where our improved upper bound is given above the best previous upper bound. The bounds in parentheses "( )" are due to Kløve [1], those in brackets "[ ]" are due to Chen, Fan, and Jin [16], and those in braces "{ }" are due to Chen [15]. The blocks for difference triangle sets with the improved scopes are available from the authors.

VI. Concluding Remarks

One of the problems suggested by the results in Section II is the determination of the asymptotic behavior of $m(n,k)$. Our results show that for $f(n)$ satisfying $\lim\ \sup_{n\to\infty}\ f(n)/n<1$, we have $\lim_{n\to\infty}\ m(n,f(n))/n(f(n))^2 = 1$. It would be interesting to know what happens if $f(n)$ is allowed to grow at a faster rate.

We have also described algorithms that are used to construct difference triangle sets with the best known scopes for many intermediate values of n and k.

References

[1] T. Kløve, "Bounds on the size of optimal difference sets," *IEEE Trans. Inform. Theory*, vol. 34, pp. 355–361, 1988.

[2] ——, "Bounds and construction for difference triangle sets," *IEEE Trans. Inform. Theory*, vol. 35, pp. 879–886, 1989.

[3] J. Abrham, "Perfect systems of difference sets—A survey," *Ars Combin.*, vol. 17A, pp. 5–36, 1984.

[4] D. G. Rogers, "On critical perfect systems of difference sets," *Discr. Math.*, vol. 135, pp. 287–301, 1994.

[5] C. J. Colbourn, "Difference triangle sets," in *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. San Diego, CA: CRC Press, 1995, ch. IV.14.

[6] A. Dollas, W. T. Rankin, and D. McCracken, "New algorithms for Golomb ruler derivation and proof of the 19 mark ruler," preprint.

[7] R. O. Davies, "On Langford's problem (II)," *Math. Gaz.*, vol. 43, pp. 253–255, 1959.

[8] T. Skolem, "On certain distribution of integers into pairs with given differences," *Math. Scand.*, vol. 5, pp. 57–68, 1957.

[9] A. Kotzig and J. M. Turgeon, "Perfect systems of difference sets and additive sequences of permutations," in *Proc. 10th Southeastern Conf. on Combinatorics, Graph Theory, and Computing*, 1979, pp. 629–636.

[10] D. G. Rogers, "Addition theorems for perfect systems of difference sets," *J. London Math. Soc.*, vol. 23, pp. 385–395, 1981.

[11] J.-C. Bermond, "Graceful graphs, radio antennae, and Frence windmills," in *Graph Theory and Combinatorics*, vol. 34 of *Research Notes in Mathematics*. London, U.K.: Pittman, 1979, pp. 18–37.

[12] J.-H. Huang and S. S. Skiena, "Gracefully labelling prisms," *Ars Combin.*, vol. 38, pp. 225–242, 1994.

[13] J.-C. Bermond, A. Kotzig, and J. Turgeon, "On a combinatorial problem of antennas in radioastronomy," in *Proceedings of 18th Hungarian Combinatorial Colloquim*. Amsterdam, The Netherlands: North-Holland, 1976, pp. 135–149.

[14] P. J. Laufer, "Regular perfect systems of difference sets of size 4 and extremal systems of size 3," *Ann. Discr. Math.*, vol. 12, pp. 193–201, 1982.

[15] Z. Chen, "Further results on difference triangle sets," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1268–1270, 1994.

[16] Z. Chen, P. Fan, and F. Jin, "Disjoint difference sets, difference triangle sets, and related codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 518–522, 1992.

[17] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1938.

[18] M. J. Colbourn and C. J. Colbourn, "Recursive constructions for cyclic block designs," *J. Statist. Plann. Infer.*, vol. 10, pp. 97–103, 1984.

[19] D. R. Heath-Brown and H. Iwaniec, "On the difference between consecutive primes," *Invent. Math.*, vol. 55, pp. 49–69, 1979.

[20] W. A. Wythoff, "A modification of the game of Nim," *Nieuw Arch. Wisk (2)*, vol. 7, pp. 199–202, 1907.

[21] I. G. Connell, "A generalization of Wythoff's game," *Canad. Math. Bull.*, vol. 2, pp. 181–190, 1959.

Contribution to Munuera's Problem on the Main Conjecture of Geometric Hyperelliptic MDS Codes

Hao Chen and Stephen S.-T. Yau, *Senior Member, IEEE*

***Abstract*—In coding theory, it is of great interest to know the maximal length of MDS codes. In fact, the Main Conjecture says that the length of MDS codes over F_q is less than or equal to $q+1$ (except for some special cases). Munuera proposed a new way to attack the Main Conjecture on MDS codes for geometric codes. In particular, he proved the conjecture for codes arising from curves of genus one or two when the cardinal of the ground field is large enough. He also asked whether a similar theorem can be proved for any hyperelliptic curve. The purpose of this correspondence is to give an affirmative answer. In fact, our method also proves the Main Conjecture for geometric MDS codes for $q=2$ if the genus of the hyperelliptic curve is either 1, 2 or 3, and for $q=3$ if the genus of the curve is 1.**

***Index Terms*— Algebraic curves, algebraic-geometric codes, divisors, hyperelliptic curves, zeta function.**

I. Introduction

Let F_q be a finite field with q elements and X be a nonsingular projective curve defined over F_q with genus g. We shall write $X(F_q)$ to indicate the finite set of F_q-rational points on X. The function field of X over F_q is denoted by $F_q(X)$. Let $\mathcal{P}=\{P_1,\cdots,P_n\}$ be a set of n distinct rational points on X. By abusing notation, we also sometimes identify $\mathcal{P}$ as a divisor. Let G be a rational divisor with support disjoint from $\mathcal{P}$.

$$L(G):=\{f\in F_q(X):(f)+G\geq 0\}\cup\{0\}=H^0(X,[G])$$

where $[G]$, the line bundle corresponding to the divisor G, is a vector space, and we denote $\ell(G)$ its dimension. The complete linear system associated to G, denoted by $|G|$, is

$$\{f\in F_q(X):(f)+G\geq 0\}/F_q^*.$$

Definition: The algebraic geometry code $C(X,\mathcal{P},G)$ associated to the pair $(\mathcal{P},G)$ is the linear code of length n defined as the image of the linear map

$$\begin{aligned}\alpha: L(G)&\to F_q^n\\ f&\to (f(P_1),\cdots,f(P_n)).\end{aligned}$$

We shall let k denote the dimension of this linear code. Then $k=\ell(G)-\ell(G-\mathcal{P})$. In what follows, we shall always assume that

$$2g-2<\deg\ G<n. \tag{1.1}$$

It is well known that the dimension k and the minimum distance d of the algebraic geometric code $C(X,\mathcal{P},G)$ satisfy the following relations [11]:

$$k=\ell(G)=\deg\ G+1-g \tag{1.2}$$

$$d\geq n-\deg\ G. \tag{1.3}$$

Manuscript received July 12, 1996; revised February 3, 1997. The work of H. Chen was supported by the NSF of China and by the Guangdong Provincial NSF of China. The work of S. S.-T. Yau was supported in part by ARO DAAH04-1-0530 and NSF DMS 9321262.

H. Chen is with the Department of Mathematics, Zhongshan University, Guangzhou, Guangdong 510275, P.R. China.

S. S.-T. Yau is with the Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, Chicago, IL 60607-7045 USA.

Publisher Item Identifier S 0018-9448(97)03868-6.

For any linear code of length n, dimension k, and minimum distance d, we have the following well-known singleton bound [5]:

$$d \leq n - k + 1. \tag{1.4}$$

Codes reaching this upper bound are called *maximum-distance-separable* (MDS) codes. From now on, the code $C(X, \mathcal{P}, G)$ is always supposed to be MDS and nontrivial, that is, $1 < k < n - 1$.

Main Conjecture for MDS Codes: For every linear $[n, k, d]$ MDS code over F_q, if $1 < k < q$, then $n \leq q + 1$, except when q is even and $k = 3$ or $k = q - 1$ in which cases $n \leq q + 2$.

This conjecture is proved when $q \leq 11$ or $k \leq 5$ from the viewpoint of finite geometries [5]. In [6], Munuera introduced a beautiful new idea. He translated the conjecture for algebraic geometry codes to another problem concerning the arithmetic of the curve X. He proved it for codes arising from curves with genus 1, which had been previously proved by Katsman and Tsfasman [3], and curves of genus 2 when $q > 83$. Munuera then asked whether a similar theorem can be proved for any hyperelliptic curve. The purpose of this correspondence is to give an affirmative answer to Munuera's question.

Main Theorem: The Main Conjecture on MDS codes is true for codes arising from hyperelliptic curves of genus $g \geq 2$ if

$$q > 8g^2 + 4g + 8 + 8g\sqrt{g^2 + g + 2}$$

or

$$q < 8g^2 + 4g + 8 - 8g\sqrt{g^2 + g + 2}$$

where q is the cardinality of the finite field F_q.

Remark: 1) We observe that if the genus is equal to two, then the Main Conjecture on MDS codes is true as long as $q \geq 94$. We deduce Munuera's result when $q \geq 94$ as a corollary of our theorem above.

2) We also observe that the Main Conjecture on MDS codes is true for $q = 2$ if the genus of the hyperelliptic curve is either one, two, or three, and for $q = 3$ if the genus of the curve is one.

3) In [2], De Boer proves the above theorem for $q > C(g!)$. Since q has to grow exponentially with g, his result is much weaker than ours. In fact, the constant C is not explicitly computed.

II. Preliminaries

In this section, we shall recall some of the standard results that we need later in order to prove the Main Theorem stated in Section I.

Given $\mathcal{P}, G$ as in Section I we can define another algebraic geometry code in the following manner. For a divisor E, denote $\Omega(E) := \{\omega : \omega \text{ rational differential form with } (\omega) \geq E\} \cup \{0\}$.

Definition 2.1: The algebraic geometry code $C^*(X, \mathcal{P}, G)$ associated to the pair $(\mathcal{P}, G)$ is the linear code of length n defined as the image of the linear map

$$\begin{array}{ccc} \alpha^* : \Omega(G - \mathcal{P}) & \rightarrow & F_q^n \\ \eta & \rightarrow & (\mathrm{Res}_{P_i}(\eta), \cdots, \mathrm{Res}_{P_n}(\eta)) \end{array}$$

where $\mathrm{Res}_{P_i}(\eta)$ is the residue of η at the point P_i. Let k^* be the dimension of image of α^*.

Let K be a canonical divisor of X. Then $k^* = \ell(K - G + \mathcal{P})$ and $C(X, \mathcal{P}, G)$ and $C^*(X, \mathcal{P}, G)$ are dual to each other. Furthermore, $d^* :=$ minimal distance of $C^*(X, \mathcal{P}, G) \geq \deg G + 2 - 2g$.

Definition 2.2: We denote $\mathcal{P}(e)$ a generic effective divisor of degree e such that $\mathcal{P}(e) \leq \mathcal{P}$ (i.e., $\mathcal{P}(e) = P_{i_1} + \cdots + P_{i_e}$ where $P_{i_r} \neq P_{i_s}$ for $r \neq s$).

Let $N_r := |X(F_q r)|$, the number of F_{q^r}-rational points of X. One has $|N_r - q^r - 1| \leq 2gq^{r/2}$ which is called the Hasse–Weil bound. We only need the following information in the remainder of the correspondence:

$$|\boldsymbol{P}^1(F_{q^r})| = q^r + 1$$
$$N := |X(F_q)| \leq N_1 \leq 1 + q + 2g\sqrt{q}.$$

Lemma 2.1 If $C(X, \mathcal{P}, G)$ is an MDS code, then $L(G - \mathcal{P}(k-1))$ produces all codewords of minimal weight d locating exactly outside $\mathcal{P}(k-1)$. In particular

$$\dim L(G - \mathcal{P}(k-1)) = 1$$

and

$$L(G - \mathcal{P}(k)) = L(G - \mathcal{P}) = 0.$$

Proof: Codewords obtained from $L(G - \mathcal{P}(k-1))$ have weight at most $n - (k-1) = n + 1 - k = d$ because $C(X, \mathcal{P}, G)$ is an MDS. Hence, the codewords obtained from $L(G - \mathcal{P}(k-1))$ are either 0, or of minimal weight. The location of the nonzero coordinates of such codewords are clearly locating exactly outwide $\mathcal{P}(k-1)$. Let $f_1, f_2 \in L(G - \mathcal{P}(k-1))$ such that $\alpha(f_1)$ and $\alpha(f_2)$ are of minimal weight. Since the nonzero coordinates of $\alpha(f_1)$ and $\alpha(f_2)$ have the same location, a linear combination of $\alpha(f_1)$ and $\alpha(f_2)$, say $a_1\alpha(f_1) + a_2\alpha(f_2)$, will create a codeword with weight less than d. This is possible only if $a_1\alpha(f_1) + a_2\alpha(f_2) = 0$. This simply means that $a_1 f_1 + a_2 f_2 \in L(G - \mathcal{P})$. In particular

$$\dim L(G - \mathcal{P}(k-1))/L(G - \mathcal{P}) = 1.$$

Clearly, $L(G - \mathcal{P}(k)) \supset L(G - \mathcal{P})$. Suppose that there exists $f \in L(G - \mathcal{P}(k)) - L(G - \mathcal{P})$. Then the codeword obtained from f has weight at most $n - k = d - 1 < d$ which is not possible. Hence

$$L(G - \mathcal{P}(k)) = L(G - \mathcal{P}). \qquad \square$$

Lemma 2.2: If $C(X, \mathcal{P}, G)$ is an MDS code, then

$$\dim L(G - \mathcal{P}(k - e)) = e$$

for all $0 \leq e \leq k$.

Proof: Assuming the statement is true for e, we shall prove that the statement is true for $e + 1$. Consider the following diagram of exact sequences

$$\begin{array}{ccccccccc} & & 0 & \rightarrow & L(G) & \rightarrow & F_q^k & \rightarrow & 0 \\ & & \cap| & & \| & & \downarrow & & \\ 0 & \rightarrow & L(G - \mathcal{P}(k)) & \rightarrow & L(G) & \rightarrow & F_q^{k-e} & \rightarrow & 0 \\ & & \cap| & & \| & & \downarrow & & \\ 0 & \rightarrow & L(G - \mathcal{P}(k-e)) & \rightarrow & L(G) & \rightarrow & F_q^{k-e} & \rightarrow & 0 \\ & & \cap| & & \| & & \downarrow & & \\ 0 & \rightarrow & L(G - \mathcal{P}(k-e-1)) & \rightarrow & L(G) & \rightarrow & F_q^{k-e-1}. & & \end{array}$$

We claim that

$$\dim L(G - \mathcal{P}(k-e-1)) \geq e + 1.$$

Otherwise, we have

$$\dim L(G - \mathcal{P}(k-e-1)) \leq e = \dim L(G - \mathcal{P}(k-e)).$$

On the other hand,

$$L(G - \mathcal{P}(k-e-1)) \supseteq L(G - \mathcal{P}(k-e)).$$

So we have

$$\dim L(G - \mathcal{P}(k-e-1)) = e = \dim L(G - \mathcal{P}(k-e)).$$

The algebraic geometry code $C(X, \mathcal{P}(k-e-1), G)$ is of dimension $k - e$. But from the bottom row of the above diagram, $C(X, \mathcal{P}(k-e-1), G)$ is embeddable into F_q^{k-e-1}, which is impossible. This proves our claim.

Observe that

$$\dim L(G - \mathcal{P}(k-e-1))/L(G - \mathcal{P}(k-e)) \leq 1.$$

By induction, we deduce immediately that

$$\dim L(G - \mathcal{P}(k-e-1)) \leq e + 1,$$

Hence

$$\dim L(G - \mathcal{P}(k-e-1)) = e + 1. \qquad \square$$

Proposition 2.3: Given a geometric MDS code $C(X, \mathcal{P}, G)$. Let a and b be integers such that $\mathcal{P}_1(a)+\mathcal{P}_2(b) = \mathcal{P}$. Then the projection $F_q^n \to F_q^a$ onto the positions $\mathcal{P}_1(a)$ induces and defines

$$0 \to C(b) \to C(X, \mathcal{P}, G) \to Q(a) \to 0$$

where $C(b)$ consists of those codewords with support on $\mathcal{P}_2(b)$ and $Q(a)$ is the image of $C(X, \mathcal{P}, G)$ under the projection $F_q^n \to F_q^a$. By discarding the zero positions, we get a code which is still denoted by $C(b)$. Then

i)

$$Q(a) \approx C(X, \mathcal{P}_1(a), G)$$
$$C(b) \approx L(G - \mathcal{P}_1(a))/L(G - \mathcal{P}).$$

ii) For $k \le a \le n$, $C(b) = 0$, and $Q(a)$ has parameters $[a, k, a - k + 1]$.

iii) For $0 \le a \le k - 1$, $Q(a)$ is the trivial code $[a, a, 1]$, and $C(b)$ has parameters $[b, k - a, d]$ and

$$C(b) \approx C(X, \mathcal{P}_2(b), G - \mathcal{P}_1(a)).$$

In particular, the $C(b)$'s and the $Q(a)$'s are all geometric MDS codes.

Let us consider only the geometric case of Main Conjecture in this correspondence. If there exists a code with $n > q+2$, we can always, by using Proposition 2.3, truncate the length to $q+2$ without altering k. Therefore, if the Main Conjecture failed for algebraic geometric MDS code, then there would exist an algebraic geometric MDS code with $n = q+2$. Since a dual code of Algebraic Geometric MDS code is also an Algebraic Geometric MDS code, we deduce the following reduction proposition.

Proposition 2.4: In order to prove the Main Conjecture for algebraic geometric MDS code, it is sufficient to produce a contradiction, when $q \ge 13$ in the presence of an algebraic geometry MDS code of parameters $[n, k, d]$ where $n = q + 2$ and $6 \le k \le n/2$ (in particular $k \le q - 4$).

We now recall a beautiful observation due to Munuera [6]. Given X, $\mathcal{P}$, and G as in the Introduction, satisfying (1.1), following Munuera, we shall consider the set of divisors

$$\mathcal{C}_t(\mathcal{P}) = \{\mathcal{P}(t) : \text{all subdivisors of } \mathcal{P} \text{ of degree } t\}.$$

Recall that $\mathcal{P}(t) = P_{i_1} + \cdots + P_{i_t}$, $P_{i_r} \in \mathcal{P}$ and $P_{i_r} \ne P_{i_s}$ if $r \ne s$. Let $\sim$ be the linear equivalence among divisors. We shall consider the following hypothesis.

$\mathcal{C}[X, \mathcal{P}, t]$: There exists a class in $\mathcal{C}_t(\mathcal{P})/\sim$ such that for any two points R and S in $\mathcal{P}$, there is a representative in that class which is disjoint from both R and S.

The following proposition use the condition (1.1) that $n > \deg G$.

Proposition 2.5 (Munuera): Suppose (1.1) holds and the hypothesis $\mathcal{C}[X, \mathcal{P}, t]$ is true for $1 < t \le \frac{n}{2} - 2$, if $n > q + 1$, then there is no geometric MDS code arising from $\mathcal{P}$ for $3 < k < q$, except perhaps for $k = q - 1$ and $n = q + 2$.

Proof: Suppose that $C(X, \mathcal{P}, G)$ is an $[n, k, d]$ MDS code with $3 < k$ and $n > q+1$. If this code is not a $[q+2, q-1, d]$ code, then we can assume $3 < k \le n/2$ because the dual of geometric MDS code is again a geometric MDS code.

Since hypothesis $\mathcal{C}[X, \mathcal{P}, k-2]$ holds, we choose a class $[D]$ as in the hypothesis. For each $\mathcal{P}(k-2) \in [D]$, $\ell(G - \mathcal{P}(k-2)) = 2$ by Lemma 2.2. Therefore, $|G - \mathcal{P}(k-2)|$ has $q+1$ elements. On the other hand, let $P_i \in \mathcal{P}$, then there is an effective divisor E_i of degree

$$\deg G - (k-2) - 1 = \deg G - k + 1 = g$$

such that $G - \mathcal{P}(k-2) \sim P_i + E_i$ in view of (1.2) and Lemma 2.2. Now the claim is that all the $P_i + E_i$ are distinct. Suppose the opposite, $P_i + E_i = P_j + E_j$ for some $i \ne j$. This is possible only when there exists an effective divisor E such that

$$P_i + E_i = P_j + E_j = P_i + P_j + E.$$

Take another $\mathcal{P}'(k-2)$ in the same class $[D]$ which is disjoint from both P_i and P_j. Then

$$G - \mathcal{P}'(k-2) \sim P_i + P_j + E$$

i.e.,

$$G - \mathcal{P}'(k-2) - P_i - P_j \sim E.$$

So there is a nonzero element in $L(G - \mathcal{P}(k))$. This contradicts Lemma 2.2.

Since $P_i + E_i$, $i = 1, \cdots, n$ are pairwise distinct in $[G - \mathcal{P}(k-2)]$, we have $n \le q + 1$. □

III. Proof of the Main Theorem

Recall that for a divisor D, the complete linear system $|D|$ is the collection of all effective divisors which are linearly equivalent to D. It is the projective space associated to $L(D)$. So the dimension of a linear system is $\ell(D) - 1$. A base point of the linear system $|D|$ is a point that is contained in each effective divisor in the system. A divisor D has no base points if and only if for any point p, $\ell(D - p) = \ell(D) - 1$. By Riemann–Roch, every divisor D with $\deg D \ge 2g$ has no base points. But if $g \ge 2$, the canonical divisor K, which is of degree $2g - 2$, has no base points. For p to be a base point of $|D|$, it will mean $\ell(D - p) = \ell(D)$.

In case that $|D|$ has no base point, there is a natural map

$$\begin{array}{lll} X & \to & \boldsymbol{P}^k \qquad\qquad k = \ell(D) - 1 \\ p & \mapsto & (f_0(p) : f_1(p) : \cdots : f_k(p)) \end{array}$$

where $f_0, f_1, \cdots, f_k$ form a basis of $L(D)$. When $k = 1$, the degree of this map is the degree of the divisor.

Definition 3.1: By a g_d^r we mean the linear system of effective divisors linearly equivalent to a given divisor D (i.e., $\boldsymbol{P}(L(D))$) with $r + 1 = \ell(D)$ and $d = \deg(D)$.

Definition 3.2: A curve X of genus $g \ge 2$ is called *hyperelliptic* if its function field has an involution I such that the fixed field of I is isomorphic to $k(x)$, the field of rational functions. Equivalently, if there is a morphism of degree two onto $\boldsymbol{P}^1$.

On a hyperelliptic curve there is a unique g_2^1 which is the pull-back of the unique g_1^1 on $\boldsymbol{P}^1$, i.e., the linear system of divisors $P + P'$, where P, P' are two points with the same image under the map of our curve to $\boldsymbol{P}^1$. Every effective canonical divisor is a sum of $g - 1$ divisors from this system g_2^1. An effective divisor in g_2^1 will be denoted by J.

Lemma 3.1: Suppose X is a hyperelliptic curve of genus $g \ge 2$ defined over an algebraically closed field or a finite field. Let J be an effective divisor in g_2^1, the unique linear system of degree 2 and dimension 1 defining the degree 2 map $X \to \boldsymbol{P}^1$. Then

1) There are at most $2(g + 1)$ points T in X such that $2T \sim J$.
2) For every point P, there is a unique point Q such that $P + Q \sim J$.
3) Let $D = P_1 + \cdots + P_{g-1}$ and $D' = Q_1 + \cdots + Q_{g-1}$ be two effective divisors of degree $g - 1$. Suppose no two P_i and P_j with the property that $P_i + P_j \sim J$. Then $D \sim D'$ implies $D = D'$.

Proposition 3.2:

1) Let $D = P_1 + \cdots + P_{g+1}$ be an effective divisors of degree $g + 1$ and the dimension of the complete linear system $|D|$ be one. Then for $|D|$ to have a base point, it is necessary and sufficient that $P_i + P_j \sim J$ for some P_i, P_j.

2) Let $C(X, \mathcal{P}, G)$ be a geometric MDS code with condition (1.1). Then the complete linear system $|G - \mathcal{P}(k-2)|$ either has no base points or it is linearly equivalent to $J + E$ for some effective divisor E.

Proof:

1) Suppose that $P_1 + P_2 \sim J$. Since

$$|P_1 + P_2| \subseteq |P_1 + P_2 + \cdots + P_{g+1}|$$

by the dimension consideration, we conclude that

$$|P_1 + P_2| = |P_1 + P_2 + \cdots + P_{g+1}|.$$

So all $P_3, \cdots P_{g+1}$ are base points of $|D|$.

Conversely, let us assume P_1 is a base point of $|D|$. Then

$$\ell(D - P_1) = \ell(D) = 2 = \ell(K - D + P_1) + 1$$

by Riemann–Roch theorem, where K is an effective canonical divisor. Hence $\ell(K - D + P_1) = 1$. We get an effective divisor E, whose degree is $2g - 2 - (g+1) + 1 = g - 2$, such that $K \sim P_2 + \cdots + P_{g+1} + E$. Recall that every effective canonical divisor is a sum of $g - 1$ divisors from g_2^1. Some couple of the $P_2, \cdots, P_{g+1}$ must pair up so that their sum is linearly equivalent to J.

2) It follows directly from 1) above and Lemma 2.2. □

Proposition 3.3: Let X be a hyperelliptic curve defined over a finite field F_q. Let $C(X, \mathcal{P}, G)$ be a geometric MDS code with $\deg \mathcal{P} = n > \deg G$. Let

$$q_0 = 8g^2 + 4g + 8 + 8g\sqrt{g^2 + g + 2}$$

and

$$q_1 = 8g^2 + 4g + 8 - 8g\sqrt{g^2 + g + 2}.$$

Suppose $n > q + 1$. Then there exist at least $\left[\frac{n}{4}\right] + 3$ pairs of points (P, P') in $\mathcal{P}$ such that $P + P' \sim J$ provided $q > q_0$ or $q < q_1$.

Proof: The process of seeking, such a pair is given in 2) of Lemma 3.1, since X is hyperelliptic. Excluding the possible $2(g+1)$ points of the type in 1) of Lemma 3.1, suppose we can gather at most $\left[\frac{n}{4}\right] + 2$ pairs. Then for each of the remaining

$$n - 2(g+1) - 2\left(\left[\frac{n}{4}\right] + 2\right)$$

points P in $\mathcal{P}$ its counterpart P' is outside $\mathcal{P}$. This gives

$$n - 2(g+1) - 2\left(\left[\frac{n}{4}\right] + 2\right) \leq N - n \tag{3.1}$$

where N is the number $|X(F_q)|$. Equation (3.1) is equivalent to

$$2n - 2\left[\frac{n}{4}\right] - 2(g+1) - 4 \leq N.$$

Using $n \geq q + 2$ and the Hasse–Weil bound $N \leq 1 + q + 2g\sqrt{q}$, we deduce from (3.1)

$$\begin{aligned} 1 + q + 2g\sqrt{q} &\geq \frac{3}{2}n - 2(g+1) - 4 \\ &\geq \frac{3}{2}(q+2) - 2(g+1) - 4 \end{aligned}$$

which is equivalent to

$$4g\sqrt{q} + 4(g+2) \geq q. \tag{3.2}$$

Therefore, if X is over a finite field F_q with

$$q > 4g\sqrt{q} + 4(g+2) \tag{3.3}$$

then we will get a contradiction. It is easy to see that (3.3) holds if and only if

$$q^2 - 8q(2g^2 + g + 2) + 16(q+2)^2 > 0. \tag{3.4}$$

The roots of the left-hand side of (3.4) are given by

$$q = 8g^2 + 4g + 8 \pm 8g\sqrt{g^2 + g + 2}.$$

Hence (3.3) holds if and only if $q > q_0$ or $q < q_1$. □

Proposition 3.4: Let X be a hyperelliptic curve defined over a finite field F_q. Let $C(X, \mathcal{P}, G)$ be a geometric MDS code with word length $n > q + 1$, dimension $k \leq \frac{n}{2}$, and $\deg \mathcal{P} = n > \deg G$. Let

$$q_0 = 8g^2 + 4g + 8 + 8g\sqrt{g^2 + g + 2}$$

and

$$q_1 = 8g^2 + 4g + 8 - 8g\sqrt{g^2 + g + 2}.$$

Suppose k is odd and

$$\mathcal{P}(k-3) = P_1 + P_2 + \cdots + P_{k-3}$$

consists of pairs

$$P_1 + P_2 \sim P_3 + P_4 \sim \cdots \sim P_{k-4} + P_{k-3} \sim J.$$

Then

1) For any $Q \in \mathcal{P} \backslash \mathcal{P}(k-3)$, the complete linear system $|G - \mathcal{P}(k-3) - Q|$ has no base point for $q > q_0$, or $q < q_1$.
2) The complete linear system $|G - \mathcal{P}(k-3)|$ has no base point for $q > q_0$, or $q < q_1$.
3) The complete linear system $|G - \mathcal{P}(k-5)|$ has no base point for $q > q_0$ or $q < q_1$ where $\mathcal{P}(k-5) = P_1 + \cdots + P_{k-5}$ consists of pairs

$$P_1 + P_2 \sim P_3 + P_4 \sim \cdots \sim P_{k-6} + P_{d-5} \sim J.$$

Proof:

1) In view of Proposition 3.3, there are $t = \left[\frac{n}{4}\right] + 3$ pairs of $\{Q_i, Q_i'\}$ such that $Q_i + Q_i' \sim J$. For any $Q \in \mathcal{P} \backslash \mathcal{P}(k-3)$, if the complete linear system $|G - \mathcal{P}(k-3) - Q|$ has a base point, then by 2) of Proposition 3.2, we have

$$G - \mathcal{P}(k-3) - Q \sim J + E$$

for some effective divisor E. Since

$$\frac{k-3}{2} + 1 \leq \frac{n}{4} + 2 < t$$

we can take one pair of $\{Q_i, Q_i'\}$, which is disjoint from both $\mathcal{P}(k-3)$ and Q, to represent J. From this we get $G - \mathcal{P}(k) \sim E$ for some $\mathcal{P}(k)$, which contradicts Lemma 2.2. So we have shown that for any $Q \in \mathcal{P} \backslash \mathcal{P}(k-3)$, the complete linear system $|G - \mathcal{P}(k-3) - Q|$ has no base point.

2) Observe that if A and B are two divisors such that $A = B + C$ for some effective divisor $C \geq 0$, then $|B| \subseteq |A|$. If p is a base point of $|A|$, then it either appears in C, or is a base point of $|B|$. For any $Q \in \mathcal{P} \backslash \mathcal{P}(k-3)$, we consider $G - \mathcal{P}(k-3) = G - \mathcal{P}(k-3) - Q + Q$. If $|G - \mathcal{P}(k-3)|$ has base points, then Q must be a base point of $|G - \mathcal{P}(k-3)|$. But this is true for any $Q \in \mathcal{P} \backslash \mathcal{P}(k-3)$. Therefore,

$$\begin{aligned} n - (k-3) &= \deg\left(\mathcal{P} \backslash \mathcal{P}(k-3)\right) \leq \deg\left(G - \mathcal{P}(k-3)\right) \\ &= \deg G - (k-3) \end{aligned}$$

which contradicts to our hypothesis $n > \deg G$.

3)

$$\begin{aligned} &G - \mathcal{P}(k-5) \\ &\quad = (G - \mathcal{P}(k-5) - P_{k-4} - P_{k-3}) + (P_{k-4} + P_{k-3}) \\ &\quad = (G - \mathcal{P}(k-3)) + (P_{k-4} + P_{k-3}). \end{aligned}$$

Recall that $\ell(G - \mathcal{P}(k-3)) = 3$. So $G - \mathcal{P}(k-3)$ is a linear equivalent to an effective divisor. Since $|G - \mathcal{P}(k-3)|$ and $|P_{k-4} + P_{k-3}| = |J|$ have no base point, $G - \mathcal{P}(k-5)$ has no base point. □

Theorem 3.5: Let X be a hyperelliptic curve of genus g defined over F_q with

$$q > 8g^2 + 4g + 8 + 8g\sqrt{g^2+g+2}$$

or

$$q < 8g^2 + 4g + 8 - 8g\sqrt{g^2+g+2}.$$

Let $\mathcal{P}$ and G be divisors with $2g-2 < \deg G < n$. If $C(X,\mathcal{P},G)$ is a geometric MDS code, then its length $n \le q+2$.

Proof: By taking the dual code, we may assume that the code is of dimension $k \le n/2$. By Proposition 3.3, there are $t = [\frac{n}{4}] + 3$ pairs $\{P_i, P_i'\}$ such that $P_i + P_i' \sim J$.

Case i). k is even. Observe that the class

$$[D] = [P_1 + P_1' + \cdots + P_{(k-2)/2} + P'_{(k-2)/2}]$$

satisfies the hypothesis $\mathcal{C}[X,\mathcal{P},k-2]$ since

$$[\frac{n}{4}] + 3 \ge \frac{k-2}{2} + 3.$$

By the proof of Proposition 2.5, we have $n \le q+1$.

Case ii). k is odd. Consider the divisor

$$D = G - P_1 - P_1' - \cdots - P_{(k-3)/2} - P'_{(k-3)/2} - Q$$

from some $(k-3)/2$ pairs and a $Q \in \mathcal{P}$ not in $\{P_1, P_1', \cdots, P_{(k-3)/2}, P'_{(k-3)/2}\}$. D is a divisor of degree

$$\deg(G) - (k-3) - 1 = \deg G - k + 2 = g + 1$$

by (1.2). By Lemma 2.2, $\ell(D) = 2$. In view of 2) of Proposition 3.4, we know that $|D|$ has no base point. Hence the complete linear system $|D|$ defines a morphism $\phi : X \to \mathbf{P}^1$. This map is defined over F_q. If $n \ge q+3$, then the map ϕ restricted on $\mathcal{P}\backslash\{Q\}$ is not one-to-one since $\boldsymbol{P}^1$ has only $q+1$ rational points. Suppose $\phi(Q_1) = \phi(Q_2)$ for a distinct Q_1 and Q_2 in $\mathcal{P}\backslash\{Q\}$. Then there is an effective divisor in the system $|D|$ of the form $Q_1 + Q_2 + E$, where E is an effective divisor. Thus

$$G \sim P_1 + P_1' + \cdots + P_{(k-3)/2} + P'_{(k-3)/2} + Q + Q_1 + Q_2 + E.$$

Since $[n/4] + 3 \ge (k-3)/2 + 3$, we can replace those pairs $\{P_i, P_i'\}$ which hit Q_1 or Q_2. Given that situation, all the P's and Q's are distinct and we have

$$G - \mathcal{P}(k) \sim E.$$

This contradicts Lemma 2.2. □

Lemma 3.6: Let S be a set of $q+2$ rational points in the projective plane $\boldsymbol{P}^2$ over F_q. Suppose that q is odd. Then there exist three distinct points in S which are colinear.

Proof: The observation is that for any point there are exactly $q+1$ lines passing this point. Suppose on the contrary that there are no three distinct points in S which are colinear. For any $Q \in S$, each line passing Q must pass exactly one other point in $S\backslash\{Q\}$ since no three points are colinear and there are $q+1$ points in $S\backslash\{Q\}$. Thus points of S are coupled into pairs by lines. Hence $q+2$ is an even number, which is impossible if q is odd. □

The following lemma was proved by finite geometry in [5, pt I, pp. 326–328]. In fact, it is equivalent to the nonexistence of MDS $[q+2, 5, q-2]$ linear code. (For q odd and $q > 49$, see [8]. For q even and $q > 7$, see [10].)

Lemma 3.7: Let S be a set of $q+2$ rational points in the projective space $\boldsymbol{P}^4$ over F_q where q is even. Then there exists five distinct points in S, lying on a hyperplane of $\boldsymbol{P}^4$.

Theorem 3.8: Let X be a hyperelliptic curve of genus g defined over F_q with

$$q > 8g^2 + 4g + 8 + 8g\sqrt{g^2+g+2}$$

or

$$q < 8g^2 + 4g + 8 - 8g\sqrt{g^2+g+2}.$$

Let $\mathcal{P}$ and G be divisors with $2g-2 < \deg G < n$. If $C(X,\mathcal{P},G)$ is a geometric MDS code, then $n \le q+1$ unless q even and $k=3$ or $k = q-1$ in which cases $n \le q+2$.

Proof: By the argument of Proposition 2.4, we may assume that the code is of dimension $6 \le k \le \frac{n}{2}$. In view of Proposition 3.3, there are $t = [\frac{n}{4}] + 3$ pairs $\{P_i, P_i'\}$ such that $P_i + P_i' \sim J$.

Case i). k is even. The proof is the same as the proof of Theorem 3.5, case i).

Case ii). k is odd. By Proposition 2.4, we can certainly assume $n = q+2$.

a) k is odd and q is odd. Let

$$\mathcal{P}(k-3) = P_1 + P_1' + \cdots + P_{(k-3)/2} + P'_{(k-3)/2}$$

where $P_i + P_i' \sim J$. Then $\ell(G - \mathcal{P}(k-3)) = 3$ and the complete linear system $|G - \mathcal{P}(k-3)|$ has no base point by Proposition 3.4. Consider the map $\phi : X \to \boldsymbol{P}^2$ defined by this complete linear system. Since q is odd, Lemma 3.6, we can find three distinct points A, B, and $C \in \mathcal{P}$ such that $\phi(A)$, $\phi(B)$, and $\phi(C)$ are on the line L in $\boldsymbol{P}^2$. Thus there exists an effective divisor E such that

$$G - \mathcal{P}(k-3) \sim A + B + C + E.$$

Since

$$[\frac{n}{4}] + 3 \ge \frac{k-3}{2} + 3$$

we can change appropriate pairs in $\mathcal{P}(k-3)$ so that all the $\mathcal{P}(k-3)$, A, B, and C are distinct. Therefore, $G - \mathcal{P}(k) \sim E$. Observe that

$$\begin{aligned}\deg E &= \deg(G - \mathcal{P}(k-3)) - 3 \\ &= \deg G - k = g - 1 > 0\end{aligned}$$

by (1.2). This gives a contradiction to Lemma 2.2.

b) k is odd and q is even. Let

$$\mathcal{P}(k-5) = P_1 + P_1' + \cdots + P_{(k-5)/2} + P'_{(k-5)/2}$$

where $P_i + P_i' \sim J$. Then $\ell(G - \mathcal{P}(k-5)) = 5$ and the complete linear system $|G - \mathcal{P}(k-5)|$ has no base point by Proposition 3.4. Consider the map $\phi : X \to \mathbf{P}^4$ defined by this complete linear system. By Lemma 3.7, we can find five distinct points $A_1, \cdots, A_5 \in \mathcal{P}$ such that $\phi(A_1), \cdots, \phi(A_5)$ are lying on a hyperplane H in $\boldsymbol{P}^4$. Thus there exists an effective divisor E such that

$$G - \mathcal{P}(k-5) \sim A_1 + \cdots + A_5 + E.$$

Recall that $n = q+2$ is an even number. So we have

$$\left[\frac{n}{4}\right] + \frac{1}{2} \ge \frac{n}{4}$$

and hence

$$\left[\frac{n}{4}\right] + 3 \ge \frac{k-5}{2} + 5.$$

By Proposition 3.3, there are at least $[\frac{n}{4}] + 3$ pairs of points (P, P') is $\mathcal{P}$ such that $P + P' \sim J$. We can change appropriate pairs in $\mathcal{P}(k-5)$ so that all the $\mathcal{P}(k-5)$, $A_1, \cdots, A_5$ are distinct. Therefore, $G - \mathcal{P}(k) \sim E$. Observe that

$$\begin{aligned}\deg E &= \deg\left(G - \mathcal{P}(k-5)\right) - 5 \\ &= \deg G - k = g - 1 > 0\end{aligned}$$

by (1.2). This gives a contradiction to Lemma 2.2. □

ACKNOWLEDGMENT

The authors wish to thank the referees for pointing out some misprints and their suggestions of improving the presentation of our correspondence.

REFERENCES

[1] H. Chen, "On the main conjecture of geometric MDS codes," *Int. Math. Res. Notices*, no. 8, pp. 313–318, 1994.
[2] M. A. De Boer, "MDS codes from hyperelliptic curves," preprint.
[3] G. Katsman and M. A. Tsfasman, "Spectra of algebraic geometric codes," *Probl. Pered. Inform.*, vol. 23, no. 4, pp. 18–34, 1987.
[4] S. Lang, *Fundamentals of Diophatine Geometry*. New York, Berlin, Heidelberg, Tokyo: Springer-Verlag, 1983.
[5] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes* (Parts I and II). Amsterdam, The Netherlands: North Holland, 1977.
[6] C. Munuera, "On the main conjecture on geometric MDS codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1573–1577, 1992.
[7] S. Roman, *Coding and Information Theory* (GTM 134). Berlin, Germany: Springer-Verlag, 1992.
[8] R. M. Roth and A. Lempel, "On MDS codes via Cauchy matrices," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1314–1319, 1989.
[9] H. Stichtenoth, *Algebraic Function Fields and Codes* (Universitext). Berlin, Germany: Springer-Verlag, 1993.
[10] L. Storme and J. A. Thas, "MDS codes and arcs in $PG(n, q)$ with q even: An improvement on the bounds of Bruen, Thas, and Blokhuis," *J. Comb. Theory A*, vol. 62, pp. 139–154, 1993.
[11] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic Geometric Codes*, vol. 58. Dordrecht, The Netherlands: Kluwer, 1991.

Surfaces and the Weight Distribution of a Family of Codes

M. van der Vlugt

***Abstract*—We derive the weight distribution of the binary trace codes with words $(\mathrm{Tr}\,(ax^{q+1} + bx^3 + cx)_{x \in \mathbb{F}^*_{q^2}}$ where a, b, $c \in \mathbb{F}_{q^2}$ and Tr is the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_2$. The weights of these words determine the exponential sums which were considered earlier by Moreno, Kumar, and Lahtonen. Results from the theory of quadratic forms play a role but the decisive argument is of an algebraic-geometric nature, namely, from the theory of surfaces.**

***Index Terms*—Exponential sum, quadratic form, surface, trace code, weight distribution.**

I. INTRODUCTION

In two recent papers [10] and [8], the exponential sums

$$S(a, b, c) = \sum_{x \in \mathbb{F}_{q^2}} (-1)^{\mathrm{Tr}(\mathrm{ax}^{\mathrm{q+1}} + \mathrm{bx}^3 + \mathrm{cx})}$$

were considered. Here $\mathbb{F}_{q^2}$ is a finite field of characteristic 2 and cardinality $q^2 = 2^{2m}$ with $m \geq 2$, Tr is the trace map from $\mathbb{F}_{q^2}$ onto $\mathbb{F}_2$, and a, b, $c \in \mathbb{F}_{q^2}$. Since an element of $\mathbb{F}_{q^2}$ has trace zero if and only if it is of the form $y^2 + y$ for some $y \in \mathbb{F}_{q^2}$, we see that $\#\{x \in \mathbb{F}_{q^2} : \mathrm{Tr}\,(ax^{q+1} + bx^3 + cx) = 0\}$ is half the number $\#C^{\mathrm{aff}}(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points on the affine curve C^{aff} given by

$$y^2 + y = ax^{q+1} + bx^3 + cx. \tag{1}$$

Hence $S(a, b, c) = \#C^{\mathrm{aff}}(\mathbb{F}_{q^2}) - q^2$. The nonsingular projective curve C^{proj} defined by the affine equation (1) has genus $g = q/2$ for $a \neq 0$. The curve C^{proj} has one point at infinity, namely $(0 : 1 : 0)$, so

$$\#C^{\mathrm{proj}}(\mathbb{F}_{q^2}) = \#C^{\mathrm{aff}}(\mathbb{F}_{q^2}) + 1.$$

Then the Weil bound for the number of rational points on a curve implies that for $a \neq 0$

$$|S(a, b, c)| = |\#C^{\mathrm{proj}}(\mathbb{F}_{q^2}) - 1 - q^2| 2gq = q^2.$$

In [10], Moreno and Kumar proved for triples

$$(a, b, c) \notin \mathbb{F}_q \times \{0\} \times \{0\}$$

the much sharper upper bound

$$|S(a, b, c)| \leq 4q$$

which is attained for $m \equiv 3 (\mathrm{mod}\ 6)$. Thereafter, in [8] Lahtonen showed that if $q = 2^m$ with m even then

$$|S(a, b, c)| \leq 2q, \qquad \text{for } (a, b, c) \notin \mathbb{F}_q \times \{0\} \times \{0\}.$$

The last author poses the problem whether the upper bound is $2q$ or $4q$ in case $m \equiv 1$ or $5 (\mathrm{mod}\, 6)$.

Strongly related to the exponential sums $S(a, b, c)$ is the binary trace code of length $q^2 - 1$

$$\mathcal{C} = \{\boldsymbol{c}_{a, b, c} = (\mathrm{Tr}\,(ax^{q+1} + bx^3 + cx)_{x \in \mathbb{F}^*_{q^2}}) : a, b, c \in \mathbb{F}_{q^2}\}.$$

Manuscript received April 3, 1996; revised November 19, 1996.

The author is with the Department of Mathematics and Computer Science, University of Leiden, NL-2300 RA Leiden, The Netherlands.

Publisher Item Identifier S 0018-9448(97)03776-0.