ADVANCES IN APPLIED MATHEMATICS **21,** 124–145 (1998)
ARTICLE NO. AM980591

Explicit Computation of Generalized Hamming Weights for Some Algebraic Geometric Codes

Hao Chen*

Department of Mathematics, Zhongshan University, Guangzhou, Guangdong 510275, People's Republic of China

Hing Sun Luk†

Department of Mathematics, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong

and

Stephen Yau‡

Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 South Morgan Street, Chicago, Illinois 60607-7045

Received November 14, 1997; accepted January 3, 1998

The generalized Hamming weights, introduced a few years ago by V. K. Wei, provide substantial information of codes and thus play a central role in coding theory. For algebraic geometric codes, there have been many works on their generalized Hamming weights (or weight hierarchy). However, for lots of codes from Hermitian curves and the Klein quartic, some generalized Hamming weights still have not yet been found explicitly. In this paper, we first prove a general result (Theorem 1.4) on the computation of generalized Hamming weights of geometric Goppa codes on plane curves, using the configuration of F_q-rational points on the curves. Then we give the exact values (Theorem 2.2) of the first and second generalized Hamming weights of some codes arising from the Klein quartic. Our main result (Theorem 2.3) gives the exact values of the second and third generalized Hamming weights of certain codes from Hermitian curves. In the Appendix, a previous known result of Yang, Kumar, and Stichtenoth for Hermitian codes is shown to follow from Theorem 1.4. We also give the exact values of the first three generalized Hamming weights for Fermat codes. © 1998 Academic Press

[*] Research supported by NSF of China and Guangdong Provincial NSF of China.

[†] E-mail: hsluk@math.cuhk.edu.hk.

[‡] Research partially supported by ARO DAAH04-1-0530, NSF DMS 9321262. E-mail: yau@uic.edu.

0196-8858/98 $25.00

0. INTRODUCTION

Let F_q be a finite field with q elements, where q is a power of the prime $p = \operatorname{char} F_q$. For a linear $[n, k]$ code C over F_q (i.e., a linear subspace $C \subseteq F_q^n$ of dimension k), it was Wei [21] who first introduced the notion of generalized Hamming weights d_r for $1 \leq r \leq k$ which provide substantial information on the codes. Since then, the generalized Hamming weights have played a central role in coding theory. For any subset $A \subseteq C$, we define

$$\operatorname{supp} A = \{i: \text{there is an element } a = (a_1, \dots, a_n) \in A \text{ with } a_i \neq 0\}.$$

The rth generalized Hamming weight d_r of C is defined by

$$d_r := \min\{\# \operatorname{supp} D: D \text{ is an } r\text{-dimensional subcode of } C\},$$

where $\# \operatorname{supp} D$ is the cardinality of the set $\operatorname{supp} D$. It is clear that d_1 is the minimum distance of C. These notions, which were introduced by Wei because of a problem in cryptography, give new insight into coding theory. The generalized Hamming weights have been studied by many authors (Hamming codes, Reed–Muller codes, Golay codes, and MDS codes [21]; some classes of BCH codes [5–8]; some trace codes [17]; duals of BCH codes and Melas codes [6, 9]; codes from Hermitian varieties [11]; and codes from hyperelliptic curves [15]). For an excellent survey of this subject, we refer to [20].

For algebraic geometric codes (or geometric Goppa codes), Yang, Kumar, and Stichtenoth [23] and Munuera [15] gave very nice works on the generalized Hamming weights. They proved some fundamental results (e.g., Theorem 12 in [23] and Corollary 1 in [15]) and used these results and the gonality sequences of Hermitian curves (also of the Klein quartic and hyperelliptic curves in [15]) to determine d_r in many cases. Their approaches are basically algebraic. In case of Hermitian codes C_m (i.e., codes from Hermitian curves with rational divisor mQ_∞ and the set of q^3 F_q-rational points disjoint from Q_∞), only when m or $q^3 - m$ is a pole number at Q_∞ can explicit results about d_r be obtained (see Theorems 22 and 25 in [23] and Proposition 13 in [15]). In Theorem 27 of [23], some quite restrictive results on d_r of C_m were given in case $q^3 - m$ is not a pole number at Q_∞. In all of their results on d_r ($r \geq 2$), they need that the equality in Theorem 12 of [23] holds. This motivates us to study the generalized Hamming weights of Hermitian codes C_m with $m = q^3 - q + b$, $1 \leq b \leq q - 2$. Our approach is basically geometric and uses a very careful analysis of linear systems on Hermitian curves. We determine explicitly d_2 and d_3 for C_m in this case. It seems that the previous algebraic method cannot be applied here because our results show that the equality in Theorem 12 of [23] cannot hold for d_2, d_3 in this case. Comparing our approach with Hansen's work [10], we also give some new results on d_r (especially d_1) for codes from the Klein quartic which have been studied in [10].

The starting point of our work is the beautiful result due to Munuera [15] (Proposition 1.1 below) that, in practice, gives us the upper bounds of the generalized Hamming weights. This, together with another beautiful observation of Yang, Kumar, and Stichtenoth on the lower bounds of the generalized Hamming weights, should give us precise information on the generalized Hamming weights.

In Section 1, for the convenience of the reader, we recall some basic results on d_r for algebraic geometric codes and Pellikaan's results about gonality sequences of plane curves over perfect fields. We then prove a general result on the computation of generalized Hamming weights for algebraic geometric codes using the configuration of F_q-rational points on the curves (see Theorem 1.4). In Section 2, we prove our main results, Theorems 2.3 and 2.2. In Section 3, we study the generalized Hamming weights for Fermat curves. To make our paper more self-contained, we give, in an appendix, geometric proofs of Munuera's upper bounds and Yang, Kumar, and Stichtenoth's lower bounds mentioned above. Our proofs are different from their algebraic proofs and are more in line with our approach in this paper. To show the usefulness of Theorem 1.4, we use it to recover a result on the generalized Hamming weights of Hermitian curves due to Yang, Kumar, and Stichtenoth.

1. GENERAL RESULTS

Let X be an irreducible smooth projective curve over F_q (finite field with q elements) of genus g, G be an F_q-rational divisor on X, and $P = \{P_1, P_2, \ldots, P_n\}$ be a set of n F_q-rational points of X. We assume that G is disjoint from P and $2g - 2 < \deg G < n$ for simplicity. The algebraic geometric code $C = C(X, P, G)$ is defined to be the image of the following evaluation map:

$$\begin{aligned} ev_p\colon L(G) &\to F_q^n \\ f &\mapsto (f(P_1), f(P_2), \ldots, f(P_n)), \end{aligned}$$

where $L(G) = \{f \in F_q(X)\colon (f) + G \geq 0\} \cup \{0\}$ is the function space associated to G (see [19, 20]). There are many interesting works about generalized Hamming weights of algebraic geometric codes ([15, 23] and the references in [20]). We refer to II, Section 5 in [20] for a survey. The following two results due to Munuera [15] and Yang, Kumar, and Stichtenoth [23] are fundamental to our paper.

PROPOSITION 1.1 (Munuera [15]). *For the algebraic geometric code $C = C(X, P, G)$ as above, we have the rth generalized Hamming weight*

$$d_r = \min\{\deg P' : 0 \le P' \le P \textit{ such that } \ell(G - P + P') \ge r\}$$

for any r, $1 \le r \le \dim C$.

PROPOSITION 1.2 (Yang, Kumar, and Stichtenoth [23]). *For the rth generalized Hamming weight of the algebraic geometric code $C = C(X, P, G)$ as above, we have*

$$d_r \ge n - \deg G + \nu_r,$$

where $\nu_r = \min\{\deg D \colon D$ effective, $\ell(D) \ge r\}$ is the rth gonality of X for any r, $1 \le r \le \dim C$.

From the previous two results, we understand that the gonality sequence ν_r for $r = 1, 2, \dots$ is of fundamental importance for determining the generalized Hamming weights of algebraic geometric codes.

Remark 1.1. Obviously, $\nu_1 = 0$, since we may choose D to be the zero divisor in the definition of ν_1. ν_2 is the usual gonality (see Remark 10 in [23]), which is the smallest degree of a nonconstant map, defined over the field F_q, from X to the projective line. It was shown in [12] that ν_2 is equal to $\deg(X) - 1$. In general, we have the following proposition.

PROPOSITION 1.3 (Pellikaan [16]). *Let X be a nonsingular plane curve of degree d over a perfect field (any finite field is a perfect field). Let k be a positive integer, and write $k = \frac{1}{2}(j+1)(j+2) - i$ with $0 \le i \le j$. Then*

$$\nu_k = \begin{cases} k + g - 1 & \textit{if } k > g, \\ jd - i & \textit{if } k \le g, \end{cases}$$

where g is the genus of X ($g = \frac{1}{2}(d-1)(d-2)$).

THEOREM 1.4. *Let $X \subset \mathbf{P}^2$ be an irreducible smooth plane curve over F_q of degree $d \ge 4$ and Q be an F_q-rational point on X. Let $L_1, L_2, \dots, L_t$ be t F_q-lines in $\mathbf{P}^2$ (i.e., curve defined over F_q with degree 1) that intersect X at F_q-rational points $\{Q, P_1^1, P_2^1, \dots, P_{d-1}^1\}$, $\{Q, P_1^2, P_2^2, \dots, P_{d-1}^2\}, \dots,$ $\{Q, P_1^t, P_2^t, \dots, P_{d-1}^t\}$.*

Assume that there exists a hyperplane divisor on X of the form dQ. Consider the algebraic geometric code $C = C(X, P, G)$, where $G = u(d-1)Q$ and $P = \{P_1^1, P_2^1, \dots, P_{d-1}^1, P_1^2, P_2^2, \dots, P_{d-1}^2, \dots, P_1^t, P_2^t, \dots, P_{d-1}^t\}$ with $u < t$.

Let d_1, d_2, d_3 be the generalized Hamming weights of $C = C(X, P, G)$. Then

$$d_1 = (t-u)(d-1),$$
$$d_2 = (t-u+1)(d-1),$$
$$d_3 \geq (t-u)(d-1) + d.$$

Proof. Let L be a hyperplane divisor on X. For any effective divisor P' with $0 \leq P' \leq P = P_1^1 + P_2^1 + \cdots + P_{d-1}^1 + P_1^2 + P_2^2 + \cdots + P_{d-1}^2 + \cdots + P_1^t + P_2^t + \cdots + P_{d-1}^t$, we have

$$G - P + P' \sim u(L-Q) - (L_1 - Q) - (L_2 - Q) - \cdots - (L_t - Q) + P'$$
$$\sim P' - (L_1 - Q) - (L_2 - Q) - \cdots - (L_{t-u} - Q).$$

Thus, for $P' = (L_1 - Q) + (L_2 - Q) + \cdots + (L_{t-u} - Q)$, we have $\ell(G - P + P') = 1$. So we have $d_1 \leq \deg P' = (t-u)(d-1)$. On the other hand, it is well known that (see, e.g., Lemma 2.3(i) of [4]) $d_1 \geq n - \deg G = (t-u)(d-1)$. Hence, we have $d_1 = (t-u)(d-1)$.

For d_2, we first recall that $\nu_2 = d-1$ by Remark 1.1. In view of Proposition 1.2, we have $d_2 \geq (t-u)(d-1) + d - 1$. On the other hand, take $P' = (L_1 - Q) + (L_2 - Q) + \cdots + (L_{t-u} - Q) + (L_{t-u+1} - Q)$ in the definition of d_2. In view of the previous calculation, we have $G - P + P' \sim L_{t-u+1} - Q$. Therefore, $\ell(G - P + P') = \ell(L_{t-u+1} - Q) = 2$, since $\ell(L_{t-u+1}) = 3$. By Proposition 1.1, $d_2 \leq \deg P' = (d-1)(t-u+1)$. Thus, we get the conclusion $d_2 = (t-u+1)(d-1)$.

For d_3, we first apply Proposition 3 in [15], which is due to Pellikaan, to get the 3-gonality $\nu_3 = d$. By Proposition 1.2, $d_3 \geq n - \deg G + \nu_3 = t(d-1) - u(d-1) + d = (t-u)(d-1) + d$. Q.E.D.

2. CODES FROM HERMITIAN CURVE AND KLEIN QUARTIC

We first treat the codes arising from a Klein quartic. A Klein quartic X is defined in $\mathbf{P}^2$ with $F_{2^3} = F_8$ with the equation

$$x^3y + y^3z + z^3x = 0. \tag{2.1}$$

It is clear that this is a smooth curve and therefore has genus $g = 3$. Since $x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x-1)(x^6 + x^4 + x^3 + x^5 + x^3 + x^2 + x^3 + x + 1) = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$ (because char $F_q = 2$), we can find an element $\alpha \in F_8$ such that $\alpha^3 + \alpha + 1 = 0$. The following proposition is due to Hansen [10].

PROPOSITION 2.1 (Hansen [10]). *Let F_8 be represented as $\mathbf{Z}_2[\alpha]/(1+\alpha+\alpha^3)$, and let $X \subseteq \mathbf{P}^2$ over F_8 be the Klein quartic with* (2.1). *Then*

(1) *The automorphisms A and B with matrices*

$$A = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^4 & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in GL_3(F_8)$$

are rational automorphisms of X.

(2) *The group $\mathfrak{G} = \langle A, B \rangle$ of automorphisms generated by A and B is the Frobenius group of order* 21. *In fact, $A^7 = I$, $B^3 = I$, and $B^{-1}AB = A^4$.*

(3) *The curve X has precisely* 24 *rational points, namely, $Q_0 = (1:0:0)$, $Q_1 = (0:1:0)$, $Q_2 = (0:0:1)$, and*

$$P_{ij} = B^i A^j P_{00}, \qquad i = 0, 1, 2,\ j = 0, 1, \dots, 6,$$

where $P_{00} = (1 : \alpha^2 : \alpha + \alpha^2)$.

(4) *The action of the Frobenius group $\mathfrak{G}$ on the* 24 *rational points of X has two orbits, namely, $\{Q_0, Q_1, Q_2\}$ and $\{P_{ij}\colon i = 0, 1, 2,\ j = 0, 1, \dots, 6\}$.*

In what follows, we shall describe X in a more geometric way. We first observe that the F_8-rational line $x = y$ intersects X on the four F_8-rational points $\{(0:0:1), (\beta_1 : \beta_1 : 1), (\beta_2 : \beta_2 : 1), (\beta_3 : \beta_3 : 1)\}$, where $\beta_1, \beta_2, \beta_3$ are three distinct roots of $x^3 + x^2 + 1 = 0$ in F_8. The transformation of the line $x = y$ under A also intersects X at four F_8-rational points. Note that A is of order 7. So we have seven lines. Denote $Q_0 = (1:0:0)$, $Q_1 = (0:1:0)$, $Q_2 = (0:0:1)$:

$L_1\colon x = y$	Q_2, P_1^1, P_2^1, P_3^1
$L_2\colon \alpha^3 x = y$	Q_2, P_1^2, P_2^2, P_3^2
$L_3\colon \alpha^6 x = y$	Q_2, P_1^3, P_2^3, P_3^3
$L_4\colon \alpha^2 x = y$	Q_2, P_1^4, P_2^4, P_3^4
$L_5\colon \alpha^5 x = y$	Q_2, P_1^5, P_2^5, P_3^5
$L_6\colon \alpha x = y$	Q_2, P_1^6, P_2^6, P_3^6
$L_7\colon \alpha^4 x = y$	Q_2, P_1^7, P_2^7, P_3^7

These seven lines intersect X at $1 + 7 \times 3 = 22$ F_8-rational points. Adding Q_0 and Q_1, we get 24 F_8-rational points on X. The Weil−Serre bound says that there are at most 24 F_8-rational points on X. Therefore, there are exactly 24 F_q-rational points on X.

We observe that by applying B to the seven lines $L_1, \ldots, L_7$, we get another seven lines passing through $B(Q_2) = Q_0$. Clearly, $\bigcup_{i=1}^{7}(B(L_i) - \{Q_0\}) = \bigcup_{i=1}^{7}(L_i - \{Q_2\})$ because B leaves the set $\{P_j^i\colon 1 \le i \le 7, 1 \le j \le 3\}$ invariant. We can repeat the same construction and get seven lines passing through Q_1.

Consider the hyperplane defined by $x = 0$. It is easy to check that this hyperplane intersects X only at two points: Q_2 with multiplicity 3 and Q_1 with multiplicity 1. Let H denote the hyperplane divisor on X. Then, by considering $x = 0$, we get $H \sim 3Q_2 + Q_1$ (where $\sim$ denotes the usual linear equivalence of divisors). Similarly, we have $H \sim 3Q_0 + Q_2 \sim 3Q_1 + Q_0$.

We now use the configuration of F_8-rational points on the Klein quartic to compute the generalized Hamming weights of the algebraic geometric code $C = C(X, P, G)$, where $G = m(Q_0 + Q_1 + Q_2)$ with $m = 3, 4, 6$ and $P = \{P_j^i\}$, $1 \le i \le 7$, $1 \le j \le 3$. Hansen [10] has given the lower bound of the minimal distance of this code. However, some of the lists on page 924 of [10] are wrong (e.g., (21, 16, 3) is wrong, and there also might be some problem with lists (21, 4, 15) and (21, 13, 6)).

THEOREM 2.2. *For the algebraic geometric code $C = C(X, P, G)$ defined as above, we have $2g - 2 < \deg G < n$ for $m \ge 3$. Moreover,*

(i) *if $m = 3$, then $d_1 = 12$ and $d_2 = 15$;*

(ii) *if $m = 4$, then $d_1 = 9$ and $d_2 = 12$;*

(iii) *if $m = 6$, then $d_1 \ge 4$.*

Proof. (i) We take three lines as follows:

$$\begin{array}{ll}
L_1\colon x = y & Q_2, P_1^1, P_2^1, P_3^1 \\
B(L_1)\colon y = z & Q_0, B\left(P_1^1\right), B\left(P_2^1\right), B\left(P_3^1\right) \\
B^2(L_1)\colon z = x & Q_1, B^2\left(P_1^1\right), B^2\left(P_2^1\right), B\left(P_3^1\right)
\end{array}$$

Let $P' = P - (L_1 - Q_2) - (B(L_1) - Q_0) - (B^2(L_1) - Q_1)$. Then $G - P + P' = 3(Q_0 + Q_1 + Q_2) - P + P'$. Let H denote the hyperplane divisor on X. Recall that $H \sim 3Q_2 + Q_1$ $(x = 0)$, $H \sim 3Q_0 + Q_2$ $(y = 0)$, and $H \sim 3Q_1 + Q_2$ $(z = 0)$. Therefore, $G - P + P' = 4(Q_0 + Q_1 + Q_2) - 3H \sim 0$. In view of Proposition 1.1, we have $d_1 \le \deg P' = \deg P - 9 = 21 - 9 = 12$. On the other hand, for the algebraic geometry code $C(X, P, G)$, we have $d_1 \ge n - \deg G$ (see Proposition 1.2 and Remark 1.1 above or Lemma 2.3(i) of [4]). So $d_1 \ge 21 - 3 \times 3 = 12$. The conclusion $d_1 = 12$ follows.

For d_2, we shall take $P' = P - (L_1 - Q_2) - (B(L_1) - Q_0)$. Then $G - P + P' = 3(Q_0 + Q_1 + Q_2) - (P - P') = 3(Q_0 + Q_1 + Q_2) - (L_1 - Q_2) - (B(L_1) - Q_0) = 4(Q_0 + Q_1 + Q_2) - 2H \sim Q_1 \sim H - Q_1$. So $\ell(G - P + P') = \ell(H - Q_1) = 2$. In view of Proposition 1.1, we have

$d_2 \leq \deg P' = 21 - 3 - 3 = 15$. On the other hand, by Proposition 1.2 and Remark 1.1, we have $d_2 \geq n - \deg G + \nu_2 = 21 - 9 + 3 = 15$. The conclusion $d_2 = 15$ follows.

(ii) Let $P' = (L_1 - Q_1) + (B(L_1) - Q_0) + (B^2(L_1) - Q_2)$. Now we are going to show that $P \sim 6H - Q_0 - Q_1 - Q_2$, where H denotes the hyperplane divisor on X. Consider the six lines

$$\begin{aligned} &U_1\colon x = y,\\ &U_2\colon y = z,\\ &U_3\colon z = x,\\ &U_4\colon \beta_1^3 x + \beta_1^2 y + z = 0,\\ &U_5\colon x + \beta_1^3 y + \beta_1^2 z = 0,\\ &U_6\colon \beta_1^2 x + y + \beta_1^3 z = 0, \end{aligned}$$

where $\beta_1^3 + \beta_1^2 + 1 = 0$ and $\beta_1 = \alpha^5$. Note that all six lines pass through the point $(1, 1, 1)$ which is not in the Klein quartic. Thus, any of these two lines do not have an intersection point on the Klein quartic. It is quite clear that each of the first three lines U_1, U_2, and U_3 intersects the Klein quartic at the points in P and one point in $\{Q_1, Q_2, Q_3\}$. Line U_4 intersects the Klein quartic at the four points $\{(\beta_1^2, \beta_1^6, 1), (\beta_1, \beta_1^4, 1), (1, \beta_1^2, \beta_1), (\beta_1^5, \beta_1^3, 1)\}$ in P. Here we have to use the facts $\beta_1^3 + \beta_1^2 + 1 = 0$, $\beta_1^5 + \beta_1 + 1 = 0$, and $\beta_1^6 + \beta_1^4 + 1 = 0$. Note that the lines U_5 and U_6 are the images of U_4 under suitable power of the transformation B. Thus, they intersect the Klein quartic also at F_8-rational points. Clearly, the intersection of the union of these six lines $U_1, \ldots, U_6$ with the Klein quartic gives us precisely the 24 points $P \cup \{Q_0, Q_1, Q_2\}$. Thus, we have shown that $P \sim 6H - Q_0 - Q_1 - Q_2$,

$$\begin{aligned} G - P + P' &\sim 4(Q_0 + Q_1 + Q_2) - 6H + Q_0 + Q_1 + Q_2 + P'\\ &\sim 3H - 6H + 3H \sim 0. \end{aligned}$$

In view of Proposition 1.1, we have $d_1 \leq \deg P' = 9$. On the other hand, for the algebraic geometry code $C(X, P, G)$, we have $d_1 \geq n - \deg G = 21 - 12 = 9$. The conclusion $d_1 = 9$ follows.

For d_2, we take P' to be the union of $(L_1 - Q) + (G(L_1) - Q_0) + (B^2(L_1) - Q_2)$ and any three intersection points of U_4 with X. Then, $G - P + P' \sim$ the three intersection points of U_4 with X. So $\ell(G - P + P') = 2$. In view of Proposition 1.1, we have $d_2 \leq \deg P' = 9 + 3 = 12$. On the other hand, by Proposition 1.2 and Remark 1.1, we have $d_2 \geq n - \deg G + \nu_2 = 21 - 12 + 3 = 12$. The conclusion $d_2 = 12$ follows.

(iii) By Proposition 1.2 and Remark 1.1, we have $d_1 \geq n - \deg G = 21 - 18 = 3$. If $d_1 = 3$, we can find $P' \subseteq P$ such that P' consists of three points and $\ell(G - P + P') \geq 1$. Observe that $\deg(G - P + P') = 18 - 21 + 3 = 0$. Hence, $G - P + P' \sim 0$, that is, $6(Q_0 + Q + Q_2) - 6H + Q_0 + Q_1 + Q_2 + P' \sim 8(Q_0 + Q_1 + Q_2) - 6H + P' - Q_0 - Q_1 - Q_2 \sim P' - Q_0 - Q_1 - Q_2 \sim 0$. This implies $P' \sim Q_0 + Q_1 + Q_2$. It follows that $\ell(Q_0 + Q_1 + Q_2) \geq 2$. From the Riemann–Roch theorem for curves, we have

$$\ell_X(Q_0 + Q_1 + Q_2) - \ell_X(K_X - (Q_0 + Q_1 + Q_2)) \\ = \deg(Q_0 + Q_1 + Q_2) - g + 1,$$

where K_X is the canonical divisor of X. So we have $\ell_X(K_X - (Q_0 + Q_1 + Q_2)) = \ell_X(Q_0 + Q_1 + Q_2) - 1 \geq 1$. Note that the degree of the curve is 4. By the adjunction formula, we have $K_X = H$ on X, where H is a line in $\mathbf{P}^2$. So we have $\ell_X(H - (Q_0 + Q_1 + Q_2)) \geq 1$. Clearly, $L_X(H - (Q_0 + Q_1 + Q_2)) \subseteq L_X(H)$. From the exact sequence

$$0 \to \mathcal{O}_{\mathbf{P}^2}(-3) \to \mathcal{O}_{\mathbf{P}^2}(H) \to \mathcal{O}_X(H) \to 0,$$

we have $L_X(H) = L_{\mathbf{P}^2}(H)$. On the other hand, $L_{\mathbf{P}^2}(H)$ is spanned by three coordinates x, y, z over F_8. Hence, we can find a function $(ax + by + cz)/(a_0 x + b_0 y + c_0 z)$ vanishing at Q_0, Q_1, and Q_2. Here we assume that H is defined by $a_0 x + b_0 y + c_0 z = 0$. Therefore, Q_0, Q_1, and Q_2 are collinear. This is a contradiction. Thus, we have proved $d_1 \geq 4$. Q.E.D.

Let K be a finite field F_{q^2} of q^2 elements, where q is a power of the prime char K. The Hermitian curve X is defined over F_{q^2} by

$$y^q z + y z^q = x^{q+1}.$$

It is a smooth curve with genus $g = \frac{1}{2}q(q-1)$. It is well known that, for any $\alpha \in F_q \subset F_{q^2}$, we have exactly q roots $T_1, \ldots, T_q$ for the equation $T^q + T = \alpha^{q+1}$ (see [23]). These correspond to the q intersection points $(\alpha : T_i : 1)$ for $1 \leq i \leq q$ of the line $x = \alpha z$ with X. The remaining intersection point of this line with X (note $\deg X = q + 1$) is $(0:1:0)$, which is denoted by Q_∞. Thus, we have q^2 lines $L_1, \ldots, L_{q^2}$ as above correspondingly and $1 + q^2 \cdot q = q^3 + 1$ F_{q^2}-rational points of X. This achieves the Hasse–Weil bound, and we know that we have got all F_{q^2}-rational points of X.

We consider the algebraic geometric code $C(X, G, P)$ defined by $G = mQ_\infty$ and $P = q^2 \cdot q$ intersection points of $L_1, \ldots, L_{q^2}$ with X except Q_∞. Note that the line $z = 0$ intersects X only at Q_∞. Thus, we find that

$L - Q_\infty \cong qQ_\infty$ for any hyperplane divisor L on X. Our main theorem is as follows:

THEOREM 2.3. *Let X be the Hermitian curve $y^q z + yz^q = x^{q+1}$ defined over F_{q^2}, where $q \geq 3$. Let $G = mQ_\infty$ and $P = X(F_q) - Q_\infty$, where $Q_\infty = (0:1:0)$. For $m = q^3 - q + b$ with $1 \leq b \leq q-2$, the generalized Hamming weights of the algebraic geometry code $C(X, G, P)$ are as follows*:

(i) $d_1 = q$ (*due to* [22]);

(ii) $d_2 = 2q - 1$;

(iii) $d_3 = 2q$.

Proof. (i) We shall prove $d_1 = q$ by Proposition 1.1. First we claim that, for any divisor P' with $0 \leq P' \leq P$ such that $\ell(G - P + P') \geq 1$, we have $\deg P' \geq q$. We notice that

$$\begin{aligned} G - P + P' &\sim (q^3 - q + b)Q_\infty - q^2(L - Q_\infty) + P' \\ &\sim P' - (q-b)Q_\infty, \end{aligned} \tag{2.2}$$

where L is any rational line passing through the point Q_∞ so that $L \sim (q+1)Q_\infty$. It is clear that $L(P') = F_{q^2}$ if $\ell(P') = 1$. Thus, we know that $\ell(P') \geq 2$ if $\ell(P' - (q-b)Q_\infty) \geq 1$. Otherwise, $L(P')$ consists of constant functions, and hence $L(P' - (q-b)Q_\infty) = 0$, which would contradict $\ell(P' - (q-b)Q_\infty) \geq 1$. The linear system $L(P')$ gives a degree P' map from X into $\mathbf{P}^1$. By Remark 1.1, we know that the second gonality is q, and we also know that the second gonality is at most degree P'. Therefore, we have shown that $\deg P' \geq q$, and the claim is proven. It follows from Proposition 1.1 that $d_1 \geq q$.

Now we wish to find a divisor P' with $0 \leq P' \leq P$ and $\deg P' = q$ such that $\ell(G - P + P') = \ell(P' - (q-b)Q_\infty) \geq 1$. We can take P' to $L_1 \cap X \setminus Q_\infty$. Then we have $\ell(P' - (q-b)Q_\infty) = \ell(bQ_\infty) \geq 1$ because $L_1 \sim (q+1)Q_\infty$. In view of Proposition 1.1, we have $d_1 \leq q$. So (i) is proved.

(ii) We shall first prove $d_2 \leq 2q - 1$. Take $P' = (L_1 \cap X - Q_\infty) + (L_2 \cap X - Q_\infty - P_1)$, where P_1 is any point different from Q_∞ in $L_2 \cap X$. Then we have

$$\begin{aligned} G - P + P' &\sim P' - (q-b)Q_\infty \\ &\sim bQ_\infty + (L_2 \cap X - Q_\infty - P_1) \\ &\sim (L_2 \cap X - P_1) + (b-1)Q_\infty. \end{aligned}$$

Obviously, $\ell(H \cap X -$ a point in $H \cap X) \geq 2$ for any plane curve X and hyperplane H. So we have $\ell(L_2 \cap X - P_1 + (b-1)Q_\infty) \geq \ell(L_2 \cap X - P_1) \geq 2$. Hence, by Proposition 1.1, $d_2 \leq \deg P' = 2q - 1$.

We next prove $d_2 \geq 2q-1$. We first prove that $d_2 \geq 2q-2$. Suppose, on the contrary, that $d_2 \leq 2q-3$. In view of Proposition 1.1, we can find a divisor U with $0 \leq U \leq P$ and $\deg U \leq 2q-3$ such that $\ell(G-P+U) \geq 2$. We are going to produce a contradiction. Observe that

$$G - P + U \sim U - (q-b)Q_\infty.$$

So we have $\ell(U-(q-b)Q_\infty) = \ell(G-P+U) \geq 2$. Let L be a hyperplane divisor on X. Then, by the adjunction formula, we know that the canonical divisor of the Hermitian curve X is given by $(q-2)L$. The genus of the Hermitian curve is $q(q-1)/2$. From the Riemann–Roch theorem, we have

$$\begin{aligned}\ell(U-(q-b)Q_\infty) - \ell((q-2)L - U + (q-b)Q_\infty)\\ = \deg U - q + b - q(q-1)/2 + 1.\end{aligned}$$

It follows that

$$\ell((q-2)L - U + (q-b)Q_\infty) \geq q(q-1)/2 + 1 - \deg U + (q-b). \tag{2.3}$$

From the exact sequence

$$0 \to \mathcal{O}((q-2)L - U) \to \mathcal{O}((q-2)L - U + (q-b)Q_\infty) \to F_{q^2}^{q-b} \to 0,$$

we have

$$\ell((q-2)L - U + (q-b)Q_\infty) - \ell((q-2)L - U) \leq q - b. \tag{2.4}$$

Since the first cohomology of a locally free sheaf on $\mathbf{P}^2$ is 0, we also have the following from the long cohomology exact sequence:

$$L((q-2)L) = L_{\mathbf{P}^2}((q-2)L). \tag{2.5}$$

Here $L((q-2)L)$ is the space associated with the divisor $(q-2)L \cap X$ on the Hermitian curve, and $L_{\mathbf{P}^2}((q-2)L)$ denotes the space associated with the divisor $(q-2)L$ on the $\mathbf{P}^2$. Thus, we have

$$L((q-2)L - U) = L_{\mathbf{P}^2}((q-2)L - U), \tag{2.6}$$

where $L_{\mathbf{P}^2}((q-2)L - U)$ represents the subsystem of the $(q-2)$ degree linear system on $\mathbf{P}^2$ passing through points of U. According to Lemma 2.5, if no $q-2+2=q$ points in U are collinear, then we have

$$\dim L_{\mathbf{P}^2}((q-2)L - U) = \dim L_{\mathbf{P}^2}((q-2)L) - \deg U. \tag{2.7}$$

From (2.6) and (2.7), we have

$$\ell((q-2)L-U)=\frac{q(q-1)}{2}-\deg U. \tag{2.8}$$

Equations (2.3) and (2.8) imply

$$\ell((q-2)L-U+(q-b)Q_\infty)-\ell((q-2)L-U)\geq 1+(q-b),$$

which contradicts (2.4). Therefore, we conclude that there exist q points in U that are collinear. We can assume that the divisor U is of the form $U=H-h+U'$, where H is a hyperplane divisor on the Hermitian curve X, h is the point that is not in U, and U' is a divisor with $\deg U'\leq q-3$. By Proposition 1.3, the fourth gonality ν_4 of the Hermitian curve X is $2q$. Since $\deg(H+U')\leq q+1+q-3=2q-2<2q$, we have $\ell(H+U')\leq 3$ by the definition of the gonality. On the other hand, the space $L(H)$, which is spanned by the three coordinate functions $x/e, y/e, z/e$, where e is the defining equation of the line H, is naturally included in the space $L(H+U')$. We have

$$L(G-P+U)=L(H-h-(q-b)Q_\infty+U')\subseteq L(H+U')=L(H).$$

We claim that there is no linear subspace of dimension at least 2 in $L(H)$ of the form $L(H-h-(q-b)Q_\infty+U')$. To prove this claim, we need only to show that there exists at most one hyperplane section that contains $h+(q-b)Q_\infty$. Since $q-b\geq 2$, we shall show that there is at most one line in the linear system $[H]$ passing through the point Q_∞ of order at least 2.

The tangent line of the Hermitian curve at the point $Q_\infty=(0,1,0)$ is $z=0$. Let L be the line passing through the point Q_∞ of order at least 2. Then the equation of L must be the form $ax+cz=0$ because $(0,1,0)$ satisfies the equation. From the local intersection theory, we know that the intersection multiplicity of L and the Hermitian curve at Q_∞ is $\dim F_{q^2}[[x,z]]/(ax+cz, z^q+z-x^{q+1})$. If $a\neq 0$, the intersection multiplicity of L and the Hermitian curve at Q_∞ must be 1. Thus, we have proven that $d_2\geq 2q-2$.

We now need to prove that d_2 cannot be $2q-2$. If $d_2=2q-2$, we would have a divisor U with $0\leq U\leq P$ with $\deg U=2q-2$ such that $\ell(G-P+U)=\ell(U-(q-b)Q_\infty)\geq 2$ by Proposition 1.1. By the

Riemann−Roch theorem,

$$\begin{aligned}\ell((q-2)L - U + (q-b)Q_\infty)\\ &= \ell(U - (q-b)Q_\infty) - \deg U - 1 + \frac{q(q-1)}{2} + q - b\\ &\geq 2 - \deg U - 1 + \frac{q(q-1)}{2} + q - b\\ &= \frac{(q+1)(q-2)}{2} + 2 - \deg U + q - b. \qquad (2.9)\end{aligned}$$

If no q points in U are collinear, we can apply Lemma 2.5 to the set $U-u$, where u is an arbitrary point in U. Thus, we have

$$\begin{aligned}\ell((q-2)L - (U-u)) &= \frac{(q-2)(q+1)}{2} + 1 - \deg(U-u)\\ &= \frac{(q-2)(q+1)}{2} + 2 - \deg U. \qquad (2.10)\end{aligned}$$

Now, we wish to show that (2.10) cannot be true; that is, there are q collinear points in the set $U-u$. Otherwise, from (2.9) and (2.10), we have

$$\begin{aligned}&\ell((q-2)L - (U-u) + (q-b)Q_\infty - u)\\ &\quad -\ell((q-2)L - (U-u)) \geq q - b, \qquad (2.11)\end{aligned}$$

which implies

$$\begin{aligned}&\ell((q-2)L - (U-u) + (q-b)Q_\infty)\\ &\quad -\ell((q-2)L - (U-u)) \geq q - b.\end{aligned}$$

On the other hand, it is clear that

$$\begin{aligned}&\ell((q-2)L - (U-u) + (q-b)Q_\infty)\\ &\quad -\ell((q-2)L - (U-u)) \leq q - b.\end{aligned}$$

So we have

$$\begin{aligned}&\ell((q-2)L - (U-u) + (q-b)Q_\infty)\\ &\quad -\ell((q-2)L - (U-u)) = q - b. \qquad (2.12)\end{aligned}$$

Equations (2.11) and (2.12) imply

$$\begin{aligned}\ell\big((q-2)L-(U-u)+(q-b)Q_\infty-u\big)\\ \geq \ell\big((q-2)L-(U-u)+(q-b)Q_\infty\big).\end{aligned} \tag{2.13}$$

Obviously,

$$\begin{aligned}\ell\big((q-2)L-(U-u)+(q-b)Q_\infty-u\big)\\ \leq \ell\big((q-2)L-(U-u)+(q-b)Q_\infty\big),\end{aligned} \tag{2.14}$$

and so (2.13) and (2.14) imply

$$\begin{aligned}\ell\big((q-2)L-(U-u)+(q-b)Q_\infty-u\big)\\ = \ell\big((q-2)L-(U-u)+(q-b)Q_\infty\big).\end{aligned} \tag{2.15}$$

Consider the sheaf exact sequence

$$\begin{aligned}0 &\to \mathscr{O}_X\big((q-2)L-U+(q-b)Q_\infty\big)\\ &\to \mathscr{O}_X\big((q-2)L-(U-u)+(q-b)Q_\infty\big)\\ &\to \mathscr{O}_X(q-2)L-(U-u)+(q-b)Q_\infty)/\\ &\quad Q_X\big((q-2)L-U+(q-b)Q_\infty\big)\to 0.\end{aligned}$$

From (2.15), we have the following exact sequence:

$$\begin{aligned}0 &\to F_{q^2} \to H^1\big(X, \mathscr{O}_X((q-2)L-U+(q-b)Q_\infty)\big)\\ &\to H^1\big(X, \mathscr{O}_X((q-2)L-U+u+(q-b)Q_\infty)\big)\to 0.\end{aligned} \tag{2.16}$$

From the Serre duality, (2.16) becomes

$$\begin{aligned}0 &\to H^0\big(X, \mathscr{O}_X(U-(q-b)Q_\infty-u)\big)\\ &\to H^0\big(X, \mathscr{O}_X(U-(q-b)Q_\infty)\big)\to F_{q^2}\to 0.\end{aligned} \tag{2.17}$$

Recall that $\ell(U-(q-b)Q_\infty) = \ell(G-P+U) \geq 2$. Therefore, (2.17) implies there is a nonzero function in $L(U-u)$, which vanishes at Q_∞ with order at least $q-b$. Since $L(U-u)$ contains a constant function (because $U-u$ is an effective divisor), $\ell(U-u)\geq 2$. By the

Riemann−Roch theorem, we have

$$\begin{aligned}\ell((q-2)L-(U-u)) &= \ell(U-u) - \deg U + 1 + \frac{q(q-1)}{2} - 1 \\ &\geq \frac{(q-2)(q+1)}{2} + 1 - \deg(U-u) + 1 \\ &> \frac{(q-2)(q+1)}{2} + 2 - \deg U.\end{aligned}$$

Therefore, we have shown that (2.10) cannot be true and there are q collinear points in the set $U-u$. Then we have $U = H - h + U'$, where U' is a divisor of degree $q-2$, and $L(H) = L(H+U') \supset L(H - h - (q-b)Q_\infty + U')$ by the same argument as before. This leads to a contradiction, as we have seen above. The conclusion that d_2 cannot be $2q-2$ is proved. Combining this with the earlier conclusion, we have $d_2 = 2q-1$.

(iii) We shall prove that $d_3 \leq 2q$. Take $P' = (L_1 \cap X - Q_\infty) + (L_2 \cap X - Q_\infty)$. Then we have

$$\begin{aligned}G - P + P' &\sim P' - (q-b)Q_\infty \\ &\sim bQ_\infty + (L_2 \cap X - Q_\infty) \\ &\sim L_2 \cap X + (b-1)Q_\infty.\end{aligned}$$

It follows that $\ell(G-P+P') \geq \ell_2(L_2 \cap X) = 3$. So $d_3 \leq 2q$ by Proposition 1.1. On the other hand, it is known that $d_2 < d_3$ by Theorem 1 of [21]. The conclusion $d_3 = 2q$ follows immediately. Q.E.D.

Remark 2.1. If we apply the result of Yang, Kumar, and Stichtenoth [23] to Theorem 2.3, we can only get the following estimates:

$$d_1 \geq q - b, \qquad d_2 \geq 2q - b, \qquad d_3 \geq 2q + 1 - b.$$

Hence, the results in Theorem 2.3 are highly nontrivial.

In the following, we shall prove a lemma that is needed in the proof of Theorem 2.3. We recall that a set $S = \{P_1, \ldots, P_d\}$ of distinct points in $\mathbf{P}^2$ is said to impose independent conditions on curves of degree n if

$$\ell\big(\mathbf{P}^2, \mathscr{I}_S(n)\big) = \ell\big(\mathbf{P}^2, \mathscr{O}_{\mathbf{P}^2}(n)\big) - d,$$

where $\mathscr{I}_S \subseteq \mathscr{O}_{\mathbf{P}^2}$ is the ideal sheaf of the zero-dimensional variety S.

LEMMA 2.4. *If a set S of $2n+1$ distinct points in $\mathbf{P}^2$ fails to impose independent conditions on curves of degree n, then S must include $n+2$ collinear points.*

Proof. We first note that the linear system of degree $n+2$ passing $2n+1$ points S can separate any two points in $\mathbf{P}^2$ if $n \geq 2$. So this linear system is ample over $\mathbf{P}^2$. Thus, we can find a degree $n+2$ smooth projective plane curve T passing these $2n+1$ points by the Bertini theorem.

Second, we observe that, for any hyperplane H in $\mathbf{P}^2$, we have

$$\begin{aligned}\dim L_T(nH) &= n(n+2) - g(T) + 1\\ &= n(n+2) - \frac{n(n+1)}{2} + 1\\ &= \frac{(n+2)(n+1)}{2}\\ &= \dim L_{\mathbf{P}^2}(n).\end{aligned}$$

Hence, $L_{\mathbf{P}^2}(n) = L_T(nH)$ and also $L_{\mathbf{P}^2}(nH-S) = L_T(nH-S)$. By the Riemann–Roch theorem, for the divisor $nH-S$ in T we have

$$\begin{aligned}\dim L_{\mathbf{P}^2}(nH-S) &= \dim L_T(nH-S)\\ &= n(n+2) - \deg S - \frac{n(n+1)}{2} + 1\\ &\quad + \dim L_T(K_T - nH + S).\end{aligned}$$

Recall that $K_T = (n+2)H - 3H = (n-1)H$. We have

$$\dim L_{\mathbf{P}^2}(nH-S) = \frac{(n+2)(n+1)}{2} - \deg S + \dim L_T(S-H).$$

If these $2n+1$ points of S do not impose independent conditions on $\mathcal{O}_{\mathbf{P}^2}(nH)$, namely,

$$\begin{aligned}\dim L_{\mathbf{P}^2}(nH-S) &= \frac{(n+2)(n+1)}{2} - \deg S + \dim L_T(S-H)\\ &> \dim L_{\mathbf{P}^2}(nH) - \deg S\\ &= \frac{(n+2)(n+1)}{2} - \deg S,\end{aligned}$$

then we have $\dim L_T(S-H) \geq 1$; that is, $S-H$ is linear equivalent to an effective divisor E. So we have $S \sim H+E$ and $|H| \subset |H+E| = |S|$. On the other hand, $\deg S = 2n+1 < 2n+2 = \nu_4$ by Proposition 1.3. Thus, we have $\dim L(S) \leq 3$ by the definition of ν_4. It follows that

$\dim L(S) = \dim L(H) = 3$. Clearly, the inclusion $|H| \subset |H+E| = |S|$ is natural. Hence, we have $|H| = |S|$. Therefore, every member of $|S|$ has to be in the form of a line plus E. In particular, S has to be in the form of a line plus E. This means that there are $n+2$ points in S that are collinear. Q.E.D.

3. OTHER EXAMPLES

In this section, we give two more examples in which we can apply Proposition 1.2 to determine their generalized Hamming weights.

EXAMPLE 3.1. Let $q = r^2$, where r is a power of odd prime. Let F_q be the finite field of q elements. X is the curve defined over F_q by the equation

$$x^{r+1} + y^{r+1} + z^{r+1} = 0.$$

It is easy to check that X is an irreducible nonsingular curve. For any $\alpha \in F_q$ such that $\alpha^{r+1} \neq -1$, since r is divisible by char F_q, we have

$$(1+\alpha^{r+1})^r = 1 + (\alpha^{r+1})^r = 1 + \alpha^{r^2+r} = 1 + \alpha^{r+1}.$$

Thus, $(-1-\alpha^{r+1})^{r-1} = 1$. Note that $F_q - \{0\} = F_q^*$ is a multiplicative cyclic group of order $q - 1 = (r-1)(r+1)$. We find that $-(1+\alpha^{r+1})$ has to be an $(r+1)$ power β^{r+1} for some $\beta \in F_q^*$. Therefore, the line L_α: $x = \alpha y$ intersects X at $(r+1)$ F_q-rational points of X, which are denoted by $P_{\alpha, \beta_1}, \dots, P_{\alpha, \beta_{r+1}}$, where $\beta_1, \dots, \beta_{r+1}$ are $(r+1)$-distinct elements in F_q^* such that $(\beta_i)^{r+1} = -(1+\alpha^{r+1})$. It is clear that, for any two distinct α_1 and α_2, $L_{\alpha_1} \cap L_{\alpha_2} = \{(0,0,1)\}$, which is outside X. Hence, all those P_{α, β_i} are distinct. We consider the algebraic geometric code $C = C(X, G, P)$, where $G = mL$, where L is a hyperplane divisor and $P = \bigcup_{i=1}^{n}(L_{\alpha_i} \cap X)$ for n distinct $\alpha_1, \alpha_2, \dots, \alpha_n \in F_q$ such that $1 + \alpha_i^{r+1} \neq 0$. Here we also assume that $2g(X) - 2 = r^2 - r - 2 < m(r+1) < n(r+1)$ (i.e., $2g(X) - 2 < \deg G < \deg P$). Then we can use Propositions 1.1 and 1.2 to prove the following statement.

THEOREM 3.1. *For the algebraic geometric code $C = C(X,G,P)$ as above, suppose $r \geq 3$. Then the generalized Hamming weights are as follows*:

(i) $d_1 = (n-m)(r+1)$;

(ii) $d_2 = (n-m)(r+1) + r$;

(iii) $d_3 = (n-m+1)(r+1)$.

Proof. (i) To prove $d_1 = (n-m)(r+1)$, we take $P' = \sum(L_{\alpha_i} \cap X)$, where the sum is over $n-m$ distinct α_i in $\alpha_1, \ldots, \alpha_n$. Then $G - P + P' \sim mL - nL + (n-m)L \sim 0$ and $\ell(G - P + P') = 1$. Thus, $d_1 \leq \deg P' = (n-m)(r+1)$ by Proposition 1.1. On the other hand, Proposition 1.2 says that $d_1 \geq \deg P - \deg G = (n-m)(r+1)$. Hence, $d_1 = (n-m)(r+1)$.

(ii) To prove $d_2 = (n-m)(r+1) + r$, we take $P' = (L_{\alpha_1} \cap X) + \cdots + (L_{\alpha_{n-m}} \cap X) + ((L_{\alpha_{n-m+1}} \cap X) - P)$, where P is a point in $L_{\alpha_{n-m+1}} \cap X$. Then $G - P + P' \sim (L_{\alpha_{n-m+1}} \cap X) - P$ and $\ell(G - P + P') = 2$. Thus, $d_2 \leq \deg P' = (n-m)(r+1) + r$ by Proposition 1.1. On the other hand, Proposition 1.2 says that $d_2 \geq \deg P - \deg G + \nu_2$. In view of Proposition 1.3, we have $\nu_2 = r$. Thus, $d_2 \geq (n-m)(r+1) + r$. We have proven $d_2 = (n-m)(r+1) + r$.

(iii) To prove $d_3 = (n-m+1)(r+1)$, we take $P' = (L_{\alpha_1} \cap X) + \cdots + (L_{\alpha_{n-m+1}} \cap X)$. Then $G - P + P' \sim L$ and $\ell(G - P + P') = 3$. Thus, $d_1 \leq \deg P' = (n-m+1)(r+1)$ by Proposition 1.1. On the other hand, Proposition 1.2 says that $d_3 \geq \deg P - \deg G + \nu_3$. In view of Proposition 1.3, we have $\nu_3 = r+1$. Thus, $d_3 \geq (n-m)(r+1) + r + 1 = (n-m+1)(r+1)$. We have proven $d_3 = (n-m)(r+1) + r + 1$. Q.E.D.

Remark. The code in Example 3.1 was considered in Example 4 on page 814 of the famous paper of Justesen *et al.* [14].

EXAMPLE 3.2. Let p be an odd prime ≥ 5. We consider the curve X over $F_p = \mathbf{Z}/(p\mathbf{Z})$ defined by

$$x^{p-1} + y^{p-1} + z^{p-1} = 0.$$

It is easy to check that X is an irreducible nonsingular curve in $\mathbf{P}^2$. Note that, for $x, y, z \in F_p$, we have $x^{p-1}, y^{p-1}, z^{p-1}$ equal to either 1 or 0. Hence, $x^{p-1} + y^{p-1} + z^{p-1}$ has to be 0, 1, 2, or 3. Since we assume $p \geq 5$, the only solution of $x^{p-1} + y^{p-1} + z^{p-1} = 0$ is $(x, y, z) = (0, 0, 0)$, which is not in $\mathbf{P}^2$. Thus, X has no F_p-rational point. However, as indicated in [2, 3], over a sufficiently large extension field F_q of F_p, where $q = p^r$ with r sufficiently large, many F_q-rational lines intersect X at F_q-rational points. For example, if we take $\alpha_1, \alpha_2, \ldots, \alpha_n \in F_{p^2}$ to be distinct elements and let $F_q \supset F_{p^2}$ be the splitting field of the equation $u^{p-1} + (1 + \alpha_i^{p-1}) = 0$, then the n F_q-rational lines $x = \alpha_i y$ for $1 \leq i \leq n$ intersect X at F_q-rational points $P = \{P_1^1, P_2^1, \ldots, P_{p-1}^1, P_1^2, P_2^2, \ldots, P_{p-1}^2, \ldots, P_{p-1}^n, \ldots, P_{p-1}^n\}$. Note that any two lines intersect at $(0, 0, 1)$, which is not in X. Let L be a hyperplane divisor that is disjoint from P. We consider the algebraic geometric code (over F_q) $C(X, G, P)$, where $G = mL$ and P as above, with the assumption that $2g(X) - 2 < m(p - 1) < n(p - 1) = \deg P$. The same argument as in Theorem 2.1 gives us the following statement.

THEOREM 3.1. *For the algebraic geometric code $C(X, G, P)$ as above, we have*

(i) $d_1 = (n - m)(p - 1)$;

(ii) $d_2 = (n - m)(p - 1) + p - 2$;

(iii) $d_3 = (n - m + 1)(p - 1)$.

4. APPENDIX

In this appendix, we prove Propositions 1.1 and 1.2 and a result of Yang, Kumar, and Stichtenoth [23] (mentioned in Remark 2.1). Our geometric proofs, which are different from the original algebraic proofs, may be easier to understand and make our paper more self-contained.

Proof of Proposition 1.1. We first note that ev_p is injective, since the kernel of ev_p is $L(G - P)$, which is 0 because $\deg G < n$. Thus, we can find an r-dimensional subcode or, equivalently, an r-dimensional subspace V of $L(G)$ such that all functions in V are 0 at $n - d_r$ points $P_{i_1}, P_{i_2}, \dots, P_{i_{n-d_r}}$ of P. Let $f_1, f_2, \dots, f_r$ be a base of V, and we have

$$\begin{aligned}
(f_1) &= -G + P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d_r}} + U_1,\\
(f_2) &= -G + P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d_r}} + U_2,\\
&\vdots\\
(f_r) &= -G + P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d_r}} + U_r,
\end{aligned}$$

where $U_1, U_2, \dots, U_r$ are effective divisors. Hence, we find that $\ell(G - P_{i_1} - \cdots - P_{i_{n-d_r}}) \geq r$ and $d_r \geq \min\{\deg P' \colon 0 \leq P' \leq P$ such that $\ell(G - P + P') \geq r\}$.

On the other hand, suppose $P'' = \{P_{i_1}, \dots, P_{i_t}\} \subseteq P$ such that $t = \deg P'' = \min\{\deg P' \colon 0 \leq P' \leq P,\ \ell(G - P + P') \geq r\}$. We can find r independent functions $g_1, \dots, g_r \in L(G - P + P'')$. Thus, $g_1, \dots, g_r$ vanish at $n - t$ points $P - P''$. Let V'' be the image of the linear span of $\{g_1, \dots, g_r\}$ under the evaluation map. We have $\dim V'' = r$ and $\#\operatorname{supp}(V'') \leq t$. We find that $d_r \leq \min\{\deg P' \colon 0 \leq P' \leq P$ such that $\ell(G - P + P') \geq r\} = t$. The conclusion is proved. Q.E.D.

Proof of Proposition 1.2. By Proposition 1.1, we can find an effective divisor P'' with $\deg P'' = d_r$, $0 \le P'' \le P$ and $\ell(G - P + P'') = \dim L(G - P + P'') \ge r$. Let f be an arbitrary nonzero function in $L(G - P + P'')$ and $U = (f) + G - P + P''$ be an effective divisor. Clearly, we have $\ell(U) = \ell(G - P + P'') \ge r$ and $\deg U \ge \nu_r$ by the definition of the rth gonality. On the other hand, $\deg U = \deg G - \deg P + \deg P'' = \deg G - n + d_r$. Thus, $d_r \ge n - \deg G + \nu_r$. Q.E.D.

Finally, we show that the next result follows immediately from our Theorem 1.4.

THEOREM (Yang, Kumar, and Stichtenoth [23]). *For* $q \ge 3$, $2q^2 - q - 2 < m < q^3$, *and* $m \equiv 0 \pmod q$, *we have the generalized Hamming weights of* $C(X, G, P)$ *as follows*:

$$d_1 = q^3 - m,$$

$$d_2 = q^3 - m + q,$$

$$d_3 = q^3 - m + q + 1.$$

Proof. We apply Theorem 1.4 with $t = q^2$, $d = q + 1$, and $u = m/q$. Then we get $d_1 = q^3 - m$, $d_2 = q^3 - m + q$, and $d_3 \ge q^3 - m + q + 1$.

It remains to prove $d_3 \le q^3 - m + q + 1$. In view of Proposition 1.1, it suffices to find an effective divisor $P' \le P$ such that $\ell(G - P + P') \ge 3$ and $\deg P' \le q^3 - m + q + 1$. Because of the assumptions $q \ge 3$, $m > 2q^2 - q - 2$, and $m \equiv 0 \pmod q$, we have $m/q > q + 1$. Let β be a solution of $\beta^q + \beta = 1$. Observe that the points $(\alpha_i, \beta, 1)$ in X, where $\alpha_i^{q+1} = 1$, are not in the lines L_α: $x = \alpha z$, where $\alpha^{q+1} \ne 1$. We take

$$P' = \sum_{\alpha_j^{q+1} \ne 1}^{q^2 - m/q} \left(L_{\alpha_j} - Q_\infty\right) + \sum_{\substack{i=1 \\ \alpha_i^{q+1} = 1}}^{q+1} (\alpha_i : \beta : 1).$$

So we have

$$\begin{aligned} G - P + P' \\ &= \frac{m}{q}(qQ_\infty) - \sum_{i=1}^{q^2} (L_i - Q_\infty) + P' \\ &\sim \frac{m}{q}(qQ_\infty) - \frac{m}{q}(L - Q_\infty) + \sum_{\substack{i=1 \\ \alpha_i^{q+1} = 1}}^{q+1} (\alpha_i : \beta : 1) \\ &\sim \sum_{\substack{i=1 \\ \alpha_i^{q+1} = 1}}^{q+1} (\alpha_i : \beta : 1). \end{aligned}$$

Note that the line $y = \beta z$ intersects X exactly at those $q + 1$ points $(\alpha_i : \beta : 1)$, $\alpha_i^{q+1} = 1$. We find that, for this P', $\ell(G - P + P') = \ell(L) = 3$. Thus, by Proposition 1.1, $d_3 \leq \deg P' = (q^2 - m/q)q + q + 1 = q^3 - m + q + 1$. Q.E.D.

ACKNOWLEDGMENTS

We thank Professor M. A. Tsfasman for sending us his joint work with Professor S. G. Vladut on generalized Hamming weights [20].

REFERENCES

1. M. Boguslavsky, ‘‘Veronese Varieties and Hamming Weights,’’ 4th-year thesis, Moscow State University, 1994.
2. H. Chen, On the main conjecture of geometric MDS codes, *Internat. Math. Res. Notices* **8** (1994), 313–318.
3. H. Chen and L. Xu, On the main conjecture on geometric MDS codes arising from plane curves, preprint.
4. H. Chen and S. S.-T. Yau, Solution to Munuera’s problem on the main conjecture of geometric hyperelliptic MDS codes, *IEEE Trans. Inform. Theory* **43**, No. 4, (1997), 1349–1354.
5. H. Chung, The 2nd generalized Hamming weight of double error correcting binary BCH codes and their dual codes, *Lecture Notes in Comput. Sci.* **539** (1991), 118–129.
6. I. M. Duursma, H. Stichtenoth, and C. Voss, Generalized Hamming weights of duals of BCH codes and maximal algebraic function fields, *in* ‘‘Proceedings of the AGCT-4, Luming 1993,’’ de Gruyter, Berlin, 1995.
7. G. van der Geer and M. van der Vlugt, Curves over finite fields of characteristic 2 with many rational points, *C. R. Acad. Sci. Paris Sér. I Math.* **317** (1993), 593–597.
8. G. van der Geer and M. van der Vlugt, On generalized Hamming weights of BCH codes, *IEEE Trans. Inform. Theory* **40**(2) (1994), 543–546.
9. G. van der Geer and M. van der Vlugt, Generalized Hamming weights of Melas codes and dual Melas codes, *SIAM J. Discrete Math.* (1994).
10. J. P. Hansen, Codes on the Klein quartic, ideals, and decoding, *IEEE Trans. Inform. Theory* **33**(6) (1987), 923–925.
11. J. W. P. Hirschfield, M. A. Tsfasman, and S. G. Vlădut, The weight hierarchy of higher-dimensional Hermitian codes, *IEEE Trans. Inform. Theory* **40**(1) (1994), 275–278.
12. M. Homma, Funny plane curves in char $p > 0$, *Comm. Algebra* **15** (1987), 1469–1501.
13. N. Jacobson, ‘‘Basic Algebra I,’’ 2nd ed., Freeman, New York, 1985.
14. J. Justesen, K. J. Karsen, H. E. Jensen, A. Havemuse, and T. Høholdt, Construction and decoding of a class of algebraic geometry codes, *IEEE Trans. Inform. Theory* **35** (1989), 811–821.
15. C. Munuera, On the generalized Hamming weight of geometric Goppa codes, *IEEE Trans. Inform. Theory* **40**(6) (1994), 2092–2099.
16. R. Pellikaan, On special divisors and the two variable zeta function of curves over finite fields, *in* ‘‘Proceedings of the AGCT-4, 1994.’’
17. H. Stichtenoth and C. Voss, Generalized Hamming weights of trace codes, *IEEE Trans. Inform. Theory* **40**(2) (1994), 554–558.

18. M. A. Tsfasman, Finite geometry and codes of higher rank, a program, handwritten notes of limited circulation.
19. M. A. Tsfasman and S. G. Vlǎdut, ''Algebraic Geometric Codes,'' Kluwer Academic, Dordrecht, 1991.
20. M. A. Tsfasman and S. G. Vlǎdut, Geometric approach to higher weights, *IEEE Trans. Inform. Theory* **41**(6) (1995), 1564–1588.
21. V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37**(5) (1991), 1412–1218.
22. K. Yang and P. V. Kumar, On the true minimum distance of Hermitian codes, *Lecture Notes in Math.*, **1518** (1992), 99–107.
23. K. Yang, P. V. Kumar, and H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, *IEEE Trans. Inform. Theory* **40**(3) (1994), 913–920.