# On Codes from Norm-Trace Curves

Olav Geil
Department of Mathematics, Aalborg University,
Fredrik Bajersvej 7G, DK-9220 Aalborg Ø, Denmark
E-mail: olav@math.auc.dk

Version: February 12, 2003

The main results of this paper are derived by using only simple Gröbner basis techniques. We present a new construction of evaluation codes from Miura-Kamiya curves $C_{ab}$. We estimate the minimum distance of the codes and estimate the minimum distance of a class of related one-point geometric Goppa codes. With respect to these estimates the new codes perform at least as well as the related geometric Goppa codes. In particular we consider codes from norm-trace curves. We show that our estimates give actually the true minimum distance of these codes. The new codes from norm-trace curves perform rather well. In many cases much better than the corresponding geometric Goppa codes. It turns out that an alternative description of the new codes from norm-trace curves can be made by using Høholdt et al.'s construction of improved dual codes ([11]).

*Key Words:* Algebraic geometry codes, evaluation codes, footprint, Goppa bound, Gröbner basis, hyperbolic codes, minimum distance, norm, order bound, trace.
*Insert header for classifications:* On Codes from Norm-Trace Curves

## 1. INTRODUCTION

In [17], Saints and Heegard considered a class of codes called hyperbolic cascaded Reed-Solomon codes which can be seen as a considerable improvement of the generalized Reed-Muller codes $\mathrm{RM}_q(r,2)$ for $q > 2$. The construction was further generalized by Feng and Rao in [2] to a considerable improvement of the generalized Reed-Muller codes $\mathrm{RM}_q(r,m)$ for arbitrary $m \geq 2$ and $q > 2$. In [11], Høholdt, van Lint and Pellikaan named these codes hyperbolic codes. In [11], [6] and [5] the codes were treated by use of order domain theory. The codes were viewed as improved dual codes (see [11, Sec. 4.3]) coming from the order domain $\mathbb{F}_q[X_1,\ldots,X_m]$. That is the codes were described by means of parity check matrices and their minimum distances were estimated by the order bound. The generator matrices of the codes were not known. In [8] Geil and Høholdt gave a new description of a class of evaluation codes related to the factor ring $\mathbb{F}_q[X_1,\ldots,X_m]/\langle X_1^q - X_1,\ldots,X_m^q - X_m\rangle$. These codes are described by

their generator matrices and their minimum distances are easily found. The description of the codes involves nothing but simple Gröbner basis theory. It was shown in [8] that the class of codes is actually equal to the class of hyperbolic codes. Hence, the new description solves the problem of finding generator matrices for the hyperbolic codes and solves the problem of finding the actual minimum distances of these codes. It turns out that the order bound gives the true minimum distance of the hyperbolic codes.

It is obvious to try to use the techniques from [8] on more complicated algebraic structures than the ones studied in [8]. In this paper we use the methods from [8] to construct evaluation codes from Miura-Kamiya curves $C_{ab}$ (see [14] and [15]). That is, we consider the factor ring

$$R = \mathbb{F}_q[X,Y]/\langle X^a - \mu Y^b - F'(X,Y), X^q - X, Y^q - Y\rangle \tag{1}$$

where $a$ and $b$ are relatively prime, where $\mu$ is non zero, and where any monomial $X^\alpha Y^\beta$ in the support of $F'(X,Y)$ satisfies $\alpha b + \beta a < ab$. We consider two classes of codes. Namely the codes $E(s)$ and the codes $\tilde{E}(s)$. The codes $E(s)$ are examples of one-point geometric Goppa codes whereas the code construction $\tilde{E}(s)$ is new. The description is given in section 2. It involves an estimation of the minimum distance of the codes. With respect to this estimation the codes $\tilde{E}(s)$ are at least as good and sometimes better than the codes $E(s)$. An introduction to the necessary Gröbner basis theoretical concepts is included. In the remaining part of the paper we concentrate on a particular subset of the algebraic structures (1), namely the ones given by

$$\mathbb{F}_{q^r}[X,Y]/\langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y, X^{q^r} - X, Y^{q^r} - Y\rangle. \tag{2}$$

We will call the corresponding curves *norm-trace curves*. In section 3 we show that the estimation of the minimum distance of the codes from norm-trace curves actually gives the true minimum distance. We demonstrate that many of the codes perform rather well in terms of their length, minimum distance and dimension. In some cases the codes $\tilde{E}(s)$ perform much better than the corresponding one-point geometric Goppa codes $E(s)$. In section 4 we show that the codes $\tilde{E}(s)$ can also be described as improved dual codes (see [11]) related to the order domain

$$\mathbb{F}_{q^r}[X,Y]/\langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y\rangle.$$

It turns out that the order bound gives the true minimum distance for these codes. These results are identical to the results in [8] concerning the hyperbolic codes. Section 5 is the conclusion. Appendix A contains proofs of some results that are needed in section 3 and appendix B contains a proof of the main result in section 4.

## 2. A NEW CLASS OF EVALUATION CODES

Throughout this section let $F(X,Y) := X^a - \mu Y^b - F'(X,Y) \in \mathbb{F}_q[X,Y]$ be chosen such that $a$ and $b$ are relatively prime, such that $\mu$ is non zero, and such that any monomial $X^\alpha Y^\beta$ in the support of $F'(X,Y)$ satisfies $\alpha b + \beta a < ab$. We define the ideal $J := \langle F(X,Y), X^q - X, Y^q - Y \rangle \subseteq \mathbb{F}_q[X,Y]$. With this notation the algebraic structure in (1) can be written $R = \mathbb{F}_q[X,Y]/J$. Denote by $\mathbb{F}_q^l$ the $l$-dimensional vector space over $\mathbb{F}_q$. Consider the variety $\{P_1, \ldots, P_n\} = \{P \in \mathbb{F}_q^2 \mid F(P) = 0\}$. It is well known that the map $\varphi : R \to \mathbb{F}_q^n$ given by $\varphi(H+J) := (H(P_1), \ldots, H(P_n))$ is well defined and is an isomorphism (see [4]). We will consider codes defined as the image under $\varphi$ of certain subspaces of $R$. That is, we will consider some particular examples of what Fitzgerald and Lax in [4] call affine variety codes. As a first step in describing the subspaces of $R$ that we are interested in we will restrict ourselves to consider a particular basis $B$ for $R$ as a vector space over $\mathbb{F}_q$. To describe this basis we will need some definitions and results. In the following let $\mathcal{M}(X_1, \ldots, X_m)$ denote the set of monomials in the variables $X_1, \ldots, X_m$.

DEFINITION 1. Given positive integers $a, b$ let $\prec_w$ denote the weighted graded ordering on $\mathcal{M}(X,Y)$ defined as follows. We have $X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if one of the following conditions holds

(1) $\alpha b + \beta a < \gamma b + \delta a$ (2) $\alpha b + \beta a = \gamma b + \delta a$ and $\beta < \delta$.

Let $\prec'_w$ be the weighted graded ordering defined as $\prec_w$ but with the equality in (2) reversed.

DEFINITION 2. Let $k$ be a field and let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal. Given a monomial ordering $\prec$ on $\mathcal{M}(X_1, \ldots, X_m)$ the set

$$\Delta_\prec(I) := \{X_1^{\alpha_1} \cdots X_m^{\alpha_m} \mid X_1^{\alpha_1} \cdots X_m^{\alpha_m} \text{ is not a leading monomial of any polynomial in } I\}$$

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

The name "footprint" was suggested by D. Blahut in 1991. The footprint was previously called the delta-set, the excluded point set and other things (see [10]). In the examples of this paper the footprints are easily found. In more complicated cases one will need to find a Gröbner basis for $I$ by use of Buchberger's algorithm to be able to detect the footprint. By [1, Pro. 4 in Par. 5.3] we have.

PROPOSITION 1. *Let $I$ and $\prec$ be given as in Definition 2. The set $\{M + I \mid M \in \Delta_\prec(I)\}$ is a basis for $k[X_1, \ldots, X_m]/I$ as a vector space over $k$.*

Applying Proposition 1 we see that $B := \{M + J \mid M \in \Delta_{\prec_w}(J)\}$ is a basis for $R$ as a vector space over $\mathbb{F}_q$. The sub vector spaces of $R$ that we will consider in the construction of the evaluation codes are generated by certain subsets of $B$. We are now in the position that we can define the codes.

DEFINITION 3. Let $D : \mathcal{M}(X,Y) \to \mathbb{N}_0$ be the map given by

$$D(X^iY^j) := \min\{bq - (b-j)(q-i), aq - (a-i)(q-j), bi + aj\},$$

and let $\rho : \mathcal{M}(X,Y) \to \mathbb{N}_0$ be the map given by $\rho(X^iY^j) := bi + aj$. For $s \in \mathbb{N}_0$ define $K_s := \operatorname{span}_{\mathbb{F}_q}\{M + J \mid M \in \Delta_{\prec_w}(J), D(M) \leq s\}$ and define $L_s := \operatorname{span}_{\mathbb{F}_q}\{M + J \mid M \in \Delta_{\prec_w}(J), \rho(M) \leq s\}$. Define the code $\tilde{E}(s) := \varphi(K_s)$ and the code $E(s) := \varphi(L_s)$.

As explained in the following remark $F(X,Y)$ is a smooth curve and the map $\rho$ respectively the spaces $L_s$ are closely related to the valuation associated with the place at infinity respectively the corresponding $\mathcal{L}$-spaces. In particular the codes $E(s)$ are one-point geometric Goppa codes. The map $D$ is new and so are the corresponding codes $\tilde{E}(s)$. The parameters of the new codes are discussed in Lemma 1 and Theorem 1 below.

The reader that is not familiar with geometric Gopppa codes may want to skip the following remark. The reader interested in establishing the proofs herein may want to consult [16, Th. 5.11], [13, Th. 1] and [5, Pro. 1].

*Remark 1.* Write $T := \mathbb{F}_q[X,Y]/\langle F(X,Y)\rangle$ then $T$ is an integral domain and the quotient field of $T$ is an algebraic function field of transcendence degree one. Also $T$ is an order domain of transcendence degree one (notion as in [9]). The curve $F(X,Y)$ has a single place $\mathcal{P}_\infty$ at infinity and $T$ is the union of $\mathcal{L}$-spaces corresponding to $\mathcal{P}_\infty$. The discrete valuation corresponding to the place $\mathcal{P}_\infty$ is given as follows. Given a residue class $h \in T$ let $H(X,Y)$ be the polynomial with support contained in $\Delta_{\prec_w}(\langle F(X,Y)\rangle)$ such that $h = H(X,Y) + \langle F(X,Y)\rangle$ (the existence and uniqueness of $H$ is guaranteed by Proposition 1). We have

$$v_{\mathcal{P}_\infty}(h) = -\max\{\rho(M) \mid M \text{ is in the support of } H\}.$$

The points $P_1, \ldots, P_n$ correspond to rational places $\mathcal{P}_1, \ldots, \mathcal{P}_n$. Define $D' := \mathcal{P}_1 + \cdots + \mathcal{P}_n$. The code $E(s)$ is equal to the one-point geometric Goppa code $C_{\mathcal{L}}(D', s\mathcal{P}_\infty)$. Let $0 = s_1 < s_2 < \cdots < s_n$ be the $n$ numbers such that $L_{s_i - 1} \neq L_{s_i}$ holds for $i = 2, \ldots n$ then the codes $E(s_1), \ldots, E(s_n)$ constitutes all the geometric Goppa codes $C_{\mathcal{L}}(D', m\mathcal{P}_\infty)$.

To describe the parameters of the codes $\tilde{E}(s)$ and the codes $E(s)$ we will need some results. First we state a well-known corollary to Proposition 1.

COROLLARY 1. *Consider an ideal*

$$\begin{aligned} I &= \langle F_1(X_1,\ldots,X_m),\ldots,F_l(X_1,\ldots,X_m),X_1^q-X_1,\ldots,X_m^q-X_m\rangle \\ &\subseteq \mathbb{F}_q[X_1,\ldots,X_m]. \end{aligned}$$

*Let $\prec$ be any monomial ordering on $\mathcal{M}(X_1,\ldots,X_m)$ and let $\mathbb{V}_{\mathbb{F}_q}(I)$ denote the variety of $I$. The footprint $\Delta_\prec(I)$ is finite and $\#\mathbb{V}_{\mathbb{F}_q}(I) = \#\Delta_\prec(I)$ holds.*

*Proof.* Let $\mathbb{V}_{\mathbb{F}_q}(I) = \{Q_1,\ldots,Q_N\}$. It is well-known that the map $\phi : \mathbb{F}_q[X_1,\ldots,X_m]/I \to \mathbb{F}_q^N$ given by $\phi(H+I) = (H(Q_1),\ldots,H(Q_N))$ is well defined and is an isomorphism (see [4]). The corollary now follows immediately from Proposition 1. ∎

Given a polynomial $G$, let $\mathrm{Supp}(G)$ denote the support of $G$. The following lemma is an improvement of [3, Th. 4.1] and [7, Pro. 4].

LEMMA 1. *Consider a polynomial $G(X,Y) \in \mathbb{F}_q[X,Y]$ such that*

$$\mathrm{Supp}(G) \subseteq \Delta_{\prec_w}(J). \tag{3}$$

*Let $X^iY^j$ be the leading monomial of $G$ with respect to $\prec_w$. The equation set $F(X,Y) = G(X,Y) = 0$ has at most $D(X^iY^j)$ solutions in $\mathbb{F}_q^2$.*

*Proof.* By Corollary 1 the equation set has

$$\begin{aligned} & \#\Delta_{\prec_w}(\langle F(X,Y), X^q-X, Y^q-Y, G(X,Y)\rangle) \\ = \; & \#\Delta_{\prec'_w}(\langle F(X,Y), X^q-X, Y^q-Y, G(X,Y)\rangle) \end{aligned} \tag{4}$$

solutions. The strategy of the proof is to establish three upper bounds on this number. The leading monomial of $F(X,Y)$ with respect to $\prec_w$ is $Y^b$. Hence the above number is upper bounded by $\#\Delta_{\prec_w}(\langle Y^b, X^q, Y^q, X^iY^j\rangle)$. As by (3) we have $i < q$ and $j < \min\{b,q\}$ this number is at most $bq-(b-j)(q-i)$. To derive the second bound we observe that no two different monomials in $\Delta_{\prec_w}(J)$ are of the same weight, therefore if $M_1, M_2 \in \Delta_{\prec_w}(J)$ and $M_1 \prec_w M_2$ then also $M_1 \prec'_w M_2$ holds. In particular $X^iY^j$ is the leading monomial of $G(X,Y)$ with respect to $\prec'_w$. The leading monomial of $F(X,Y)$ with respect to $\prec'_w$ is $X^a$. Hence, (4) is upper bounded by $\#\Delta_{\prec'_w}(\langle X^a, X^q, Y^q, X^iY^j\rangle)$. This number is at most $aq-(a-i)(q-j)$. The last bound

$$\#\Delta_\prec(\langle F(X,Y), X^q-X, Y^q-Y, G(X,Y)\rangle) \le bi+aj$$

is shown in the proof of [7, Pro. 4]. By definition the smallest value of $bq-(b-j)(q-i)$, $aq-(a-i)(q-j)$ and $bi+aj$ is $D(X^iY^j)$. The proof is complete. ∎

DEFINITION 4. For $s \in \mathbb{N}_0$ we define $\sigma(s) := \max\{D(M) \mid M \in \Delta_{\prec_w}(J), \rho(M) \le s\}$.

We are now in the position that we can describe the parameters of the evaluation codes.

THEOREM 1. *The codes $\tilde{E}(s)$ and $E(s)$ are of length $n = \#\Delta_{\prec_w}(J) = \#\mathbb{V}_{\mathbb{F}_q}(J)$. The dimension of $\tilde{E}(s)$ is $\#\{M \in \Delta_{\prec_w}(J) \mid D(M) \leq s\}$ and the dimension of $E(s)$ is $\#\{M \in \Delta_{\prec_w}(J) \mid \rho(M) \leq s\}$. The minimum distance of $\tilde{E}(s)$ is at least $n-s$. The minimum distance of $E(s)$ is at least $n - \sigma(s)$. In particular the minimum distance of $E(s)$ is at least $n - s$.*

*Proof.* The result concerning the length of the codes is obvious. The result concerning the dimension of the codes is a consequence of Proposition 1 and the fact that the map $\varphi$ is an isomorphism from $R$ to $\mathbb{F}_q^n$. To see the result concerning the minimum distance of the $\tilde{E}(s)$ code consider any code word $\boldsymbol{c}$ in $\tilde{E}(s)$. It is of the form $\boldsymbol{c} = (G(P_1), \ldots, G(P_n))$ where $G$ is a polynomial in $\mathbb{F}_q[X, Y]$ with $\mathrm{Supp}(G) \subseteq \{M \mid M \in \Delta_{\prec_w}(J), D(M) \leq s\}$. Let $X^iY^j$ be the leading monomial of $G$ with respect to $\prec_w$. By Lemma 1 there are at most $D(X^iY^j)$ indices $l \in \{1, \ldots, n\}$ such that $G(P_l) = 0$. Therefore $\mathrm{wt}(\boldsymbol{c}) \geq n - D(X^iY^j)$ holds. But $D(X^iY^j)$ is at most equal to $s$ and the bound on the minimum distance follows. The proof of the first bound on the minimum distance of the $E(s)$ code follows the same lines. Clearly $\sigma(s) \leq s$ and the last result follows. ∎

The reader familiar with geometric Goppa codes may observe that the very last result concerning the codes $E(s)$ in Theorem 1 is just an example of the Goppa bound.

*Remark 2.* It is clear by Definition 3 that $E(s) \subseteq \tilde{E}(\sigma(s))$ holds. By Theorem 1 both codes are of minimum distance at least $n - \sigma(s)$. We conclude that if Theorem 1 gives the true minimum distance of $E(s)$ and $\tilde{E}(\sigma(s))$ then $\tilde{E}(\sigma(s))$ will have parameters at least as good as $E(s)$. If further $E(s) \subsetneq \tilde{E}(\sigma(s))$ holds then $\tilde{E}(\sigma(s))$ can be viewed as an improvement of $E(s)$.

In the next section we will see that Theorem 1 allows us to find the true minimum distance of the codes defined from the algebraic structure (2).

## 3. THE CODES FROM NORM-TRACE CURVES

Consider the polynomial

$$X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y, \tag{5}$$

over $\mathbb{F}_{q^r}$, where $q$ is a prime power and $r$ is a positive integer $r \geq 2$. Clearly $(q^r - 1)/(q - 1)$ and $q^{r-1}$ are relatively prime and any monomial $X^\alpha Y^\beta$ in the support of $-Y^{q^{r-2}} - \cdots - Y$ satisfies $\alpha q^{r-1} + \beta(q^r - 1)/(q - 1) < ((q^r - 1)/(q - 1))q^{r-1}$. Hence, the polynomial described in (5) is an example of the polynomial $F(X, Y)$ from section 2. In the remaining part of this paper we will always assume that $F(X, Y)$ is of the form (5). Hence

given $q$ and $r$, from now on we have $a = (q^r - 1)/(q - 1)$ and $b = q^{r-1}$, $J = \langle F(X,Y), X^{q^r} - X, Y^{q^r} - Y \rangle$ and $R = \mathbb{F}_{q^r}[X,Y]/J$. To treat the corresponding codes we will need some results and a definition.

DEFINITION 5. For $\alpha \in \mathbb{F}_{q^r}$ the norm $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ of $\alpha$ over $\mathbb{F}_q$ is defined by $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) := \alpha^{(q^r-1)/(q-1)}$. The trace $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ of $\alpha$ over $\mathbb{F}_q$ is defined by $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) := \alpha^{q^{r-1}} + \alpha^{q^{r-2}} + \cdots + \alpha^q + \alpha$.

Hence, the zeros of $F(X,Y)$ in $\mathbb{F}_{q^r}^2$ are the points $(\alpha, \beta)$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$.

LEMMA 2. *The equation $F(X,Y) = 0$ has precisely $q^{2r-1}$ solutions in $\mathbb{F}_{q^r}^2$.*

*Proof.* The lemma is proved in appendix A. ∎

LEMMA 3. *We have $\Delta_{\prec_w}(J) = \{X^\alpha Y^\beta \mid \alpha < q^r, \beta < b\}$.*

*Proof.* Consider the monomial ordering $\prec_w$. The leading monomial of $F(X,Y)$ is $Y^b$ and the leading monomial of $X^{q^r} - X$ is $X^{q^r}$. We therefore have

$$\Delta_{\prec_w}(J) \subseteq \{X^\alpha Y^\beta \mid \alpha < q^r, \beta < b\}. \tag{6}$$

By Lemma 2 and Proposition 1 the set on the left hand side of (6) is at least of size $q^{2r-1}$. It is easily recognized that the set on the right hand side is of size $q^{2r-1}$. Hence, the two sets must be equal. ∎

Applying the notation from Definition 3 we have

$$K_s = \text{span}_{\mathbb{F}_{q^r}}\{X^\alpha Y^\beta + J \mid \alpha < q^r, \beta < b, D(X^\alpha Y^\beta) \leq s\}.$$

LEMMA 4. *For $X^i Y^j \in \Delta_{\prec_w}(J)$ there exists a polynomial $G(X,Y)$ that satisfies the following conditions. The leading monomial of $G$ with respect to $\prec_w$ is $X^i Y^j$ and any monomial $M$ in the support of $G$ satisfies $D(M) \leq D(X^i Y^j)$ and satisfies $\rho(M) \leq \rho(X^i Y^j)$. Finally if $X^i Y^j$ is in the set*

$$\{X^\alpha Y^\beta \mid \alpha \leq q^r - a, \beta < b\} \cup \{X^\alpha Y^\beta \mid \alpha < q^r, \beta = 0\} \tag{7}$$

*then the equation set $F(X,Y) = G(X,Y) = 0$ has $bi + aj$ solutions in $\mathbb{F}_{q^r}^2$, and if $X^i Y^j$ is in the set*

$$\{X^\alpha Y^\beta \mid q^r - a < \alpha < q^r, 0 < \beta < b\} \tag{8}$$

*then the equation set $F(X,Y) = G(X,Y) = 0$ has*

$$bq^r - (b-j)(q^r - i) = bi + q^r j - ij$$

*solutions in $\mathbb{F}_{q^r}^2$.*

*Proof.* The lemma is proved in appendix A. ∎

LEMMA 5. *Let $X^iY^j \in \Delta_{\prec_w}(J)$, then*

$$D(X^iY^j) = \begin{cases} bi + aj & \text{for } i \leq q^r - a \\ bi + q^r j - ij & \text{for } i > q^r - a \end{cases}$$

*Proof.* By inspection of Definition 3. ∎

It is now an easy task to construct the various codes $\tilde{E}(s)$. The next theorem gives the precise parameters of the $\tilde{E}(s)$ codes and the $E(s)$ codes.

THEOREM 2. *The codes $\tilde{E}(s)$ and the codes $E(s)$ related to $R$ are of length $n = q^{2r-1}$. If the index $s$ is chosen such that an $M \in \Delta_{\prec_w}(J)$ exists with $D(M) = s$, then the minimum distance of $\tilde{E}(s)$ is $d = n - s$. The minimum distance of $E(s)$ is $d = n - \sigma(s)$.*

*Proof.* The result concerning the length follows immediately from Lemma 2. To see that $d = n - s$ holds for the code $\tilde{E}(s)$ we need by Theorem 1 only to find a code word in $\tilde{E}(s)$ of Hamming weight equal to $n - s$. That is we need only to find a polynomial $G(X, Y)$ such that any monomial $M$ in the support of $G$ satisfies $M \in \Delta_{\prec_w}(J)$, $D(M) \leq s$ and such that the equation set $G(X, Y) = F(X, Y) = 0$ has $s$ solutions in $\mathbb{F}_{q^r}^2$. The existence of such a polynomial is guaranteed by Lemma 4. To prove the result concerning the minimum distance of the code $E(s)$ we need only find a polynomial $G(X, Y)$ such that any monomial $M$ in the support of $G$ satisfies $M \in \Delta_{\prec_w}(J)$, $\rho(M) \leq s$ and such that the equation set $G(X, Y) = F(X, Y) = 0$ has $\sigma(s)$ solutions in $\mathbb{F}_{q^r}^2$. The existence of such a polynomial is guaranteed by Lemma 4. ∎

In the case of $r = 2$ the quotient field of $\mathbb{F}_{q^r}[X, Y]/\langle F(X, Y)\rangle$ is the Hermitian function field. We note that the true parameters of the geometric Goppa codes $E(s)$ corresponding to the Hermitian function field are described in [19] and [20]. We further note that for $q \geq 3$, $r \geq 3$ the true parameters of the geometric Goppa codes $E(s)$ can be found by applying [15, Th. 6].
By Remark 2 and Theorem 2 the parameters of the code $\tilde{E}(\sigma(s))$ are indeed at least as good as the parameters of the code $E(s)$. The next example illustrates the fact that the former is in many cases actually much better than the latter.

EXAMPLE 1. Consider the field extension $\mathbb{F}_{2^7}/\mathbb{F}_2$. The corresponding codes over $\mathbb{F}_{2^7}$ are of length $n = 2^{13}$. The parameters of the codes are plotted in Figure 1. The point set marked with + is the set of the best geometric Goppa codes $E(s)$ (more precisely, if one code $E(s)$ has parameters $[n, k', d']$ and another has parameters $[n, k'', d']$ where $k' < k''$ then the point $(k'/n, d'/n)$ is not included in the figure). The point set marked with $\diamond$ is the set of $\tilde{E}(s)$ codes. For most rates the codes $\tilde{E}(s)$ perform much better than the codes $E(s)$.

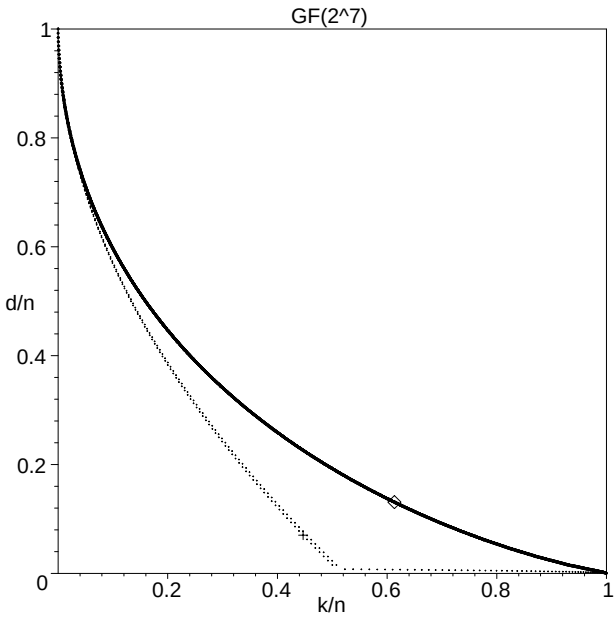


**FIG. 1**

EXAMPLE 2. In this example we consider the codes $E(s)$ in the case $q = 2$ and $r$ is arbitrary. It is easily verified that for $i = 0, \ldots, 2^r - 1$ the minimum distance of $E(D(X^i))$ is equal to $n - D(X^i) = 2^{2r-1} - i2^{r-1}$. Using the fact

$$2\rho(X) = \rho(Y) + 1 \tag{9}$$

it is possible to verify that the dimension is $1 - \frac{\xi}{4} + i + \frac{i^2}{4}$ where $\xi = 1$ if $i$ is odd and $\xi = 0$ if $i$ is even. Hence, if $E(s)$ is a code such that $\frac{d}{n} \in [2^{-r}, 1]$ and $r$ is not too small then

$$\frac{k}{n} \approx 2^{-2^r+1} + 2^{-r+1}\left(1 - \frac{d}{n}\right) + \frac{1}{2}\left(1 - \frac{d}{n}\right)^2 \tag{10}$$

is a good approximation. It is easily verified that for $j = 0, \ldots, 2^{r-1} - 1$ the minimum distance of $E(D(X^{2^{r-1}}Y^j))$ is equal to $n - D(X^{2^{r-1}}Y^j) = 2^{r-1} - j$. Using (9) it is possible to verify that the dimension is $2^{2r-2} + 2^{r-1} + 2^{r-1}j - j^2$. Hence, if $E(s)$ is a code such that $\frac{d}{n} \in [0, 2^{-r}]$ and $r$ is not too small then

$$\frac{k}{n} \approx 1 + \frac{d}{n} - 2^{2r-1}\left(\frac{d}{n}\right)^2 \tag{11}$$

is a good approximation. Consider the plot in Figure 1 of the parameters of the codes $E(s)$ from Example 1. The steep part of the curve corresponds to (10) and the flat part of the curve corresponds to (11).

EXAMPLE 3. By Remark 1 the quotient field of $\mathbb{F}_{q^r}[X,Y]/\langle F(X,Y)\rangle$ is an algebraic function field and the codes $E(s)$ are corresponding geometric Goppa codes. By [11, Pro. 5.11] the function field is of genus $g = (a-1)(b-1)/2$. A version of the geometric Goppa bound states that

$$\frac{d}{n} + \frac{k}{n} \geq 1 - \frac{g}{n} + \frac{1}{n}$$

holds for the codes $E(s)$ with $s < n$. That is, we have

$$\frac{d}{n} + \frac{k}{n} \geq 1 - \frac{q^{2r-1} - 2q^r + q}{2q^{2r} - 2q^{2r-1}} + \frac{1}{q^{2r-1}}.$$

Hence, for $r$ fixed and $q \to \infty$ the codes perform nearly as good as MDS-codes. For $r = 3$ already for $q = 4$ the geometric Goppa bound states that $d/n + k/n \geq 0.8545$ holds for the codes $E(s)$. These codes are of length $n = 4^5$. Nevertheless, Figure 2 illustrates that there is still room for improvement. The $+$'s are the best codes $E(s)$ over $\mathbb{F}_{4^3}$ corresponding to the field extension $\mathbb{F}_{4^3}/\mathbb{F}_4$ (the phrase "best" is explained in Example 1) and the $\diamond$'s are the corresponding codes $\tilde{E}(s)$. For $r = 4$ already for $q = 4$ we have for the codes $E(s)$ $d/n + k/n \geq 0.8386$. These codes are of length $n = 4^7$. For $q$ fixed we have

$$\operatorname{liminf}_{r\to\infty} \left( \frac{d}{n} + \frac{k}{n} \right) \geq \frac{2q-3}{2q-2}. \tag{12}$$

EXAMPLE 4. In this example we consider codes over $\mathbb{F}_{64}$. In Figure 3 the point set marked with $+$ is the set of codes $\tilde{E}(s)$ corresponding to the field extension $\mathbb{F}_{64}/\mathbb{F}_8$. These codes are of length $n = 2^9$. The point set marked with $\diamond$ is the set of codes $\tilde{E}(s)$ corresponding to the field extension $\mathbb{F}_{64}/\mathbb{F}_4$. These codes are of length $n = 2^{10}$. The point set marked with $\square$ is the set of codes $\tilde{E}(s)$ corresponding to the field extension $\mathbb{F}_{64}/\mathbb{F}_2$. These codes are of length $n = 2^{11}$. Finally, the point set marked with $\circ$ is the set of hyperbolic codes $\mathrm{Hyp}_{64}(s,2)$. These codes are of length $n = 2^{12}$. We see that the codes $\tilde{E}(s)$ over $\mathbb{F}_{64}$ get worse as $n$ increases. However, never worse than the hyperbolic codes.

EXAMPLE 5. In this example we consider the codes $\tilde{E}(s)$ in the case $q = 2$ and $r$ is arbitrary. Studying Lemma 5 we see that for this particular case all but a negligible number of the elements $X^iY^j \in \Delta_{\prec_w}(J)$ satisfy $D(X^iY^j) = 2^{r-1}i + 2^r j - ij$ (observe that for $j = 0$ as well as for $i = q^r - a$ the two expressions in Lemma 5 coincide). That is, all but a negligible number of elements satisfy $j = \frac{D(X^iY^j) - 2^{r-1}i}{2^r - i}$. Hence, if $r$ is large and $s$ satisfies $0 \leq s \leq D(X^{2^r-2}) = n - 2^r$ then the dimension of $\tilde{E}(s)$ is approximately

$$\int_0^{s/2^{r-1}} \frac{s - 2^{r-1}i}{2^r - i} di = n - d + d \ln\left(\frac{d}{n}\right).$$

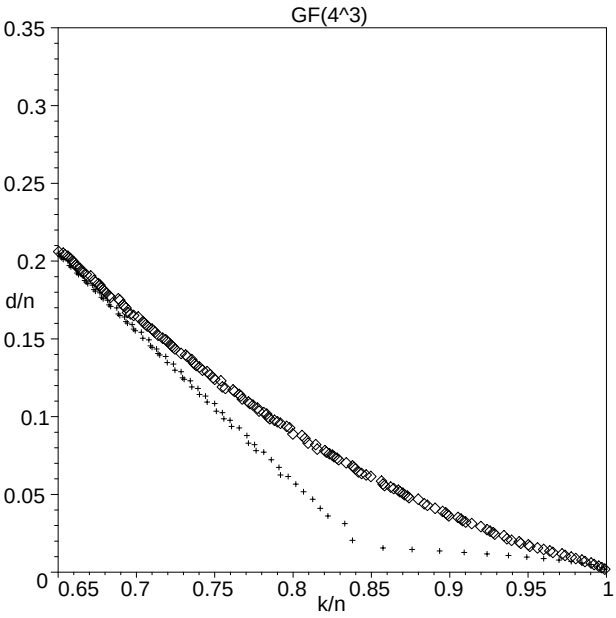
GF(4^3)
0.35
0.3
0.25
0.2
d/n
0.15
0.1
0.05
0
0.65
0.7
0.75
0.8
0.85
0.9
0.95
1
k/n

**FIG. 2**

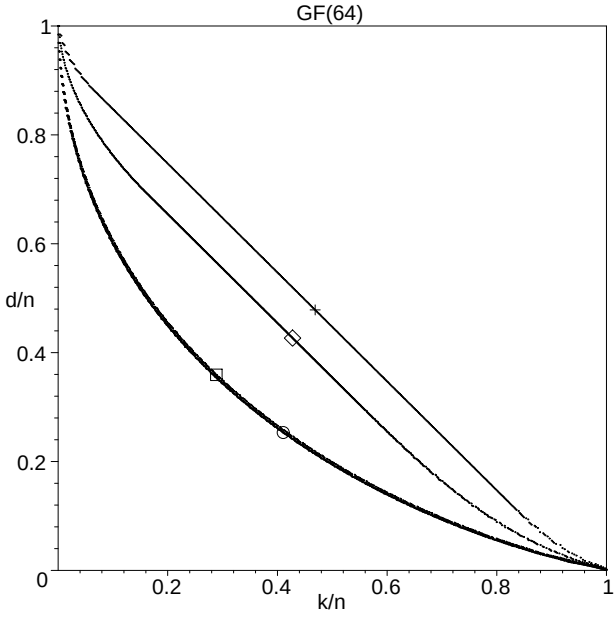
GF(64)
1
0.8
0.6
d/n
0.4
0.2
0
0.2
0.4
0.6
0.8
1
k/n

**FIG. 3**

We conclude that if $r$ is large then for any code $\tilde{E}(s)$

$$\frac{k}{n} \approx 1 - \frac{d}{n} + \frac{d}{n} \ln\left(\frac{d}{n}\right) \tag{13}$$

is a good approximation. Observe for comparison, that the bound (12) only predicts that

$$\text{liminf}_{r\to\infty}\left(\frac{d}{n} + \frac{k}{n}\right) \geq \frac{1}{2}$$

holds. Using similar arguments as above one can show that if $q' \to \infty$ then any hyperbolic code $\text{Hyp}_{q'}(s,2)$ approximately satisfies (13). Consider the plot in Figure 3 of the parameters of the codes from Example 4. The above observations explain why the point sets $\square$ and $\circ$ almost coincide. The curve described by the point set $\square$ as well as the curve described by $\circ$ is very close to the curve described in (13).

## 4. THE CODES $\tilde{E}(S)$ FROM NORM-TRACE CURVES ARE IMPROVED DUAL CODES

In this section we derive parity check matrices for the codes $\tilde{E}(s)$ from the norm-trace curve. More precisely we show that the codes $\tilde{E}(s)$ can be viewed as an example of the improved dual code construction that are described by Høholdt et al. in [11].

DEFINITION 6. For $X^iY^j \in \Delta_{\prec_w}(J)$ define $\mu(X^iY^j)$ to be the number of ordered pairs $(X^{i'}Y^{j'}, X^{i''}Y^{j''})$ such that $X^{i'}Y^{j'}, X^{i''}Y^{j''} \in \Delta_{\prec_w}(\langle J\rangle)$ and $\rho(X^{i'}Y^{j'}) + \rho(X^{i''}Y^{j''}) = \rho(X^iY^j)$.

Recall from section 2 that the map

$$\varphi : R = \mathbb{F}_{q^r}[X,Y]/\langle F(X,Y), X^{q^r} - X, Y^{q^r} - Y\rangle \to \mathbb{F}_q^n$$

is given by $\varphi(H+J) := (H(P_1), \ldots, H(P_n))$, where $\{P_1, \ldots, P_n\}$ is the set of zeros of $F(X,Y)$ in $\mathbb{F}_{q^r}^2$.

DEFINITION 7. Define the code

$$\begin{aligned}\tilde{C}_\varphi(\delta) \quad := \quad & \{\boldsymbol{c} \in \mathbb{F}_{q^r}^n \mid \langle \boldsymbol{c}, \varphi(M+J)\rangle = 0, \\ & \text{for all } M \in \Delta_{\prec_w}(J) \text{ that satisfies } \mu(M) < \delta\}.\end{aligned}$$

Here $\langle\ ,\ \rangle$ denotes the standard inner product in $\mathbb{F}_q^n$.

For readers familiar with the terminology in [11] we include the following remark. We do not include a proof of the result mentioned in the remark. The reader interested in establishing the proof may want to consult Remark 1 and [6, Pro. 6].

*Remark 3.* The code $\tilde{C}_\varphi(\delta)$ is an example of the improved dual code construction that is described in [11, Def. 4.22]. It is related to the order domain $\mathbb{F}_{q^r}[X,Y]/\langle F(X,Y)\rangle$. By the order bound (see [11, Pro. 4.23]) the minimum distance of $\tilde{C}_\varphi(\delta)$ is at least $\delta$.

We leave the proof of the following lemma for the reader.

LEMMA 6. *Let* $X^iY^j \in \Delta_{\prec_w}(J)$, *then*

$$\mu(X^iY^j) = \begin{cases} (i+1)(j+1) & \text{for } i < a-1 \\ ib + aj - ab + a + b & \text{for } i \geq a-1 \end{cases}$$

It turns out that there is a strong connection between the code constructions $\tilde{E}(s)$ and $\tilde{C}_\varphi(\delta)$. We have

THEOREM 3. $\tilde{E}(q^{2r-1} - \delta) = \tilde{C}_\varphi(\delta)$

*Proof.* The theorem is proved in appendix B. ∎

*Remark 4.* From Theorem 2 and Theorem 3 it follows immediately that if $\delta$ is chosen in such a way that $\delta \in \mu(\Delta_{\prec_w}(J))$ then the minimum distance of $\tilde{C}_\varphi(\delta)$ is $\delta$. Hence, by Remark 3 the order bound actually gives the true minimum distance of $\tilde{C}_\varphi(\delta)$.

As by Remark 3 the codes $\tilde{C}_\varphi(\delta)$ are of the type described in [11] they can be decoded up to half the minimum distance by applying the fast decoding algorithm in [11, Sect. 7] and [18].

## 5. CONCLUSION

In this paper we have modified the methods from [8] to derive new descriptions of evaluation codes related to Miura-Kamiya curves $C_{ab}$. We have presented estimates on the minimum distance of the new codes and presented estimates on the minimum distance of a class of related one-point geometric Goppa codes. With respect to these estimates the new codes are always at least as good as the one-point geometric Goppa codes. In particular we have considered codes from norm-trace curves. For these codes our estimates of the minimum distance turn out to give the true value of the minimum distance. Many of the new codes from norm-trace curves perform rather well. Many of them perform much better than the corresponding one-point geometric Goppa codes. We have shown that the new codes from norm-trace curves can also be constructed by the improved dual code construction from order domain theory. In particular we have established a new large class of cases where the order bound gives the true minimum distance of the improved dual codes. The paper [8] and the present paper deals with the same problems, but are concerned with constructing evaluation codes from different algebraic structures. The algebraic structures considered in [8] are very simple. The algebraic structures considered in

the present paper are a little more complicated, but still rather simple. It is obvious to try to use the methods on other algebraic structures than the already considered ones. Also it is obvious to investigate more examples of the Miura-Kamiya curves in details. The paper [8] and the present paper give examples of families of codes for which the order bound from order domain theory actually gives the true minimum distance. One may try to derive some general conditions that ensure that a code has this behavior.

## APPENDIX A: PROOF OF LEMMA 2 AND LEMMA 4

Recall that the zeros of $F(X,Y)$ in $\mathbb{F}_{q^r}^2$ are the points $(\alpha,\beta)$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$. It is well known that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ and $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ map $\mathbb{F}_{q^r}$ onto $\mathbb{F}_q$ (see [12, Th. 2,23 and Th. 2.28]).

LEMMA 7. *The only element in $\mathbb{F}_{q^r}$ that is mapped to 0 under $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ is 0. Given $c \in \mathbb{F}_q\backslash\{0\}$ there are precisely $a = (q^r-1)/(q-1)$ elements in $\mathbb{F}_{q^r}$ that are mapped to $c$ under $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$. Given any $c \in \mathbb{F}_q$ there are precisely $b = q^{r-1}$ elements in $\mathbb{F}_{q^r}$ that are mapped to $c$ under $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}$.*

*Proof.* The lemma is a consequence of the fact that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ is a homomorphism from the multiplicative group $\mathbb{F}_{q^r}\backslash\{0\}$ to the multiplicative group $\mathbb{F}_q\backslash\{0\}$, and that $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ is a homomorphism from the additive group $\mathbb{F}_{q^r}$ to the additive group $\mathbb{F}_q$ (see [12, Th. 2.23]). ∎

DEFINITION 8. For $c \in \mathbb{F}_q$ we denote by $\mathcal{N}(q,r,c)$ the set of elements in $\mathbb{F}_{q^r}$ that are mapped to $c$ under $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$. Similarly we denote by $\mathcal{T}(q,r,c)$ the set of elements that are mapped to $c$ under $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}$.

*Proof of Lemma 2.* The result follows from Lemma 7. ∎

*Proof of Lemma 4.* Let $X^iY^j \in \Delta_{\prec_w}(J)$ be given. That is, let $i,j$ satisfy $0 \le i < q^r$, $0 \le j < b$. Consider any two sets $A, B \subseteq \mathbb{F}_{q^r}$ such that $\#A = i$ and $\#B = j$. The polynomial

$$\prod_{\alpha\in A}(X-\alpha)\prod_{\beta\in B}(Y-\beta) \tag{14}$$

clearly has $X^iY^j$ as leading monomial and any monomial in the support of (14) satisfies $D(M) \le D(X^iY^j)$ and satisfies $\rho(M) \le \rho(X^iY^j)$. We next want to choose $A$ and $B$ in such a way that the number of solutions of $F(X,Y) = \prod_{\alpha\in A}(X-\alpha)\prod_{\beta\in B}(Y-\beta) = 0$ is maximized. We start by introducing some notation and recalling some results. Write $\mathbb{F}_q\backslash\{0\} = \{c_2,\ldots,c_q\}$, and recall from Lemma 7 that we have $\#\mathcal{N}(q,r,0) = 1$ and $\#\mathcal{N}(q,r,c_i) = a$ for $i = 2,\ldots,q$. Recall also that $\#\mathcal{T}(q,r,0) = \#\mathcal{T}(q,r,c_2) = \cdots = \#\mathcal{T}(q,r,c_q) = b$ holds. Write $\alpha_1 := 0$ and let the elements of $\mathbb{F}_{q^r}\backslash\{0\}$ be enumerated $\alpha_2,\ldots\alpha_{q^r}$ such that the first $a$ elements of lowest index constitute the set $\mathcal{N}(q,r,c_2)$, the next $a$ elements of

lowest index constitute the set $\mathcal{N}(q, r, c_3)$ and so on. Write $\mathcal{T}(q, r, c_q) = \{\beta_1, \ldots, \beta_b\}$. Now choose $A := \{\alpha_1, \ldots, \alpha_i\}$ and $B := \{\beta_1, \ldots, \beta_j\}$ and define $G(X, Y) := \prod_{\alpha \in A}(X - \alpha) \prod_{\beta \in B}(Y - \beta)$. The solutions of $F(X, Y) = G(X, Y) = 0$ are $S_A \cup S_B$ where

$$S_A := \{(\alpha, \eta) \mid \alpha \in A, Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\eta) = N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)\}$$

$$S_B := \{(\zeta, \beta) \mid \beta \in B, N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\zeta) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)\}.$$

If $X^i Y^j$ is in the set (7) then $S_A$ and $S_B$ are disjoint. Hence, the number of solutions simply is $\#S_A + \#S_B = bi + aj$. If $X^i Y^j$ is in the set (8) then $S_A$ and $S_B$ are no longer disjoint. Counting the number $\#(S_A \cup S_B)$ carefully we get that the equation set $F(X, Y) = G(X, Y) = 0$ has

$$(q^r - a)b + ja + (i - (q^r - a))(b - j) = bi + q^r j - ij$$

solutions. ∎

## APPENDIX B: PROOF OF THEOREM 3

In this appendix we give a proof of Theorem 3. We start by observing that the maps $\mu$ and $D$ are strongly related.

LEMMA 8. *If $X^i Y^j \in \Delta_{\prec_w}(J)$ then $X^{q^r-1-i} Y^{q^{r-1}-1-j} \in \Delta_{\prec_w}(J)$, and*

$$\mu(X^i Y^j) + D(X^{q^r-1-i} Y^{q^{r-1}-1-j}) = q^{2r-1}. \tag{15}$$

*Proof.* Combine Lemma 5 and Lemma 6 and recall that $b = q^{r-1}$ holds. ∎

To show that any code $\tilde{E}(s)$ from a norm-trace curve is actually a $\tilde{C}_\varphi(\delta)$ code we will need the following lemma. A proof of the lemma is given at the end of appendix B.

LEMMA 9. *Let $i, j, s, t$ be integers such that $0 \leq i, s < q^r$, $0 \leq j, t < q^{r-1}$ and such that $D(X^i Y^j) + \mu(X^s Y^t) < q^{2r-1}$. We have*

$$\sum_{c \in \mathbb{F}_q} \sum_{\alpha \in \mathcal{N}(q,r,c)} \sum_{\beta \in \mathcal{T}(q,r,c)} \alpha^{i+s} \beta^{j+t} = 0.$$

*Proof of Theorem 3.* Let $M_1(X, Y) = X^i Y^j$ be any element in $\Delta_{\prec_w}(J)$ such that $\mu(X^i Y^j) < \delta$ and let $M_2(X, Y) = X^s Y^t$ be any element in $\Delta_{\prec_w}(J)$ such that $D(X^s Y^t) \leq q^{2r-1} - \delta$. Recall, that the variety $\{P_1, \ldots, P_n\}$ of $J$ consists of those $(\alpha, \beta)$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ holds. By Lemma 9 we have $\langle (M_1(P_1), \ldots, M_1(P_n)), (M_2(P_1), \ldots, M_2(P_n)) \rangle = 0$. With the definitions of the codes in mind we conclude that

$$\tilde{E}(q^{2r-1} - \delta) \subseteq \tilde{C}_\varphi(\delta). \tag{16}$$

The dimension of $\tilde{C}_\varphi(\delta)$ is $n = q^{2r-1}$ minus the number of elements in $\Delta_{\prec_w}(J)$ that are of $\mu$ value smaller than $\delta$. In other words the dimension is equal to the number of elements $N_1$ in $\Delta_{\prec_w}(J)$ such that $\mu(N_1) \geq \delta$. The dimension of $\tilde{E}(q^{2r-1} - \delta)$ is equal to the number of elements $N_2$ in $\Delta_{\prec_w}(J)$ such that $D(N_2) \leq q^{2r-1} - \delta$. Hence, by Lemma 8 the two codes are of the same dimension. Therefore the two codes must be identical. ∎

What remains is to give a proof of Lemma 9. The proof calls for some other lemmas.

LEMMA 10. *Assume $c \in \mathbb{F}_q$ and that $i$ is an integer, $0 \leq i < q^{r-1} - 1$. We have*

$$\sum_{\beta \in \mathcal{T}(q,r,c)} \beta^i = 0. \tag{17}$$

*Proof.* We first observe that if $i = 0$, then

$$\sum_{\beta \in \mathcal{T}(q,r,c)} \beta^i = \sum_{j=1}^{q^{r-1}} 1 = 0.$$

In the following we assume $i > 0$. Let the characteristic of $\mathbb{F}_{q^r}$ be $p$. If $i = kp$ where $k$ is a positive integer, then

$$\sum_{\beta \in \mathcal{T}(q,r,c)} \beta^i = \left( \sum_{\beta \in \mathcal{T}(q,r,c)} \beta^k \right)^p.$$

Hence, by induction the proof will be complete if we can show (17) in the case of $i$ being not divisible by $p$, $i > 0$. Assume in the following that such an $i$ is given. Define

$$P_c(X) := \prod_{j=1}^{i} \left( Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\varepsilon^j X) - c \right) \tag{18}$$

where $\varepsilon$ is a primitive $i$th root of unity in $\mathbb{F}_{q^s}$. For any $j$ the set of roots of $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\varepsilon^j X) - c$ is $\{\varepsilon^{-j}\beta \mid \beta \in \mathcal{T}(q,r,c)\}$. So if we write $\mathcal{T}(q,r,c) = \{\beta_1, \ldots, \beta_{q^{r-1}}\}$, then we have

$$\begin{aligned} P_c(X) &= \prod_{j=1}^{i} \left( (X - \varepsilon^{-j}\beta_1) \cdots (X - \varepsilon^{-j}\beta_{q^{r-1}}) \right) \\ &= \prod_{s=1}^{q^{r-1}} \prod_{j=1}^{i} (X - \varepsilon^{-j}\beta_s) \\ &= \prod_{s=1}^{q^{r-1}} (X^i - \beta_s^i) \end{aligned} \tag{19}$$

where the last equality follows from the observation that $\varepsilon^{-j}\beta_s$ is a root of $X^i - \beta_s^i$ for any $j = 1, \ldots, i$. From (19) it is clear that the coefficient to $X^{i(q^{r-1}-1)}$ in $P_c(X)$ is

$$-\sum_{s=1}^{q^{r-1}} \beta_s^i = -\sum_{\beta \in \mathcal{T}(q,r,c)} \beta^i.$$

Hence, if we can show that the coefficient to $X^{i(q^{r-1}-1)}$ in $P_c(X)$ is zero, then we will be done. We have $i(q^{r-1}-1) = (i-1)q^{r-1} + (q^{r-1}-i)$ and by assumptions $0 < i < q^{r-1}-1$ holds. Therefore $q^{r-1}-i \in \{2, \ldots, q^{r-1}-1\}$. Combining these observations with a study of the very definition of $P_c(X)$ (see (18)) we conclude that if the coefficient of $X^{i(q^{r-1}-1)}$ is non zero then

$$i(q^{r-1}-1) = (i-1)q^{r-1} + q^h \tag{20}$$

holds for some $h \in \{1, \ldots, r-2\}$. But then by (20) $i$ must be divisible by $q$ and therefore in particular by $p$. This is impossible by our assumptions. The proof is complete. ∎

Recall from section 3 that $a = (q^r - 1)/(q-1)$.

LEMMA 11. *Given $c \in \mathbb{F}_q$ consider an integer $i > 0$ such that $i \not\equiv 0$ mod $a$. We have*

$$\sum_{\alpha \in \mathcal{N}(q,r,c)} \alpha^i = 0.$$

*Proof.* If $c = 0$ then the result follows immediately. Assume in the following that $c \neq 0$. Let $\gamma$ be an element in $\mathcal{N}(q,r,c)$. We have

$$\mathcal{N}(q,r,c) = \{\gamma, \gamma\tau^{q-1}, \gamma\tau^{2(q-1)}, \ldots, \gamma\tau^{(a-1)(q-1)}\},$$

where $\tau$ is a primitive element of $\mathbb{F}_{q^r}$ with respect to the field extension $\mathbb{F}_{q^r}/\mathbb{F}_q$. Hence,

$$\begin{aligned} \sum_{\alpha \in \mathcal{N}(q,r,c)} \alpha^i &= \gamma^i \sum_{j=0}^{a-1} \tau^{j(i(q-1))} \\ &= \gamma^i \left( \frac{1 - \tau^{i(q^r-1)}}{1 - \tau^{i(q-1)}} \right) = 0. \end{aligned}$$

∎

LEMMA 12. *Let $j$ be an integer $0 \leq j \leq 2(q^{r-1}-1)$ we have*

$$\sum_{c \in \mathbb{F}_q} \sum_{\beta \in \mathcal{T}(q,r,c)} \beta^j = 0. \tag{21}$$

*Proof.* The left hand side of (21) is equal to $\sum_{\beta\in\mathbb{F}_{q^r}}\beta^j$ which in turn is equal to 0 as $j<q^r-1$ holds. ∎

LEMMA 13. *Write* $\mathbb{F}_q\backslash\{0\}=\{c_2,\ldots,c_q\}$. *Let* $j$ *be an integer,* $q^{r-1}-1\le j\le 2(q^{r-1}-1)$. *We have*

$$\sum_{\beta\in\mathcal{T}(q,r,c_2)}\beta^j=\cdots=\sum_{\beta\in\mathcal{T}(q,r,c_q)}\beta^j.$$

*Proof.* Throughout the proof let $c$ be any element in $\mathbb{F}_q\backslash\{0\}$. We first consider the case $j=q^{r-1}-1$. If $\mathcal{T}(q,r,1)=\{\gamma_1,\ldots,\gamma_{q^{r-1}}\}$ then $\mathcal{T}(q,r,c)=\{c\gamma_1,\ldots,c\gamma_{q^{r-1}}\}$ holds. We have

$$\sum_{\beta\in T(q,r,c)}\beta^{q^{r-1}-1}=c^{q^{r-1}-1}\sum_{\beta\in\mathcal{T}(q,r,1)}\beta^{q^{r-1}-1}=\sum_{\beta\in T(q,r,1)}\beta^{q^{r-1}-1}.$$

This concludes the proof for the case $j=q^{r-1}-1$. In the following we consider an arbitrary integer $j$, $q^{r-1}\le j\le 2(q^{r-1}-1)$. For $\beta\in\mathcal{T}(q,r,c)$ we have $\beta^{q^{r-1}}=c-\beta^{q^{r-2}}-\cdots-\beta^q-\beta$. Therefore

$$\begin{aligned}\beta^j &= \sigma_1\beta+\sigma_2\beta^2+\cdots+\sigma_{q^{r-1}-1}\beta^{q^{r-1}-1}\\ &\quad +c\left(\eta_1\beta+\eta_2\beta^2+\cdots+\eta_{q^{r-1}-2}\beta^{q^{r-1}-2}\right)\end{aligned}$$

where $\sigma_1,\ldots,\sigma_{q^{r-1}-1},\eta_1,\ldots,\eta_{q^{r-1}-2}\in\mathbb{F}_q$ are independent of the actual choice of $c$. We conclude

$$\sum_{\beta\in\mathcal{T}(q,r,c)}\beta^j=\sum_{\beta\in\mathcal{T}(q,r,c)}\sigma_{q^{r-1}-1}\beta^{q^{r-1}-1}=\sigma_{q^{r-1}-1}\sum_{\beta\in\mathcal{T}(q,r,1)}\beta^{q^{r-1}-1}. \quad (22)$$

The last expression in (22) is independent of the actual choice of $c$ and we are through. ∎

LEMMA 14. *Let* $s,j$ *be integers* $1\le s\le q-2$, $q^{r-1}-1\le j\le 2(q^{r-1}-1)$. *The following holds*

$$\sum_{c\in\mathbb{F}_q}\sum_{\alpha\in\mathcal{N}(q,r,c)}\sum_{\beta\in\mathcal{T}(q,r,c)}\alpha^{sa}\beta^j=0.$$

*Proof.* Denote $\kappa=\sum_{\beta\in\mathcal{T}(q,r,1)}\beta^j$. We have

$$\begin{aligned}\sum_{c\in\mathbb{F}_q}\sum_{\alpha\in\mathcal{N}(q,r,c)}\sum_{\beta\in\mathcal{T}(q,r,c)}\alpha^{sa}\beta^j &= \sum_{c\in\mathbb{F}_q\backslash\{0\}}\sum_{\alpha\in\mathcal{N}(q,r,c)}\sum_{\beta\in\mathcal{T}(q,r,c)}c^s\beta^j\\ &= \sum_{c\in\mathbb{F}_q\backslash\{0\}}\sum_{\alpha\in\mathcal{N}(q,r,c)}c^s\kappa\\ &= a\kappa\sum_{c\in\mathbb{F}_q}c^s=0.\end{aligned}$$

Here the second equality follows from Lemma 13. The proof is complete. ∎

*Proof of Lemma 9.* By Lemma 8 the conditions implies that not both $i + s \geq q^r - 1$ and $j + t \geq q^{r-1} - 1$ holds. The lemma now follows by applying Lemma 10, Lemma 11, Lemma 12 and Lemma 14 in turn. ∎


## ACKNOWLEDGMENTS

The author wishes to thank Professor T. Høholdt for providing the idea needed in the proof of Lemma 10.


## REFERENCES


[1] D. Cox , J. Little and D. O'Shea, "Ideals, Varieties, and Algorithms, 2nd ed.," Springer, Berlin, 1997.

[2] G.-L. Feng and T.R.N. Rao, Improved Geometric Goppa Codes, Part I:Basic theory, *IEEE Trans. Inform. Theory*, **41**, (Nov. 1995), 1678-1693.

[3] G.-L. Feng, J. Zhu, X. Wu, T.R.N. Rao, High Dimensional Generalized Bezout's Theorem, preprint, Univ. Southwestern Lousiana, 1998.

[4] J. Fitzgerald and R. F. Lax, Decoding Affine Variety Codes Using Gröbner Bases, *Designs, Codes and Cryptography*, **13**, no. 2 (1998), 147-158.

[5] O. Geil, Codes from Order Domains, Proc. of 2001 IEEE International Symposium on Inform. Theory, Washington, USA, June 24-29, 2001, p. 308.

[6] O. Geil, On The Construction of Codes from Order Domains, Manuscript, 2001.

[7] O. Geil and T. Høholdt, Footprints or Generalized Bezout's Theorem, *IEEE Trans. Inform. Theory*, **46** (March 2000), 635-641.

[8] O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci. 2227*, Springer, Berlin 2001, 159-171.

[9] O. Geil and R. Pellikaan, On the Structure of Order Domains, *Finite Fields and their Applications*, **8**, no. 3 (2002), 369-396.

[10] T. Høholdt, On (or in) Dick Blahut's 'footprint', in "Codes, Curves and Signals," (A. Vardy, ed.), Kluwer Academic, Norwell, MA, 1998, 3-9.

[11] T. Høholdt, J. van Lint and R. Pellikaan, Algebraic Geometry Codes, Chapter 10 in "Handbook of Coding Theory," (V.S. Pless and W.C. Huffman, Eds.), vol. 1, Elsevier, Amsterdam, 1998, 871-961.

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

[13] 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**, no. 10 (1999), 2007-2010.

[14] S. Miura, Algebraic geometric codes on certain plane curves, *IEICE Trans. Fundamentals*, **J75-A**, no. 11 (Nov. 1992), 1735-1745 (In Japanese).

[15] S. Miura and N. Kamiya, Geometric-Goppa codes on some maximal curves and their minimum distance, Proc. of 1993 IEEE Information Theory Workshop, Susono-shi, Shizuoka, Japan, June 4-8, 1993, 85-86.

[16] R. Pellikaan, On the existence of order functions, *Journal of Statistical Planning and Inference,* **94**, no. 2 (2001), 287-301.

[17] K. Saints and C. Heegard, On hyperbolic cascaded Reed-Solomon codes, Proc. AAECC-10, *Lecture Notes in Comput. Sci. 673*, Springer, Berlin 1993, 291-303.

[18] S. Sakata, J. Justesen, Y. Madelung, H.E. Jensen, T. Høholdt, A Fast Decoding Method of AG Codes from Miura-Kamiya Curves $C_{ab}$ up to Half the Feng-Rao Bound, *Finite Fields and Their Applications,* **1**, no. 1 (1995), 83-101.

[19] H. Stichtenoth, A Note on Hermitian Codes, *IEEE Trans. Inform. Theory,* **34** (Sept. 1988), 1345-1348.

[20] K. Yang and P. V. Kumar, On the True Minimum Distance of Hermitian Codes, *Lecture Notes in Math. 1518*, Springer, Berlin 1992, 99-107.