mathematics

MDPI

Article

On the Dimension of Algebraic-Geometric Trace Codes

Phong Le [1,*] and Sunil Chetty [2]

[1] Department of Mathematics and Computer Science, Goucher College, Baltimore, MD 21204, USA

[2] Department of Mathematics, College of Saint Benedict and Saint John's University, Collegeville, MN 56321, USA; schetty@csbsju.edu

* Correspondence: phong.le@goucher.edu; Tel.: +1-410-337-6239

Academic Editor: Hari M. Srivastava
Received: 29 January 2016; Accepted: 22 April 2016; Published: 7 May 2016

Abstract: We study trace codes induced from codes defined by an algebraic curve X. We determine conditions on X which admit a formula for the dimension of such a trace code. Central to our work are several dimension reducing methods for the underlying functions spaces associated to X.

Keywords: error correcting codes; trace codes; exponential sums; number theory

MSC: 11T71

1. Introduction

Many good error correcting codes defined over a finite field can be constructed from other codes using the trace map. More generally, given a code C over a finite field $\mathbb{F}$, one can construct a subfield subcode by restriction (e.g., in the coordinates) to a subfield of $\mathbb{F}$. In [1], Katsman and Tsfasman prove that one can often obtain better parameters than those guaranteed by trivial bounds. Precise lower bounds on the dimension of subfield subcodes have been given in, e.g., [1–3]. Delsarte's Theorem [4] is used to describe subfield subcodes as trace codes. BCH-codes, classical and generalized Goppa codes, and alternant codes can all be realized as the dual of trace codes.

Algebraic-geometric (AG) codes 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. We shall consider trace codes associated to algebraic-geometric codes. In some cases the exact dimension can be determined. As in [5,6] a key ingredient in the present work is understanding the kernel of the trace map. Our use of Bombieri's estimate, following [7], and consideration of a more general class of codes differ from the methods and setting of [5,6].

The main result, Theorem 1, is an extension of results that appear in [7]. The bound in [7] applies for trace maps from the original field to the prime field. We modify this to include trace maps to intermediate fields. Significant modifications of the original proof are needed to accommodate the more general trace in the execution of Bombieri's estimate for exponential sums [8]. The primary modification is summarised in Proposition 17.

For a general introduction on AG codes and trace codes, see [9].

2. Definition of Code and Main Result

2.1. Background

Let p be a prime number and $q = p^r$. Given a linear code C of length n over $\mathbb{F}_{q^m}$, a trace code over $\mathbb{F}_q$ is constructed from C by applying the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ coordinate-wise to the letters of the words of C. This q-ary code is denoted $\mathrm{Tr}_{q^m/q}C$ or simply $\mathrm{Tr}(C)$ if the base fields in question are clear.

Let X be a geometrically irreducible, non-singular projective curve of genus $\mathfrak{g}$ defined over $\mathbb{F}_{q^m}$. Consider $\mathbb{F}_{q^m}(X)$ the $\mathbb{F}_{q^m}$-rational function field of X. Throughout, by a point Q on X we mean $Q \in X(\overline{\mathbb{F}}_q)$ is a geometric point defined over $\overline{\mathbb{F}}_q$. A divisor $G = \sum n_Q Q$ defined over $\mathbb{F}_{q^m}$ is a formal sum over points Q defined over $\mathbb{F}_{q^m}$, and is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^m})$. Any divisor $G = \sum n_Q Q$ may be 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 $G = G^+ + G^-$. The sum $\sum_i n_i$ of the coefficients of G is called the degree of G, denoted $\deg(G)$. We denote the support of G to be $\mathrm{Supp}(G) := \{Q \mid n_Q \neq 0\}$.

Define $L(G)$ 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 code from $L(G)$ we take a subset of n distinct $\mathbb{F}_{q^m}$-rational points away from the support of the divisor G:

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

For our purposes we will take $D = X(\mathbb{F}_{q^m}) \setminus \mathrm{Supp}(G)$ the largest possible set.

We define our AG code to be

$$C := C(D, G) = \{(f(P_1), \ldots, f(P_n)), f \in L(G)\}$$

When $2\mathfrak{g} - 2 < \deg(G)$, by Riemann-Roch we have

$$\dim_{\mathbb{F}_{q^m}} L(G) = \deg(G) + 1 - \mathfrak{g}$$

Since $\deg(G) < n$ the evaluation map

$$\begin{cases} L(G) \to \mathbb{F}_{q^n} \\ f \mapsto (f(P_1), \ldots, f(P_n)) \end{cases}$$

is injective. Hence the dimension of C as an $\mathbb{F}_{q^m}$-vector space is also k. In this way we identify $f \in L(G)$ with its image in C.

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

$$\mathrm{Tr}(C) := \{(\mathrm{Tr}_{q^m/q}(f(P_1)), \ldots, \mathrm{Tr}_{q^m/q}(f(P_n))), f \in L(G)\}$$

2.2. Main Result

For $r \in \mathbb{R}$, let $[r]$ denote the greatest integer function. Consider the divisor

$$[G/q] := \sum_{n_Q>0} [n_Q/q]Q + \sum_{n_Q<0} n_Q Q$$

That is, we are dividing the positive coefficients by q and rounding down to the nearest integer. We are in a sense dividing the pole part of G by q. 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 $\mathrm{Tr}(C)$.

Theorem 1. *Let $2\mathfrak{g} - 2 \leq \deg([G/q])$ and $\deg(G) < n$. Consider the following two conditions:*

$$|\mathrm{Supp}(G^-)| \leq 1 \tag{1}$$

$$|X(\mathbb{F}_{q^m})| > (2\mathfrak{g} - 2 + \deg(G^+))q^{m/2} + |\mathrm{Supp}(G^+)|(q^{m/2} + 1) \tag{2}$$

Under these conditions we have an exact formula for the dimension:

$$\dim_{\mathbb{F}_q} \mathrm{TrC} = m(\deg(G) - \deg([G/q])) + \delta$$

where

$$\delta = \begin{cases} 1 & \text{if } deg(G^-) \leq 1 \\ 0 & \text{otherwise} \end{cases}$$

If q is a prime number, this theorem reduces to the main result of [7]. Theorem 1 is applicable for a more general trace when $q = p^r$ for some prime p and $r > 1$. In this setting, complications arise in the dimension reducing argument using Bombieri's estimate used in [7]. Bombieri's estimate alone does not collapse the dimension of the kernel of the trace map enough. We have addressed these complications with the addition of a degree argument that shows that the kernel can be reduced in a way that aligns with the result in [7].

2.3. Examples

Example 1. Let $q = p^r$. Consider an elliptic curve E defined over $\mathbb{F}_{q^m}$. A formula for counting points on E is given by

$$E(\mathbb{F}_{q^m}) = q^m + 1 - \pi^m - \overline{\pi}^m$$

where $\pi\overline{\pi} = q$ and $\pi + \overline{\pi} = a_p$, the linear coefficient of the numerator of an associated zeta function as described in ([10], p. 301).

For $G = kP_\infty$ we see that condition (2) is

$$q^{m/2} - \frac{\pi^m + \overline{\pi}^m}{q^{m/2}} > k$$

Assuming this, Theorem 1 states that for any D such that $|D| > \deg(G)$ we have

$$\dim_{\mathbb{F}_q} \mathrm{Tr}(C(D,G)) = m(k - [k/q]) + 1$$

Example 2. For a smooth projective curve X defined over $\mathbb{F}_{q^m}$, let $G = kP_\infty$ for some positive integer k. Using the the Hasse-Weil bound we have

$$||X(\mathbb{F}_{q^m})| - (q^m + 1)| \leq 2\mathfrak{g}q^{m/2}$$

By condition (2) of Theorem 1 we must also require the inequality

$$|X(\mathbb{F}_{q^m})| > (2\mathfrak{g} - 2 + k)q^{m/2} + (q^{m/2} + 1)$$

Combining these two inequalities, we see that condition (2) is satisfied when

$$q^{m/2} - 4\mathfrak{g} + 1 > k$$

Using Theorem 1 we obtain the following:

Corollary 2. *For X a smooth projective curve over $\mathbb{F}_{q^m}$ and $G = kP_\infty$, if $2\mathfrak{g} - 2 \leq [k/q]$ and $k < \min(n, q^{m/2} - 4\mathfrak{g} + 1)$ then*

$$\dim_{\mathbb{F}_q} \mathrm{Tr}(C) = m(k - [k/q]) + 1$$

Example 3. This is a generalization from an example in [7]. 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 $D = \sum_{x \in \mathbb{F}_{q^m}} P_x$. From condition (2) we obtain the inequality

$$\deg(g(z)) + s < \frac{q^m + 1}{\sqrt{q^m}} + 2$$

Write $g(z) = g_1^q g_2$, where $g_1(z), g_2(z) \in \mathbb{F}_{q^m}[z]$ of degrees r_1, r_2 respectively, and $g_2(z)$ q-th power free. With sufficiently many points as above, applying Theorem 1 we have

$$\dim_{\mathbb{F}_q} \operatorname{Tr}(C(D,G)) = m((q-1)r_1 + r_2)$$

3. Proof of Main Result

Observe C is a vector space over $\mathbb{F}_{q^m}$ and $\operatorname{Tr}(C)$ is a vector space over $\mathbb{F}_q$. From this we have the bound

$$\dim_{\mathbb{F}_{q^m}} C \leq \dim_{\mathbb{F}_q} \operatorname{Tr}(C) \leq m(dim_{\mathbb{F}_{q^m}} C)$$

Using the $\mathbb{F}_q$-linearity of the trace map we have an exact sequence

$$0 \to K' \to C \to \operatorname{Tr}(C) \to 0$$

where K' is the kernel of the trace map. Note the trace map defines an $\mathbb{F}_q$-linear subspace of C. Let K be the subspace of $L(G)$ that is the inverse image of evaluation at $D = \{P_1, \ldots, P_n\}$. That is

$$K := \{f \in L(G) | (f(P_1), \ldots, f(P_n)) \in K\}$$

Notice that K' is isomorphic to K as $\mathbb{F}_q$ vector spaces. Therefore

$$m \dim_{\mathbb{F}_{q^m}} C - \dim_{\mathbb{F}_q} K = \dim_{\mathbb{F}_q} \operatorname{Tr}(C) \tag{3}$$

We can obtain the dimension of $\operatorname{Tr}(C)$ by determining $\dim_{\mathbb{F}_q} K$. In practice, this is difficult. Consider the space of functions

$$E := \{f = h^q - h \mid f \in L(G), h \in \mathbb{F}_{q^m}(X)\}$$

Using Bombieri's estimate and a degree argument, we will determine a sufficient condition (condition 2 of Theorem 1) when $K = E$ and E is isomorphic to K'. But to make this useful we will first show Theorem 1 is sufficient to determine the dimension of E.

3.1. Dimension of E

For $f = h^q - h \in L(G)$, by definition $(h^q - h) + G \geq 0$. Counting with multiplicity, each pole in h corresponds to q poles in f. For $h \in L([G/q])$, we have $h^q - h \in L(G)$.

Consider the map $\phi : L([G/q]) \to E$ where $\phi(h) = h^q - h$. By definition, the kernel is $\mathbb{F}_q \cap L([G/q])$. Note that for a general G the map ϕ is not surjective.

Lemma 3. *When* $\deg(G^-) \leq 1$ *the map* ϕ *is surjective.*

Proof. Recall that the divisor $[G/q]$ only changes the positive coefficients of G and does not change G^-. When $G^- = \emptyset$, there is no restriction on zeros in $L(G)$. Therefore, in this case ϕ is onto.

If $|\operatorname{Supp}(G^-)| = 1$, then $G^- = n_p P$ for some point $P \in X(\mathbb{F}_{q^m})$ and negative integer n_p. Every function in $L([G/q])$ must have a zero at P. In the factorization $h^q - h = \prod_{b \in \mathbb{F}_q}(h - b)$, this zero must occur in at least one factor $h - b$. Though h may not be in $L([G/q])$, there will always exist some $b \in \mathbb{F}_q$ such that $h - b \in L([G/q])$. Observe $h^q - h = (h-b)^q - (h-b) = \phi(h-b)$. In this case, ϕ is onto. □

If $G^- = \emptyset$, then the kernel of ϕ is $\mathbb{F}_q$. If $G^- \neq \emptyset$, then ϕ is injective. Therefore the δ defined in Theorem 1 is merely $\delta = \dim_{\mathbb{F}_q} \ker \phi$. Using Lemma 3, we have the following proposition.

Proposition 4. *If $deg(G^-) \leq 1$, then the sequence*

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{F}_q \cap L([G/q]) \arrow[r] & L([G/q]) \arrow[r, "\phi"] & E \arrow[r] & 0 \end{tikzcd}$$

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

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

In general, ϕ may not be surjective. There is still a dimension bound:

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

Note in [7], a similar result is obtained with the use of group cohomology and other auxillary constructions.

3.2. Bombieri's Estimate

A key step in determining when $K = E$ is a bound developed by Bombieri [8].

Theorem 5 (Bombieri's estimate)**.** *Let X be a complete, geometrically irreducible, nonsingular curve of genus $\mathfrak{g}$, defined over $\mathbb{F}_{q^m}$. Let $f \in \mathbb{F}_{q^m}(X), f \neq h^p - h$ for $h \in \overline{\mathbb{F}}_q(X)$, with pole divisor $(f)_\infty$ on X. Then*

$$\left| \sum_{P \in X(\mathbb{F}_{q^m}) \setminus \mathrm{Supp}(f)_\infty} \zeta_p^{\mathrm{Tr}_{q^m/p}(f(P))} \right| \leq (2\mathfrak{g} - 2 + t + \deg(f)_\infty) q^{m/2}$$

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

Let $\overline{E} = \{f \in K \mid f = h^p - h$ for some $h \in \overline{\mathbb{F}}_q(X)\}$. On this subspace of K the conditions of Bombieri's Estimate are not met.

Lemma 6. *$E \subseteq \overline{E}$.*

Proof. Recall that $q = p^r$. Therefore, for $g^q - g \in E$ we have

$$\begin{aligned} g^q - g &= g^{p^r} - g \\ &= (g^{p^{r-1}} + \ldots + g)^p - (g^{p^{r-1}} + \ldots + g) \end{aligned}$$

Let $h = g^{p^{r-1}} + \ldots + g$. From this we see clearly that $g^q - g = h^p - h$. □

Lemma 7. *For each $g \in \overline{\mathbb{F}}_q(X)$, there exists an $h \in \mathbb{F}_{q^m}(X)$ and $c \in \mathbb{F}_{q^m}$ such that $g^p - g = h^p - h + c$. Therefore,*

$$\overline{E} \subseteq \{f \in \mathbb{F}_{q^m}(X) \mid f = h^p - h + c \text{ for some } h \in \mathbb{F}_{q^m}(X), c \in \mathbb{F}_{q^m}\}$$

Proof. Suppose there is an $f \in \mathbb{F}_{q^m}(X)$ and an $h \in \overline{\mathbb{F}}_q(X)$ such that $f = h^p - h$. Consider $\sigma = \mathrm{Frob}_{q^m}$, the coefficient-wise q^m-Frobenius endomorphism on $\overline{\mathbb{F}}_q^m$. Observe

$$\begin{aligned} \sigma(f) &= \sigma(h^p - h) \\ &= \sigma(h^p) - \sigma(h) \\ &= \sigma(h)^p - \sigma(h) \end{aligned}$$

Furthermore, $\sigma(f) = f$. Rearranging by exponents of p we see

$$\begin{aligned} \sigma(h)^p - \sigma(h) &= h^p - h \\ \sigma(h)^p - h^p &= \sigma(h) - h \\ (\sigma(h) - h)^p &= \sigma(h) - h \end{aligned}$$

By considering the order of poles of $\sigma(h) - h$, we determine that $\sigma(h) - h$ must be a constant $a \in \mathbb{F}_p$. There is a b in $\overline{\mathbb{F}}_q$ such that $a = b^{q^m} - b$. Then $\sigma(b) = b + a$ and $\sigma(h - b) = h + a - (b + a) = h - b$. Therefore, $h - b \in \mathbb{F}_{q^m}(X)$. Let $h_1 = h - b$. Observe $f - b^p + b = h_1^p - h_1$. Also, $\sigma(b^p - b) = b^p - b$, so $b^p - b \in \mathbb{F}_{q^m}$. Therefore, $f = h_1^p - h_1 + b^p - b$. □

Consider $f \in K$, and $P \in D = X(\mathbb{F}_{q^m}) \setminus \mathrm{Supp}(G)$ as defined in our definition of the trace code. By the definition of K, we have $\mathrm{Tr}(f(P)) = 0$. Observe that if $f \in K \setminus \overline{E}$ then f satisfies the conditions of Bombieri's Estimate. Hence, $\zeta_p^{\mathrm{Tr}(f(P))} = 1$ for each P. For such f, each term of the sum in the left-hand-side in Theorem 5 contributes 1. This is a total contribution of $|X(\mathbb{F}_q) \setminus (f)_\infty|$. Hence for $f \in K \setminus \overline{E}$, we have

$$\left| \sum_{P \in X(\mathbb{F}_{q^m}) \setminus \mathrm{Supp}(f)_\infty} \zeta_p^{\mathrm{Tr}_{q^m/p}(f(P))} \right| = |(X(\mathbb{F}_{q^m}) \setminus (f)_\infty)| \leq (2\mathfrak{g} - 2 + t + \deg(f)_\infty) q^{m/2}$$

Observe $t \leq |\mathrm{Supp}(G^+)|$ and $\deg(f)_\infty \leq \deg(G^+)$. Using these two inequalities, we obtain a more general bound:

$$|X(\mathbb{F}_{q^m})| \leq (2\mathfrak{g} - 2 + \deg(G^+)) q^{m/2} + |\mathrm{Supp}(G^+)|(q^{m/2} + 1)$$

Proposition 8. *If*

$$|X(\mathbb{F}_{q^m})| > (2\mathfrak{g} - 2 + \deg(G^+)) q^{m/2} + |\mathrm{Supp}(G^+)|(q^{m/2} + 1)$$

then $K = \overline{E}$.

The condition presented in Proposition 8 is exactly condition (2) from Theorem 1.

3.3. *E and* $\overline{E}$

Recall the definitions of E and $\overline{E}$:

$$E := \{f = h^q - h \mid f \in L(G), h \in \mathbb{F}_{q^m}(X)\}$$

$$\overline{E} := \{f \in K \mid f = h^p - h \text{ for some } h \in \overline{\mathbb{F}}_q(X)\}$$

In the case presented in [7], Van der Vlugt had $\overline{E} = E$. In the current more general case, Proposition 8 provides conditions forcing all elements of K to be of the form $h^p - h$, for $h \in \overline{\mathbb{F}}_q(X)$. However, it may be that elements of this form that are not of the form $g^q - g$, with $g \in \mathbb{F}_{q^m}(X)$. We will show that this is not the case and that condition (2) of Theorem 1 is sufficient to force $K = E$. It will be useful to develop our understanding of the interplay of K, $\overline{E}$ and E, and the nature of the degree of functions therein.

As is the case in Lemma 6, elements of the form $g^q - g$, for $g \in \mathbb{F}_{q^m}(X)$, can also be written in the form $h^p - h$, for $h \in \overline{\mathbb{F}}_q(X)$. Also notice that for any $f \in K$ and $y \in \mathbb{F}_q$, the function yf is an element of K. Furthermore, for any $f \in E$ and $y \in \mathbb{F}_q$, yf is in E. Consider the following:

Definition 9. For $f \in \overline{\mathbb{F}}_q(X)$, let $D(f)$ be the elements $y \in \mathbb{F}_q$ such that $yf = h^p - h$, for some $h \in \overline{\mathbb{F}}_q(X)$.

We see that for $f \in K$, when $|D(f)| < q$, there is a y such that $yf \in K \setminus \overline{E}$.

Proposition 10. *For $f \in K$, $D(f)$ is an $\mathbb{F}_p$-subspace of $\mathbb{F}_q$.*

Proposition 11. *If $D(f) = \mathbb{F}_q$ and $D(g) = \mathbb{F}_q$ then $D(af + bg) = \mathbb{F}_q$ for each $a, b \in \mathbb{F}_q$.*

Lemma 12. *Let $f = h^p - h \neq 0$ for some $h \in \overline{\mathbb{F}}_q(X)$ and $D(f) \neq \{0\}$. Then*

$$|D(f)| \leq p|D(h)|$$

Proof. Let $y \in D(f)$, $y \neq 0$. Then $yf = g^p - g$ for some $g \in \overline{\mathbb{F}}_q(X)$. Hence

$$yf = g^p - g = yh^p - yh = (y^{1/p}h)^p - (y^{1/p}h) + (y^{1/p}h) - yh$$

Rearranging terms we see that

$$(y^{1/p} - y)h = (g^p - g) - ((y^{1/p}h)^p - (y^{1/p}h))$$

Therefore $(y^{1/p} - y)$ is in $D(h)$. Hence, for every $x, y \in D(f)$, $x^{1/p} - x$ and $y^{1/p} - y$ are in $D(h)$. Suppose $x \neq y$ but $x^{1/p} - x = y^{1/p} - y$. Then

$$\begin{aligned} x^{1/p} - x &= y^{1/p} - y \\ (x - y)^{1/p} &= (x - y) \\ (x - y) &= (x - y)^p \end{aligned}$$

The only elements of $\mathbb{F}_q$ equal to their own p^{th} power are elements of $\mathbb{F}_p$. Hence $x = y + t$ for some $t \in \mathbb{F}_p$. From this we see that $D(f)/\mathbb{F}_p$ can be identified with a subgroup of $D(h)$. Hence $|D(f)| \leq p|D(h)|$. □

Definition 13. For $f \in \mathbb{F}_{q^m}(X)$, define the p-linear degree of f, denoted $e(f)$, to be the largest possible integer such that $f = a_c + a_0 g + a_1 g^p + \ldots + a_{e(f)} g^{p^{e(f)}}$, where $a_c, a_0, \ldots, a_{e(f)} \in \mathbb{F}_{q^m}$, $g \in \mathbb{F}_{q^m}(X)$.

The following properties of $e(f)$ are straightforward:

Proposition 14.

1. *For $f \in \overline{E}$, we have $e(f) \geq 1$. This is a restatement of Lemma 7.*
2. *For $g \in E$, we have $e(g) \geq r$.*
3. *For $a \in \mathbb{F}_{q^m}^*, b \in \mathbb{F}_{q^m}$, we have $e(f) = e(af + b)$.*

Proposition 15. *Suppose $f \in \mathbb{F}_{q^m}(X)$ such that either $e(f) = 0$ or $f = h^p - h$, for some $h \in \overline{\mathbb{F}_q}(X)$. Then we have the inequality:*

$$|D(f)| \leq p^{e(f)}$$

Proof. We proceed by induction on $e(f)$. Suppose $e(f) = 0$. By Lemma 7, we have $yf \neq h^p - h + c$, for any $y \in \mathbb{F}_{q^m}^*$, any $h \in \mathbb{F}_{q^m}(X)$, and $c \in \mathbb{F}_{q^m}$. Therefore $D(f) = \{0\}$ and $|D(f)| = 1 = p^0 = p^{e(f)} = 1$.

Now consider a positive integer k and $f \in \mathbb{F}_{q^m}(X)$ such that $e(f) = k$. Without loss of generality, we may assume that $|D(f)| > 1$. There is a nonzero $y \in D(f)$ such that $yf = h^p - h$. Therefore,

$f = y^{-1}h^p - y^{-1}h$. From this we obtain $e(f) \geq 1 + e(h)$. Since $e(f) = k$ we have $e(h) < k$. By the inductive hypothesis, $|D(h)| \leq p^{e(h)}$. Combining this with Lemma 12 we have

$$|D(f)| \leq p|D(h)| = p^{e(h)+1} \leq p^{e(f)}$$

□

Corollary 16. *If $|D(f)| = q = p^r$, then $e(f) \geq r$.*

Proposition 17. *Suppose condition (2) from Theorem 1 holds. That is, suppose*

$$|X(\mathbb{F}_{q^m})| > (2\mathfrak{g} - 2 + \deg(G^+))q^{m/2} + |\mathrm{Supp}(G^+)|(q^{m/2} + 1)$$

If $K \neq E$, then $K \setminus \overline{E}$ is nonempty.

Proof. Suppose $K \neq E$ 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. Choose $f \in K \setminus E$ with the least number of poles. In other words, $\deg(f)_\infty$ is minimal and positive. Applying Corollary 16, there is some $l \in \mathbb{Z}_{\geq 0}$, $h \in \mathbb{F}_{q^m}(X)$ and $a_c, a_1, \ldots, a_{r+l} \in \mathbb{F}_{q^m}$ such that

$$f = a_{r+l}h^{p^{r+l}} + a_{r+l-1}h^{p^{r+l-1}} + \ldots + a_1h + a_c$$

This may be rewritten as

$$f = f_E + f_1$$

where

$$f_E = (a_{r+l}h^{p^l})^q - (a_{r+l}h^{p^l}),$$

$$f_1 = (a_{r+l}h^{p^l}) + a_{r+l-1}h^{p^{r+l-1}} + \ldots + a_1h + a_c \in \mathbb{F}_{q^m}(X)$$

Observe $f_E \in K$ and $D(f_E) = \mathbb{F}_q$. Hence $f_1 = f - f_E \in K$. By Proposition 11, $D(f_1) = \mathbb{F}_q$. But

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

and

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

This contradicts the choice of an f with minimal poles. Hence, when $K \neq E$, we can choose an $f \in K$ not of the form $h^p - h$. □

4. Conclusions

Proof of Theorem 1. Let $2\mathfrak{g} - 2 \leq \deg([G/q])$, $\deg(G) < n$ and also assume condition (1) and condition (2).

By condition (2), Proposition 8 and Proposition 17, we see that $K = E$. Then, using condition (1) and Proposition 4, we compute the dimension of E. We apply this to Equation (3) to obtain Theorem 1, a dimension formula for algebraic-geometric trace codes, as desired. □

Author Contributions: Both authors contributed equally to this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Katsman, G.; Tsafsman, M. A remark on algebriac geometric codes. *Contemp. Math.* **1989**, *93*, 197–200.
2. Wirtz, M. On the parameters of Goppa codes. *IEEE Trans. Inform. Theory* **1988**, *34*, 1341–1343.
3. Stichtenoth, H. On the dimension of subfield subcodes. *IEEE Trans. Inform. Theory* **1990**, *36*, 90–93.

4. Delsarte, P. On the subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory* **1975**, *21*, 575–576.
5. Hernando, F.; Marshall, K.; O'Sullivan, M. The dimension of subcode-subfields of shortened generalized Reed-Solomon codes. *Des. Codes Cryptogr.* **2013**, *69*, 131–142.
6. Véron, P. True dimension of some binary quadratic trace Goppa codes. *Des. Codes Cryptogr.* **2001**, *24*, 81–97.
7. Van der Vlugt, M. A new upper bound for the dimension of trace codes. *Bull. Lond. Math. Soc.* **1991**, *23*, 395–400.
8. Bombieri, E. Exponential sums in finite fields. *Am. J. Math.* **1966**, *88*, 71–105.
9. Stichtenoth, H. *Algebraic Function Fields and Codes*; Springer-Verlag: Berlin, Germany, 1993.
10. Ireland, K.; Rosen, M. *A Classical Introduction to Modern Number Theory*; Springer-Verlag: Berlin, Germany, 1998.