DECREASING NORM-TRACE CODES

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

Abstract. This paper introduces 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. As a particular case, 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, minimum distance, and the dual code. 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 in Information Theory **64** (2), 900-908, 2018) for the one-point AG codes over the extended norm-trace curve.

1. Introduction

Decreasing monomial codes, which are evaluation codes where 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 classical families of Reed-Solomon and Reed-Muller codes can be considered decreasing monomial codes and have amply motivated the study of decreasing codes. Decreasing monomial-Cartesian codes, also known as variants of Reed-Muller codes over finite grids, are slightly more general families than Reed-Muller codes that have been studied because of their applications to certain symmetric channels [9], distributed storage systems [26], and efficient decoding algorithms [31]. In this paper, we introduce decreasing codes from curves, focusing on the extended norm-trace curve.

Let $\mathbb{F}_{q^r}$ be a finite field with q^r elements and u 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

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

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

The first author was partially supported by FAPEMIG APQ-00864-21. The second author was partially supported by NSF DMS-2201094. The third author was partially supported by NSF DMS-2201075 and the Commonwealth Cyber Initiative.

We introduce in this work 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 points in $\mathcal{X}_u = \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_{q^r}^2$. The *evaluation map*, denoted ev, is the $\mathbb{F}_{q^r}$-linear map given by

$$\begin{array}{rccc} \mathrm{ev}\colon & \mathbb{F}_{q^r}[x,y] & \to & \mathbb{F}_{q^r}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)) \,. \end{array}$$

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 $\mathcal{L} = \mathbb{F}_{q^r}\mathcal{M}$ be the $\mathbb{F}_{q^r}$-subspace of $\mathbb{F}_{q^r}[x,y]$ generated by the set $\mathcal{M}$. The image of $\mathcal{L}$ under the evaluation map, denoted by $\mathrm{ev}(\mathcal{M})$, is called a *decreasing norm-trace code*. We can see that the extended norm-trace codes introduced and recently studied in [7] and [21] are particular instances of decreasing norm-trace codes. Even more, we check later that the family of decreasing norm-trace codes contains, in 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 give 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 the 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 show that these decreasing codes generalize the one-point AG codes over the norm-trace curve (Remark 4.2) and determine their basic parameters, such as the length, dimension, and minimum distance (Theorem 4.5).

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 [23]. 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 in Section 6.

References for vanishing ideals and related algebraic concepts used in this work are [12, 13, 19, 32].

2. Preliminaries

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

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

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

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

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, 15, 24, 28, 30]. 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, 21].

Results from Gröbner bases theory have been used in coding theory for some time to determine parameters of codes (see, e.g., [15, 16, 11]). We now recall important concepts and results from this theory.

Let $\mathcal{M}$ be the set of monomials of $\mathbb{F}_{q^r}[x_1, \ldots, x_m]$. 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 $\mathbb{F}_{q^r}[x_1, \ldots, x_m]$. The greatest monomial which appears in f is called the *leading monomial* of f, denoted by $\mathrm{lm}(f)$. Given an ideal $I \subseteq \mathbb{F}_{q^r}[x_1, \ldots, x_m]$, a *Gröbner basis* for I is a set $\{f_1, \ldots, f_s\} \subseteq I$ such that for every polynomial $f \in I \setminus \{0\}$, we have that $\mathrm{lm}(f)$ is a multiple of $\mathrm{lm}(f_i)$ for some $i \in \{1, \ldots, s\}$. The Gröbner basis concept was introduced in the Ph.D. thesis of Bruno Buchberger (see [8]) in which the author proves that if $\{f_1, \ldots, f_s\}$ is a Gröbner basis for I then $I = (f_1, \ldots, f_s)$, and that every ideal admits a Gröbner basis (w.r.t. a fixed monomial order).

Let $\{f_1, \ldots, f_s\}$ be a Gröbner basis for I. The *footprint* of I is the set $\Delta_\prec(I)$ of monomials which are not multiples of $\mathrm{lm}(f_i)$, for all $i = 1, \ldots, n$. One of the main results in Buchberger's thesis states that the set of classes $\{M + I \mid M \in \Delta_\prec(I)\} \subseteq \mathbb{F}_{q^r}[x_1, \ldots, x_m]/I$ is a basis for $\mathbb{F}_{q^r}[x_1, \ldots, x_m]/I$ 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, from [5, Prop. 8.14], $I_{\mathcal{X}_u}$ is a radical ideal. From [17, Thm. 2.3], it follows that $I_{\mathcal{X}_u}$ is the ideal of all polynomials which vanish on $\mathcal{X}_u$. $\square$

The following result is a particular case of [21, Theorem 21]. We add 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 lexicographic order with $x \prec y$. Moreover, $\mid \mathcal{X}_u \mid= q^{r-1}((q-1)u+1)$. 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 lexicographic order with $x \prec y$, and $\mid \mathcal{X} \mid= q^{2r-1}$.*

Proof. Let (α, β) 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

$$\left(x^{(q-1)u(v-1)}+x^{(q-1)u(v-2)}+\cdots+x^{(q-1)u}+1\right)\left(x^{(q-1)u+1}-x\right)=x^{q^r}-x$$

and

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

Since the leading monomials $\operatorname{lm}(Tr(y))=y^{q^{r-1}}$ and $\operatorname{lm}(x^{(q-1)u+1}-x)=x^{(q-1)u+1}$ are coprime, $\{Tr(y)-x^u, x^{(q-1)u+1}-x\}$ is a Gröbner basis for $I_{\mathcal{X}_u}$ according to [12, Prop. 4, p. 104]. Since $I_{\mathcal{X}_u}$ is a radical ideal and $\mathbb{F}_{q^r}$ is a perfect field, $\mid \mathcal{X}_u \mid=\mid \Delta_{\prec}(I_{\mathcal{X}_u}) \mid$ [5, Thm. 8.32]. □

3. Standard indicator functions

Some of the properties of the decreasing evaluation codes depend on the indicator functions of the curve $\mathcal{X}_u$. Take $n :=\mid \mathcal{X}_u \mid$. One may show (see [14] or [11, Prop. 3.7]) that the following linear transformation is an isomorphism

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

So, for each $P\in\mathcal{X}_u$, there exists an 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, 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.

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

Proof. From Theorem 2.2, we know that if $(\alpha,\beta)\in\mathcal{X}_u$, then α is a root of $x^{(q-1)u+1}-x$. 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 α, 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 $x^{(q-1)u+1}-x=x\prod_{\gamma\in\mathbb{F}_q^*}(x^u-\gamma)$. For every $\gamma\in\mathbb{F}_q$, it is well known that there are q^{r-1} elements β such that $Tr(\beta) = \alpha^u$. This shows that $A_\gamma \subseteq \mathcal{X}_u$ for all $\gamma \in \mathbb{F}_q$ and that $\mid A_0 \mid = q^{r-1}$ and $\mid A_\gamma \mid = uq^{r-1}$ 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*

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

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 Theorem 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 β' 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 $\beta = \beta_1, \ldots, \beta_{q^{r-1}} \in \mathbb{F}_{q^r}$ 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 $\alpha = \alpha_1, \ldots, \alpha_{u(q-1)+1}$ 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 $\mathrm{char}(\mathbb{F}_q)$. Hence $u \neq 0$ in $\mathbb{F}_q$. $\square$

4. Parameters of decreasing norm-trace codes

This section defines and computes the basic parameters of a new family of evaluation codes called decreasing norm-trace codes. Consider the *evaluation map*, denoted ev, is the $\mathbb{F}_{q^r}$-linear map given by

$$\begin{array}{rccc} \mathrm{ev}\colon & \mathbb{F}_{q^r}[x,y] & \to & \mathbb{F}_{q^r}^n \\ & f & \mapsto & (f(P_1),\ldots,f(P_n)) \end{array}$$

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

Definition 4.1. A *decreasing norm-trace code* is an evaluation code $\mathrm{ev}(\mathcal{M})$ 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 $M' \in \mathcal{M}$.

Remark 4.2. The family of decreasing norm-trace codes contains, as a particular case, the family of one-point geometric Goppa codes over the norm-trace. Indeed, define $\mathcal{L}_s := \left\{ x^i y^j \mid i q^{r-1} + j \frac{q^r-1}{q-1} \leq s \right\}$. It is straightforward to check that $\mathcal{L}_s$ is closed under divisibility. As the one-point geometric Goppa codes over the norm-trace are precisely $\mathrm{ev}\left(\mathcal{L}_s\right)$ (see, e.g. [15, 20]), we obtain the result.

The extended norm-trace codes introduced and studied in [7] and [21] are also particular instances of decreasing norm-trace codes.

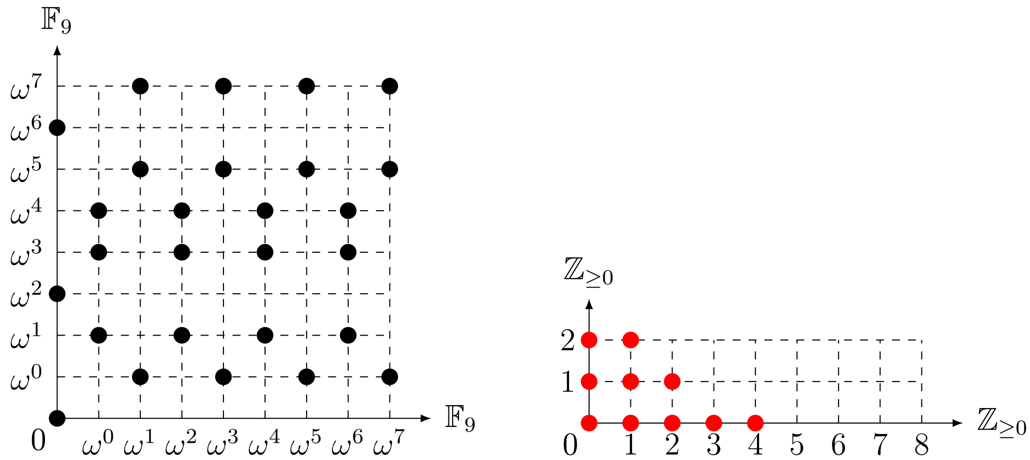
Example 4.3. Take $q = 3$ and $r = 2$. Figure 1 (a) shows the points of the norm-trace curve $\mathcal{X}$. Let $\mathcal{M}$ be the set of monomials in $\mathbb{F}_{q^r}[x,y]$ whose exponents are the points in Figure 1 (b). Note that $\mathcal{M}$ is closed under divisibility. Using the coding theory package [3] for Macaulay2 [18] and Magma [6], we obtain that $\mathrm{ev}(\mathcal{M})$ is a $[27, 10, 15]$ decreasing norm-trace code over $\mathbb{F}_9$.

Let $\Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$ be the set of monomials that are not multiples of either of these two monomials.

Lemma 4.4. *Let* $\mathrm{ev}(\mathcal{M})$ *be a decreasing Goppa norm-trace code. There exists a monomial set* $\mathcal{M}' \subseteq \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$ *such that* $\mathrm{ev}(\mathcal{M}) = \mathrm{ev}(\mathcal{M}')$.

Proof. The kernel of ev is the ideal $I_{\mathcal{X}_u} = (Tr(y) - x^u, x^{q^r} - x, y^{q^r} - y)$ by Lemma 2.1. Even more, 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 graded lexicographic order with $x \prec y$ by Theorem 2.2.

Note the evaluation map induces an isomorphism of $\mathbb{F}_{q^r}$-linear spaces between $\mathbb{F}_{q^r}[x,y]/I_{\mathcal{X}_u}$ and $\mathbb{F}_{q^r}^n$. So, the image of a monomial $x^a y^b \in \mathcal{M}$ under the function ev equals the image of its reminder $x^i y^j$ modulo $I_{\mathcal{X}_u}$, which satisfies $i < (q-1)u+1$ and $j < q^{r-1}$. $\square$



(a) Evaluation points (b) Evaluation monomials

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 $\mathrm{ev}(\mathcal{M})$ is an $[27, 10, 15]$ decreasing norm-trace code over $\mathbb{F}_9$.

We assume from now on that $\mathcal{M} \subseteq \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$ by Lemma 4.4.

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

Theorem 4.5. *The decreasing norm-trace code* $\mathrm{ev}(\mathcal{M})$ *has the following basic parameters.*

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

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

Proof. (1) It is a consequence of Theorem 2.2. (2) It follows from Lemma 4.4 and its proof. (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 $V(I_{\mathcal{X}_u} + (f))$. Since $I_{\mathcal{X}_u} + (f)$ is a radical ideal (see [5, Prop. 8.14]), [5, Thm. 8.32] implies that $\mid V(I_{\mathcal{X}_u} + (f)) \mid= \Delta_\prec(I_{\mathcal{X}_u} + (f))$. Let $x^a y^b$ be the leading monomial of f and let $\Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}, x^a y^b\right)$ 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

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

On the other hand, from [16, Proposition 4]), we get that $\mid V(I_{\mathcal{X}_u} + (f)) \mid \leq aq^{r-1} + bu$.

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 $\gamma \in fq^*$, the number of distinct elements of $\mathbb{F}_{q^r}$, which appear as the first entry of points in A_γ 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 $\alpha_1, \ldots, \alpha_a \in \mathbb{F}_{q^r}$ such that for all $i = 1, \ldots, a$ 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 $\beta_1, \ldots, \beta_b \in \mathbb{F}_{q^r}$ be distinct elements such that $Tr(\beta_j) = \gamma$ for all $j = 1, \ldots, b$. Let $g(x,y) = \prod_{i=1}^{a}(x-\alpha_i) \cdot \prod_{j=1}^{b}(y-\beta_j)$. For every $i = 1, \ldots, a$, there exist q^{r-1} points in $\mathcal{X}_u$ of the form (α_i, β), none of them in A_γ. For every $j = 1, \ldots, b$, there exist u points of $\mathcal{X}_u$ of the form (α, β_j), all of them in A_γ. Hence, $\mid V(I_{\mathcal{X}_u} + (g)) \mid = aq^{r-1} + bu$.

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 $\beta_1, \ldots, \beta_b \in \mathbb{F}_{q^r}$ to be distinct elements such that $Tr(\beta_j) = \gamma$ for all $j = 1, \ldots, b$. Let $\alpha_1, \ldots, \alpha_a \in \mathbb{F}_{q^r}$ be distinct elements such that for all $i = 1, \ldots, a$ 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 α_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 $\alpha \in \{\alpha_1, \ldots, \alpha_a\}$ we have q^{r-1} elements $(\alpha, \beta) \in \mathcal{X}_u$, which are also zeros of h. For each $\beta \in \{\beta_1, \ldots, \beta_b\}$ 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 $\mid V(I_{\mathcal{X}_u} + (h)) \mid = aq^{r-1} + b((q-1)u+1-a)$.

If $b = 0$, then $aq^{r-1} + ((q-1)u+1-a)b = aq^{r-1} + bu$. Taking $\alpha_1, \ldots, \alpha_a \in \mathbb{F}_{q^r}$ such that for all $i = 1, \ldots, a$, 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 $\mid V(I_{\mathcal{X}_u} + (t)) \mid = aq^{r-1}$.

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 $\mid V(I_{\mathcal{X}_u} + (f)) \mid$ 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 4.6. 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 4.5, $\mathrm{ev}(\mathcal{M})$ is a $[32, 12, 12]$ decreasing norm-trace code over $\mathbb{F}_{16}$.

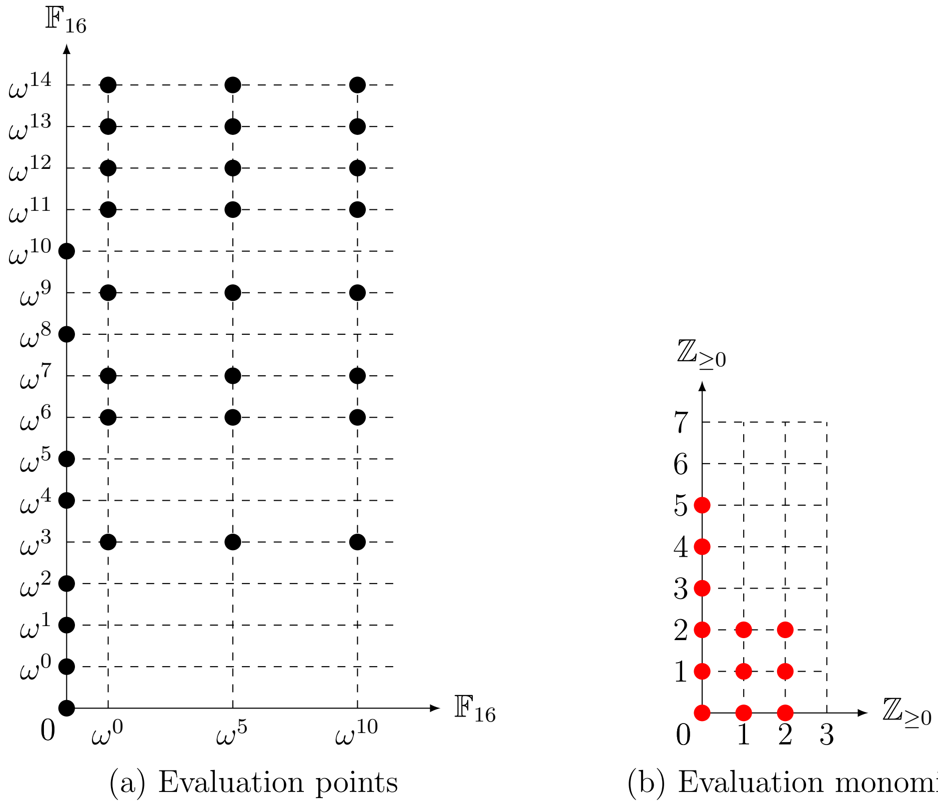


FIGURE 2. Take $q = 2$, $r = 4$, and $u = 3$. (a) Shows the points of the norm-trace curve $\mathcal{X}_u : x^3 = y^8 + y^4 + y^2 + y$. Let $\mathcal{M}$ be the set of monomials whose exponents are the points in (b). The evaluation code $\mathrm{ev}(\mathcal{M})$ is an $[32, 12, 12]$ decreasing norm-trace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

One may notice that

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

meaning decreasing norm-trace codes have a gap of

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

to the Singleton Bound $k + d \leq n + 1$. One may compare this with algebraic geometry codes which see a gap of at most g, where g denotes the genus of the curve.

Note that Theorem 4.5 allows one 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 [15], where such codes are denoted by $E(s)$. Moreover, the improved codes $\tilde{E}(s)$, which appear in [15], are also decreasing norm-trace codes, and our results recover those of [15] regarding their parameters.

5. Dual of decreasing norm-trace codes

This section proves that the dual of a decreasing norm-trace code is monomially equivalent to a decreasing norm-trace code. Even more, 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 *monomially equivalent* if there is $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_{q^r}^n$ such that $\beta_i \neq 0$ for all i and $C_2 = \boldsymbol{\beta} \cdot C_1 := \{\beta \cdot c \mid c \in C_1\}$, where $\boldsymbol{\beta} \cdot c := (\beta_1 c_1, \ldots, \beta_n c_n)$ for $c = (c_1, \ldots, c_n) \in C_1$.

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 *monomially equivalent* if there is $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_{q^r}^n$ such that $\beta_i \neq 0$ for all i and $C_2 = \boldsymbol{\beta} \cdot C_1 := \{\beta \cdot c \mid c \in C_1\}$, where $\boldsymbol{\beta} \cdot c := (\beta_1 c_1, \ldots, \beta_n c_n)$ for $c = (c_1, \ldots, c_n) \in C_1$.

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

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

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

$$\operatorname{ev}(\mathcal{M})^\perp = \boldsymbol{\beta} \cdot \operatorname{ev}\left(\mathcal{M}^\complement\right),$$

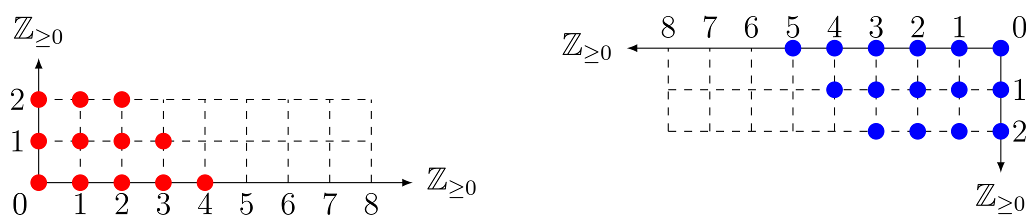
where $\beta_i := \begin{cases} u^{-1} & \text{if the } x\text{-coordinate of } P_i \text{ is nonzero} \\ 1 & \text{otherwise.} \end{cases}$

Proof. The result is trivial when $\mathcal{M} = \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$. For the case $\mathcal{M} \subsetneq \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$, we base our proof on [27, Theorem 5.4]. By Lemma 2.1, $I_{\mathcal{X}_u}$ is the vanishing ideal of $\mathcal{X}_u$. Even more, $\Delta_\prec(I_{\mathcal{X}_u}) = \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$ by Theorem 2.2. The monomial $x^{(q-1)u} y^{q^{r-1}-1}$ is the largest monomial in $\Delta_\prec(I_{\mathcal{X}_u})$ and it is essential by Theorem 3.2, meaning that it appears in each indicator function for every point in $\mathcal{X}_u$. Note that

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

which implies that [27, Theorem 5.4] (1) is valid. As $\mathcal{M}$ is closed under divisibility and $\mathcal{M} \subsetneq \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$, given $x^a y^b \in \mathcal{M}$ and $\frac{x^{(q-1)u} y^{q^{r-1}-1}}{x^i y^j} \in \mathcal{M}^{\complement}$, we have that either $i > a$ or $j > b$. Thus, $x^{(q-1)u} y^{q^{r-1}-1}$ cannot divide the product $\left(x^a y^b\right)\left(\frac{x^{(q-1)u} y^{q^{r-1}-1}}{x^i y^j}\right)$. This implies that [27, Theorem 5.4] (2) is valid. $\square$

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 $\mathcal{M}^{\complement}$, whose exponents are the points in Figure 3 (b). By Theorem 5.1, the dual code $\mathrm{ev}(\mathcal{M})^{\perp}$ is monomially equivalent to the code $\mathrm{ev}\left(\mathcal{M}^{\complement}\right)$.



(a) Monomials of degree at most 4. (b) Complement of (a) on $\mathcal{X}$.

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 $\mathcal{M}^{\complement}$, the complement of $\mathcal{M}$ on $\mathcal{X}$. By Theorem 5.1, the dual code $\mathrm{ev}(\mathcal{M})^{\perp}$ is monomially equivalent to the code $\mathrm{ev}\left(\mathcal{M}^{\complement}\right)$.

Recall the hull of a code C is $\mathrm{Hull}(C) := C \cap C^{\perp}$. 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 $\mathcal{X}_u = \{P_1, \ldots, P_n\}$ and let $\mathrm{ev}(\mathcal{M})$ be a decreasing norm-trace code. If the equation $x^2 = u$ has a solution α in $\mathbb{F}_{q^r}$, then*

$$\mathrm{Hull}(\boldsymbol{\lambda} \cdot \mathrm{ev}(\mathcal{M})) = \boldsymbol{\lambda} \cdot \mathrm{ev}\left(\mathcal{M} \cap \mathcal{M}^{\complement}\right),$$

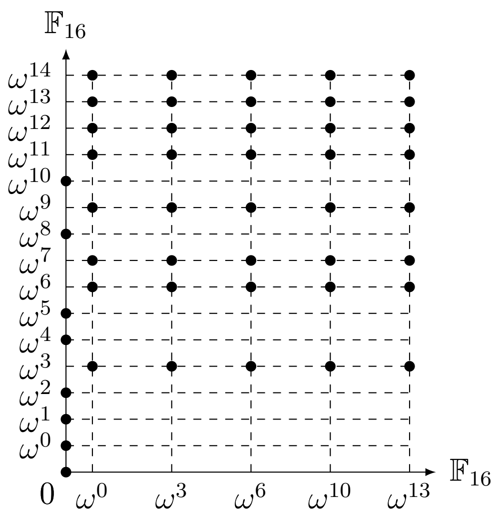
where $\lambda_i := \begin{cases} \alpha^{-1} & \text{if the } x\text{-coordinate of } P_i \text{ is nonzero} \\ 1 & \text{otherwise.} \end{cases}$

Proof. Denote by $\boldsymbol{\lambda}^{-1}$ the vector whose entries are λ_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, $(\boldsymbol{\lambda} \cdot \mathrm{ev}(\mathcal{M}))^{\perp} = \boldsymbol{\lambda}^{-1} \cdot \mathrm{ev}(\mathcal{M})^{\perp} = \boldsymbol{\lambda}^{-1}\boldsymbol{\beta} \cdot \mathrm{ev}\left(\mathcal{M}^{\complement}\right) = \boldsymbol{\lambda} \cdot \mathrm{ev}\left(\mathcal{M}^{\complement}\right)$. $\square$

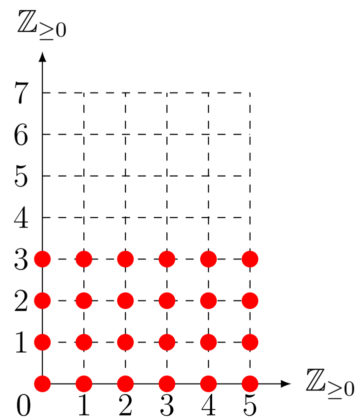
Corollary 5.4. *Assume $\mathcal{X}_u = \{P_1, \ldots, P_n\}$ and the equation $x^2 = u$ has a solution α in $\mathbb{F}_{q^r}$. If $\mathcal{M} \subseteq \mathcal{M}^{\complement}$, then $\boldsymbol{\lambda} \cdot \mathrm{ev}(\mathcal{M})$ is a self-dual dual code, where λ_i is as in Theorem 5.3. If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

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

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 $\mathrm{Hull}(\mathrm{ev}(\mathcal{M})) = \mathrm{ev}\left(\mathcal{M} \cap \mathcal{M}^{\complement}\right) = \mathrm{ev}(\mathcal{M})$ by Theorem 5.3. Thus, $\mathrm{ev}(\mathcal{M})$ is a self-dual code by Corollary 5.4.



(a) Evaluation points



(b) Evaluation monomials

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 $\mathrm{ev}(\mathcal{M})$ 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 $\dfrac{b}{nr}$ is called *bandwidth rate.*

Recall that $\Delta\left(x^i, y^j\right)$ denotes the set of monomials which are not multiples of either of these two monomials. From Lemma 4.4, we may assume that an arbitrary element of $\mathrm{ev}(\mathcal{M})$ is of the type $\mathrm{ev}(f)$, where every monomial which appears in f is in $\Delta_{\prec}(I_{\mathcal{X}_u}) = \Delta\left(x^{(q-1)u+1}, y^{q^{r-1}}\right)$. Take $n := ((q-1)u+1)q^{r-1}$. Since $\mathrm{ev}(f) \in \mathbb{F}_{q^r}^n$, the element $\mathrm{ev}(f)$ depends on n symbols (over $\mathbb{F}_{q^r}$) or, equivalently, on nr subsymbols (over $\mathbb{F}_q$).

Remark 6.1. [25, Definition 2.30 and Theorem 2.40] Let $\mathcal{B} = \{z_1, \ldots, z_r\}$ be a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. Then there exists a basis $\{z_1', \ldots, z_r'\}$ of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$, called the dual basis of $\mathcal{B}$ such that $Tr(z_i z_j') = \delta_{ij}$ is a delta function and for $\alpha \in \mathbb{F}_{q^r}$,

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

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

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

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

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

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

for $i \in [r]$. We have that $\{1, y, \ldots, y^{q^{r-1}-1}\} \subseteq \mathcal{M}^{\complement}$ as $\mathcal{M} \subseteq \Delta\left(x^{(q-1)u}, y^{q^{r-1}}\right)$. The element $\boldsymbol{\beta} \cdot (p_i(P_1), \ldots, p_i(P_n))$ is in $\mathrm{ev}\left(\mathcal{M}\right)^{\perp}$ for $i \in [r]$ and $\boldsymbol{\beta}$ defined in Theorem 5.1. We, therefore, obtain the r equations

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

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

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

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 $P = (\alpha,\beta) \in \mathcal{X}_u \setminus \Gamma,\ p_i(P) = \dfrac{Tr(z_i(\beta-\beta^*))}{(\beta-\beta^*)}$. We obtain that for $i \in [r]$

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

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

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

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

Consequently, we obtain the following result for the norm-trace curve.

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

$$|\,\mathcal{X}\,| -1 + (r-1)(q^r-1).$$

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

$$q^3+q^2-2.$$

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 $r=2$. ☐

Jin et al. introduced in [22] a repair scheme for single erasures of algebraic geometry codes. In particular, [22, 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 [10]. Both schemes, [22, 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 $\mathrm{ev}(\mathcal{M})$. By Theorem 4.5, the length of the code $\mathrm{ev}(\mathcal{M})$ 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 $\mathcal{M} = \Delta\left(x^{(q-1)u}, y^{q^{r-1}}\right)$, where the dimension is

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

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 [29, Thm. 13]). In the context of [22, 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

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

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 $k_{eq} > k_{AG}$.

We close this section by finding the maximum rate that a monomial decreasing norm-trace code $\mathrm{ev}(\mathcal{M})$ 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 $\mathrm{ev}(\mathcal{M})$ when $\mathcal{M} \subseteq \Delta\left(x^{(q-1)u}, y^{q^{r-1}}\right)$. Thus, we have the following bound for the rate of the code:

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

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:

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

Conclusion

This work introduced 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*, to appear.

[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] B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Dissertation an dem Math. Inst. der Universität von Innsbruck, 1965.

[9] 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.

[10] 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.

[11] C. Carvalho. Gröbner bases methods on coding theory. In *Algebra for Secure and Reliable Communication Modeling*, volume 642, pages 73–86. Contemporary Mathematics, 2015.

[12] J. L. D. Cox and D. O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics, Springer-Verlag, 2008.

[13] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry.* Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.

[14] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.

[15] O. Geil. On codes from norm-trace curves. *Finite Fields and Their Applications*, 9(3):351–371, 2003.

[16] O. Geil and T. Høholdt. Footprints or generalized bezout's theorem. *IEEE Transactions on Information Theory*, 46(2):635–641, 2000.

[17] S. R. Ghorpade. A note on Nullstellensatz over finite fields. *Contemp. Math.*, 738:23–32, 2019.

[18] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.

[19] J. Harris. *Algebraic Geometry. A first course*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[20] T. Høholdt, J. van Lint, and R. Pellikaan. *Algebraic Geometry Codes*, volume 1, pages 871–961. Elsevier, Amsterdam, 1998.

[21] 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.

[22] L. Jin, Y. Luo, and C. Xing. Repairing algebraic geometry codes. *IEEE Transactions on Information Theory*, 64(2):900–908, 2018.

[23] 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.

[24] B. Kim. Quantum codes from one-point codes on norm-trace curves. *Cryptography Commun.*, 14(5):1179–1188, sep 2022.

[25] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, 2 edition, 1994.

[26] 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.

[27] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Designs, Codes and Cryptography*, 89(7):1367–1403, 2021.

[28] 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.

[29] S. Miura. Algebraic geometric codes on certain plane curves. *Electronics and Communications in Japan, Part 3*, 76(12):1–13, 2003.

[30] 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.

[31] S. Srinivasan, U. Tripathi, and S. Venkitesh. Decoding variants of Reed-Muller codes over finite grids. *ACM Trans. Comput. Theory*, 12(4), Nov. 2020.

[32] R. H. Villarreal. *Monomial Algebras*. Monographs and Research Notes in Mathematics, 2015.

(Cícero Carvalho) Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, MG Brazil

Email address: cicero@ufu.br

(Hiram H. López) Department of Mathematics, Cleveland State University, Cleveland, OH USA

Email address: h.lopezvaldez@csuohio.edu

(Gretchen L. Matthews) Department of Mathematics, Virginia Tech, Blacksburg, VA USA

Email address: gmatthews@vt.edu