Projective Nested Cartesian Codes

Cícero Carvalho, Hiram H. López, V. G. Lopez Neumann*

Faculdade de Matemática, Universidade Federal de Uberlândia
Uberlândia - Minas Gerais, Brazil
victor.neumann@ufu.br

1. Introduction

Let $\mathbb{F}_q$ be a field with q elements and let $A_0, \ldots, A_n$ be a collection of non-empty subsets of $\mathbb{F}_q$. Consider a *projective cartesian set*

$$\mathcal{X} := [A_0 \times A_1 \times \cdots \times A_n] := \{(a_0 : \cdots : a_n) \ : \ a_i \in A_i \text{ for all } i\} \subset \mathbb{P}^n,$$

where $\mathbb{P}^n$ is a projective space over the field $\mathbb{F}_q$.
In what follows d_i denotes $|A_i|$, the cardinality of A_i for $i = 0, \ldots, n$.
Let $S := \mathbb{F}_q[X_0, \ldots, X_n]$ be a polynomial ring over the field $\mathbb{F}_q$, let $P_1, \ldots, P_m$ be the points of $\mathcal{X}$ written with the usual representation for projective points, that is, zeros to the left and the first nonzero entry equal 1, and let S_d be the $\mathbb{F}_q$-vector space of all homogeneous polynomials of S of degree d together with the zero polynomial. The *evaluation map*

$$\varphi_d \colon S_d \longrightarrow \mathbb{F}_q^{|\mathcal{X}|}, \qquad f \mapsto (f(P_1), \ldots, f(P_m)),$$

defines a linear map of $\mathbb{F}_q$-vector spaces. The image of φ_d, denoted by $C_{\mathcal{X}}(d)$, defines a linear code (as usual by a *linear code* we mean a linear subspace of $\mathbb{F}_q^{|\mathcal{X}|}$). We call $C_{\mathcal{X}}(d)$ a *projective cartesian code* of order d defined over $A_0, \ldots, A_n$.
The *dimension* and the *length* of $C_{\mathcal{X}}(d)$ are given by $\dim_{\mathbb{F}_q} C_{\mathcal{X}}(d)$ (dimension as $\mathbb{F}_q$-vector space) and $|\mathcal{X}|$ respectively. The *minimum distance* of $C_{\mathcal{X}}(d)$ is given by

$$\delta_{\mathcal{X}}(d) = \min\{|\varphi_d(f)| \ : \ \varphi_d(f) \neq 0; f \in S_d\},$$

where $|\varphi_d(f)|$ is the number of non-zero entries of $\varphi_d(f)$. These are the main parameters of the code $C_{\mathcal{X}}(d)$ and they are presented in the main results of this work, although we find the minimum distance only when the $A_i's$ satisfy certain conditions (Definition 2.1).
We compute the length and the dimension of $C_{\mathcal{X}}(d)$ using some concepts of commutative algebra which we now recall. The *vanishing ideal* of $\mathcal{X} \subset \mathbb{P}^n$, denoted by $I(\mathcal{X})$, is the ideal of S generated by the homogeneous polynomials that vanish on all points of $\mathcal{X}$. We are interested in the algebraic invariants (degree, Hilbert function) of $I(\mathcal{X})$, because the kernel of the evaluation map, φ_d, is precisely $I(\mathcal{X})_d$, where $I(\mathcal{X})_d := S_d \cap I(\mathcal{X})$.
In general, for any subset (ideal or not) $\mathcal{F}$ of S we define $\mathcal{F}_d := \mathcal{F} \cap S_d$. The *Hilbert function* of $S/I(\mathcal{X})$ is given by

$$H_{\mathcal{X}}(d) := \dim_{\mathbb{F}_q}(S_d/I(\mathcal{X})_d),$$

so $H_{\mathcal{X}}(d)$ is precisely the dimension of $C_{\mathcal{X}}(d)$. According to J. Harris, we have that $H_{\mathcal{X}}(d) = |\mathcal{X}|$ for $d \geq |\mathcal{X}| - 1$, which means that the length $|\mathcal{X}|$ of $C_{\mathcal{X}}(d)$ is the *degree* of $S/I(\mathcal{X})$ in the sense of algebraic geometry.
Set $\mathcal{Y} := A_1 \times \cdots \times A_n \subset \mathbb{A}^n$, where $\mathbb{A}^n$ is the n-dimensional affine space defined over $\mathbb{F}_q$. For a nonnegative integer d write $S_{\leq d}$ for the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ formed by the polynomials in $\mathbb{F}_q[X]$ of degree up to d together with the zero polynomial. Clearly $|\mathcal{Y}| = \Pi_{i=1}^n d_i =: \tilde{m}$ and let $Q_1, \ldots, Q_{\tilde{m}}$ be the points of $\mathcal{Y}$. Define

$$\phi_d : S_{\leq d} \to \mathbb{F}_q^{\tilde{m}}, \qquad g \mapsto (g(Q)_1), \ldots, g(Q_{\tilde{m}})),$$

The image $C^*_{\mathcal{Y}}(d)$ of ϕ_d is a subvector space of $\mathbb{F}_q^{\tilde{m}}$ called the *affine cartesian code* (of order d) defined over the sets $A_1, \ldots, A_n$. These codes were introduced in [6], and also appeared independently and in a generalized form in [4]. They are a type of affine variety code, as defined in [3]. Define $\bar{\mathcal{Y}} := [1 \times A_1 \times \cdots \times A_n]$ (it may be viewed as the closure of $\mathcal{Y}$ in $\mathbb{P}^n$).

Theorem 1.1 *[6, Thm. 2.5]* $I(\bar{\mathcal{Y}}) = \langle \Pi_{a_1 \in A_1}(X_1 - a_1 X_0), \ldots, \Pi_{a_n \in A_n}(X_n - a_n X_0) \rangle$

Theorem 1.2 *[6, Thm. 3.1 and Thm. 3.8]*
1) The dimension of $C^*_{\mathcal{Y}}(d)$ is $\tilde{m}$ (i.e. ϕ_d is surjective) if $d \geq \sum_{i=1}^n (d_1 - 1)$, and for $0 \leq d < \sum_{i=1}^n (d_1 - 1)$ we have

$$\dim_{\mathbb{F}_q}(C^*_{\mathcal{Y}}(d)) = \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-d_i}{d-d_i} + \cdots +$$
$$(-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \binom{n+d-d_{i_1} - \cdots - d_{i_j}}{d-d_{i_1} - \cdots - d_{i_j}} + \cdots + (-1)^n \binom{n+d-d_1 - \cdots - d_n}{d-d_1 - \cdots - d_n}$$

where we set $\binom{a}{b} = 0$ if $b < 0$.
2) The minimum distance $\delta^*_{\mathcal{Y}}(d)$ of $C^*_{\mathcal{Y}}(d)$ 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

$$\delta^*_{\mathcal{Y}}(d) = (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$$

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

2. Length and dimension

For A, B subsets of $\mathbb{F}_q$ we write we define $\frac{A}{B} := \left\{\frac{a}{b} \ : \ a \in A, b \in B^{\neq 0}\right\}$.

Definition 2.1 Let $A_0, A_1, \ldots, A_n$ be a collection of non-empty subsets of $\mathbb{F}_q$ such that
(i) for all $i = 0, \ldots, n$ we have $0 \in A_i$,
(ii) for every $i = 1, \ldots, n$ we have $\frac{A_j}{A_{i-1}} \subset A_j$ for $j = i, \ldots, n$.
Under these conditions, the projective cartesian set $\mathcal{X} = [A_0 \times A_1 \times \cdots \times A_n]$ is called *projective nested cartesian set*. For any $d \geq 0$, $C_{\mathcal{X}}(d)$ is called a *projective nested cartesian code*.

Remark 2.2 *Projective Reed-Muller codes are projective nested cartesian codes.*

Lemma 2.3 *If $\mathcal{X} = [A_0 \times A_1 \times A_2 \times \cdots \times A_n]$ is a projective nested cartesian set then*

$$I(\mathcal{X}) = \left\langle X_i \prod_{a_j \in A_j} \left(X_j - a_j X_i\right) \ : \ i < j, i, j = 0, \ldots, n \right\rangle.$$

Definition 2.4 *Let $\mathcal{X} = [A_0 \times \cdots \times A_n]$ be a projective nested cartesian set. To compute the Hilbert function of $I(\mathcal{X})$ we define*

$$\mathcal{X}_i := [A_{n-i} \times \cdots \times A_n], \text{ and } I(\mathcal{X}_i) \subset \mathbb{F}_q[X_{n-i}, \ldots, X_n], \text{ for } i = 0, \ldots, n;$$
$$\mathcal{X}_i^* := [1 \times A_{n+1-i} \times \cdots \times A_n], \text{ and } I(\mathcal{X}_i^*) \subset \mathbb{F}_q[X_{n-i}, \ldots, X_n], \text{ for } i = 1, \ldots, n.$$

Lemma 2.5 *For any positive integer d, $H_{\mathcal{X}_n}(d) = H_{\mathcal{X}_{n-1}}(d) + H_{\mathcal{X}_n^*}(d-1)$.*

Theorem 2.6 *Let $C_{\mathcal{X}}(d)$ be a projective nested cartesian code over $A_0, \ldots, A_n$. The length of the code is given by $m = 1 + \sum_{i=1}^n d_i \cdots d_n$ and its dimension by*

$$\dim_{\mathbb{F}_q} C_{\mathcal{X}}(d) = 1 + \sum_{j=1}^{n} \left[\binom{j+d-1}{d-1} - \sum_{i=n+1-j}^{n} \binom{j+d-1-d_i}{d-1-d_i} + \cdots + \right.$$
$$(-1)^k \sum_{n+1-j \leq i_1 < \cdots < i_k \leq n} \binom{j+d-1-(d_{i_1} + \cdots + d_{i_k})}{d-1-(d_{i_1} + \cdots + d_{i_k})} + \cdots +$$
$$\left. (-1)^j \binom{j+d-1-(d_{n+1-j} + \cdots + d_n)}{d-1-(d_{n+1-j} + \cdots + d_n)} \right].$$

Let $\prec$ be the graded lexicographic monomial order $\prec$ in S, where $X_0 \prec \cdots \prec X_n$.

Proposition 2.7 *Let $\mathcal{X} = [A_0 \times \cdots \times A_n]$ be a projective nested cartesian set. The set $\mathcal{G} = \left\{X_i \prod_{a_j \in A_j} \left(X_j - a_j X_i\right) \ : \ i < j, i, j = 0, \ldots, n\right\}$ is a Gröbner basis for $I(\mathcal{X})$.*

3. Minimum Distance

Lemma 3.1 *If $\mathcal{X}$ is the projective nested cartesian set over $A_0, \ldots, A_n$, then the minimum distance of $C_{\mathcal{X}}(d)$ satisfies $\delta_{\mathcal{X}}(d) \leq (d_{k+1} - \ell)\, d_{k+2} \cdots d_n$ if $1 \leq d \leq \sum_{i=1}^n (d_i - 1)$, and $\delta_{\mathcal{X}}(d) = 1$ in otherwise, where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that $d - 1 = \sum_{i=1}^k (d_i - 1) + \ell$.*

Let $K_0 \subset \cdots \subset K_n$ be subfields of $\mathbb{F}_q$. Then $\mathcal{X} = [K_0 \times \cdots \times K_n]$ is a projective nested cartesian set which is called a *projective nested product of fields*.
Let $g \in S$ a polynomial of degree d not necessarily homogeneous. We say that g is *homogeneous on $\mathcal{X}$*, and we write $g \in \widetilde{S}_d$, if for every $i \in \{0, \ldots, n\}$ and every $x = (0 : \cdots : 0 : 1 : x_{i+1} : \cdots : x_n) \in \mathcal{X}$ we have that for any given $c \in A_i^{\neq 0}$ there exists $\tilde{c} \in A_i^{\neq 0}$ such that

$$g(0, \ldots, 0, c, cx_{i+1}, \ldots, cx_n) = \tilde{c} g(0, \ldots, 0, 1, x_{i+1}, \ldots, x_n).$$

For a set $\mathcal{A} \subset \mathcal{X}$ and $f \in \widetilde{S}_d \backslash I(\mathcal{A})$, define $Z_{\mathcal{A}}(f) := \{P \in \mathcal{A} \ : \ f(P) = 0\}$. In this way, for a codeword $v = (f(P_1), \ldots, f(P_m)) \neq 0$, where $f(X) \in S_d \backslash I(\mathcal{X})_d$, the weight of v is $|\mathcal{X} \backslash Z_{\mathcal{X}}(f)|$, and the minimum distance of $C_{\mathcal{X}}(d)$ is $\delta_{\mathcal{X}}(d) = \min\{|\mathcal{X} \backslash Z_{\mathcal{X}}(f)| \ : \ f \in S_d \backslash I(\mathcal{X})_d\}$.

Lemma 3.2 *Let f be an element of $\widetilde{S}_d$ such that for all $t \leq j \leq n$ we have $Z_{\mathcal{X}}(X_j) \subset Z_{\mathcal{X}}(f)$. Then there exists $g_t(X)$ in $\widetilde{S}_{d-(n-t+1)}$ such that $f - g_t \cdot X_t \cdots X_n \in I(\mathcal{X})$.*

Proposition 3.3 *Let $\mathcal{X}$ be the projective nested product of fields over $K_0, \ldots, K_n$, and let $f \notin I(\mathcal{X})$ be a not necessarily homogeneous polynomial on S of degree at most d and homogeneous on $\mathcal{X}$. If $1 \leq d < \sum_{i=1}^n (d_i - 1)$, then $|\mathcal{X} \backslash Z_{\mathcal{X}}(f)| \geq (d_{k+1} - \ell)\, d_{k+2} \cdots d_n$ where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are the unique integers such that $d - 1 = \sum_{i=1}^k (d_i - 1) + \ell$.*

Theorem 3.4 *If $\mathcal{X}$ is the projective nested product of fields over $K_0, \ldots, K_n$, then the minimum distance of $C_{\mathcal{X}}(d)$ is given by*

$$\delta_{\mathcal{X}}(d) = \begin{cases} (d_{k+1} - \ell)\, d_{k+2} \cdots d_n & \text{if} \quad 1 \leq d \leq \sum_{i=1}^n (d_i - 1), \\ 1 & \text{if} \quad \sum_{i=1}^n (d_i - 1) < d, \end{cases}$$

where $0 \leq k \leq n-1$ and $0 \leq \ell < d_{k+1} - 1$ are integers such that $d - 1 = \sum_{i=1}^k (d_i - 1) + \ell$.

Corollary 3.5 *Let $K_0, \ldots, K_n$ be subfields of $\mathbb{F}_q$ such that $\mathcal{X} = [K_0 \times K_1 \times \cdots \times K_n]$ is a projective nested product of fields and let $\mathcal{X}_i^* = K_{n+1-i} \times \cdots \times K_n \subset \mathbb{A}^i$, where $i = 1 \ldots, n$. Set $\mathcal{X}_0^* = \{1\}$ If $C_{\mathcal{X}}(d)$ is a $[|\mathcal{X}|, \dim C_{\mathcal{X}}(d), \delta_{\mathcal{X}}(d)]$-code and $C_{\mathcal{X}_i^*}(d)$ is a $\left[\left|\mathcal{X}_i^*\right|, \dim C_{\mathcal{X}_i^*}(d), \delta_{\mathcal{X}_i^*}(d)\right]$-code, then*

$$|\mathcal{X}| = \sum_{i=0}^{n} |\mathcal{X}_i^*|, \qquad \dim C_{\mathcal{X}}(d) = \sum_{i=0}^{n} \dim C_{\mathcal{X}_i^*}(d-1) \qquad \text{and} \qquad \delta_{\mathcal{X}}(d) = \delta_{\mathcal{X}_n^*}(d-1),$$

where $\mathcal{X}_0^* = [1]$ and $\delta_{\mathcal{X}_n^*}(0) := d_1 \cdots d_n$.

Example 3.6 *Let $\mathbb{F}_{25}$ be a finite field with 25 elements and let $K_0 = K_1 = \mathbb{F}_5, K_2 = \mathbb{F}_{25}$ be subsets of $\mathbb{F}_{25}$. Then $\mathcal{X} = [K_0 \times K_1 \times K_2]$ is a projective nested cartesian product, and the length, the dimension and the minimum distance of the code $C_{\mathcal{X}}(d)$ are:*

d	1	2	3	4	5	6	7	8	9	10	25
$\lvert\mathcal{X}\rvert$	151	151	151	151	151	151	151	151	151	151	151
$\dim C_{\mathcal{X}}(d)$	3	6	10	15	21	27	33	39	45	51	141
$\delta_{\mathcal{X}}(d)$	125	100	75	50	25	24	23	22	21	20	5

References

[1] C. Carvalho, On the second Hamming weight of some Reed-Muller type codes, Finite Fields Appl. **24** (2013) 88–94.
[2] S. Ballet, R. Rolland, On low weight codewords of generalized affine and projective Reed-Muller codes, Des. Codes Cryptogr. **73**(2) (2014) 271–297.
[3] J. Fitzgerald, R.F. Lax, Decoding affine variety codes using Göbner bases, Des. Codes and Cryptogr. **13**(2) (1998) 147–158.
[4] O. Geil, C. Thomsen, Weighted Reed-Muller codes revisited, Des. Codes Cryptogr. **66**(1–3) (2013) 195–220.
[5] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. **81**(2) (1990) 217–221.
[6] H. H. López, C. Rentería-Márquez, R. H. Villarreal, Affine cartesian codes, Des. Codes Cryptogr. **71**(1) (2014) 5–19.
[7] C. Rentería, Tapia-Recillas H., Reed-Muller codes: an ideal theory approach, Commu. Algebra **25**(2) (1997) 401–413.
[8] A. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inform. Theory **37**(6) (1991) 1567–1576.

Poster. XXI Coloquio Latinoamericano de Álgebra, Buenos Aires, Argentina, July 25 – 29, 2016.

Partially supported by FAPEMIG - Brazil