AALBORG UNIVERSITY

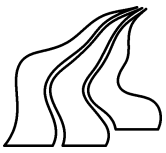
On Puncturing of Codes from Norm-Trace Curves

by

Henning E. Andersen

R-2005-10 March 2005

Department of Mathematical Sciences
Aalborg University
Fredrik Bajers Vej 7 G ▪ DK - 9220 Aalborg Øst ▪ Denmark
Phone: +45 96 35 80 80 ▪ Telefax: +45 98 15 81 29
URL: http://www.math.aau.dk



ISSN 1399–2503 ▪ On-line version ISSN 1601–7811

On Puncturing of Codes from Norm-Trace Curves

Henning E. Andersen

Department of Mathematical Sciences
Aalborg University
Fredrik Bajers Vej 7 G
9220 Aalborg East, Denmark

henning@math.aau.dk

Abstract: *Constructing new codes from existing ones by puncturing is in this paper viewed in the context of order domains R where puncturing can be seen as redefinition of the evaluation map $\varphi : R \to \mathbb{F}_q^n$. The order domains considered her are on the form $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ where redefinition can be done by adding one or more polynomials to the basis of the defining ideal I to form a new ideal J in such a way that the number of points in the variety $\mathbb{V}(I)$ is reduced by t to form $\mathbb{V}(J)$ and puncturing in t coordinates is achieved. An explicit construction of such polynomials is given in the case of codes defined by Norm-Trace curves and examples are given of both evaluation codes and dual codes. Finally, it is demonstrated that the improvement in minimum distance can be significant when comparing to the lower bound obtained by ordinary puncturing.*

Key words: *Gröbner basis, Footprint, Evaluation codes, Dual codes, Puncturing, Minimum distance, Norm, Trace, Order domain.*

1 Introduction

Constructing codes from existing ones is not a new idea and over the years several ways of doing so has been developed. One such construction is by means of puncturing. Puncturing an (n, M, d) code t times yields an $(n-t, M, \geqslant d-t)$ code where the parameter $d - t$ is a lower bound on the minimum distance (see [1, p. 28]).

However, it is not clear how to select which t coordinates to erase on an existing code to get the best result or whether an optimal strategy for making such a selection exists for a given code and a given value t. The general bound given above is not tight which will be shown by an example.

Here we consider codes from Norm-Trace curves[1] which were studied in detail in [3]. Here we use nothing but order domains and simple Gröbner basis theory for code construction and the methods developed in [4, 5, 6, 7, 8] for estimating the minimum distances of the codes.

The notion of an order domain was introduced in [4, 6] to make understanding of a large class of algebraic geometry codes easier and to give the code construction presented in [7, 8][2] a simpler foundation. Many of the results in [4, 6, 9] were found independently by Miura and published in Japanese in [10, 11, 12][3] (See [14] for details).

By [15] every finitely generated order domain can be represented as a factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, where $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is an ideal on a special form. Using such an order domain and the usual evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_q^n$ we define $\tilde{E}$ codes as a linear subspace of $\mathbb{F}_q^n$ spanned by the image of selected elements from $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ under φ and $\tilde{C}$ codes as the dual of such an image under φ (These are the improved $\tilde{E}$ codes from [5] and the improved $\tilde{C}$ codes from [4, 8]).

In this setting puncturing a code can be done by reducing the dimension of the corresponding factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as a vector space over $\mathbb{F}_q$ by adding extra polynomials to the basis of the defining ideal I to define an new ideal J. This corresponds to redefining the evaluation map by leaving out a number of points from the variety $\mathbb{V}(I)$, since $I \subset J$ has the consequence that $\mathbb{V}(J) \subset \mathbb{V}(I)$ (See [16]).

Leaving out t points from the variety $\mathbb{V}(I)$ can be done in several ways by adding different sets of polynomials to the basis of the ideal I to form the ideal J such that $\#\mathbb{V}(J) = \#\mathbb{V}(I) - t$. The evaluation map φ is still a morphism using $\mathbb{V}(J)$ and the methods developed in [4, 5, 8] enables us to estimate the minimum distances of the codes constructed by using the variety $\mathbb{V}(J)$. This in turn allows us to choose the set of polynomials added to the basis of I (i.e. choose the ideal J) which has the smallest cost in terms of loss in minimum distance for a given integer t and a given code rate.

The main result in this paper is the fact that for any positive value $t < n$ it is possible to construct a set of polynomials $\{g_1, g_2, \ldots, g_s\}$ such that a code of length $n-t$ is obtained by using the ideal $J = I + \langle g_1, g_2, \ldots, g_s \rangle$ and the affine variety $\mathbb{V}(J)$. Furthermore, the proof given here is constructive and examples of such constructions are included.

The paper is organized as follows: In Section 2 a short presentation of order domains is given, Section 3 is an introduction to the necessary Gröbner basis theory used to

[1] Norm-Trace curves are a special case of the C_{ab} curves classified by Miura and Kamiya in [2]

[2] Readers interested in the connection between the theory of order domains and the theory of algebraic curves, or equivalently the theory of function fields, are recommended to read [4, 9]

[3] A proof in English of some of the results from [10, 11, 12] can be seen in [13].

construct order domains, Section 4 presents the construction of codes from Norm-Trace curves and Section 5 gives the new construction which can be seen as punctured codes from Norm-Trace curves. Section 6 contains some examples and Section 7 is the conclusion.

2 Order domains and codes

The presentation of order domains given here is based on [5, 15]. For a more complete introduction to order domains the reader is referred to the literature.

Recall that an $\mathbb{F}$-algebra is a commutative ring with unity that contains $\mathbb{F}$ as a unitary subring (See [4, p. 901]).

Given a set Γ and a total ordering $\prec$ on Γ, then $(\Gamma, \prec)$ is called a well-order if every non-empty subset of Γ has a smallest element with respect to $\prec$. And given a well-order $(\Gamma, \prec)$, we add an element $-\infty$ to Γ such that $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ and extend the ordering $\prec$ with the rule $-\infty \prec \gamma$, for all $\gamma \in \Gamma$, then $(\Gamma_{-\infty}, \prec)$ is a well-order.

Let $\mathbb{N}_0$ denote the non-negative integers and let $\Gamma \subset \mathbb{N}_0$. We add an element $-\infty$ to Γ such that $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ and let $-\infty < n$ for all $n \in \mathbb{N}_0$, then $(\Gamma_{-\infty}, <)$ is a well-order. In the remaining part of this article we will only consider the well-order $(\Gamma_{-\infty}, <)$ defined here.[4]

Definition 1 *Let $(\Gamma_{-\infty}, <)$ be a well-order, let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra. A surjective map $\rho : R \to \Gamma_{-\infty}$ that satisfies the following five conditions for all $f, g, h \in R$ is called an order function on R.*

1. *$\rho(f) = -\infty$ if and only if $f = 0$.*
2. *$\rho(af) = \rho(f)$ for all non-zero $a \in \mathbb{F}$.*
3. *$\rho(f + g) \leqslant max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) \neq \rho(g)$.*
4. *If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$.*
5. *If f and g are non-zero and $\rho(f) = \rho(g)$, then there exists a non-zero $a \in \mathbb{F}$ such that $\rho(f - ag) < \rho(g)$.*

Since $+$ is well-defined on $\Gamma \subset \mathbb{N}_0$ we can also give the following definition.

Definition 2 *Let $(\Gamma_{-\infty}, <)$ be a well-order, let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra. A weight function on R is an order function ρ on R that also satisfy the condition*

[4] A more general discussion of well-orders can be seen in [15].

6. $\rho(fg) = \rho(f) + \rho(g)$

where $+$ is the ordinary $+$ on $\mathbb{N}_0$ extended with the rule $-\infty + \gamma = -\infty$ for $\gamma \in \Gamma_{-\infty}$.

An order structure and an order domain can now be defined.

Definition 3 *Let $\mathbb{F}$ be a field, let R be an $\mathbb{F}$-algebra, ρ an order function and Γ a well-order. Then (R, ρ, Γ) is called an order structure and R is called an order domain (over $\mathbb{F}$).*

From [15, Def. 3.1 & Pro. 3.2] we have

Theorem 4 *Given an order structure (R, ρ, Γ) then any set $\mathcal{B} = \{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ constitutes a basis for R as a vector space over $\mathbb{F}$. For any $f = c_{\gamma_1} f_{\gamma_1} + \cdots + c_{\gamma_d} f_{\gamma_d}$ with $c_{\gamma_1}, \ldots, c_{\gamma_d} \in \mathbb{F}_q \setminus \{0\}$, $\rho(f) = \max_\prec\{\gamma_1, \ldots, \gamma_d\}$ holds. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$ as a vector space over $\mathbb{F}$.*

Definition 5 *Let R be an $\mathbb{F}_q$-algebra. A map $\varphi : R \to \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$, where $*$ denotes component-wise multiplication.*

In the remaining part we will only consider surjective morphisms φ.

Definition 6 *Given an order domain (R, ρ, Γ) and a surjective morphism φ, let 0 be the smallest element of Γ and define $\alpha(1) = 0$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfying $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$, for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.*

From Definition 6 we see that the set $B = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$.

The set $\Delta(R, \rho, \varphi)$ has the following property from [5, Pro. 3].

Proposition 7 *Consider $\alpha(l) \in \Delta(R, \rho, \varphi)$ and assume $\beta_1, \beta_2 \in \Gamma$ satisfies $\rho(f_{\beta_1} f_{\beta_2}) = \alpha(l)$. Then $\beta_1, \beta_2 \in \Delta(R, \rho, \varphi)$ holds.*

As we shall see later one interesting consequence of Proposition 7 is that removing β_1 or β_2 from the set $\Delta(R, \rho, \varphi)$ (removing in a way that will be explained later) forces us to remove $\alpha(l)$ from the set as well if we want to make sure that φ continues to be a morphism. Later on we will also show the significance of this statement when dealing with certain ideals.

First, we need the following definition.

Definition 8 *For $\alpha(i) \in \Delta(R, \rho, \varphi)$ define*

$$N(\alpha(i)) = \{(\beta_1, \beta_2) \in (\Delta(R, \rho, \varphi))^2 \mid \rho(f_{\beta_1} f_{\beta_2}) = \alpha(i)\}$$

and define $\mu(\alpha(i)) = \#N(\alpha(i))$. Furthermore, for $\alpha(j) \in \Delta(R, \rho, \varphi)$ define

$$M(\alpha(j)) = \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \rho(f_{\alpha(j)} f_\beta) = \gamma\}$$

and define $\sigma(\alpha(j)) = \#M(\alpha(j))$.

Note that if ρ in Definition 8 is a weight function then the two sets $N(\alpha(i))$ and $M(\alpha(j))$ can be defined as

$$N(\alpha(i)) = \{(\beta_1, \beta_2) \in (\Delta(R, \rho, \varphi))^2 \mid \beta_1 + \beta_2 = \alpha(i)\}$$

and

$$M(\alpha(j)) = \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \alpha(j) + \beta = \gamma\}.$$

In this case calculating $\mu(\alpha(i))$ and $\sigma(\alpha(j))$ involves nothing but the ordinary $+$ from $\mathbb{N}_0$.

Both the evaluation codes and dual codes from an order domain can now be defined. The codes considered here are the improved codes $\tilde{E}$ and $\tilde{C}$ from [3, 4, 5].

Definition 9 *Consider a basis $\{f_\gamma \mid \rho(f_\gamma) = \lambda\}_{\lambda \in \Gamma}$ for an order structure (R, ρ, Γ) over $\mathbb{F}_q$. Let φ be a morphism as in Definition 5 and let $\Delta(R, \rho, \varphi)$ be as in Definition 6 so $B = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$. Define*

$$\tilde{C}(\eta) = \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_{\alpha(i)}) = 0 \text{ for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \eta\}$$
$$\tilde{E}(\delta) = \mathit{Span}_{\mathbb{F}_q}(\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R, \rho, \varphi) \text{ and } \sigma(\alpha(i)) \geqslant \delta)$$

The following result concerning $\tilde{C}(\eta)$ is from [4, 8] and the result concerning $\tilde{E}(\delta)$ is from [5].

Theorem 10 *The minimum distance of $\tilde{C}(\eta)$ and $\tilde{E}(\delta)$ satisfy $d(\tilde{C}(\eta)) \geqslant \eta$ and $d(\tilde{E}(\delta)) \geqslant \delta$.*

We now know (at least in principle) how to construct the $\tilde{E}$ and $\tilde{C}$ codes and estimate their minimum distance using Theorem 10 above but we need a practical way of constructing order domains. This is where Gröbner basis theory comes into action as shown in the next section.

3 The Gröbner basis approach to order domains

In this section we give a short introduction to order domains constructed using Gröbner basis theory (See [9, 15] for a detailed description). First we introduce the necessary concepts and a few results from Gröbner basis theory.

Let $\mathbb{F}_q$ denote a field with q elements and let $\mathcal{M}_m$ denote the set of monomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ given by $\mathcal{M}_m = \left\{ x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} \;\middle|\; (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{N}_0^m \right\}$.

Recall that a monomial ordering $\prec$ on $\mathcal{M}_m$ is a relation on $\mathbb{N}_0^m$ satisfying the following conditions:

1. $\prec$ is a total ordering on $\mathbb{N}_0^m$.
2. If $\alpha \prec \beta$ and $\gamma \in \mathbb{N}_0^m$, then $\alpha + \gamma \prec \beta + \gamma$.
3. Every non-empty subset of $\mathbb{N}_0^m$ has a smallest element under $\prec$ (that is: $\prec$ is a well-ordering on $\mathbb{N}_0^m$).

Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{N}_0^m$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and let i, where $1 \leqslant i \leqslant m$, be the smallest index such that $\alpha_i - \beta_i \neq 0$ in the vector difference $\boldsymbol{\alpha} - \boldsymbol{\beta}$. Then $\boldsymbol{\alpha}$ is said to be lexicographically smaller than $\boldsymbol{\beta}$, denoted $\boldsymbol{\alpha} \prec_{lex} \boldsymbol{\beta}$, if $\alpha_i - \beta_i < 0$. We write $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} \prec_{lex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$ if $\boldsymbol{\alpha} \prec_{lex} \boldsymbol{\beta}$.

Given positive integers $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}$ define a monomial function $w : \mathcal{M}_m \to \mathbb{N}$ by $w(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}) = \sum_{i=1}^{m} \alpha_i w(x_i)$. For a monomial $m \in \mathcal{M}_m$ we call $w(m)$ the weight of m.

Remark 1: The weights $w(x_1), w(x_2), \ldots, w(x_m)$ can be defined as v-tuples from $\mathbb{N}_0^v \cup \{-\infty\}$. See [5] or [15, Sec. 4] for details. In this paper we only consider the case $v = 1$ which was studied in detail in [4, 17].

Definition 11 *The weighted degree ordering $\prec_w$ induced by w and $\prec_{lex}$ is the monomial ordering defined as follows. Given $m_1, m_2 \in \mathcal{M}_m$ then $m_1 \prec_w m_2$ if one of the following two conditions hold:*

1) $w(m_1) < w(m_2)$ *2) $w(m_1) = w(m_2)$ and $m_1 \prec_{lex} m_2$.*

Given a monomial ordering $\prec$ on $\mathcal{M}_m$ and a polynomial $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ let $lm(f)$ denote the leading monomial in the support of f with respect to $\prec$ and let $lt(f)$ denote the leading term in f with respect to $\prec$.

Definition 12 *Let $\mathbb{F}$ be a field and let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal. Given a monomial ordering $\prec$ on $\mathcal{M}_m$ the set*

$$\Delta_{\prec}(I) = \left\{ m \in \mathcal{M}_m \middle| m \text{ is not a leading monomial of any } f \in I \right\}$$

is called the footprint of I with respect to $\prec$.

A Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ for an ideal I is a basis for I with the property that $\langle lm(g_1), lm(g_2), \ldots, lm(g_t)\rangle = \langle lm(I)\rangle$, where $\langle lm(I)\rangle$ denotes the ideal generated by the leading monomials of $f \in I$ with respect to a given monomial ordering $\prec$. The footprint of I can always be found by constructing a Gröbner basis for I using Buchberger's algorithm (see [16, §2.7]) since (using Definition 12 and the definition of a Gröbner basis) the monomials in $\Delta_\prec(I)$ are exactly the monomials in $\mathcal{M}_m$ which can't be divided by any of the leading monomials in G.

Let $I = \langle f_1, f_2, \ldots, f_s\rangle$ be an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_m]$, let $\mathbb{V}(I)$ denote the corresponding variety given by $\mathbb{V}(I) = \{p_1, p_2, \ldots, p_n\} = \{p \in \mathbb{F}^m \mid f(p) = 0 \text{ for all } f \in I\}$. The following proposition from [16, Pro. 8] and [18, Pro. 2.7] is known as the footprint bound.

Theorem 13 *Let $\mathbb{F}$ be a field and let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal. Then $\#\mathbb{V}(I) \leqslant \#\Delta(I)$. Furthermore, if I is a radical ideal and $\mathbb{F}$ is algebraically closed then equality holds.*

Given an ideal $I \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ consider the quotient of $\mathbb{F}[x_1, x_2, \ldots, x_m]$ modulo I, denoted $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$ (see [16, §5.2]). Let $[f]$ denote the class of a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ given by

$$[f] = \{g \in \mathbb{F}[x_1, x_2, \ldots, x_m] \mid g \equiv f (mod\ I)\},$$

where $g \equiv f (mod\ I)$ (read: g and f are congruent modulo I), if $g - f \in I$. Addition and multiplication in $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$ are well-defined and can be done using representatives of the equivalence classes in $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$, denoted$[f]$. Furthermore, unique standard representatives can be found by using the remainder from dividing f by a Gröbner basis for I (See [16, Pro. 1, §5.3]) as a representative. Let $\bar{f}$ denote the unique standard representative for the equivalence class $[f]$ found this way.

From [16, Pro. 4, §5.3] we have the following result.

Proposition 14 *Let $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be an ideal and let $\prec$ be a monomial ordering on $\mathcal{M}_m$. Then the set $B = \{[m] \mid m \in \Delta_\prec(I)\}$ is a basis for $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as a vector space over $\mathbb{F}_q$.*

Consider the ideal $I_q = \langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ and the variety $\mathbb{V}(I_q) = \{p_1, p_2, \ldots, p_n\}$, then the evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I_q \to \mathbb{F}_q^n$ given by

$$\varphi([f]) = (\bar{f}(p_1), \bar{f}(p_2), \ldots, \bar{f}(p_n)) = (f(p_1), f(p_2), \ldots, f(p_n))$$

is well-defined and is an isomorphism (See [19]). The following well-known corollary of Proposition 14 then follows (see [3, Cor. 1]).

Corollary 15 *Consider an ideal* $I \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, *let* $I_q = I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m \rangle$ *and let* $\prec$ *be any monomial ordering on* $\mathcal{M}_m$. *Then the footprint* $\Delta_\prec(I_q)$ *is finite and* $\#\mathbb{V}(I_q) = \#\Delta_\prec(I_q)$ *holds.*

Our goal in this section is to be able to use the factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as our order domain in Definition 3 but to do so we are required to find an order function on $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$. Pellikaan's factor ring theorem from [9, Thm. 5.11] given below gives us one way of doing this.

Theorem 16 *Let* I *be an ideal in* $\mathbb{F}[x_1, x_2, \ldots, x_m]$ *with Gröbner basis* $\mathcal{B}$ *with respect to* $\prec_w$ *(See Definition 11). Suppose that the elements of the footprint of* I *have mutually distinct weights and that every element of* $\mathcal{B}$ *has exactly two monomials of highest weight in its support. Then there exists a weight function* ρ *on* $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ *with the property that* $\rho([f]) = w(\bar{f})$, *for all polynomials* f, *where* $[f]$ *is the coset of* f *modulo* I *and* $\bar{f}$ *is the standard representative for* $[f]$.

Note that $w(\bar{f})$ in the theorem above is just the highest weight $w(m)$ of the monomials m in the support of $\bar{f}$, i.e. $w(\bar{f}) = \max\{w(m) \mid m \in Supp(\bar{f})\}$.

The consequence of Theorem 16 is that we can construct an order domain by defining an ideal $I \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ with Gröbner basis $\mathcal{B}$, such that the elements in $\mathcal{B}$ and the monomials in $\Delta_\prec(I)$ satisfy the conditions in the theorem. This gives us the order structure (R, ρ, Γ) where $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$, $\rho([f]) = w(\bar{f})$ and $\Gamma = \{w(m) \mid m \in \Delta_\prec(I)\} \subseteq \mathbb{N}_0$. This approach to constructing an order domain is shown in the next section.

4 Codes from Norm-Trace curves

The introduction to codes from Norm-Trace curves given here is based on the description in [3] where the evaluation codes $\tilde{E}$ from Definition 9 constructed using the order structure described in this section were studied in detail. Note that from here on the field $\mathbb{F}_{q^r}$ will be playing the role of $\mathbb{F}_q$ in Section 3. Furthermore, here we adopt the viewpoint from [20] where $\mathbb{F}_{q^r}$ is seen as a vector space over $\mathbb{F}_q$.

First we need the definition of Norm and Trace of an element in $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

Definition 17 *For* $\alpha \in \mathbb{F}_{q^r}$ *the Norm* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ *of* α *over* $\mathbb{F}_q$ *is defined as* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \prod_{j=0}^{r-1} \alpha^{q^j} = \alpha^{(q^r-1)/(q-1)}$. *The Trace* $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ *of* β *over* $\mathbb{F}_q$ *is defined as* $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta) = \sum_{j=0}^{r-1} \beta^{q^j}$.

Let $a = (q^r - 1)/(q - 1)$ and $b = q^{r-1}$. Let R be the factor ring given by $R = \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]/I$, where $I = \langle x^a - y^b - y^{q^{r-2}} - \cdots - y \rangle$ and let $\prec$ be the monomial order

induced by $w(x) = b, w(y) = a$ and $x \prec_{lex} y$. Since the polynomial $x^a - y^b - y^{q^{r-2}} - \cdots - y$ is a Gröbner basis for I satisfying the condition in Theorem 16 by definition, all we have to do is to check that the monomials in $\Delta_{\prec_w}(I) = \{x^i y^j \mid i, j \in \mathbb{N}_0 \text{ and } j < b\}$ have mutually distinct weights in order to use the theorem.

Let $x^{i_1}y^{j_1}, x^{i_2}y^{j_2} \in \Delta_{\prec_w}(I)$ and assume that $w(x^{i_1}y^{j_1}) = w(x^{i_2}y^{j_2})$. This is the same as $i_1 b + j_1 a = i_2 b + j_2 a \Leftrightarrow (i_1 - i_2)b = (j_2 - j_1)a$ but since $gcd(a, b) = 1$ then $(j_2 - j_1)$ must be equal to some integer c times b. Since $0 \leqslant j_1, j_2 < b$ then $c = 0$ is the only option. Hence $i_1 = i_2$ and $j_1 = j_2$.

Define $\Gamma = \{w(m) \mid m \in \Delta_{\prec_w}(I)\}$ and $\Gamma_{-\infty}$ as in Section 2, then the function $w(m) : R \to \Gamma_{-\infty}$ is a weight function (using Theorem 16) on R making $(R, w, \Gamma_{-\infty})$ an order structure and R an order domain. In the remaining part of this paper we will let $(R, \rho, \Gamma_{-\infty})$ denote an order structure as described here.

We still need a way of finding the set $\Delta(R, \rho, \varphi)$ in Definition 6 but the following proposition which is a more general version of [5, Pro. 7] gives us a way to do so. The proof given here is a modified version of the one given in [5].

Note that Proposition 18 contains [5, Pro. 7] as the special case where $J = I_{q^r} = I + \langle x_1^{q^r} - x_1, x_2^{q^r} - x_2, \ldots, x_m^{q^r} - x_m \rangle$.

Proposition 18 *Let $R = \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]/I$ be an order domain as in Theorem 16, let $J = I + \langle x_1^{q^r} - x_1, x_2^{q^r} - x_2, \ldots, x_m^{q^r} - x_m, g_1, g_2, \ldots, g_s \rangle$, where $g_1, g_2, \ldots, g_s \in \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]$, and consider the affine variety $\mathbb{V}(J) = \{p_1, p_2, \ldots, p_n\}$.*

The affine variety map $\varphi : R \to \mathbb{F}_{q^r}^n$ given by $\varphi([f]) = (\bar{f}(p_1), \bar{f}(p_2), \ldots, \bar{f}(p_n))$ is a morphism as in Definition 5. Moreover, φ is surjective.

Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be given as in Definition 6. We have

$$\Delta(R, \rho, \varphi) = \{w(m) \mid m \in \Delta_{\prec_w}(J)\}. \tag{1}$$

Proof:
Clearly φ is well-defined and satisfies the conditions in Definition 5 which establish the first result. The surjectivity of φ follows from the comment after Proposition 14.

By Corollary 15 the equality $\#\mathbb{V}(J) = \#\Delta_{\prec_w}(J)$ holds and using Definition 6 the two sets in (1) must have the same number of elements. Thus if we can show that $\alpha(i) \in \{w(m) \mid m \in \Delta_{\prec_w}(J)\}$ for all $i = 1, 2, \ldots, n$ then we are done. Now, consider a fixed $\alpha(s) \in \Delta(R, \rho, \varphi)$ and a class $[f] \in R$ such that $\rho([f]) = \alpha(s)$ (Note that both f and $\bar{f}$ must be non-zero by Definition 6).

Furthermore, the standard representative $\bar{f}$ for $[f]$ can by definition be written as a linear combination of monomials in the footprint $\Delta_{\prec_w}(I)$ since $\bar{f}$ is the unique remainder of f divided by a Gröbner basis for I. Thus we have

$$\bar{f} = \sum_{i=1}^{t} a_i m_i$$

where $t \geqslant 1$, $a_i \in \mathbb{F}_{q^r} \setminus \{0\}$, $m_i \in \Delta_{\prec_w}(I)$, for $1 \leqslant i \leqslant t$, $w(m_1) < w(m_2) < \cdots < w(m_t)$ and $\alpha(s) = \rho([f]) = wdeg(\bar{f}) = w(m_t)$.

Let $\mathcal{B}'$ be a Gröbner basis for J. By reducing $\bar{f}$ modulo $\mathcal{B}'$ we get the (unique) remainder $\bar{r}$ given by

$$\bar{r} = \sum_{i=1}^{u} b_i n_i$$

where $u \geqslant 1$, $b_i \in \mathbb{F}_{q^r}$, $n_i \in \Delta_{\prec_w}(J)$, for $1 \leqslant i \leqslant u$, and $w(n_1) < w(n_2) < \cdots < w(n_u)$. Because $f - \bar{f} \in I$, $\bar{f} - \bar{r} \in J$ and $I \subseteq J$ (which means that $\mathbb{V}(J) \subseteq \mathbb{V}(I)$ (See [16, §4.2, Thm. 7])) we have

$$\varphi(\bar{r}) = \varphi(\bar{r}) + \varphi(\bar{f} - \bar{r}) = \varphi(\bar{r} + \bar{f} - \bar{r}) = \varphi(\bar{f}) = \varphi([f]), \tag{2}$$

since φ is a morphism (See Definition 5).

Note that $\varphi([f])$ in (2) by the definition of $\alpha(s)$ is non-zero which implies that $\bar{r}$ is non-zero. This fact and the fact that $\Delta_{\prec_w}(J) \subset \Delta_{\prec_w}(I)$ implies that $\rho([\bar{r}]) = w(n_u)$.

Using the division algorithm and the definition of $\prec_w$ we have $wdeg(\bar{f}) \geqslant wdeg(\bar{r})$ (See [16, §2.3, Thm. 3]) which is the same as saying that

$$\alpha(s) \geqslant w(n_u). \tag{3}$$

Comparing (2) and (3) and using the definition of $\alpha(s)$ in Definition 6 gives $\alpha(s) = w(n_u) \in \{w(m) \mid m \in \Delta_{\prec_w}(J)\}$. Since $\alpha(s)$ was arbitrary we have proved the theorem. □

Proposition 18 allows us to construct codes using J and to use the technique described in Section 2 to estimate their minimum distance. The remaining part of this paper will focus on the $\tilde{E}(\delta)$ and $\tilde{C}(\eta)$ codes in Definition 9 constructed by evaluating points from $\mathbb{V}(J)$ using selected monomials in $\Delta_{\prec_w}(J)$.

5 Puncturing codes from Norm-Trace curves

In this section let $I = \langle x^a - y^b - y^{q^{r-2}} - \cdots - y \rangle$, let $(R, \varphi, \Gamma_{-\infty})$ be as in Proposition 18 and let $I_{q^r} = I + \langle x^{q^r} - x, y^{q^r} - y \rangle$. The variety $\mathbb{V}(I_{q^r})$ contains q^{2r-1} points (α, β) in $\mathbb{F}_{q^r}^2$ where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ (See [3]) and the set $\{\varphi(m) \mid m \in \Delta_{\prec_w}(I_{q^r})\}$ is a basis for $\mathbb{F}_{q^r}^n$, where $n = q^{2r-1}$.

Puncturing a code from a Norm-Trace curve in t coordinates corresponds to redefining the evaluation map $\varphi : \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_{q^r}^n$ by leaving out t points from the variety $\mathbb{V}(I_{q^r})$ when evaluating, i.e. φ is redefined as:

$$\varphi([f]) = (\bar{f}(p_{i_1}), \bar{f}(p_{i_2}), \ldots, \bar{f}(p_{i_{n-t}})),$$

where $\{p_{i_1}, p_{i_2}, \ldots, p_{i_{n-t}}\} \subset \mathbb{V}(I_{q^r})$. Selecting these points more or less at random gives no guaranty that they correspond to a variety of an ideal.

This section shows how to construct a set of polynomials $S = \{g_1, g_2, \ldots, g_s\}$ such that $\#\mathbb{V}(I_{q^r} + \langle g_1, g_2, \ldots, g_s\rangle) = n - t$. For a given t a set S can be constructed in several different ways using the technique developed here but the important fact is that the construction given here ensures that Proposition 18 holds. Hence we can use the tools from Section 2 to estimate the minimum distance of the resulting codes and thereby select the best possible set S using this estimate.

Furthermore, the construction of $g_1, g_2, \ldots, g_s$ given here ensures that we remove nothing from the set $\{w(m) \mid m \in \Delta_{\prec_w}(I_{q^r})\}$ but the weights that we are forced to remove according to Proposition 7 when we want φ to stay a morphism. In other words: the minimum distance of the resulting codes is the best possible using Theorem 10 when reducing the size of the footprint $\Delta_{\prec_w}(I_{q^r})$ by adding $g_1, g_2, \ldots, g_s$ to the basis of I_{q^r} (and thereby redefining the map φ).

It is well-known that Norm and Trace maps $\mathbb{F}_{q^r}$ onto $\mathbb{F}_q$ (See [20]). Furthermore, Trace maps q^{r-1} elements from $\mathbb{F}_{q^r}$ on every element in $\mathbb{F}_q$ and Norm maps $\frac{q^r-1}{q-1}$ non-zero elements on every non-zero element in $\mathbb{F}_q$ (and only zero is mapped on zero using Norm). We now define the following two sets for every element in $\mathbb{F}_q$.

Definition 19 *Let $\mathbb{F}_q = \{\gamma_0, \gamma_1, \ldots, \gamma_{q-1}\} \subset \mathbb{F}_{q^r}$. Let $0 \leqslant i \leqslant q-1$ and define $\mathcal{N}(q, r, \gamma_i) \subset \mathbb{F}_{q^r}$ to be the set $\{\alpha \in \mathbb{F}_{q^r} \mid N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \gamma_i\}$, where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ is the Norm from Definition 17.*

Furthermore, define $\mathcal{T}(q, r, \gamma_i)$ to be the set $\{\beta \in \mathbb{F}_{q^r} \mid Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta) = \gamma_i\}$, where and $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ is the Trace from Definition 17.

Using the sets in Definition 19 we can define the following two orderings of the elements in $\mathbb{F}_{q^r}$.

Definition 20 *Let $\mathbb{F}_q = \{\gamma_0, \gamma_1, \ldots, \gamma_{q-1}\} \subset \mathbb{F}_{q^r}$, where $\gamma_0 = 0$, let $a = \frac{q^r-1}{q-1}$ and let $b = q^{r-1}$. Let $\mathbb{F}_{q^r}^{(\alpha)} = \{\alpha_0, \alpha_1, \ldots, \alpha_{q^r-1}\}$ be the elements in $\mathbb{F}_{q^r}$ ordered such that*

$$\begin{aligned}
\mathcal{N}(q, r, \gamma_0) &= \{\alpha_0\} \\
\mathcal{N}(q, r, \gamma_1) &= \{\alpha_1, \ldots, \alpha_a\} \\
\mathcal{N}(q, r, \gamma_2) &= \{\alpha_{a+1}, \ldots, \alpha_{2a}\} \\
&\vdots \\
\mathcal{N}(q, r, \gamma_{q-1}) &= \{\alpha_{(q-2)a+1}, \ldots, \alpha_{q^r-1}\}.
\end{aligned}$$

Furthermore, let $\mathbb{F}_{q^r}^{(\beta)} = \{\beta_0, \beta_1, \ldots, \beta_{q^r-1}\}$ *be the elements in* $\mathbb{F}_{q^r}$ *ordered such that*

$$\begin{aligned}
\mathcal{T}(q, r, \gamma_0) &= \{\beta_0, \ldots, \beta_{b-1}\} \\
\mathcal{T}(q, r, \gamma_1) &= \{\beta_b, \ldots, \beta_{2b-1}\} \\
\mathcal{T}(q, r, \gamma_2) &= \{\beta_{2b}, \ldots, \beta_{3b-1}\} \\
&\vdots \\
\mathcal{T}(q, r, \gamma_{q-1}) &= \{\beta_{(q-1)b}, \ldots, \beta_{q^r-1}\}.
\end{aligned}$$

Now we can construct the extra polynomials $g_1(x, y), g_2(x, y), \ldots, g_s(x, y)$ we need.

Definition 21 *Let* $a = \frac{q^r-1}{q-1}, b = q^{r-1}$ *and let* $\{(i_1, j_1), (i_2, j_2), \ldots, (i_s, j_s)\}$ *be given such that* $0 \leqslant i_1 < i_2 < \cdots < i_{s-1} < i_s < \min\{i_1 + a, q^r\}$ *and* $0 \leqslant j_s < j_{s-1} < \cdots < j_2 < j_1 < b$. *Define* $g_1(x, y), g_2(x, y), \ldots, g_s(x, y)$ *as follows.*

First define the polynomial $g(x) \in \mathbb{F}_{q^r}[x, y]$ *as*

$$g(x) = \prod_{u=0}^{i_1-1} (x - \alpha_u)$$

Then for every $1 \leqslant k \leqslant s$ *define the polynomial* $g_k(x, y) \in \mathbb{F}_{q^r}[x, y]$ *as*

$$g_k(x, y) = g(x) \prod_{u=q^r-(i_k-i_1)}^{q^r-1} (x - \alpha_u) \prod_{v=q^r-j_k}^{q^r-1} (y - \beta_v),$$

where the product over an empty set is defined to be 1.

Remark 2: Note that the polynomials in Definition 21 have no multiple roots. This is easily seen since the only way multiple roots could occur is if $i_1 > (q-2)a + 1$ and $q^r - (i_k - i_1) < i_1$ for some $1 \leqslant k \leqslant s$. But this is not possible since $q^r - (i_k - i_1) < i_1 \Leftrightarrow q^r < i_k$, which contradicts the condition $0 \leqslant i_1 < i_2 < \cdots < i_s < \min\{i_1 + a, q^r\}$ from Definition 21.

Furthermore, we need the following definition (See [16, §2.6]).

Definition 22 *Let* $\mathbb{F}$ *be a field, let* $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ *be non-zero polynomials and let* $\prec$ *be a monomial ordering on the monomials in* $\mathbb{F}[x_1, x_2, \ldots, x_m]$. *Let* $lm(f) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ *and let* $lm(g) = x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$, *where* $lm(f)$ *denotes the leading monomial of* f *with respect to* $\prec$, *and define* $x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}$ *where* $\gamma_i = \max\{\alpha_i, \beta_i\}$, *for* $1 \leqslant i \leqslant m$. *The the S-polynomial of* f *and* g, *written* $S(f, g)$, *is the combination*

$$S(f, g) = \frac{x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}}{lt(f)} \cdot f - \frac{x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}}{lt(g)} \cdot g,$$

where $lt(f)$ is the leading term of f with respect to $\prec$.

The polynomials $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$ in Definition 21 have the following properties.

Proposition 23 *Let $g_1(x,y), g_2(x,y), \ldots, g_s(x,y) \in \mathbb{F}_{q^r}[x,y]$ be the polynomials from Definition 21 and let $\prec_w$ be the monomial ordering in Definition 11 where $w(x) = b = q^{r-1}, w(y) = a = \frac{q^r-1}{q-1}$ and $x \prec_{lex} y$. Furthermore, let $f(x,y) = x^a - y^b - y^{q^{r-2}} - \cdots - y^q - y$. Then the following holds:*

1. *$lm(g_k(x,y)) = x^{i_k}y^{j_k}$ with respect to the monomial ordering $\prec_w$, for all $1 \leqslant k \leqslant s$.*
2. *$\#\mathbb{V}\left(\langle f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y)\rangle\right)$ $= \#\Delta_{\prec}\left(\langle y^b, x^{q^r}, x^{i_1}y^{j_1}, \ldots, x^{i_s}y^{j_s}, x^{i_1+a}\rangle\right)$*
3. *The set $\{f(x,y), x^{q^r}-x, y^{q^r}-y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y), S(f,g_1)\}$ is a Gröbner basis for $\langle f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), \ldots, g_s(x,y)\rangle$*

where $S(f,g_1)$ denotes the S-polynomial of $f(x,y)$ and $g_1(x,y)$.

Proof:
That $lm(g_k(x,y)) = x^{i_k}y^{j_k}$, for $1 \leqslant k \leqslant s$, follows directly from Definition 21.

Let $J = \langle f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y)\rangle$. Since the S-polynomial $S(f,g_1)$ is in J, we have that

$$\#\mathbb{V}(J) \leqslant \#\Delta_{\prec_w}(J) \leqslant \#\Delta_{\prec_w}\left(\langle y^b, x^{q^r}, x^{i_1}y^{j_1}, x^{i_2}y^{j_2}, \ldots, x^{i_s}y^{j_s}, x^{i_1+a}\rangle\right) \tag{4}$$

because the polynomial $S(f,g_1)$ has leading monomial x^{i_1+a}.

Let $\lambda = \min\{i_1 + a, q^r\}$. From Definition 21 we have that $0 \leqslant i_1 < i_2 < \cdots < i_{s-1} < i_s < \lambda$ and $0 \leqslant j_s < j_{s-1} < \cdots < j_2 < j_1 < b$.

The number at the right hand side of (4) is then equal to

$$\begin{aligned} &i_1 b + (i_2 - i_1)j_1 + (i_3 - i_2)j_2 + (i_4 - i_3)j_3 + \cdots + (i_s - i_{s-1})j_{s-1} + (\lambda - i_s)j_s \\ &\quad = i_1 b + \sum_{u=2}^{s}(i_u - i_{u-1})j_{u-1} + (\lambda - i_s)j_s \end{aligned} \tag{5}$$

The rest of the theorem is proved by showing that the number of points in $\mathbb{V}(J)$ is equal to the sum in (5) and thereby showing that the set $\{f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y), S(f,g_1)\}$ is a Gröbner basis for J.

Define $\xi = \max\{i_1, (q-2)a + 1\}$. In Figure 1 a graphical representation of the set $\mathcal{N}(q,r,\gamma_{q-1}) = \{\alpha_{(q-2)a+1}, \ldots, \alpha_{q^r-1}\}$ in $\mathbb{F}_{q^r}^{(\alpha)}$ and $\mathcal{T}(q,r,\gamma_{q-1}) = \{\beta_{(q-1)b}, \ldots, \beta_{q^r-1}\}$ in $\mathbb{F}_{q^r}^{(\beta)}$ in the situation from Definition 21, for a given set $\{(i_1,j_1), (i_2,j_2), \ldots, (i_s,j_s)\}$.

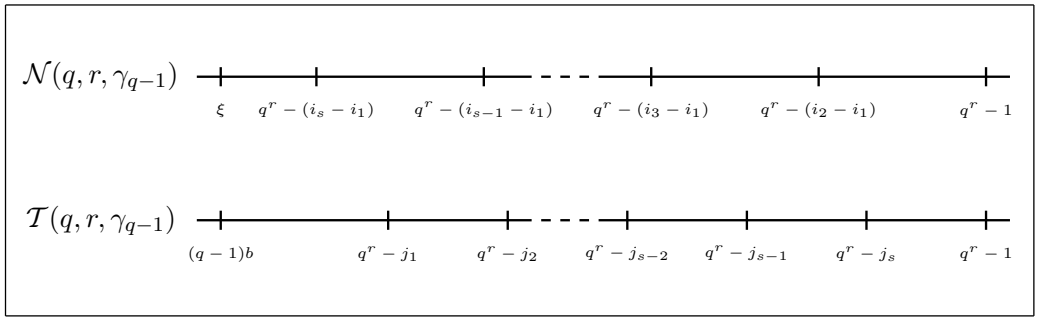


Figure 1: A graphical representation of the two sets $\mathcal{N}(q,r,\gamma_{q-1})$ and $\mathcal{T}(q,r,\gamma_{q-1})$ in the situation from Definition 21 where $\xi = \max\{i_1+a,(q-2)a+1\}$.

Note that when counting elements in $\mathbb{V}(J)$ we have no multiple roots (See Remark 5) and we have to make sure that we only count points (α,β) with $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/fq}(\beta)$.
By definition of the polynomials $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$ in Definition 21, the following number of points must be in the set $\mathbb{V}(J)$ (For reference see Figure 1):

- $i_1 b$ points (α_k,β) where $0 \leqslant k < i_1$, since for every choice of $\alpha_k \in \mathbb{F}_{q^r}^{(\alpha)}$ there exists b different elements $\beta \in \mathbb{F}_{q^r}^{(\beta)}$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha_k) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$. These points are all the zeroes of $g(x)$ and thereby zeroes of every polynomial $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$.

- $(i_2-i_1)j_1$ points (α_k,β_l) where $\alpha_k \in \mathcal{N}(q,r,\gamma_{q-1})$, for $q^r - i_2 + i_1 \leqslant k < q^r$, and $\beta_l \in \mathcal{T}(q,r,\gamma_{q-1})$, for $q^r - j_1 \leqslant l < q^r$. This is true because every counted α_k is a zero of $g_2(x,y), \ldots, g_s(x,y)$ since $i_2 < i_3 < \cdots < i_s$ and every counted β_l is a zero of $g_1(x,y)$.

- $(i_3-i_2)j_2$ points (α_k,β_l) where $\alpha_k \in \mathcal{N}(q,r,\gamma_{q-1})$, for $q^r - (i_3 - i_1 - (i_2 - i_1)) = q^r - i_3 + i_2 \leqslant k < q^r$, and $\beta_l \in \mathcal{T}(q,r,\gamma_{q-1})$, for $q^r - j_2 \leqslant l < q^r$. This holds because these α_k's are all zeroes of $g_3(x,y), \ldots, g_s(x,y)$ because $i_3 < i_4 < \cdots < i_s$ and the β_l's are all zeroes of $g_1(x,y)$ and $g_2(x,y)$ since $j_1 > j_2$. Furthermore, the choice of α_k's ensures that these points haven't been counted before.

- In general we have $(i_u - i_{u-1})j_{u-1}$ points (α_k,β_l) where α_k is a zero of $g_u(x,y)$, $g_{u+1}(x,y), \ldots, g_s(x,y)$ and β_l is a zero of $g_1(x,y), \ldots, g_{u-1}(x,y)$ for every choice of $2 \leqslant u < s$. The construction in Definition 21 ensures that these points are zeroes of $g_1(x,y), \ldots, g_s(x,y), f(x,y)$ and are all different.

- Finally, we have $(q^r - (i_s - i_1) - \xi)j_s$ points (α_k,β_l) where every β_l is a zero of $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$ and the α_k's haven't been counted before. Since $\xi =$

$\max\{i_1, (q-2)a+1\} \Leftrightarrow \xi + a = \max\{i_1 + a, (q-1)a + 1\} = \max\{i_1 + a, q^r\}$ and $\lambda = \min\{i_1 + a, q^r\}$, then $(q^r - (i_s - i_1) - \xi)j_s = (\lambda - i_s)j_s$ holds.

The number of points in $\mathbb{V}(J)$ is then at least $i_1 b + \sum_{u=2}^{s}(i_u - i_{u-1})j_{u-1} + (\lambda - i_s)j_s$ and equality must hold in (4) making the set $\{f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y), S(f,g_1)\}$ a Gröbner basis for J. □

Before we move on to our main result, we would like to give an example of the construction of polynomials as in Definition 21 to make the proof of Proposition 23 clear to the reader.

Example 24

The example given here is based on the Hermitian curve $f(x,y) = x^5 - y^4 - y$ *over* $\mathbb{F}_{16} = \{0, 1, \nu, \nu^2, \ldots, \nu^{14}\}$ *where* ν *is a root of* $1 + x^3 + x^4$ *over* $\mathbb{F}_2$, $q = 4$ *and* $q^2 = 16$. *Let* $a = 5$, $b = 4$, $w(x) = b$, $w(y) = a$ *and* $x \prec_{lex} y$.

We have that $\mathbb{F}_4 = \{0, 1, \nu^5, \nu^{10}\} \subset \mathbb{F}_{16}$.

$\mathbb{F}_{16}^{(\alpha)}$ *from Definition 20 is then*

$$\mathbb{F}_{16}^{(\alpha)} = \{\alpha_0, \ldots, \alpha_{15}\} = \{0, 1, \nu^3, \nu^6, \nu^9, \nu^{12}, \nu, \nu^4, \nu^7, \nu^{10}, \nu^{13}, \nu^2, \nu^5, \nu^8, \nu^{11}, \nu^{14}\}$$

where

$$\begin{aligned}
&\mathcal{N}(4,2,0) = \{0\} = \{\alpha_0\},\\
&\mathcal{N}(4,2,1) = \{1, \nu^3, \nu^6, \nu^9, \nu^{12}\} = \{\alpha_1, \ldots, \alpha_5\},\\
&\mathcal{N}(4,2,\nu^5) = \{\nu, \nu^4, \nu^7, \nu^{10}, \nu^{13}\} = \{\alpha_6, \ldots, \alpha_{10}\},\\
&\mathcal{N}(4,2,\nu^{10}) = \{\nu^2, \nu^5, \nu^8, \nu^{11}, \nu^{14}\} = \{\alpha_{11}, \ldots, \alpha_{15}\}.
\end{aligned}$$

Furthermore, we have

$$\mathbb{F}_{16}^{(\beta)} = \{\beta_0, \ldots, \beta_{15}\} = \{0, 1, \nu^5, \nu^{10}, \nu^7, \nu^{11}, \nu^{13}, \nu^{14}, \nu, \nu^3, \nu^4, \nu^{12}, \nu^2, \nu^6, \nu^8, \nu^9\}$$

where

$$\begin{aligned}
&\mathcal{T}(4,2,0) = \{0, 1, \nu^5, \nu^{10}\} = \{\beta_0, \ldots, \beta_3\},\\
&\mathcal{T}(4,2,1) = \{\nu^7, \nu^{11}, \nu^{13}, \nu^{14}\} = \{\beta_4, \ldots, \beta_7\},\\
&\mathcal{T}(4,2,\nu^5) = \{\nu, \nu^3, \nu^4, \nu^{12}\} = \{\beta_8, \ldots, \beta_{11}\},\\
&\mathcal{T}(4,2,\nu^{10}) = \{\nu^2, \nu^6, \nu^8, \nu^9\} = \{\beta_{12}, \ldots, \beta_{15}\}.
\end{aligned}$$

Let $(i_1, j_1) = (8, 3)$ *and* $(i_2, j_2) = (10, 2)$. *We first define*

$$g(x) = \prod_{u=0}^{7}(x - \alpha_u) = x(x-1)(x-\nu^3)(x-\nu^6)(x-\nu^9)(x-\nu^{12})(x-\nu)(x-\nu^4)$$

as in Definition 21 since $i_1 = 8$.

Then define $g_1(x,y) = g(x)\prod_{v=13}^{15}(y-\beta_v) = g(x)(y-\nu^6)(y-\nu^8)(y-\nu^9)$ *since* $j_1 = 3$.

Finally, define $g_2(x,y) = g(x)\prod_{u=14}^{15}(x-\alpha_u)\prod_{v=14}^{15}(y-\beta_v) = g(x)(x-\nu^{11})(x-\nu^{14})(y-\nu^8)(y-\nu^9)$ *since* $j_2 = 2$ *and* $i_2 - i_1 = 2$.

The following points are in $\mathbb{V}\left(\langle f(x,y), x^{16}-x, y^{16}-y, g_1(x,y), g_2(x,y)\rangle\right)$*:*

- *All points on the form* (α_u, β) *where* $0 \leqslant u < i_1 = 8$ *and* $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_u) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta)$ *because these points are both zeroes of* $g(x)$ *and* $f(x,y)$ *and thereby zeroes of* $g_1(x,y), g_2(x,y)$ *and* $f(x,y)$*. There are* $i_1 \cdot b = 8 \cdot 4 = 32$ *of these points since trace maps* $b = 4$ *elements from* $\mathbb{F}_{q^2}$ *on every element in* $\mathbb{F}_q$*.*
- *We then have* $(i_2 - i_1)j_1 = 2 \cdot 3 = 6$ *points* (α_u, β_v) *where* $u = 14, 15$ *and* $v = 13, 14, 15$ *since* α_{14} *and* α_{15} *are zeroes in* $g_2(x,y)$ *and* β_{13}, β_{14} *and* β_{15} *are zeroes in* $g_1(x,y)$*.*
- *Finally, we have the points* (α_u, β_v) *where* $v = 14, 15$ *and* $\alpha_u \in \mathcal{N}(4, 2, \nu^{10})$ *for* $u \neq 14$ *and* $u \neq 15$*. These points haven't been counted before and are zeroes of both* $g_1(x,y), g_2(x,y)$ *and* $f(x,y)$ *since every* β_v *that is a zero of* $g_2(x,y)$ *is also a zero of* $g_1(x,y)$ *by construction. We have* $(a-(i_2-i_1))j_2 = (i_1+a-i_2)j_2 = (8+5-10)\cdot 2 = 6$ *of these points.*

We have found at least $32 + 6 + 6 = 44$ *points in*

$$\mathbb{V}\left(\langle f(x,y), x^{16}-x, y^{16}-y, g_1(x,y), g_2(x,y)\rangle\right)$$

which is equal to the size of the footprint of $\langle y^4, x^{16}, x^8y^3, x^{10}y^2, x^{13}\rangle$. ▲

Definition 25 *Let* $I \subseteq \mathbb{F}_{q^r}[x,y]$ *be an ideal, let* $\prec$ *be a monomial ordering and let* $w(m)$ *denote the weight of a monomial* m*. Define*

$$W(I) = \{w(m) \mid m \in \Delta(I)\}$$

and for $\alpha \in W(I)$ *define*

$$M(\alpha) = \{\gamma \in W(I) \mid \exists\ \beta \in W(I) \text{ such that } \alpha + \beta = \gamma\}.$$

Theorem 26 *Let* $g_1(x,y), g_2(x,y), \ldots, g_s(x,y) \in \mathbb{F}_{q^r}[x,y]$ *be the polynomials from Definition 21 and let* $\prec$ *be the monomial ordering in Definition 11 where* $w(x) = b = q^{r-1}, w(y) = a = \frac{q^r-1}{q-1}$ *and* $x \prec_{lex} y$*. Furthermore, let* $f(x,y) = x^a - y^b - y^{q^{r-2}} - \cdots - y^q -$

y, let $I_{q^r} = \langle f(x,y), x^{q^r} - x, y^{q^r} - y\rangle \subset \mathbb{F}_{q^r}[x,y]$ and let $J = I_{q^r} + \langle g_1(x,y), g_2(x,y), \ldots, g_s(x,y)\rangle$. Then the following equality holds:

$$W(J) = W(I_{q^r}) \setminus \bigcup_{k=1}^{s} M\Big(w\big(lm(g_k(x,y))\big)\Big). \tag{6}$$

Proof:
Since $\rho(m) = w(m)$ is a weight function (See Definition 2) we have that for every monomial $x^s y^t \in \Delta(I_{q^r})$, which can be divided by $x^{i_k} y^{j_k}$, the weight $w(x^s y^t) = sb + ta$ must be in the set $M(w(g_k(x,y)))$.

Because the set $\{f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), \ldots, g_s(x,y), S(f,g_1)\}$ is a Gröbner basis for J (using Proposition 23) we only remove monomials from $\Delta(I_{q^r})$ which can be divided by at least one of the monomials $x^{i_1} y^{j_1}, \ldots, x^{i_s} y^{j_s}, x^{i_1+a}$ thereby having the equality

$$W(J) = W(I_{q^r}) \setminus \left\{ \bigcup_{k=1}^{s} M(w(x^{i_k} y^{j_k})) \cup M(w(x^{i_1+a})) \right\}.$$

The only thing we need to prove is that $M(w(x^{i_1+a})) \subset M(w(x^{i_1} y^{j_1}))$ in order to have the equality in (6) and prove the theorem. This can be done by showing that $w(x^{i_1+a}) \in M(w(x^{i_1} y^{j_1}))$.

We consider the following two cases:

Case 1: $j_1 = 0$
In this case $x^{i_1} y^{j_1} = x^{i_1}$ which obviously divides x^{i_1+a} so $w(x^{i_1+a}) \in M(w(x^{i_1}))$.

Case 2: $j_1 > 0$
We have to find a monomial $x^s y^t \in \Delta(I_{q^r})$ such that

$$\begin{aligned} & w(x^s y^t) + w(x^{i_1} y^{j_1}) = w(x^{i_1+a}) \\ \Updownarrow & \\ & sb + ta + i_1 b + j_1 a = (i_1 + a)b \;\Leftrightarrow\; sb + (t + j_1)a = ab \end{aligned}$$

which has the solution $s = 0, t = b - j_1$ and since $y^{b-j_1} \in \Delta(I_{q^r})$, we have proved the theorem. □

The result in Theorem 26 has the consequence that by adding polynomials constructed as in Definition 21 to the ideal I_{q^r} we remove exactly the smallest possible set of weights from $W(I_{q^r})$ (smallest in the sense that we remove nothing except the weights that we are forced to remove from the set $W(I_{q^r})$ according to Proposition 7).

6 Examples

In this section we give a few examples of codes using the construction described in Section 5 and compare to known codes punctured in t coordinates.

Example 27
Here we continue Example 24 using the ideal $I_{16} = \langle x^5 - y^4 - y, x^{16} - x, y^{16} - y \rangle \in \mathbb{F}_{16}[x, y]$. *Then*

$$W(I_{16}) = \{0, 4, 5, 8, 9, 10, 12, 13, \ldots, 62, 63, 65, 66, 67, 70, 71, 75\}.$$

Let $t = 11$ *so we want to puncture the Hermitian code at* 11 *coordinates to create codes of length* 53. *In Table 1 the first column is the parameters for the original improved Hermitian codes and the second column is the parameters for the punctured version we get by using ordinary puncturing* 11 *times.*

The column labeled "Construction 1" in Table 1 is the parameters for the codes we get by using $J_{16}^{(1)} = I_{16} + \langle g_1^{(1)}(x, y), g_2^{(1)}(x, y) \rangle$ *where* $lm(g_1^{(1)}(x, y)) = x^{11}y^2$ *and* $lm(g_2^{(1)}(x, y)) = x^{15}y$. *That is we have*

$$\begin{aligned} W(J_{16}^{(1)}) &= W(I_{16}) \setminus \{M(54) \cup M(65)\} \\ &= \{0, 4, 5, 8, 9, 10, 12, 13, \ldots, 52, 53, 55, 56, 57, 60, 61\}. \end{aligned}$$

The column labeled "Construction 2" is the parameters for the codes we get by using $J_{16}^{(2)} = I_{16} + \langle g_1^{(2)}(x, y), g_2^{(2)}(x, y) \rangle$ *where* $lm(g_1^{(2)}(x, y)) = x^{13}y$ *and* $lm(g_2^{(2)}(x, y)) = x^{14}$. *We have*

$$\begin{aligned} W(J_{16}^{(2)}) &= W(I_{16}) \setminus \{M(56) \cup M(57)\} \\ &= \{0, 4, 5, 8, 9, 10, 12, 13, \ldots, 52, 53, 54, 55, 58, 59, 63\}. \end{aligned}$$

For dimensions $38, 40, 41, 42, 43, 44, 45, 46, 49$ *and* 51 *one or both of the two constructions are better than the bound obtained by ordinary puncturing. Also note that none of the two constructions are the best choice for every dimension since using construction 1 we get a* $[53, 38, 11]$ *code while using construction 2 we get a* $[53, 38, 10]$ *code. But using construction 2 gives a* $[53, 40, 9]$ *code and a* $[53, 47, 4]$ *code while construction 1 gives a* $[53, 39, 9]$ *code and a* $[53, 46, 4]$.

Furthermore, notice that the parameters in Table 1 can be calculated without actually constructing any polynomials but simply by using Theorem 26, the code construction $\tilde{E}$ *in Definition 9 and the bound on the minimum distance given in Theorem 10. We could easily construct the generator matrices by using definition 21 to construct* $g_1(x, y)$ *and* $g_2(x, y)$, *find the* 53 *common zeros in* $\mathbb{V}(J_{16})$ *and use the evaluation map* φ *on the monomials selected in Definition 9 to construct the rows in the generator matrix for* $\tilde{E}(\delta)$ *for any given* $\delta = 1, 2, \ldots, 53$.

Table 1: Parameters for the improved Hermitian codes $\tilde{E}$, improved Hermitian codes punctured at 11 coordinates and parameters for construction 1 and 2 with length 53.

Improved Hermitian codes ($\tilde{E}$)	Punctured improved Hermitian codes ($\tilde{E}$)	Construction 1	Construction 2
$[64, 1, 64]$	$[53, 1, 53]$	$[53, 1, 53]$	$[53, 1, 53]$
$[64, 2, 60]$	$[53, 2, 49]$	$[53, 2, 49]$	$[53, 2, 49]$
$[64, 3, 59]$	$[53, 3, 48]$	$[53, 3, 48]$	$[53, 3, 48]$
$[64, 4, 56]$	$[53, 4, 45]$	$[53, 4, 45]$	$[53, 4, 45]$
$[64, 5, 55]$	$[53, 5, 44]$	$[53, 5, 44]$	$[53, 5, 44]$
$[64, 6, 54]$	$[53, 6, 43]$	$[53, 6, 43]$	$[53, 6, 43]$
$[64, 7, 52]$	$[53, 7, 41]$	$[53, 7, 41]$	$[53, 7, 41]$
$[64, 8, 51]$	$[53, 8, 40]$	$[53, 8, 40]$	$[53, 8, 40]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[64, 35, 24]$	$[53, 35, 13]$	$[53, 35, 13]$	$[53, 35, 13]$
$[64, 36, 23]$	$[53, 36, 12]$	$[53, 36, 12]$	$[53, 36, 12]$
$[64, 37, 22]$	$[53, 37, 11]$	-	$[53, 37, 11]$
$[64, 38, 21]$	$[53, 38, 10]$	$[53, 38, 11]$	$[53, 38, 10]$
$[64, 39, 20]$	$[53, 39, 9]$	$[53, 39, 9]$	-
$[64, 40, 19]$	$[53, 40, 8]$	-	$[53, 40, 9]$
$[64, 41, 18]$	$[53, 41, 7]$	$[53, 41, 8]$	$[53, 41, 8]$
$[64, 42, 17]$	$[53, 42, 6]$	-	-
$[64, 43, 16]$	$[53, 43, 5]$	$[53, 43, 7]$	-
$[64, 44, 15]$	$[53, 44, 4]$	-	$[53, 44, 6]$
$[64, 45, 14]$	$[53, 45, 3]$	$[53, 45, 5]$	$[53, 45, 5]$
$[64, 46, 13]$	$[53, 46, 2]$	$[53, 46, 4]$	-
-	-	-	$[53, 47, 4]$
$[64, 48, 12]$	$[53, 48, 1]$	-	-
$[64, 49, 10]$	$[53, 49, 1]$	$[53, 49, 3]$	$[53, 49, 3]$
$[64, 51, 9]$	$[53, 51, 1]$	$[53, 51, 2]$	$[53, 51, 2]$
$[64, 53, 8]$	$[53, 53, 1]$	$[53, 53, 1]$	$[53, 53, 1]$

We could have constructed codes with length 53 *in several other ways than the two shown here but the two used here are the best choices. The remaining 10 possibilities*

are:

$$
\begin{aligned}
W(J_{16}) &= W(I_{16}) \setminus \{M(55) \cup M(62)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(56) \cup M(59)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(57) \cup M(58)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(57) \cup M(59)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(56) \cup M(62) \cup M(63)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(57) \cup M(60) \cup M(63)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(58) \cup M(59) \cup M(60)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(58) \cup M(59) \cup M(61)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(58) \cup M(60) \cup M(61)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(59) \cup M(60) \cup M(61) \cup M(62)\}
\end{aligned}
$$

▲

Example 28

In this example we use the same ideal, I_{16}*, and the two constructions given in Example 27 but this time we construct the* $\tilde{C}$ *codes from Definition 9 using construction 1 and 2 from Example 27 instead. Note that the Hermitian codes* $\tilde{C}(\eta)$ *(and the ordinary puncturing of these) have the same parameters as the Hermitian* $\tilde{E}(\delta)$ *codes in Example 27 (see [5, Prop. 8]) but when using the new construction given here the resulting* $\tilde{E}$ *and* $\tilde{C}$ *no longer have the same parameters. The results are given in Table 2 below.*

Notice that for dimensions $1, 2, \ldots, 6$ *construction 1 and 2 are actually doing worse than ordinary puncturing but for dimensions* $37, 40, 42, 44, 45, 48, 50$ *and* 52 *constructions 1 and 2 are equally good and both better than ordinary puncturing.*

Again, the parameters in Table 2 can be calculated without actually constructing any polynomials but we could construct the rows in the parity check matrix for $\tilde{C}(\eta)$ *for any given* $\eta = 1, 2, \ldots, 53$*.*

Furthermore, we could also have constructed codes with length 53 *in several other ways than the two shown here. The remaining 10 possibilities are the same as in Example 27.*

▲

Remark 3: Notice that the function $\mu(\eta)$ from Definition 8 and the bound in Theorem 10 underestimates the minimum distance of the dimension 1 $\tilde{C}(\eta)$ codes in construction 1 and 2 in Example 28. This suggests that Theorem 10 doesn't give the true minimum distance of $\tilde{C}$ codes from an ideal not having a footprint meeting the condition in [5, Prop. 8]. This contradicts the conjecture in the conclusion of [21] for general codes.

Table 2: Parameters for the improved Hermitian codes $\tilde{C}$, improved Hermitian codes punctured at 11 coordinates and parameters for construction 1 and 2 with length 53.

Improved Hermitian codes ($\tilde{C}$)	Punctured improved Hermitian codes ($\tilde{C}$)	Construction 1	Construction 2
$[64, 1, 64]$	$[53, 1, 53]$	$[53, 1, 50]$	$[53, 1, 52]$
$[64, 2, 60]$	$[53, 2, 49]$	$[53, 2, 49]$	$[53, 2, 48]$
$[64, 3, 59]$	$[53, 3, 48]$	$[53, 3, 46]$	$[53, 3, 47]$
$[64, 4, 56]$	$[53, 4, 45]$	$[53, 4, 45]$	$[53, 4, 44]$
$[64, 5, 55]$	$[53, 5, 44]$	$[53, 5, 44]$	$[53, 5, 43]$
$[64, 6, 54]$	$[53, 6, 43]$	$[53, 6, 42]$	$[53, 6, 42]$
$[64, 7, 52]$	$[53, 7, 41]$	$[53, 7, 41]$	$[53, 7, 41]$
$[64, 8, 51]$	$[53, 8, 40]$	$[53, 8, 40]$	$[53, 8, 40]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[64, 35, 24]$	$[53, 35, 13]$	$[53, 35, 13]$	$[53, 35, 13]$
$[64, 36, 23]$	$[53, 36, 12]$	-	-
$[64, 37, 22]$	$[53, 37, 11]$	$[53, 37, 12]$	$[53, 37, 12]$
$[64, 38, 21]$	$[53, 38, 10]$	$[53, 38, 10]$	$[53, 38, 10]$
$[64, 39, 20]$	$[53, 39, 9]$	-	-
$[64, 40, 19]$	$[53, 40, 8]$	$[53, 40, 9]$	$[53, 40, 9]$
$[64, 41, 18]$	$[53, 41, 7]$	-	-
$[64, 42, 17]$	$[53, 42, 6]$	$[53, 42, 8]$	$[53, 42, 8]$
$[64, 43, 16]$	$[53, 43, 5]$	-	-
$[64, 44, 15]$	$[53, 44, 4]$	$[53, 44, 6]$	$[53, 44, 6]$
$[64, 45, 14]$	$[53, 45, 3]$	$[53, 45, 5]$	$[53, 45, 5]$
$[64, 46, 13]$	$[53, 46, 2]$	-	-
-	-	-	-
$[64, 48, 12]$	$[53, 48, 1]$	$[53, 48, 4]$	$[53, 48, 4]$
$[64, 49, 10]$	$[53, 49, 1]$	-	-
-	-	$[53, 50, 3]$	$[53, 50, 3]$
$[64, 51, 9]$	$[53, 51, 1]$	-	-
-	-	$[53, 52, 2]$	$[53, 52, 2]$
$[64, 53, 8]$	$[53, 53, 1]$	$[53, 53, 1]$	$[53, 53, 1]$

Example 29

In this final example let $q = 2$ and $r = 6$ over $\mathbb{F}_{64}$ such that

$$I_{64} = \langle x^{63} - y^{32} - y^{16} - y^8 - y^4 - y^2 - y, x^{64} - x, y^{64} - y \rangle.$$

The resulting codes have length $q^{2r-1} = 2^{11} = 2048$.

Let $t = 64$, $w(x) = 32$, $w(y) = 63$, $x \prec_{lex} y$ *and* $lm(g_1(x,y)) = x^{62}$ *such that* $J_{64} = I_{64} + \langle g_1(x,y) \rangle$ *and* $W(J_{64}) = W(I_{64}) \setminus M(1984)$. *The codes constructed from* $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/J_{64}$ *have length* 1984 *and a comparison with the ordinary puncturing of the codes from Norm-Trace curves of length* 2048 *can be seen in Figure 2.*

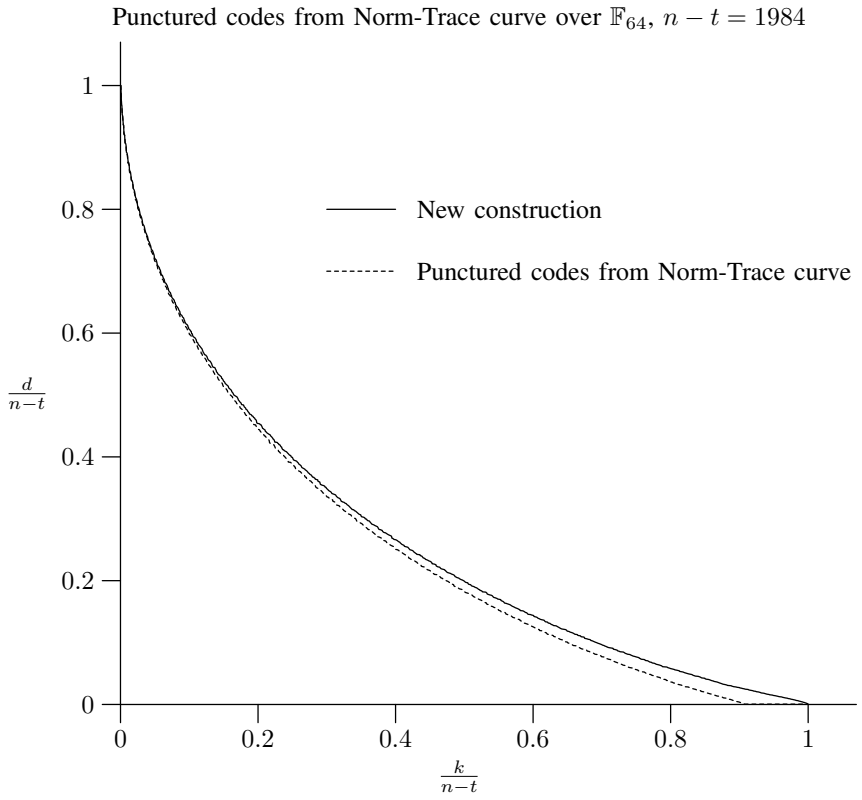


Figure 2: Code rates $\frac{k}{n-t}$ plotted with relative minimum distance $\frac{d}{n-t}$ for ordinarily punctured codes from Norm-Trace curves and codes from the new construction, both of length $n - t = 1984$.

Notice that for rates about 0.9 *the difference between the two codes is the biggest. Parameters for a few codes with approximately this rate are given in Table 3.*

▲

Table 3: Parameters for some $\tilde{E}$ codes from Norm-Trace curves, $\tilde{E}$ codes punctured at 64 coordinates and parameters for the new construction for rates about 0.9.

$\tilde{E}$ codes from Norm-Trace curves	Punctured $\tilde{E}$ codes from Norm-Trace curves	New construction
$[2048, 1791, 69]$	$[1984, 1791, 5]$	-
-	-	$[1984, 1792, 52]$
$[2048, 1794, 68]$	$[1984, 1794, 4]$	-
-	-	$[1984, 1795, 51]$
$[2048, 1799, 66]$	$[1984, 1799, 2]$	-
-	-	$[1984, 1800, 50]$
$[2048, 1801, 65]$	$[1984, 1801, 1]$	-
-	-	$[1984, 1802, 49]$

7 Conclusion

In this paper it was demonstrated that the bound on the minimum distance of codes punctured in t coordinates can be substantially improved in the case of codes from Norm-Trace curves by adding polynomials to the ideal used to construct the order domain. Furthermore, a specific construction of such polynomials is given.

In cases where the puncturing in t coordinates can be constructed using several choices of polynomials, no single choice is the best possible for all code rates as demonstrated in Example 27. Furthermore, Example 28 shows a case where the order bound clearly doesn't give the true minimum distance when constructing the improved dual codes $\tilde{C}$ with extra polynomials added to the ideal.

The technique used here allows for explicit construction of generator or parity check matrices for evaluation codes and dual codes and the improvement compared to the ordinary bound on puncturing can be substantial as demonstrated in Example 29 where a puncturing in $t = 64$ coordinates results in a loss in minimum distance of at most 16 (for $k = 1802$ and $n - t = 1984$).

Acknowledgments

The author would like to thank Olav Geil and Christian Thommesen for helpful discussions.

References

[1] F. MacWilliams, N. Sloane, The Theory of Error-Correcting Codes, North-Holland Amsterdam, 1977.

[2] S. Miura, N. Kamiya, On the Minimum Distance of Codes from Some Maximal Curves, Tech. Rep. IT92-147, IEICE, March 1993, (In Japanese).

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

[4] T. Høholdt, J. van Lint, R. Pellikaan, Chapter 10: "Algebraic geometry codes" in Handbook of coding theory, V. S. Pless and W. C. Huffman (Eds.), vol. 1., Elsevier, Amsterdam, 1998.

[5] H. Andersen, O. Geil, The Missing Evaluation Codes from Order Domain Theory, submitted - preprint available at:
`http://www.math.aau.dk/research/reports/R-2004-17.pdf`.

[6] T. Høholdt, J. H. van Lint, R. Pellikaan, Order functions and evaluation codes, in: Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997), Vol. 1255 of Lecture Notes in Comput. Sci., Springer, Berlin, 1997, pp. 138–150.

[7] G. L. Feng, T. R. N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves, IEEE Trans. Inform. Theory 40 (4) (1994) 1003–1012.

[8] G.-L. Feng, T. R. N. Rao, Improved geometric Goppa codes. I. Basic theory, IEEE Trans. Inform. Theory 41 (6, part 1) (1995) 1678–1693, special issue on algebraic geometry codes.

[9] R. Pellikaan, On the existence of order functions, Journal of Statistical Planning and Inference 94 (2001) 287–301.

[10] S. Miura, Algebraic geometric codes on certain plane curves, IEICE Trans. J75-A (11) (1992) 1735–1745, (In Japanese).

[11] S. Miura, Linear codes on affine algebraic curves, IEICE Trans. J81-A (10) (1998) 1398–1421, (In Japanese).

[12] S. Miura, Ph.D. thesis, University of Tokyo, May 1997, (In Japanese).

[13] R. Matsumoto, The C_{ab} Curve,
Available at: `http://www.rmatsumoto.org/cab.html`.

[14] R. Matsumoto, Miura's Generalization of One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization, IEICE Trans. Fundamentals E82-A (10) (1999) 2007–2010.

[15] O. Geil, R. Pellikaan, On the Structure of Order Domains, Finite Fields and Their Applications 8 (2002) 369–396.

[16] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra, 2nd Edition, Springer Verlag, New York, 1997.

[17] R. Matsumoto, S. Miura, On construction and generalization of algebraic geometry codes, in: T. Katsura et al. (Ed.), Proc. of Algebraic Geometry, Number Theory, Coding Theory and Cryptography, University of Tokyo, Tokyo, Japan, 2000, pp. 3–15.

[18] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer Verlag, New York, 1998.

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

[20] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1986.

[21] C. Munuera, D. Ramirez, The second and third generalized Hamming weights of Hermitian codes, IEEE Trans. Inform. Theory 45 (2) (1999) 709–712.