Affine Cartesian codes with complementary duals

Hiram H. López[*], Felice Manganiello, and Gretchen L. Matthew[†]

Clemson University

Virginia Tech

Abstract

A linear code C with the property that $C \cap C^{\perp} = \{0\}$ is said to be a linear complementary dual, or LCD, code. In this paper, we consider generalized affine Cartesian codes which are LCD. Generalized affine Cartesian codes arise naturally as the duals of affine Cartesian codes in the same way that generalized Reed-Solomon codes arise as duals of Reed-Solomon codes. Generalized affine Cartesian codes are evaluation codes constructed by evaluating multivariate polynomials of bounded degree at points in an m-dimensional Cartesian set over a finite field K and scaling the coordinates. The LCD property depends on the scalars used. Because Reed-Solomon codes are a special case, we obtain a characterization of those generalized Reed-Solomon codes which are LCD along with the more general result for generalized affine Cartesian codes. These results are independent of the characteristic of the underlying field.

Keywords: generalized affine Cartesian codes; evaluation codes; dual codes; linear complementary dual (LCD) codes; Extended Euclidean algorithm.
MSC2010 classification codes: 11T71; 94B27; 14G50

1 Introduction

In this paper, we consider linear codes which are linear complementary dual (LCD), a property introduced by Massey in 1992 [**?**]. An LCD code is a linear code that has only the zero word in common with its dual. Recall that a linear code C is a K-subspace of K^n, where K is a finite field. Given such a code C, its dual is $C^{\perp} := \{w \in K : w \cdot c = 0 \ \forall c \in C\}$. Hence, if $C \subseteq K^n$ is LCD, then $C \cap C^{\perp} = \{0\}$ and $C \oplus C^{\perp} = K^n$; of course, if K is not finite and instead has characteristic 0, then this naturally holds.

[*]The first author was partially supported by CONACyT, CVU No. 268999 project "Network Codes", and Universidad Autónoma de Aguascalientes.

[†]The second and third authors were partially supported by the National Science Foundation under grant DMS-1547399.

In 2015, Carlet and Guilley [?] demonstrated how LCD codes provide countermeasures to side-channel attack (SCA) and fault-injection attack. They use the observation (made by Massey) that a generator matrix G of an LCD code C has the property that GG^T is nonsingular; certainly, the same holds for a parity-check matrix H of an LCD code C, meaning HH^T is nonsingular. Suppose that data $x \in K^n$ is masked as $z := x + e$ where $e \in K^n$. Since $C \oplus C^\perp = K^n$, there exists $(x', y) \in K^k \times K^{n-k}$ with

$$z = x'G + yH.$$

Then

$$zG^T(GG^T)^{-1} = x'GG^T(GG^T)^{-1} + \underbrace{yHG^T(GG^T)^{-1}}_{0} = x'$$

and

$$zH^T(HH^T)^{-1} = \underbrace{x'GH^T(HH^T)^{-1}}_{0} + yHH^T(HH^T)^{-1} = y.$$

According to Carlet and Guilley, the countermeasure is $(d-1)^{th}$ degree secure where d is the minimum distance of C, and the greater the degree of the countermeasure, the harder it is to pass a successful SCA. To consider a fault injection attack, suppose z is modified into $z + \epsilon$ where $\epsilon \in K^n$. Then $\epsilon = eG + fH$ for some $(e, f) \in K^k \times K^{n-k}$. Detection amounts to distinguishing z from $z + \epsilon$. We have that

$$z + \epsilon = (x' + e)G + (y + f)H.$$

Then

$$(z + \epsilon)H^T(HH^T)^{-1} = (x' + e)GH^T(HH^T)^{-1} + (y + f)HH^T(HH^T)^{-1} = y + f.$$

Notice that $z + \epsilon = y$ if and only if $f = 0$ if and only if $\epsilon \in C$. Thus, fault is not detected if $\epsilon \in C$. If $wt(\epsilon) < d$, where d is the minimum distance of C, then fault is detected. Both of these applications motivate the need for LCD codes C with large minimum distance.

Recently, it was shown that every linear code over $\mathbb{F}_q$ with $q > 3$ is equivalent to an LCD code, as demonstrated by Carlet, Mesnager, Tang, Qi, and Pellikaan [?]. However, explicit constructions of LCD codes remain elusive. There have been results on the characterizations of LCD codes from particular families. Among them, there are some results for algebraic geometry codes, a particular family of evaluation code [?], cyclic codes [?], quasi-cyclic codes [?], and generalized Reed-Solomon codes [?].

In this paper, we consider LCD codes which are a special type of evaluation code, called a generalized affine Cartesian code. Generalized Reed-Solomon codes are a special case. Our results on generalized Reed-Solomon codes differ from those in [?, ?] in that we provide a characterization of which generalized Reed-Solomon codes are LCD and give explicit constructions, as opposed to determining the existence of such codes with a particular set of parameters; our results apply to codes over fields of any characteristic and also include cartesian codes which are not generalized Reed-Solomon codes.

A generalized affine Cartesian code is defined as follows. Let $K := \mathbb{F}_q$ be a finite field with q elements, and let $A_1, \ldots, A_m$ be non-empty subsets of K. Set $K^* := K \setminus \{0\}$. Define the *Cartesian product set*

$$\mathcal{A} := A_1 \times \cdots \times A_m \subseteq K^m.$$

Let $S := K[X_1, \ldots, X_m]$ be a polynomial ring, let $\boldsymbol{a_1}, \ldots, \boldsymbol{a_n}$ be the points of $\mathcal{A}$, and let $S_{<k}$ be the K-vector space of all polynomials of S of degree less than k, where k is a non-negative integer. Fix $v_1, \ldots, v_n \in K^*$, and set $\boldsymbol{v} = (v_1, \ldots, v_n)$. The *evaluation map*

$$\begin{array}{rlcl} \mathrm{ev}_k\colon & S_{<k} & \to & K^{|\mathcal{A}|} \\ & f & \mapsto & (v_1 f(\boldsymbol{a_1}), \ldots, v_n f(\boldsymbol{a_n})) \end{array}$$

defines a linear map of K-vector spaces. The image of ev_k, denoted by $C_k(\mathcal{A}, \boldsymbol{v})$, defines a linear code, called the *generalized affine Cartesian evaluation code* (*Cartesian code* for short) of degree k associated to $\mathcal{A}$ and $\boldsymbol{v}$. The *dimension* and the *length* of $C_k(\mathcal{A}, \boldsymbol{v})$ are given by $\dim_K C_k(\mathcal{A}, \boldsymbol{v})$ (dimension as K-vector space) and $|\mathcal{A}|$, respectively. The *minimum distance* of $C_k(\mathcal{A}, \boldsymbol{v})$ is given by

$$d(C_k(\mathcal{A}, \boldsymbol{v})) := \min\{\|\mathrm{ev}_k(f)\|\colon \mathrm{ev}_k(f) \neq 0; f \in S_{\leq k}\},$$

where $\|\mathrm{ev}_k(f)\|$ is the number of non-zero entries of $\mathrm{ev}_k(f)$. Generalized affine Cartesian codes arise naturally as duals of affine Cartesian codes; this is seen in the computation by Beelen and Datta [?], though the codes are not mentioned by name. In this paper, we investigate them more fully.

Cartesian codes are special types of affine Reed-Muller codes in the sense of [?, p. 37] and a type of affine variety codes, which were defined in [?]. Cartesian codes are a generalization of q-ary Reed-Muller codes, which are Cartesian codes with $A_1 = \ldots = A_m = K$.

Cartesian codes have been studied in different works when $\boldsymbol{v} = \mathbf{1}$, the vector of ones: they appeared first time in [?] and then independently in [?]. In [?], the authors study the basic parameters of Cartesian codes, they determine optimal weights for the case when $\mathcal{A}$ is the product of two sets, and then present two list decoding algorithms. In [?] the authors study the vanishing ideal $I(\mathcal{A})$ and then, using commutative algebra tools, for instance regularity, degree, Hilbert function, the authors determine the basic parameters of Cartesian codes in terms of the sizes of the components of the Cartesian set. In [?], the author shows some results on higher Hamming weights of Cartesian codes and gives a different proof for the minimum distance using the concepts of Gröbner basis and footprint of an ideal. In [?] the authors find several values for the second least weight of codewords, also known as the next-to-minimal Hamming weight. In [?] the authors find the generalized Hamming weights and the dual of Cartesian codes.

This paper is organized as follows. Section **??** details properties of generalized affine Cartesian codes, hereafter referred to as Cartesian codes. In Section **??**, we provide a characterization of Cartesian codes which are LCD. Examples are found in Section **??**, and our results are summarized in Section **??**.

For all unexplained terminology and additional information, we refer to [?, ?, ?] for commutative algebra and the theory of Hilbert functions, [?, ?] for the theory of linear codes, and [?, ?, ?, ?, ?, ?, ?] for other families of evaluation codes, including several variations of Reed-Muller codes and projective versions of the Cartesian codes.

2 Properties of generalized affine Cartesian codes

In what follows, $n_i := |A_i|$, the cardinality of A_i for $i = 1, \dots, m$. An important characteristic for Cartesian codes and evaluation codes in general is the fact that we can use commutative algebra methods to study them. The reason is because the kernel of the evaluation map ev_k, is precisely $S_{<k} \cap I(\mathcal{A})$, where $I(\mathcal{A})$ is the *vanishing ideal* of $\mathcal{A}$ consisting of all polynomials of S that vanish on $\mathcal{A}$. Thus, the algebra of $S/\left(S_{<k} \cap I(\mathcal{A})\right)$ is related to the basic parameters of $C_k(\mathcal{A}, \boldsymbol{v})$. Observe the kernel of the evaluation map ev_k is independent of $\boldsymbol{v}$ because every entry of $\boldsymbol{v}$ is non-zero. In fact, the vanishing ideal of $\mathcal{A} = A_1 \times \cdots \times A_m$ is given by $I(\mathcal{A}) = \left(\prod_{a_1 \in A_1}(X_1 - a_1), \dots, \prod_{a_m \in A_m}(X_m - a_m)\right)$ [?, Lemma 2.3].

A *monomial matrix* is a square matrix with exactly one nonzero entry in each row and column. A monomial matrix M can be written either in the form DP or the form PD, where D is a diagonal matrix with nonzero entries on the diagonal and P is a permutation matrix. Let C_1 and C_2 be codes of the same length over the field K, and let G_1 be a generator matrix for C_1. Then C_1 and C_2 are monomially equivalent provided there is a monomial matrix M over the same field K so that $G_1 M$ is a generator matrix of C_2. Monomially equivalent codes have the same length, dimension and minimum distance. For more properties of monomially equivalent codes, see [?] and references there.

Using properties of monomially equivalent codes along with [?, Theorems 3.1 and 3.8], we have the following result.

Theorem 2.1. *Let $C_k(\mathcal{A}, \boldsymbol{v})$ be a Cartesian code.*

1. *The length of $C_k(\mathcal{A}, \boldsymbol{v})$ is $n = n_1 \cdots n_m$.*

2. *The dimension of $C_k(\mathcal{A}, \boldsymbol{v})$ is $n_1 \cdots n_m$ (i.e. ev_k is surjective) if $k - 1 \geq \sum_{i=1}^{m}(n_i - 1)$, and*

$$\dim(C_k(\mathcal{A}, \boldsymbol{v})) = \sum_{j=0}^{m} (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq m} \binom{m + k - n_{i_1} - \cdots - n_{i_j}}{k - n_{i_1} - \cdots - n_{i_j}}$$

   otherwise.

3. *The minimum distance of $C_k(\mathcal{A}, \boldsymbol{v})$ is 1 if $k - 1 \geq \sum_{i=1}^{m}(n_i - 1)$, and for $0 \leq k - 1 < \sum_{i=1}^{m}(n_i - 1)$ we have*

$$d(C_k(\mathcal{A}, \boldsymbol{v})) = (n_{s+1} - \ell) \prod_{i=s+2}^{m} n_i,$$

   where s and ℓ are uniquely defined by $k - 1 = \sum_{i=1}^{s}(n_i - 1) + \ell$ with $0 \leq \ell < n_{s+1} - 1$ (if $s + 1 = m$ we understand that $\prod_{i=s+2}^{m} n_i = 1$, and if $k - 1 < n_1 - 1$ then we set $s = 0$ and $\ell = k$).

In light of Theorem **??**, from now on we assume that $k-1<\sum_{i=1}^{m}(n_i-1)$.

The rest of this section is devoted to proving that the dual of the Cartesian code $C_k(\mathcal{A},\boldsymbol{v})$ is $C_{k'}(\mathcal{A},\boldsymbol{v'})$, where $k':=\sum_{i=1}^{m}(n_i-1)-k+1$ and $\boldsymbol{v'}$ is as described below. The dual of the Cartesian code $C_k(\mathcal{A},\mathbf{1})$, the case when $\boldsymbol{v}$ is the vector of ones, was previously found in [**?**].

Given a positive integer ℓ, we define $[\ell]:=\{1,\ldots,\ell\}$. Let $\prec$ be the *graded-lexicographic order* on the set of monomials of S. This order is defined in the following way: $X_1^{t_1}\cdots X_m^{t_m}\prec X_1^{s_1}\cdots X_m^{s_m}$ if and only if $\sum_{i=1}^{m}t_i<\sum_{i=1}^{m}s_i$ or $\sum_{i=1}^{m}t_i=\sum_{i=1}^{m}s_i$ and the leftmost nonzero entry in $(s_1-t_1,\ldots,s_m-t_m)$ is positive. From now on we fix the order $\prec$. Denote the variables $X_1,\ldots,X_m$ by $\boldsymbol{X}$. For each $i\in[m]$, define the polynomial

$$L_i(X_i):=\prod_{a_i\in A_i}(X_i-a_i)\,. \tag{2.1}$$

Then, according to [**?**, Lemma 2.3], and [**?**, Proposition 4], $\{L_1(X_1),\ldots,L_m(X_m)\}$ is a Gröbner basis of $I(\mathcal{A})$.

Notice that for evaluation purposes we can assume that $\deg_{X_i}(f(\boldsymbol{X}))<n_i$, for $i\in[m]$, meaning

$$C_k(\mathcal{A},\boldsymbol{v})=\left\{\mathrm{ev}_k(f(\boldsymbol{X}))\colon f(\boldsymbol{X})\in S_{<k},\deg_{X_i}(f(\boldsymbol{X}))<n_i \text{ for } i\in[m]\right\}.$$

Indeed, if $c\in C_k(\mathcal{A},\boldsymbol{v})$, then there exists $f(\boldsymbol{X})\in S_{<k}$ such that $\mathrm{ev}_k(f(\boldsymbol{X}))=c$. By the division algorithm in S [**?**, Theorem 1.5.9], there are $f_1(\boldsymbol{X}),\ldots,f_m(\boldsymbol{X}),r(\boldsymbol{X})\in S$ such that

$$f(\boldsymbol{X})=\sum_{i=1}^{m}f_i(\boldsymbol{X})L_i(\boldsymbol{X})+r(\boldsymbol{X}),$$

where $\deg_{X_i}(r(\boldsymbol{X}))<n_i$ for $i=1,\ldots,m$, and $\deg(r(\boldsymbol{X}))\le\deg(f(\boldsymbol{X}))<k$. Then $\mathrm{ev}_k(f(\boldsymbol{X}))=\mathrm{ev}_k(r(\boldsymbol{X}))$ and $C_k(\mathcal{A},\boldsymbol{v})\subseteq\left\{\mathrm{ev}(f(\boldsymbol{X}))\colon f(\boldsymbol{X})\in S_{<k},\deg_{X_i}(f(\boldsymbol{X}))<n_i \text{ for } i\in[m]\right\}$. Given this, moving forward, we make the assumption that $\deg_{X_i}(f(\boldsymbol{X}))<n_i$.

Next we point out that the map ev_k is injective when $\deg_{X_i}(f)<n_i$ for $i\in[m]$. It is easy to see that $f(\boldsymbol{a})=g(\boldsymbol{a})$ for all $\boldsymbol{a}\in\mathcal{A}$ implies $(f-g)(\boldsymbol{X})\in I(\mathcal{A})$. However, $\deg_{X_i}(f)<n_i$ and $\deg_{X_i}(g)<n_i$ for $i\in[m]$ force $\deg_{X_i}(f-g)<n_i$ for $i\in[m]$. As a result, $(f-g)(\boldsymbol{X})=0$ meaning $f(\boldsymbol{X})=g(\boldsymbol{X})$.

For each element $\boldsymbol{a}=(a_1,\ldots,a_m)\in\mathcal{A}$, define the polynomial

$$L_{\boldsymbol{a}}(\boldsymbol{X}):=\frac{L_1(X_1)}{(X_1-a_1)}\cdots\frac{L_m(X_m)}{(X_m-a_m)}\in S. \tag{2.2}$$

For $\boldsymbol{b}=(b_1,\ldots,b_m)$, it is straightforward to check that $L_{\boldsymbol{a}}(\boldsymbol{b})=0$ if and only if $\boldsymbol{a}\ne\boldsymbol{b}$. In addition, $L_{\boldsymbol{a}}(\boldsymbol{a})=L_1'(a_1)\cdots L_m'(a_m)$, where $L_i'(X_i)$ denotes the formal derivative of $L_i(X_i)$. Writing $L_{\boldsymbol{a}}(\boldsymbol{a})$ in terms of the derivatives is convenient at times for computational purposes.

Given $c=(c_{\boldsymbol{a_1}},\ldots,c_{\boldsymbol{a_n}})\in C_k(\mathcal{A},\boldsymbol{v})$, there exists a polynomial $f(\boldsymbol{X})$ in $S_{<k}$ such that $\mathrm{ev}_k(f(\boldsymbol{X}))=c$ and $\deg_{X_i}(f(\boldsymbol{X}))<n_i$ for $i\in[m]$. Define the polynomial

$$f_c(\boldsymbol{X}):=\sum_{\boldsymbol{a}\in\mathcal{A}}\frac{L_{\boldsymbol{a}}(\boldsymbol{X})}{L_{\boldsymbol{a}}(\boldsymbol{a})}c_{\boldsymbol{a}}.$$

Then $f_c(\boldsymbol{a_i}) = c_{\boldsymbol{a_i}}$ and $\mathrm{ev}_k(f_c) = c$. By definition of $L_{\boldsymbol{a}}$, we have $\deg_{X_i}(f_c(\boldsymbol{X})) < n_i$ for $i \in [m]$. Based on the injectivity of ev_k, when we restrict to polynomials with $\deg_{X_i}(f_c(\boldsymbol{X})) < n_i$, $f_c(\boldsymbol{X})$ is the unique polynomial in $S_{<k}$ such that $\mathrm{ev}_k(f_c(\boldsymbol{X})) = c$ and $\deg_{X_i}(f_c(\boldsymbol{X})) < n_i$ for $i \in [m]$.

Using these ideas we are almost ready to find the dual of a Cartesian code. Just one more result.

Lemma 2.2. *Let* $k' = \sum_{i=1}^{m}(n_i-1)-k+1$. *Then* $\dim(C_k(\mathcal{A}, \boldsymbol{v}))+\dim(C_{k'}(\mathcal{A}, \boldsymbol{v})) = n_1 \cdots n_m$.

Proof. Observe that the dimension of $C_k(\mathcal{A}, \boldsymbol{v})$ given in Theorem **??** (2) is the number of integer solutions of the following inequality

$$x_1 + \cdots + x_m \leq k - 1, \quad \text{where} \quad 0 \leq x_i \leq n_i - 1 \quad \text{for } i \in [m]. \tag{2.3}$$

The number of integer solutions of the inequality

$$x_1 + \cdots + x_m > k - 1, \quad \text{where} \quad 0 \leq x_i \leq n_i - 1 \quad \text{for } i \in [m], \tag{2.4}$$

is the same that the number of integer solutions of the inequality

$$x_1 + \cdots + x_m < \sum_{i=1}^{m}(n_i - 1) - k + 1 = k', \quad \text{where} \quad 0 \leq x_i \leq n_i - 1 \quad \text{for } i \in [m],$$

which is the dimension of $C_{k'}(\mathcal{A}, \boldsymbol{v})$. As the total number of integer solutions of (**??**) plus the total number of integer solutions of (**??**) is $n_1 \cdots n_m$, we obtain the result. □

We come to the main result of this section.

Theorem 2.3. *Let* $\boldsymbol{a_1}, \ldots, \boldsymbol{a_n}$ *be points of the Cartesian set* $\mathcal{A} = A_1 \times \cdots \times A_m$. *The dual of* $C_k(\mathcal{A}, \boldsymbol{v})$ *is*

$$C_k(\mathcal{A}, \boldsymbol{v})^{\perp} = C_{k'}(\mathcal{A}, \boldsymbol{v'}),$$

where $k' = \sum_{i=1}^{m}(n_i - 1) - k + 1$ *and* $\boldsymbol{v'}$ *is given by* $v'_i := (v_i L_{\boldsymbol{a_i}}(\boldsymbol{a_i}))^{-1}$.

Proof. Let $f(\boldsymbol{X})$ be an element of $S_{<k}$ such that $\deg_{X_i}(f(\boldsymbol{X})) < n_i$ for $i \in [m]$ and let $g(\boldsymbol{X})$ be an element of $S_{<k'}$ such that $\deg_{X_i}(g(\boldsymbol{X})) < n_i$ for $i \in [m]$. By the division algorithm in S [**?**, Theorem 1.5.9], there are $f_1(\boldsymbol{X}), \ldots, f_m(\boldsymbol{X}), r(\boldsymbol{X}) \in S$ such that

$$f(\boldsymbol{X})g(\boldsymbol{X}) = \sum_{i=1}^{m} f_i(\boldsymbol{X})L_i(X_i) + r(\boldsymbol{X}),$$

where $\deg_{X_i}(r(\boldsymbol{X})) < n_i$ for $i = 1, \ldots, m$, and

$$\deg(r(\boldsymbol{X})) \leq \deg((fg)(\boldsymbol{X})) \leq \sum_{i=1}^{m}(n_i - 1) - 1. \tag{2.5}$$

Observe that $r(\boldsymbol{a}) = (fg)(\boldsymbol{a})$ for all $\boldsymbol{a} \in \mathcal{A}$. Then

$$r(\boldsymbol{X}) = \sum_{\boldsymbol{a}\in\mathcal{A}} \frac{L_{\boldsymbol{a}}(\boldsymbol{X})}{L_{\boldsymbol{a}}(\boldsymbol{a})}(fg)(\boldsymbol{a}). \tag{2.6}$$

The coefficient of the monomial of degree $\sum_{i=1}^{m}(n_i - 1)$ on the right-hand side of (**??**) is given by:

$$\sum_{\boldsymbol{a}\in\mathcal{A}} \frac{(fg)(\boldsymbol{a})}{L_{\boldsymbol{a}}(\boldsymbol{a})} = \sum_{\boldsymbol{a}\in\mathcal{A}} \frac{f(\boldsymbol{a})g(\boldsymbol{a})}{L_{\boldsymbol{a}}(\boldsymbol{a})} = \sum_{\boldsymbol{a}\in\mathcal{A}} \frac{v_{\boldsymbol{a}} f(\boldsymbol{a})g(\boldsymbol{a})}{v_{\boldsymbol{a}} L_{\boldsymbol{a}}(\boldsymbol{a})} = \tag{2.7}$$

$$= (v_{\boldsymbol{a_1}} f(\boldsymbol{a_1}), \ldots, v_{\boldsymbol{a_n}} f(\boldsymbol{a_n})) \cdot \left(\frac{g(\boldsymbol{a_1})}{v_{\boldsymbol{a_1}} L_{\boldsymbol{a_1}}(\boldsymbol{a_1})}, \ldots, \frac{g(\boldsymbol{a_n})}{v_{\boldsymbol{a_n}} L_{\boldsymbol{a_n}}(\boldsymbol{a_n})} \right). \tag{2.8}$$

By (**??**) $\deg(r(\boldsymbol{X})) < \sum_{i=1}^{m}(n_i - 1)$, so the coefficient of the monomial of degree $\sum_{i=1}^{m}(n_i - 1)$ on the left-side of (**??**) is 0. Thus the dot product shown on (**??**) is 0. The left-hand side of the dot product given in (**??**) is an arbitrary element of $C_k(\mathcal{A}, \boldsymbol{v})$, and right-hand side of the dot product of Equation (**??**) is an arbitrary element of $C_{k'}(\mathcal{A}, \boldsymbol{v'})$. Thus, the proof is complete, because $\dim(C_{k'}(\mathcal{A}, \boldsymbol{v'})) = \dim(C_{k'}(\mathcal{A}, \boldsymbol{v})) = \dim(C_k(\mathcal{A}, \boldsymbol{v})^{\perp})$ where the last equality follows from Lemma **??**. □

3 Finding LCD codes from Cartesian codes

In this section, we determine which Cartesian codes $C_k(\mathcal{A}, \boldsymbol{v})$, where $\mathcal{A} := A_1 \times \cdots \times A_m \subseteq K^m$, are LCD. As a result, a number of explicit constructions for LCD codes are found.

3.1 Generalized Reed-Solomon codes (i.e., the case $m = 1$)

We start with the case when $m = 1$, meaning $\mathcal{A} = A := \{a_1, \ldots, a_n\} \subseteq K$, so $n_1 = n$. Observe that in this case the Cartesian code $C_k(A, \boldsymbol{v})$ is the *generalized Reed-Solomon code* $GRS_k(A, \boldsymbol{v})$, which is given by

$$GRS_k(A, \boldsymbol{v}) := \{(v_1 f(a_1), \ldots, v_n f(a_n)) \mid f(X) \in K[X], \deg f(X) < k\}.$$

Recall $L(X) = \prod_{a\in A}(X - a)$ and $L_a(X) = \frac{L(X)}{(X-a)}$ for each element $a \in A$. By (**??**),

$$\begin{aligned} C_k(A, \boldsymbol{v})^{\perp} &= \left\{ \left(\frac{g(a_1)}{v_1 L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_n L_{a_n}(a_n)} \right) \mid g(X) \in K[X], \deg g(X) < n - k \right\} \\ &= C_{n-k}(A, \boldsymbol{v'}) = GRS_{n-k}(A, \boldsymbol{v'}). \end{aligned}$$

We are interested in finding conditions on A and $\boldsymbol{v}$ such that $C_k(A, \boldsymbol{v})$ is LCD. Observe that the Cartesian code $C_k(A, \boldsymbol{v})$ is not LCD if and only if there are nonzero polynomials $f(X)$ and $g(X)$ such that $\deg(f(X)) < k$, $\deg(g(X)) < n - k$ and

$$(v_1 f(a_1), \ldots, v_n f(a_n)) = \left(\frac{g(a_1)}{v_1 L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_n L_{a_n}(a_n)} \right).$$

This holds if and only if

$$v_i^2 L_{a_i}(a_i) f(a_i) = g(a_i), \quad \text{for all } a_i \in A. \tag{3.1}$$

Define the polynomial associated to $C_k(A, \boldsymbol{v})$ by

$$H(X) := \sum_{a_i \in A} v_i^2 L_{a_i}(X). \tag{3.2}$$

Notice that $H(a_i) = v_i^2 L_{a_i}(a_i)$ for all $a_i \in A$ and $\deg(H) < n$. Moreover, $H(X)$ and $L(X)$ are coprime in $K[X]$. To see this, observe that $L(a) = 0$ if and only if $a \in A$ whereas $H(a) \neq 0$ if $a \in A$. Since $L(X)$ factors into linear terms over K, $H(X)$ and $L(X)$ have no nonconstants common factors. Then we have the following result.

Proposition 3.1. *The Cartesian code $C_k(A, \boldsymbol{v})$ is LCD if and only if for all nonzero polynomials $f(X), g(X) \in K[X]$ with $\deg(f(X)) < k$ and $\deg(g(X)) < n - k$ we have*

$$H(X)f(X) - g(X) \notin \langle L(X) \rangle$$

where $H(X)$ is defined in (**??**)*.*

Proof. Equation (**??**) holds if and only if $L(x)$ divides $H(X)f(X) - g(X)$. □

As $H(X)$ and $L(X)$ are coprime, by the Extended Euclidean Algorithm [**?**, Chapter 3], there exists a natural number t, polynomials $g_i(X)$, $h_i(X)$, $f_i(X) \in K[X]$ for $i \in \{0, \ldots, t+1\}$ and polynomials $q_i(X) \in K[X]$ for $i \in \{1, \ldots, t\}$ such that

$$\begin{aligned}
& g_0 = L, \ g_1 = H, \ h_0 = f_1 = 1, \ h_1 = f_0 = 0 && \\
& g_{i-1} = q_i g_i + g_{i+1} \text{ where } \deg g_{i+1} < \deg g_i && \forall\, i \in \{1, \ldots, t\} \\
& g_i = h_i L + f_i H && \forall\, i \in \{0, \ldots, t\} \qquad (3.3) \\
& \deg f_i = \deg L - \deg g_{i-1} = n - \deg g_{i-1} && \forall\, i \in \{1, \ldots, t\} \qquad (3.4) \\
& g_{t+1} = 1. &&
\end{aligned}$$

The following is the basis of our main results of this section.

Proposition 3.2. *Let $C_k(A, \boldsymbol{v})$ be a Cartesian code and $g_0(X), \ldots, g_{t+1}(X)$ be the remainders from the Extended Euclidean Algorithm applied to polynomials $L(X) = \prod_{a_i \in A}(X - a_i)$ and $H(X) = \sum_{a_i \in A} v_i^2 L_{a_i}(X)$. Then, $C_k(A, \boldsymbol{v})$ is LCD if and only if for all $i \in \{1, \ldots, t+1\}$,*

$$\deg(g_{i-1}(X)) \leq n - k \quad \text{or} \quad \deg(g_i(X)) \geq n - k.$$

Proof. We prove both implications via the contrapositives.

($\Rightarrow$) Assume there is $i \in \{1, \ldots, t\}$ such that $\deg(g_i(X)) < n - k < \deg(g_{i-1}(X))$. Then by (**??**) and (**??**), there are $f_i(X), g_i(X)$ and $h_i(X)$ in $K[X]$ such that $L(X)h_i(X) + H(X)f_i(X) = g_i(X)$, and $\deg(g_i(X)) < n - k$ and $\deg(f_i(X)) = n - \deg(g_{i-1}(X)) < k$. By Proposition **??**, $C_k(A, \boldsymbol{v})$ is not LCD.

($\Leftarrow$) Assume $C_k(A,\boldsymbol{v})$ is not LCD. By Proposition **??**, there are polynomials $f(X), g(X)$ and $h(X)$ in $K[X]$ such that $\deg(f(X)) < k$, $\deg g(X) < n-k$ and

$$L(X)h(X) + H(X)f(X) = g(X). \tag{3.5}$$

Let $g_i(X)$ be the remainder such that $\deg(g_i(X)) \leq \deg(g(X))$ and $\deg(g_{i-1}(X)) > \deg(g(X))$. Observe $\deg(g_i(X)) \leq \deg(g(X)) < n-k$. This means that now we just need to prove $\deg(g_{i-1}(X)) > n-k$.

Combining (**??**) with (**??**), we obtain that

$$L(X)\left(h(X)g_i(X) - h_i(X)g(X)\right) + H(X)\left(f(X)g_i(X) - f_i(X)g(X)\right) = 0.$$

Because $L(X)$ and $H(X)$ are coprime, $L(X) \mid f(X)g_i(X) - f_i(X)g(X)$. Moreover it holds that

$$\begin{aligned} \deg((fg_i)(X)) &= \deg(f(X)) + \deg(g_i(X)) \leq \deg(f(X)) + \deg(g(X)) < n, \text{ and} \\ \deg((f_ig)(X)) &= \deg(f_i(X)) + \deg(g(X)) = \\ &= n - \deg(g_{i-1}(X)) + \deg(g(X)) < n - \deg(g(X)) + \deg(g(X)) = n. \end{aligned}$$

Then

$$f(X)g_i(X) = f_i(X)g(X),$$

which implies $\deg(f_i(X)) = \deg(f(X)) + \deg(g_i(X)) - \deg(g(X))$. Then by (**??**)

$$\deg(g_{i-1}(X)) = n - \deg(f_i(X)) = n - \deg(f(X)) - \deg(g_i(X)) + \deg(g(X)) > n-k,$$

which completes the proof.

□

The following theorem is the main result of this section and a corollary of Proposition **??**.

Theorem 3.3. *Let $C_k(A,\boldsymbol{v})$ be a Cartesian code and $g_0(X), \ldots, g_{t+1}(X)$ be the remainders from the Extended Euclidean Algorithm applied to polynomials $L(X) = \prod_{a_i \in A}(X - a_i)$ and $H(X) = \sum_{a_i \in A} v_i^2 L_{a_i}(X)$. Then, $C_k(A,\boldsymbol{v})$ is LCD if and only if*

$$n - k \in \{n-1, n-2, \ldots, \deg(g_1(X)), \deg(g_2(X)), \ldots, \deg(g_{t+1}(X))\}.$$

3.2 Affine Cartesian codes on $m > 1$ components

Let $\boldsymbol{a_1}, \ldots, \boldsymbol{a_n}$ be the points of the Cartesian set $\mathcal{A} = A_1 \times \cdots \times A_m$. Now we are ready to determine whether a Cartesian code $C_k(\mathcal{A},\boldsymbol{v})$ is LCD. By (**??**), the dual of $C_k(\mathcal{A},\boldsymbol{v})$ is given by

$$C_k(\mathcal{A},\boldsymbol{v})^\perp = C_{k'}(\mathcal{A},\boldsymbol{v}'),$$

where $k' = \sum_{i=1}^{m}(n_i - 1) - k + 1$ and $\boldsymbol{v}'$ is defined by $v'_i := v_i^{-1} L_{\boldsymbol{a_i}}(\boldsymbol{a_i})^{-1}$. Thus the Cartesian code $C_k(\mathcal{A}, \boldsymbol{v})$ is not LCD if and only if there are nonzero polynomials $f(\boldsymbol{X}) \in S_{<k}$ and $g(\boldsymbol{X}) \in S_{<k'}$ such that

$$(v_1 f(\boldsymbol{a_1}), \ldots, v_n f(\boldsymbol{a_n})) = \left(\frac{g(\boldsymbol{a_1})}{v_1 L_{\boldsymbol{a_1}}(\boldsymbol{a_1})}, \ldots, \frac{g(\boldsymbol{a_n})}{v_n L_{\boldsymbol{a_n}}(\boldsymbol{a_n})} \right). \tag{3.6}$$

Equation (**??**) holds if and only if

$$v_i^2 L_{\boldsymbol{a_i}}(\boldsymbol{a_i}) f(\boldsymbol{a_i}) = g(\boldsymbol{a_i}), \quad \text{ for all } \boldsymbol{a_i} \in \mathcal{A}. \tag{3.7}$$

The *polynomial associated* to $C_k(\mathcal{A}, \boldsymbol{v})$ is defined by

$$H(\boldsymbol{X}) := \sum_{\boldsymbol{a_i} \in \mathcal{A}} v_i^2 L_{\boldsymbol{a_i}}(\boldsymbol{X}). \tag{3.8}$$

Notice that

1. for all $\boldsymbol{a_i} \in \mathcal{A}$, $H(\boldsymbol{a_i}) = v_i^2 L_{\boldsymbol{a_i}}(\boldsymbol{a_i})$ and
2. $\deg_{X_i}(H(\boldsymbol{X})) < n_i$ for all $i \in [n]$.

Moreover, if $G(\boldsymbol{X})$ is an element of S that satisfies 1. and 2., then $G(\boldsymbol{X}) = H(\boldsymbol{X})$. We have the following characterization for LCD codes.

Proposition 3.4. *The Cartesian code $C_k(\mathcal{A}, \boldsymbol{v})$ is LCD if and only if for all nonzero polynomials $f(\boldsymbol{X}), g(\boldsymbol{X}) \in S$ with $\deg(f(\boldsymbol{X})) < k$, and $\deg(g(\boldsymbol{X})) \leq \sum_{i=1}^{m}(n_i - 1) - k$ we have*

$$H(\boldsymbol{X}) f(\boldsymbol{X}) - g(\boldsymbol{X}) \notin I(\mathcal{A}),$$

where $H(\boldsymbol{X})$ is the polynomial associated to $C_k(\mathcal{A}, \boldsymbol{v})$ defined in (**??**)

Proof. Equation (**??**) holds if and only if $(Hf - g)(\boldsymbol{X}) \in I(\mathcal{A})$. □

Next, we focus on a special family of Cartesian codes.

Definition 3.5. For $i \in [m]$, write $A_i := \{a_{i1}, \ldots, a_{in_i}\} \subseteq K$ and let $\boldsymbol{v_i} := (v_{i1}, \ldots, v_{in_i}) \in (K^*)^{n_i}$. The Cartesian vector $\boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m} \in K^n$ is defined as a vector of length $n := n_1 \cdots n_m$ with

$$(\boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})_{\boldsymbol{a}} := v_{1j_1} \cdots v_{mj_m} \quad \text{ where } \quad \boldsymbol{a} = (a_{1j_1}, \ldots, a_{mj_m}).$$

In a few words, the following result says that if the Cartesian code $C_k(\mathcal{A}, \boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})$ is not LCD, then one of its components $C_{t_i}(A_i, \boldsymbol{v_i})$ is not LCD, for some $t_i \leq \min\{k, n_i - 1\}$.

Theorem 3.6. *If for all $i \in \{1, \ldots, m\}$ we have that $C_{t_i}(A_i, \boldsymbol{v_i})$ is LCD for all $t_i < \min\{k, n_i\}$, then $C_k(\mathcal{A}, \boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})$ is LCD.*

Proof. Assume $C_k(\mathcal{A}, \boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})$ is not LCD. By Proposition **??**, there are polynomials $f(\boldsymbol{X})$ and $g(\boldsymbol{X})$ such that $\deg(f(\boldsymbol{X})) < k$, $\deg(g(\boldsymbol{X})) \leq \sum_{i=1}^{m}(n_i - 1) - k$, and $H(\boldsymbol{X})f(\boldsymbol{X}) - g(\boldsymbol{X}) \in I(\mathcal{A})$, where $H(\boldsymbol{X})$ is the polynomial associated to $C_k(\mathcal{A}, \boldsymbol{v}_1 \times \cdots \times \boldsymbol{v}_m)$ defined on Equation **??**. Thus, there are $h_i(X_i) \in S$, for $i = 1, \ldots, m$, such that $\sum_{i=1}^{m} L_i(X_i)h_i(X_i) \in I(\mathcal{A})$ and

$$\sum_{i=1}^{m} L_i(X_i)h_i(X_i) + H(\boldsymbol{X})f(\boldsymbol{X}) = g(\boldsymbol{X}).$$

As $\deg_{X_i}(f(\boldsymbol{X})) < n_i$, by Combinatorial Nullstellensatz [**?**, Theorem 1.2], there are $a_1 \in A_1, \ldots, a_m \in A_m$ such that $f(a_1, \ldots, a_m) \neq 0$, which implies $g(a_1, \ldots, a_m) \neq 0$. These a_i's give the following m equations:

$$\begin{array}{rcl} L_1(X_1)h_1(X_1) + H(X_1, a_2, \ldots, a_m)f(X_1, a_2, \ldots, a_m) & = & g(X_1, a_2 \ldots, a_m) \\ L_1(X_2)h_2(X_2) + H(a_1, X_2, \ldots, a_m)f(a_1, X_2, \ldots, a_m) & = & g(a_1, X_2, \ldots, a_m) \\ & \vdots & \\ L_m(X_m)h_m(X_m) + H(a_1, a_2, \ldots, X_m)f(a_1, a_2, \ldots, X_m) & = & g(a_1, a_2, \ldots, X_m). \end{array}$$

Let $t_i := \deg_{X_i}(f(\boldsymbol{X}))$. Observe that

$$\begin{aligned} \sum_{i=1}^{m} \deg_{X_i}(g(a_1, \ldots, X_i, \ldots, a_m)) \leq \deg(g(\boldsymbol{X})) &\leq \sum_{i=1}^{m}(n_i - 1) - k \\ &< \sum_{i=1}^{m}(n_i - 1) - \sum_{i=1}^{m} t_i = \sum_{i=1}^{m}(n_i - t_i - 1). \end{aligned}$$

Thus, there is $i \in \{1, \ldots, m\}$ such that

$$\deg_{X_i}(g(a_1, \ldots, a_{i-1}, X_i, a_{i+1}, \ldots, a_m)) < n_i - t_i - 1.$$

Observe that $H(a_1, \ldots, a_{i-1}, X_i, a_{i+1}, \ldots, a_m) = \ell v_i^2 L_i(X_i)$ where ℓ is a nonzero constant. Thus the i-th equation implies by Proposition **??** that the Cartesian code $C_{t_i}(A_i, \boldsymbol{v_i})$ is not LCD. □

Theorem 3.7. *If $k < \min\{n_i \mid i \in [m]\}$ and $C_k(\mathcal{A}, \boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})$ is LCD, then $C_k(A_i, \boldsymbol{v_i})$ is LCD for all $i \in \{1, \ldots, m\}$.*

Proof. If there is $i \in \{1, \ldots, m\}$ such that $C_k(A_i, \boldsymbol{v_i})$ is not LCD, by Proposition **??**, there are polynomials $f(X_i), g(X_i)$ and $h(X_i)$ in $K[K_i]$ such that $\deg(f(X_i)) < k$, $\deg g(X_i) < n_i - k$ and

$$L_i(X_i)h(X_i) + H_i(X_i)f(X_i) = g(X_i).$$

For $j \neq i$, let $H_j(X_j)$ be the polynomial associated to $C_k(A_j, \boldsymbol{v_j})$ defined in Equation **??**. The following equations holds:

$$H(X_1) \cdots H_m(X_m)f(X_i) = g(X_i)H(X_1) \cdots H_{i-1}(X_{i-1})H_{i+1}(X_{i+1}) \cdots H_m(X_m) \bmod L_i(X_i).$$

Observe $\deg(gH \cdots H_{i-1}H_{i+1} \cdots H_m) < \sum_{i=1}^{m}(n_i - 1) - k + 1$. As $H(X_1) \cdots H(X_m)$ is the polynomial associated to $C_k(\mathcal{A}, \boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})$, the thesis follows from Proposition **??**. □

We come to one of the main results of this section.

Theorem 3.8. *If at least one of the Cartesian codes* $C_{t_1}(A_1, \boldsymbol{v_1}), \ldots, C_{t_m}(A_m, \boldsymbol{v_m})$ *is not LCD, then* $C_{t_1+\cdots+t_m}(\mathcal{A}, \boldsymbol{v_1} \times \cdots \times \boldsymbol{v_m})$ *is not LCD.*

Proof. Assume for all $i \in \{1, \ldots, m\}$ $C_{t_i}(A_i, \boldsymbol{v_i})$ is not LCD. By Proposition **??** there are polynomials $f_i(X_i), g_i(X_i)$ and $h_i(X_i)$ in $K[X_i]$ such that $\deg(f_i(X_i)) < t_i$, $\deg(g_i(X_i)) < n_i - t_i$ and

$$L_i(X_i)h_i(X_i) + H_i(X_i)f_i(X_i) = g_i(X_i) \qquad \text{for} \qquad i \in \{1, \ldots, m\}, \tag{3.9}$$

where $H_i(X_i)$ is the polynomial associated to $C_{t_i}(A_i, \boldsymbol{v}_i)$ defined on Equation **??**. Multiplying the all m equations from Equation (**??**) we obtain an expresion of the form

$$L(\boldsymbol{X})G + H(\boldsymbol{X})f_1(X_1)\cdots f_m(X_m) = g_1(X_1)\cdots g_m(X_m),$$

where $L(\boldsymbol{X}) \in I(\mathcal{A})$, $H(\boldsymbol{X}) := H(X_1)\cdots H_m(X_m)$ is the polynomial associated to $C_{t_1+\cdots+t_m}(\mathcal{A}, \boldsymbol{v_1}\times\cdots\times\boldsymbol{v_m})$, $\deg(f_1(X_1)\cdots f_m(X_m)) < t_1+\cdots+t_m$ and $\deg(g_1(X_1)\cdots g_m(X_m)) \leq \sum_{i=1}^{m}(n_i - 1) - (t_1 + \cdots + t_m)$. Proposition **??** gives the result. □

4 Families and examples of LCD codes

In this section, we illustrate some examples of our results. One of the works in literature regarding families or algorithms to construct families of LCD codes is [**?**]. The authors give an explanation about how to find LCD codes that are cyclic codes. A main purpose of this paper is to determine when a given affine Cartesian code is LCD. It is possible to construct families of LCD codes based on Theorems **??** and **??**. Here is an instance of such a family.

Proposition 4.1. *Let* $A_1, \ldots, A_m$ *be non-empty subsets of* K*, and set*

$$\mathfrak{m} = \min\{|A_j| - \deg(H_j(X)) \mid j = 1, \ldots, m\}$$

where $H_j(X) = \sum_{a_i \in A_j} v_i^2 L_{a_i}(X)$*. Then* $C_k(A_1 \times \ldots \times A_m, \mathbf{1} \times \cdots \times \mathbf{1})$ *is LCD for all* $k = 1, \ldots, \mathfrak{m}$.

Proof. By Theorem **??** and since $H_j(X) = g_1^j(X)$, $C_{k_j}(A_j, \boldsymbol{v})$ is LCD for all $k_j = 1, \ldots, |A_j| - \deg(g_1^j(X))$. By Theorem **??**, $C_k(A_1 \times \ldots \times A_m, \mathbf{1} \times \cdots \times \mathbf{1})$ is LCD for $k = 1, \ldots, \mathfrak{m}$. □

We note that for $m > 1$, the result above gives a family of LCD codes which are not generalized Reed-Solomon codes. It can be modified to give additional families by choosing k so that $|A_j| - k \in \left\{|A_j| - 1, |A_j| - 2, \ldots, \deg(g_1^j(X)), \deg(g_2^j(X)), \ldots, \deg(g_{t+1}^j(X))\right\}$ for all $j, 1 \leq j \leq m$.

Contrary to the length, the dimension, and the minimum distance of a Cartesian code, the LCD property depends on the choice of evaluation points and columns multipliers as shown in the following example.

Example 4.2. Let $K := \mathbb{F}_7$.

- A generator matrix of the code $C_2(\mathcal{A}, \boldsymbol{v})$ with $A := \{0, 1, 2\}$ and $\boldsymbol{v} := (1, 1, 1)$ is $G := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. As $GG^T = \begin{pmatrix} 3 & 3 \\ 3 & 0 \end{pmatrix}$, which is invertible, then the code $C_2(\mathcal{A}, \boldsymbol{v})$ is LCD.

- A generator matrix of the code $C_2(\mathcal{A}, \boldsymbol{v})$ with $A := \{0, 1, 2\}$ and $\boldsymbol{v} := (1, 1, 2)$ is $G := \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 4 \end{pmatrix}$. As $GG^T = \begin{pmatrix} 6 & 2 \\ 2 & 3 \end{pmatrix}$, which is singular, then the code $C_2(\mathcal{A}, \boldsymbol{v})$ is not LCD.

- A generator matrix of the code $C_2(\mathcal{A}, \boldsymbol{v})$ $A := \{0, 1, 3\}$ and $\boldsymbol{v} := (1, 1, 1)$ is $G := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \end{pmatrix}$. As $GG^T = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$, which is singular, then the code $C_2(\mathcal{A}, \boldsymbol{v})$ is not LCD.

In [**?**, Theorem I.1] and in [**?**, Theorem 1] the authors show that assuming some conditions over q, k and n, it is always possible to find LCD MDS codes. The following example shows that our results are complementary to theirs.

Example 4.3. Let $A = \{0, 2, 3, 5, 6, 8, 10, 11\} \subset \mathbb{F}_q$ with $q = 13, 17$.

- If $q = 13$ then the degrees of the remainders of the Extended Euclidean Algorithm are $0, 3, 4, 5, 6$ and 7. Thus, the generalized Reed-Solomon code $GRS_k(A, \mathbf{1})$ is LCD if and only if $k \in \{1, 2, 3, 4, 5, 8\}$.

- If $q = 17$ then the degrees of the remainders of the Extended Euclidean Algorithm are $0, \ldots, 7$. Thus, the generalized Reed-Solomon code $GRS_k(A, \mathbf{1})$ is always LCD.

5 Conclusion

In this paper, we studied affine Cartesian codes which are LCD codes. In doing so, it was necessary to consider generalized affine Cartesian codes, because they arise as duals of the affine Cartesian codes. Some results on this more general family of codes are included. We provide a characterization of which generalized Reed-Solomon codes are LCD, regardless of the characteristic of the ambient field, as well of which affine Cartesian codes are LCD. In addition, we explore certain families of generalized affine Cartesian codes which inherit the LCD property from their factors. This work allows us to find additional instances and explicit constructions of LCD codes.

References

[1] W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.

[2] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Maŕtraháza, 1995), Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.

[3] P. Beelen, M. Datta, Generalized Hamming Weights of affine Cartesian Codes, Finite Fields and Their Applications **51** (2018) 130–145.

[4] C. Carlet and S. Guilley, Complementary Dual Codes for Counter-Measures to Side-Channel Attacks, Advances in Mathematics of Communications **10** (2016) 131–150.

[5] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, IEEE Transactions on Information Theory **64** (2018), no. 4, 3010–3017.

[6] C. Carvalho, On the second Hamming weight of some Reed-Muller type codes, Finite Fields and Their Applications **24** (2013) 88–94.

[7] C. Carvalho, V. G. Neumann, On the next-to-minimal weight of affine Cartesian codes, Finite Fields and Their Applications **44** (2017) 113–134.

[8] C. Carvalho, V. G. Neumann, Projective ReedMuller type codes on rational normal scrolls, Finite Fields and Their Applications **37** (2016) 85–107.

[9] C. Carvalho, V. G. Neumann, H. H. López, Projective Nested Cartesian Codes, Bull Braz Math Soc, New Series (2016).

[10] B. Chen, H. Liu, New constructions of MDS codes with complementary duals, IEEE Transactions on Information Theory **64** (2018), no. 8, 5776 – 5782.

[11] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, Third Edition, 2008.

[12] P. Delsarte, J. M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, Information and Control **16** (1970), 403–442.

[13] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, 1995.

[14] M. Esmaeili and S. Yari, On complementary-dual quasi-cyclic codes, Finite Fields and Their Applications, 15(2009), 375-386.

[15] J. Fitzgerald, R.F. Lax, Decoding affine variety codes using Göbner bases, Des. Codes and Cryptogr. **13**(2) (1998) 147–158.

[16] O. Geil, C. Thomsen, Weighted Reed-Muller codes revisited, Des. Codes Cryptogr. **66**(1–3) (2013) 195–220.

[17] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed-Muller-type codes over the Segre variety, Finite Fields Appl. **8** (2002), no. 4, 511–518.

[18] W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[19] L. Jin, Construction of MDS Codes With Complementary Duals, IEEE Transactions on Information Theory **63** (2017), no. 5, 2843 – 2847.

[20] G. Lachaud, The parameters of projective Reed-Muller codes, Discrete Math. **81** (1990), no. 2, 217–221.

[21] C. Li, C. Ding, S. Li, LCD cyclic codes over finite fields, IEEE Transactions on Information Theory, **63** (2017), no. 7, 4344–4356.

[22] H. H. López, C. Rentería-Márquez, R. H. Villarreal, Affine Cartesian codes, Des. Codes Cryptogr. **71** (2014), no. 1, 5–19.

[23] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1977.

[24] James L. Massey, Linear codes with complementary duals, Discrete Mathematics, **106–107** (1992), 337–342.

[25] S. Mesnager, C. Tang, and Y. Qi, Complementary Dual Algebraic Geometry Codes, IEEE Transactions on Information Theory **64** (2018), no. 4., 2390–2397.

[26] A. Sørensen, Projective Reed-Muller codes, IEEE Transactions on Information Theory **37** (1991), no. 6, 1567–1576.

[27] A. Tochimani, M. Vaz Pinto, R. H.Villarreal, Direct products in projective Segre codes, Finite Fields Appl. **39** (2016) 96–110.

[28] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[29] R. H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

[30] J. von zur Gathen and J. Gerhard, Modern Computer Algebra, Third Edition, Cambridge University Press, 2013.

[31] X. Yang and J. L. Massey, The condition for a cyclic code to have a complementary dual. Discret. Math. 126(1), 391–393 (1994).