \in K_j$ and $\alpha_t \neq \alpha_s$ for $1 \leq t \neq s \leq \ell$. If $d_j = d_{k+1} - \ell$, the last product is 1.