ON PARAMETERS OF SUBFIELD SUBCODES OF EXTENDED NORM-TRACE CODES

HEERALAL JANWA
Department of Mathematics, Faculty of Natural Sciences
University of Puerto Rico – Rio Piedras Campus
San Juan, Puerto Rico, 00925 USA

FERNANDO L. PIÑERO
Department of Mathematics
University of Puerto Rico – Ponce Campus
Ponce, Puerto Rico, 00716 USA

(Communicated by Domingo Gomez-Perez)

Abstract. In this article we describe how to find the parameters of subfield subcodes of extended Norm–Trace codes (ENT codes). With a Gröbner basis of the ideal of the \( \mathbb{F}_{q^r} \) rational points of the extended Norm–Trace curve one can determine the dimension of the subfield subcodes or the dimension of the trace code. We also find a BCH–like bound from the minimum distance of the original code. The ENT codes we study here are a more general class of codes than those given in [1]. We study their subfield subcodes as well. We give an example of ENT subfield subcodes that have optimal parameters. Furthermore, we give examples of binary subfield subcodes of ENT codes of very large length for modern applications (e.g. for flash memories).

1. Background and motivation

Extended Norm–Trace codes were introduced in [1]. Extended Norm–Trace codes generalize Norm–Trace codes and Hermitian codes. Our aim is to understand subfield subcodes of extended Norm–Trace codes. These codes include algebraic geometry codes from quasi-Hermitian curves and Norm–Trace curves. BCH codes and binary classical Goppa codes are subfield subcodes of RS codes and subfield subcodes of special algebraic geometric (AG) codes of genus 0 curves (i.e. very special MDS codes). A subfield subcode inherits the minimum distance, the automorphism group and encoding and decoding algorithms from its parent supercode. We have previously used the Gröbner bases approach in [11] to find results regarding the parameters and decoding of subfield subcodes of Hermitian curves. Among such codes we also found codes which are optimal or best known. Now we generalize these results to subfield subcodes of extended Norm-Trace codes. In this article we provide a Gröbner basis framework to study these codes. With a Gröbner basis for the set of \( \mathbb{F}_{q^r} \)–rational points of an extended Norm–Trace curve we prove results that help us give explicit algorithms for computing the parameters of subfield subcodes of extended Norm–Trace codes. These results are easily adaptable to encoding and decoding. We have implemented these algorithms in symbolic software.
We finish with some subfield subcodes of extended Norm–Trace codes which either have optimal parameters or are as good as any known code. Their optimality is deduced from [8].

We fix $q = p^l$ a prime power and $r > 1$ a positive integer. In addition $t$ is a prime power power such that $F_t \subseteq F_{qr}$. We denote the trace function of $F_t$ over $F_{qr}$ by $T_{F_{qr}/F_t}$.

2. Subfield subcodes

For the material in this section, we refer the reader to [12].

**Definition 1.** Let $C$ be a code over $F_{qr}$ of length $n$. The subfield subcode of $C$ is defined as

$$C|F_t := C \cap F_t^n.$$ 

The trace code of $C$ is defined as

$$T_{F_{qr}/F_t}(C) := \{ (T_{F_{qr}/F_t}(c_1), T_{F_{qr}/F_t}(c_2), \ldots, T_{F_{qr}/F_t}(c_n)) \mid (c_1, c_2, \ldots, c_n) \in C \}.$$ 

Both $C|F_t$ and $T_{F_{qr}/F_t}(C)$ are linear codes over $F_t$ of length $n$. In fact, Delsarte’s Theorem shows how to calculate the dual of a subfield code, using trace codes:

**Proposition 1 ([12] Delsarte’s Theorem).** Let $C$ be a linear code over $F_{qr}$. Then

$$(C|F_t)^\perp = T_{F_{qr}/F_t}(C^\perp).$$

The map $x \mapsto x^t$ is an automorphism of $F_{qr}$ which fixes $F_t$ pointwise. In fact, this automorphism generates the Galois group of $F_{qr}$ over $F_t$. One can extend this map to a linear space as follows:

**Definition 2 ([12]).** Let $C$ be a code over $F_{qr}$ of length $n$. Define

$$C^{(t)} := \{(c_1^t, c_2^t, \ldots, c_n^t) \mid c \in C \}.$$ 

Stichtenoth in [12] showed that $C|F_t$ and $T_{F_{qr}/F_t}(C)$ have the same parameters when considered as codes over the superfield $F_{qr}$.

**Proposition 2 ([12]).** Suppose that $q^r = t^m$. Let $C$ be a code over $F_{qr}$. Define the codes $C^o := \bigcap_{i=0}^{m-1} C^{(t)}$ and $C^w := \sum_{i=0}^{m-1} C^{(t)}$. Then $C^o$ is the $F_{qr}$-linear code spanned by $C|F_t$ over $F_{qr}$ and $C^w$ the $F_{qr}$-linear code spanned by $T_{F_{qr}/F_t}(C)$ over $F_{qr}$. Moreover $C^o$ and $C|F_t$ have the dimension and minimum distance. The codes $C^w$ and $T_{F_{qr}/F_t}(C)$ also have the same dimension and minimum distance.

3. Gröbner bases and affine variety codes

In this section we give the theory of Gröbner bases and discuss how it relates to polynomial functions over a set $V$. In order to simplify our notation, we will focus on the case of two variables, although the theory applies to any finite set of variables. We suppose that $X$ and $Y$ are two variables and that $F$ denotes a field.

**Definition 3 ([2] Chapter 2, Section 2, Definition 1, page 55]).** A monomial ordering is a total ordering of the monomials in $F[X,Y]$ which satisfies:

$$X^{i_1}Y^{j_1} < X^{i_2}Y^{j_2}$$ implies that $X^{i_1+i_2}Y^{j_1+j_2} < X^{i_2+i_1}Y^{j_2+j_1}$

for any integers $i, i_1, i_2, j, j_1, j_2$. 

**Advances in Mathematics of Communications** Volume 11, No. 2 (2017), 379–388.
Definition 4 ([2]. Chapter 2, Section 2, Definition 7, page 59). Let \( \prec \) be a monomial order in \( \mathbb{F}[X, Y] \). Suppose \( f(X, Y) = \sum f_{X, Y^j}X^iY^j \) is a polynomial in \( \mathbb{F}[X, Y] \). The leading term of \( f \) is the largest monomial under \( \prec \) where the coefficient \( f_{X, Y^j} \) is nonzero. This term is denoted by \( \text{lt}_\prec(f) \).

Definition 5 ([2]). Let \( I \) be an ideal of \( \mathbb{F}[X, Y] \) and suppose that \( \prec \) is a monomial order in \( \mathbb{F}[X, Y] \). Let \( \text{lt}_\prec(I) \) denote the set of all monomials which are the leading term of some \( f \in I \). The Normal Basis for \( I \) under \( \prec \) is the set
\[
\Delta_\prec(I) := \{ X^i Y^j \mid X^i Y^j \notin \text{lt}_\prec(I) \}.
\]

Definition 6 ([2]. Chapter 1, Section 4, Definition 5, page 32]). Let \( V \) be a subset of points of \( \mathbb{F}^2 \). The ideal of \( V \) is defined as
\[
I_V := \{ f(X, Y) \in \mathbb{F}[X, Y] \mid f(x, y) = 0 \forall (x, y) \in V \}.
\]

We can relate the polynomial functions on the points of \( V \) to the ideal \( I_V \) and the Normal Basis \( \Delta_\prec(I_V) \).

Proposition 3 ([2. Chapter 5, Section 1, Proposition 2, page 217]). Let \( V \) be a subset of points of \( \mathbb{F}^2 \). Then
\[
f(P_i) = g(P_i) \forall (x_i, y_i) \in V \text{ if and only if } f - g \in I_V.
\]

The following bound is known as the footprint bound.

Proposition 4 ([7]). Let \( V \) be a subset of points of \( \mathbb{F}^2 \). Suppose that \( V \) is finite. Let \( I \) be an ideal of \( \mathbb{F}[X, Y] \) such that \( f(x, y) = 0 \) for all \( (x, y) \in V \). Then \( \#V \leq \#\Delta_\prec(I) \).

Proposition 5. Let \( V = \{ P_1, P_2, \ldots, P_n \} \) be a set of points of \( \mathbb{F}^2 \). Suppose that \( \prec \) is a monomial order in \( \mathbb{F}[X, Y] \). Let \( L \) be a linear subspace of \( \mathbb{F}[X, Y] \). The kernel of the map \( \text{ev}_V(f) : L \to \mathbb{F}^n \), which maps the polynomial \( f \in L \) to the point \( (f(P_1), f(P_2), \ldots, f(P_n)) \), is a linear map whose kernel is \( I_V \cap L \).

Proof. Clearly, if \( f \in I_V \cap L \), then it belongs to the kernel of \( \text{ev}_V \). Suppose \( \text{ev}_V(f) \) is equal to the zero vector. A polynomial \( f \in L \) evaluates to 0 over each point of \( V \) if and only if \( f \in I_V \). Therefore \( \text{ev}_V(f) \) evaluates to 0 implies that \( f \in L \cap I_V \).

Definition 7 ([3]). Suppose that \( V = \{ P_1, P_2, \ldots, P_n \} \subseteq \mathbb{F}_q^m \) is a finite set and \( L \) is an \( \mathbb{F}_q \)-linear subspace of polynomials. Then the affine variety code is defined as
\[
C(V, L) := \{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L \}.
\]

Note that Proposition 5 states precisely that \( \dim C(V, L) = \dim L - \dim L \cap I_V \). In order to understand the subfield subcode construction better, we state a simple way of expressing the Trace code of an affine variety code.

Lemma 8. Suppose that \( V = \{ P_1, P_2, \ldots, P_n \} \subseteq \mathbb{F}_q^m \) is a finite set and \( L \) is an \( \mathbb{F}_q \)-linear subspace of polynomials. Then
\[
T_{\mathbb{F}_q^m/\mathbb{F}_q}(C(V, L)) = C(V, T_{\mathbb{F}_q^m/\mathbb{F}_q}(L)) = C(V, \sum_{i=0}^{m-1} (L^{(i'}})).
\]

Proof. Let \( c \in T_{\mathbb{F}_q^m/\mathbb{F}_q}(C(V, L)) \). Then
\[
c = (T_{\mathbb{F}_q^m/\mathbb{F}_q}(f(P_1)), T_{\mathbb{F}_q^m/\mathbb{F}_q}(f(P_2)), \ldots, T_{\mathbb{F}_q^m/\mathbb{F}_q}(f(P_n)))
\]
for some \( f \in L \). Then
\[
c = (g(P_1), g(P_2), \ldots, g(P_n))
\]
where \( g = \mathcal{T}_{F_q^r/F_{q^r}}(f) \). Therefore \( c \in C(V, \mathcal{T}_{F_q^r/F_{q^r}}(L)) = C(V, \sum_{i=0}^{m-1} (L^{(i)})). \quad \Box
\]

4. Codes on curves related to the Norm–Trace curve

We start with the codes in this section as an example to help the reader. The codes in this section are generalization of Norm–Trace codes as found in [5]. These codes are a special case of the extended Norm–Trace codes presented in [1]. We fix \( q \) a prime power and \( r \) an integer. In this case, we let \( u = \frac{q^r - 1}{q - 1} \). The case \( u = \frac{q^r - 1}{q - 1} \) is the Norm–Trace curve.

**Definition 9.** The curve \( X^u - \mathcal{T}_{F_q^r/F_{q^r}}(Y) = 0 \) over \( F_q^r \) is known as an extended Norm–Trace curve over \( F_q^r \). Denote by
\[
\mathcal{N}^u := \{(x, y) \in F_q^r \mid x^u = \mathcal{T}_{F_q^r/F_{q^r}}(y)\}.
\]

**Definition 10.** The \((q^r - 1, u)\)-weight of a monomial is defined as
\[
\rho_{q^r - 1, u}(X^iY^j) = iq^{r-1} + ju.
\]

We denote by
\[
\mathcal{M}_{q^r - 1, u}(s) := \{X^iY^j \mid iq^{r-1} + ju \leq s, 0 \leq i, j\}.
\]

**Definition 11.** The extended Norm–Trace code of weight \( s \) is
\[
\mathcal{N}^u(s) := C(\mathcal{N}^u, \mathcal{M}_{q^r - 1, u}(s)).
\]

**Proposition 6 ([1]).** The following equality,
\[
\mathcal{N}^u(s) = \mathcal{N}^u(q^{r-1}(u - 1) + u(q^{r-1} - 1) - 1 - s),
\]
holds.

Our aim is to find or bound the dimension of \( \mathcal{N}^u(s)|F_t \).

**Lemma 12.**
\[
\dim \mathcal{N}^u(s)|F_t = n - \dim \mathcal{T}_{F_q^r/F_{q^r}}(\mathcal{N}^u(q^{r-1}(u - 1) + u(q^{r-1} - 1) - 1 - s)).
\]

**Proof.** Delsarte’s theorem implies that \((C|F_t)^{\perp} = \mathcal{T}_{F_q^r/F_{q^r}}(C^{\perp})\) for any code \( C \). Therefore \( \mathcal{N}^u(s)|F_t = \mathcal{T}_{F_q^r/F_{q^r}}(\mathcal{N}^u(s)^{\perp}) \). \( \mathcal{N}^u(s)^{\perp} \) states that
\[
\mathcal{N}^u(s)^{\perp} = \mathcal{N}^u(q^{r-1}(u - 1) + u(q^{r-1} - 1) - 1 - s).
\]

Therefore
\[
\mathcal{N}^u(s)|F_t = \mathcal{T}_{F_q^r/F_{q^r}}(\mathcal{N}^u(q^{r-1}(u - 1) + u(q^{r-1} - 1) - 1 - s)^{\perp}).
\]
Now the Lemma follows easily. \( \Box \)

As \( \mathcal{N}^u(s) \) is an affine variety code, \( \mathcal{T}_{F_q^r/F_{q^r}}(\mathcal{N}^u(s)) \) is also an affine variety code. Our aim is to find a bound for \( \dim(\mathcal{T}_{F_q^r/F_{q^r}}(\mathcal{N}^u(s))) \). In order to determine the kernel of the evaluation of the functions in \( \sum_{i=0}^{m-1} (\mathcal{M}_{q^r - 1, u}(s)^{(i)}) \) on the points of \( \mathcal{N}^u \), we compute a Gröbner basis for the ideal corresponding to \( \mathcal{N}^u \).

**Lemma 13.** The ideal of polynomial functions which vanish on \( \mathcal{N}^u \) is generated by \( X^u - \mathcal{T}_{F_q^r/F_{q^r}}(Y) \) and \( X^{u(q^{r-1}+1)} - X \).
This is a particular case of Theorem 19. We refer the reader to the proof therein. The next proposition is an immediate consequence of the previous result and Proposition 3.

Proposition 7.

\[ f(P_i) = g(P_i) \quad \forall P_i \in \mathcal{N}_u \quad \text{if and only if} \quad f - g \in \langle X^u - T(Y), X^{u(q-1)+1} - X \rangle. \]

Lemma 14. The \((q^{r-1}, u)\)-weights of the terms of \(X^u - T_{q^{r-1}}/\mathbb{F}_q(Y)\) are congruent \(\mod (q - 1)u\). Likewise, the \((q^{r-1}, u)\)-weights of the terms of \(X^{u(q-1)+1} - X\) are congruent \(\mod (q - 1)u\).

Proof. Note that \(\rho_{q^{r-1},u}(X^u) = q^{r}u\) and \(\rho_{q^{r-1},u}(Y^q) = q^{r}u\). Clearly the result is true for \(X^u - T_{q^{r-1}}/\mathbb{F}_q(Y)\). The \((q^{r-1}, u)\)-weight of \(X^{u(q-1)+1}\) is \(q^{r-1}(u(q-1)+1)\).

Corollary 15. If the \((q^{r-1}, u)\)-weights of the monomials of the nonzero terms of \(f\) are congruent \(\mod (q - 1)u\), then the \((q^{r-1}, u)\)-weights of the monomials of the nonzero terms of \(f \mod (X^u - T(Y), X^{q^r} - X)\) are also congruent \(\mod (q - 1)u\).

Proof. As \(\{X^u - T(Y), X^{q^r} - X\}\) is a Gröbner basis for \(\langle X^u - T(Y), X^{q^r} - X \rangle\) with respect to the lexicographic order with \(Y\) greater than \(X\), it means that remainders \(\mod (X^u - T(Y), X^{q^r} - X)\) are obtained by repeated divisions by \(X^u - T(Y)\) and \(X^{q^r} - X\). Since each division preserves the \((q^{r-1}, u)\)-weights \(\mod q^r - 1\) and the remainder of the sum equals the sum of the remainders, the corollary follows.

In [9] the authors used simpler techniques to prove that Lemma 14 and Corollary 15 hold for Norm–Trace curves. As there are fewer monomials, but a similar structure remains, the computations will be faster for extended Norm–Trace codes as the divisor \(u\) decreases. As the authors state in [1], we can find a lower bound of the minimum distance of \(\mathcal{N}_u(s)\) from the theory of order domain codes. We use the following minimum distance bound from [6].

Proposition 8 ([6]). Let \(\Delta = \{X^iY^j \mid 0 \leq i \leq u(q-1), 0 \leq j \leq q^{r-1}\}\). Then the minimum distance of \(\mathcal{N}_u(s)\) satisfies:

\[
d(\mathcal{N}_u(s)) \geq \min_{P \in \mathcal{M}_u(s)} \# \{K \in \Delta \mid \exists K' \in \Delta \text{ s.t. } \rho_u(K') + \rho_u(P) = \rho_u(K)\}.
\]

5. Extended Norm–Trace codes

The extended Norm–Trace curve and their associated linear codes were introduced in [11]. Our definition varies slightly from the definition therein. First we need some facts about linearized polynomials. In order to simplify our statement of the definitions, we shall assume \(L(Y)\) is a particular linearized polynomial defined as follows:

Definition 16 ([11] Definition 3.49, page 99]). A \(q\)-polynomial over \(\mathbb{F}_q\) is polynomial of the form \(L(Y) = \sum_{i=0}^{d} a_i Y^{q^i}\). Such a polynomial is also called a linearized polynomial in \(Y\). We define

\[ D_L := \{L(\alpha) \mid \alpha \in \mathbb{F}_q\} \quad \text{and} \quad A_L(Y) := \prod_{\beta \in D_L} (Y - \beta). \]
It can be shown that $L$ is a linear transformation on any extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. In fact, the set $D_L$ is the image of $L$ as a linear transformation from $\mathbb{F}_{q^r}$ to $\mathbb{F}_{q^s}$. From the definition of $A_L$ it is clear that the polynomial $A_L(L(Y))$ evaluates to 0 over $\mathbb{F}_{q^r}$. We say that $A_L$ annihilates $L$ over $\mathbb{F}_{q^r}$. The next proposition shows $A_L$ is a linearized polynomial as well.

**Proposition 9** ([1]) Let $L$ be a linearized polynomial over $\mathbb{F}_{q^r}$ and let $D$ be an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^r}$. The polynomial

$$\prod_{\beta \in D} (Y - \beta)$$

is a separable linearized polynomial.

**Proposition 10** ([1] Theorem 3.50, page 99). Suppose that $L(Y) = \sum_{i=0}^{d} a_i Y^{q^i}$ is a linearized polynomial in $\mathbb{F}_{q^r}$ such that $a_d, a_0 \neq 0$. Then:

- The polynomial $L(Y)$ is separable.
- The map $\alpha \mapsto L(\alpha)$ is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^r}$ to itself.
- The set $\{\beta \in \mathbb{F}_{q^r} \mid L(\beta) = 0\}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^r}$ of dimension $d' \leq d$.
- The set $\{L(\beta) \mid \beta \in \mathbb{F}_{q^r}\}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^r}$ of dimension $r - d'$.
- The evaluation map $\alpha \mapsto L(\alpha)$ is a $q^{d'}$-to-1 map.
- $Y^{q^r} - Y$ divides $A_L(L(Y))$.

**Definition 17** ([1]). Let $L$ be a linearized polynomial over $\mathbb{F}_{q^r}$ of degree $q^d$. Suppose that $u | q^r - 1$. The curve

$$NT_{u,L}(X,Y) : X^u - L(Y) = 0$$

is known as an Extended Norm–Trace curve over $\mathbb{F}_{q^r}$. Denote by

$$NT_{u,L}(\mathbb{F}_{q^r}) := \{(x,y) \in \mathbb{F}_{q^r}^2 \mid x^u = L(y)\}$$

the set of $\mathbb{F}_{q^r}$-rational points of $NT_{u,L}(X,Y)$.

When $u = \frac{q^r - 1}{q^d}$ and $L(Y) = T_{\mathbb{F}_{q^r}/\mathbb{F}_q}(Y)$ the curve is a Norm–Trace curve. When $r = 2$ and $d = 1$ the curve is equivalent to a quasi–Hermitian curve. In [1] the authors also give an additional condition on $u$. Namely, that there exists $v | q^d - 1$ such that $u | v$ and that all $v$ powers of the elements of $\mathbb{F}_{q^r}$ are contained in $D_L = \{L(\beta) \mid \beta \in \mathbb{F}_{q^r}\}$. This is done to find the exact number of points in $NT_{u,L}(\mathbb{F}_{q^r})$.

We shall consider a more general case. Our approach will be to bound or estimate the number of $\mathbb{F}_{q^r}$-rational points by considering the polynomial $A_L(X^u)$.

**Lemma 18.** Let $L$ be a linearized, separable polynomial in $\mathbb{F}_q$ of degree $q^d$ where $\{\beta \in \mathbb{F}_{q^r} \mid L(\beta) = 0\}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^r}$ of dimension $d$. Suppose that $u | q^r - 1$ and suppose that $h(X)$ is the greatest common divisor of $A_L(X^u)$ and $X^{q^d} - X$. Then the number of $\mathbb{F}_{q^r}$-rational points of $X^u - L(Y)$ is $\deg(h) q^d$.

**Proof.** Let $L(Y)$ be as in the hypothesis. By the definition of $A_L$, the elements $\{L(\beta) \mid \beta \in \mathbb{F}_{q^r}\}$ are precisely the roots of $A_L(Y)$. Suppose that $x \in \mathbb{F}_{q^r}$ and $y \in \mathbb{F}_{q^r}$ satisfy $x^u = L(y)$. Then $x^u \in \{L(\beta) \mid \beta \in \mathbb{F}_{q^r}\}$. Therefore $A_L(x^u) = 0$. As $L(Y)$ is an $q^d$-to-1 function, for each root, $x$, of $h(X)$ there are $q^d$ elements $y \in \mathbb{F}_{q^r}$ such that $x^u = L(y)$. Thus, there are $\deg(h) q^d$ solutions to $X^u - L(Y)$.

---

**Advances in Mathematics of Communications** Volume 11, No. 2 (2017), 379–388

---

**Hearalal Janwa and Fernando L. Piñero**
Let $\text{Theorem 19.}$

In fact, for $L(Y) = \bar{T}_{F_{q^r}/F_q}(Y)$, $A_L(Y)$ is equal to $Y^g - Y$.

In the next theorem, we find a good basis for the ideal $I_{NT_{u,L}(F_{q^r})}$. We prove this by stating that a certain ideal is contained in $I_{NT_{u,L}(F_{q^r})}$. Then we prove that both ideals have the same footprint, which implies equality.

**Theorem 19.** Let $L$ be a linearized, separable polynomial in $F_{q^r}$ of degree $q^d$ where \{\beta \in F_{q^r} \mid L(\beta) = 0\} is an $F_q$-linear subspace of $F_{q^r}$ of dimension $d$. Suppose that \(u \mid q^r - 1\) and that $h(X)$ is the greatest common divisor of $A_L(X^u)$ and $X^{q^d} - X$. Then $I_{NT_{u,L}(F_{q^r})}$ is generated by $X^u - L(Y)$ and $h(X)$.

**Proof.** Let $J = (X^u - L(Y), h(X))$. Lemma [18] implies the polynomials $X^u - L(Y)$ and $h(X)$ vanish on the points in $NT_{u,L}$. Therefore $\#NT_{u,L} \leq \Delta \Delta h(J)$. Let $\prec$ be a monomial order where $X^u \prec Y^{q^d}$. As $X^{deg \circ}$ and $Y^{q^d}$ are leading terms of polynomials in $J$, then $\# \Delta \Delta h(J) \leq q^d \deg h$. Note that $J \subseteq I_{NT_{u,L}}$. Which implies $F_{q^r}[X,Y]/I_{NT_{u,L}} = F_{q^r}[X,Y]/J$ as $q^d \deg h = \# \Delta \Delta h(I_{NT_{u,L}}) \leq \# \Delta \Delta (J) \leq q^d \deg h$.

Therefore $\dim_{F_{q^r}} F_{q^r}[X,Y]/J = \dim_{F_{q^r}} F_{q^r}[X,Y]/I_{NT_{u,L}}$. This implies $J = I_{NT_{u,L}}$, which is what we wanted to prove.

**Definition 20.** For any nonnegative integer $s$, the extended Norm–Trace code of weight $s$ is defined as $\text{NT}_{u,L}(s) := C(\text{NT}_{u,L}(F_{q^r}), \mathcal{M}_{u,q^d}(s))$.

### 6. Dimension of Subfield Subcodes of Extended Norm–Trace Codes

We aim to either find the exact value or bound the dimension of $\text{NT}_{u,L}(s)|F_t$. As $\text{NT}_{u,L}(s)$ is an affine variety code, Lemma [19] implies that $\bar{T}_{F_{q^r}/F_t}(\text{NT}_{u,L}(s))$ is also an affine variety code. Our aim is to find a bound for $\dim_{F_t}(\bar{T}_{F_{q^r}/F_t}(\text{NT}_{u,L}(s)))$. We shall determine the kernel of the evaluation of the functions in $\sum_{i=0}^{m-1} (\mathcal{M}_{q^r-1,u}(s)(i))^i$ on the points of $\text{NT}_{u,L}$. Luckily, we have already computed a Gröbner basis for the ideal of polynomial functions which vanish on $\text{NT}_{u,L}(F_{q^r})$.

**Theorem 21.** Let $L$ be a linearized, separable polynomial in $F_{q^r}$ of degree $q^d$ where \{\beta \in F_{q^r} \mid L(\beta) = 0\} is an $F_q$-linear subspace of $F_{q^r}$ of dimension $d$. Suppose that \(u \mid q^r - 1\) and that $h(X)$ is the greatest common divisor of $A_L(X^u)$ and $X^{q^d} - X$. Let $f(X,Y)$ be a polynomial spanned by the monomials in $\mathcal{M}_{u,q^d}(s)$. Suppose that $g$ is the remainder of $f$ after dividing by $h(X)$ and $X^u - L(Y)$ under a monomial ordering where $Y^{q^d}$ is the leading monomial of $X^u - L(Y)$. Then $g(X,Y) \in \mathcal{M}_{u,q^d}(s)$.

**Proof.** If one divides the monomial $X^iY^j$ by $X^u - L(Y)$, the leading term is $X^{i+iu}Y^{j-lq^d}$ where $d$ is the quotient when dividing $j$ by $q^d$. Note that the monomials $X^iY^j$ and $X^{i+iu}Y^{j-lq^d}$ have the same $(q^d, u)$-weight. Thus polynomial division by $X^u - L(Y)$ also preserves the $(q^d, u)$-weight. Clearly when one divides any polynomial by the univariate polynomial $h(X)$, the $(q^d, u)$-weight may not increase.

Extending the argument of [11], we can find a lower bound of the minimum distance of $\text{NT}_{u,L}(s)$ from the theory of order domain codes. We use the following minimum distance bound from [10].

---

*Parameters of subfield subcodes of extended norm-trace codes* 385

*Advances in Mathematics of Communications* Volume 11, No. 2 (2017), 379–388
Proposition 11 (6). Let \( L \) be a linearized, separable polynomial in \( \mathbb{F}_{q^r} \) of degree \( q^d \) where \( \{ \beta \in \mathbb{F}_{q^r} \mid L(\beta) = 0 \} \) is an \( \mathbb{F}_q \)-linear subspace of \( \mathbb{F}_{q^r} \) of dimension \( d \). Suppose that \( u|q^d - 1 \) and that \( h(X) \) is the greatest common divisor of \( A_L(X^s) \) and \( X^q - X \). Denote by \( \Delta \) the footprint of \( I_{NT_u,L}(\mathbb{F}_{q^r}) \) under lexicographical order where \( Y > X \). For a nonnegative integer \( s \), let \( M'_{u,q^d}(s) = M_{u,q^d}(s) \cap \Delta \). Then the minimum distance of \( NT_{u,L}(s) \) satisfies:

\[
d(NT_{u,L}(s)) \geq \min_{p \in M'_{u,q^d}(s)} |\{K \in \Delta \mid \exists N \in \Delta \text{ s.t. } \rho_{u,q^d}(N) + \rho_{u,q^d}(P) = \rho_{u,q^d}(K)\}|
\]

And the minimum distance of \( NT_{u,L}(s) \vdash \) satisfies:

\[
d(NT_{u,L}(s) \vdash) \geq \min_{p \in \Delta \setminus M'_{u,q^d}(s)} |\{K \in \Delta \mid \exists K' \in \Delta \text{ s.t. } \rho_{u,q^d}(K) + \rho_{u,q^d}(P) \in \Delta\}|
\]

This lower bound is a BCH-like bound. We use this lower bound to estimate the minimum distance of some subfield subcodes of extended Norm–Trace codes as in the following examples.

7. Search for good subfield subcodes of extended Norm–Trace codes

In order to find the parameters of \( NT_{u,L}(s) \vdash [F_{q^r}] \), we use the minimum distance of the supercode \( NT_{u,L}(s) \vdash \) itself as a lower bound on the minimum distance of the subfield subcode. The reason we have chosen to work with the subfield subcode of the dual code, \( NT_{u,L}(s) \vdash [F_{q^r}] \), rather than with the subfield subcode of the primary code \( NT_{u,L}(s)[F_{q^r}] \), is that it is quite difficult to work with \( NT_{u,L}(s)[F_{q^r}] \) directly. Delsarte’s theorem allows us to find the dimension of \( T_{F_{q^r}/F_r}, NT_u(L) \), which can be done by looking at the different \( t \) powers of the monomials in \( M_{u,q^d}(s) \) reduced modulo the ideal of \( NT_{u,L} \).

7.1. The case \( L(Y) = T_{F_{q^r}/F_r}(Y) \) and \( u|q^n - 1 \) over the field \( \mathbb{F}_{q^r} \). In this case, \( L(Y) = T_{F_{q^r}/F_r}(Y) \). Since \( L(Y)^q - L(Y) = Y^{q^r} - Y \), the polynomial \( A_L(Y) = Y^{q^r} - Y \). If \( u|q^n - 1 \), then \( u(q - 1)|q^r - 1 \). The greatest common divisor of \( A_L(X^s) \) and \( Y^{q^r} - X \) is \( A_L(X^u)/X^{u-1} = X^{u(q-1)+1} - X \). Therefore the length of the codes is \( n = q^r - 1(u(q - 1) + 1) \).

7.1.1. Binary subcodes. First we consider the extended Norm–Trace curve given by \( u = 3 \) and \( L(Y) = T_{F_{16}/F_2}(Y) \) over \( \mathbb{F}_{16} \). We would like to find \( \dim NT_{3,T_{F_{16}/F_2}}(36)[F_2] \). In this case \( NT_{3,T_{F_{16}/F_2}}(36) \vdash = NT_{3,T_{F_{16}/F_2}}(8) \). Note that \( M_3(8) = \{1, Y, Y^2, X\} \). Thus \( M_{3,8}(8) \vdash \) is spanned by \( 1, Y, Y^2, Y^4, Y^8, X, X^2, X^4, X^8 \). Now we reduce these monomials modulo \( NT_{3,T_{F_{16}/F_2}}(36) \vdash \), which is the ideal generated by the polynomials \( X^4 + X + X^3 + Y^8 + Y^4 + Y^2 + Y \). In this case \( X^4 \) is equivalent to \( X, X^8 \) is equivalent to \( X^2 + Y + Y^2 + Y \). We find that \( T_{F_{16}/F_2}(M_{3,8}(8)) \) is generated by \( 1, Y, Y^2, Y^4, X^3, X, X^2 \). Thus \( \dim NT_{3,T_{F_{16}/F_2}}(36)[F_2] = 7 \) and \( \dim NT_{3,T_{F_{16}/F_2}}(36)[F_2] = 25 \). Following Geil [9], the code \( NT_{3,T_{F_{16}/F_2}}(36) \) has minimum distance at least 3. However, as \( T_{F_{16}/F_2}(NT_{3,T_{F_{16}/F_2}}(8)) \) contains the all ones codeword, all codewords of \( NT_{3,T_{F_{16}/F_2}}(36)[F_2] \) have even weight. From the table of Grassl [9] we determine that \( NT_{3,T_{F_{16}/F_2}}(36)[F_2] \) is an optimal \([32, 25, 4]\) binary code.

Now we consider the extended Norm–Trace curve given by \( L(Y) = T_{F_{16}/F_2} \) and \( u = 5 \) over \( \mathbb{F}_{16} \). The code \( NT_{5,T_{F_{16}/F_2}}(65) \) has parameters \([48, 44, 3]\) over \( \mathbb{F}_{16} \). The dual code is \( NT_{5,T_{F_{16}/F_2}}(65) \vdash = NT_{5}(10) \). In this case \( M_{5.8}(10) = \{1, Y, Y^2, X\} \).
The set $\mathcal{M}_{5,8}(10)^\wedge$ is spanned by the monomials $1, Y, Y^2, Y^4, Y^8, X, X^2, X^4, X^8$. By considering reductions modulo $X^6 + X$ and $X^5 + Y^8 + Y^4 + Y^2 + Y$ we find that $Y^8$ is equivalent to $X^3 + Y^4 + Y^2 + Y$ and $X^8$ is equivalent to $X^3$. Therefore the evaluation of $Y^8$ is a linear combination of the evaluation of the remaining monomials in $\mathcal{M}_{5,8}(10)^\wedge$ and we obtain that $\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(10))$ is generated by $\{1, Y, Y^2, Y^4, X, X^2, X^4, X^5\}$. Thus $\dim\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(10)) = 8$ and $\dim\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(10)) = 40$. As in the previous example, the code $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(10))$ has minimum distance at least 3. However as $\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(10))$ contains the all ones codeword, the code $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(10))$ is an optimal [48, 40, 4] binary code.

7.1.2. Quaternary subcodes. For the curve $X^5 + Y^8 + Y^4 + Y^2 + Y$ we will study the codes $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(60))$ and $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(62))$. Geil’s bound on the minimum distance implies that we $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(60))$ and $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(62))$ are codes over $\mathbb{F}_{16}$ with parameters $[48, 43, 3]$ and $[48, 44, 3]$ respectively. If one reduces the monomials in $\mathcal{M}_{5,8}(60)^{(4)}$ modulo the ideal $\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(60))$ one finds that the reductions of the 43 monomials are contained in $\mathcal{M}_{5,8}(60)$. Therefore the code $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(60))$ is invariant under the Frobenius automorphism $x \mapsto x^4$. This implies that the code $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(60))$ is equal to $\mathcal{N}\mathcal{T}_{\mathbb{F}_{16}/\mathbb{F}_2}(\mathcal{M}_{5,8}(60))^{\otimes 2}$ and there exists a $[48, 43, 3]$ optimal quaternary code. The reductions of the monomials in $\mathcal{M}_{5,8}(62)^{(4)}$ are also contained in $\mathcal{M}_{5,8}(62)$. The same argument implies that there is also an optimal $[48, 44, 3]$ quaternary code.

7.2. The case $L(Y) = Y^8 + Y$ over the field $\mathbb{F}_{64}$. This case corresponds to a subcover of the Hermitian curve over $\mathbb{F}_{64}$. In this case $A_L(Y) = Y^8 - Y$. We shall suppose that $u = 3$. The greatest common divisor of $A_L(X^3) = X^{24} - X^3$ and $X^{64} - X$ is $A_L(X^3)/X^2 = X^{22} - X$. Therefore the length of the codes is $n = 176$.

7.2.1. Binary subcodes. We would like to find $\dim(\mathcal{N}\mathcal{V}_{\mathbb{F}_{64}}(L(8)^\perp))\mathbb{F}_2$. Note that $\mathcal{M}_{4,8}(8) = \{1, Y, Y^2, X\}$. Thus $\mathcal{M}_{4,8}(8)^\perp$ contains $1, Y, Y^2, X, X^2$. Geil’s bound implies that the minimum distance of $C(\mathcal{N}\mathcal{V}_{\mathbb{F}_{64}}(L(8)^\perp), \mathcal{M}_{4,8}(8))$ is at least 4. By looking at the different 2-powers of 1, Y, and X, we obtain that the dimension of $C(\mathcal{N}\mathcal{V}_{\mathbb{F}_{64}}(L(8)^\perp), \mathcal{M}_{4,8}(8))$ is at least $176 - 1 - 2(6) = 163$. A binary code with parameters [176, 163, 4] is optimal.

The binary and quaternary codes found in this section have optimal minimum distance for their given dimension or have the best known minimum distance [8].

7.3. ENT codes for applications. We find binary subfield subcodes of very large lengths for modern applications—for example to Flash Memories [4]. The binary subfield subcode of the extended Norm-Trace curves,

$$X^m = Y^{128} + Y^{64} + Y^{32} + Y^{16} + Y^8 + Y^4 + Y^2 + Y$$

over $\mathbb{F}_{256}$ yields a binary [11008, 8923, 110] code. These types of codes are needed in several applications (for example, in flash memories see [4]). To use a binary code of comparable parameters, $(r, \delta) = (8923/11008, 110/11008)$, one would have to use a code of much larger length, for example a [16383, 15612, 110] BCH code. It is possible to shorten such a BCH code, but that would degrade the parameters while interfering with decoding. Also, there are no corresponding BCH codes that could lead to codes of length 11008 and rate $< 5375/11008$. Therefore, by our subfield subcodes of extended Norm–Trace codes, we are able to obtain a vast array of codes that have substantial practical applications as well.
ACKNOWLEDGMENTS

The authors would like to thank Domingo Gómez, Tom Høholdt and the reviewers for helpful suggestions.

REFERENCES

[1] M. Bras-Amorós and M. E. O’Sullivan, Extended norm-trace codes with optimized correction capability in *Int. Symp. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer, 2007, 337–346.

[2] D. A. Cox, J. Little and D. O’Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, 2007.

[3] J. Fitzgerald and R. F. Lax, Decoding affine variety codes using Gröbner bases, *DCC*, 13 (1998), 147–158.

[4] E. E. Gad, W. Huang, Y. Li and J. Bruck, Rewriting flash memories by message passing, 2016, US Patent App. 15/011,537.

[5] O. Geil, On codes from norm-trace curves *Finite Fields Appl.*, 9 (2003), 351–371.

[6] O. Geil, Evaluation codes from an affine variety code perspective in *Advances in Algebraic Geometry Codes*, World Scientific, 2008.

[7] O. Geil and T. Hoholdt, Footprints or generalized bezout’s theorem *IEEE Trans. Inf. Theory*, 46 (2006), 635–641.

[8] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, available at http://www.codetables.de

[9] H. Janwa and F. Piñero, On the parameters of subfield subcodes of norm-trace codes, *Congr. Numerant.*, 206 (2010), 99–113.

[10] R. Lidl and H. Niederreiter, *Finite fields*, in *Encyclopaedia of Mathematics and Its Applications*, Cambridge Univ. Press, 1997.

[11] F. L. Piñero and H. Janwa, On the subfield subcodes of Hermitian codes *Des. Codes Crypt.*, 70 (2014), 157–173.

[12] H. Stichtenoth, On the dimension of subfield subcodes *IEEE Trans. Inf. Theory*, 36 (1990), 90–93.

Received February 2016; revised March 2016.

E-mail address: hjanwa@gmail.com
E-mail address: pinerofernando@gmail.com