

# DECREASING NORM-TRACE CODES

CÍCERO CARVALHO, HIRAM H. LÓPEZ, AND GRETCHEN L. MATTHEWS

**ABSTRACT.** The decreasing norm-trace codes are evaluation codes defined by a set of monomials closed under divisibility and the rational points of the extended norm-trace curve. In particular, the decreasing norm-trace codes contain the one-point algebraic geometry (AG) codes over the extended norm-trace curve. We use Gröbner basis theory and find the indicator functions on the rational points of the curve to determine the basic parameters of the decreasing norm-trace codes: length, dimension, and minimum distance. We also obtain their dual codes. We give conditions for a decreasing norm-trace code to be a self-orthogonal or a self-dual code. We provide a linear exact repair scheme to correct single erasures for decreasing norm-trace codes, which applies to higher rate codes than the scheme developed by Jin, Luo, and Xing (IEEE Transactions on Information Theory **64** (2), 900-908, 2018) when applied to the one-point AG codes over the extended norm-trace curve.

## 1. INTRODUCTION

Decreasing monomial codes, which are evaluation codes in which the set of monomials is closed under divisibility, were introduced by Bardet, Dragoi, Otmani, and Tillich in [4] to algebraically analyze the polar codes defined by Arikan [1]. The families of monomials satisfying a closure property also appeared in an earlier construction for optimized evaluation codes [8].

The classical families of Reed-Solomon and Reed-Muller codes are decreasing monomial codes and have amply motivated the study of wider classes of decreasing monomial codes. Decreasing monomial-Cartesian codes, also known as variants of Reed-Muller codes over finite grids, are more general families than Reed-Muller codes that have been studied due

---

(Cícero Carvalho) FACULDADE DE MATEMÁTICA, UNIVERSIDADE FEDERAL DE UBERLÂNDIA, UBERLÂNDIA, MG BRAZIL

(Hiram H. López) DEPARTMENT OF MATHEMATICS, VIRGINIA TECH, BLACKSBURG, VA USA

(Gretchen L. Matthews) DEPARTMENT OF MATHEMATICS, VIRGINIA TECH, BLACKSBURG, VA USA

*E-mail addresses:* cicero@ufu.br, hhlopez@vt.edu, gmatthews@vt.edu.

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

*Key words and phrases.* Evaluation codes, decreasing monomial codes, norm-trace curves, repair scheme, dual codes.

Cícero Carvalho was partially supported by FAPEMIG APQ-00864-21. Hiram H. López was partially supported by NSF DMS-2201094 and NSF DMS-2401558. Gretchen L. Matthews was partially supported by NSF DMS-2201075 and the Commonwealth Cyber Initiative.

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

to their applications to certain symmetric channels [10], distributed storage systems [28], and efficient decoding algorithms [34].

In [11], Camps, Martínez-Moro, and Rosales introduced Vardøhus codes, which are polar codes defined by kernels from castle curves. They proved that Vardøhus codes are polar codes for a discrete memoryless channel that is symmetric with respect to the field operations.

In this paper, we study decreasing norm-trace codes, which are decreasing monomial codes where the evaluation points are the rational points of the extended norm-trace curve. As a consequence of [11] and the fact that the extended norm-trace curve is castle, the decreasing norm-trace codes can be considered as polar codes for discrete memoryless channels symmetric with respect to the field operations.

Let  $\mathbb{F}_{q^r}$  be the finite field with  $q^r$  elements. Norm-trace codes are defined using the *norm-trace curve* which is an affine curve over  $\mathbb{F}_{q^r}$  defined by

$$N(x) = \text{Tr}(y)$$

where  $N(x)$  is the norm and  $\text{Tr}(y)$  is the trace, both taken with respect to the extension  $\mathbb{F}_{q^r}/\mathbb{F}_q$ . Let  $u$  be a positive integer such that  $u \mid \frac{q^r-1}{q-1}$ . The *extended norm-trace curve*, denoted by  $\mathcal{X}_u$ , is the affine curve over  $\mathbb{F}_{q^r}$  defined by the equation

$$x^u = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y.$$

We focus in this work on decreasing norm-trace codes, which are codes defined by evaluating monomials on the rational points of the curve  $\mathcal{X}_u$ . We now give more details.

Enumerate the rational points on  $\mathcal{X}_u$  so that  $\mathcal{X}_u = \{P_1, \dots, P_n\} \subseteq \mathbb{F}_{q^r}^2$ . The *evaluation map*, denoted  $\text{ev}$ , is the  $\mathbb{F}_{q^r}$ -linear map given by

$$\begin{aligned} \text{ev}: \quad \mathbb{F}_{q^r}[x, y] &\rightarrow \mathbb{F}_{q^r}^n \\ f &\mapsto (f(P_1), \dots, f(P_n)). \end{aligned}$$

Let  $\mathcal{M} \subseteq \mathbb{F}_{q^r}[x, y]$  be a set of monomials closed under divisibility, meaning that if  $M \in \mathcal{M}$  and  $M'$  divides  $M$ , then  $M' \in \mathcal{M}$ . Let  $\mathcal{L}$  be the  $\mathbb{F}_{q^r}$ -subspace of  $\mathbb{F}_{q^r}[x, y]$  generated by the set  $\mathcal{M}$ . We call the image of  $\mathcal{L}$  under the evaluation map, denoted by  $\text{ev}(\mathcal{M})$ , a *decreasing norm-trace code*. We can see that the extended norm-trace codes introduced and recently studied in [7] and [23] are particular instances of decreasing norm-trace codes; norm-trace codes and generalizations also appear in [8]. Moreover, we check later that the family of decreasing norm-trace codes contains, as a specific case, the family of one-point geometric Goppa codes over the Hermitian curve and the more general norm-trace curve.

We organize this paper as follows. In Section 2, we describe the vanishing ideal  $I_{\mathcal{X}_u}$  of the extended norm-trace curve  $\mathcal{X}_u$  (Lemma 2.1), which is the ideal of all polynomials

that vanish on  $\mathcal{X}_u$ . We recall essential concepts from the Gröbner basis theory, such as the footprint of an ideal, and determine a Gröbner basis for  $I_{\mathcal{X}_u}$  (Proposition 2.2) with respect to a certain graded lexicographic order.

The main result of Section 3 shows the standard indicator function of every rational point of the extended norm-trace curve  $\mathcal{X}_u$  (Theorem 3.2). Given a rational point  $P$  on  $\mathcal{X}_u$ , a standard indicator function  $f_P$  is a linear combination of monomials that belong to the footprint of  $I_{\mathcal{X}_u}$  such that  $f_P(P) = 1$  and  $f_P(P') = 0$  for every other rational point  $P' \neq P$  of  $\mathcal{X}_u$ .

In Section 4, we formally introduce decreasing norm-trace codes (Definition 4.1). We determine their basic parameters, such as the length, dimension, and minimum distance (Theorem 4.3). We show that these decreasing monomial codes generalize the one-point AG codes over the norm-trace curve.

In Section 5, we give an explicit expression for the dual of a decreasing norm-trace code (Theorem 5.1) in terms of the complement of the set of monomials. The hull of a linear code is the intersection of the code with its dual. The hull has several applications, e.g., it has been used to classify finite projective planes [2] and to construct entanglement-assisted quantum error-correcting codes [25]. We show instances where the hull of a decreasing norm-trace code is computed explicitly (Theorem 5.3). We also give conditions on the set of monomials, so that the decreasing norm-trace code is a self-orthogonal or a self-dual code.

In Section 6, we apply our results to study linear repair schemes for decreasing norm-trace codes. A repair scheme is an algorithm that recovers the value at any entry of a codeword using limited information from the values at the other entries. After presenting the basic definitions of this theory, we prove results that show the existence of a repair scheme for decreasing norm-trace codes (Theorem 6.2). We close with some conclusions at the end of Section 6.

References for vanishing ideals and related algebraic concepts used in this work are [13, 14, 21, 35].

## 2. PRELIMINARIES

Let  $\mathbb{F}_q$  be the finite field with  $q$  elements and  $r \geq 2$  an integer. Define the polynomials  $N(x) := x^{\frac{q^r-1}{q-1}}$  and  $Tr(y) := y^{q^{r-1}} + y^{q^{r-2}} + \dots + y^q + y$  in  $\mathbb{F}_{q^r}[x, y]$ . The *trace* with respect to the extension  $\mathbb{F}_{q^r}/\mathbb{F}_q$  is the map

$$\begin{aligned} Tr : \mathbb{F}_{q^r} &\rightarrow \mathbb{F}_q \\ \alpha &\mapsto Tr(\alpha). \end{aligned}$$

The *norm* with respect to the extension  $\mathbb{F}_{q^r}/\mathbb{F}_q$  is the map

$$\begin{aligned} N : \mathbb{F}_{q^r} &\rightarrow \mathbb{F}_q \\ \alpha &\mapsto N(\alpha). \end{aligned}$$

The *norm-trace curve*, denoted by  $\mathcal{X}$ , is the affine plane curve over  $\mathbb{F}_{q^r}$  given by the equation

$$x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y.$$

The curve  $\mathcal{X}$  has been extensively studied in the literature to construct linear codes [7, 16, 26, 31, 33]. We are interested in a slightly more general curve. Let  $u$  be a positive integer such that  $u \mid \frac{q^r-1}{q-1}$ . The *extended norm-trace curve*, denoted by  $\mathcal{X}_u$ , is the affine curve over  $\mathbb{F}_{q^r}$  defined by the equation

$$x^u = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y.$$

We use the rational points of the curve  $\mathcal{X}_u$  to construct a family of decreasing evaluation codes, which contains, as a particular case, the extended norm-trace codes [7, 23].

Results from Gröbner bases theory have been used in coding theory for some time to determine parameters of codes (see, e.g., [16, 17, 12]). We now recall important concepts and results from this theory.

Let  $\mathcal{M}$  be the set of monomials of  $\mathbb{F}_{q^r}[x_1, \dots, x_m]$ . A *monomial order*  $\prec$  on  $\mathcal{M}$  is a total order where 1 is the least monomial and if  $M_1 \prec M_2$ , then  $MM_1 \prec MM_2$ , for all  $M, M_1, M_2 \in \mathcal{M}$ . Fix a monomial order in  $\mathcal{M}$  and let  $f$  be a nonzero polynomial in  $\mathbb{F}_{q^r}[x_1, \dots, x_m]$ . The greatest monomial which appears in  $f$  is called the *leading monomial* of  $f$ , denoted by  $\text{lm}(f)$ . Given an ideal  $I \subseteq \mathbb{F}_{q^r}[x_1, \dots, x_m]$ , a *Gröbner basis* for  $I$  is a set  $\{f_1, \dots, f_s\} \subseteq I$  such that for every polynomial  $f \in I \setminus \{0\}$ , we have that  $\text{lm}(f)$  is a multiple of  $\text{lm}(f_i)$  for some  $i \in \{1, \dots, s\}$ . The Gröbner basis concept was introduced in the Ph.D. thesis of Bruno Buchberger (see [9]), in which the author proves that every ideal admits a Gröbner basis (w.r.t. a fixed monomial order) and that if  $\{f_1, \dots, f_s\}$  is a Gröbner basis for  $I$ , then  $I = (f_1, \dots, f_s)$ .

Let  $\{f_1, \dots, f_s\}$  be a Gröbner basis for  $I$ . The *footprint* of  $I$  is the set  $\Delta_\prec(I)$  of monomials which are not multiples of  $\text{lm}(f_i)$  for all  $i = 1, \dots, n$ . One of the main results in Buchberger's thesis states that the set of classes  $\{M + I \mid M \in \Delta_\prec(I)\} \subseteq \mathbb{F}_{q^r}[x_1, \dots, x_m]/I$  is a basis for  $\mathbb{F}_{q^r}[x_1, \dots, x_m]/I$  as a  $\mathbb{F}_{q^r}$ -vector space.

We now define an ideal associated with the extended norm-trace curve  $\mathcal{X}_u$ :

$$I_{\mathcal{X}_u} := (Tr(y) - x^u, x^{q^r} - x, y^{q^r} - y) \subseteq \mathbb{F}_{q^r}[x, y].$$

Next, we consider some relevant properties of this ideal.

**Lemma 2.1.** *The ideal  $I_{\mathcal{X}_u}$  is radical and is the ideal of all polynomials which vanish on  $\mathcal{X}_u$ .*

*Proof.* Since  $x^{q^r} - x, y^{q^r} - y \in I_{\mathcal{X}_u}$ , for any monomial order, the footprint is finite and consists of monomials of the form  $x^a y^b$  where  $a$  and  $b$  are less than  $q^r$ . Hence,  $I_{\mathcal{X}_u}$  is a zero-dimensional ideal. Thus,  $I_{\mathcal{X}_u}$  is a radical ideal by [5, Prop. 8.14]. From [18, Thm. 2.3], it follows that  $I_{\mathcal{X}_u}$  is the ideal of all polynomials which vanish on  $\mathcal{X}_u$ . The fact that  $I_{\mathcal{X}_u}$  is radical also follows immediately from [18, Thm. 2.3] being a vanishing ideal.  $\square$

From now on we work with the following graded lexicographic order  $\prec$ : we say that  $x^a y^b \prec x^c y^d$  if either  $aq^{r-1} + bu < cq^{r-1} + du$ , or  $aq^{r-1} + bu = cq^{r-1} + du$  and  $b < d$ .

The following result is a particular case of [23, Theorem 19]. We add a detailed proof here for completeness.

**Proposition 2.2.** *The set  $\{Tr(y) - x^u, x^{(q-1)u+1} - x\}$  is a Gröbner basis for  $I_{\mathcal{X}_u}$  with respect to the order  $\prec$  defined above. Moreover,  $|\mathcal{X}_u| = q^{r-1}((q-1)u+1)$ . In particular, if  $u = \frac{q^r-1}{q-1}$ , then  $I_{\mathcal{X}}$  is the vanishing ideal of  $\mathcal{X}$ , the set  $\{Tr(y) - N(x), x^{q^r} - x\}$  is a Gröbner basis for  $I_{\mathcal{X}}$  with respect to the order  $\prec$ , and  $|\mathcal{X}| = q^{2r-1}$ .*

*Proof.* Let  $(\alpha, \beta)$  be a point on  $\mathcal{X}_u$ . As  $\alpha^u = Tr(\beta)$ ,  $\alpha^u \in \mathbb{F}_q$ . Thus, the polynomial  $x^{(q-1)u+1} - x = x((x^u)^{q-1} - 1)$  vanishes at all points of  $\mathcal{X}_u$  and from Lemma 2.1,  $x^{(q-1)u+1} - x \in I_{\mathcal{X}_u}$ . To prove that  $I_{\mathcal{X}_u} = (Tr(y) - x^u, x^{(q-1)u+1} - x)$ , we show that  $x^{q^r} - x, y^{q^r} - y \in (Tr(y) - x^u, x^{(q-1)u+1} - x)$ . Indeed, let  $v$  be the positive integer such that  $uv = \frac{q^r-1}{q-1}$ . Then one easily checks that

$$\begin{aligned} & (x^{(q-1)u(v-1)} + x^{(q-1)u(v-2)} + \cdots + x^{(q-1)u} + 1) (x^{(q-1)u+1} - x) = x^{q^r} - x \\ \text{and } & ((Tr(y) - x^u)^{q-1} - 1) (Tr(y) - x^u) + x^{u-1} (x^{(q-1)u+1} - x) \\ & = (Tr(y) - x^u)^q - (Tr(y) - x^u) + x^{uq} - x^u \\ & = Tr(y)^q - x^{uq} - Tr(y) + x^u + x^{uq} - x^u \\ & = (y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y)^q - (y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y) \\ & = y^{q^r} - y. \end{aligned}$$

Since the leading monomials  $\text{lm}(Tr(y) - x^u) = y^{q^{r-1}}$  and  $\text{lm}(x^{(q-1)u+1} - x) = x^{(q-1)u+1}$  are coprime,  $\{Tr(y) - x^u, x^{(q-1)u+1} - x\}$  is a Gröbner basis for  $I_{\mathcal{X}_u}$  according to [13, Prop. 4, p. 104]. Since  $I_{\mathcal{X}_u}$  is a radical ideal and  $\mathbb{F}_{q^r}$  is a perfect field,  $|\mathcal{X}_u| = |\Delta_{\prec}(I_{\mathcal{X}_u})|$  [5, Thm. 8.32].  $\square$

## 3. STANDARD INDICATOR FUNCTIONS

Some of the properties of the decreasing evaluation codes depend on the indicator functions of the curve  $\mathcal{X}_u$ . For a standard reference on indicator functions in the context of evaluation codes, please see [29, Sections 4 and 5]. Take  $n := |\mathcal{X}_u|$ . One may show (see [15] or [12, Prop. 3.7]) that the following linear transformation is an isomorphism

$$\begin{aligned}\varphi: \mathbb{F}_{q^r}[x, y]/I_{\mathcal{X}_u} &\rightarrow \mathbb{F}_{q^r}^n \\ f + I_{\mathcal{X}_u} &\mapsto (f(P_1), \dots, f(P_n)).\end{aligned}$$

So, for each  $P \in \mathcal{X}_u$ , there exists a unique class  $g_P + I_{\mathcal{X}_u}$  such that  $g_P(P) = 1$  and  $g_P(Q) = 0$ , for every  $Q \in \mathcal{X}_u \setminus \{P\}$ . Since  $\{M + I_{\mathcal{X}_u} \mid M \in \Delta_{\prec}(I_{\mathcal{X}_u})\}$  is a basis for  $\mathbb{F}_{q^r}[x, y]/I_{\mathcal{X}_u}$  as an  $\mathbb{F}_{q^r}$ -vector space (see e.g. [5, Prop. 6.52]), there is a unique  $\mathbb{F}_{q^r}$ -linear combination of monomials in  $\Delta_{\prec}(I_{\mathcal{X}_u})$ , which we denote by  $f_P$ , such that  $f_P(P) = 1$  and  $f_P(Q) = 0$ , for every  $Q \in \mathcal{X}_u$ . We call this polynomial  $f_P$  the *standard indicator function* of  $P$ . The existence and uniqueness of the standard indicator function  $f_P$  may also be seen as a consequence of [29, Lemma 4.2(c)].

We first describe the set of points of  $\mathcal{X}_u$  in a way that will be useful in the next section.

**Lemma 3.1.** *For every  $\gamma \in \mathbb{F}_q$ , define  $A_\gamma := \{(\alpha, \beta) \in \mathbb{A}^2(\mathbb{F}_{q^r}) \mid \text{Tr}(\beta) = \alpha^u = \gamma\}$ . Then, we have  $\mathcal{X}_u = \bigcup_{\gamma \in \mathbb{F}_q} A_\gamma$ . Moreover,  $|A_0| = q^{r-1}$  and  $|A_\gamma| = uq^{r-1}$  for all  $\gamma \in \mathbb{F}_q^*$ .*

*Proof.* If  $(\alpha, \beta) \in \mathcal{X}_u$ , then  $\alpha$  is a root of  $x^{(q-1)u+1} - x$  by Proposition 2.2. Furthermore,  $x^{(q-1)u+1} - x \mid x^{q^r} - x$ , so  $x^{(q-1)u+1} - x$  has  $(q-1)u+1$  distinct roots. For each nonzero root  $\alpha$ , we have  $(\alpha^u)^{q-1} = 1$ , so  $\alpha^u \in \mathbb{F}_q^*$  and  $x^{(q-1)u+1} - x$  must be a factor of  $x \prod_{\gamma \in \mathbb{F}_q^*} (x^u - \gamma)$ . Since the last two polynomials have the same degree and are monic, we actually have  $x^{(q-1)u+1} - x = x \prod_{\gamma \in \mathbb{F}_q^*} (x^u - \gamma)$ .

There are  $q^{r-1}$  elements  $\beta$  such that  $\text{Tr}(\beta) = \alpha^u$  for every  $\gamma \in \mathbb{F}_q$ . This shows that  $A_\gamma \subseteq \mathcal{X}_u$  for all  $\gamma \in \mathbb{F}_q$ , and that  $|A_0| = q^{r-1}$  and  $|A_\gamma| = uq^{r-1}$  when  $\gamma \in \mathbb{F}_q^*$ . On the other hand, if  $(\alpha, \beta) \in \mathcal{X}_u$  and  $\alpha^u = \gamma$ , then  $(\alpha, \beta) \in A_\gamma$ .  $\square$

**Theorem 3.2.** *Let  $P = (\alpha, \beta) \in \mathcal{X}_u$ . The polynomial*

$$f_P(x, y) := c \left( \frac{x^{(q-1)u+1} - x}{x - \alpha} \right) \left( \frac{\text{Tr}(y) - \text{Tr}(\beta)}{y - \beta} \right)$$

*is the standard indicator function for  $P$  where*

$$c := \begin{cases} -1 & \text{if } \alpha = 0 \\ (-u)^{-1} \in \mathbb{F}_q & \text{otherwise.} \end{cases}$$

*In particular,  $y^{q^{r-1}-1} x^{(q-1)u}$  is the leading monomial of the standard indicator function for  $P$ .*

*Proof.* Observe that  $f_P(\alpha, \beta) \neq 0$ . Let  $P' = (\alpha', \beta')$  be a point in  $\mathcal{X}_u$  different from  $P$ . If  $\alpha \neq \alpha'$ , then  $\left(\frac{x^{(q-1)u+1}-x}{x-\alpha}\right) \Big|_{x=\alpha'} = 0$  by Proposition 2.2; thus  $f_P(P') = 0$ . If  $\alpha = \alpha'$ , then  $\beta \neq \beta'$  and  $Tr(\beta') = (\alpha')^u = \alpha^u = Tr(\beta)$ . This means that  $\beta'$  is a root of  $Tr(y) - Tr(\beta)$  and  $\left(\frac{Tr(y)-Tr(\beta)}{y-\beta}\right) \Big|_{y=\beta'} = 0$ ; thus  $f_P(P') = 0$ . We conclude that  $f_P(\alpha', \beta') = 0$  for every  $(\alpha', \beta') \in \mathcal{X}_u \setminus \{(\alpha, \beta)\}$ .

Let  $\beta = \beta_1, \dots, \beta_{q^{r-1}} \in \mathbb{F}_{q^r}$  be the distinct roots of  $Tr(y) - Tr(\beta)$ , so that  $Tr(y) - Tr(\beta) = \prod_{i=1}^{q^{r-1}} (y - \beta_i)$ . Taking the formal derivative, we have that  $1 = \sum_{j=1}^{q^{r-1}} \prod_{i=1, i \neq j}^{q^{r-1}} (y - \beta_i)$ . Thus,

$$\left(\frac{Tr(y) - Tr(\beta)}{y - \beta}\right) \Big|_{y=\beta} = \prod_{i=2}^{q^{r-1}} (\beta - \beta_i) = 1.$$

Likewise, let  $\alpha = \alpha_1, \dots, \alpha_{u(q-1)+1}$  be such that  $x^{(q-1)u+1} - x = \prod_{i=1}^{(q-1)u+1} (x - \alpha_i)$ . Taking the formal derivative, we get  $((q-1)u+1)x^{(q-1)u} - 1 = \sum_{j=1}^{(q-1)u+1} \prod_{i=1, i \neq j}^{(q-1)u} (x - \alpha_i)$ , so

$$\left(\frac{x^{(q-1)u+1} - x}{x - \alpha}\right) \Big|_{x=\alpha} = \prod_{i=2}^{(q-1)u} (\alpha - \alpha_i) = ((q-1)u+1)\alpha^{(q-1)u} - 1.$$

If  $\alpha \neq 0$ , then we have  $\alpha^u \in \mathbb{F}_q^*$  from the proof of Lemma 3.1. Thus,

$$((q-1)u+1)\alpha^{(q-1)u} - 1 = ((q-1)u+1)(\alpha^u)^{q-1} - 1 = (q-1)u = -u.$$

As  $u \mid \frac{q^r-1}{q-1}$ , the integer  $u$  is not a multiple of  $\text{char}(\mathbb{F}_q)$ . Hence  $u \neq 0$  in  $\mathbb{F}_q$ .  $\square$

#### 4. CODE CONSTRUCTION

In this section, we define and compute the basic parameters of a new family of evaluation codes called decreasing norm-trace codes. We then consider their relationship with algebraic geometry codes defined on (extended) norm-trace curves

**4.1. Code parameters.** The *evaluation map*, denoted  $\text{ev}$ , is the  $\mathbb{F}_{q^r}$ -linear map given by

$$\begin{aligned} \text{ev}: \quad \mathbb{F}_{q^r}[x, y] &\rightarrow \mathbb{F}_{q^r}^n \\ f &\mapsto (f(P_1), \dots, f(P_n)), \end{aligned}$$

where  $\mathcal{X}_u = \{P_1, \dots, P_n\} \subseteq \mathbb{F}_{q^r}^2$  and  $n := q^{r-1}((q-1)u+1)$ .

**Definition 4.1.** A *decreasing norm-trace code* is an evaluation code  $\text{ev}(\mathcal{M})$  such that  $\mathcal{M} \subseteq \mathbb{F}_{q^r}[x, y]$  is closed under divisibility, meaning if  $M \in \mathcal{M}$  and  $M'$  divides  $M$ , then  $M' \in \mathcal{M}$ .

**Example 4.2.** Take  $q = 3$  and  $r = 2$ . Figure 1 (a) shows the points of the norm-trace curve  $\mathcal{X}$ . Let  $\mathcal{M}$  be the set of monomials in  $\mathbb{F}_{q^r}[x, y]$  whose exponents are the points in Figure 1 (b). Note that  $\mathcal{M}$  is closed under divisibility. Using the coding theory package [3] for Macaulay2 [20] and Magma [6], we obtain that  $\text{ev}(\mathcal{M})$  is a  $[27, 10, 15]$  decreasing norm-trace code over  $\mathbb{F}_9$ .

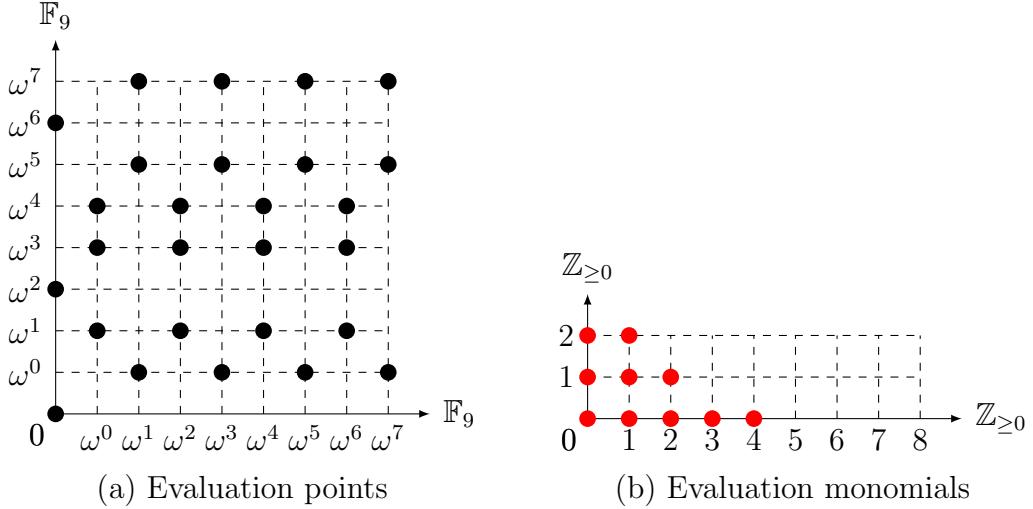


FIGURE 1. Take  $q = 3$  and  $r = 2$ . (a) Shows the points of the norm-trace curve  $\mathcal{X} : x^4 = y^3 + y$ . Let  $\mathcal{M}$  be the set of monomials whose exponents are the points in (b). The evaluation code  $\text{ev}(\mathcal{M})$  is an  $[27, 10, 15]$  decreasing norm-trace code over  $\mathbb{F}_9$ .

Denote by  $\Delta(x^{(q-1)u+1}, y^{q^{r-1}})$  the set of monomials that are not multiples of either of these two monomials. From now on, we assume that  $\mathcal{M} \subseteq \Delta(x^{(q-1)u+1}, y^{q^{r-1}})$ .

We come to one of the main results of this work, which computes the basic parameters of a decreasing norm-trace code.

**Theorem 4.3.** *The decreasing norm-trace code  $\text{ev}(\mathcal{M})$  has the following basic parameters.*

- (1) *Length*  $n = |\mathcal{X}_u| = ((q-1)u+1)q^{r-1}$ .
- (2) *Dimension*  $k = |\mathcal{M}|$ .
- (3) *Minimum distance*

$$d = ((q-1)u+1)q^{r-1}$$

$$- \max \left( \{ \min (aq^{r-1} + (u(q-1) + 1 - a)b, aq^{r-1} + bu) \mid x^a y^b \in \mathcal{M} \} \right).$$

*Proof.* Statement (1) is a consequence of Proposition 2.2. Statement (2) follows from the fact that  $\{M + I_{\mathcal{X}_u} \mid M \in \Delta_{\prec}(I_{\mathcal{X}_u})\}$  is a basis for  $\mathbb{F}_{q^r}[x, y]/I_{\mathcal{X}_u}$  as an  $\mathbb{F}_{q^r}$ -vector

space together with the fact that the linear transformation  $\varphi$ , defined at the beginning of Section 3, is an isomorphism. To prove Statement (3), let  $f$  be a nonzero polynomial in the  $\mathbb{F}_{q^r}$ -vector space generated by the monomials in  $\mathcal{M}$ . The set of points in  $\mathcal{X}_u$  which are zeros of  $f$  is the set of the zeros of the ideal  $I_{\mathcal{X}_u} + (f) \subseteq \mathbb{F}_{q^r}[x, y]$ , denoted by  $V(I_{\mathcal{X}_u} + (f))$ . The ideal  $I_{\mathcal{X}_u} + (f)$  is a radical ideal; see [5, Prop. 8.14]. Therefore, [5, Thm. 8.32] implies that  $|V(I_{\mathcal{X}_u} + (f))| = \Delta_{\prec}(I_{\mathcal{X}_u} + (f))$ . Let  $x^a y^b$  be the leading monomial of  $f$  and let  $\Delta(x^{(q-1)u+1}, y^{q^{r-1}}, x^a y^b)$  be the set of monomials that are not multiples of either of these three monomials. Then  $\Delta_{\prec}(I_{\mathcal{X}_u} + (f)) \subseteq \Delta(x^{(q-1)u+1}, y^{q^{r-1}}, x^a y^b)$  so that

$$\begin{aligned} |V(I_{\mathcal{X}_u} + (f))| &\leq |\Delta(x^{(q-1)u+1}, y^{q^{r-1}}, x^a y^b)| \\ &= ((q-1)u+1)q^{r-1} - ((q-1)u+1-a)(q^{r-1}-b) \\ &= aq^{r-1} + ((q-1)u+1-a)b. \end{aligned}$$

On the other hand, from [17, Proposition 4]), we have that  $|V(I_{\mathcal{X}_u} + (f))| \leq aq^{r-1} + bu$  (to verify a hypothesis in [17, Proposition 4] one must use that if  $x^c y^e$  and  $x^{c'} y^{e'}$  are monomials in  $\mathcal{M}$  then  $cq^{r-1} + eu \neq c'q^{r-1} + e'u$ ).

Assume that  $aq^{r-1} + bu \leq aq^{r-1} + ((q-1)u+1-a)b$  and  $b \neq 0$ , so we have  $a \leq (q-2)u+1$ . According to Lemma 3.1 (and its proof), for all  $\gamma \in \mathbb{F}_q^*$ , the number of distinct elements of  $\mathbb{F}_{q^r}$ , which appear as the first entry of points in  $A_\gamma$ , is  $u$ , while 0 is the first entry in all points of  $A_0$ . Fix  $\gamma \in \mathbb{F}_q^*$ . Since  $a \leq (q-2)u+1$ , we may choose  $\alpha_1, \dots, \alpha_a \in \mathbb{F}_{q^r}$  such that for all  $i = 1, \dots, a$  we have  $(\alpha_i, \beta_i) \in \mathcal{X}_u$  for some  $\beta_i \in \mathbb{F}_{q^r}$  and  $\alpha_i^u \neq \gamma$ . Recall that  $b < q^{r-1}$ , and let  $\beta_1, \dots, \beta_b \in \mathbb{F}_{q^r}$  be distinct elements such that  $Tr(\beta_j) = \gamma$  for all  $j = 1, \dots, b$ . Let  $g(x, y) = \prod_{i=1}^a (x - \alpha_i) \cdot \prod_{j=1}^b (y - \beta_j)$ . For every  $i = 1, \dots, a$ , there exist  $q^{r-1}$  points in  $\mathcal{X}_u$  of the form  $(\alpha_i, \beta)$ , none of them in  $A_\gamma$ . For every  $j = 1, \dots, b$ , there exist  $u$  points of  $\mathcal{X}_u$  of the form  $(\alpha, \beta_j)$ , all of them in  $A_\gamma$ . Hence,  $|V(I_{\mathcal{X}_u} + (g))| = aq^{r-1} + bu$ .

Now assume that  $aq^{r-1} + ((q-1)u+1-a)b < aq^{r-1} + bu$  and  $b \neq 0$ . Then  $a > (q-2)u+1$ . Again, we fix  $\gamma \in \mathbb{F}_q^*$  and take  $\beta_1, \dots, \beta_b \in \mathbb{F}_{q^r}$  to be distinct elements such that  $Tr(\beta_j) = \gamma$  for all  $j = 1, \dots, b$ . Let  $\alpha_1, \dots, \alpha_a \in \mathbb{F}_{q^r}$  be distinct elements such that for all  $i = 1, \dots, a$  we have  $(\alpha_i, \beta_i) \in \mathcal{X}_u$  for some  $\beta_i \in \mathbb{F}_{q^r}$  and for exactly  $a - (q-2)u-1$  elements  $\alpha_i$  we have  $\alpha_i^u = \gamma$  (note that since  $a < (q-1)u+1$  we get  $a - (q-2)u-1 < u$ ). Let  $h(x, y) = \prod_{i=1}^a (x - \alpha_i) \cdot \prod_{j=1}^b (y - \beta_j)$ , for each  $\alpha \in \{\alpha_1, \dots, \alpha_a\}$  we have  $q^{r-1}$  elements  $(\alpha, \beta) \in \mathcal{X}_u$ , which are also zeros of  $h$ . For each  $\beta \in \{\beta_1, \dots, \beta_b\}$  we have  $u - (a - (q-2)u-1) = (q-1)u+1-a$  elements of the form  $(\alpha, \beta) \in \mathcal{X}_u$  which

are zeros of  $h$  and have not been counted yet. Thus, the total number of zeros of  $h$  in  $\mathcal{X}_u$  is  $|V(I_{\mathcal{X}_u} + (h))| = aq^{r-1} + b((q-1)u + 1 - a)$ .

If  $b = 0$ , then  $aq^{r-1} + ((q-1)u + 1 - a)b = aq^{r-1} + bu$ . Taking  $\alpha_1, \dots, \alpha_a \in \mathbb{F}_{q^r}$  such that for all  $i = 1, \dots, a$ , we have  $(\alpha_i, \beta_i) \in \mathcal{X}_u$  for some  $\beta_i \in \mathbb{F}_{q^r}$ , the polynomial  $t(x, y) = \prod_{i=1}^a (x - \alpha_i)$  is such that  $|V(I_{\mathcal{X}_u} + (t))| = aq^{r-1}$ .

Thus, we have proved that for every monomial  $x^a y^b \in \mathcal{M}$ , there exists a polynomial  $f$  in the  $\mathbb{F}_{q^r}$ -vector space generated by the monomials in  $\mathcal{M}$  having  $x^a y^b$  as its leading monomial, and such that  $|V(I_{\mathcal{X}_u} + (f))|$  attains its greatest possible value, namely  $\min \{aq^{r-1} + (u(q-1) + 1 - a)b, aq^{r-1} + bu\}$ . This completes the proof.  $\square$

**Example 4.4.** Take  $q = 2$ ,  $r = 4$ , and  $u = 3$ . Figure 2 (a) shows the points of the extended norm-trace curve  $\mathcal{X}_u$ . Let  $\mathcal{M}$  be the set of monomials in  $\mathbb{F}_{q^r}[x, y]$  whose exponents are the points in Figure 2 (b). Note that  $\mathcal{M}$  is closed under divisibility. By Theorem 4.3,  $\text{ev}(\mathcal{M})$  is a  $[32, 12, 12]$  decreasing norm-trace code over  $\mathbb{F}_{16}$ .

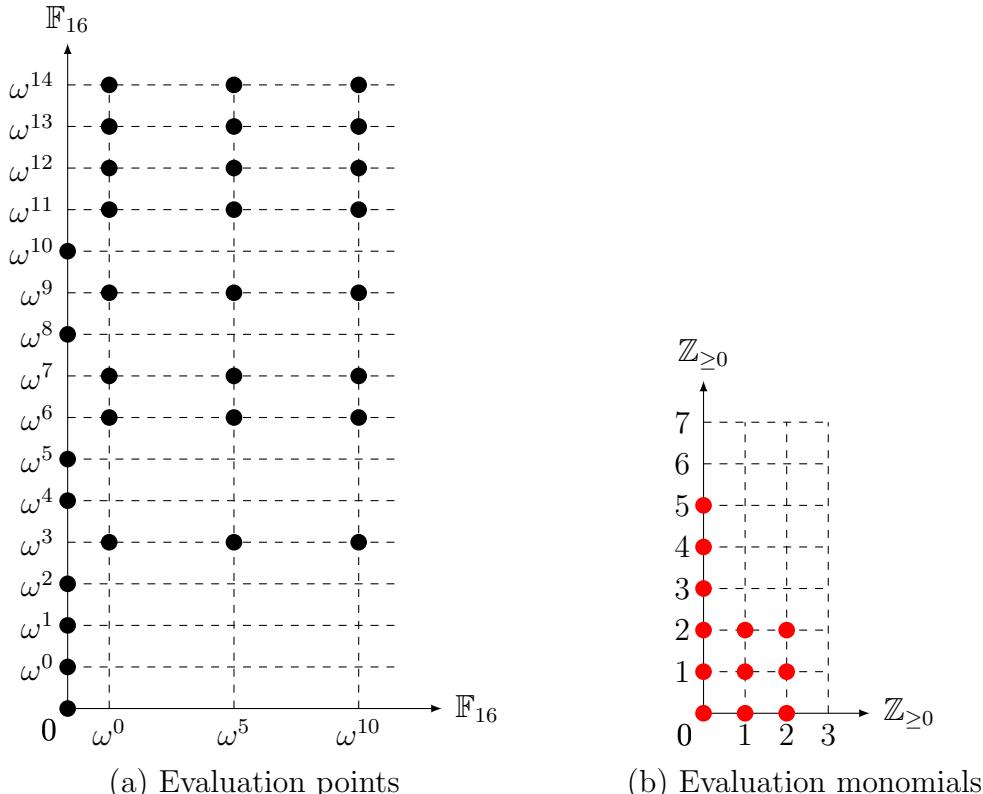


FIGURE 2. Take  $q = 2$ ,  $r = 4$ , and  $u = 3$ . (a) Shows the points of the norm-trace curve  $\mathcal{X}_u : x^3 = y^8 + y^4 + y^2 + y$ . Let  $\mathcal{M}$  be the set of monomials whose exponents are the points in (b). The evaluation code  $\text{ev}(\mathcal{M})$  is an  $[32, 12, 12]$  decreasing norm-trace code over  $\mathbb{F}_{16}$ .

**4.2. Relationship with one-point algebraic geometric codes.** The family of decreasing norm-trace codes contains, as a particular case, the family of one-point geometric codes over the norm-trace. Indeed, define  $\mathcal{L}_s := \left\{ x^i y^j \in \Delta(I_{\mathcal{X}_u}) \mid iq^{r-1} + j \frac{q^r - 1}{q-1} \leq s \right\}$ . It is straightforward to check that  $\mathcal{L}_s$  is closed under divisibility, and that the one-point geometric Goppa codes over the norm-trace are obtained, as detailed below, through the evaluation, at the points of  $\mathcal{X}_u$ , of the polynomials in the space generated by  $\mathcal{L}_s$  (see, e.g. [16, 22]). We note that the new constructions of decreasing norm-trace codes is more general. Example 4.4 is not a one-point code. The nearest one-point codes are  $C(D, G)$  with  $G = \{18, 19, 20\}P_\infty$ , which are  $[32, \{12, 13, 14\}, \geq \{14, 13, 12\}]$  codes.

The extended norm-trace codes introduced and studied in [7] and [23] are also particular instances of decreasing norm-trace codes.

**Remark 4.5.** Note that Theorem 4.3 allows us to recover the exact minimum distances of one-point codes on  $\mathcal{X}_u$  by choosing specific sets  $\mathcal{M} \subseteq \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$ . For the norm-trace curve, this approach had already appeared in [16], where such codes are denoted by  $E(s)$ . Moreover, the improved codes  $\tilde{E}(s)$ , which appear in [16], are also decreasing norm-trace codes, and our results recover those of [16] with respect to their parameters.

One may notice that  $k + d =$

$$n+1 - \left( \max \left( \{ \min (aq^{r-1} + (u(q-1) + 1 - a)b, aq^{r-1} + bu) \mid x^a y^b \in \mathcal{M} \} \right) - |\mathcal{M}| + 1 \right),$$

meaning decreasing norm-trace codes have a gap of

$$\max \left( \{ \min (aq^{r-1} + (u(q-1) + 1 - a)b, aq^{r-1} + bu) \mid x^a y^b \in \mathcal{M} \} \right) - |\mathcal{M}| + 1$$

to the Singleton Bound  $k + d \leq n + 1$ .

Let  $\mathcal{X}$  be the nonsingular curve defined over  $\mathbb{F}_{q^r}$  which has

$$x^{\frac{q^r - 1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$$

as an affine plane model. Then  $\mathcal{X}$  has only one point at infinity, say  $P_\infty$ , which is a rational point, and  $\mathcal{X}$  has exactly  $q^{2r-1}$  other rational points. The pole divisor of  $x$  is  $q^{r-1}P_\infty$  and the pole divisor of  $y$  is  $\frac{q^r - 1}{q-1}P_\infty$ . Let  $D$  be the divisor which is the sum of the  $q^{2r-1}$  affine rational points of  $\mathcal{X}$ . All AG-codes of the form  $C_{\mathcal{L}}(D, sP_\infty)$  coincide with codes  $\text{ev}(L_s)$ , where  $L_s$  is the  $\mathbb{F}_{q^r}$ -vector space generated by

$$A_s = \left\{ x^a y^b \mid 0 \leq a \leq q^r - 1, 0 \leq b \leq q^{r-1} - 1, aq^{r-1} + b \frac{q^r - 1}{q-1} \leq s \right\}$$

(see [16] Remark 1] and the references therein). The dimension of  $L_s$  is  $|A_s|$ , and if, for a given  $s$ , there exists a monomial  $x^a y^b \in A_s$  such that

$$\min \left( aq^{r-1} + (q^r - a)b, aq^{r-1} + b \frac{q^r - 1}{q - 1} \right) = s,$$

then the minimum distance of  $L_s$  is equal to  $q^{2r-1} - \sigma(s)$ , where

$$\sigma(s) = \max \left\{ \min \left( aq^{r-1} + (q^r - a)b, aq^{r-1} + b \frac{q^r - 1}{q - 1} \right) \mid x^a y^b \in A_s \right\}$$

(see [16] Thm. 1 and Thm. 2]). We present now some numerical examples comparing codes constructed in this paper with the algebraic geometry codes described above.

**Example 4.6.** We start by taking  $q = 3$  and  $r = 2$ .

Choosing  $s = 23$ , we get that

$$A_{23} = \{x^a y^b \mid 0 \leq a \leq 8, 0 \leq b \leq 2, 3a + 4b \leq 23\}.$$

Thus  $x^5 y^2 \in A_{23}$  and  $\min(5 \cdot 3 + (9 - 5) \cdot 2, 5 \cdot 3 + 2 \cdot 4) = 23$ , so the minimum distance is equal to  $27 - \sigma(23) = 27 - 23 = 4$ . It is easy to check that

$$A_{23} = \{x^a y^b \mid 0 \leq a \leq 5, 0 \leq b \leq 2\} \cup \{x^6, x^6 y, x^7\},$$

so  $\dim(L_{23}) = 21$ . Now we take  $\mathcal{M}_{23} := A_{23} \cup \{x^7 y\}$ . Then  $\mathcal{M}_{23}$  is closed under divisibility, and from the formulas of Theorem 4.3, we get that  $\text{ev}(\mathcal{M}_{23})$  has dimension 22 and minimum distance equal to 4. Both codes have the same length, so  $\text{ev}(\mathcal{M}_{23})$  is better.

We also obtain a better code choosing  $s = 21$ ; in this case

$$A_{21} = \{x^a y^b \mid 0 \leq a \leq 4, 0 \leq b \leq 2\} \cup \{x^5, x^5 y, x^6, x^7\},$$

so  $\dim(L_{21}) = 19$  and the minimum distance is equal to  $27 - 21 = 6$  (here we use that  $x^7 \in A_{21}$ ). Taking  $\mathcal{M}_{21} := A_{21} \cup \{x^6 y\}$ , we get from Theorem 4.3 that  $\dim(\text{ev}(\mathcal{M}_{21})) = 20$  and has minimum distance equal to 6.

Both  $\mathcal{M}_{23}$  and  $\mathcal{M}_{21}$  have the best minimum distance among known codes defined over  $\mathbb{F}_{3^2}$  with length 27 and, respectively, dimensions 22 and 20, according to the tables in [19].

By taking higher values for the field over which the codes are defined we may obtain more striking differences.

**Example 4.7.** Take  $q = 3$  and  $r = 4$ , so that  $q^r = 81$ ,  $q^{r-1} = 27$  and  $(q^r - 1)/(q - 1) = 40$ . Set  $s = 57 \cdot 27 = 1539$ . Unlike the above example, which was computed by hand, in this one we used Magma ([6]) to find out that  $|A_{1539}| = 1033$ . Thus,  $\dim(L_{1539}) = 1033$

$\mathcal{M}$	$\dim(\text{ev}(\mathcal{M}))$	min. dist. of $\text{ev}(\mathcal{M})$
$\{1, y\}$	2	13
$\{1, y, x\}$	3	12
$\{1, y, y^2, x\}$	4	11
$\{1, y, y^2, x, xy\}$	5	10
$\{1, y, y^2, x, xy, x^2\}$	6	9
$\{1, y, y^2, x, xy, xy^2, x^2\}$	7	8
$\{1, y, y^2, x, xy, xy^2, x^2, x^2y\}$	8	7
$\{1, y, y^2, x, xy, xy^2, x^2, x^2y, x^3\}$	9	6
$\{1, y, y^2, x, xy, xy^2, x^2, x^2y, x^2y^2, x^3\}$	10	5
$\{1, y, y^2, x, xy, xy^2, x^2, x^2y, x^2y^2, x^3, x^3y\}$	11	4
$\{1, y, y^2, x, xy, xy^2, x^2, x^2y, x^2y^2, x^3, x^3y, x^4\}$	12	3

TABLE 1. Code parameters.

and using the formulas above (and the fact that  $x^{57} \in A_{1539}$ ), we get that the minimum distance of this code is  $q^{2r-1} - 1539 = 2187 - 1539 = 648$ . Now we take

$$\begin{aligned} \mathcal{M}_{1539} := A_{1539} \cup \{ &x^{44}y^9, x^{45}y^9, x^{46}y^8, x^{47}y^7, x^{48}y^7, x^{49}y^6, x^{50}y^5, \\ &x^{50}y^6, x^{51}y^5, x^{52}y^4, x^{53}y^3, x^{54}y^3, x^{55}y^2, x^{56}y \}. \end{aligned}$$

One may check that  $\mathcal{M}_{1539}$  is closed under divisibility, and using the formulas of Theorem 4.3, we get that  $\text{ev}(\mathcal{M}_{1539})$  has dimension equal to 1047 and minimum distance equal to 648.

We also get good codes when  $u$  is a proper divisor of  $(q^r - 1)/(q - 1)$  as the next example demonstrates.

**Example 4.8.** Take  $q = 3$  and  $r = 2$ , but this time we choose  $u = 2$ , a proper divisor of  $(q^r - 1)/(q - 1) = 4$ . We construct codes of length  $((q - 1)u + 1)q^{r-1} = 15$  using the monomials from the first column of Table 1. The parameters of these codes are given in the second and third column of Table 1. According to the tables in [19], these are the best minimum distances for the corresponding dimensions, considering codes of length 15 defined over  $\mathbb{F}_{3^2}$ .

## 5. DUALS OF DECREASING NORM-TRACE CODES

This section proves that the dual of a decreasing norm-trace code is equivalent to a decreasing norm-trace code. In addition, we describe the dual code in terms of the monomial set and the coefficients of the indicator functions. We then give conditions to find families of self-dual and self-orthogonal codes.

Recall that the two linear codes  $C_1$  and  $C_2$  in  $\mathbb{F}_{q^r}^n$  are *equivalent* if there is  $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{F}_{q^r}^n$  such that  $\beta_i \neq 0$  for all  $i$  and  $C_2 = \beta \cdot C_1 := \{\beta \cdot c \mid c \in C_1\}$ , where  $\beta \cdot c := (\beta_1 c_1, \dots, \beta_n c_n)$  for  $c = (c_1, \dots, c_n) \in C_1$ . Some authors call such codes monomially equivalent, but we will simply say equivalent as no other type of equivalence is considered in this paper.

We come to one of the main results of this work, which computes the dual of a decreasing norm-trace code. Recall that the two linear codes  $C_1$  and  $C_2$  in  $\mathbb{F}_{q^r}^n$  are *equivalent* if there is  $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{F}_{q^r}^n$  such that  $\beta_i \neq 0$  for all  $i$  and  $C_2 = \beta \cdot C_1 := \{\beta \cdot c \mid c \in C_1\}$ , where  $\beta \cdot c := (\beta_1 c_1, \dots, \beta_n c_n)$  for  $c = (c_1, \dots, c_n) \in C_1$ .

**Theorem 5.1.** *Assume  $\mathcal{X}_u = \{P_1, \dots, P_n\}$  and let  $\text{ev}(\mathcal{M})$  be a decreasing norm-trace code. The dual code  $\text{ev}(\mathcal{M})^\perp$  is equivalent to the code  $\text{ev}(\mathcal{M}^c)$  where*

$$\mathcal{M}^c := \left\{ \frac{x^{(q-1)u} y^{q^{r-1}-1}}{x^i y^j} : x^i y^j \in \Delta \left( x^{(q-1)u+1}, y^{q^{r-1}} \right) \setminus \mathcal{M} \right\}$$

denotes the complement of  $\mathcal{M}$ . More precisely,

$$\text{ev}(\mathcal{M})^\perp = \beta \cdot \text{ev}(\mathcal{M}^c),$$

where  $\beta_i := \begin{cases} u^{-1} & \text{if the } x\text{-coordinate of } P_i \text{ is nonzero} \\ 1 & \text{otherwise.} \end{cases}$

*Proof.* From Theorem 3.2, we get that  $y^{q^{r-1}-1} x^{(q-1)u}$  is the leading monomial of the standard indicator function for all points in  $\mathcal{X}_u$ . We also note that

$$|\mathcal{M}| + |\mathcal{M}^c| = \left| \Delta \left( x^{(q-1)u+1}, y^{q^{r-1}} \right) \right| = |\mathcal{X}_u|.$$

Thus, according to [30, Theorem 5.4] ([30, Theorem 5.4] is an updated version of [29, Theorem 5.4]), to prove the Theorem it suffices to prove that, given  $x^a y^b \in \mathcal{M}$  and  $x^c y^d \in \mathcal{M}^c$ , the coefficient of the monomial  $x^{(q-1)u} y^{q^{r-1}-1}$  in the unique  $\mathbb{F}_{q^r}$ -linear combination of monomials in  $\Delta_{\prec}(I_{\mathcal{X}_u})$  which has the same class, in  $\mathbb{F}_{q^r}[x, y]/I_{\mathcal{X}_u}$ , as  $x^{a+c} y^{b+d}$ , is equal to zero.

Before we prove that, we claim that if  $a + c \geq (q-1)u$ , then  $b + d < q^{r-1} - 1$ . Indeed, assume that  $b + d \geq q^{r-1} - 1$ . We set  $c' = (q-1)u - c$  and  $d' = q^{r-1} - 1 - d$ , and from the definition of  $\mathcal{M}^c$ , we get that  $x^{c'} y^{d'} \notin \mathcal{M}$ . From  $d \geq q^{r-1} - 1 - b$ , we get  $d' \leq b$ . Since  $\mathcal{M}$  is closed under divisibility, we must have  $c' > a$ , so  $(q-1)u - c > a$  and  $a + c < (q-1)u$ , which proves the claim.

This shows that either  $a+c \geq (q-1)u$  and  $b+d < q^{r-1} - 1$ , or  $b+d \geq q^{r-1} - 1$  and  $a+c < (q-1)u$ .

Assume that  $a+c > (q-1)u$ . Since  $a+c \leq 2(q-1)u$ , we write  $a+c = ((q-1)u+1)+r$  with  $0 \leq r \leq (q-1)u-1$ . Then  $x^{a+c} + I_{\mathcal{X}_u} = x^{(q-1)u+1}x^r + I_{\mathcal{X}_u} = x^{r+1} + I_{\mathcal{X}_u}$  and we get, in this case, that  $x^{a+c}y^{b+d} + I_{\mathcal{X}_u} = x^{r+1}y^{b+d} + I_{\mathcal{X}_u}$  with  $x^{r+1}y^{b+d} \in \Delta_{\prec}(I_{\mathcal{X}_u}) \setminus \{x^{(q-1)u}y^{q^{r-1}-1}\}$ , since  $b+d < q^{r-1} - 1$ .

Now assume that  $b+d > q^{r-1} - 1$  (and then  $a+c < (q-1)u$ ). Note that  $b+d \leq 2q^{r-1} - 2$ , so we write  $b+d = 2q^{r-1} - 2 - e$ , with  $0 \leq e \leq q^{r-1} - 2$ . We have

$$\begin{aligned} y^{2q^{r-1}-2-e} &= y^{q^{r-1}-2-e}(y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y - x^u) \\ &\quad - y^{q^{r-1}-2-e}(y^{q^{r-2}} + \cdots + y^q + y - x^u) \end{aligned}$$

so that

$$x^{a+c}y^{b+d} + I_{\mathcal{X}_u} = -x^{a+c}y^{q^{r-1}-2-e}(y^{q^{r-2}} + \cdots + y^q + y - x^u) + I_{\mathcal{X}_u}.$$

If  $q^{r-1} + q^{r-2} - 2 - e \leq q^{r-1} - 1$  then all the monomials in the polynomial  $x^{a+c}y^{q^{r-1}-2-e}(y^{q^{r-2}} + \cdots + y^q + y - x^u)$  are in  $\Delta_{\prec}(I_{\mathcal{X}_u}) \setminus \{x^{(q-1)u}y^{q^{r-1}-1}\}$ , except possibly for  $x^{a+b+u}$ , which may be reduced, as above, to a power of  $x$  in  $\Delta_{\prec}(I_{\mathcal{X}_u})$ .

The last case to consider is when  $q^{r-1} + q^{r-2} - 2 - e \geq q^{r-1}$ . In this case, we have to find proper representatives for some monomials in  $x^{a+c}y^{q^{r-1}-2-e}(y^{q^{r-2}} + \cdots + y^q + y - x^u)$ . We write  $q^{r-1} + q^{r-2} - 2 - e = 2q^{r-1} - 2 - e'$ , where  $e' = q^{r-1} - q^{r-2} + e$ , and we have  $q^{r-1} - q^{r-2} \leq e' \leq q^{r-1} - 2$ . From

$$\begin{aligned} y^{2q^{r-1}-2-e'} &= y^{q^{r-1}-2-e'}(y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y - x^u) \\ &\quad - y^{q^{r-1}-2-e'}(y^{q^{r-2}} + \cdots + y^q + y - x^u), \end{aligned}$$

we get that  $x^{a+c}y^{2q^{r-1}-2-e'} + I_{\mathcal{X}_u} = -x^{a+c}y^{q^{r-1}-2-e'}(y^{q^{r-2}} + \cdots + y^q + y - x^u) + I_{\mathcal{X}_u}$ . Since  $q^{r-1} + q^{r-2} - 2 - e' \leq 2q^{r-2} - 2 < q^{r-1} - 1$ , we get that the monomials in the polynomial  $x^{a+c}y^{q^{r-1}-2-e'}(y^{q^{r-2}} + \cdots + y^q + y - x^u)$  are in  $\Delta_{\prec}(I_{\mathcal{X}_u}) \setminus \{x^{(q-1)u}y^{q^{r-1}-1}\}$ , except possibly for  $x^{a+b+u}$  which may be represented by a power of  $x$  in  $\Delta_{\prec}(I_{\mathcal{X}_u})$ . This takes care of the monomial  $x^{a+c}y^{q^{r-1}+q^{r-2}-2-e}$  in  $x^{a+c}y^{q^{r-1}-2-e}(y^{q^{r-2}} + \cdots + y^q + y - x^u)$ . In the same way we prove that if, for some integer  $s \geq 3$ , we get  $q^{r-1} + q^{r-s} - 2 - e \geq q^{r-1}$ , then  $y^{q^{r-1}+q^{r-s}-2-e} + I_{\mathcal{X}_u} = -y^{q^{r-1}-2-e''}(y^{q^{r-2}} + \cdots + y^q + y - x^u) + I_{\mathcal{X}_u}$ , where  $q^{r-1} - q^{r-s} \leq e'' \leq q^{r-1} - 2$ , so  $q^{r-1} + q^{r-s} - 2 - e'' \leq q^{r-2} + q^{r-s} - 2 < q^{r-1} - 1$ . This proves that, also in the case where  $q^{r-1} + q^{r-2} - 2 - e \geq q^{r-1}$ , the unique  $\mathbb{F}_{q^r}$ -linear combination of monomials in  $\Delta_{\prec}(I_{\mathcal{X}_u})$ , which has the same class as  $x^{a+c}y^{q^{r-1}-2-e}(y^{q^{r-2}} + \cdots + y^q + y - x^u)$  in

$\mathbb{F}_{q^r}[x, y]/I_{\mathcal{X}_u}$ , has zero as the coefficient of the monomial  $x^{(q-1)u}y^{q^{r-1}-1}$ , which completes the proof of the Theorem.  $\square$

**Example 5.2.** Take  $q = 3$  and  $r = 2$ . Figure 1 (a) shows the points of the norm-trace curve  $\mathcal{X} : x^4 = y^3 + y$ . Let  $\mathcal{M}$  be the set of monomials in  $\Delta(x^9, y^3)$  of degree at most 4. The exponents of these monomials are the points in Figure 3 (a). The complement of  $\mathcal{M}$  on  $\mathcal{X}$  is the set of monomials  $\mathcal{M}^c$ , whose exponents are the points in Figure 3 (b). By Theorem 5.1, the dual code  $\text{ev}(\mathcal{M})^\perp$  is equivalent to the code  $\text{ev}(\mathcal{M}^c)$ .

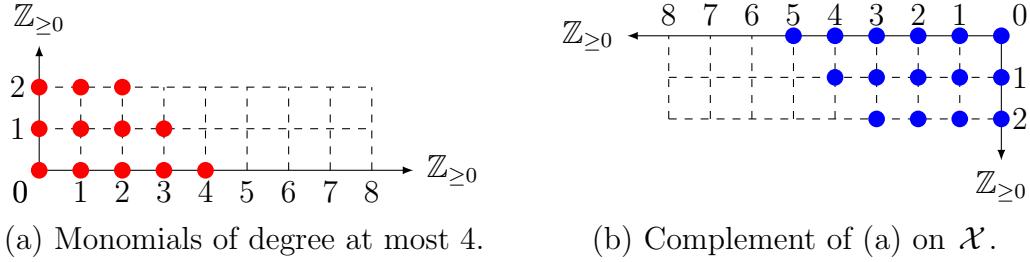


FIGURE 3. (a) shows the exponents of the set of monomials  $\mathcal{M}$  in  $\Delta(x^9, y^3)$  of degree at most 4. (b) shows the exponents of  $\mathcal{M}^c$ , the complement of  $\mathcal{M}$  on  $\mathcal{X}$ . By Theorem 5.1, the dual code  $\text{ev}(\mathcal{M})^\perp$  is equivalent to the code  $\text{ev}(\mathcal{M}^c)$ .

Recall that the hull of a code  $C$  is  $\text{Hull}(C) := C \cap C^\perp$ . The code  $C$  is *self-dual* if  $C = C^\perp$  and *self-orthogonal* if  $C \subseteq C^\perp$ . Theorem 5.1 gives a powerful tool for designing self-dual and self-orthogonal codes.

**Theorem 5.3.** Assume  $\mathcal{X}_u = \{P_1, \dots, P_n\}$  and let  $\text{ev}(\mathcal{M})$  be a decreasing norm-trace code. If the equation  $x^2 = u$  has a solution  $\alpha$  in  $\mathbb{F}_{q^r}$ , then

$$\text{Hull}(\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M})) = \boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M} \cap \mathcal{M}^c),$$

where  $\lambda_i := \begin{cases} \alpha^{-1} & \text{if the } x\text{-coordinate of } P_i \text{ is nonzero} \\ 1 & \text{otherwise.} \end{cases}$

*Proof.* Denote by  $\boldsymbol{\lambda}^{-1}$  the vector whose entries are  $\lambda_i^{-1}$ . By Theorem 5.1, we have that  $\boldsymbol{\lambda}\boldsymbol{\lambda} = \boldsymbol{\beta}$ , so  $\boldsymbol{\lambda} = \boldsymbol{\lambda}^{-1}\boldsymbol{\beta}$ , where the product between vectors is pointwise. Thus,  $(\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M}))^\perp = \boldsymbol{\lambda}^{-1} \cdot \text{ev}(\mathcal{M})^\perp = \boldsymbol{\lambda}^{-1}\boldsymbol{\beta} \cdot \text{ev}(\mathcal{M}^c) = \boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M}^c)$ .  $\square$

**Corollary 5.4.** Assume  $\mathcal{X}_u = \{P_1, \dots, P_n\}$  and the equation  $x^2 = u$  has a solution  $\alpha$  in  $\mathbb{F}_{q^r}$ . If  $\mathcal{M} \subseteq \mathcal{M}^c$ , then  $\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M})$  is a self-orthogonal code, where  $\lambda_i$  is as in Theorem 5.3. If  $\mathcal{M} = \mathcal{M}^c$ , then  $\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M})$  is a self-dual code.

*Proof.* If  $\mathcal{M} \subseteq \mathcal{M}^{\complement}$ , then  $\text{Hull}(\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M})) = \boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M} \cap \mathcal{M}^{\complement}) = \boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M})$  by Theorem 5.3. Thus,  $\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M}) = \text{Hull}(\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M})) \subseteq (\boldsymbol{\lambda} \cdot \text{ev}(\mathcal{M}))^{\perp}$ . The case  $\mathcal{M} = \mathcal{M}^{\complement}$  is analogous.  $\square$

**Example 5.5.** Take  $q = 2$ ,  $r = 4$ , and  $u = 5$ . Figure 4 (a) shows the points of the set  $\mathcal{X}_u$ . Let  $\mathcal{M}$  be the set of monomials in  $\mathbb{F}_{q^r}[x, y]$  with degree in  $x$  at most 5 and degree in  $y$  at most 4. The exponents of these monomials are the points in Figure 4 (b). As  $5 \equiv 1$  in  $\mathbb{F}_2$ , then  $\text{Hull}(\text{ev}(\mathcal{M})) = \text{ev}(\mathcal{M} \cap \mathcal{M}^{\complement}) = \text{ev}(\mathcal{M})$  by Theorem 5.3. Thus,  $\text{ev}(\mathcal{M})$  is a self-dual code by Corollary 5.4.

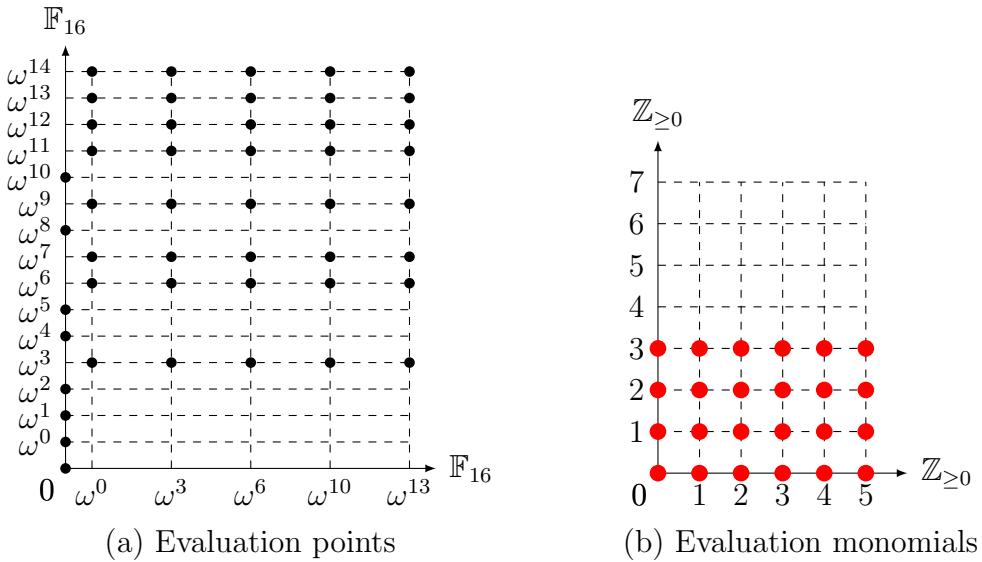


FIGURE 4. (a) shows the points of the curve  $\mathcal{X} : x^u = y^8 + y^4 + y^2 + y$ . Let  $\mathcal{M}$  be the set of monomials whose exponents are the points in (b). The evaluation code  $\text{ev}(\mathcal{M})$  is a self-dual code over  $\mathbb{F}_{16}$ .

## 6. SINGLE ERASURE REPAIR SCHEME

This section defines a repair scheme that repairs a single erasure for specific decreasing norm-trace codes. An element of  $\mathbb{F}_{q^r}$  may be thought of as a vector in  $\mathbb{F}_q^r$ . In this theory, the elements of  $\mathbb{F}_{q^r}$  are called *symbols* and the elements of  $\mathbb{F}_q$  are called *subsymbols*. Given a code  $C \subset \mathbb{F}_{q^r}^n$ , a repair scheme is an algorithm that recovers the entry of any vector of  $C$  using the other entries. The *bandwidth*  $b$  is the number of subsymbols required by the algorithm to repair the entry. A codeword is defined by  $nr$  subsymbols, and the fraction  $\frac{b}{nr}$  is called *bandwidth rate*.

Recall that  $\Delta(x^i, y^j)$  denotes the set of monomials which are not multiples of either of these two monomials. Using that  $\{M + I_{\mathcal{X}_u} \mid M \in \Delta_{\prec}(I_{\mathcal{X}_u})\}$  is a basis for  $\mathbb{F}_{q^r}[x, y]/I_{\mathcal{X}_u}$

as an  $\mathbb{F}_{q^r}$ -vector space, we may assume that an arbitrary element of  $\text{ev}(\mathcal{M})$  is of the type  $\text{ev}(f)$ , where every monomial that appears in  $f$  is in  $\Delta_{\prec}(I_{\mathcal{X}_u}) = \Delta(x^{(q-1)u+1}, y^{q^{r-1}})$ . Take  $n := ((q-1)u+1)q^{r-1}$ . Since  $\text{ev}(f) \in \mathbb{F}_{q^r}^n$ , the element  $\text{ev}(f)$  depends on  $n$  symbols (over  $\mathbb{F}_{q^r}$ ) or, equivalently, on  $nr$  subsymbols (over  $\mathbb{F}_q$ ).

**Remark 6.1.** [27, Definition 2.30 and Theorem 2.40] Let  $\mathcal{B} = \{z_1, \dots, z_r\}$  be a basis of  $\mathbb{F}_{q^r}$  over  $\mathbb{F}_q$ . Then there exists a basis  $\{z'_1, \dots, z'_r\}$  of  $\mathbb{F}_{q^r}$  over  $\mathbb{F}_q$ , called the dual basis of  $\mathcal{B}$ , such that  $\text{Tr}(z_i z'_j) = \delta_{ij}$  is a delta function and for  $\alpha \in \mathbb{F}_{q^r}$ ,

$$\alpha = \sum_{i=1}^r \text{Tr}(\alpha z_i) z'_i.$$

Thus, determining  $\alpha$  is equivalent to finding  $\text{Tr}(\alpha z_i)$  for  $i \in \{1, \dots, r\}$ .

**Theorem 6.2.** Let  $\mathcal{M} \subseteq \Delta(x^{(q-1)u}, y^{q^{r-1}})$  be a monomial set that is closed under divisibility. There exists a repair scheme of  $\text{ev}(\mathcal{M})$  for one erasure with bandwidth at most

$$|\mathcal{X}_u| - 1 + (u-1)(r-1).$$

*Proof.* Take  $\mathcal{X}_u = \{P_1, \dots, P_n\}$  and let  $\text{ev}(f) = (f(P_1), \dots, f(P_n))$  be an element of  $\text{ev}(\mathcal{M})$ . Assume that the coordinate  $f(P^*)$  of  $\text{ev}(f)$  is erased, where  $P^* = (\alpha^*, \beta^*) \in \mathcal{X}_u$ . We define the following polynomials

$$p_i(y) = \frac{\text{Tr}(z_i(y - \beta^*))}{(y - \beta^*)} = z_i + z_i^q(y - \beta^*)^{q-1} + \dots + z_i^{q^{r-1}}(y - \beta^*)^{q^{r-1}-1}$$

for  $i \in \{1, \dots, r\}$ . We have  $\{1, y, \dots, y^{q^{r-1}-1}\} \subseteq \mathcal{M}^{\complement}$ , as  $\mathcal{M} \subseteq \Delta(x^{(q-1)u}, y^{q^{r-1}})$ . The element  $\beta \cdot (p_i(P_1), \dots, p_i(P_n))$  is in  $\text{ev}(\mathcal{M})^{\perp}$  for  $i \in \{1, \dots, r\}$  and  $\beta$  defined in Theorem 5.1. Therefore, we obtain the  $r$  equations

$$(1) \quad \beta_{P^*} p_i(P^*) f(P^*) = - \sum_{\mathcal{X}_u \setminus \{P^*\}} \beta_P p_i(P) f(P), \quad i \in \{1, \dots, r\}.$$

As  $p_i(P^*) = z_i$ , applying the trace function to both sides of previous equations and employing the linearity of the trace function, we obtain

$$\text{Tr}(z_i \beta_{P^*} f(P^*)) = - \sum_{\mathcal{X}_u \setminus \{P^*\}} \text{Tr}(\beta_P p_i(P) f(P)), \quad i \in \{1, \dots, r\}.$$

Define the set  $\Gamma = \{(\alpha, \beta) \in \mathcal{X}_u : \beta = \beta^*\}$ . We have that  $p_i(P) = z_i$  for  $P \in \Gamma$ . For  $P = (\alpha, \beta) \in \mathcal{X}_u \setminus \Gamma$ ,  $p_i(P) = \frac{\text{Tr}(z_i(\beta - \beta^*))}{(\beta - \beta^*)}$ . We have that for  $i \in \{1, \dots, r\}$ ,

$$\begin{aligned} \sum_{\mathcal{X}_u \setminus \{P^*\}} \text{Tr}(\beta_P p_i(P) f(P)) &= \sum_{\Gamma \setminus \{P^*\}} \text{Tr}(\beta_P p_i(P) f(P)) + \sum_{\mathcal{X}_u \setminus \Gamma} \text{Tr}(\beta_P p_i(P) f(P)) \\ &= \sum_{\Gamma \setminus \{P^*\}} \text{Tr}(\beta_P z_i f(P)) + \sum_{\mathcal{X}_u \setminus \Gamma} \text{Tr}\left(\beta_P \frac{\text{Tr}(z_i(\beta - \beta^*))}{(\beta - \beta^*)} f(P)\right) \\ &= \sum_{\Gamma \setminus \{P^*\}} \text{Tr}(\beta_P z_i f(P)) + \sum_{\mathcal{X}_u \setminus \Gamma} \text{Tr}(z_i(\beta - \beta^*)) \text{Tr}\left(\frac{\beta_P f(P)}{(\beta - \beta^*)}\right). \end{aligned}$$

The element  $\beta_{P^*} f(P^*)$ , and  $f(P^*)$  as a consequence, can be recovered from its  $r$  independent traces  $\text{Tr}(z_i \beta_{P^*} f(P^*))$  by Remark 6.1. The traces are obtained by downloading:

- For each  $P \in \Gamma \setminus \{P^*\}$ , the  $r$  subsymbols  $\text{Tr}(\beta_P z_1 f(P)), \dots, \text{Tr}(\beta_P z_r f(P))$ .
- For each  $P \in \mathcal{X}_u \setminus \Gamma$ , the subsymbol  $\text{Tr}\left(\frac{\beta_P f(P)}{(\beta - \beta^*)}\right)$ .

Hence, the bandwidth is  $b = r(|\Gamma| - 1) + |\mathcal{X}_u \setminus \Gamma| \leq r(u - 1) + |\mathcal{X}_u| - u = |\mathcal{X}_u| + (u - 1)(r - 1) - 1$ .  $\square$

Using a very similar proof one shows the existence of a repair scheme for  $\text{ev}(\mathcal{M})$ , for one erasure, with the same value for the bandwidth as above, if one assumes that  $\mathcal{M} \subseteq \Delta(x^{q^r}, y^{q^{r-1}-1})$ . Consequently, we obtain the following result for the norm-trace curve.

**Corollary 6.3.** *If  $\mathcal{M} \subseteq \Delta(x^{q^r}, y^{q^{r-1}-1})$  or  $\mathcal{M} \subseteq \Delta(x^{q^r-1}, y^{q^{r-1}})$  is a monomial set that is closed under divisibility, then there exists a repair scheme of the decreasing norm-trace code  $\text{ev}(\mathcal{M})$  for one erasure with bandwidth at most*

$$|\mathcal{X}_u| - 1 + \left(\frac{q^r - 1}{q - 1} - 1\right)(r - 1).$$

*In particular, there exists a repair scheme for the Hermitian decreasing code for one erasure with bandwidth at most*

$$q^3 + q - 1.$$

*Proof.* This is a consequence of Theorem 6.2 for the particular case when  $u = \frac{q^r - 1}{q - 1}$ . The Hermitian case is obtained when  $r = 2$ .  $\square$

Jin et al. introduced in [24] a repair scheme for single erasures of algebraic geometry codes. In particular, [24, Theorem 3.3] repairs a single erasure on one-point AG codes

defined over the curve  $\mathcal{X}_u$ , which can also be considered as monomial decreasing norm-trace codes [11]. Both schemes, [24, Theorem 3.3] and Theorem 6.2, have restrictions and can repair codes with up to a maximum dimension. One of the main advantages of Theorem 6.2 is the ability to repair single erasures on codes with a higher dimension that use the rational points of the curve  $\mathcal{X}_u$  as evaluation points. Indeed, consider the case where we want to repair an erasure on a monomial decreasing norm-trace code  $\text{ev}(\mathcal{M})$ . By Theorem 4.3, the length of the code  $\text{ev}(\mathcal{M})$  is  $n = |\mathcal{X}_u| = ((q-1)u+1)q^{r-1}$ . By the hypothesis of Theorem 6.2, the maximum dimension where the repair scheme can be applied is when  $\mathcal{M} = \Delta(x^{(q-1)u}, y^{q^{r-1}})$ , where the dimension is

$$(2) \quad k_{ev} := (q-1)uq^{r-1} = |\mathcal{X}_u| - q^{r-1}.$$

Now, consider the case where we want to repair an erasure on a one-point AG code over the curve  $\mathcal{X}_u$ . The curve  $\mathcal{X}_u$  has genus  $\mathfrak{g} := \frac{(u-1)(q^{r-1}-1)}{2}$  (see [32, Thm. 13]). In the context of [24, Theorem 3.3], the maximum dimension of the one-point AG code where the repair scheme can be applied is when  $m = |\mathcal{X}_u| - (q-1)(\mathfrak{g}+1)$ , which implies that the dimension would be

$$(3) \quad k_{AG} := m - \mathfrak{g} = |\mathcal{X}_u| - (q-1)(\mathfrak{g}+1) - \mathfrak{g} = |\mathcal{X}_u| - q(\mathfrak{g}-1) + 1.$$

**Example 6.4.** Taking  $u = \frac{q^r-1}{q-1}$ , we have that  $\mathfrak{g} := \frac{(u-1)(q^{r-1}-1)}{2} = \frac{\left(\frac{q^r-1}{q-1}-1\right)(q^{r-1}-1)}{2}$ . From Equation 3,  $k_{AG} = |\mathcal{X}_u| - q(\mathfrak{g}-1) + 1 = |\mathcal{X}_u| - \frac{1}{2}q^{2r-1} + \text{lower terms}$ . As  $k_{ev} = |\mathcal{X}_u| - q^{r-1}$  in Equation 2, we can see that there are values of  $q$  and  $r$  for which  $k_{eq} > k_{AG}$ .

**Example 6.5.** Taking  $u = \frac{q^r-1}{q-1}$ , we have that  $\mathfrak{g} := \frac{(u-1)(q^{r-1}-1)}{2} = \frac{\left(\frac{q^r-1}{q-1}-1\right)(q^{r-1}-1)}{2}$ . From Equation 3,  $k_{AG} = |\mathcal{X}_u| - q(\mathfrak{g}-1) + 1 = |\mathcal{X}_u| - \frac{1}{2}q^{2r-1} + \text{lower terms}$ . As  $k_{ev} = |\mathcal{X}_u| - q^{r-1}$  in Equation 2, we can see that there are values of  $q$  and  $r$  for which  $k_{eq} > k_{AG}$ .

We close this section by finding the maximum rate that a monomial decreasing norm-trace code  $\text{ev}(\mathcal{M})$  would have when the repair scheme of Theorem 6.2 can be applied. As  $|\mathcal{X}_u| = ((q-1)u+1)q^{r-1}$ , we can see that we can repair an erasure on a monomial decreasing norm-trace code  $\text{ev}(\mathcal{M})$  when  $\mathcal{M} \subseteq \Delta(x^{(q-1)u}, y^{q^{r-1}})$ . Thus, we have the following bound for the rate of the code:

$$(4) \quad \text{Rate}(\text{ev}(\mathcal{M})) \leq \frac{(q-1)uq^{r-1}}{((q-1)u+1)q^{r-1}} = 1 - \frac{1}{(q-1)u+1},$$

where the inequality is tight when  $\mathcal{M} = \Delta \left( x^{(q-1)u}, y^{q^{r-1}} \right)$ . In the particular case where  $u = \frac{q^r-1}{q-1}$ , the inequality in [4] becomes:

$$\text{Rate}(\text{ev}(\mathcal{M})) \leq 1 - \frac{1}{q^r}.$$

## CONCLUSION

This work focuses on decreasing norm-trace codes, which are evaluation codes defined by a set of monomials closed under divisibility and the rational points of the extended norm-trace curve. We used Gröbner basis theory and indicator functions to find the basic parameters of these codes: length, dimension, minimum distance, and dual code. By exploiting the basic parameters, we gave conditions over the set of monomials, so a decreasing norm-trace code is a self-orthogonal or a self-dual code. We presented a repair scheme for a single erasure on a decreasing norm-trace code that repairs codes with higher rates than the AG codes over the norm-trace curve.

## 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(7):3051–3073, 2009.
- [2] E. Assmus and J. Key. Affine and projective planes. *Discrete Mathematics*, 83(2):161–187, 1990.
- [3] T. Ball, E. Camps, H. Chimal-Dzul, D. Jaramillo-Velez, H. H. López, N. Nichols, M. Perkins, I. Soprunov, G. Vera-Martínez, and G. Whieldon. Coding theory package for Macaulay2. *Journal of Software for Algebra and Geometry*, 11:113–122, 2021.
- [4] M. Bardet, V. Dragoi, A. Otmani, and J.-P. Tillich. Algebraic properties of polar codes from a new polynomial formalism. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 230–234, 2016.
- [5] T. Becker and V. Weispfenning. *Gröbner Bases - A computational approach to commutative algebra*, volume 2nd. pr. Berlin, Germany: Springer Verlag, 1998.
- [6] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.
- [7] M. Bras-Amorós and M. E. O’Sullivan. Extended norm-trace codes with optimized correction capability. In S. Boztaş and H.-F. F. Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 337–346, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
- [8] M. Bras-Amorós and M. E. O’Sullivan. Duality for some families of correction capability optimized evaluation codes. *Advances in Mathematics of Communications*, 2(1):15–33, 2008.
- [9] B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Dissertation an dem Math. Inst. der Universität von Innsbruck, 1965.
- [10] E. Camps, H. H. López, G. L. Matthews, and E. Sarmiento. Polar decreasing monomial-cartesian codes. *IEEE Transactions on Information Theory*, 67(6):3664–3674, 2021.

- [11] E. Camps Moreno, E. Martínez-Moro, and E. Sarmiento Rosales. Vardøhus codes: Polar codes based on castle curves kernels. *IEEE Transactions on Information Theory*, 66(2):1007–1022, 2020.
- [12] C. Carvalho. Gröbner bases methods on coding theory. In *Algebra for Secure and Reliable Communication Modeling*, volume 642, pages 73–86. Contemporary Mathematics, 2015.
- [13] J. L. D. Cox and D. O’Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics, Springer-Verlag, 2008.
- [14] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.
- [15] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.
- [16] O. Geil. On codes from norm-trace curves. *Finite Fields and Their Applications*, 9(3):351–371, 2003.
- [17] O. Geil and T. Høholdt. Footprints or generalized bezout’s theorem. *IEEE Transactions on Information Theory*, 46(2):635–641, 2000.
- [18] S. R. Ghorpade. A note on Nullstellensatz over finite fields. *Contemp. Math.*, 738:23–32, 2019.
- [19] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. <http://www.codetables.de>.
- [20] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.
- [21] J. Harris. *Algebraic Geometry. A first course*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1992.
- [22] T. Høholdt, J. van Lint, and R. Pellikaan. *Algebraic Geometry Codes*, volume 1, pages 871–961. Elsevier, Amsterdam, 1998.
- [23] H. Janwa and F. L. Piñero. On parameters of subfield subcodes of extended norm-trace codes. *Advances in Mathematics of Communications*, 11(2):379–388, 2017.
- [24] L. Jin, Y. Luo, and C. Xing. Repairing algebraic geometry codes. *IEEE Transactions on Information Theory*, 64(2):900–908, 2018.
- [25] S. J. K. Guenda and T. A. Gulliver. Constructions of good entanglement assisted quantum error correcting codes. *Designs, Codes and Cryptography*, 86(1):121–136, 2018.
- [26] B. Kim. Quantum codes from one-point codes on norm-trace curves. *Cryptography Commun.*, 14(5):1179–1188, sep 2022.
- [27] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, 2 edition, 1994.
- [28] H. H. López, G. L. Matthews, and D. Valvo. Erasures repair for decreasing monomial-cartesian and augmented reed-muller codes of high rate. *IEEE Transactions on Information Theory*, 2021.
- [29] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Designs, Codes and Cryptography*, 89(7):1367–1403, 2021.
- [30] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *arXiv:2012.10016v2*, <https://arxiv.org/abs/2012.10016v2>, 2023.
- [31] G. L. Matthews and A. W. Murphy. Norm-trace-lifted codes over binary fields. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 3079–3084, 2022.
- [32] S. Miura. Algebraic geometric codes on certain plane curves. *Electronics and Communications in Japan, Part 3*, 76(12):1–13, 2003.

- [33] C. Munuera, G. C. Tizziotti, and F. Torres. Two-point codes on norm-trace curves. In Á. Barbero, editor, *Coding Theory and Applications*, pages 128–136, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
- [34] S. Srinivasan, U. Tripathi, and S. Venkitesh. Decoding variants of Reed-Muller codes over finite grids. *ACM Trans. Comput. Theory*, 12(4), Nov. 2020.
- [35] R. H. Villarreal. *Monomial Algebras*. Monographs and Research Notes in Mathematics, 2015.