MONOMIAL-CARTESIAN CODES AND THEIR DUALS, WITH APPLICATIONS TO LCD CODES, QUANTUM CODES, AND LOCALLY RECOVERABLE CODES

HIRAM H. LÓPEZ, GRETCHEN L. MATTHEWS, AND IVAN SOPRUNOV

Abstract. A monomial-Cartesian code is an evaluation code defined by evaluating a set of monomials over a Cartesian product. It is a generalization of some families of codes in the literature, for instance toric codes, affine Cartesian codes, and J-affine variety codes. In this work we use the vanishing ideal of the Cartesian product to give a description of the dual of a monomial-Cartesian code. Then we use such description of the dual to prove the existence of quantum error correcting codes and MDS quantum error correcting codes. Finally we show that the direct product of monomial-Cartesian codes is a locally recoverable code with t-availability if at least t of the components are locally recoverable codes.

1. Introduction

Let $K = \mathbb{F}_q$ be a finite field with q elements and $R = K[x_1, \ldots, x_m]$ the polynomial ring over K in m variables. We write $K^* = K \setminus \{0\}$ for the multiplicative group of K. Given a lattice point $\boldsymbol{a} \in \mathbb{Z}_{\geq 0}^m$ we use $\boldsymbol{x}^{\boldsymbol{a}}$ to denote the corresponding monomial in R, i.e. $\boldsymbol{x}^{\boldsymbol{a}} = x_1^{a_1} \cdots x_m^{a_m}$ for $\boldsymbol{a} = (a_1, \ldots, a_m)$. Given a positive integer ℓ, we define $[\ell] := \{1, \ldots, \ell\}$.

A monomial-Cartesian code is defined as follows. Fix non-empty subsets $S_1, \ldots, S_m$ of K. Define their *Cartesian product* as

$$\mathcal{S} := S_1 \times \cdots \times S_m \subseteq K^m.$$

Furthermore, let $A \subseteq \mathbb{Z}_{\geq 0}^m$ be a finite lattice set and $\mathcal{L}(A)$ the subspace of polynomials of R that are K-linear combinations of monomials with exponents in A:

$$\mathcal{L}(A) = \mathrm{Span}_K\{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in A\} \subseteq R.$$

Fix a linear order of the points in $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\}$, $\boldsymbol{s}_1 \prec \cdots \prec \boldsymbol{s}_n$. This defines the *evaluation map*

$$\begin{array}{rccc} \mathrm{ev}_{\mathcal{S}}\colon & \mathcal{L}(A) & \to & K^{|\mathcal{S}|} \\ & f & \mapsto & (f(\boldsymbol{s}_1), \ldots, f(\boldsymbol{s}_n)). \end{array}$$

In what follows, $n_i := |S_i|$, the cardinality of S_i for $i \in [m]$. From now on, we assume that $A \subseteq \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\}$, that is the degree of each $f \in \mathcal{L}(A)$ in x_i is less than $|S_i|$. In this case, the evaluation map $\mathrm{ev}_{\mathcal{S}}$ is injective (see the proof of Proposition 2.1).

2010 *Mathematics Subject Classification.* 94B05; 11T71; 14G50.

The second author was supported by NSF DMS-1855136.

Definition 1.1. Let $\mathcal{S} \subseteq K^m$ and $A \subseteq \mathbb{Z}_{\geq 0}^m$ be as above. The image $\mathrm{ev}_{\mathcal{S}}(\mathcal{L}(A)) \subseteq K^{|\mathcal{S}|}$ is called the *monomial-Cartesian code* associated with $\mathcal{S}$ and A. We denote it by $C(\mathcal{S}, A)$. By an abuse of notation, if $\boldsymbol{a} \in A$ then $\mathcal{L}(\boldsymbol{a})$ means $\mathcal{L}(\{\boldsymbol{a}\})$ and $C(\mathcal{S}, \boldsymbol{a})$ denotes the code $C(\mathcal{S}, \{\boldsymbol{a}\})$.

The monomial-Cartesian code has the following parameters (Proposition 2.1). Its length and dimension are given by $n = |\mathcal{S}|$ and $k = \dim_K C(\mathcal{S}, A) = |A|$, respectively. Recall that the *minimum weight* of a code C is given by

$$\delta(C) = \min\{|\operatorname{supp}(c)| : 0 \neq c \in C\},$$

where $\operatorname{supp}(c)$ denotes the support of c, that is, the set of all non-zero entries of c. Unlike the case of the length and the dimension, in general, there is no explicit formula for $\delta(C(\mathcal{S}, A))$ in terms of $\mathcal{S}$ and A. For toric codes, some explicit formulas appear in [35] and non-trivial bounds appear in [34] when $m = 2$. However, there is a simple relation between the minimum weights of two monomial-Cartesian codes $C(\mathcal{S}_1, A)$ and $C(\mathcal{S}_2, A)$ and of their Cartesian product $C(\mathcal{S}_1 \times \mathcal{S}_2, A \times B)$ (see Proposition 3.1), which we make use of in Section 3.

The *dual* of the code C is defined by

$$C^{\perp} = \{\boldsymbol{w} \in K^n : \boldsymbol{w} \cdot \boldsymbol{c} = 0 \text{ for all } \boldsymbol{c} \in C\},$$

where $\boldsymbol{w} \cdot \boldsymbol{c}$ represents the *Euclidean inner product*. The code C is called a *linear complementary dual* (*LCD*) [30] if $C \cap C^{\perp} = \{\mathbf{0}\}$ and is called a *self-orthogonal* code if $C^{\perp} \subseteq C$. In [10], Carlet, Mesnager, Tang, Qi, and Pellikaan show that any linear code over $\mathbb{F}_q$ with $q > 3$ is equivalent to an LCD code; even so, explicit constructions can be elusive. In this paper, we provide a characterization for monomial-Cartesian codes which are LCD, thus providing explicit constructions of LCD codes.

Instances of monomial-Cartesian codes for particular families of lattice sets A and Cartesian products $\mathcal{S}$ have been extensively studied in the literature. For example, a Reed-Muller code of order r in the sense of [39, p. 37] is the monomial-Cartesian code $C(K^m, A_r)$, where $A_r = \{(a_1, \ldots, a_m) \in \mathbb{Z}_{\geq 0}^m : a_1 + \cdots + a_m \leq r\}$. Note that in this case $\mathcal{L}(A_r) = R_{\leq r}$, the set of all polynomials of degree at most r.

Another example of a monomial-Cartesian code is a *toric code* $C((K^*)^m, A_P)$, where $A_P = P \cap \mathbb{Z}^m$ is the set of lattice points of a convex lattice polytope $P \subseteq \mathbb{R}^m$ and $(K^*)^m$ is the Cartesian product with $S_1 = \cdots = S_m = K^*$. Good references for toric codes are [23, 25, 35].

An *affine Cartesian code of order* r is a monomial-Cartesian code $C(\mathcal{S}, A_r)$, where A_r is as above and $\mathcal{S}$ is an arbitrary Cartesian set. This family of codes appeared first time in [20] and then independently in [28]. In [20], the authors study the basic parameters of Cartesian codes, they determine optimal weights for the case when A_r is the Cartesian product of two sets, and then present two list decoding algorithms. In [28] the authors study the vanishing ideal $I(\mathcal{S})$. Using commutative algebra tools such as regularity, degree, and Hilbert function, the authors determine the basic parameters of Cartesian codes in terms of the size of the components of the Cartesian product. In [11], 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 [12] the authors find several values for the second least weight of

codewords, also known as the next-to-minimal Hamming weight. In [2] the authors find the generalized Hamming weights and the dual of Cartesian codes. In [27] the authors study the dual of a generalized Cartesian product and the property of being LCD, i.e., when the code and the dual have zero intersection.

Let $\mathcal{S} \subseteq K^m$ and $A \subseteq \mathbb{Z}_{\geq 0}^m$ be as above. In this work we are interested in the properties and applications of the monomial-Cartesian code $C(\mathcal{S}, A)$. In Section 2 we give a nice description of the dual of the code $C(\mathcal{S}, A)$ in terms of the complement of the set A and the vanishing ideal of the set of points $\mathcal{S}$. Our main theorem generalizes some results of [3, 19, 18] and [33], where the dual of toric codes, J-affine variety codes and generalized toric codes are studied. The representation for the dual gives rise to a Goppa representation for $C(\mathcal{S}, A)$, which may open the path for an efficiently decoding algorithm, because such a representation is the key to decoding the well-known Reed-Solomon codes. It is important to remark that there are decoding algorithms in the literature that can be used to decode particular cases of monomial-Cartesian codes, but the complexity is not as good as the one for the Reed-Solomon codes. For instance, the decoding algorithm developed by [17] depends of finding a Gröbner basis for each received codeword, and it would decode monomial-Cartesian codes in the case when $\mathcal{S}$ is arbitrary and $A \subseteq \mathbb{Z}_{\geq 0}^m$ are the smallest elements for a fixed monomial order in $Z_{\geq 0}^m$. Excellent references about how to decode linear codes using Gröbner basis are [4, 5, 6] and [7].

The monomial-Cartesian code construction provides the flexibility needed for some applications, such as that of quantum error-correcting codes and locally recoverable codes. Quantum codes support resilience of quantum information by correcting bit and phase flip errors in qudits, quantum digits, which is fundamental to fault-tolerant quantum computation. While the goal of quantum codes is similar to that of linear codes, new techniques are needed for their construction due to the inability to duplicate quantum information. Even so, there is a link between quantum codes and classical linear codes, due to independent work of Calderbank and Shor [8] and Steane [37]. Indeed, the CSS construction uses linear codes which contain their duals to construct quantum codes. A family of codes called J-affine variety codes were introduced and studied in [19] and [18], respectively. This family of codes can be seen as monomial-Cartesian codes $C(\mathcal{S}, A)$ with the condition that $n_i - 1$ divides $q - 1$. Inspired by those works, where the authors use J-affine variety codes to prove the existence of quantum error correcting codes, we use monomial-Cartesian codes in Section 3 to prove the existence of quantum error correcting codes with certain parameters. An $[[n, k, d]]_q$ quantum code satisfies the quantum Singleton bound [26]

$$k \leq n - 2d + 2.$$

If $k = n - 2d + 2$, then the quantum code is called *quantum maximum-distance-separable* (MDS) code. We obtain quantum MDS codes from monomial-Cartesian codes, making use of knowledge of the dual.

The idea of a locally recoverable code is that every coordinate depends on a few other coordinates. By "depends" we mean that if one of the coordinates is erased, then that coordinate can be recovered using some other coordinates. Of course, it is desirable that "some" is small. The concept of t-availability means that for any coordinate there are

t pair disjoint subsets of a few coordinates each in such a way that the each subset can be used to recover such coordinate. Traditionally, for locality and availability it is assumed that the received coordinates are correct, but it may happens in practice that the received coordinates that are not erased contain also errors. Previous situation with errors gives rise to the codes known as locally recoverable codes with local error detection, which was introduced recently in [32]. Section 4 we study local properties for direct product of monomial-Cartesian codes.

More information about basic theory for coding theory can be found in [24, 29, 40]. More constructions of evaluation codes can be seen in [13, 14, 21, 31]. Excellent references for theory of vanishing ideals and its properties are [15, 16, 22, 41].

2. Dual of Monomial-Cartesian codes

Denote the variables $x_1, \ldots, x_m$ by $\boldsymbol{x}$. An important characteristic for monomial-Cartesian codes and evaluation codes in general is the fact that we can use commutative algebra methods to study them. The kernel of the evaluation map $\mathrm{ev}_{\mathcal{S}}$ is precisely $\mathcal{L}(A) \cap I(\mathcal{S})$, where $I(\mathcal{S})$ is the *vanishing ideal* of $\mathcal{S}$ consisting of all polynomials of R that vanish on $\mathcal{S}$. Thus, algebraic properties of $R/\left(\mathcal{L}(A) \cap I(\mathcal{S})\right)$ are related to the basic parameters of $C(\mathcal{S}, A)$. For each $i \in [m]$, define the polynomial

$$L_i(x_i) := \prod_{s_j \in S_i} (x_i - s_j)\,. \tag{2.1}$$

The vanishing ideal of the Cartesian product $\mathcal{S}$ is given by $I(\mathcal{S}) = (L_1(x_1), \ldots, L_m(x_m))$, [28, Lemma 2.3]. Moreover, let $\prec$ be the *graded-lexicographic order* on the set of monomials of R. This order is defined in the following way: $x_1^{a_1} \cdots x_m^{a_m} \prec x_1^{b_1} \cdots x_m^{b_m}$ if and only if $\sum_{i=1}^m a_i < \sum_{i=1}^m b_i$ or $\sum_{i=1}^m a_i = \sum_{i=1}^m b_i$ and the leftmost nonzero entry in $(b_1 - a_1, \ldots, b_m - a_m)$ is positive. From now on, we fix the order $\prec$. Then, according to [15, Proposition 4], $\{L_1(x_1), \ldots, L_m(x_m)\}$ is a Gröbner basis of $I(\mathcal{S})$, relative to the order $\prec$.

Proposition 2.1. *The dimension and the length of the monomial-Cartesian code $C(\mathcal{S}, A)$ are given by $|A|$ and $|\mathcal{S}|$, respectively.*

Proof. It is enough to show that the evaluation map $\mathrm{ev}_{\mathcal{S}} \colon \mathcal{L}(A) \to K^{|\mathcal{S}|}$ is injective. By above $\mathrm{Ker}(\mathrm{ev}_{\mathcal{S}}) = \mathcal{L}(A) \cap I(\mathcal{S})$. On one hand, by assumption $\deg_{x_i}(f) < n_i$ for every $f \in \mathcal{L}(A)$ and $i \in [m]$. On the other hand, $I(\mathcal{S})$ has a Gröbner basis $\{L_1(x_1), \ldots, L_m(x_m)\}$ with $\deg_{x_i}(L_i) = n_i$ for each $i \in [m]$. Therefore, $\mathcal{L}(A) \cap I(\mathcal{S})$ is trivial. □

Definition 2.2. For $\boldsymbol{s} = (s_1, \ldots, s_m) \in \mathcal{S}$ and $f \in R$, define the *residue* of f at $\boldsymbol{s}$ as

$$\mathrm{Res}_{\boldsymbol{s}} f = f(\boldsymbol{s}) \left(\prod_{i=1}^{m} \prod_{s_i' \in S_i \setminus \{s_i\}} (s_i - s_i') \right)^{-1}. \tag{2.2}$$

For simplicity, we introduce the following notation for the residues vector

$$\mathrm{Res}_{\mathcal{S}} f = \left(\mathrm{Res}_{\boldsymbol{s}_1} f, \ldots, \mathrm{Res}_{\boldsymbol{s}_n} f\right).$$

Remark 2.3. Note that $\mathrm{Res}_{\mathcal{S}} : R \to K^{|\mathcal{S}|}$ is a linear map which is injective on the subspace of polynomials f satisfying $\deg_{x_i}(f) < n_i$. This follows from the definition of the residue and the proof of Proposition 2.1.

By [2, Theorem 5.7] or [27, Theorem 2.3], the dual of the monomial-Cartesian code $C(\mathcal{S}, \mathbf{0}) \subseteq K^{|\mathcal{S}|}$, where $\mathbf{0}$ is the zero vector in $\mathbb{Z}^m_{\geq 0}$, is given by

$$C(\mathcal{S}, \mathbf{0})^{\perp} = \mathrm{Span}_K \Big\{ \mathrm{Res}_{\mathcal{S}} f : \deg(f) < \sum_{i=1}^{m} (n_i - 1), \deg_{x_i}(f) < n_i \Big\}.$$

Thus

$$\sum_{i=1}^{n} \mathrm{Res}_{\boldsymbol{s}_i} f = 0, \text{ for } f \in R \text{ with } \deg(f) < \sum_{i=1}^{m} (n_i - 1) \text{ and } \deg_{x_i}(f) < n_i. \tag{2.3}$$

This follows since $1 \in \mathcal{L}(\mathbf{0})$. By the division algorithm, there are polynomials $q_{i,j}$ and $r_{i,j}$ in $K[x_i]$ for $i \in [m]$, such that

$$L_i = x_i^j q_{i,j-1} + r_{i,j-1}, \tag{2.4}$$

and $\deg(r_{i,j-1}) < j$. For every $\boldsymbol{b} = (b_1, \ldots, b_m)$ in $\mathbb{Z}^m_{\geq 0}$, define the polynomial

$$Q_{\boldsymbol{b}}(\boldsymbol{x}) := \prod_{i=1}^{m} q_{i,b_i}(x_i). \tag{2.5}$$

These polynomials $Q_{\boldsymbol{b}} \in R$ help to describe the dual of a monomial-Cartesian code.

Lemma 2.4. *Let $B = \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\}$. For any $\boldsymbol{a} \in B$, the set $\{\mathrm{Res}_{\mathcal{S}} Q_{\boldsymbol{b}} : \boldsymbol{b} \in B, \boldsymbol{b} \neq \boldsymbol{a}\}$ forms a basis for the dual $C(\mathcal{S}, \boldsymbol{a})^{\perp}$ of the monomial-Cartesian code $C(\mathcal{S}, \boldsymbol{a})$.*

Proof. By definition, $\deg_{x_i}(Q_{\boldsymbol{b}}) = n_i - (b_i + 1)$. This implies that the $Q_{\boldsymbol{b}}$ for $\boldsymbol{b} \in B$ have pairwise distinct multidegrees (with respect to the graded-lexicographic order). Thus the set $\{Q_{\boldsymbol{b}} : \boldsymbol{b} \in B, \boldsymbol{b} \neq \boldsymbol{a}\}$ is linearly independent. Furthermore, by Remark 2.3, its image under the residue map $\{\mathrm{Res}_{\mathcal{S}} Q_{\boldsymbol{b}} : \boldsymbol{b} \in B, \boldsymbol{b} \neq \boldsymbol{a}\}$ spans a subspace of dimension $\sum_{i=1}^{m} (n_i - 1) - 1 = \dim C(\boldsymbol{a}, \mathcal{S})^{\perp}$.

Now we check the inner product. Let $\overline{f}$ denote the normal form of f with respect to the Gröbner basis $\{L_1(x_1), \ldots, L_m(x_m)\}$. Note that $\mathrm{Res}_{\boldsymbol{s}_i} f = \mathrm{Res}_{\boldsymbol{s}_i} \overline{f}$ for any $i \in [n]$ and $f \in R$. Therefore,

$$(\boldsymbol{s}_1^{\boldsymbol{a}}, \ldots, \boldsymbol{s}_n^{\boldsymbol{a}}) \cdot \mathrm{Res}_{\mathcal{S}} Q_{\boldsymbol{b}} = \sum_{i=1}^{n} \boldsymbol{s}_i^{\boldsymbol{a}} \mathrm{Res}_{\boldsymbol{s}_i} Q_{\boldsymbol{b}} = \sum_{i=1}^{n} \mathrm{Res}_{\boldsymbol{s}_i} \boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}} = \sum_{i=1}^{n} \mathrm{Res}_{\boldsymbol{s}_i} \overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}}.$$

It remains to be shown that $\sum_{i=1}^{n} \mathrm{Res}_{\boldsymbol{s}_i} \overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}} = 0$. For this we check the conditions in Equation (2.3). We have

$$\deg_{x_i} \big(\overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}(\boldsymbol{x})} \big) \leq \begin{cases} a_i + n_i - (b_i + 1) & \text{if } a_i \leq b_i, \\ a_i - 1 & \text{if } a_i > b_i. \end{cases} \tag{2.6}$$

Indeed, the first inequality is clear. For the second one, when $a_i > b_i$ the division algorithm and Equation 2.4 provide

$$\deg_{x_i} \big(\overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}(\boldsymbol{x})} \big) = \deg_{x_i} \big(\overline{x_i^{a_i} q_{i,b_i}(x_i)} \big) = \deg_{x_i} \big(x_i^{a_i - (b_i+1)} r_{i,b_i}(x_i) \big) < a_i.$$

Now, since $\boldsymbol{a} \neq \boldsymbol{b}$, there is $j \in [m]$ such that $a_j \neq b_j$. Then (2.6) implies

$$\deg_{x_j}\left(\overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}(\boldsymbol{x})}\right) < n_j - 1.$$

Also, (2.6) provides $\deg_{x_i}\left(\overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}(\boldsymbol{x})}\right) < n_i$ for all $i \in [m] \setminus \{j\}$. Therefore, both conditions of (2.3) are satisfied which shows that $\sum_{i=1}^{n} \operatorname{Res}_{\boldsymbol{s}_i} \overline{\boldsymbol{x}^{\boldsymbol{a}} Q_{\boldsymbol{b}}} = 0$. □

Example 2.5. Let $K = \mathbb{F}_7$ and assume $\mathcal{S} = \{1, 3, 4, 5\} \subseteq K$. In this case, $L_1(x_1) = (x_1 - 1)(x_1 - 3)(x_1 - 4)(x_1 - 5)$ and

$$L_1(x_1) = x_1 \underbrace{\left(x_1^3 + x_1^2 + 3x_1 + 5\right)}_{q_0(x_1)} + \underbrace{4}_{r_0(x_1)}, \quad L_1(x_1) = x_1^2 \underbrace{\left(x_1^2 + x_1 + 3\right)}_{q_1(x_1)} + \underbrace{5x_1 + 4}_{r_1(x_1)},$$

$$L_1(x_1) = x_1^3 \underbrace{(x_1 + 1)}_{q_2(x_1)} + \underbrace{3x_1^2 + 5x_1 + 4}_{r_2(x_1)}, \qquad L_1(x_1) = x_1^4 \underbrace{(1)}_{q_3(x_1)} + \underbrace{x^3 + 3x_1^2 + 5x_1 + 4}_{r_3(x_1)}.$$

Then we have the following duals of $C(\mathcal{S}, a)$ for $a \in A$:

$$\begin{aligned} C(\mathcal{S}, 0)^{\perp} &= \operatorname{Span}_K \{\operatorname{Res}_{\mathcal{S}} q_1, \operatorname{Res}_{\mathcal{S}} q_2, \operatorname{Res}_{\mathcal{S}} q_3\}, \\ C(\mathcal{S}, 1)^{\perp} &= \operatorname{Span}_K \{\operatorname{Res}_{\mathcal{S}} q_0, \operatorname{Res}_{\mathcal{S}} q_2, \operatorname{Res}_{\mathcal{S}} q_3\}, \\ C(\mathcal{S}, 2)^{\perp} &= \operatorname{Span}_K \{\operatorname{Res}_{\mathcal{S}} q_0, \operatorname{Res}_{\mathcal{S}} q_1, \operatorname{Res}_{\mathcal{S}} q_3\}, \\ C(\mathcal{S}, 3)^{\perp} &= \operatorname{Span}_K \{\operatorname{Res}_{\mathcal{S}} q_0, \operatorname{Res}_{\mathcal{S}} q_1, \operatorname{Res}_{\mathcal{S}} q_2\}. \end{aligned}$$

Example 2.6. Let $K = \mathbb{F}_7$. Consider the Cartesian set: $\mathcal{S} = \{0, 2, 3\} \times \{0, 1, 3, 5, 6\} \subseteq K^2$. In this case, $L_1(x_1) = x_1(x_1 - 2)(x_1 - 3)$ and $L_2(x_2) = x_2(x_2 - 1)(x_2 - 3)(x_2 - 5)(x_2 - 6)$. Then we have

$$L_1(x_1) = x_1 \underbrace{\left(x_1^2 + 2x_1 + 6\right)}_{q_{1,0}(x_1)} + \underbrace{0}_{r_{1,0}(x_1)}, \quad L_2(x_2) = x_2 \underbrace{\left(x_2^4 + 6x_2^3 + x_2 + 6\right)}_{q_{2,0}(x_2)} + \underbrace{0}_{r_{2,0}(x_2)},$$

$$L_1(x_1) = x_1^2 \underbrace{(x_1 + 2)}_{q_{1,1}(x_1)} + \underbrace{6x_1}_{r_{1,1}(x_1)}, \qquad L_2(x_2) = x_2^2 \underbrace{\left(x_2^3 + 6x_2^2 + 1\right)}_{q_{2,1}(x_2)} + \underbrace{6x_2}_{r_{2,1}(x_2)},$$

$$L_1(x_1) = x_1^3 \underbrace{(1)}_{q_{1,2}(x_1)} + \underbrace{2x_1^2 + 6x_1}_{r_{1,2}(x_1)}, \qquad L_2(x_2) = x_2^3 \underbrace{\left(x_2^2 + 6x_2\right)}_{q_{2,2}(x_2)} + \underbrace{x_2^2 + 6x_2}_{r_{2,2}(x_2)},$$

$$L_2(x_2) = x_2^4 \underbrace{(x_2 + 6)}_{q_{2,3}(x_2)} + \underbrace{x_2^2 + 6x_2}_{r_{2,3}(x_2)},$$

$$L_2(x_2) = x_2^5 \underbrace{(1)}_{q_{2,4}(x_2)} + \underbrace{6x_2^4 + x_2^2 + 6x_2}_{r_{2,4}(x_2)}.$$

Then, the dual of $C(\mathcal{S}, \boldsymbol{a})$ for $\boldsymbol{a} = (2, 3)$ is given by

$$C(\mathcal{S}, (2,3))^{\perp} = \operatorname{Span}_K \{\operatorname{Res}_{\mathcal{S}} Q_{\boldsymbol{b}} : b \in \{0, 1, 2\} \times \{0, 1, 2, 3, 4\}, b \neq (2, 3)\}.$$

In other words, we take the residue of all the products $q_{1,i} q_{2,j}$ except when (i, j) is the given point $(2, 3)$.

Theorem 2.7. *Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq K^m$ and $B = \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\} \subseteq \mathbb{Z}^m$. For any $A \subseteq B$, the set $\{\mathrm{Res}_{\mathcal{S}}\, Q_{\boldsymbol{b}} : \boldsymbol{b} \in B \setminus A\}$ forms a basis for the dual $C(\mathcal{S}, A)^{\perp}$ of the monomial-Cartesian code $C(\mathcal{S}, A)$.*

Proof. As for any two points $\boldsymbol{a}_1, \boldsymbol{a}_2 \in A$ we have that $C(\mathcal{S}, \{\boldsymbol{a}_1, \boldsymbol{a}_2\})^{\perp} = C(\mathcal{S}, \boldsymbol{a}_1)^{\perp} \cap C(\mathcal{S}, \boldsymbol{a}_2)^{\perp}$, the result is a consequence of Lemma 2.4. □

Example 2.8. Let $K = \mathbb{F}_7$ and assume $\mathcal{S} = \{1, 3, 4, 5\} \subseteq K$ as in Example 2.5. As before we have $L_1(x_1) = (x_1 - 1)(x_1 - 3)(x_1 - 4)(x_1 - 5)$ and

$$L_1(x_1) = x_1 \underbrace{\left(x_1^3 + x_1^2 + 3x_1 + 5\right)}_{q_0(x_1)} + \underbrace{4}_{r_0(x_1)}, \quad L_1(x_1) = x_1^2 \underbrace{\left(x_1^2 + x_1 + 3\right)}_{q_1(x_1)} + \underbrace{5x_1 + 4}_{r_1(x_1)},$$

$$L_1(x_1) = x_1^3 \underbrace{(x_1 + 1)}_{q_2(x_1)} + \underbrace{3x_1^2 + 5x_1 + 4}_{r_2(x_1)}, \qquad L_1(x_1) = x_1^4 \underbrace{(1)}_{q_3(x_1)} + \underbrace{x^3 + 3x_1^2 + 5x_1 + 4}_{r_3(x_1)}.$$

Then we obtain the following dual codes:

$$\begin{aligned} C(\mathcal{S}, \{2, 3\})^{\perp} &= \mathrm{Span}_K \left\{\mathrm{Res}_{\mathcal{S}}\, q_0, \mathrm{Res}_{\mathcal{S}}\, q_1\right\}, \\ C(\mathcal{S}, \{0, 2\})^{\perp} &= \mathrm{Span}_K \left\{\mathrm{Res}_{\mathcal{S}}\, q_1, \mathrm{Res}_{\mathcal{S}}\, q_3\right\} \\ C(\mathcal{S}, \{1, 2, 3\})^{\perp} &= \mathrm{Span}_K \left\{\mathrm{Res}_{\mathcal{S}}\, q_0\right\}. \end{aligned}$$

Example 2.9. Let $K = \mathbb{F}_7$. Consider the following Cartesian set: $\mathcal{S} = \{0, 2, 3\} \times \{0, 1, 3, 5, 6\} \subseteq K^2$. On this case $L_1(x_1) = x_1(x_1 - 2)(x_1 - 3)$ and $L_2(x_2) = x_2(x_2 - 1)(x_2 - 3)(x_2 - 5)(x_2 - 6)$. We have

$$L_1(x_1) = x_1 \underbrace{\left(x_1^2 + 2x_1 + 6\right)}_{q_{1,0}(x_1)} + \underbrace{0}_{r_{1,0}(x_1)}, \quad L_2(x_2) = x_2 \underbrace{\left(x_2^4 + 6x_2^3 + x_2 + 6\right)}_{q_{2,0}(x_2)} + \underbrace{0}_{r_{2,0}(x_2)},$$

$$L_1(x_1) = x_1^2 \underbrace{(x_1 + 2)}_{q_{1,1}(x_1)} + \underbrace{6x_1}_{r_{1,1}(x_1)}, \qquad L_2(x_2) = x_2^2 \underbrace{\left(x_2^3 + 6x_2^2 + 1\right)}_{q_{2,1}(x_2)} + \underbrace{6x_2}_{r_{2,1}(x_2)},$$

$$L_1(x_1) = x_1^3 \underbrace{(1)}_{q_{1,2}(x_1)} + \underbrace{2x_1^2 + 6x_1}_{r_{1,2}(x_1)}, \qquad L_2(x_2) = x_2^3 \underbrace{\left(x_2^2 + 6x_2\right)}_{q_{2,2}(x_2)} + \underbrace{x_2^2 + 6x_2}_{r_{2,2}(x_2)},$$

$$L_2(x_2) = x_2^4 \underbrace{(x_2 + 6)}_{q_{2,3}(x_2)} + \underbrace{x_2^2 + 6x_2}_{r_{2,3}(x_2)},$$

$$L_2(x_2) = x_2^5 \underbrace{(1)}_{q_{2,4}(x_2)} + \underbrace{6x_2^4 + x_2^2 + 6x_2}_{r_{2,4}(x_2)}.$$

Then, the dual of the code $C(\mathcal{S}, \{(0, 1), (3, 5)\})$ is given by

$$C(\mathcal{S}, \{(0, 1), (3, 5)\})^{\perp} = \mathrm{Span}_K \left\{\mathrm{Res}_{\mathcal{S}}\, Q_{\boldsymbol{b}} : b \in \{0, 1, 2\} \times \{0, 1, 2, 3, 4\}, b \notin \{(0, 1), (3, 5)\}\right\}.$$

In other words, we take the residue of all the products $q_{1,i} q_{2,j}$ except when (i, j) is either $(0, 1)$ or $(3, 5)$.

3. Quantum error correcting codes

In this section, we give some applications of monomial-Cartesian codes to quantum error correcting codes. Our main result shows how to use monomial-Cartesian codes to find quantum error correction codes and MDS quantum error correction codes. We continue using the same notation as in the previous sections, in particular $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq K^m$, $n_i := |S_i|$, $A \subseteq \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\}$, and $\mathcal{L}(A) = \mathrm{Span}_K\{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in A\} \subseteq R$.

We start by showing the multiplicative property of the minimum distance of a monomial-Cartesian code. A particular case of this result appears in [35, Theorem 2.1]. Also, it can be derived from [42, Theorem 3 (c)]. We give a proof along the lines of the proof of [35, Theorem 2.1].

Proposition 3.1. *Let $C(\mathcal{S}_1, A)$ and $C(\mathcal{S}_2, B)$ be monomial-Cartesian codes and consider their direct product $C(\mathcal{S}_1 \times \mathcal{S}_2, A \times B)$. Then*

$$\delta\left(C(\mathcal{S}_1 \times \mathcal{S}_2, A \times B)\right) = \delta\left(C(\mathcal{S}_1, A)\right)\delta\left(C(\mathcal{S}_2, B)\right).$$

Proof. We set $R = K[x_1, \ldots, x_{m_1}, y_1, \ldots, y_{m_2}]$, $A \subseteq \mathbb{Z}^{m_1}$, $B \subseteq \mathbb{Z}^{m_2}$, and identify the elements of $\mathcal{L}(A)$ and $\mathcal{L}(B)$ with polynomials in R depending only on $\boldsymbol{x} = (x_1, \ldots, x_{m_1})$ and $\boldsymbol{y} = (y_1, \ldots, y_{m_2})$, respectively.

Let δ_1 and δ_2 denote the minimum weights of $C(\mathcal{S}_1, A)$ and $C(\mathcal{S}_2, B)$, respectively. Furthermore, let $f_1 \in \mathcal{L}(A)$ and $f_2 \in \mathcal{L}(B)$ be polynomials such that the corresponding codewords $\mathrm{ev}_{\mathcal{S}_1}(f_1)$ and $\mathrm{ev}_{\mathcal{S}_2}(f_2)$ have weights δ_1 and δ_2, respectively. By definition, the product $f' = f_1 f_2$ lies in $\mathcal{L}(A \times B)$. Also, for any $(\boldsymbol{s}_1, \boldsymbol{s}_2) \in \mathcal{S}_1 \times \mathcal{S}_2$ we have

$$f'(\boldsymbol{s}_1, \boldsymbol{s}_2) = f_1(\boldsymbol{s}_1) f_2(\boldsymbol{s}_2),$$

which is non-zero if and only if both $f_1(\boldsymbol{s}_1)$ and $f_2(\boldsymbol{s}_2)$ are non-zero. This implies that $\mathrm{ev}_{\mathcal{S}_1 \times \mathcal{S}_2}(f')$ has weight $\delta_1\delta_2$.

It remains to show that the weight of $\mathrm{ev}_{\mathcal{S}_1 \times \mathcal{S}_2}(f)$ is at least $\delta_1\delta_2$ for an arbitrary non-zero $f \in \mathcal{L}(A \times B)$. By definition, any non-zero $f \in \mathcal{L}(A \times B)$ can be written as

$$f(\boldsymbol{x}, \boldsymbol{y}) = \sum_{\boldsymbol{b} \in B} f_{\boldsymbol{b}}(\boldsymbol{x}) \boldsymbol{y}^{\boldsymbol{b}},$$

where $f_{\boldsymbol{b}}$ are polynomials in $\mathcal{L}(A)$ at least one of which is non-zero. Let $\mathcal{S} \subseteq \mathcal{S}_1$ be the subset of those $\boldsymbol{s}$ for which $f_{\boldsymbol{b}}(\boldsymbol{s}) \neq 0$ for at least one $\boldsymbol{b} \in B$. Given $\boldsymbol{s} \in \mathcal{S}$, $f(\boldsymbol{s}, \boldsymbol{y})$ is a non-zero polynomial in $\mathcal{L}(B)$ and, hence, the corresponding codeword $\mathrm{ev}_{\mathcal{S}_2} f(\boldsymbol{s}, \boldsymbol{y})$ has weight at least δ_2. Therefore, the weight of $\mathrm{ev}_{\mathcal{S}_1 \times \mathcal{S}_2} f(\boldsymbol{x}, \boldsymbol{y})$ is at least $|\mathcal{S}| \cdot \delta_2$. On the other hand, the number of $\boldsymbol{s} \in \mathcal{S}$ cannot be less than the weight of each $\mathrm{ev}_{\mathcal{S}_1}(f_{\boldsymbol{b}})$. Therefore, $|\mathcal{S}| \geq \delta_1$, which completes the proof of the above statement.

□

We remark that there is also an inductive lower bound for $\delta\left(C(\mathcal{S}, A)\right)$ in terms minimum weights of monomial-Cartesian codes corresponding to projections and fibers of A along coordinate subspaces. It is stated in [36, Theorem 4.1] in the case of generalized toric codes, but the statement and the proof can be easily adapted to arbitrary monomial-Cartesian codes.

Next, we provide a slightly different representation for the dual of a monomial-Cartesian code.

Definition 3.2. Let $F(\boldsymbol{x})$ be the unique element in R such that $\deg_{x_i} F(\boldsymbol{x}) < n_i$ and $F(\boldsymbol{s}) = \left(\prod_{i=1}^{m} \prod_{s_i' \in S_i \setminus \{s_i\}} (s_i - s_i')\right)^{-1}$ for every $\boldsymbol{s} = (s_1, \ldots, s_m) \in \mathcal{S}$.

Observe that the polynomial $F(\boldsymbol{x})$ can be found using interpolation:

$$F(\boldsymbol{x}) = \sum_{(s_1,\ldots,s_m)\in\mathcal{S}} \frac{\prod_{i=1}^{m} \prod_{s_i' \in S_i \setminus \{s_i\}} (x_i - s_i')}{\left(\prod_{i=1}^{m} \prod_{s_i' \in S_i \setminus \{s_i\}} (s_i - s_i')\right)^2}.$$

Theorem 3.3. *Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq K^m$ and $B = \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\} \subseteq \mathbb{Z}^m$. Let $F(\boldsymbol{x})$ be as defined in Definition 3.2. For any $A \subseteq B$, the set $\{\mathrm{ev}_{\mathcal{S}}(FQ_{\boldsymbol{b}}) : \boldsymbol{b} \in B \setminus A\}$ forms a basis for the dual $C(\mathcal{S}, A)^{\perp}$ of the monomial-Cartesian code $C(\mathcal{S}, A)$.*

Proof. Because the definition of $F(\boldsymbol{x})$ and $\mathrm{Res}_{\mathcal{S}} Q_{\boldsymbol{b}}$, it is clear that $\mathrm{Res}_{\mathcal{S}} Q_{\boldsymbol{b}} = \mathrm{ev}_{\mathcal{S}}(FQ_{\boldsymbol{b}})$. □

Lemma 3.4. *Let $f_1, \ldots, f_k, g_1, \ldots, g_\ell \in \mathcal{L}(A)$. Then $\mathrm{Span}_K\{\mathrm{ev}_{\mathcal{S}}(f_1), \ldots, \mathrm{ev}_{\mathcal{S}}(f_k)\} \subseteq \mathrm{Span}_K\{\mathrm{ev}_{\mathcal{S}}(g_1), \ldots, \mathrm{ev}_{\mathcal{S}}(g_\ell)\}$ if and only if $\mathrm{Span}_K\{f_1, \ldots, f_k\} \subseteq \mathrm{Span}_K\{g_1, \ldots, g_\ell\}$.*

Proof. This is a consequence of the fact that the evaluation function $\mathrm{ev}_{\mathcal{S}}$ is injective. □

Using the previous result we can give conditions for when a monomial-Cartesian code is self-orthogonal or LCD. An important application of LCD codes can be found in [9].

Theorem 3.5. *Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq K^m$ and $A \subseteq B = \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\} \subseteq \mathbb{Z}^m$. Let $F(\boldsymbol{x})$ be as defined in Definition 3.2. Then*
(a) *$C(\mathcal{S}, A)^{\perp} \subseteq C(\mathcal{S}, A)$ if and only if $\mathrm{Span}_K\left\{\overline{FQ_{\boldsymbol{b}}} : \boldsymbol{b} \in B \setminus A\right\} \subseteq \mathrm{Span}_K\left\{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in A\right\}$.*
(b) *$C(\mathcal{S}, A)$ is LCD if and only if $\mathrm{Span}_K\left\{\overline{FQ_{\boldsymbol{b}}} : \boldsymbol{b} \in B \setminus A\right\} \bigcap \mathrm{Span}_K\left\{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in A\right\} = 0$.*
Here, $\overline{FQ_{\boldsymbol{b}}}$ denotes the normal form of the polynomial $FQ_{\boldsymbol{b}}$ with respect to the Gröbner basis $\{L_1(x_1), \ldots, L_m(x_m)\}$.

Proof. The result is a consequence of Lemma 3.4 and Theorem 3.3. □

Next, we describe some properties for the polynomial $F(\boldsymbol{x})$ in order to find conditions that satisfy part (a) from Theorem 3.5.

Proposition 3.6. *If $q > n_i \geq q/2$ for all $i \in [m]$, then $\deg_{x_i}(F(\boldsymbol{x})) \leq q - n_i$.*

Proof. Define

$$F'(\boldsymbol{x}) := \frac{\prod_{i=1}^{m} \prod_{s_i' \in K \setminus S_i} (x_i - s_i')}{(-1)^m}.$$

Observe that if $\boldsymbol{s} = (s_1, \ldots, s_m) \in \mathcal{S}$, then

$$F'(\boldsymbol{s}) = \frac{\prod_{s_i' \in K \setminus S_i} (s_1 - s_i')}{-1} \cdots \frac{\prod_{s_i' \in K \setminus S_i} (s_m - s_i')}{-1} = \left(\prod_{i=1}^{m} \prod_{s_i' \in S_i \setminus \{s_i\}} (s_i - s_i')\right)^{-1}.$$

The last equality is true because for every $i \in [m]$ we have $-1 = \prod_{s_i' \in K \setminus \{s_i\}} (s_i - s_i')$. If $n_i > q/2$, then $\deg_{x_i} F'(\boldsymbol{x}) = q - n_i < n_i$. Thus $F(\boldsymbol{x}) = F'(\boldsymbol{x})$, because $F(\boldsymbol{x}) - F'(\boldsymbol{x}) \in I(\mathcal{S})$. If $n_i = q/2$, then defining F by interpolation we get $\deg_{x_i} F < n_i = q - n_i$. □

The following theorem gives a path for constructing quantum and MDS quantum codes.

Theorem 3.7. *Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq K^m$ such that $q > n_i = |S_i| \geq q/2$ for all $i \in [m]$. For every $\boldsymbol{t} = (t_1, \ldots, t_m) \in \{0, \ldots, n_1 - \lceil \frac{q}{2} \rceil\} \times \cdots \times \{0, \ldots, n_m - \lceil \frac{q}{2} \rceil\} \subseteq \mathbb{Z}^m$, define the set $A_{\boldsymbol{t}} = \{0, \ldots, n_1 - 1 - t_1\} \times \cdots \times \{0, \ldots, n_m - 1 - t_m\}$. Then $C(\mathcal{S}, A_{\boldsymbol{t}})^{\perp} \subseteq C(\mathcal{S}, A_{\boldsymbol{t}})$.*

Proof. Define $B = \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_m - 1\} \subseteq \mathbb{Z}^m$ and take $\boldsymbol{b} \in B \setminus A_{\boldsymbol{t}}$. By Theorem 3.5 (a) we just need to check that $\overline{FQ_{\boldsymbol{b}}} \in \mathrm{Span}_K \{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in A_{\boldsymbol{t}}\}$. By definition, $Q_{\boldsymbol{b}}(\boldsymbol{x}) = \prod_{i=1}^m q_{i,b_i}(x_i)$, where $L_i(x_i) = x_i^{b_i+1} q_{i,b_i}(x_i) + r_{i,b_i}(x_i)$. It means $q_{i,b_i}(x_i) \in \mathrm{Span}_K \{1, \ldots, x_i^{n_i - b_i - 2}\}$. As $\boldsymbol{b} \in B \setminus A_{\boldsymbol{t}}$, $n_i - 1 - t_i < b_i$; thus, $n_i - b_i - 2 < t_i - 1$. We obtain $\deg q_{i,b_i}(x_i) < t_i - 1$. By Proposition 3.6, $\deg_{x_i}(F(\boldsymbol{x})) \leq q - n_i$. Thus $\deg_{x_i} FQ_{\boldsymbol{b}} < q - n_i + t_i - 1 \leq n_i - 1 - t_i$. The last inequality holds because $t_i \leq n_i - \lceil \frac{q}{2} \rceil$ and it follows that $\overline{FQ_{\boldsymbol{b}}} = FQ_{\boldsymbol{b}} \in \mathrm{Span}_K \{\boldsymbol{x}^{\boldsymbol{a}} : \boldsymbol{a} \in A_{\boldsymbol{t}}\}$. □

Now we state an important result on constructing stabilizer codes. We recall that a quantum code is *pure to* a natural number d if its stabilizer group does not contain non-scalar matrices of weight less than d. A quantum code is called *pure* if it is pure to its minimum distance. For more information about quantum codes see [26] and references therein.

Lemma 3.8. [1, Lemma 17] *If there exists a classical linear $[n, k, d]_q$ code C such that $C^{\perp} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code that is pure to d. If the minimum distance of $C^{\perp}$ exceeds d, then the stabilizer code is pure and has minimum distance d.*

Theorem 3.9. *Let $\mathcal{S} = S_1 \times \cdots \times S_m \subseteq K^m$ such that $q > n_i = |S_i| \geq q/2$ for all $i \in [m]$. For every $\boldsymbol{t} = (t_1, \ldots, t_m) \in \{0, \ldots, n_1 - \lceil \frac{q}{2} \rceil\} \times \cdots \times \{0, \ldots, n_m - \lceil \frac{q}{2} \rceil\} \subseteq \mathbb{Z}^m$ there exists an $[[\prod_{i=1}^m n_i, 2\prod_{i=1}^m (n_i - t_i) - n, \prod_{i=1}^m (t_i + 1)]]_q$ stabilizer code that is pure to $t_1 \cdots t_m$.*

Proof. The idea is to apply Lemma 3.8 to Theorem 3.7. By Theorem 3.7 we have that for $A_{\boldsymbol{t}} = \{0, \ldots, n_1 - 1 - t_1\} \times \cdots \times \{0, \ldots, n_m - 1 - t_m\}$, $C(\mathcal{S}, A_{\boldsymbol{t}})^{\perp} \subseteq C(\mathcal{S}, A_{\boldsymbol{t}})$. It is clear that the length and dimension of $C(\mathcal{S}, A_{\boldsymbol{t}})$ are given by n and $\prod_{i=1}^m (n_i - t_i)$, respectively. Finally, the minimum distance comes from Proposition 3.1. □

The previous result gives a very simple path to prove the existence of quantum error correcting codes with certain parameters.

Example 3.10. Let $K = \mathbb{F}_{49}$ and take $n_1 = 35, n_2 = 40, t_1 = 5$ and $t_2 = 8$. By Theorem 3.9 we have that there exist the following quantum error correcting codes: $[[35, 25, 6]]_{49}$, $[[40, 24, 9]]_{49}$ and $[[1400, 520, 54]]_{49}$.

Observe that the first two of the previous examples are quantum MDS codes. Actually, it is possible to prove the existence of more of them.

Corollary 3.11. *For every $q > n \geq q/2$ and every $0 \leq t \leq n - \lceil \frac{q}{2} \rceil$ there exists an MDS quantum code $[[n, n-2t, t+1]]_q$.*

Proof. This is the particular case of Theorem 3.9 when $m = 1$. □

Using Theorem 3.9 is straightforward to find quantum error correcting codes with length larger than q.

Example 3.12. Let $K = \mathbb{F}_{121}$ and take $n_1 = 80, n_2 = 90, t_1 = 19$ and $t_2 = 29$. By Theorem 3.9 we have that there exist the following quantum error correcting codes: $[[80, 42, 20]]_{121}$, $[[90, 32, 30]]_{121}$ and $[[7200, 242, 600]]_{121}$.

4. Local properties of direct products

Local properties for linear codes have been studied extensively in the context of distributed storage. The idea is that every coordinate of a linear code can be used to save the information of a server, so n servers store a linear code of length n. Informally speaking, a linear code is said to have locality r if for all elements of the code, every coordinate i is a function of other r coordinates. It is important to remark that the set of these r coordinates depend on i, but not on the codeword. In terms of distributed storage, locality r means that if one of the n servers fails, then the information of the failed server can be recovered by accessing r other servers (rather than $n-1$). If one of these r servers also fails, local recovery might not be possible. For that reason it is useful to have availability. A linear code with availability t means that every coordinate can be recovered from t pairwise disjoint sets. Formal definitions follow.

Definition 4.1. A linear code C of length n over K is a *locally recoverable code* with locality r if for every position $i \in [n]$ there exist a set $\mathcal{R}_i \subseteq [n] \setminus \{i\}$ and a function $\phi_i : K^r \to K$ such that $|\mathcal{R}_i| = r$ and for all $c = (c_1, \ldots, c_n)$ in C, $c_i = \phi_i(c\ |_{\mathcal{R}_i})$. This definition represents that every coordinate c_i for any codeword c can be recovered by the coordinates c_j, where $j \in \mathcal{R}_i$. The set $\mathcal{R}_i$ is called a *recovery set* for the i-th position.

Definition 4.2. A linear code C is said to have *t-availability* with locality $(r_1, \ldots, r_t)$ if every position $i \in [n]$ has t pairwise disjoint recovery sets $\mathcal{R}_{i1}, \ldots, \mathcal{R}_{it}$ with $|\mathcal{R}_{ij}| = r_j$, for $j \in [t]$.

Lemma 4.3. *Let $C(\mathcal{S}_1, A)$ and $C(\mathcal{S}_2, B)$ be locally recoverable monomial-Cartesian codes with localities r_1 and r_2, respectively. The direct product $C(\mathcal{S}_1 \times \mathcal{S}_2, A \times B)$ has 2-availability with locality (r_1, r_2).*

Proof. Observe that the coordinates of a monomial-Cartesian code are indexed by the elements of the Cartesian product, for this reason every position will be given in terms of the elements of the Cartesian product. Let $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ be elements of $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively. Let $\mathcal{R}_{\boldsymbol{s}_1}$ be a recovery set for $\boldsymbol{s}_1$ of cardinality r_1 and $\mathcal{R}_{\boldsymbol{s}_2}$ a recovery set for $\boldsymbol{s}_2$ of cardinality r_2, which exist because $C(\mathcal{S}_1, A)$ and $C(\mathcal{S}_2, B)$ are locally recoverable monomial-Cartesian codes with locality r_1 and r_2, respectively. In the code $C(\mathcal{S}_1 \times \mathcal{S}_2, A \times B)$, we claim the position $(\boldsymbol{s}_1, \boldsymbol{s}_2)$ has recovery sets $\mathcal{R}_{\boldsymbol{s}_1} \times \{\boldsymbol{s}_2\}$ and $\{\boldsymbol{s}_1\} \times \mathcal{R}_{\boldsymbol{s}_2}$.

Let c be an element of $C(\mathcal{S}_1 \times \mathcal{S}_2, A \times B)$. By definition of the direct product, there is a polynomial $f(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{L}(A \times B) \subseteq K[x_1, \ldots, x_{m_1}, y_1, \ldots, y_{m_2}]$ such that $c = (f(\boldsymbol{s}, \boldsymbol{s}'))|_{(\boldsymbol{s},\boldsymbol{s}') \in \mathcal{S}_1 \times \mathcal{S}_2}$. As $f(\boldsymbol{x}, \boldsymbol{s}_2) \in \mathcal{L}(A) \subseteq K[x_1, \ldots, x_{m_1}]$, we can use the set $\{f(\boldsymbol{s}, \boldsymbol{s}_2) \mid \boldsymbol{s} \in \mathcal{R}_{\boldsymbol{s}_1}\}$ to recover the value $f(\boldsymbol{s}_1, \boldsymbol{s}_2)$. Thus $\mathcal{R}_{\boldsymbol{s}_1} \times \{\boldsymbol{s}_2\}$ is a recovery set for $(\boldsymbol{s}_1, \boldsymbol{s}_2)$. In analogous way, $\{\boldsymbol{s}_1\} \times \mathcal{R}_{\boldsymbol{s}_2}$ is a second recovery set for the same position $(\boldsymbol{s}_1, \boldsymbol{s}_2)$. □

We come to the main result of this section, which shows how locally recoverable monomial-Cartesian codes give rise to codes with availability.

Theorem 4.4. *Let $C(\mathcal{S}_1, A_1), \ldots, C(\mathcal{S}_t, A_t)$ be locally recoverable monomial-Cartesian codes with localities $r_1, \ldots, r_t$, respectively. The direct product $C(\mathcal{S}_1 \times \cdots \times \mathcal{S}_t, A_1 \times \cdots \times A_t)$ has t-availability with locality $(r_1, \ldots, r_t)$.*

Proof. This is a consequence of Lemma 4.3 because the product of two monomial-Cartesian codes is again a monomial-Cartesian code. □

Remark 4.5. As a corollary of Theorem 4.4 we obtain the family of codes obtained in [38, Construction 4], which are direct products of sub-codes of Reed-Solomon codes.

References

[1] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, On quantum and classical BCH codes, IEEE Trans. Inf. Theory **53** (2007), no. 3, 1183–1188.

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

[3] M. Bras-Amorós and M. E. O'Sullivan, Duality for some families of correction capability optimized evaluation codes, Adv. Math. Commun **2** (2008), no.1, 15–33.

[4] S. Bulygin, R. Pellikaan, Bounded distance decoding of linear error-correcting codes with Gröbner bases. Journal of Symbolic Computation **44** (2009), 1626–1643.

[5] S. Bulygin, R. Pellikaan, Decoding and finding the minimum distance with Gröbner bases : history and new insights. In Series on Coding Theory and Cryptology vol. 7. Selected Topics in Information and Coding Theory, I. Woungang, S. Misra and S.C. Misra, Eds., World Scientific **7** (2010), 585–622.

[6] S. Bulygin, R. Pellikaan, Decoding error-correcting codes with Gröbner bases. Proceedings of the 28-th Symposium on Information Theory in the Benelux, WIC 2007, R. Veldhuis, H. Cronie, H. Hoeksema, Eds., Enschede, May 24-25, (2007), 3–10.

[7] S. Bulygin, R. Pellikaan, Decoding linear error-correcting codes up to half the minimum distance with Gröbner bases. In Gröbner Bases, Coding, and Cryptography, M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso Eds., Springer, Berlin, (2009), 361–365.

[8] A. R. Calderbank, P. W. Shor, Good quantum error-correcting codes exist, Physical Review A **54** (1996), 1098–1105.

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

[10] 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.

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

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

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

[14] C. Carvalho, V. G. Neumann, H. H. López, Projective Nested Cartesian Codes, Bull Braz Math Soc, New Series **48** (2017), 283–302.
[15] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, Third Edition, 2008.
[16] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, 1995.
[17] J. Farr and S. Gao, Gröbner bases, Padé approximation, and decoding of linear codes, Coding Theory and Quantum Computing, Contemporary Mathematics, Amer. Math. Soc., Providence, RI **381** (2005), 3–18.
[18] C. Galindo, O. Geil, F. Hernando, D. Ruano, On the distance of stabilizer quantum codes from J-affine variety codes, Quantum Information Processing **16** (2017), no. 4.
[19] C. Galindo, F. Hernando, D. Ruano, Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement, Quantum Information Processing **14** (2015), no. 9.
[20] O. Geil, C. Thomsen, Weighted Reed-Muller codes revisited, Designs, Codes and Cryptography **66** (2013), no. 1–3, 195–220.
[21] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed-Muller-type codes over the Segre variety, Finite Fields and Their Applications **8** (2002), no. 4, 511–518.
[22] J. Harris, *Algebraic Geometry. A first course*, Graduate Texts in Mathematics **133**, Springer-Verlag, New York, 1992.
[23] J. P. Hansen, Toric Surfaces and Error-correcting Codes, Coding Theory, Cryptography and Related Areas, Springer, Berlin, Heidelberg, 132–142.
[24] W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
[25] D. Joyner, Toric codes over finite fields, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79.
[26] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary Stabilizer Codes over Finite Fields, IEEE Transactions on Information Theory **52** (2006), no. 11, 4892–4914.
[27] H. H. López, F. Manganiello, G. L. Matthews, Affine Cartesian codes with complementary duals, Finite Fields and Their Applications **57** (2019), 13–28.
[28] H. H. López, C. Rentería-Márquez, R. H. Villarreal, Affine Cartesian codes, Designs, Codes and Cryptography **71** (2014), no. 1, 5–19.
[29] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1977.
[30] James L. Massey, Linear codes with complementary duals, Discrete Mathematics **106–107** (1992), 337–342.
[31] C. Rentería and H. Tapia-Recillas, Reed-Muller codes: an ideal theory approach, Comm. Algebra **25** (1997), no. 2, 401–413.
[32] C. Munuera, Locally Recoverable Codes with Local Error Detection, `https://arxiv.org/pdf/1812.00834.pdf`.
[33] D. Ruano, On the structure of generalized toric codes, J. Symbolic Comput. **44** (2009), no. 5, 499–506.
[34] I. Soprunov, J. Soprunova, Toric surface codes and Minkowski length of polygons, SIAM J. Discrete Math. **23** (2009), no. 1, 384–400.
[35] I. Soprunov, J. Soprunova, Bringing Toric Codes to the Next Dimension, SIAM Journal on Discrete Mathematics **24** (2010), no. 2, 655–665.
[36] I. Soprunov, Lattice polytopes in coding theory, Journal of Algebra Combinatorics Discrete Structures and Applications **2** (2015), no. 2, 85–94.
[37] A. M. Steane, Multiple-particle interference and quantum error correction. Proc. Roy. Soc. London Ser. A **452** (1996), no. 1954, 2551–2577.
[38] I. Tamo, A. Barg, A Family of Optimal Locally Recoverable Codes, IEEE Transactions on Information Theory **60** (2014), no. 8, 4661–4676.

[39] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.
[40] J. H. van Lint, *Introduction to coding theory*, Third edition, Graduate Texts in Mathematics **86**, Springer-Verlag, Berlin, 1999.
[41] R. H. Villarreal, *Monomial Algebras*, second edition, Monographs and and Research notes in Mathematics, 2015.
[42] V. K. Wei, K. Yang, On the Generalized Hamming Weights of Product Codes, IEEE Transactions on Information Theory **30** (1993), no. 5, 1079–1713.

(Hiram H. López) Department of Mathematics, Cleveland State University, Cleveland, OH USA
E-mail address: h.lopezvaldez@csuohio.edu

(Gretchen L. Matthews) Department of Mathematics, Virginia Tech, Blacksburg, VA USA
E-mail address: gmatthews@vt.edu

(Ivan Soprunov) Department of Mathematics, Cleveland State University, Cleveland, OH USA
E-mail address: i.soprunov@csuohio.edu