ON THE DIMENSION OF AG TRACE CODES

PHONG LE AND DAIQING WAN

ABSTRACT. We determine the dimension of certain $q$-ary algebraic-geometric trace codes, extending previous results of Van Der Vlugt for $p$-ary algebraic-geometric trace codes.

1. INTRODUCTION

Many good error correcting codes over a finite field $\mathbb{F}_q$ can be constructed from another existing code using the trace map. More commonly, Delsarte’s Theorem is used to describe subfield subcodes as the dual of trace codes [2]. BCH-codes, classical Goppa codes and their generalizations, and alternant codes all can be realized as the dual of trace codes. An important parameter of error correcting codes is the dimension.

Algebraic-geometric (AG) codes over $\mathbb{F}_q$ arise from the evaluation of the elements of an $\mathbb{F}_{q^m}$-vector space of functions in a set of $\mathbb{F}_{q^m}$ rational points on a curve $X$ defined over $\mathbb{F}_{q^m}$. We shall consider trace codes over $\mathbb{F}_q$ obtained from algebraic-geometric codes over $\mathbb{F}_{q^m}$ by taking the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Under a mild condition, the dimension of an AG code can be easily determined via the Riemann-Roch theorem. However, the dimension of an AG trace code is generally quite complicated to determine. For instance, the dimension of the classical Goppa codes is already not known in general. A partial general result of Van Der Vlugt gives the dimension formula for certain $p$-ary AG trace codes, when the ground field is the prime field of $p$ elements. In fact, most of the deeper properties on AG trace codes seem to restrict to the case when the ground field is the prime field of $p$ elements, see [3] for an exposition.

The aim of this paper is to extend Van Der Vlugt’s results from $p$-ary trace codes to $q$-ary trace codes, that is, we allow the ground field to be any finite field of $q$ elements. Significant modifications of his proof are needed to accommodate the more generalized trace in the execution of Bombieri’s estimate for exponential sums [1]. Our main new idea is the proof of Lemma 3.4, which is clear if $q = p$ but non-trivial for a general prime power $q$. It is possible that our new technique to handle the general trace can be useful to study other deeper properties of AG trace codes.

2. DEFINITION OF CODE AND MAIN RESULT

Let $p$ be a prime number and $q = p^e$. Given a linear code $C$ of length $n$ over the extension field $\mathbb{F}_{q^m}$, where $m \geq 2$ is a positive integer, one way to construct a new code over the ground field $\mathbb{F}_q$ is to apply the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ to the letters of the words of $C$. This $q$-ary code is denoted $\text{Tr}_{q^m/q} C$ or just $\text{Tr} C$ if the base fields in question are clear.
Let $X$ be a geometrically irreducible, non-singular projective curve of genus $g$ defined over $\mathbb{F}_{q^m}$. Denote the function field of $X$ by $\mathbb{F}_{q^m}(X)$. A divisor $G = \sum n_Q Q$, defined over $\mathbb{F}_{q^m}$, may split into two divisors $G^+$ and $G^-$ where $G^+ = \sum_{n_Q > 0} n_Q Q$ and $G^- = \sum_{n_Q < 0} n_Q Q$. Hence $G = G^+ + G^-$ separating $G$ in terms of positive and negative coefficients. Define $\mathcal{L}(G)$ to be the vector space of functions $L(G) = \{ f \in \mathbb{F}_{q^m}(X) \mid (f) + G \geq 0 \} \cup \{0\}$.

To generate a linear code from $\mathcal{L}(G)$, we take a subset of $n$ distinct $\mathbb{F}_{q^m}$-rational points away from the poles of $\mathcal{L}(G)$:

$$D := \{ P_1, \ldots, P_n \} \subseteq X(\mathbb{F}_{q^m}) \setminus \text{Supp}(G^+)$$

where for a divisor $G$ we denote the support of $G$ to be $\text{Supp}(G) := \{ Q \mid n_Q \neq 0 \}$. Usually, $D$ is taken to be the largest possible set

$$D_{\text{max}} := X(\mathbb{F}_{q^m}) \setminus \text{Supp}(G^+).$$

We define our AG code over $\mathbb{F}_{q^m}$ to be

$$C := C(D, G) = \{ (f(P_1), \ldots, f(P_n)), f \in \mathcal{L}(G) \}.$$ In the most interesting case $D = D_{\text{max}}$, we denote $C$ by $C_{\text{max}}$.

When $2g - 2 < \deg(G) < n$, by a theorem of Riemann and Roch we have

$$k := \dim_{\mathbb{F}_{q^m}}(\mathcal{L}(G)) = \deg(G) + 1 - g.$$ Since $\deg(G) \leq n$, the dimension of $C$ as a $\mathbb{F}_{q^m}$-vector space is also $k$. In this way we can identify $f$ with its image in $C$.

An AG trace code is defined as the coordinate-wise application of the trace map

$$\text{Tr}C := \{ (\text{Tr}_{q^m/q}(f(P_1)), \ldots, \text{Tr}_{q^m/q}(f(P_n))), f \in \mathcal{L}(G) \}.$$ Consider the divisor $[G/q] := \sum_{n_Q > 0}[n_Q/q] Q + \sum_{n_Q < 0} n_Q Q$ where $[x]$ denotes the greatest integer that is less or equal to $x$. This construction will be useful in determining the kernel of the trace map.

Section 3 is devoted to the proof of the following dimension formula for $\text{Tr}C_{\text{max}}$:

**Theorem 2.1.** Let $2g - 2 \leq \deg([G/q])$. Assume the following:

(1) \hspace{1cm} \#\text{Supp}(G^-) \leq 1,

(2) \hspace{1cm} \#X(\mathbb{F}_{q^m}) > (2g - 2 + \deg(G^+))q^{m/2} + \text{Supp}(G^+)(q^{m/2} + 1).

Then, we have

$$\dim_{\mathbb{F}_q}(\text{Tr}C_{\text{max}}) = m(\deg(G) - \deg([G/q])) + \delta,$$

where

$$\delta = \begin{cases} 1 & \text{if } \#\text{Supp}(G^-) = 0, \\ 0 & \text{otherwise}. \end{cases}$$

If $q = p$, this theorem reduces to the main result of [4].
2.1. Examples.

Example 2.2. For a smooth projective curve $X$ defined over $\mathbb{F}_{q^m}$, let $G = kP_\infty$ for $k \in \mathbb{Z}_{\geq 0}$, where $P_\infty \in X(\mathbb{F}_{q^m})$. By the Hasse-Weil bound, we have
\[
|\#X(\mathbb{F}_{q^m}) - (q^m + 1)| \leq 2gq^{m/2}.
\]

By (2) we want
\[
\#X(\mathbb{F}_{q^m}) > (2g - 2 + k)q^{m/2} + (q^{m/2} + 1).
\]
Combining these two inequalities, we see that (2) is satisfied when
\[
q^{m/2} - 4g + 1 > k.
\]

Using Theorem 2.1 we obtain the following:

Corollary 2.3. For $X$ a smooth projective curve over $\mathbb{F}_{q^m}$ and $G = kP_\infty$ with $P_\infty \in X(\mathbb{F}_{q^m})$, if $(2g - 2)q \leq k < q^{m/2} - 4g + 1$, then
\[
\dim_{\mathbb{F}_q} \text{TrC}_{\text{max}} = m(k - [k/q]) + 1.
\]

Example 2.4. This example is a generalization from an example in [4], which has applications to classical Goppa codes. Let $q = p^r$, $X = \mathbb{P}^1$ and $G = (g)_0 - P_\infty$ where $(g)_0$ is the zero divisor of a polynomial $g(z) \in \mathbb{F}_{q^m}[z]$ which has no zeros in $\mathbb{F}_{q^m}$. Denote the number of different zeros of $g(z)$ by $s$. Furthermore, we take $D = D_{\text{max}} = \sum_{x \in \mathbb{F}_{q^m}} P_x$. The condition (2) is clearly satisfied if
\[
\deg(g(z)) + 2s < \frac{q^m + 1}{\sqrt{q^m}} + 2.
\]
Write $g(z) = g_1^q g_2$, with $g_1(z), g_2(z) \in \mathbb{F}_{q^m}[z]$ of degrees $r_1, r_2$ respectively, and $g_2(z)$ $q$-th power free. With these conditions, Theorem 2.1 states:
\[
\dim_{\mathbb{F}_q} \text{TrC}_{\text{max}} = m((q - 1)r_1 + r_2).
\]

3. Proof of Theorem 2.1

3.1. Bounding the dimension. Since $C$ is a vector space over $\mathbb{F}_{q^m}$ and $\text{TrC}$ is a vector space over $\mathbb{F}_q$, we immediately have the bound
\[
\dim_{\mathbb{F}_q}(C) \leq \dim_{\mathbb{F}_q}(\text{Tr}(C)) \leq m(\dim_{\mathbb{F}_q}(C)).
\]
The trace map is $\mathbb{F}_q$-linear. Thus, we have an exact sequence
\[
0 \to K \to C \to \text{TrC} \to 0,
\]
where $K$ is the kernel, an $\mathbb{F}_q$-linear subspace of $C$. Hence
\[
(3) \quad m\dim_{\mathbb{F}_q}(C) - \dim_{\mathbb{F}_q}K = \dim_{\mathbb{F}_q}(\text{Tr}(C)).
\]
Therefore, to understand the dimension of $\text{TrC}$ we can instead understand $\dim_{\mathbb{F}_q}K$. Using Hilbert 90 as a guide, we observe that functions of the form $h^q - h$ must be in $K$. Functions of this form are a subspace of $K$ denoted by $E$. More formally:
\[
E := \{ f = h^q - h \mid f \in \mathcal{L}(G), h \in \mathbb{F}_{q^m}(X) \}.
\]

We will determine a sufficient condition when $E = K$. But to make this useful we first find conditions to determine the dimension of $E$. 
3.2. The dimension of $E$. Observe $(h^q - h) + G \geq 0$ when $f = h^q - h \in \mathfrak{L}(G)$. Therefore $f$ has $q$ times as many poles as $h$ does, counting multiplicity. For $h \in \mathfrak{L}((G/q))$, we have $h^q - h \in \mathfrak{L}(G)$.

Consider the map $\phi : \mathfrak{L}((G/q)) \to E$ where $\phi(h) = h^q - h$. Using a degree argument we know the kernel is $\mathbb{F}_q \cap \mathfrak{L}((G/q))$. However $\phi$ may not be surjective.

If $G^- = \emptyset$, that is, there is no requirement on zeros to be in $\mathfrak{L}(G)$, then $\phi$ is clearly onto. More generally, observe $h^q - h = \prod_{b \in \mathbb{F}_q} (h - b)$. If $\# \text{Supp}(G^-) = 1$, then every function $f = h^q - h \in E$ must have a zero at some point $P \in \text{Supp}(G^-)$. This zero must occur in some factor $h - b$ for some $b \in \mathbb{F}_q$. Therefore, while $h$ may not be in $\mathfrak{L}((G/q))$, $h - b$ will for some $b \in \mathbb{F}_q$. Since $h^q - h = (h - b)^q - (h - b)$ we see that if $\#G^- \leq 1$ then $\phi$ is always surjective. Note that the zeros of $h - a$ and $h - b$ must be distinct for $a \neq b$, this allows coefficients of $G^-$ to be greater than 1.

If $G^- = \emptyset$, then the kernel of $\phi$ is $\mathbb{F}_q$. If $G^- \neq \emptyset$, then $\phi$ is injective. Therefore $\delta = \dim_{\mathbb{F}_q}(\ker \phi)$ and we have the following proposition.

**Proposition 3.1.** If $\# \text{Supp}(G^-) \leq 1$, then the sequence

$$0 \to \mathbb{F}_q \cap \mathfrak{L}((G/q)) \to \mathfrak{L}((G/q)) \overset{\phi}{\to} E \to 0$$

is exact. Therefore we have a dimension formula for $E$:

$$\dim_{\mathbb{F}_q} E = \dim_{\mathbb{F}_q} \mathfrak{L}((G/q)) - \dim_{\mathbb{F}_q} (\mathbb{F}_q \cap \mathfrak{L}((G/q))).$$

Note that the condition in the above proposition is exactly condition [1] from Theorem 2.1.

Even if $\phi$ is not exact we still have derived the known dimension bound:

$$\dim_{\mathbb{F}_q} E \geq \dim_{\mathbb{F}_q} \mathfrak{L}((G/q)) - \dim_{\mathbb{F}_q} (\mathbb{F}_q \cap \mathfrak{L}((G/q))).$$

So now we know exactly what $E$ is under certain restrictions.

3.3. **Conditions when $K = E$.** Our primary tool for discerning when $K = E$ is an estimate developed by Bombieri [1]. For this purpose, we assume from now on that $D = D_{\text{max}}$ and thus $C = C_{\text{max}}$.

**Theorem 3.2** (Bombieri’s estimate). Let $X$ be a geometrically irreducible, nonsingular projective curve of genus $g$, defined over $\mathbb{F}_q$. Let $f \in \mathbb{F}_q(X), f \neq h^p - h$ for $h \in \mathbb{F}_q(X)$, with pole divisor $(f)_\infty$ on $X$. Then

$$\left| \sum_{P \in \text{Supp}(e_0(f))] (f)_\infty} \zeta_p \right| \leq (2g - 2 + t + \deg(f)_\infty) q^{m/2},$$

where $\zeta_p = \exp(2\pi i / p)$ is a primitive $p$-th root of unity and $t$ is the number of distinct poles of $f$ on $X$.

Suppose $K \neq E$. Lemma 3.3 below shows that there is always an $f \in K \setminus E$ not of the form $h^p - h$ for any $h \in \mathbb{F}_q(X)$. In other words, $f$ satisfies the conditions of Bombieri’s estimate. Since elements of $K$ maximize the left-hand side of Bombieri’s estimate we have the inequality

$$\#(X(\mathbb{F}_q) \setminus (f)_\infty) \leq (2g - 2 + t + \deg(f)_\infty) q^{m/2}.$$ 

This inequality implies the following proposition:
Lemma 3.3. If
\[ \#X(\mathbb{F}_q^m) > (2g - 2 + \deg(G^+))q^{m/2} + \#\text{Supp}(G^+)(q^{m/2} + 1), \]
then \( K = E \).

Note that the hypothesis of this proposition is condition (2) from Theorem 2.1. This proposition, combined with Proposition 3.1, will provide exact conditions to determine the dimension of \( \text{TrC}_{\max} \).

Lemma 3.4. Suppose \( K \neq E \). Then there is an \( f \in K \setminus E \) not of the form \( h^p - h \) where \( h \in \mathbb{F}_q(X) \).

To prove Lemma 3.4 the following definition is useful.

Definition 3.5. Let \( D(f) \) be the set of elements \( y \in \mathbb{F}_q \) such that \( yf = h^p - h \) for some \( h \in \mathbb{F}_q(X) \).

In other words, \( y \in D(f) \) if and only if \( yf \) is of the form that does not satisfy the conditions of Bombieri’s estimate. Since \( K \) is an \( \mathbb{F}_q \)-vector space, to prove Lemma 3.4 it suffices to show that \( |D(f)| < q \) for some \( f \).

For \( y \in \mathbb{F}_q \) and \( h \in \mathbb{F}_q(X) \),
\[ y(h^q - h) = (yh)^q - (yh) \]
\[ = (yh)^p - (yh) \]
\[ = ((yh)^{p-1} + \ldots + (yh))((yh)^{p-1} + \ldots + (yh)). \]

Therefore, for each \( f \in E \), \( D(f) = \mathbb{F}_q \). This shows we must really be looking in \( K \setminus E \) to use Bombieri’s estimate.

Suppose there is an \( f \in \mathbb{F}_q^m(X) \) and an \( h \in \mathbb{F}_q(X) \) such that \( f = h^p - h \). Take \( \sigma = \text{Frob}_q \), the \( q^m \)-th power Frobenius automorphism on \( \mathbb{F}_q^m \). Since \( \sigma(f) = f \), we may rewrite this so that \( \sigma(h) - h \) is constant. By considering the order of poles of \( \sigma(h) - h \) we determine that \( \sigma(h) - h \) must be a constant \( a \in \mathbb{F}_p \). Let \( a = b^m - b \) for some \( b \in \mathbb{F}_q^m \). Then \( \sigma(b) = b + a \). Also \( \sigma(h - b) = h + a - (b + a) = h - b \), therefore \( h - b \in \mathbb{F}_q^m(X) \). Let \( h_1 = h - b \). Observe \( f - bp + b = h_1^p - h_1 \). Also \( \sigma(b^p - b) = b^p - b \), so \( b^p - b \in \mathbb{F}_q^m \). Hence we obtain the following:

Lemma 3.6. Consider the two sets:
\[ \overline{E} = \{ f \in \mathbb{F}_q^m(X) | f = h^p - h \text{ for some } h \in \mathbb{F}_q(X) \} \]
\[ E_c = \{ f \in \mathbb{F}_q^m(X) | f = h^p - h + c \text{ for some } h \in \mathbb{F}_q^m(X), c \in \mathbb{F}_q \} \]
These two sets are equal.

This allows us to think \( yf \) for \( y \in D(f) \) more concretely. One more definition is useful.

Definition 3.7. Let \( f \in \mathbb{F}_q^m(X) \). Let \( e(f) \) be the largest non-negative integer such that \( f \) can be written in the form
\[ f = a_0 + a_1h + a_2h^p + \ldots + a_{e(f)}h^{p^{e(f)}}, \]
where \( a_i \in \mathbb{F}_q^m \), \( h \in \mathbb{F}_q^m(X) \). Then we say that the \( p \)-linear degree of \( f \) is \( e(f) \).

Lemma 3.8.
\[ |D(f)| \leq p^{e(f)}. \]
Proof. If $e(f) = 0$, then $yf \neq h^p - h + c$, for $y \neq 0$ and any $h \in \mathbb{F}_q^m(X), c \in \mathbb{F}_q^m$. Observe $e(f) = e(af + b)$ where $a \in \mathbb{F}_q^m, b \in \mathbb{F}_q^m$ (linear shift). Therefore, by Lemma 3.6 $D(f) = \emptyset$ and $|D(f)| = 1 \leq p^{e(f)} = p^0 = 1$.

Assume now $e(f) \geq 1$. Without loss of generality, we can assume $|D(f)| > 1$ and $f = h^p - h + a$ for some $h \in \mathbb{F}_q^m(X)$ and $a \in \mathbb{F}_q^m$.

Then for $y \in \mathbb{F}_q, yf = (y^{1/p}h)^p - y^{1/p}h + (y^{1/p} - y)h + ya$. Observe $(y^{1/p}h)^p - y^{1/p}h \not\in \mathbb{F}_q$. Therefore $yf \not\in \mathbb{F}_q$ if and only if $(y^{1/p} - y)h \in \mathbb{F}_q$. Hence we reduce our examination of $D(f)$ to an examination of $D(h)$:

$$D(f) = \{ y \in \mathbb{F}_q \mid y^{1/p} - y \in D(h) \}.$$ Observe $e(f) = 1 + e(h)$. Hence $|D(f)| \leq |D(h)|p$. By induction we know $|D(f)| \leq p^{e(h)+1} = p^{e(f)}$ as desired. □

Corollary 3.9. If $|D(f)| = q = p^r$, then the $p$-linear degree of $f$ is at least $r$.

Corollary 3.10. If $D(f) = \mathbb{F}_q$ and $D(g) = \mathbb{F}_q$, then $D(af + bg) = \mathbb{F}_q$ for each $a, b \in \mathbb{F}_q$.

Now we are in position to prove Lemma 3.4

Proof. Suppose $K \not\subset E$ and $D(f) = \mathbb{F}_q$ for each $f \in K \setminus E$. Such an $f \in \mathbb{F}_q^m(X)$ cannot be constant, since a constant function with trace zero has to be in $E$ already. Choose $f \in K \setminus E$ with the least number of poles, that is, $\deg(f)_\infty$ is minimal and positive. By Cor 3.9 there is some $l \in \mathbb{Z}_\geq 0$, $h \in \mathbb{F}_q^m(X)$ and $a_i \in \mathbb{F}_q^m$ such that

$$f = h^{p^{r+i}} + a_1 h^{p^{r+i-1}} + \ldots + a_{r+i} h + a_{r+i+1}.$$

We may rewrite this as

$$f = (h^p)^q - h^p + f_1,$$

where

$$f_1 = h^p + a_1 h^{p^{r+i-1}} + \ldots + a_{r+i} h + a_{r+i+1} \in \mathbb{F}_q^m(X).$$

Observe $D((h^p)^q - h^p) = \mathbb{F}_q$. By Corollary 3.10 $D(f_1) = \mathbb{F}_q$. But

$$\deg(f_1)_\infty \leq p^{r+i-1} \cdot \deg(h)_\infty$$

and

$$\deg(f)_\infty = p^{r+i} \deg(h)_\infty.$$

This contradicts the choice of an $f$ with minimal poles. The proof is complete. □

References

[1] E. Bombieri. Exponential sums in finite fields. Amer. J. Math., 88 (1966) 71-105.
[2] P. Delsarte. On the subfield subcodes of modified Reed-Solomon codes. IEEE Trans. Inform. Theory., 21 (1975), 575-576.
[3] H. Stichtenoth. Algebraic function fields and codes. Springer-Verlag, 1993.
[4] M. Van Der Vlugt. A new upper bound for the dimension of trace codes. Bull. London Math. Soc., 23 (1991), 395-400.

Department of Mathematics
University of California
Irvine, CA 92697-3875
ple@math.uci.edu
dwan@math.uci.edu