Eduardo Camps, Hiram H. López, Gretchen L. Matthews, and Eliseo Sarmiento

Monomial-Cartesian codes closed under divisibility

...

DOI ..., Received ...; accepted ...

Abstract: A monomial-Cartesian code closed under divisibility is an evaluation code defined by a set of monomials that is closed under divisibility, evaluated over a Cartesian product. In this work we prove that the dual of a monomial-Cartesian code closed under divisibility is monomially equivalent to a code that belongs to this same family of codes. Then we describe the length, the dimension and the minimum distance of these codes in terms of the minimal generating set of monomials.

Keywords: Cartesian codes, monomial codes, monomial-Cartesian codes, decreasing codes

PACS: ...

Communicated by: ...
Dedicated to ...

1 Introduction

Evaluation codes form an important family of error-correcting codes, including Cartesian codes, algebraic geometry codes, and many variants finely tuned for specific applications, such as the locally recoverably codes defined by Tamo, Barg, and Vladut [11]. In this paper, we consider a particular class of evaluation codes,

Eduardo Camps, Escuela Superior de Física y Matemáticas , Instituto Politécnico Nacional, Mexico City, Mexico. ecfmd@hotmail.com
Hiram H. López, Department of Mathematics, Cleveland State University, Cleveland, OH USA. h.lopezvaldez@csuohio.edu
Gretchen L. Matthews, Department of Mathematics, Virginia Tech, Blacksburg, VA USA. gmatthews@vt.edu
Eliseo Sarmiento, Escuela Superior de Física y Matemáticas , Instituto Politécnico Nacional, Mexico City, Mexico. esarmiento@ipn.mx

called monomial-Cartesian code closed under divisibility. Monomial-Cartesian codes closed under divisibility generalize Reed-Solmon and Reed-Muller codes, as we will see.

A monomial-Cartesian code closed under divisibility is defined using the following concepts. Let $K := \mathbb{F}_q$ be a finite field with q elements and $R := K[x_1, \dots, x_m]$ be the polynomial ring over K in m variables. Let $\mathcal{M} \subseteq R$ be a set of monomials such that $M \in \mathcal{M}$ and M' divides M, then $M' \in \mathcal{M}$. We say that such a set is **closed under divisibility**. Let $L(\mathcal{M})$ be the subspace of polynomials of R that are K-linear combinations of monomials of $\mathcal{M}$:

$$L(\mathcal{M}) := \operatorname{Span}_K\{M : M \in \mathcal{M}\} \subseteq R.$$

Fix non-empty subsets $S_1, \dots, S_m$ of K. Define their **Cartesian product** as

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

In what follows, $n_i := |S_i|$, the cardinality of S_i for $i \in [m] := \{1, \dots, m\}$, and $n := |\mathcal{S}|$, the cardinality of $\mathcal{S}$. Fix a linear order on $\mathcal{S} = \{\boldsymbol{s}_1, \dots, \boldsymbol{s}_n\}$, $\boldsymbol{s}_1 \prec \cdots \prec \boldsymbol{s}_n$. We define the **evaluation map**

$$\begin{array}{rccc} \operatorname{ev}_{\mathcal{S}}\colon & L(\mathcal{M}) & \to & K^n \\ & f & \mapsto & (f(\boldsymbol{s}_1), \dots, f(\boldsymbol{s}_n)). \end{array}$$

From now on, we assume that the degree of each monomial $M \in \mathcal{M}$ in x_i is less than n_i. In this case the evaluation map $\operatorname{ev}_{\mathcal{S}}$ is injective, see [5, Proposition 2.1]. The **complement** of $\mathcal{M}$ in $\mathcal{S}$ denoted by $\mathcal{M}^c_{\mathcal{S}}$, is the set of all monomials in R that are not in $\mathcal{M}$ and their degree respect i is less than n_i.

Definition 1.1. If $\mathcal{M} \subseteq R$ is closed under divisibility, then the image $\operatorname{ev}_{\mathcal{S}}(L(\mathcal{M})) \subseteq K^n$ is called the **monomial-Cartesian code closed under divisibility** associated to $\mathcal{S}$ and $\mathcal{M}$. We denote it by $C(\mathcal{S}, \mathcal{M})$.

The length and the dimension of a monomial-Cartesian code $C(\mathcal{S}, \mathcal{M})$ are given by $n = |\mathcal{S}|$ and $k = \dim_K C(\mathcal{S}, \mathcal{M}) = |\mathcal{M}|$, respectively [5, Proposition 2.1]. Recall that the **minimum distance** of a code C is given by

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

where $\operatorname{Supp}(\boldsymbol{c})$ denotes the support of $\boldsymbol{c}$, that is the set of all non-zero entries of $\boldsymbol{c}$. Unlike the case of the length and the dimension, in general, there is no explicit formula for $\delta(C(\mathcal{S}, \mathcal{M}))$ in terms of $\mathcal{S}$ and $\mathcal{M}$.

The **dual** of a 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**) [8] if $C \cap C^{\perp} = \{\mathbf{0}\}$, and is called a **self-orthogonal** code if $C^{\perp} \subseteq C$.

Instances of monomial-Cartesian codes closed under divisibility for particular families of Cartesian products $\mathcal{S}$ and monomials sets that are closed under divisibility $\mathcal{M}$ have been previously studied in the literature. For example, a Reed-Muller code of order r in the sense of [12, p. 37] is monomial-Cartesian code closed under divisibility $C(K^m, M_r)$, where M_r is the set of monomials of degree less than r. An **affine Cartesian code** of order r is the monomial-Cartesian code closed under divisibility $C(\mathcal{S}, M_r)$. This family of affine Cartesian codes appeared first time in [4] and then independently in [6]. In [1], the authors studied the case when the finite field K is $\mathbb{F}_2$ and the set of monomials satisfy some decreasing conditions; then their results were generalized in [2] for $K = \mathbb{F}_q$ and monomials associated to curve kernels. The case when the set of monomials $\mathcal{M}$ is a tensor product, the minimum distance of the associated code can be computed using the same ideas that [9].

It is important to note that some families of monomial-Cartesian codes are not closed under divisibility. For instance, the family of codes given in [10], which is well-known for its applications to distributed storage, are not closed under divisibility because these are subcodes of Reed-Solomon codes where some monomials are omitted. To be precise, fix $r \geq 2$ with $r+1|n$. Set

$$V := \left\langle g(x)^j x^i : 0 \leq j \leq \frac{k}{r} - 1, 0 \leq i \leq r-1 \right\rangle$$

where $g(x) \in \mathbb{F}_q[x]$ has $\deg g = r+1$ and $\mathbb{F}_q = A_1 \dot{\cup} \cdots \dot{\cup} A_{\frac{n}{r+1}}$ with $|A_j| = r$ for all j so that $\forall \beta, \beta' \in A_j$,

$$g(\beta) = g(\beta').$$

Then $C(\mathbb{F}_q, V)$ is not closed under divisibility as $g(x)^j x^i \in V$ and x divides $g(x)^j x^i$ but $x \notin V$.

This notion of divisibility will be restricted to codes defined by sets of monomials as defined above. Recall that given a curve X over a finite field $\mathbb{F}$ and a divisor G on X, the space of rational functions associated with G, sometimes called the Riemann-Roch space of G, is

$$\mathcal{L}(G) := \{f \in \mathbb{F}(X) : (f) + G \geq 0\} \cup \{0\}$$

where (f) denotes the divisor of f. In general $\mathcal{L}(G)$ is not closed under divisibility, meaning $f \in \mathcal{L}(G)$ and $f = gh$ does not imply $g, h \in \mathcal{L}(G)$. For instance, if one considers the Hermitian curve X given by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$, then

$y \in \mathcal{L}((q+1)P_\infty)$. However, $y = x\frac{y}{x}$, but $\left(\frac{y}{x}\right) = (y) - (x) = qP_{00} - P_\infty - \sum_{b\neq 0} P_{0b} \not\geq -(q+1)P_\infty$. Hence, $\frac{y}{x} \notin \mathcal{L}((q+1)P_\infty)$.

In the next section we prove that the dual of a monomial-Cartesian code closed under divisibility is also a code of the same type. Then we describe its basic parameters in terms of the minimal generating set. For more information about coding theory we recommend [7, 13]. For algebraic concepts not described in this notes we suggest to the reader [14]. We close this section with a bit of notation that will be useful in the remainder of this paper. We will use $K^* := K \setminus \{0\}$ to denote the multiplicative group of K. Given a point $\boldsymbol{a} = (a_1, \ldots, a_m) \in \mathbb{Z}_{\geq 0}^m$, $\boldsymbol{x}^{\boldsymbol{a}}$ is the corresponding monomial in R; i.e. $\boldsymbol{x}^{\boldsymbol{a}} := x_1^{a_1} \cdots x_m^{a_m}$.

2 Basic parameters

In this section we continue with the same notation as in Section 1, in particular $\mathcal{M} \subseteq R$ is a set of monomials that is closed under divisibility, $\mathcal{S}$ represents a Cartesian set $\mathcal{S} = S_1 \times \cdots \times S_m$, $n_i = |S_i|$, for $i \in [m]$, $n = |\mathcal{S}|$ and $C(\mathcal{S}, \mathcal{M})$ represents the decreasing monomial-Cartesian code associated to $\mathcal{S}$ and $\mathcal{M}$.

A **monomial matrix** is a square matrix with exactly one nonzero entry in each row and column. Let C_1 and C_2 be codes of the same length over 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 with entries 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.

Definition 2.1. For $\boldsymbol{s} = (s_1, \ldots, s_m) \in \mathcal{S}$ and $f \in R$, define the **residue** of f at $\boldsymbol{s}$ as

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

and the **residues vector** of f at $\mathcal{S}$ as

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

Theorem 2.2. *The dual of the code $C(\mathcal{S}, \mathcal{M})$ is monomially equivalent to a monomial-Cartesian code closed under divisibility. Even more, the set*

$$\Delta := \left\{ \operatorname{Res}_{\mathcal{S}} \frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{M} : M \in \mathcal{M}^c \right\}$$

forms a basis for the dual $C(\mathcal{S},\mathcal{M})^{\perp}$, *meaning*

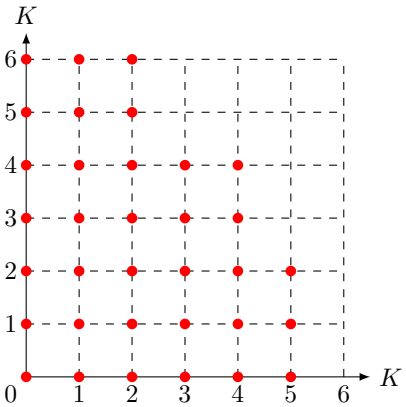
$$C(\mathcal{S},\mathcal{M})^{\perp} = \mathrm{Span}_K(\Delta).$$

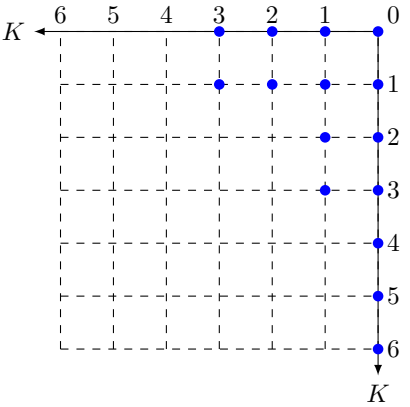
Proof. We start by proving that the set

$$\Delta' := \left\{ \frac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M} : M \in \mathcal{M}_{\mathcal{S}}^c \right\}$$

is closed under divisibility. Let $M \in \mathcal{M}_{\mathcal{S}}^c$ and $\boldsymbol{x^a}$ a divisor of $\frac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M}$. Then there exists a monomial $\boldsymbol{x^b}$ in R such that $\frac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M} = \boldsymbol{x^a x^b}$. As $M \in \mathcal{M}^c$ and $\mathcal{M}$ is closed under divisibility, then $\boldsymbol{x^b}M \in \mathcal{M}^c$ and $\boldsymbol{x^a} = \frac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{\boldsymbol{x^b}M} \in \Delta'$. This proves that the set Δ' is closed under divisibility. Due to [5, Theorem 2.7] and its proof, Δ is a basis for the dual $C(\mathcal{S},\mathcal{M})^{\perp}$. Finally, it is clear that $\mathrm{Span}_K\{\boldsymbol{c} : \boldsymbol{c} \in \Delta\}$ is monomially equivalent to $\mathrm{ev}_{\mathcal{S}}(\Delta')$, which is a monomial-Cartesian code closed under divisibility. □

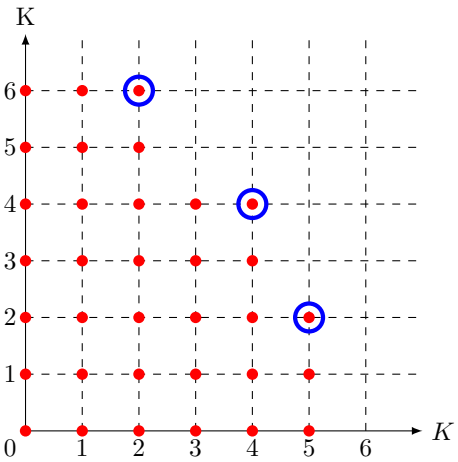
Example 2.3. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ the set of monomials of $K[x_1, x_2]$ whose exponents are the points in the left picture below. Then the code $C(\mathcal{S},\mathcal{M})$ is generated by the vectors $\mathrm{ev}_{\mathcal{S}}(M)$, where M is a monomial whose exponent is a point in the left picture below and the dual $C(\mathcal{S},\mathcal{M})^{\perp}$ is generated by the vectors $\mathrm{Res}_{\mathcal{S}}(M)$, where M is a monomial whose exponent is a point in the right picture below.





Definition 2.4. A subset $\mathcal{B}(\mathcal{M}) \subseteq \mathcal{M}$ is a **generating set** of $\mathcal{M}$ if for every $M \in \mathcal{M}$ there exists a monomial $B \in \mathcal{B}(\mathcal{M})$ such that M divides B. A generating set $\mathcal{B}(\mathcal{M})$ is called **minimal** if for every two elements $B_1, B_2 \in \mathcal{B}(\mathcal{M})$, B_1 does not divide B_2 and B_2 doesn't divide B_1.

Example 2.5. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ the set of monomials of $K[x_1, x_2]$ whose exponents are the points in the left picture of Example 2.3. The circles in the following picture are the exponents of the monomials that belong to the minimal generating set of $\mathcal{M}$.



From now on, $\mathcal{B}(\mathcal{M})$ denotes the minimal generating set of $\mathcal{M}$. We are going to describe properties of the code $C(\mathcal{S}, \mathcal{M})$ in terms of $\mathcal{B}(\mathcal{M})$. The following proposition says how to find a generating set of $\mathcal{M}^c_{\mathcal{S}}$ in terms of $\mathcal{B}(\mathcal{M})$.

Proposition 2.6. *Given a monomial* $M = x_1^{a_1} \cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})$, *define the monomials* $P(M) := \left\{ \dfrac{x_1^{n_1-1} \cdots x_n^{n_m-1}}{x_i^{a_i-1}} : i \in [m], \text{ and } n_i - a_i - 2 \geq 0 \right\}$. *The set*

$$\gcd\left(P(M)\right)_{M \in \mathcal{B}(\mathcal{M})}$$

is a generating set of $\mathcal{M}^c$. *The set* gcd *is defined by induction, if* M_1, M_2 *and* M_3 *are elements of* $\mathcal{B}(\mathcal{M})$, *then*

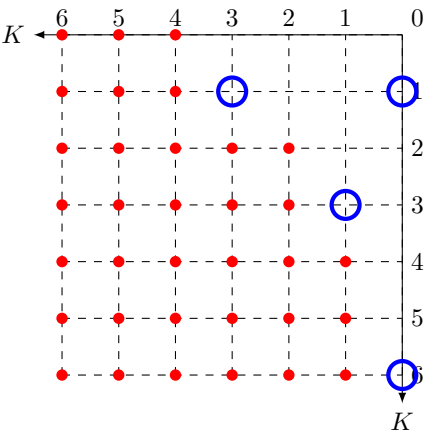
$$\gcd(P(M_1), P(M_2), P(M_3)) = \gcd(\gcd(P(M_1), P(M_2)), P(M_3)),$$

where $\gcd(P(M_1), P(M_2)) = \{\gcd(M_1', M_2') : M_1' \in M_1, M_2' \in M_2\}$.

Proof. It is clear that for every monomial $M = x_1^{a_1} \cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})$ the set $P(M)$ is a minimal generating set for $\{M\}^c$. Given any two monomials M_1 and M_2, the set $\{\gcd(M_1, M_2)\}$ is a minimal generating set for the set of monomials that divide M_1 and M_2, thus the result follows. □

It is important to note that the set $\gcd(P(M))_{M\in\mathcal{B}(\mathcal{M})}$ from Proposition 2.6 is not always a minimal generating set, as the following example shows.

Example 2.7. Let $K=\mathbb{F}_7$, $\mathcal{S}=K^2$ and $\mathcal{M}$ the set of monomials of $K[x_1,x_2]$ whose exponents are the points in the left picture of Example 2.3. The circles in the picture of Example 2.5 are the exponents of the monomials that belong to $\mathcal{B}(\mathcal{M})$. The circles below are the exponents that belong to $\gcd(P(M))_{M\in\mathcal{B}(\mathcal{M})}$. It is clear that it is not a minimal generating set.



Theorem 2.8. *Let P_i be the subsets of size i of $\mathcal{B}(\mathcal{M})$. Then*
(i) *The length of $C(\mathcal{S},\mathcal{M})$ is given by $\prod_{i=1}^{m} n_i$.*
(ii) *The dimension of the code $C(\mathcal{S},\mathcal{M})$ is*

$$\sum_{i=1}^{|\mathcal{B}(\mathcal{M})|}\left((-1)^{i-1}\sum_{T\in P_i}\prod_{j=1}^{n}(t_j+1)\right),$$

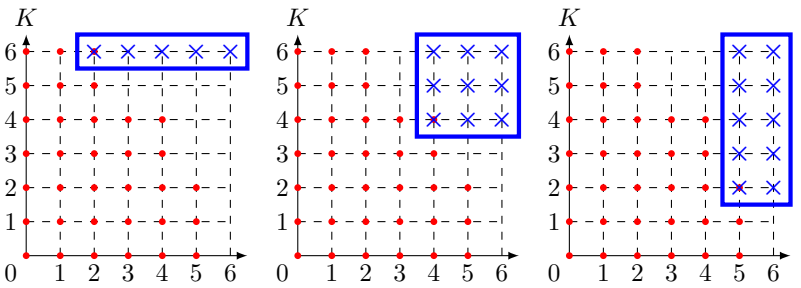
where $(t_1,\ldots,t_m)$ is the exponent of the gcd *of the elements of T.*
(iii) *The minimum distance of $C(\mathcal{S},\mathcal{M})$ is given by*

$$\min\left\{\prod_{i=1}^{m}(n_i-a_i) : x_1^{a_1}\cdots x_m^{a_m}\in\mathcal{B}(\mathcal{M})\right\}.$$

Proof. (i) It is clear because $\prod_{i=1}^{m} n_i$ is the cardinality of $\mathcal{S}$. (ii) Given two monomials M and M', we see that $\gcd(M,M')$ is the minimal generating set of the set of monomials that divide to M and also to M'. For any monomial $M=x_1^{t_1}\cdots x_m^{t_m}$,

$\prod_{j=1}^{n}(t_j+1)$ is the number of monomials that divide M. Thus the dimension follows from the inclusion exclusion theorem. (iii) Let $\prec$ be the graded-lexicographical order and take $f \in \mathrm{Span}_K\{M : M \in \mathcal{M}\}$. If $M = x_1^{b_1}\cdots x_m^{b_m}$ is the leading monomial of f, in [3, Proposition 2.3] the author proved that $|\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, f)| \geq \prod_{i=1}^{m}(n_i - b_i)$. As $\mathcal{B}(\mathcal{M})$ is a minimial generating set of $\mathcal{M}$, there exists $M' = x_1^{a_1}\cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})$ such that M divides M'. Thus $|\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, f)| \geq \prod_{i=1}^{m}(n_i - a_i)$ and $\delta(C(\mathcal{S},\mathcal{M})) \geq \min\left\{\prod_{i=1}^{m}(n_i - a_i) : x_1^{a_1}\cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})\right\}$. Assume for $i \in [m]$, $S_i = \{s_{i1},\ldots,s_{in_i}\}$. Let $x_1^{\alpha_1}\cdots x_m^{\alpha_m} \in \mathcal{B}(\mathcal{M})$ such that $\prod_{i=1}^{m}(n_i - \alpha_i) = \min\left\{\prod_{i=1}^{m}(n_i - a_i) : x_1^{a_1}\cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})\right\}$. Define $f_\alpha := \prod_{i=1}^{m}\prod_{j=1}^{\alpha_i}(x_i - s_{ij})$. As $|\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, f_\alpha)| = \prod_{i=1}^{m}(n_i - a_i)$, and $f_\alpha \in \mathrm{Span}_K\{M : M \in \mathcal{M}\}$ because all monomials that appear in f_α divide $x_1^{\alpha_1}\cdots x_m^{\alpha_m}$, then we have $\delta(C(\mathcal{S},\mathcal{M})) \leq \min\left\{\prod_{i=1}^{m}(n_i - a_i) : x_1^{a_1}\cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})\right\}$ and the result follows. □

Example 2.9. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ the set of monomials of $K[x_1, x_2]$ whose exponents are the points in the left picture of Example 2.3. The length of the code is 49, which is the total number of grid points in $\mathcal{S}$. The dimension is 34, which is the total number of points in the left picture of Example 2.3. The minimal generating set $\mathcal{B}(\mathcal{M})$ is $\{x_1^2x_2^6, x_1^4x_2^4, x_1^5x_2^2\}$. By Theorem 2.8 $|\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, x^2y^6)| \geq 5$, which is the number of grid points between the point $(2,6)$ and the point $(6,6)$. See first picture (from left to right) below. In a similar way $|\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, x_1^4x_2^4)| \geq 9$ and $|\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, x_1^5x_2^2)| \geq 10$. See second and third picture (from left to right) below. As $\min\{5, 9, 10\} = 5$, the minimum distance $\delta(C(\mathcal{S},\mathcal{M}))$ is 5.



Acknowledgments

The first and fourth author were partially supported by SIP-IPN, project 20195717, and CONACyT. The third author is partially supported by NSF DMS-1855136.

References

[1] M. Bardet, V. Dragoi, A. Otmani, J. P. Tillich, Algebraic properties of polar codes from a new polynomial formalism, In 2016 IEEE International Symposium on Information Theory (2016, July), pp. 230–234.

[2] E. Camps, E. Martínez-Moro, E. Sarmiento, Vardøhus Codes: Polar Codes Based on Castle Curves Kernels, IEEE Transactions on Information Theory, (2019) DOI:10.1109/TIT.2019.2932405.

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

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

[5] H. H. López, G. L. Matthews, Ivan Soprunov, Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes, https://arxiv.org/pdf/1907.11812.pdf

[6] H. H. López, C. Rentería-Márquez, R. H. Villarreal, Affine Cartesian codes, Des. Codes Cryptogr. **71**(1) (2014) 5–19.

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

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

[9] I. Soprunov, J. Soprunova, Bringing Toric Codes to the Next Dimension, SIAM Journal on Discrete Mathematics, **24** (2010), no. 2, 655–665.

[10] I. Tamo, A. Barg, A Family of Optimal Locally Recoverable Codes, IEEE Transactions on Information Theory **60** (2014), no. 8, 4661–4676.

[11] A. Barg, I. Tamo, and S. Vladut, Locally Recoverable Codes on Algebraic Curves, IEEE Transactions on Information Theory **63** (2017), no. 8, 4928 – 4939.

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

[13] J. H. Van Lint, **Introduction to coding theory**, Third edition, Graduate Texts in Mathematics **86**, Springer-Verlag, Berlin, 1999.

[14] R. H. Villarreal, **Monomial Algebras**, second edition, Monographs and and Research notes in Mathematics, 2015.