

Received February 8, 2022, accepted March 27, 2022, date of publication April 5, 2022, date of current version April 15, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3165032

# A Family of Codes With Locality Containing Optimal Codes

BRUNO ANDRADE<sup>1</sup>, CÍCERO CARVALHO<sup>1</sup>, VICTOR G. L. NEUMANN<sup>1</sup>,  
AND ANTÔNIO C. P. VEIGA<sup>2</sup>

<sup>1</sup>Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia 38408-902, Brazil

<sup>2</sup>Faculdade de Engenharia Elétrica, Universidade Federal de Uberlândia, Uberlândia 38408-902, Brazil

Corresponding author: Bruno Andrade (brunoandrade@ufu.br)

This work was supported in part by FAPEMIG—Fundação de Amparo à Pesquisa de Minas Gerais, Brazil, under Grant APQ-03518-18 and Grant APQ-00864-21.

**ABSTRACT** Locally recoverable codes were introduced by Gopalan *et al.* in 2012, and in the same year Prakash *et al.* introduced the concept of codes with locality, which are a type of locally recoverable codes. In this work we introduce a new family of codes with locality, which are subcodes of a certain family of evaluation codes. We determine the dimension of these codes, and also bounds for the minimum distance. We present the true values of the minimum distance in special cases, and also show that some elements of this family are “optimal codes”, as defined by Prakash *et al.*

**INDEX TERMS** Locally recoverable codes, affine cartesian codes.

## I. INTRODUCTION

The class of locally recoverable codes was introduced in 2012 by Gopalan *et al.* (see [16]). The idea was to ensure reliable communication when using distributed storage systems. Thus the authors define a code as having locality  $r$  if an entry at position  $i$  of a codeword of length  $n$  may be recovered from a set (which may vary with  $i$ ) of at most  $r$  other entries, for all  $i = 1, \dots, n$ . This would ensure the recovering of a codeword even in the presence of an erasure, due for example to a failure of some node in the network. In that same year Prakash *et al.* (see [19]) introduced the concept of codes with locality  $(r, \delta)$ , also called  $(r, \delta)$ -locally recoverable codes, which are codes of length  $n$  such that for every position  $i \in \{1, \dots, n\}$  there is a subset  $S_i \subset \{1, \dots, n\}$  containing  $i$  and of size at most  $r + \delta - 1$  such that the  $i$ -th entry of a codeword may be recovered from any subset of  $r$  entries with positions in  $S_i \setminus \{i\}$ , so that we may recover any entry even with  $\delta - 2$  other erasures in the code.

In this paper we define a family consisting of subcodes of the so-called affine cartesian codes (see Definition 2.2) which are  $(r, \delta)$ -locally recoverable codes. We determine their dimension (see Corollary 3.4 and Theorem 3.6) together with lower and upper bounds for the minimum distance (see Theorem 4.1). We list some cases where the codes are optimal

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang<sup>1</sup>.

(see Corollary 4.2) and we also determine the exact value of the minimum distance in some special cases of the code (see Theorem 4.1, Theorem 5.8 and Corollary 5.9).

The content of the paper is as follows. In the next section we introduce a family of codes, which we prove that are locally recoverable. In Section 3 we present several results on the dimension of these codes, after recalling some facts from Gröbner basis theory which we will need. In the following section we present lower and upper bounds for the minimum distance of these codes, and determine the exact values in some cases. We also prove that some of the codes we introduced are optimal codes. In Section 5 we treat a special case of the codes that we have introduced, and for this case we determine more values for the minimum distance. The paper ends with several numerical examples.

## II. A FAMILY OF LOCALLY RECOVERABLE CODES

Let  $\mathbb{F}_q$  be a finite field with  $q$  elements.

**Definition 2.1:** Let  $m, r, \delta$  be positive integers, with  $\delta \geq 2$  and  $r + \delta - 1 \leq m$ . We say that a (linear) code  $\mathcal{C} \subset \mathbb{F}_q^m$  is  $(r, \delta)$ -locally recoverable if for every  $i \in \{1, \dots, m\}$  there exists a subset  $S_i \subset \{1, \dots, m\}$ , containing  $i$  and of cardinality at most  $r + \delta - 1$ , such that the punctured code obtained by removing the entries which are not in  $S_i$  has minimum distance at least  $\delta$ .

The condition on the minimum distance in the above definition shows that one cannot have two distinct codewords in the punctured code which coincide in (at least)  $r$  positions,

so any  $r$  positions in the set  $S_i$  determine the remaining  $\delta - 1$  positions.

Let  $K_1, \dots, K_n$  be a collection of non-empty subsets of  $\mathbb{F}_q$ , and let

$$\begin{aligned} \mathcal{X} &:= K_1 \times \dots \times K_n \\ &:= \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in K_i \text{ for all } i\} \subset \mathbb{F}_q^n. \end{aligned}$$

Let  $d_i := |K_i|$  for  $i = 1, \dots, n$ , so clearly  $|\mathcal{X}| = \prod_{i=1}^n d_i =: m$ , and let  $\mathcal{X} = \{\alpha_1, \dots, \alpha_m\}$ . It is not difficult to check that the ideal of polynomials in  $\mathbb{F}_q[X_1, \dots, X_n]$  which vanish on  $\mathcal{X}$  is

$$I_{\mathcal{X}} = \left( \prod_{\alpha_1 \in K_1} (X_1 - \alpha_1), \dots, \prod_{\alpha_n \in K_n} (X_n - \alpha_n) \right)$$

(see e.g. [18, Lemma 2.3] or [7, Lemma 3.11]). The evaluation morphism

$$\begin{aligned} \Psi: \mathbb{F}_q[X_1, \dots, X_n] &\rightarrow \mathbb{F}_q^m \\ f &\mapsto (f(\alpha_1), \dots, f(\alpha_m)) \end{aligned}$$

is an  $\mathbb{F}_q$ -linear map and  $\ker \Psi = I_{\mathcal{X}}$ . Actually, this is a surjective map because for each  $i \in \{1, \dots, m\}$  there exists a polynomial  $f_i$  such that  $f_i(\alpha_j)$  is equal to 1, if  $j = i$ , or 0, if  $j \neq i$ .

Let  $d$  be a nonnegative integer. In what follows we will denote by  $\mathbb{F}_q[X_1, \dots, X_n]_{\leq d}$  the  $\mathbb{F}_q$ -vector space formed by all polynomials of degree up to  $d$ , together with the zero polynomial.

**Definition 2.2:** Let  $d$  be a nonnegative integer. The *affine cartesian code* (of order  $d$ )  $\mathcal{C}_{\mathcal{X}}(d)$  defined over the sets  $K_1, \dots, K_n$  is the image, by  $\Psi$ , of the polynomials in  $\mathbb{F}_q[X_1, \dots, X_n]_{\leq d}$ .

These codes appeared independently in [18] and [15] (in [15] in a generalized form). In the special case where  $K_1 = \dots = K_n = \mathbb{F}_q$  we have the well-known generalized Reed-Muller code of order  $d$ . In [18] the authors prove that we may ignore, in the cartesian product, sets with just one element and moreover may always assume that  $2 \leq d_1 \leq \dots \leq d_n$ . The dimension and the minimum distance of these codes are known (see e.g. [18] or [15]).

In what follows we construct  $(r, \delta)$ -locally recoverable codes which are subcodes of affine cartesian codes.

**Definition 2.3:** Let  $d$  and  $\delta$  be integers with  $d \geq 0$  and  $\delta \geq 2$ , let  $s \in \{1, \dots, n\}$  and let  $\mathcal{P}_d^{(\delta, s)}$  be the set of polynomials  $f \in \mathbb{F}_q[X_1, \dots, X_n]_{\leq d}$  such that  $\deg_{X_s} f < d_s - \delta + 1$ , together with the zero polynomial. We denote by  $\mathcal{D}_{\mathcal{X}}^{(\delta, s)}(d)$  the code which is the image by  $\Psi$  of the set  $\mathcal{P}_d^{(\delta, s)}$ .

**Theorem 2.4:** Let  $K_1, \dots, K_n$  be subsets of  $\mathbb{F}_q$  such that  $|K_i| = d_i \geq 2$  for all  $i = 1, \dots, n$ , with  $n \geq 2$ , let  $\delta \geq 2$  be an integer such that  $d_s - \delta + 1 \geq 1$  and let  $d$  be a nonnegative integer. For any  $s \in \{1, \dots, n\}$  the code  $\mathcal{D}_{\mathcal{X}}^{(\delta, s)}(d)$  is locally recoverable with locality  $(r, \delta)$ , where  $r = d_s - \delta + 1$ .

*Proof:* Let  $f \in \mathcal{P}_d^{(\delta, s)}$ , so  $(f(\alpha_1), \dots, f(\alpha_m)) \in \mathcal{D}_{\mathcal{X}}^{(\delta, s)}(d)$ . Let  $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathcal{X}$  and let

$$I_{\alpha} = \{(\alpha_1, \dots, \alpha_{s-1}, \beta, \alpha_{s+1}, \dots, \alpha_n) \mid \beta \in K_s\},$$

a set which has  $d_s = r + \delta - 1$  elements. Assume that there exist  $\beta_1, \dots, \beta_r \in I_{\alpha}$  such that we know the values  $f(\beta_k) =: c_k$ , for  $k \in \{1, \dots, r\}$ . We will prove that then we can deduce the value of  $f(\beta)$  for any  $\beta \in I_{\alpha}$ .

Write  $f = \sum_{i=0}^{r-1} g_i X_s^i$ , where  $g_1, \dots, g_{r-1}$  are polynomials in the variables  $X_1, \dots, X_{s-1}, X_{s+1}, \dots, X_n$ , and let  $b_i := g_i(\alpha_1, \dots, \alpha_{s-1}, \alpha_{s+1}, \dots, \alpha_n)$  for  $i = 0, \dots, r-1$ . Denoting by  $\beta_k$  the  $k$ -th coordinate of  $\beta_k$ , for  $k = 1, \dots, r$ , from the assumption we get that

$$c_k = f(\beta_k) = \sum_{i=0}^{r-1} b_i \beta_k^i, \quad \text{for } k \in \{1, \dots, r\}.$$

This system of equations can be rewritten as a matrix equation

$$\begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \dots & \beta_1^{r-1} \\ 1 & \beta_2 & \beta_2^2 & \dots & \beta_2^{r-1} \\ 1 & \beta_3 & \beta_3^2 & \dots & \beta_3^{r-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_r & \beta_r^2 & \dots & \beta_r^{r-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{r-1} \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_r \end{pmatrix},$$

which has a unique solution  $(b_0, b_1, \dots, b_{r-1})$ , since the square  $r \times r$  matrix is a Vandermonde matrix. This allows us to determine  $f(\beta)$  for any  $\beta \in I_{\alpha}$ .  $\square$

### III. ON THE DIMENSION OF $\mathcal{D}_{\mathcal{X}}^{(\delta, s)}(d)$

In this section we determine the dimension of  $\mathcal{D}_{\mathcal{X}}^{(\delta, s)}(d)$ , and we will need some facts about Gröbner basis which we recall below. The interested reader may want to consult one of the many books on the subject, e.g [1].

Let  $\prec$  be a monomial order in (the set of monomials of)  $\mathbb{F}_q[X_1, \dots, X_n]$ , i.e.  $\prec$  is a total order, if  $M_1 \prec M_2$  then  $MM_1 \prec MM_2$  for all monomials  $M, M_1, M_2$ , and 1 is the least monomial. The greatest monomial appearing in a polynomial  $f$  is called the leading monomial of  $f$  and is denoted by  $LM(f)$ .

**Definition 3.1:** Let  $J \subset \mathbb{F}_q[X_1, \dots, X_n]$  be an ideal. A *Gröbner basis* (with respect to a monomial order  $\prec$ ) for  $J$  is a basis  $G$  for  $J$  such that the leading monomial of any polynomial in  $J$  is a multiple of the leading monomial of some polynomial in  $G$ . The *footprint* of  $J$  (with respect to a monomial order  $\prec$ ) is the set of monomials of  $\mathbb{F}_q[X_1, \dots, X_n]$  which are not leading monomials of any polynomials in  $J$ , and is denoted by  $\Delta(J)$ .

B. Buchberger proved that, given a monomial order, any (nonzero) ideal  $J \subset \mathbb{F}_q[X_1, \dots, X_n]$  admits a Gröbner basis (see [2], [3] or [1, Sec. 1.7]). He also proved that a basis for  $\mathbb{F}_q[X_1, \dots, X_n]/J$  as an  $\mathbb{F}_q$ -vector space is given by the classes of the monomials in  $\Delta(J)$  (see e.g. [1, Prop. 2.1.6]).

**Definition 3.2:** Let  $\prec$  be a monomial order in  $\mathbb{F}_q[X_1, \dots, X_n]$  and let  $J \subset \mathbb{F}_q[X_1, \dots, X_n]$  be an ideal. Let  $\{g_1, \dots, g_r\}$  be a (not necessarily Gröbner) basis for  $J$ , we define  $\Delta(LM(g_1), \dots, LM(g_r))$  as the set of monomials of  $\mathbb{F}_q[X_1, \dots, X_n]$  which are not multiples of any of the leading monomials of  $g_1, \dots, g_r$ .

Clearly we have  $\Delta(J) \subset \Delta(LM(g_1), \dots, LM(g_r))$  and, moreover,  $\Delta(J) = \Delta(LM(g_1), \dots, LM(g_r))$  if and only if  $\{g_1, \dots, g_r\}$  is a Gröbner basis for  $J$ .

In what follows we will use the graded-lexicographic order in  $\mathbb{F}_q[X_1, \dots, X_n]$ , with  $X_n < \dots < X_1$ .

For  $i = 1, \dots, n$  let  $f_i = \prod_{\alpha \in K_i} (X_i - \alpha)$ , so that  $\deg f_i = d_i$  and  $I_{\mathcal{X}} = \langle f_1, \dots, f_n \rangle$ . Since any two of the leading monomials of  $f_1, \dots, f_n$  are coprime we get that  $\{f_1, \dots, f_n\}$  is a Gröbner basis for  $I_{\mathcal{X}}$  (see [14, Prop. 4, page 104]) so

$$\begin{aligned} \Delta(I_{\mathcal{X}}) &= \Delta(X_1^{d_1}, \dots, X_n^{d_n}) \\ &= \{X_1^{a_1} \cdots X_n^{a_n} \mid 0 \leq a_i < d_i, \forall i = 1, \dots, n\}. \end{aligned}$$

Let  $\Delta(I_{\mathcal{X}})_{\leq d} = \{M \in \Delta(I_{\mathcal{X}}) \mid \deg(M) \leq d\}$ , it is known (see e.g. [7, Prop. 3.12]) that  $\dim(\mathcal{C}_{\mathcal{X}}(d)) = |\Delta(I_{\mathcal{X}})_{\leq d}|$ . This implies that if  $d \geq \sum_{i=1}^n (d_i - 1)$  then  $\dim(\mathcal{C}_{\mathcal{X}}(d)) = |\Delta(I_{\mathcal{X}})_{\leq d}| = |\Delta(I_{\mathcal{X}})| = \prod_{i=1}^n d_i$ , while if  $0 \leq d < \prod_{i=1}^n d_i$  then

$$\begin{aligned} \dim(\mathcal{C}_{\mathcal{X}}(d)) &= \binom{n+d}{d} - \sum_{i=1}^n \binom{n+d-d_i}{d-d_i} \\ &\quad + \cdots + (-1)^j \sum_{1 \leq i_1 < \dots < i_j \leq n} \binom{n+d-d_{i_1}-\dots-d_{i_j}}{d-d_{i_1}-\dots-d_{i_j}} \\ &\quad + \cdots + (-1)^n \binom{n+d-d_1-\dots-d_n}{d-d_1-\dots-d_n} \end{aligned}$$

where we set  $\binom{a}{b} = 0$  if  $b < 0$ .

To determine the dimension of  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  we give an argument similar to the one used to prove the above formulas.

**Proposition 3.3:** Let

$$\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} = \{M \in \Delta(I_{\mathcal{X}})_{\leq d} \mid \deg_{X_s} M < d_s - \delta + 1\},$$

then  $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = |\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}|$ .

*Proof:* Given  $f \in \mathcal{P}_d^{(\delta,s)}$  let  $g \in \mathbb{F}_q[X_1, \dots, X_n]$  be its remainder in the division by  $\{f_1, \dots, f_n\}$ , then  $\Psi(f) = \Psi(g)$ . From the division algorithm we know that any monomial which appear in  $g$  is not a multiple of  $LM(f_i) = X_i^{d_i}$  for all  $i = 1, \dots, n$ , and also that  $\deg g \leq \deg f$  and  $\deg_{X_s} g < d_s - \delta + 1$ . Thus  $g \in \mathcal{P}_d^{(\delta,s)}$  and moreover,  $g$  is a linear combination of monomials in  $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$ . This shows that  $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) \leq |\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}|$ . Let

$$\bar{\Psi}: \mathbb{F}_q[X_1, \dots, X_n]/I_{\mathcal{X}} \rightarrow \mathbb{F}_q^m$$

be defined as  $\bar{\Psi}(f + I_{\mathcal{X}}) = \Psi(f)$ , we know that  $\bar{\Psi}$  is an isomorphism and clearly

$$\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \{\bar{\Psi}(h + I_{\mathcal{X}}) \mid h \in \langle \Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} \rangle\},$$

where  $\langle \Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} \rangle$  is the  $\mathbb{F}_q$ -vector space generated by the monomials in  $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$ . Since  $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} \subset \Delta(I_{\mathcal{X}})$  we know from Buchberger's result (see e.g. [1, Prop. 2.1.6]) that the classes in  $\mathbb{F}_q[X_1, \dots, X_n]/I_{\mathcal{X}}$  of the monomials in  $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$  are linearly independent over  $\mathbb{F}_q$ , thus we get

$$\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = |\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}|.$$

□

Let

$$\tilde{d} := \sum_{\substack{i=1 \\ i \neq s}}^n (d_i - 1) + d_s - \delta.$$

**Corollary 3.4:** If  $d \geq \tilde{d}$  then  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})$ , and

$$\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) = (d_s - \delta + 1) \prod_{\substack{i=1 \\ i \neq s}}^n d_i.$$

Also  $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d} - 1)) = \dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) - 1$ .

*Proof:* From the above proof we get that if  $M \in \Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)}$  then  $\deg_{X_s}(M) < d_s - \delta + 1$  and  $\deg_{X_i}(M) < d_i$  for all  $i \in \{1, \dots, n\} \setminus \{s\}$ . Thus if  $d \geq \tilde{d}$  we have  $\Delta(I_{\mathcal{X}})_{\leq d}^{(\delta,s)} = \Delta(I_{\mathcal{X}})_{\leq \tilde{d}}^{(\delta,s)}$  which implies  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})$ . We also have that

$$\begin{aligned} \dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) &= |\{X_1^{a_1} \cdots X_n^{a_n} \mid 0 \leq a_i < d_i, i = 1, \dots, n, i \neq s, \text{ and} \\ &\quad 0 \leq a_s < d_s - \delta + 1\}| = (d_s - \delta + 1) \prod_{\substack{i=1 \\ i \neq s}}^n d_i \end{aligned}$$

Observe that in  $\Delta(I_{\mathcal{X}})_{\leq \tilde{d}}^{(\delta,s)}$  there is only one monomial of degree  $\tilde{d}$ , so that  $\dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d} - 1)) = \dim(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) - 1$ . □

Now, for  $1 \leq d < \tilde{d}$  (when  $d = 0$  we have  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(0) \simeq \mathbb{F}_q$ ), we present a formula for the dimension of  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  in terms of the dimension of certain affine cartesian codes, and for that we introduce some notation.

**Definition 3.5:** For  $s \in \{1, \dots, n\}$  we denote by  $\mathcal{X}_s$  the product

$$\mathcal{X}_s = K_1 \times \cdots \times K_{s-1} \times K_{s+1} \times \cdots \times K_n.$$

In the next result we relate the dimension of  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  to the dimensions of  $\mathcal{C}_{\mathcal{X}}(d)$  and the affine cartesian code  $\mathcal{C}_{\mathcal{X}_s}(d)$ .

**Theorem 3.6:** Let  $s \in \{1, \dots, n\}$  and let  $d$  be an integer such that  $1 \leq d < \tilde{d}$ . If  $1 \leq d < r = d_s - \delta + 1$  then  $\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}}(d)$ , and if  $r \leq d \leq \tilde{d}$  then

$$\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}}(d) - \sum_{i=0}^{\delta-2} \dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}_s}(d-r-i), \quad (1)$$

where  $\dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}_s}(d-r-i) = 0$  if  $d-r-i < 0$ .

If  $1 \leq d < r = d_s - \delta + 1$  then from Definitions 2.2 and 2.3 we get that  $\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}}(d)$ , so we assume now that  $r \leq d \leq \tilde{d}$ . Define the following sets:

$$\begin{aligned} \Omega_d &= \{(a_1, \dots, a_n) \in \mathbb{N}^n \mid 0 \leq a_i < d_i, \text{ for} \\ &\quad 1 \leq i \leq n, a_1 + \cdots + a_n \leq d\}; \end{aligned}$$

$$\Omega_d^{(\delta,s)} = \{(a_1, \dots, a_n) \in \Omega_d \mid a_s \leq d_s - \delta\}.$$

From previous considerations we get that  $\dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}}(d) = |\Omega_d|$  and  $\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = |\Omega_d^{(\delta,s)}|$ .

For any  $(a_1, \dots, a_n) \in \Omega_d$  we have that either  $a_s \leq d_s - \delta$  or  $a_s = d_s - \delta + 1 + i$  for some  $i$  in the range  $0 \leq i \leq \delta - 2$  (because  $a_s \leq d_s - 1$ ). If  $a_s = d_s - \delta + 1 + i = r + i$  then we have

$$a_1 + \dots + a_{s-1} + a_{s+1} + \dots + a_n \leq d - r - i,$$

and for  $0 \leq i \leq \delta - 2$  we define

$$\Omega_{s,d-r-i}^{(0)} = \{(a_1, \dots, a_n) \in \Omega_{d-r-i} \mid a_s = 0\},$$

so that  $\Omega_{s,d-r-i}^{(0)} = \emptyset$  if  $i$  is such that  $d - r - i < 0$ .

Thus we have

$$|\Omega_d| = |\Omega_d^{(\delta,s)}| + \sum_{i=0}^{\delta-2} |\Omega_{s,d-r-i}^{(0)}|$$

and since  $\dim_{\mathbb{F}_q} \mathcal{C}_{\mathcal{X}}(d-r-i) = |\Omega_{s,d-r-i}^{(0)}|$  for all  $i \in \{0, \dots, \delta - 2\}$  the above equation implies equation (1) in the statement.

#### IV. MINIMUM DISTANCE AND OPTIMAL CODES

In this section we relate the minimum distance of  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  to the minimum distance of the affine cartesian code  $\mathcal{C}_{\mathcal{X}}(d)$ . In what follows we denote by  $W^{(1)}(C)$  the minimum distance of a code  $C$ .

Let  $d$  be an integer in the range  $1 \leq d < \sum_{i=1}^n (d_i - 1)$ , and let  $k$  and  $\ell$  be uniquely defined by writing  $d = \sum_{i=1}^k (d_i - 1) + \ell$ , with  $0 < \ell \leq d_{k+1} - 1$  (if  $d < d_1 - 1$  then take  $k = 0$  and  $\ell = d$ , if  $k + 1 = n$  then we understand that  $\prod_{i=k+2}^n d_i = 1$ ). We recall that

$$W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)) = (d_{k+1} - \ell) \prod_{i=k+2}^n d_i \quad (2)$$

(see e.g. [18, Theorem 3.8]).

*Theorem 4.1:* Let

$$d = \sum_{i=1}^k (d_i - 1) + \ell$$

where  $0 \leq k < n$  and  $0 < \ell \leq d_{k+1} - 1$ .

We have

$$\begin{aligned} W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)) &\leq W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) \leq m - \dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) \\ &\quad - \left( \left\lceil \frac{\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)}{r} \right\rceil - 1 \right) (\delta - 1) + 1. \end{aligned} \quad (3)$$

where  $m = \prod_{i=1}^n d_i$ ,  $r = d_s - \delta + 1$  and for  $x \in \mathbb{R}$ ,  $\lceil x \rceil$  is the smallest integer such that  $x \leq \lceil x \rceil$ . If

(i)  $k + 2 \leq n$  and  $d_{k+2} \leq d_s$ , or

(ii)  $d_s \leq d_{k+1}$  and  $0 \leq d_s - (d_{k+1} - \ell) < r$

then we get  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ .

*Proof:* Since  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) \subset \mathcal{C}_{\mathcal{X}}(d)$ , we have  $W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)) \leq W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$ . From Theorem 2.4 we know that  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  is locally recoverable with locality  $(r, \delta)$ , so we may apply [19, Theorem 2] and we get the second inequality of (3).

Assume that  $k + 2 \leq n$  and  $d_{k+2} \leq d_s$ . We consider two cases,  $s \geq k+2$  and  $s < k+2$ , let's suppose first that  $s \geq k+2$ . Consider an element  $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathcal{X}$ , and consider distinct elements  $\beta_1, \dots, \beta_\ell \in K_{k+1}$ . Define the polynomial

$$f = \prod_{i=1}^k \prod_{\substack{\alpha \in K_i \\ \alpha \neq \alpha_i}} (X_i - \alpha) \cdot \prod_{i=1}^{\ell} (X_{k+1} - \beta_i). \quad (4)$$

Observe that  $f \in \mathcal{P}_d^{(\delta,s)}$  so that  $\Psi(f) \in \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ . Denoting by  $w(v)$  the weight of a codeword  $v$  we have  $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ , and we're done. Assume now that  $s < k + 2$ , from  $d_{k+2} \leq d_s$  we must have  $K_s = K_{k+1} = K_{k+2}$ . Clearly  $s \in \{1, \dots, k + 1\}$  so replacing  $K_s$  by  $K_{k+2}$  in (4) we still have  $f \in \mathcal{P}_d^{(\delta,s)}$  and  $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ .

Finally suppose that (ii) is satisfied, i.e.  $s \leq k + 1$  and  $0 \leq d_s - (d_{k+1} - \ell) < r$ , and to avoid overlapping with the previous case we also assume that either  $d_s < d_{k+2}$  or  $n = k + 1$ . Now we take

$$f = \prod_{\substack{i=1 \\ i \neq s}}^{k+1} \prod_{\alpha \in K_i, \alpha \neq \alpha_i} (X_i - \alpha) \cdot \prod_{i=1}^{d_s - (d_{k+1} - \ell)} (X_s - \beta_i),$$

where  $\beta_1, \dots, \beta_{d_s - (d_{k+1} - \ell)}$  are distinct elements of  $K_s$ , and again we have  $f \in \mathcal{P}_d^{(\delta,s)}$ ,  $\Psi(f) \in \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  and  $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ .  $\square$

Following [19], we say that the code  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  is *optimal* if its minimum distance attains the upper bound presented in the above theorem.

*Corollary 4.2:* The codes  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})$  and  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d} - 1)$  are optimal, and have minimum distance equal to, respectively,  $\delta$  and  $\delta + 1$ .

*Proof:* We have

$$\tilde{d} = \sum_{\substack{i=1 \\ i \neq s}}^n (d_i - 1) + d_s - \delta = \sum_{i=1}^{n-1} (d_i - 1) + d_n - \delta$$

so from (2) we get  $W^{(1)}(\mathcal{C}_{\mathcal{X}}(\tilde{d})) = d_n - (d_n - \delta) = \delta$ . On the other hand, from Corollary 3.4 and the fact that  $r = d_s - \delta + 1$  we get that the upper bound for  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d}))$  in the above theorem is

$$\begin{aligned} m - \dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) - \left( \left\lceil \frac{\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)}{r} \right\rceil - 1 \right) (\delta - 1) + 1 \\ = \prod_{i=1}^n d_i - (d_s - \delta + 1) \prod_{\substack{i=1 \\ i \neq s}}^n d_i - \left( \prod_{\substack{i=1 \\ i \neq s}}^n d_i - 1 \right) (\delta - 1) + 1 = \delta \end{aligned}$$

so  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d})) = \delta$ . In the same way one proves that  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(\tilde{d} - 1)) = \delta + 1$ .  $\square$

One may check that if  $d_s = d_n$  and  $d \leq \tilde{d}$  then either condition (i) or condition (ii) of the above Proposition is satisfied, so we get  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ . In the following section, among other results, we present some

values for  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$  when we have  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) > W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ .

**Corollary 4.3:** Let  $\delta \geq 2, n = 2, r = 2, s = 2, d_1 \leq d_2 = \delta + 1$  and  $q$  a prime power greater or equal than  $d_2$ . For  $1 \leq d \leq (d_1 - 1) + (d_2 - \delta) = d_1$ , the code  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  is optimal with minimum distance  $(d_1 - d)(\delta + 1)$ .

*Proof:* From Corollary 4.2 for  $d = d_1 - 1$  and  $d = d_1$  the code  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  is optimal. If  $d < d_1 - 1$  then from Proposition 3.3 we get  $\dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) = \frac{(d+2)(d+1)}{2} - \frac{(d)(d-1)}{2} = 2d + 1$  and from Theorem 4.1 we get  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = (d_1 - d)d_2 = (d_1 - d)(\delta + 1)$ .

From [19], the upper bound of  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$  is  $d_1 d_2 - (2d + 1) - \left(\left\lceil \frac{2d + 1}{2} \right\rceil\right) (\delta - 1) + 1 = (d_1 - d)d_2 = W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$ .  $\square$

**V. FURTHER RESULTS ON THE MINIMUM DISTANCE IN A SPECIAL CASE**

In this section we assume that  $K_1, \dots, K_n$  are fields such that  $K_1 \subset K_2 \subset \dots \subset K_n \subset \mathbb{F}_q$ .

We write  $\text{Aff}(\mathbb{F}_q^n)$  for the affine group of  $\mathbb{F}_q^n$ , i.e. the transformations of  $\mathbb{F}_q^n$  of the type  $\alpha \mapsto A\alpha + \beta$ , where  $A \in GL(n, \mathbb{F}_q)$  and  $\beta \in \mathbb{F}_q^n$ .

**Definition 5.1:** The affine group associated to  $\mathcal{X}$  is

$$\text{Aff}(\mathcal{X}) = \{\varphi : \mathcal{X} \rightarrow \mathcal{X} \mid \varphi = \psi|_{\mathcal{X}} \text{ with } \psi \in \text{Aff}(\mathbb{F}_q^n) \text{ and } \psi(\mathcal{X}) = \mathcal{X}\}.$$

Let  $\{e_1, \dots, e_n\} \subset \mathbb{F}_q^n$  be the canonical basis of  $\mathbb{F}_q^n$ , since  $e_1, \dots, e_n \in \mathcal{X}$  we get that for each  $\varphi \in \text{Aff}(\mathcal{X})$  there exists only one  $\psi \in \text{Aff}(\mathbb{F}_q^n)$  such that  $\varphi = \psi|_{\mathcal{X}}$ .

**Lemma 5.2:** Let  $\psi \in \text{Aff}(\mathbb{F}_q^n)$  be given by  $\alpha \mapsto A\alpha + \beta$ , where

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \text{ and } \beta = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

and let  $\varphi = \psi|_{\mathcal{X}}$ . Then  $\varphi \in \text{Aff}(\mathcal{X})$  if and only if the following conditions are satisfied:

- (i) for all  $i, j \in \{1, \dots, n\}, a_{ij} \in K_i, b_j \in K_j$  and if  $K_i \not\subseteq K_j$  then  $a_{ij} = 0$ ;
- (ii) for all  $i \leq j \in \{1, \dots, n\}$  such that  $K_{i-1} \subsetneq K_i = K_j \subsetneq K_{j+1}$  the square submatrix formed by entries  $a_{uw}$  with  $i \leq u, w \leq j$  is invertible.

*Proof:* Let  $\psi : \alpha \mapsto A\alpha + \beta \in \text{Aff}(\mathbb{F}_q^n)$  and suppose that  $\psi|_{\mathcal{X}} = \varphi \in \text{Aff}(\mathcal{X})$ . For  $\alpha = 0$  we get  $\varphi(0) = \beta \in \mathcal{X}$ , which implies  $b_j \in K_j$  for all  $j \in \{1, \dots, n\}$ . We also get that the transformation  $\psi_0 : \alpha \mapsto A\alpha \in \text{Aff}(\mathbb{F}_q^n)$  is such that  $\varphi_0 = \psi_0|_{\mathcal{X}} \in \text{Aff}(\mathcal{X})$ .

Let  $\{e_1, \dots, e_n\} \subset \mathbb{F}_q^n$  be the canonical basis of  $\mathbb{F}_q^n$ . For any  $j \in \{1, \dots, n\}$  we get

$$\psi_0(e_j) = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} \in \mathcal{X}$$

and so  $a_{ij} \in K_i$  for all  $i \in \{1, \dots, n\}$ .

Let  $i, j \in \{1, \dots, n\}$  such that  $K_i \subsetneq K_j$  (so in particular  $j > i$ ) and choose  $\gamma_j \in K_j \setminus K_i$ . From  $\gamma_j e_j \in \mathcal{X}$  we get

$$\psi_0(\gamma_j e_j) = \begin{pmatrix} \gamma_j a_{1j} \\ \gamma_j a_{2j} \\ \vdots \\ \gamma_j a_{nj} \end{pmatrix} \in \mathcal{X}$$

and, in particular,  $\gamma_j a_{ij} \in K_i$  which is only possible if  $a_{ij} = 0$ .

Assume that  $K_1 \subsetneq K_n$  and let  $i_0, \dots, i_t$  be integers such that  $0 = i_0 < i_1 < \dots < i_t = n$ , with  $K_{i_{u+1}} = \dots = K_{i_u+1}$  for all  $u = 0, \dots, t - 1$  and  $K_{i_u} \subsetneq K_{i_{u+1}}$  for all  $u \in \{1, \dots, t - 1\}$ . Then the matrix  $A$  can be written as

$$A = \begin{pmatrix} B_1 & 0 & 0 & \dots & 0 \\ * & B_2 & 0 & \dots & 0 \\ * & * & B_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & * & * & B_t \end{pmatrix}$$

where for all  $j = 1, \dots, t$  the matrix  $B_j$  is of size  $(i_j - i_{j-1}) \times (i_j - i_{j-1})$ . Since  $\det A = \det B_1 \cdot \det B_2 \cdot \dots \cdot \det B_t$  and  $\det A \neq 0$  we get for all  $j = 1, \dots, t$  that  $B_j$  is invertible with coefficients in  $K_{i_j}$ . Conversely, if (i) and (ii) are satisfied then it is easy to see that  $\varphi \in \text{Aff}(\mathcal{X})$ .  $\square$

The affine group  $\text{Aff}(\mathcal{X})$  acts over the set of polynomials  $\mathbb{F}_q[X_1, \dots, X_n]$  in the following way. Let  $f \in \mathbb{F}_q[X_1, \dots, X_n]$ ,  $\varphi \in \text{Aff}(\mathcal{X})$  and  $\psi \in \text{Aff}(\mathbb{F}_q^n)$  such that  $\psi|_{\mathcal{X}} = \varphi$ . We define  $f \circ \varphi \in \mathbb{F}_q[X_1, \dots, X_n]$  as  $f \circ \varphi(X_1, \dots, X_n) = f(\psi(X_1, \dots, X_n))$ , where  $(X_1, \dots, X_n)$  is written as a column vector.

**Definition 5.3:** We say that  $f, g \in \mathbb{F}_q[X_1, \dots, X_n]$  are  $\mathcal{X}$ -equivalent if there exists  $\varphi \in \text{Aff}(\mathcal{X})$  such that  $f = g \circ \varphi$ .

In [9] affine cartesian codes were studied as images of polynomial functions evaluated at the points of  $\mathcal{X}$ , and two polynomials define the same function if their difference belongs to  $I_{\mathcal{X}}$ . In the following result we rewrite [9, Thm. 3.5] without using the function concept.

**Theorem 5.4:** Let  $d = \sum_{i=1}^k (d_i - 1) + \ell, 0 \leq k < n$  and  $0 < \ell \leq d_{k+1} - 1$ , the minimal weight codewords of  $C_{\mathcal{X}}(d)$  are of the form  $\Psi(f)$  where  $f \in \mathbb{F}_q[X_1, \dots, X_n]_{\leq d}$  is such that there exists  $g \in \mathbb{F}_q[X_1, \dots, X_n]$ , with  $f - g \in I_{\mathcal{X}}$  and  $g$  is  $\mathcal{X}$ -equivalent to a polynomial

$$h = \sigma \prod_{i=1, i \neq j}^{k+1} (X_i^{d_i-1} - 1) \prod_{t=1}^{d_j-(d_{k+1}-\ell)} (X_j - \alpha_t),$$

where  $j \in \{1, \dots, k + 1\}$  is such that  $d_j - (d_{k+1} - \ell) \geq 0, \sigma \in \mathbb{F}_q^*$  and  $\alpha_1, \dots, \alpha_{d_j-(d_{k+1}-\ell)}$  are distinct elements of  $K_j$  (if  $d_j - (d_{k+1} - \ell) = 0$  we take the second product as being equal to 1).

The following result describes a property of certain polynomials of degree 1 which will be used in the next proposition.

**Lemma 5.5:** Let  $p = \gamma_1 X_1 + \dots + \gamma_h X_h + \eta \in \mathbb{F}_q[X_1, \dots, X_n]$ , where  $\gamma_1, \dots, \gamma_h \in \mathbb{F}_q$  and  $\gamma_h \neq 0$ . Then there exists  $\varphi \in \text{Aff}(\mathcal{X})$  and  $j \in \{1, \dots, n\}$  such that  $X_j \circ \varphi = p$  if and only if  $\gamma_i \in K_j$  for all  $i \in \{1, \dots, h\}, \eta \in K_j$  and  $K_h = K_j$ .



*Proof:* Assume that there exists  $\varphi \in \text{Aff}(\mathcal{X})$  such that  $X_j \circ \varphi = p$  for some  $j \in \{1, \dots, n\}$ , and let  $\psi \in \text{Aff}(\mathbb{F}_q^n)$  be such that  $\varphi = \psi|_{\mathcal{X}}$ . If  $\psi$  is given by  $\alpha \mapsto A\alpha + \beta$ , then the  $j$ -th row of  $A$  has to be  $(\gamma_1, \dots, \gamma_h, 0, \dots, 0)$ , so  $\gamma_i \in K_j$  for all  $i \in \{1, \dots, h\}$ , likewise the  $j$ -th entry of  $\beta$  has to be  $\eta$ , so that  $\eta \in K_j$ . From the general form of  $A$ , which was described in Lemma 5.2 we get that  $K_h = K_j$ . The proof of the converse is simple and follows from Lemma 5.2.  $\square$

*Definition 5.6:* A linear form  $L = \gamma_1 X_1 + \dots + \gamma_h X_h$ , where  $\gamma_h \neq 0$ ,  $\gamma_i \in K_j$  for all  $i \in \{1, \dots, h\}$  and  $K_h = K_j$  will be called a  $\mathcal{X}$ -linear form over  $K_j$ .

*Proposition 5.7:* Let  $f \in \mathbb{F}_q[X_1, \dots, X_n]$  be a polynomial of degree

$$d = \sum_{i=1}^k (d_i - 1) + \ell,$$

where  $0 \leq k < n$  and  $0 < \ell \leq d_{k+1} - 1$ . Assume that no monomial in  $f$  is a multiple of  $X_i^{d_i}$ , for all  $i = 1, \dots, n$ .

If  $w(\Psi(f)) = (d_{k+1} - \ell) \prod_{i=k+2}^n d_i$  then there exists a mono-

mial in  $f$  of the form  $X_{t_j}^{d_j - (d_{k+1} - \ell)} \prod_{\substack{i=1 \\ i \neq j}}^{k+1} X_{t_i}^{d_i - 1}$  for some  $1 \leq$

$j \leq k + 1$  such that  $d_j \geq d_{k+1} - \ell$ , where  $t_1, \dots, t_{k+1}$  are distinct elements of  $\{1, \dots, n\}$  and  $K_{t_i} = K_i$  for all  $i \in \{1, \dots, k + 1\}$ .

*Proof:* From (2) we get that  $w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$  so from Theorem 5.4 there exist  $j \in \{1, \dots, k + 1\}$  and a polynomial

$$g = \sigma \prod_{\substack{i=1 \\ i \neq j}}^{k+1} ((L_i - \alpha_i)^{d_i - 1} - 1) \prod_{s=1}^{d_j - (d_{k+1} - \ell)} (L_j - \beta_s),$$

where  $\sigma \in \mathbb{F}_q$ ,  $\beta_1, \dots, \beta_{d_j - (d_{k+1} - \ell)}$  are distinct elements of  $K_j$ ,  $L_i$  is a  $\mathcal{X}$ -linear form over  $K_i$  and  $\alpha_i \in K_i$  for all  $i \in \{1, \dots, k + 1\}$ , the forms  $L_1, \dots, L_{k+1}$  are linearly independent over  $\mathbb{F}_q$ , and  $f - g \in I_{\mathcal{X}}$ . Since  $\deg(g) = d$  we get  $g \in \mathbb{F}_q[X_1, \dots, X_n]_{\leq d}$  and  $\Psi(g) = \Psi(f) \in \mathcal{C}_{\mathcal{X}}(d)$ .

Assume, for a moment, that there are at least two factors in the first product in the definition of  $g$ , i.e. assume that there exist  $u, w \in \{1, \dots, k + 1\}$  with  $u < w$  and  $u, w \neq j$ . Observe that evaluating the polynomial

$$((L_u - \alpha_u)^{d_u - 1} - 1)((L_w - \alpha_w)^{d_w - 1} - 1)$$

at the points of  $\mathcal{X}$  we get the value zero, except for those  $P \in \mathcal{X}$  where  $L_u(P) = \alpha_u$  and  $L_w(P) = \alpha_w$ , and at these points we get 1. For any  $\gamma \in K_w$  we get the same results evaluating the polynomial

$$((L_u - \alpha_u)^{d_u - 1} - 1)((L_w - \alpha_w - \gamma(L_u - \alpha_u))^{d_w - 1} - 1)$$

at the points of  $\mathcal{X}$ . Thus we may replace, in the polynomial  $g$ , the factor  $(L_w - \alpha_w)^{d_w - 1} - 1$  by the factor  $(L_w - \alpha_w - \gamma(L_u - \alpha_u))^{d_w - 1} - 1$  obtaining a polynomial  $\tilde{g}$  such that  $\Psi(\tilde{g}) = \Psi(g)$ , and a fortiori  $\tilde{g} - g \in I_{\mathcal{X}}$ . This reasoning shows that we may

perform a Gaussian elimination process in the set  $\{L_i - \alpha_i \mid i = 1, \dots, k + 1, i \neq j\}$ , starting with the linear form with the greatest index and proceeding to the linear form with the least index, and find a set of  $k$  integers  $1 \leq t_1 < \dots < t_{j-1} < t_{j+1} < \dots < t_{k+1} \leq n$  such that after the elimination process we may assume that  $L_i = X_{t_i} + \sum_{w < t_i, w \notin A} a_{iw} X_w$  for all  $i \in \{1, \dots, k + 1\} \setminus \{j\}$ , where  $A = \{t_i \mid i = 1, \dots, j - 1, j + 1, \dots, k + 1\}$ . Observe that  $K_{t_i} = K_i$  for all  $i \in \{1, \dots, k + 1\} \setminus \{j\}$  and we still have

$$f - \tau \prod_{\substack{i=1 \\ i \neq j}}^{k+1} ((L_i - \gamma_i)^{d_i - 1} - 1) \prod_{s=1}^{d_j - (d_{k+1} - \ell)} (L_j - \beta_s) \in I_{\mathcal{X}}$$

for some  $\tau \in \mathbb{F}_q$ , and  $\gamma_i \in K_i$  for all  $i \in \{1, \dots, k + 1\} \setminus \{j\}$ .

Let  $i \in \{1, \dots, k + 1\} \setminus \{j\}$  be such that  $K_{t_i} \subset K_j$  and let  $\xi \in K_j$ , then the polynomials

$$((L_i - \gamma_i)^{d_i - 1} - 1) \prod_{s=1}^{d_j - (d_{k+1} - \ell)} (L_j - \beta_s)$$

and

$$((L_i - \gamma_i)^{d_i - 1} - 1) \prod_{s=1}^{d_j - (d_{k+1} - \ell)} (L_j - \beta_s - \xi(L_i - \gamma_i))$$

yield the same value when evaluated at any  $P \in \mathcal{X}$ , so their difference is in  $I_{\mathcal{X}}$ . As before, after a Gauss-Jordan elimination process, we may assume that  $L_j = X_{t_j} + \sum_{w < t_j, w \notin A} a_{jw} X_w$ , with  $t_j \notin A$  and  $K_{t_j} = K_j$ . Again,

$$f - \eta \prod_{\substack{i=1 \\ i \neq j}}^{k+1} ((L_i - \gamma_i)^{d_i - 1} - 1) \prod_{s=1}^{d_j - (d_{k+1} - \ell)} (L_j - \theta_s) \in I_{\mathcal{X}}$$

still holds, for some  $\eta \in \mathbb{F}_q$  and  $\theta_s \in K_j$ ,  $s = 1, \dots, d_j - (d_{k+1} - \ell)$ . Taking the lexicographic order where  $X_1 < \dots < X_n$ , we get that the leading monomial of the right hand side polynomial in the above difference is

$$M = X_{t_j}^{(d_j - (d_{k+1} - \ell))} \prod_{\substack{i=1 \\ i \neq j}}^{k+1} X_{t_i}^{d_i - 1}.$$

Since the remainder in the division of  $f - g$  by the Gröbner basis  $\{X_1^{d_1} - X_1, \dots, X_n^{d_n} - X_n\}$  is zero, and  $M$  is not a multiple of  $X_i^{d_i}$  for all  $i = 1, \dots, n$ , we get that this monomial must also appear in  $f$ .  $\square$

We apply the above result to obtain a converse to Theorem 4.1.

*Theorem 5.8:* Assume that  $K_1, \dots, K_n$  are fields such that  $K_1 \subset K_2 \subset \dots \subset K_n \subset \mathbb{F}_q$ . Let  $d = \sum_{i=1}^k (d_i - 1) + \ell$  where

$0 \leq k < n$  and  $0 < \ell \leq d_{k+1} - 1$ . If  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$  then one of the following conditions must hold:

- (i)  $k + 2 \leq n$  and  $d_{k+2} \leq d_s$ ;
- (ii)  $d_s \leq d_{k+1}$  and  $0 \leq d_s - (d_{k+1} - \ell) < r$ .

*Proof:* Suppose that condition (i) is not satisfied, then  $n = k + 1$  or  $d_s < d_{k+2}$ , which implies, in both cases, that  $d_s \leq d_{k+1}$ . If condition (ii) is also not satisfied we must then have  $d_s - (d_{k+1} - \ell) < 0$  or  $r \leq d_s - (d_{k+1} - \ell)$ . Thus if conditions (i) and (ii) are not satisfied, then  $n = k + 1$  or  $d_s < d_{k+2}$ , and  $d_s - (d_{k+1} - \ell) < 0$  or  $d_s - (d_{k+1} - \ell) \geq r$ .

We assume that  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$  holds, and let  $f \in \mathcal{P}_d^{(\delta,s)}$  be a polynomial of degree  $d$  such that

$$w(\Psi(f)) = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d)).$$

From Proposition 5.7 there exists a monomial in  $f$  of the form

$$M_j = X_{t_j}^{d_j - (d_{k+1} - \ell)} \prod_{\substack{i=1 \\ i \neq j}}^{k+1} X_{t_i}^{d_i - 1}$$

for some  $1 \leq j \leq k + 1$  such that  $d_j \geq d_{k+1} - \ell$ , where  $t_1, \dots, t_{k+1}$  are distinct elements of  $\{1, \dots, n\}$  and  $K_{t_i} = K_i$  for all  $i \in \{1, \dots, k + 1\}$ .

If  $n = k + 1$  then  $\{t_1, \dots, t_{k+1}\} = \{1, \dots, k + 1\}$ , which implies that  $s = t_i$  for some  $i \in \{1, \dots, k + 1\}$ . If  $\deg_{X_s} M_j = d_s - 1$  then  $\deg_{X_s} M_j \geq d_s - \delta + 1$ , and if  $\deg_{X_s} M_j = d_s - (d_{k+1} - \ell)$  then we cannot have  $d_s - (d_{k+1} - \ell) < 0$  so we must have  $d_s - (d_{k+1} - \ell) \geq r$ , which leads to a contradiction since we also must have  $\deg_{X_s} M_j < d_s - \delta + 1 = r$ .

Thus we suppose now that  $k + 1 < n$  and  $d_s < d_{k+2}$ . Let  $u$  be the integer such that  $s < u \leq k + 2$  and  $d_{u-1} < d_u = d_{k+2}$ . From the definition of the set  $\{t_1, \dots, t_{k+1}\}$  we have, in particular, that  $K_{t_i} = K_i$  for all  $i \in \{1, \dots, u - 1\}$ , so  $s = t_i$  for some  $i \in \{1, \dots, u - 1\} \subset \{1, \dots, k + 1\}$ . As above, analysing the degree of  $M_j$  we get  $f \notin \mathcal{P}_d^{(\delta,s)}$ , which finishes the proof.  $\square$

Thus, if conditions (i) and (ii) of the above theorem are not satisfied, then from Theorem 5.8 we get that  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) > W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ . Since  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d) \subset \mathcal{C}_{\mathcal{X}}(d)$  we must have  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) \geq W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  where  $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  denotes the second lowest codeword weight in  $\mathcal{C}_{\mathcal{X}}(d)$ , also called next-to-minimal weight of  $\mathcal{C}_{\mathcal{X}}(d)$ . The values for  $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  were determined in the series of papers [6], [8] and [10]. These papers contain, in particular, the values for the special case where  $\mathcal{X} = \mathbb{F}_q^n$ , which had already been determined by a combination of results by several authors – the reader may find a historical survey of these results in [9]. From these papers, we get that, writing

$$d = \sum_{i=1}^k (d_i - 1) + \ell \text{ where } 0 \leq k < n \text{ and } 0 < \ell \leq d_{k+1} - 1,$$

the values for  $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  are as follows:

- 1) if  $n = k + 1$  then (see [6, Theorem 2.6])

$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = d_n - \ell + 1;$$

- 2) if  $3 \leq d_1 \leq \dots \leq d_n$  and either  $\ell = 1$  and  $d_{k+1} < d_{k+2}$ , or  $\ell \geq 2$  then (see [8, Theorem 3.10])

$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = (d_{k+1} - \ell + 1)(d_{k+2} - 1) \prod_{i=k+3}^n d_i;$$

- 3) if  $4 \leq d_i = q$  for all  $i \in \{1, \dots, n\}$  and  $\ell = 1$  then (see e.g. [10, Theorem 3.5])

$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = q^{n-k};$$

- 4) For all other cases where  $d_{k+1} = d_{k+2}$ ,  $\ell = 1$  and  $3 \leq d_1 \leq \dots \leq d_n$  then (see [10, Theorem 3.5])

$$W^{(2)}(\mathcal{C}_{\mathcal{X}}(d)) = (d_{k+1}^2 - 1) \prod_{i=k+3}^n d_i.$$

*Corollary 5.9:* Assume that  $n = k + 1$  or  $3 \leq d_1 \leq \dots \leq d_n$ , if the conditions (i) and (ii) of the above proposition are not satisfied and  $d_s - (d_{k+1} - \ell) = r$  then  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) =$

$$\begin{cases} d_n - \ell + 1 & \text{if } n = k + 1; \\ (d_{k+1} - \ell + 1)(d_{k+2} - 1) \prod_{i=k+3}^n d_i & \text{if } n > k + 1. \end{cases}$$

*Proof:* If (i) and (ii) of Theorem 5.8 are not satisfied, then, as in the above proof we get that  $n = k + 1$  or  $d_s < d_{k+2}$ , and  $d_s - (d_{k+1} - \ell) < 0$  or  $d_s - (d_{k+1} - \ell) \geq r$ . These last two inequalities we replace by the hypothesis  $d_s - (d_{k+1} - \ell) = r$ .

Let

$$g = \prod_{\substack{i=1 \\ i \neq s}}^{k+1} (X_i^{d_i - 1} - 1) \cdot \prod_{h=1}^{d_s - (d_{k+1} - \ell) - 1} (X_s - \beta_h),$$

then  $\deg(g) = \sum_{i=1, i \neq s}^{k+1} (d_i - 1) + d_s - (d_{k+1} - \ell) - 1 = \sum_{i=1}^k (d_i - 1) + \ell - 1 = d - 1$  (if  $d_s - (d_{k+1} - \ell) = 1$  then we take the second product in the definition of  $g$  as being 1 and still get  $\deg(g) = d - 1$ ). Clearly  $g \in \mathcal{P}_d^{(\delta,s)}$  since  $\deg_{X_s} g < r$ .

Suppose that  $n = k + 1$ , since  $w(\Psi(g)) = d_{k+1} - \ell + 1$  we must have  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  (from the above data on  $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ ).

We now treat the case where  $k + 1 < n$ , then we have  $d_s < d_{k+2}$ , and from the hypothesis we also have  $3 \leq d_1 \leq \dots \leq d_n$ . Assume that  $d_{k+1} < d_{k+2}$  and let  $f = g.X_{k+2}$ , then  $\deg(f) = d$  and  $f \in \mathcal{P}_d^{(\delta,s)}$ , from  $w(\Psi(f)) = (d_{k+1} - \ell + 1)(d_{k+2} - 1) \prod_{i=k+3}^n d_i$  we get  $W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)) = W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ . In the case where  $d_{k+1} = d_{k+2}$  from  $d_s < d_{k+2}$  and  $d_s - (d_{k+1} - \ell) = \ell - (d_{k+2} - d_s) = r \geq 1$  we see that we must have  $\ell \geq 2$ , so again we have  $w(\Psi(f)) = W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$ , which finishes the proof.  $\square$

## VI. EXAMPLES

In this section we present some tables with numerical data obtained from the above results and we also do some comparisons with other works. In the tables, we use the following notation:  $m = |\mathcal{X}|$  is the length of  $\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ ,  $\kappa = \dim_{\mathbb{F}_q} \mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d)$ ,  $v = W^{(1)}(\mathcal{C}_{\mathcal{X}}(d))$ ,  $w = W^{(1)}(\mathcal{D}_{\mathcal{X}}^{(\delta,s)}(d))$  and we denote by  $N = m - \kappa - \left( \left\lceil \frac{\kappa}{r} \right\rceil - 1 \right) (\delta - 1) + 1$  the upper bound for the minimum distance, which appears in Theorem 4.1. In the tables  $d$  runs in the range  $1 \leq d \leq \tilde{d}$ . When  $w \neq v$  then  $w \geq W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  and in Section 5 the values for  $W^{(2)}(\mathcal{C}_{\mathcal{X}}(d))$  are presented. When  $w \neq v$  and we

TABLE 1.  $\mathcal{X} := \mathbb{F}_7 \times \mathbb{F}_{49}$ .

	$\mathcal{D}_{\mathcal{X}}^{(25,2)}(d)$										
$d$	4	5	10	15	20	25	26	27	28	29	30
$m$	343	343	343	343	343	343	343	343	343	343	343
$\kappa$	15	21	56	91	126	160	165	169	172	174	175
$w$	147	98	45	40	35	30	29	28	27	26	25
$N$	329	323	240	181	98	40	35	31	28	26	25

TABLE 2.  $\mathcal{X} := \mathbb{F}_5 \times \mathbb{F}_{25} \times \mathbb{F}_{25}$ .

	$\mathcal{D}_{\mathcal{X}}^{(4,1)}(d)$								
$d$	2	3	24	25	26	27	47	48	49
$m$	3125	3125	3125	3125	3125	3125	3125	3125	3125
$\kappa$	9	16	625	674	721	766	1246	1249	1250
$v$	1875	1250	125	100	75	50	6	5	4
$w$	2400	$\geq 1800$	125	100	96	$\geq 72$	$\geq 7$	5	4
$N$	3105	3089	1565	1444	1325	1214	14	5	4

TABLE 3.  $\mathcal{X} := \mathbf{A}_1 \times \mathbf{A}_2$ ,  $|\mathbf{A}_1| = 10$ ,  $|\mathbf{A}_2| = 13$  and  $q \geq 13$ .

	$\mathcal{D}_{\mathcal{X}}^{(12,2)}(d)$									
$d$	1	2	3	4	5	6	7	8	9	10
$m$	130	130	130	130	130	130	130	130	130	130
$\kappa$	3	5	7	9	11	13	15	17	19	20
$w$	117	104	91	78	65	53	39	26	13	12
$N$	117	104	91	78	65	53	39	26	13	12

are in the hypotheses of Corollary 5.9, then we write the true value of  $w$ . In the table 1, for the  $d$  presented we always have  $w = v$ . In the table 2, for some values of  $d$  we have  $w \neq v$ .

From Corollary 4.3 we get optimal codes where the minimum distance is a multiple of  $\delta + 1$ , see for example Table 3.

Optimal codes have been the object of active investigation (see e.g. [4], [5], [11]–[13] and [17], among many other papers). We finish this section with comparisons of our codes with codes which appear in some of the papers above.

In [13, Corollary 1], the authors find optimal codes with minimum distance equal to  $\delta + 1$ ,  $\delta + 2$  and  $2\delta$ , while in Corollary 4.2 we have optimal codes with minimum distance equal to  $\delta$  and  $\delta + 1$ , and in Corollary 4.3 we construct optimal codes whose minimum distance may be adjusted to be one among several multiples of  $\delta + 1$ .

In [4, Example 1] the authors present an optimal code with parameters  $[12, 5, 4]$  and  $(r, \delta) = (2, 3)$ . In this case the minimum distance is  $4 = \delta + 1$ . From Corollary 4.3, choosing  $(d_1, d_2) = (3, 4)$  and the same locality  $(r, \delta)$  we get the same code as in the above mentioned example, among three optimal codes with parameters  $[12, 3, 8]$ ,  $[12, 5, 4]$  and  $[12, 6, 3]$ .

Finally we observe that in [11], the authors present cyclic optimal  $(r, \delta)$ -LRC codes such that the length divides  $q + 1$ , while the length of our codes has no such restriction.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their comments.

REFERENCES

[1] W. W. Adams and P. Loustaunau, “An introduction to Grobner bases,” in *Graduate Studies in Mathematics*, vol. 3. New York, NY, USA: AMS, 1994.

[2] B. Buchberger, “Ein algorithmus zum auffinden der baselemente des restklassenringes nach einem nulldimensionalen polynomideal,” Ph.D. dissertation, Math. Inst., Univ. Innsbruck, Innsbruck, Austria, 1965.

[3] B. Buchberger, “Bruno Buchberger’s PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal,” *J. Symbolic Comput.*, vol. 41, pp. 475–511, Mar./Apr. 2006.

[4] H. Cai, Y. Miao, M. Schwartz, and X. Tang, “On optimal locally repairable codes with super-linear length,” *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 4853–4868, Aug. 2020.

[5] H. Cai and M. Schwartz, “On optimal locally repairable codes and generalized sector-disk codes,” *IEEE Trans. Inf. Theory*, vol. 67, no. 2, pp. 686–704, Feb. 2021.

[6] C. Carvalho, “On the second Hamming weight of some Reed–Müller type codes,” *Finite Fields Appl.*, vol. 24, pp. 88–94, Nov. 2013.

[7] C. Carvalho, “Gröbner bases methods in coding theory,” in *Contemporary Mathematics*, vol. 642. Providence, RI, USA: AMS, Jan. 2015, pp. 73–86.

[8] C. Carvalho and V. G. L. Neumann, “On the next-to-minimal weight of affine Cartesian codes,” *Finite Fields Appl.*, vol. 44, pp. 113–134, Mar. 2017.

[9] C. Carvalho and V. G. L. Neumann, “An extension of Delsarte, Goethals and Mac Williams theorem on minimal weight codewords to a class of Reed–Müller type codes,” in *Integrable Systems and Algebraic Geometry V. 2*, R. Donagi and T. Shaska, Eds. Cambridge, U.K.: Cambridge Univ. Press, Mar. 2020, pp. 313–345.

[10] C. Carvalho and V. G. L. Neumann, “Completing the determination of the next-to-minimal weights of affine Cartesian codes,” *Finite Fields Appl.*, vol. 69, Jan. 2021, Art. no. 101775.

[11] B. Chen, S.-T. Xia, J. Hao, and F.-W. Fu, “Constructions of optimal cyclic  $(r, \delta)$  locally repairable codes,” *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 2499–2511, Apr. 2018.

[12] B. Chen, W. Fang, S.-T. Xia, and F.-W. Fu, “Constructions of optimal  $(r, \delta)$  locally repairable codes via constacyclic codes,” *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5253–5263, Aug. 2019.

[13] B. Chen and J. Huang, “A construction of optimal  $(r, \delta)$ -locally recoverable codes,” *IEEE Access*, vol. 7, pp. 180349–180353, 2019.

[14] D. Cox, J. Little, and D. O’Shea, *Ideals, Varieties and Algorithms*, 3rd ed. New York, NY, USA: Springer-Verlag, 2007.

[15] O. Geil and C. Thomsen, “Weighted Reed–Müller codes revisited,” *Des., Codes Cryptogr.*, vol. 66, pp. 195–220, May 2012.

[16] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, “On the locality of codeword symbols,” *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6925–6934, Aug. 2012.

[17] J. Hao, S.-T. Xia, and B. Chen, “On the linear codes with  $(r, \delta)$ -locality for distributed storage,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[18] H. H. López, C. Rentería-Márquez, and R. H. Villarreal, “Affine Cartesian codes,” *Des., Codes Cryptogr.*, vol. 71, no. 1, pp. 5–19, 2014.

[19] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, “Optimal linear codes with a local-error-correction property,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 2776–2780.



**BRUNO ANDRADE** received the degree in mathematics from the Universidade Federal de Mato Grosso do Sul, in 2010, and the master’s degree in mathematics from the Universidade Federal de Uberlândia, Brazil, in 2013, where he is currently pursuing the Ph.D. degree with the Graduate Program in Electrical Engineering. Since 2013, he has been with the Universidade Federal de Uberlândia, where he is currently an Associate Professor. His research interests include the study of finite fields and coding theory.





**CÍCERO CARVALHO** received the degree in physics and the degree in mathematics from the Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil, in 1980 and 1981, respectively, and the Ph.D. degree in mathematics from IMPA, Rio de Janeiro, in 1994. From 1996 to 1998, he was a Postdoctoral Researcher at Harvard University. Since 1986, he has been with the Universidade Federal de Uberlândia, Brazil, where he is currently a Full Professor. His research interests

include the study of curves over finite fields and coding theory.



**ANTÔNIO C. P. VEIGA** received the Ph.D. degree in electrical engineering from the Universidade Estadual de Campinas, in 2002. Since 1988, he has been with the Universidade Federal de Uberlândia, Brazil, where he is currently a Full Professor. His research interests include the study of image processing and digital communications.

...



**VICTOR G. L. NEUMANN** received the bachelor's and master's degrees from the University of Geneva, Switzerland, and the Ph.D. degree from the University of Geneva, in 2004. From 2005 to 2006, he was a Postdoctoral Researcher at the Universidade Federal de Minas Gerais. Since 2006, he has been with the Universidade Federal de Uberlândia, Brazil, where he is currently an Associate Professor. His research interests include the study of finite fields, finite geometry, and coding theory.