Polar Decreasing Monomial-Cartesian Codes

Eduardo Camps, Hiram H. López, Gretchen L. Matthews, *Senior Member, IEEE,* Eliseo Sarmiento

***Abstract*—In this paper, we introduce a new family of polar codes from evaluation codes, called polar decreasing monomial-Cartesian codes, and prove that families of polar codes with multiple kernels over certain symmetric channels can be viewed as polar decreasing monomial-Cartesian codes. This offers a unified treatment for such codes over any finite field. We define decreasing monomial-Cartesian codes as evaluation codes obtained from a set of monomials closed under divisibility over a Cartesian product and determine their parameters (length, dimension, and minimum distance). We show that the dual of a decreasing monomial-Cartesian code is monomially equivalent to a decreasing monomial-Cartesian code. Polar decreasing monomial-Cartesian codes are then obtained by utilizing decreasing monomial-Cartesian codes whose sets of monomials are closed with respect to a partial order. We prove that any sequence of invertible matrices over an arbitrary field satisfying certain conditions polarizes any channel that is symmetric over the field.**

***Index Terms*—Cartesian codes, monomial codes, monomial-Cartesian codes, decreasing codes, polar codes. 2010 Mathematics Subject Classification. Primary 11T71; Secondary 14G50.**

I. Introduction

POLAR codes, introduced in 2009 in the seminal paper [1] by Arikan, are the first class of provably capacity achieving codes for symmetric binary-input memoryless channels with explicit construction as well as efficient encoding and decoding. This breakthrough generated a flurry of activity on polar codes, as described below. Polar codes are now attracting increased attention as they are adopted in the 5th generation wireless systems (5G) standardization process of the 3rd generation partnership project (3GPP); for an overview, see for instance, [2], [5].

Originally, polar codes were constructed with Arikan's kernel, which is given by

$$G_A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

The kernel is used to create N synthetic channels from N copies of the channel in a recursive fashion, so that some of the new channels have enhanced reliability while others are inferior. In the limit, as $N \to \infty$, each channel becomes either noiseless or pure noise, which is the so-called polarization phenomenon. For an (N, K) polar code, communication takes places over the K most reliable channels, taking the corresponding codeword coordinates to be part of the information set while the remaining positions are frozen bits and not used to transfer information.

Polar codes were generalized to arbitrary discrete memoryless channels by Şaşoğlu, Telatar and Arikan [23], and Korada, Şaşoğlu, and Urbanke considered larger binary matrices as kernels and considered the speed of polarization by introducing a quantity called the exponent [11]. Polarization over nonbinary alphabets was studied by Şaşoğlu [22] as were polar codes over arbitrary finite fields by Mori and Tanaka [20] (see also [18] and [19]). Tal and Vardy pushed forward the applicability of polar codes with their introduction of a successive-cancellation list decoder [25] (see also [24]) and efficient constructions [25].

The relation between polar codes and Reed-Solomon codes is well-known. The original definition given by Arikan uses a Reed-Solomon kernel derived from a binary alphabet. Reed-Solomon kernels over large alphabets were also studied to construct polar codes in [20], with the original construction of using just one kernel for the whole polar code. In this paper, we consider *multikernel polar codes*, where the kernel is formed using submatrices from Reed-Solomon kernels. This construction forms a family that is more general than polar codes with Reed-Solomon kernels. The primary motivation for the multikernel polarization process is the construction of polar codes of different lengths, other than $N = l^n$. Different techniques, such as puncturing or shortening the original polar code, have been employed to achieve this but with some disadvantages as augmenting the decoding complexity [21], [31], [32]. Multikernel polar codes over the binary field were considered in [4] and [9] where the authors give some conditions for a sequence of matrices to polarize a channel. Here, we consider codes over arbitrary fields. The paper is organized as follows.

In Section II, we recover the definition of multikernel polarization given in [9] with a slight difference, as well as define it for matrices and channels over non-binary fields. Taking the ideas of [20], we focus on channels with a certain symmetry to describe when a sequence of square invertible matrices polarizes. This yields conditions which are easier to check than those given in [4] for binary polar codes. Later in the paper, we delve into this setting to obtain polar decreasing monomial-Cartesian codes which arise from evaluation codes defined by monomials over finite fields (of any characteristic).

Section III introduces decreasing monomial-Cartesian codes and contains our main results. Decreasing monomial-Cartesian

Corresponding author. H. H. López, e-mail: h.lopezvaldez@csuohio.edu.
The first and fourth author were partially supported by SIP-IPN, project 20195717, and CONACyT. The second author was partially supported by an AMS–Simons Travel Grant. The third author was supported in part by NSF DMS-1855136 and the Commonwealth Cyber Initiative. This paper was presented in part at [6].
E. Camps and E. Sarmiento are with the Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional, Mexico City, Mexico, e-mail addresses: camps@esfm.ipn.mx and esarmiento@ipn.mx.
H. H. López is with the Department of Mathematics and Statistics, Cleveland State University, Cleveland, OH, USA, e-mail: h.lopezvaldez@csuohio.edu.
G. L. Matthews is with the Department of Mathematics, Virginia Tech, Blacksburg, VA, USA, e-mail: gmatthews@vt.edu.

codes are a particular class of evaluation codes which generalize Reed-Solmon, Reed-Muller codes, and the family of decreasing monomial codes considered in [3]. 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 LCD codes, quantum codes, and locally recoverable codes [14]. Theorem 3.3 shows that the dual of a decreasing monomial-Cartesian codes is equivalent to a decreasing monomial-Cartesian codes. This result is stated as follows.

Theorem 3.3 The dual of the code $C(\mathcal{S},\mathcal{M})$ is monomially equivalent to a decreasing monomial-Cartesian code. In fact, $C(\mathcal{S},\mathcal{M})^{\perp} =$

$$\mathrm{Span}_K\left(\left\{\mathrm{Res}_{\mathcal{S}}\,\frac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M} : M\in\mathcal{M}_{\mathcal{S}}^c\right\}\right).$$

Moreover,

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

is a basis for $C(\mathcal{S},\mathcal{M})^{\perp}$.

Theorem 3.9 gives an explicit expression for the basic parameters of a decreasing monomial-Cartesian code: the length, the dimension and the minimum distance. This result is stated as follows.

Theorem 3.9 Let $C(\mathcal{S},\mathcal{M})$ be a decreasing monomial-Cartesian code.

(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

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

where $P_i \subseteqq \mathcal{B}(\mathcal{M})$ are those subsets with $|P_i| = i$ and $(t_1,\ldots,t_m)$ is the exponent of $\gcd T$.

(iii) The minimum distance of $C(\mathcal{S},\mathcal{M})$ is given by

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

In Section IV, we consider polar codes whose kernels are decreasing monomial-Cartesian codes, calling these polar decreasing monomial-Cartesian codes. In [3], the authors proved that polar codes constructed from G_A are polar decreasing monomial-Cartesian codes over the binary field. We extend this result to prove in Theorem 4.8 that polar codes constructed from a sequence of Reed-Solomon matrices using Definition 2.13 are polar decreasing monomial-Cartesian codes, and that any channel that is symmetric over the field is polarized by this sequence of Reed-Solomon matrices, providing a unified framework for this family of polar codes. Naturally, this holds at the cost of reducing the family of channels over which we can work, given the required symmetric condition. Section V provides a conclusion to this work.

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 a field K. The set of $m\times n$ matrices over a field K is denoted $K^{m\times n}$. Given $M\in K^{m\times n}$, $Row_i M$ denotes the i^{th} row of M and $Col_j M$ denotes its j^{th} column. For more information about coding theory, we recommend [16], [29]. For algebraic concepts not described here, we suggest [30] to the reader.

II. Polar codes defined by sequences of invertible matrices

Let $\mathbb{F}_q$ be a finite field with q elements. Consider a discrete memoryless channel (DMC) $W : \mathbb{F}_q \to \mathcal{Y}$ with transition probabilities $W(y|x)$, $y\in\mathcal{Y}$, $x\in\mathbb{F}_q$. For a sequence of invertible matrices $\{T_i\}_{i=1}^{\infty}$ where $T_i\in\mathbb{F}_q^{n_i\times n_i}$, define G'_m as

$$G'_m = T_1\otimes T_2\otimes\cdots\otimes T_m,$$

where $\otimes$ stands for the Kronecker product and

$$G_m = B_m G'_m$$

where B_m is described by the following: for any $j = 1,\ldots,n_1\cdots n_m$, there exist uniquely determined $0\le k_i\le n_i-1$, $1\le i\le m$, such that $j = 1+\sum_{i=1}^{m}k_i\prod_{j=i+1}^{m}n_j$ and B_m is the permutation matrix that sends j to the row $j' = 1+\sum_{i=1}^{m}k_i\prod_{j=1}^{i-1}n_j$. Alternatively, we may define these matrices inductively, taking $G_1 = T_1$ and for $m\ge 2$,

$$G_m = \begin{bmatrix} G_{m-1}\otimes Row_1 T_m \\ G_{m-1}\otimes Row_2 T_m \\ \vdots \\ G_{m-1}\otimes Row_{n_m} T_m \end{bmatrix}. \qquad (1)$$

Example 2.1. Let α be a primitive element of $\mathbb{F}_4$. Consider the following matrices over $\mathbb{F}_4$:

$$T_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1\end{bmatrix}, T_2 = \begin{bmatrix} 0 & 1 & \alpha^2 \\ 0 & 1 & \alpha \\ 1 & 1 & 1\end{bmatrix}.$$

Then $G'_2 = \begin{bmatrix} 0&0&0&0&1&\alpha^2\\ 0&0&0&0&1&\alpha\\ 0&0&0&1&1&1\\ 0&1&\alpha^2&0&1&\alpha^2\\ 0&1&\alpha&0&1&\alpha\\ 1&1&1&1&1&1 \end{bmatrix}$ and

$$G_2 = \begin{bmatrix} 0&0&0&0&1&\alpha^2\\ 0&1&\alpha^2&0&1&\alpha^2\\ 0&0&0&0&1&\alpha\\ 0&1&\alpha&0&1&\alpha\\ 0&0&0&1&1&1\\ 1&1&1&1&1&1 \end{bmatrix}.$$

Let us continue with the description of polarization. Starting from the channel W, we construct the following $n = \prod_{i=1}^{m} n_i$ channels:

$$W_m^{(i)} : \mathbb{F}_q \to \mathcal{Y}^N\times\mathbb{F}_q^{i-1}, \quad 1\le i\le n$$

and $W_m^{(i)}\left(y_1^n, u_1^{i-1}|u_i\right) =$

$$\frac{1}{q^{n-1}}\sum_{u_{i+1}^n\in\mathbb{F}_q^{n-1}}\prod_{j=1}^{n} W\left(y_j|u_1^n Col_j(G_m)\right).$$

As n grows, some of the channels $W_m^{(i)}$ becomes noiseless. We measure this through the symmetric rate of the channel.

Definition 2.2. Let $W : \mathbb{F}_q \to \mathcal{Y}$ be a DMC channel. We define the symmetric rate of W as

$$I(W) = \frac{1}{q} \sum_{(x,y)\in\mathbb{F}_q\times\mathcal{Y}} W(y|x) \log_q \left(\frac{W(y|x)}{\frac{1}{q}\sum_{x\in\mathcal{X}} W(y|x)} \right).$$

Definition 2.3. Let $W : \mathbb{F}_q \to \mathcal{Y}$ be a DMC channel and $\{T_i\}_{i=1}^{\infty}$ be a sequence of invertible matrices over $\mathbb{F}_q$. We say that the sequence polarizes W if for each $\delta > 0$, we have

$$\lim_{m\to\infty} \frac{\left|\left\{i\in\{1,\dots,\prod_{i=1}^m n_i\} \;\mid\; I\left(W_m^{(i)}\right)\in(1-\delta,1]\right\}\right|}{\prod_{i=1}^m n_i} = I(W), \text{ and}$$

$$\lim_{m\to\infty} \frac{\left|\left\{i\in\{1,\dots,\prod_{i=1}^m n_i\} \;\mid\; I\left(W_m^{(i)}\right)\in[0,\delta)\right\}\right|}{\prod_{i=1}^m n_i} = 1 - I(W).$$

Observe that when $T_i = G$ for all i, then we have the usual polarization process with kernel G. By taking $T_i = G_A$ for all i, we have the original polar code defined by Arikan. The previous definition is similar to that given in [9], with the difference being we use the bit-reversal matrix B_m and the field $\mathbb{F}_q$ (where q can be any prime power) instead of $\mathbb{F}_2$.

Definition 2.4. Let $W : \mathbb{F}_q \to \mathcal{Y}$ be a DMC channel. Then:

(a) W is symmetric over the sum (or additive symmetric) if for each $a \in \mathbb{F}_q$ there is a permutation σ_a of $\mathcal{Y}$ such that
$$W(y|x) = W(\sigma_a(y)|x + a), \qquad \forall x \in \mathbb{F}_q,\; y \in \mathcal{Y}.$$

(b) W is symmetric over the product if for each $a \in \mathbb{F}_q^*$ there is a permutation ψ_a of $\mathcal{Y}$ such that
$$W(y|x) = W(\psi_a(y)|ax), \qquad \forall x \in \mathbb{F}_q,\; y \in \mathcal{Y}.$$

(c) W is symmetric over the field (SOF) if it is both symmetric over the sum and over the product.

Originally, polar codes were proposed over binary symmetric channels [1]. Later, in [20], symmetry over the sum was used to guarantee that a family of matrices polarizes such channels. In [7], the authors employed symmetry over the field to describe up to a certain degree the best channels $W_n^{(i)}$; these are those with greater symmetric rate.

Example 2.5. Let $0 \le p \le 1$. The q-ary symmetric channel is defined as

$$W_{Sq} : \mathbb{F}_q \to \mathbb{F}_q,$$

$$W_{Sq}(y|x) = (1-p)\delta(x,y) + \frac{p}{q},$$

where $\delta(x,y) = 1$ if $x = y$ and 0 otherwise. This is a SOF channel.

Example 2.6. The q-ary erasure channel for $0 \le p \le 1$ is defined as

$$W_{qE} : \mathbb{F}_q \to \mathbb{F}_q \cup \{*\}$$

with transition probabilities

$$W_{qE}(y|x) = \begin{cases} 1-p & y = * \\ p & y = x \\ 0 & \text{otherwise.} \end{cases}$$

This is a SOF channel. The polar behavior of generalized Reed-Solomon codes over this channel was studied in [18].

When W is an additive symmetric channel and G and G' are invertible matrices such that $G'G^{-1}$ is an upper-triangular matrix, then using either G or G' to polarize gives rise to channels $W_1^{(i)}$ with same symmetric rate. If G polarizes, then G' polarizes W. Taking a column permutation of G does not affect the symmetric rate of the channels. If P is a permutation matrix and G polarizes, then so does GP. This leads to the following definition.

Definition 2.7. Let $G \in \mathbb{F}_q^{l\times l}$ be invertible. Let $V \in \mathbb{F}_q^{l\times l}$ be an upper-triangular invertible matrix and $P \in \mathbb{F}_q^{l\times l}$ be a permutation matrix. If $G' = VGP$ is a lower-triangular matrix with 1's in its diagonal, then G' is called a **standard form** of G.

It is important to note that standard form is not unique. Over $\mathbb{F}_4$ with primitive element α, both

$$G_1' = \begin{bmatrix} \alpha & \alpha^2 \\ 0 & \alpha \end{bmatrix} G = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} \text{ and}$$

$$G_2' = \begin{bmatrix} \alpha^2 & \alpha^2 \\ 0 & 1 \end{bmatrix} G \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \alpha^2 & 1 \end{bmatrix}$$

are standard forms of $G = \begin{bmatrix} 1 & 1 \\ 1 & \alpha^2 \end{bmatrix}$. The information given by the standard form of a sequence of invertible matrices is enough to determine if such a sequence polarizes an additive symmetric channel.

Lemma 2.8. *[20, Theorem 14] Let p be a prime such that $p|q$. The following are equivalent for an invertible matrix $G \in \mathbb{F}_q^{l\times l}$ with a non-identity standard form.*

(a) *Any additive symmetric channel is polarized by G.*

(b) *The field extension of $\mathbb{F}_p$ generated by the entries of G', denoted $\mathbb{F}_p(G')$, is $\mathbb{F}_q$ for any standard form G' of G; that is,*
$$\mathbb{F}_p(G') = \mathbb{F}_q$$
for any standard form G' of G.

(c) *There is a standard form G' of G with $\mathbb{F}_p(G') = \mathbb{F}_q$.*

Theorem 2.9. *Let $\{T_i\}_{i=1}^{\infty}$ be a sequence of invertible matrices. If for each i, T_i has a non-identity standard form T_i' such that $\mathbb{F}_p(T_i') = \mathbb{F}_q$, then the sequence $\{T_i\}_{i=1}^{\infty}$ polarizes to any additive symmetric channel W.*

Proof. The proof of the sufficency of Lemma 2.8 relies on the fact that the process $I\left(W_m^{(i)}\right)$ forms a martingale and these channels are as good as

$$\left(W_m^{(i)}\right)_1^{(2)},$$

where the last is the second splitted channel by using any $G_\gamma = \begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix}$. The same arguments apply here with slight changes to the process by substituting the sequence $\{G\}_{i=1}^{\infty}$ by any other sequence $\{T_i\}_{i=1}^{\infty}$ of invertible matrices. $\square$

The previous result does not imply that if a sequence $\{T_i\}_{i=1}^{\infty}$ polarizes, then each T_i has a non-identity standard form T_i' with $\mathbb{F}_p(T_i') = \mathbb{F}_q$. It is enough to consider a sequence $\{I_l\} \cup \{T_i\}_{i=1}^{\infty}$, where I_l is the identity matrix of size l and each T_i has a non-identity standard form with the condition desired before.

In [4], the authors gave conditions over $\mathbb{F}_2$ for a sequence to polarize. Since we are interested in SOF channels, we can strengthen the last proposition to the following result.

Corollary 2.10. *Let $\{T_i\}_{i=1}^{\infty}$ be a sequence of invertible matrices. If for each i, T_i has a non-identity standard form, then the sequence $\{T_i\}_{i=1}^{\infty}$ polarizes any SOF channel W.*

The proof of the last relies on the following lemma.

Lemma 2.11. *Let $G \in \mathbb{F}_q^{l\times l}$ be an invertible matrix and G' be the matrix with $Col_1 G' = aCol_1 G$ for some $a \in \mathbb{F}_q^*$ and $Col_j G' = Col_j G$ for $2 \le j \le n$. Let $W : \mathbb{F}_q \to \mathcal{Y}$ be a SOF channel. If $W_1^{(i)}$, $1 \le i \le l$ are the split channels of the polarization process using G and ${W'}_1^{(i)}$, $1 \le i \le l$ are the same but with G', then*

$$I\left(W_1^{(i)}\right) = I\left({W'}_1^{(i)}\right).$$

Proof. Let ψ_a the permutation of $\mathcal{Y}$ such that

$$W(y|x) = W(\psi_a(y)|ax)$$

for any $x \in \mathbb{F}_q$ and $y \in \mathcal{Y}$. Then $W_1^{(i)}\left(y_1^l, u_1^{i-1}|u_i\right)$

$$\begin{aligned} &= \textstyle\sum_{u_{i+1}^l \in \mathbb{F}_q^{l-1}} \prod_{j=1}^{l} W\left(y_j|u_1^l Col_j G\right) \\ &= \textstyle\sum_{u_{i+1}^l \in \mathbb{F}_q^{l-1}} W''_{u_{i+1}^l} \\ &= {W'}_1^{(i)}\left((\psi_a(y_1), y_2^l), u_1^{i-1}|u_i\right) \end{aligned}$$

where

$$W''_{u_{i+1}^l} := W(\psi_a(y_1)|u_1^l(aCol_1 G)) \prod_{j=2}^{l} W\left(y_j|u_1^l Col_j G\right).$$

Since $W_1^{(i)}$ and ${W'}_1^{(i)}$ have the same distribution (and a bijection over the output alphabet), they have the same symmetric rate. $\square$

If T_i has a non-identity standard form, we can multiply the $(n_i-1)^{th}$ column by some $a \in \mathbb{F}_q^*$ to obtain $\overline{T}_i$ which has a standard $\overline{T}_i'$ form such that $\mathbb{F}_p(\overline{T}_i') = \mathbb{F}_q$. Since a SOF channel is symmetric, the sequence $\{\overline{T}_i\}_{i=1}^{\infty}$ polarizes and by the last lemma, $\{T_i\}_{i=1}^{\infty}$ polarizes too. In the light of this, we can generalize the definition of polar codes using the description of the Bhattacharyya parameter.

Definition 2.12. Let $W : \mathcal{X} \to \mathcal{Y}$ be a DMC channel with $|\mathcal{X}| = q$. For $x, x' \in \mathbb{F}_q$, $x \ne x'$, we define the **Bhattacharyya distance** as

$$Z(x, x') = \sum_{y\in\mathcal{Y}} \sqrt{W(y|x)W(y|x')}$$

and the **Bhattacharyya parameter** as

$$Z(W) = \frac{1}{q(q-1)} \sum_{\substack{x,x'\in\mathcal{X}\\ x\ne x'}} Z(x, x'),$$

the average of the Bhattacharyya distances over $\mathcal{X}$.

Definition 2.13. Let $\{T_i\}_{i=1}^{\infty}$ be a sequence of invertible matrices that polarizes the channel $W : \mathbb{F}_q \to \mathcal{Y}$. Let m be a positive integer and let $n = \prod_{i=1}^{m} n_i$, where n_i are the sizes of T_i as before. We define an **information set** $\mathcal{A}_m \subset \{1, \dots, n\}$ as a set such that

$$Z\left(W_m^{(i)}\right) \le Z\left(W_m^{(j)}\right), \quad \forall i \in \mathcal{A}_m, \quad \forall j \notin \mathcal{A}_m.$$

A **polar code** is the subspace $C_{\mathcal{A}_m}$ generated by the rows of G_m indexed by $\mathcal{A}_m$.

It is known that $I(W) \to 1$ if and only if $Z(W) \to 0$ [19, Lemma 5]. Therefore, as n grows, it is the same selecting Z or I to construct $\mathcal{A}_m$, but by selecting Z we can easily (upper) bound the error probability for a successive cancellation decoder.

III. Decreasing monomial-Cartesian codes

In this section, we introduce a new family of evaluation codes, called decreasing monomial-Cartesian codes. They are obtained by evaluating certain multivariate polynomials (meaning polynomials in say m variables) at points in m-dimensional space, much in the way that Reed-Solomon codes or Reed-Muller codes are defined. By requiring that the functions to be evaluated meet specified conditions in terms of divisibility, we obtain a more general family which can be used to define multikernel polar codes (as done in Section IV). In this section, we determine important properties of the decreasing monomial-Cartesian codes, including their basic parameters and duals.

We begin by introducing notation to be used from this point in the paper onwards. 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. The monomial $\boldsymbol{x}^{\boldsymbol{a}} := x_1^{a_1} \cdots x_m^{a_m} \in R$ is sometimes denoted by its exponent $\boldsymbol{a} = (a_1, \dots, a_m) \in \mathbb{Z}_{\ge 0}^m$. A **decreasing monomial set** is a set of monomials $\mathcal{M} \subseteq R$ such that the condition $M \in \mathcal{M}$ and M' divides M imply $M' \in \mathcal{M}$. 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. The Cartesian product is defined by

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

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 an **evaluation map**

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

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 $\mathrm{ev}_{\mathcal{S}}$ is injective; see [14, Proposition 2.1]. The **complement** of $\mathcal{M}$ in $\mathcal{S}$ denoted by $\mathcal{M}_{\mathcal{S}}^c$, is the set of all monomials in R that are not in $\mathcal{M}$ and their degree with respect to x_i is less than n_i.

Definition 3.1. Let $\mathcal{M} \subseteq R$ be a decreasing monomial set. The image $\mathrm{ev}_{\mathcal{S}}(L(\mathcal{M})) \subseteq K^n$ is called the **decreasing monomial-Cartesian code** associated to $\mathcal{S}$ and $\mathcal{M}$. We denote it by $C(\mathcal{S},\mathcal{M})$.

More generally (meaning regardless of whether or not $\mathcal{M} \subseteq R$ is a decreasing monomial set), the code $\mathrm{ev}_{\mathcal{S}}(L(\mathcal{M})) \subseteq K^n$ is called **monomial-Cartesian code** [14].

A number of familiar codes may be viewed as decreasing monomial-Cartesian codes for particular families of Cartesian products $\mathcal{S}$ and particular families of decreasing monomial sets $\mathcal{M}$. For example, a **Reed-Muller code** of order r in the sense of [28, p. 37] is a decreasing monomial-Cartesian code $C(K^m, M_r)$, where M_r is the set of monomials of degree less than r; a Reed-Solomon code is obtained by taking $m = 1$ in this construction. An **affine Cartesian code** of order r is the decreasing monomial-Cartesian code $C(\mathcal{S}, M_r)$. This family of affine Cartesian codes appeared first in [10] and then independently in [15]. In [3], 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 [7] for $K = \mathbb{F}_q$ and monomials associated to curve kernels. Certainly, not all families of monomial-Cartesian codes are decreasing. For instance, the family of codes given by Tamo and Barg in [27], which is well-known for its application to distributed storage, is not decreasing. Indeed, they are subcodes of Reed-Solomon codes where some monomials are omitted, and the divisibility condition may not be satisfied. 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 decreasing as $g(x)^j x^i \in V$ and x divides $g(x)^j x^i$ but $x \notin V$.

The length and the dimension of a decreasing 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 [14, Proposition 2.1]. Recall that the **minimum distance** of a code C is given by $d(C) = \min\{|\operatorname{Supp}(\boldsymbol{c})| : \boldsymbol{0} \neq \boldsymbol{c} \in C\}$, where $\operatorname{Supp}(\boldsymbol{c})$ denotes the support of $\boldsymbol{c}$, that is the set of all nonzero entries of $\boldsymbol{c}$. Unlike the case of the length and the dimension, in general, giving an explicit formula for $d(C(\mathcal{S},\mathcal{M}))$ in terms of $\mathcal{S}$ and $\mathcal{M}$ is more challenging but addressed in this section; we note that there is no such expression if $\mathcal{M}$ is not decreasing. Recall that **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**) [17] if $C \cap C^\perp = \{\boldsymbol{0}\}$, and is called a **self-orthogonal** code if $C^\perp \subseteq C$. Given codes C_1 and C_2 of the same length over K where G_1 is a generator matrix for C_1, we say that C_1 and C_2 are **monomially equivalent** provided there is a monomial matrix M (meaning a square matrix with entries in K that has exactly one nonzero entry in each row and column) so that $G_1 M$ is a generator matrix of C_2. Monomially equivalent codes have the same length, dimension, and minimum distance.

To describe the dual of a decreasing monomial-Cartesian code $C(\mathcal{S},\mathcal{M})$, we make use of the following definition.

Definition 3.2. For $\boldsymbol{s} = (s_1, \ldots, s_m) \in \mathcal{S}$ and $f \in R$, define the **residue** of f at $\boldsymbol{s}$ as

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

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

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

We now come to one of the main results of this paper: the dual of a decreasing monomial-Cartesian code $C(\mathcal{S},\mathcal{M})$ is almost a decreasing monomial-Cartesian code $C(\mathcal{S},\mathcal{M})$. In fact, the dual is obtained by finding an appropriate decreasing monomial-Cartesian code and then multiplying every entry by a suitable constant. It is reminiscent of the fact that the dual of a Reed-Solomon code is a generalized Reed-Solomon code. As we will see, the suitable constant can be described in terms of the residue.

Theorem 3.3. *The dual of the code $C(\mathcal{S},\mathcal{M})$ is monomially equivalent to a decreasing monomial-Cartesian code. In fact,* $C(\mathcal{S},\mathcal{M})^\perp =$

$$\operatorname{Span}_K \left(\left\{ \operatorname{Res}_{\mathcal{S}} \frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{M} : M \in \mathcal{M}_{\mathcal{S}}^c \right\} \right).$$

Moreover,

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

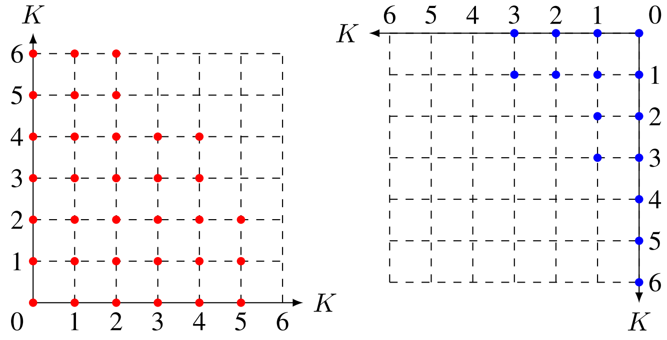
is a basis for $C(\mathcal{S},\mathcal{M})^\perp$.

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 decreasing. Let $M \in \mathcal{M}_{\mathcal{S}}^c$ and $\boldsymbol{x}^{\boldsymbol{a}}$ be a divisor of $\frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{M}$. Then there exists a monomial $\boldsymbol{x}^{\boldsymbol{b}}$ in R such that $\frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{M} = \boldsymbol{x}^{\boldsymbol{a}} \boldsymbol{x}^{\boldsymbol{b}}$. As $M \in \mathcal{M}_{\mathcal{S}}^c$ and $\mathcal{M}$ is decreasing, then $\boldsymbol{x}^{\boldsymbol{b}} M \in \mathcal{M}_{\mathcal{S}}^c$ and $\boldsymbol{x}^{\boldsymbol{a}} = \frac{x_1^{n_1-1} \cdots x_m^{n_m-1}}{\boldsymbol{x}^{\boldsymbol{b}} M} \in \Delta'$. This proves that the set Δ' is decreasing. Due to [14, Theorem 2.7] and the fact that the set $\mathcal{M}$ is decreasing, Δ is a basis for the dual $C(\mathcal{S},\mathcal{M})^\perp$. Finally, it is clear that $\operatorname{Span}_K\{\boldsymbol{c} : \boldsymbol{c} \in \Delta\}$ is monomially equivalent to $\mathrm{ev}_{\mathcal{S}}(\Delta')$, which is a decreasing monomial-Cartesian code. □

Example 3.4. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ be the set of monomials of $K[x_1, x_2]$ whose exponents are the points in Figure 1(a). 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 Figure 1(a) and the dual $C(\mathcal{S},\mathcal{M})^\perp$ is generated



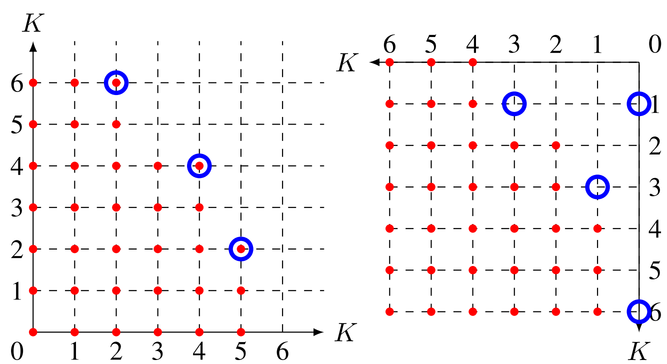
(a) (b)

Fig. 1. The code $C(\mathcal{S},\mathcal{M})$ in Example 3.4 is generated by the vectors $\mathrm{ev}_{\mathcal{S}}(M)$ where M is the set of monomials whose exponents correspond to points in (a). Its dual $C(\mathcal{S},\mathcal{M})^{\perp}$ is generated by the vectors $\mathrm{Res}_{\mathcal{S}}(M)$ where M is the set of monomials whose exponents correspond to points in (b).

by the vectors $\mathrm{Res}_{\mathcal{S}}(M)$, where M is a monomial whose exponent is a point in Figure 1(b).

Definition 3.5. 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 the **minimal generating set** if for every two elements $B_1, B_2 \in \mathcal{B}(\mathcal{M})$, B_1 does not divide B_2 and B_2 does not divide B_1. From now on, $\mathcal{B}(\mathcal{M})$ will be used to denote the minimal generating set of $\mathcal{M}$.

Example 3.6. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ be the set of monomials of $K[x_1, x_2]$ whose exponents are the points in Figure 1(a). The circled points in Figure 2(a) are the exponents of the monomials that belong to the minimal generating set $\mathcal{B}(\mathcal{M})$.



(a) (b)

Fig. 2. (a) Given the set of monomials $\mathcal{M}$ whose exponents are the points indicated, the circled points are the exponents of the monomials that belong to the minimal generating set $\mathcal{B}(\mathcal{M})$ as described in Example 3.8. (b) The circled points are the exponents of the monomials that belong to the set $\gcd\left(P(M)\right)_{M\in\mathcal{B}(\mathcal{M})}$ where $\mathcal{M}$ corresponds to the points indicated, as described in Example 3.8. .

The properties of the code $C(\mathcal{S},\mathcal{M})$ can be described in terms of $\mathcal{B}(\mathcal{M})$. The following proposition explains how to find a generating set of $\left\{ \dfrac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M} : M \in \mathcal{M}_{\mathcal{S}}^{c} \right\}$ in terms of $\mathcal{B}(\mathcal{M})$ and the gcd, which is defined as follows. The gcd of two monomials $M_1 = x_1^{a_1}\cdots x_m^{a_m}$ and $M_2 = x_1^{b_1}\cdots x_m^{b_m}$ is defined as

$$\gcd\left(M_1, M_2\right) = x_1^{\min\{a_1,b_1\}}\cdots x_m^{\min\{a_m,b_m\}}.$$

The gcd of two monomials sets $\mathcal{M}_1$ and $\mathcal{M}_2$ is defined as the monomial set

$$\gcd\left(\mathcal{M}_1, \mathcal{M}_2\right) = \left\{\gcd\left(M_1, M_2\right) \mid M_1 \in \mathcal{M}_1, M_2 \in \mathcal{M}_2\right\}.$$

The gcd of a finite number of monomials sets $\mathcal{M}_1, \ldots, \mathcal{M}_\ell$ is defined inductively by

$$\gcd\left(\mathcal{M}_1, \ldots, \mathcal{M}_\ell\right) = \gcd\left(\gcd\left(\mathcal{M}_1, \ldots, \mathcal{M}_{\ell-1}\right), \mathcal{M}_\ell\right).$$

According to Theorem 3.3, the dual of a decreasing monomial-Cartesian code is monomially equivalent to a decreasing monomial-Cartesian code which is given by a particular set of monomials. The following result describes how to represent this set of monomials more concisely, meaning in terms of a generating set. Given a monomial $M = x_1^{a_1}\cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M})$, consider the associated set of monomials

$$P(M) := \left\{ \frac{x_1^{n_1-1}\cdots x_n^{n_m-1}}{x_i^{a_i+1}} : i \in [m], \text{ and } n_i - a_i - 2 \geq 0 \right\}.$$

Proposition 3.7. *A generating set of* $\left\{ \dfrac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M} : M \in \mathcal{M}_{\mathcal{S}}^{c} \right\}$ *is given by the monomial set*

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

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 the minimal generating set for $\left\{ \dfrac{x_1^{n_1-1}\cdots x_m^{n_m-1}}{M'} : M' \text{ does not divide } M, M' \in \mathcal{M}_{\mathcal{S}}^{c} \right\}$. Given any two monomials M_1 and M_2, the set $\{\gcd(M_1, M_2)\}$ is the 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 $\gcd\left(P(M)\right)_{M\in\mathcal{B}(\mathcal{M})}$ from Proposition 3.7 is not always the minimal generating set, as the following example illustrates.

Example 3.8. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ be the set of monomials of $K[x_1, x_2]$ whose exponents are the points in Figure 1(a). The circled points in Figure 2(a) are the exponents of the monomials that belong to the minimal generating set $\mathcal{B}(\mathcal{M})$. The circled points in Figure 2(b) are the exponents of the monomials that belong to the set $\gcd\left(P(M)\right)_{M\in\mathcal{B}(\mathcal{M})}$. It is clear that it is not the minimal generating set.

Given decreasing sets $\mathcal{M}_1$ and $\mathcal{M}_1$, $\mathcal{M}_1 \cap \mathcal{M}_2$ is generated by $\gcd(\mathcal{B}(\mathcal{M}_1), \mathcal{B}(\mathcal{M}_2))$ and $\mathcal{M}_1 \cup \mathcal{M}_2$ is generated by $\mathcal{B}(\mathcal{M}_1) \cup \mathcal{B}(\mathcal{M}_2)$. To see this, note that if $M \in \mathcal{M}_1 \cap \mathcal{M}_2$, then exists $M_1 \in \mathcal{B}(\mathcal{M}_1)$ and $M_2 \in \mathcal{B}(\mathcal{M}_2)$, such that $M|M_1$ and $M|M_2$. It follows that

$$M|\gcd(M_1, M_2) \in \gcd \mathcal{B}(\mathcal{M}_1), \mathcal{B}(\mathcal{M}_2)).$$

Therefore, $\mathcal{M}_1 \cap \mathcal{M}_2 \subset \gcd(\mathcal{B}(\mathcal{M}_1), \mathcal{B}(\mathcal{M}_2))$. The other containment is clear, as is the claim for the union.

We can now determine the parameters of decreasing monomial-Cartesian codes, which is another main result of this paper. The following theorem gives an explicit expression for the length, the dimension and the minimum distance of a monomial-Cartesian code $C(\mathcal{S},\mathcal{M})$ in terms of the set of monomials that define the code itself.

Theorem 3.9. *Consider a decreasing monomial-Cartesian code $C(\mathcal{S},\mathcal{M})$ as above.*

(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*

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

where $P_i \subseteq \mathcal{B}(\mathcal{M})$ are those subsets with $|P_i| = i$ and $(t_1,\dots,t_m)$ is the exponent of $\gcd T$.
(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 M and also 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 principle. (iii) Let $\prec$ be the 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, then [8, Proposition 2.3] gives $|\,\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}} f)| \geq \prod_{i=1}^{m}(n_i-b_i)$. 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

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

Assume for $i \in [m]$, $S_i = \{s_{i1},\dots,s_{in_i}\}$. Consider $x_1^{\alpha_1}\cdots x_m^{\alpha_m}\in\mathcal{B}(\mathcal{M})$ 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

$$f_\alpha := \prod_{i=1}^{m}\prod_{j=1}^{\alpha_i}(x_i-s_{ij}).$$

Since

$$|\,\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}} f_\alpha)| = \prod_{i=1}^{m}(n_i-a_i)$$

and $f_\alpha \in \mathrm{Span}_K\{M : M \in \mathcal{M}\}$ (as all monomials that appear in f_α divide $x_1^{\alpha_1}\cdots x_m^{\alpha_m}$), then we have

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

and the result follows. □

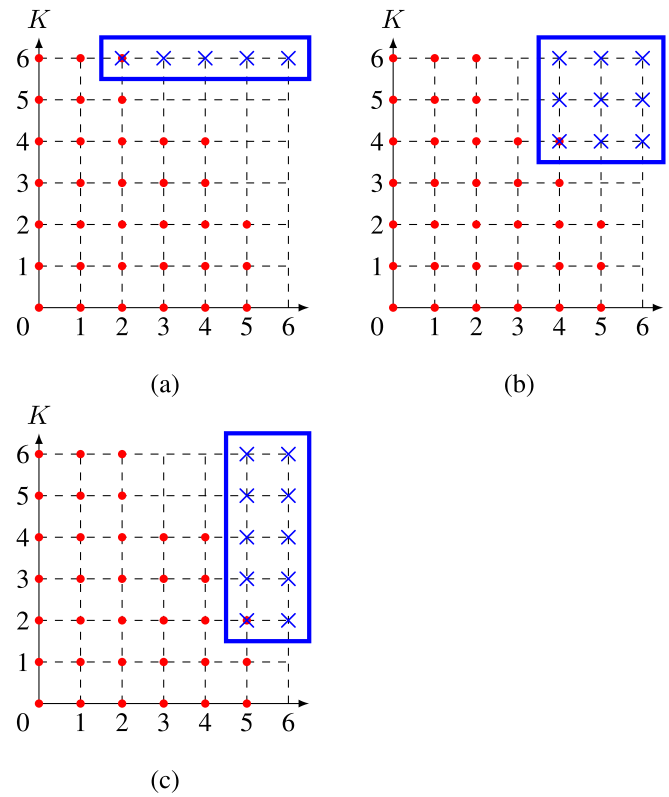


Fig. 3. The minimum distance of the code $C(\mathcal{S},\mathcal{M})$ generated by the vectors $\mathrm{ev}_{\mathcal{S}}(M)$, where M corresponds to those monomials whose exponents are the points in (a) is taken by finding the minimum number of boxed in points marked with x's in (a)-(c), as detailed in Example 3.10.

Example 3.10. Let $K = \mathbb{F}_7$, $\mathcal{S} = K^2$ and $\mathcal{M}$ be the set of monomials of $K[x_1,x_2]$ whose exponents are the points in Figure 3(a). The length of the code $C(\mathcal{S},\mathcal{M})$ 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 Figure 3(a).

Next, we consider the minimum distance of $C(\mathcal{S},\mathcal{M})$. First, note that the minimal generating set is $\mathcal{B}(\mathcal{M}) = \{x_1^2x_2^6, x_1^4x_2^4, x_1^5x_2^2\}$. By Theorem 3.9 $|\,\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, x^2y^6)| \geq 5$, which is the number of grid points between the point $(2,6)$ and the point $(6,6)$, meaning $|\,\{(2,6),(3,6),(4,6),(5,6),(6,6)\}\,|$. These points are those boxed in and marked by x's in Figure 3(a). In a similar way $|\,\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, x_1^4x_2^4)| \geq 9$, since

$$\left|\left\{\begin{array}{c}(4,4),(4,5),(4,6),(5,4),(5,5),\\(5,6),(6,4),(6,5),(6,6)\end{array}\right\}\right| = 9;$$

note that these points are boxed in and marked by x's in Figure 3(b). Likewise, $|\,\mathrm{Supp}(\mathrm{ev}_{\mathcal{S}}\, x_1^5x_2^2)| \geq 10$; see the boxed in and marked x's in Figure 3 (c), respectively. One may conclude that the minimum distance is $d(C(\mathcal{S},\mathcal{M})) = \min\{5,9,10\} = 5$.

IV. Polar codes that are polar decreasing monomial-Cartesian codes

In this section, families of polar codes will be represented as the just defined decreasing monomial-Cartesian codes, keeping the notation from the previous section. We will see that when the set $\mathcal{M}$ is also closed under a monomial order called $\trianglelefteq$ (to be described in this section) the evaluation code is a polar decreasing monomial-Cartesian code. We prove that families of polar codes with multiple kernels can be viewed as decreasing monomial-Cartesian codes by strengthening the symmetry required of the channel and using matrices associated with subsets of a finite field $\mathbb{F}_q$.

To begin, given a set $S = \{a_1, \dots, a_l\} \subseteq \mathbb{F}_q$, we associate to it the following matrix:

$$T(S) = \begin{array}{c} \\ x^{l-1} \\ \vdots \\ x \\ 1 \end{array} \begin{array}{c} \begin{array}{cccc} a_1 & a_2 & \cdots & a_l \end{array} \\ \begin{bmatrix} a_1^{l-1} & a_2^{l-1} & \cdots & a_l^{l-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_l \\ 1 & 1 & \cdots & 1 \end{bmatrix} \end{array}.$$

Each $T(S)$ is a typical Reed-Solomon kernel using the elements of S. Notice that $T(S)$ is invertible, it has a non-identity standard form and it is a generator matrix of the decreasing monomial-Cartesian code $C(S, \{1, \dots, x^{l-1}\})$. Take $S_1, S_2, \dots, S_m \subseteq K$ and let $T_i = T(S_i)$. If $S_i = \{a_{i1}, \dots, a_{in_i}\}$, we can order the set $\mathcal{S} = S_1 \times \cdots \times S_m$ with the order inherited from the lexicographical order; i.e.,

$$(a_{1j_1}, \dots, a_{mj_m}) \preceq (a_{1h_1}, \dots, a_{mh_m}) \iff j_k < h_k,$$

where

$$k = \min\{r \in \{1, \dots, m\} \mid a_{rj_r} \neq a_{rh_r}\}.$$

Let $\mathcal{M} = \{x_1^{a_1} \cdots x_m^{a_m} \mid a_i \leq n_i - 1,\ 1 \leq i \leq m\}$ and order this set with the inverse lexicographical order. Then we have that G_m as described in Equation (1) has as rows the evaluations $ev_{\mathcal{S}}$ of $\mathcal{M}$ in decreasing order.

Example 4.1. Let α be a primitive element of $\mathbb{F}_4$ and $S_1 = \{0, 1\}$, $S_2 = \{0, 1, \alpha\}$. Then

$$T_1 = \begin{array}{c} \\ x \\ 1 \end{array} \begin{array}{c} \begin{array}{cc} 0 & 1 \end{array} \\ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \end{array}, T_2 = \begin{array}{c} \\ y^2 \\ y \\ 1 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & \alpha \end{array} \\ \begin{bmatrix} 0 & 1 & \alpha^2 \\ 0 & 1 & \alpha \\ 1 & 1 & 1 \end{bmatrix} \end{array}$$

Therefore,

$$G_2 = \begin{array}{c} \\ y^2x \\ y^2 \\ yx \\ y \\ x \\ 1 \end{array} \begin{array}{c} \begin{array}{cccccc} 00 & 01 & 0\alpha & 10 & 11 & 1\alpha \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & \alpha^2 \\ 0 & 1 & \alpha^2 & 0 & 1 & \alpha^2 \\ 0 & 0 & 0 & 0 & 1 & \alpha \\ 0 & 1 & \alpha & 0 & 1 & \alpha \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \end{array}$$

Since each row of G_m can be viewed as a monomial, by an abuse of notation, for a monomial $M \in \mathcal{M}$, we can write $I(M)$ and $Z(M)$ for $I\left(W_m^{(i)}\right)$ and $Z\left(W_m^{(i)}\right)$ respectively, where

$$Row_i G_m = ev_{\mathcal{S}}(M).$$

In the usual polarization process, for a square matrix $G \in \mathbb{F}_q^{l \times l}$, the speed of polarization is measured via the exponent. This is defined as the number $E(G)$ such that for any channel W the following hold:

(i) For any fixed $\beta < E(G)$,

$$\liminf_{n \to \infty} P[Z_n \leq 2^{-l^{n\beta}}] = I(W).$$

(ii) For any fixed $\beta > E(G)$,

$$\liminf_{n \to \infty} P[Z_n \geq 2^{-l^{n\beta}}] = 1.$$

Therefore, if $D_j = d(Row_j G, \langle Row_{j+1} G, \dots, Row_l G \rangle)$, then

$$E(G) = \sum_{j=1}^{l} \frac{\ln D_j}{l \ln l};$$

here, we use the notation $d(w, V) := \min\{d(w, v) : v \in V\}$ where $d(w, v)$ denotes the Hamming distance between vectors w and v.

Remark 4.2. A lower bound on the exponent of the matrix G_m can be calculated directly from the set of monomials as follows: $E(G_m) = \sum_{j=1}^{l} \frac{\ln D_j}{l \ln l}$

$$= \sum_{j=1}^{l} \frac{\ln d(Row_j G_m, \langle Row_{j+1} G_m, \dots, Row_l G_m \rangle)}{l \ln l}$$

$$= \sum_{j=1}^{l} \frac{\ln d(Row_j G_m, Row_{j+1} G_m, \dots, Row_l G_m)}{l \ln l} \geq$$

$$\geq \frac{1}{l \ln l} \sum_{j=1}^{l} \ln \min \left\{ \prod_{i=1}^{m} (n_i - a_i) : x_1^{a_1} \cdots x_m^{a_m} \in \mathcal{B}(\mathcal{M}^j) \right\},$$

where $\mathcal{M}^j$ represents the last j monomials of the set $\mathcal{M}$ according to the inverse lexicographical order.

Remark 4.3. If G_1 and G_2 are two square non-singular matrices over $\mathbb{F}_q$, of sizes l_1 and l_2 respectively, then

$$E(G_1 \otimes G_2) = \frac{E(G_1)}{\log_{l_1}(l_1 l_2)} + \frac{E(G_2)}{\log_{l_2}(l_1 l_2)};$$

this was proven first in [13] for matrices over $\mathbb{F}_2$ and later for any finite field in [7].

From this, we have that

$$E(G_1 \otimes \cdots \otimes G_s) = \sum_{j=1}^{s} \frac{E(G_j)}{\log_{l_j}(l_1 \cdots l_s)}. \qquad (*)$$

Redefining in the obvious way the exponent for the multikernel process, in [4] the authors proved that if $T_1, \dots, T_s$ are kernels with size $l_1, \dots, l_s$ and exponents $E_1, \dots, E_s$ are used to construct a multikernel polar code in which each T_j appears with frequency p_j on G_N (the Kronecker product of these matrices) as $N \to \infty$, then the exponent of the multikernel process is

$$E = \sum_{j=1}^{s} \frac{p_j \log_2(l_j)}{\sum_{k=1}^{s} p_k \log_2(l_k)} E_j = \lim_{N\to\infty} E(G_N),$$

due to $(*)$.

In the case at hand, each T_i has size $l_i \leq q$ and we know $E(T_i) = \frac{\ln l_i!}{l_i \ln l_i}$, which is the best exponent over all the matrices of size l_i. Given $G_m = B_m(T_1 \otimes \cdots \otimes T_m)$, there exists a matrix permutation P such that $G_m P = T_m \otimes \cdots \otimes T_1$ and

$$E(G_m) = E(T_m \otimes \cdots \otimes T_1) = \sum_{i=1}^{m} \frac{E(T_i)}{\log_{l_i}(l_1 \cdots l_m)}.$$

Therefore, for any other matrix $G = M_1 \otimes \cdots \otimes M_m$, such that M_i is a square matrix of size l_i, $E(G) \leq E(G_m)$. Even more, for any sequence $\{T_i\}_{i=1}^{\infty}$, where T_i is associated to a subset from $\mathbb{F}_q$, we have

$$\lim_{n\to\infty} \sum_{k=1}^{n} \frac{E(T_k)}{\ln(l_1 \cdots l_k)} \leq \frac{\ln q!}{q \ln q},$$

suggesting that the results in [4] could be generalized for this case.

The following monomial order is inspired by the order introduced in [3]. They coincide when $K = \mathbb{F}_2$ and $S_1 = \cdots = S_m = \mathbb{F}_2$. It is the key to defining polar decreasing monomial-Cartesian codes in terms of decreasing monomial-Cartesian codes.

Definition 4.4. Let $S_1, \ldots, S_m \subseteq K$ and $M, M', \tilde{M}, \tilde{M}'$ be monomials in R. Define the monomial order $\trianglelefteq$ in R as follows.

(i) If $M'|M$, then $M' \trianglelefteq M$.
(ii) Suppose $S_{i_1} = \cdots = S_{i_r}$, and consider subsets $\{j_1, \ldots, j_s\}, \{h_1, \ldots, h_s\} \subseteq \{i_1, \ldots, i_r\}$ with $j_l < j_{l+1}$, $h_l < h_{l+1}$, for $l = 1, \ldots, s-1$, and $i_l < i_{l+1}$ for $l = 1, \ldots, r-1$. Then
$$x_{j_1}^{a_1} \cdots x_{j_s}^{a_s} \trianglelefteq x_{h_1}^{a_1} \cdots x_{h_s}^{a_s}$$
if and only if $j_k \leq h_k$ for all $1 \leq k \leq s$.
(iii) Let $1 \leq k \leq m-1$. For $M, M' \in K[x_1, \ldots, x_k]$, $\tilde{M}, \tilde{M}' \in K[x_{k+1}, \ldots, x_m]$, if $M \trianglelefteq M'$ and $\tilde{M} \trianglelefteq \tilde{M}'$, then
$$M\tilde{M} \trianglelefteq M'\tilde{M}'.$$

Notice that $\trianglelefteq$ is a partial order on R.

Example 4.5. Over $\mathbb{F}_5$, take $S_1 = S_2 = \{0, 1, 2\}$ and $S_3 = \mathbb{F}_5$. As $x_3 | x_2^2 x_3$, $x_3 \trianglelefteq x_2^2 x_3$. Since $S_2 = S_1$, $x_1 \trianglelefteq x_2$. Finally, since $x_1 \trianglelefteq x_2$, $x_1 x_3 \trianglelefteq x_2 x_3$.

A **polar decreasing monomial-Cartesian code** is a decreasing monomial-Cartesian code $C(\mathcal{S}, \mathcal{M})$, where $\mathcal{M}$ is closed under $\trianglelefteq$.

In [3], the authors described the information set of a binary polar code over any symmetric binary channel using the last order. In [7], the authors extended the result to SOF channels using kernels from algebraic curves. In both works, authors proved that they can analyse the polarization process inductively and then we can change the kernel in any step in order to build polar codes of any length without changing the structural analysis of the final code. Theorem 4.8 will demonstrate that given a SOF channel W, any (multikernel) polar code constructed from $\{T_i\}_{i=1}^m$ kernels of size $n_i \times n_i$ as before is a polar decreasing monomial-Cartesian code. In preparation, we consider the next result which shows that if M and M' are two monomials in $K[x_1, \ldots, x_m]$ such that $M \trianglelefteq M'$, then M represents a better channel than M'. Indeed, if M divides M', then the support of M' contains the support of M and by the SOF property, the channel associated to M' is less relevant than the one associated to M.

Lemma 4.6. *Let $\{T_i\}_{i=1}^m$ be the sequence of matrices associated to the sequence of sets $\{S_i\}_{i=1}^m$ of K. Let $G_m = B_m(T_1 \otimes \cdots \otimes T_m)$ as before. Let W be a SOF channel. If M, M' are two monomials in $K[x_1, \ldots, x_m]$ and $M \trianglelefteq M'$, then*

$$I(M) \geq I(M') \qquad \text{and} \qquad Z(M) \leq Z(M').$$

Proof. Set $n = \prod_{i=1}^m n_i$ and suppose that the output alphabet of W is $\mathcal{Y}$ and consider

$$f : \mathcal{Y}^n \times K^{n_m(i-1)} \to \left(\mathcal{Y}^{\frac{n}{n_m}} \times K^{i-1}\right)^{n_m}$$

defined by $f\left(y_1^n, u_1^{n_m(i-1)}\right) =$

$$\left(y_{(k-1)\frac{n}{n_m}}^{k\frac{n}{n_m}+1}, u_1^{n_m} Col_k(T_m), \ldots, u_{(i-2)n_m+1}^{(i-1)n_m} Col_k(T_m)\right).$$

Since f is just a reordering of the entries of a vector, f is a bijection between the output alphabets of $(W_{m-1}^{(i)})_1^{(j)}$ (using the kernel T_m) and $W_m^{((i-1)n_m+j)}$, which implies that their mutual information and their Bhattacharyya parameters are equal (cf. [7, Proposition 8]).

From the previous paragraph, we have that if M is associated to $W_{m-1}^{(i)}$ for some $1 \leq i \leq \frac{n}{n_m}$, then Mx_m^j is associated to the channel $W_m^{((i-1)n_m+j)}$. Any Reed-Solomon kernel $T(S)$ can be viewed as the kernel associated to the projective line, which is a curve of genus 0 and therefore a Castle curve. Due to [7, Theorem 24], we have that if $j < j'$, the associated channel to $Mx_m^{j'}$ is degraded from Mx_m^j, and by [7, Proposition 21] this means that

$$I(Mx_m^j) \geq I(Mx_m^{j'}) \qquad \text{and} \qquad Z(Mx_m^j) \leq Z(Mx_m^{j'}).$$

The last statement applies to any $m \geq 1$. Therefore by [7, Proposition 22] we can conclude that if $M|M'$ then the conclusion holds.

On the other hand, if $M' \trianglelefteq M$ in the sense of (ii) in Definition 4.4, by using similar arguments in the proof of [7, Proposition 34], we can conclude the result. $\square$

If the set $\mathcal{A}_m$ given in Definition 2.13 is given as monomials, rather than indices of rows, then a characterization of $\mathcal{A}_m$ is obtained as follows.

Proposition 4.7. *Let $\{T_i\}_{i=1}^m$ be the sequence of matrices associated with a sequence of sets $\{S_i\}_{i=1}^m$ of K. Let $\mathcal{A}_m$ be an* *information set given in Definition 2.13 using a SOF channel W by the sequence $\{T_i\}_{i=1}^m$. If $M \in \mathcal{A}_m$ and $M' \trianglelefteq M$, then $M' \in \mathcal{A}_m$.*

Proof. If $M' \trianglelefteq M$, for the last lemma we have $Z(M') \leq Z(M)$. However, by the definition of polar code, since $M \in \mathcal{A}_m$, M' cannot be in $\mathcal{A}_m$, and we have the conclusion. □

We now come to one of the main results of this section. The following theorem shows that any polar code constructed from a sequence of subsets of K is a polar decreasing monomial-Cartesian code.

Theorem 4.8. *Let $\{S_i\}_{i=1}^\infty$ be a sequence of subsets of $\mathbb{F}_q$, $|S_i| \geq 2$ for any $i \in \mathbb{N}$, and let $\{T_i\}_{i=1}^\infty$ be the sequence of associated matrices. Then $\{T_i\}_{i=1}^\infty$ polarizes any SOF channel and a polar code $C_{\mathcal{A}_m}$ given in Definition 2.13 is a polar decreasing monomial-Cartesian code.*

Proof. It is clear that $C_{\mathcal{A}_m}$ is the monomial-Cartesian code using the monomials of $\mathcal{A}_m$ as stated before. If $M'|M \in \mathcal{A}_m$, in particular we have $M' \trianglelefteq M$ and by the last Proposition we have $M' \in \mathcal{A}_m$. Therefore, $\mathcal{A}_m$ is a decreasing set and $C_{\mathcal{A}_m}$ is decreasing too. □

In [12], the authors analyzed through a different order the information set for polar codes constructed with G_A.We can find a set of monomials $\mathcal{M}'$ such that

$$\mathcal{A}_n = \{M \mid M \trianglelefteq M',\ M' \in \mathcal{M}'\}.$$

If we choose $\mathcal{M}'$ to be minimal, then we can called it a generating set of $\mathcal{A}_n$ as in [12]. However, since $\trianglelefteq$ considers more than just the divisibility, if $\mathcal{B}(\mathcal{A}_n)$ is the minimal generating set in the sense of Definition 3.5, $\mathcal{B}(\mathcal{A}_n)$ could be bigger than $\mathcal{M}'$. For example, consider $S_1 = S_3 = \{0, 1, 2\} \subseteq \mathbb{F}_5$ and $S_2 = \mathbb{F}_5$. If we take

$$\mathcal{A}_3 = \{x_2^2x_3, x_2x_3, x_3, x_2^2, x_2, x_1, 1\},$$

a minimal basis respect to $\trianglelefteq$ is $\{x_2^2x_3\}$, but $\mathcal{B}(\mathcal{A}_3) = \{x_2^2x_3, x_1\}$.

V. Conclusion

In this paper, we prove that if a sequence of invertible matrices $\{T_i\}_{i=1}^\infty$ over an arbitrary field $\mathbb{F}_q$ has the property that every T_i has a non-identity standard form, then the sequence $\{T_i\}_{i=1}^\infty$ polarizes any symmetric over the field channel (SOF channel) W. Given a sequence $\{T_i\}_{i=1}^\infty$ that polarizes, and a natural number m, we define a polar code as the space generated by some rows of the matrix G_m, where G_m is defined inductively taking $G_1 = T_1$ and for $m \geq 2$,

$$G_m = \begin{bmatrix} G_{m-1} \otimes Row_1 T_m \\ G_{m-1} \otimes Row_2 T_m \\ \vdots \\ G_{m-1} \otimes Row_{l_m} T_m \end{bmatrix}.$$

Given a set of monomials $\mathcal{M}$ that is closed under divisibility and a Cartesian product $\mathcal{S}$, we used the theory of evaluation codes to study decreasing monomial-Cartesian codes, which are defined by evaluating the monomials of $\mathcal{M}$ over the set $\mathcal{S}$. We prove that the dual of a decreasing monomial-Cartesian code is a code of the same type. Then we describe its basic parameters in terms of the minimal generating set of $\mathcal{M}$. These codes are important because when the set $\mathcal{M}$ is also closed under the monomial order $\trianglelefteq$, then the evaluation code is a polar decreasing monomial-Cartesian code. Strengthening the symmetry required of the channel and using matrices associated with subsets of a finite field $\mathbb{F}_q$, we prove that families of polar codes with multiple kernels can be viewed as decreasing monomial-Cartesian codes and therefore any information set $\mathcal{A}_n$ can be described in a similar way, offering a unified treatment for this kind of codes.

Acknowledgments

The authors wish to thank the editor and reviewers whose comments and suggestions have improved this manuscript.

The first and fourth author were partially supported by SIP-IPN, project 20195717, and CONACyT. The second author was partially supported by an AMS–Simons Travel Grant. The third author was supported in part by NSF DMS-1855136 and the Commonwealth Cyber Initiative.

References

[1] E. Arikan, Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels, IEEE Transactions on Information Theory, **55** (2019), no. 7, 3051–3073. https://doi.org/10.1109/TIT.2009.2021379

[2] J. Bae, A. Abotabl, H. Lin, K. Song and J. Lee, An overview of channel coding for 5G NR cellular communications, APSIPA Transactions on Signal and Information Processing, **8** (2019), E17. https://doi.org/10.1017/ATSIP.2019.10

[3] M. Bardet, V. Dragoi, A. Otmani and J. Tillich, Algebraic properties of polar codes from a new polynomial formalism, 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona (2016), 230–234. https://doi.org/10.1109/ISIT.2016.7541295

[4] M. Benammar, V. Bioglio, F. Gabry and I. Land, Multi-kernel polar codes: Proof of polarization and error exponents, 2017 IEEE Information Theory Workshop (ITW), Kaohsiung (2017), 101–105. https://doi.org/10.1109/ITW.2017.8277949

[5] V. Bioglio, C. Condo and I. Land, Design of Polar Codes in 5G New Radio, IEEE Communications Surveys & Tutorials (2020). https://doi.org/10.1109/COMST.2020.2967127

[6] E. Camps, H. López, G. Matthews and E. Sarmiento, Monomial-Cartesian codes closed under divisibility, De Gruyter Proceedings in Mathematics (2020), 199–208. https://doi.org/10.1515/9783110621730-014

[7] E. Camps Moreno, E. Martínez-Moro and E. Sarmiento Rosales, Vardohus Codes: Polar Codes Based on Castle Curves Kernels, IEEE Transactions on Information Theory, **66** (2020), no. 2, 1007–1022. https://doi.org/10.1109/TIT.2019.2932405

[8] C. Carvalho, On the second Hamming weight of some Reed-Muller type codes, Finite Fields and Their Applications, **24** (2013), 88–94. https://doi.org/10.1016/j.ffa.2013.06.004

[9] F. Gabry, V. Bioglio, I. Land and J. Belfiore, Multi-kernel construction of polar codes, 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris (2017), 761–765. https://doi.org/10.1109/ICCW.2017.7962750

[10] O. Geil, and C. Thomsen, Weighted Reed-Muller codes revisited, Designs Codes and Cryptography, **66** (2013), 195–220. https://doi.org/10.1007/s10623-012-9680-8

[11] S. B. Korada, E. Şaşoğlu and R. Urbanke, Polar Codes: Characterization of Exponent, Bounds, and Constructions, IEEE Transactions on Information Theory, **56** (2010), no. 12, 6253–6264. https://doi.org/10.1109/TIT.2010.2080990

[12] D. Kim, K. Oh, D. Kim and J. Ha, Information set analysis of polar codes, 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju (2016), 813–815. https://doi.org/10.1109/ICTC.2016.7763304

[13] M. Lee and K. Yang, The exponent of a polarizing matrix constructed from the Kronecker product, Designs Codes and Cryptography, **70** (2014), 313–322. https://doi.org/10.1007/s10623-012-9689-z

[14] H. H. López, G. L. Matthews and I. Soprunov, Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes, Designs Codes and Cryptography, **88** (2020), 1673–1685. https://doi.org/10.1007/s10623-020-00726-x

[15] H. H. López, C. Rentería-Márquez and R. H. Villarreal, Affine Cartesian codes, Designs Codes and Cryptography, **71** (2014), no. 1, 5–19. https://doi.org/10.1007/s10623-012-9714-2

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

[17] J. L. Massey, Linear codes with complementary duals, Discrete Mathematics, **106–107** (1992), no. 1, 337–342. https://doi.org/10.1016/0012-365X(92)90563-U

[18] R. Mori and T. Tanaka, Non-binary polar codes using Reed–Solomon codes and algebraic geometry codes, 2010 IEEE Information Theory Workshop, Dublin (2010), 1–5. https://doi.org/10.1109/CIG.2010.5592755

[19] R. Mori and T. Tanaka, Channel polarization on q-ary discrete memoryless channels by arbitrary kernels, 2010 IEEE International Symposium on Information Theory, Austin, TX (2010), 894–898. https://doi.org/10.1109/ISIT.2010.5513568

[20] R. Mori and T. Tanaka, Source and Channel Polarization Over Finite Fields and Reed–Solomon Matrices, IEEE Transactions on Information Theory, **60** (2014), no. 5, 2720–2736. https://doi.org/10.1109/TIT.2014.2312181

[21] K. Niu, K. Chen and J. Lin, Beyond turbo codes: Rate-compatible punctured polar codes, 2013 IEEE International Conference on Communications (ICC), Budapest (2013), 3423–3427. https://doi.org/10.1109/ICC.2013.6655078

[22] E. Şaşoğlu, Polar Coding Theorems for Discrete Systems, Doctoral dissertation, École Polytechnique Fédérale de Lausanne. https://infoscience.epfl.ch/record/168993?ln=en

[23] E. Şaşoğlu, E. Telatar and E. Arikan, Polarization for arbitrary discrete memoryless channels, 2009 IEEE Information Theory Workshop, Taormina (2009), 144–148. https://doi.org/10.1109/ITW.2009.5351487

[24] G. Sarkis, P. Giard, A. Vardy, C. Thibeault and W. J. Gross, Fast List Decoders for Polar Codes, IEEE Journal on Selected Areas in Communications, **34** (2016), no. 2, 318–328. https://doi.org/10.1109/JSAC.2015.2504299

[25] I. Tal and A. Vardy, How to Construct Polar Codes, IEEE Transactions on Information Theory, **59** (2013), no. 10, 6562–6582. https://doi.org/10.1109/TIT.2013.2272694

[26] I. Tal and A. Vardy, List decoding of polar codes, 2011 IEEE International Symposium on Information Theory Proceedings, St. Petersburg (2011), 1–5. https://doi.org/10.1109/ISIT.2011.6033904

[27] I. Tamo and A. Barg, A Family of Optimal Locally Recoverable Codes, IEEE Transactions on Information Theory, **60** (2014), no. 8, 4661–4676. https://doi.org/10.1109/TIT.2014.2321280

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

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

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

[31] R. Wang and R. Liu, A Novel Puncturing Scheme for Polar Codes, IEEE Communications Letters, **18** (2014), no. 12, 2081–2084. https://doi.org/10.1109/LCOMM.2014.2364845

[32] R. Wang and R. Liu, A Novel Puncturing Scheme for Polar Codes, IEEE Communications Letters, **18** (2014), no. 12, 2081–2084. https://doi.org/10.1109/LCOMM.2014.2364845

Eduardo Camps received the B. Sc. and M. Sc. degree in mathematics and physics from Instituto Politécnico Nacional, México, in 2018 and 2019 respectively. He is currently pursuing his Ph.D. degree in Science in the same institution. His research interests include subjects related to information theory, coding theory and commutative algebra.

Hiram H. López is an Assistant Professor at Cleveland State University. He earned the B.S. degree in applied mathematics from Autonomous University of Aguascalientes in 2008 and the Ph.D. degree in mathematics from CINVESTAV-IPN in 2016. After a postdoctoral position at Clemson University from 2016 to 2018 he joined Cleveland State University in 2019. His research interests include coding theory, commutative algebraic and image processing.

Eliseo Sarmiento received the B. Sc. and M. Sc. degree in mathematics and phyisics from Instituto Politécnico Nacional in 2007 and 2008 respectively; he received the Ph.D. degree in Science from CINVESTAV-IPN in 2012. He is currently researcher at Instituto Politécnico Nacional. His research interests include subjects related to information theory, coding theory, combinatorics and algebra.

Gretchen L. Matthews is a Professor in the Department of Mathematics at Virginia Tech. She earned the B.S. degree in mathematics from Oklahoma State University in 1995 and the Ph.D. degree in mathematics from Louisiana State University in 1999. Following postdoctoral work at the University of Tennessee, she was on the faculty at Clemson University before joining Virginia Tech in 2018. Her research interests include algebraic geometry and combinatorics and their applications to coding theory.