ELSEVIER

Journal of Pure and Applied Algebra 123 (1998) 153–163

JOURNAL OF PURE AND APPLIED ALGEBRA

The generalized Hamming weights of some hyperelliptic codes

Mario A. de Boer

Discrete Mathematics, Dept. of Mathematics and Computer Science, Eindhoven, University of Technology, P.O. Box 513, 5600 MB, Eindhoven, Netherlands

Communicated by F. Oort; received 22 September 1994; received in revised form 12 January 1995

Abstract

In this paper we will determine the complete set of generalized Hamming weights of a special class of algebraic geometric codes arising from hyperelliptic curves. © 1998 Elsevier Science B.V.

1991 Math. Subj. Class.: 94B27, 14H45

1. Introduction

In this section the codes are introduced that we will study and define what we mean by generalized Hamming weights. Moreover, we will list some known results concerning these subjects that are relevant for this paper.

In Section 2 we will prove some results on hyperelliptic curves that we need in order to determine the complete set of generalized Hamming weights of the codes in Section 3. To show that good examples of such codes exist, in Section 4 we will construct a class of hyperelliptic curves that meet the Weil bound and have a maximal number of hyperelliptic points.

1.1. Generalized Hamming weights

For an arbitrary code D we define the support as

$$\mathrm{supp}(D) = \{i \mid \text{there is a } d \in D \text{ with } d_i \neq 0\}.$$

PII S0022-4049(97)00160-6

Let C be a linear code with parameters $[n,k,d]$. For any r, $1 \le r \le k$ we define the rth generalized Hamming weight as

$$d_r = \min\{\#\mathrm{supp}(D) \mid D \text{ } r\text{-dimensional subcode of } C\},$$

where the cardinality of a set S is denoted by $\#S$.

Since the definition of generalized Hamming weights by Wei in [7], many papers have appeared that investigate these parameters for different classes of codes.

1.2. Algebraic geometric codes

Let $\mathscr{X}$ be an absolutely irreducible smooth curve over $\mathbb{F}_q$ of genus g. For a set $\mathscr{P} = \{P_1, \ldots, P_n\}$ of rational points of $\mathscr{X}$ and a rational divisor G of $\mathscr{X}$ with $\deg(G) < n$ and $\mathrm{supp}(G) \cap \mathscr{P} = \emptyset$, we define the algebraic geometric code $C(\mathscr{P}, G)$ as the image of the map

$$\phi : L(G) \to \mathbb{F}_q^n, \qquad f \mapsto (f(P_1), \ldots, f(P_n)).$$

The code $C(\mathscr{P}, G)$ is linear with parameters $[n,k,d]$ satisfying $k = l(G) \ge \deg(G) + 1 - g$ and $d \ge n - \deg(G)$.

In papers [4, 9] the authors study the generalized Hamming weights of algebraic geometric codes. Munuera proved the following for algebraic geometric codes $C(\mathscr{P}, G)$:

$$d_r(C) = n - \max\left\{ \deg(D) \mid 0 \le D \le \sum_{P \in \mathscr{P}} P,\ l(G - D) \ge r \right\}.$$

For an extensive treatment of algebraic geometric codes (excluding generalized Hamming weights), see [5, 6].

1.3. Hyperelliptic codes

An absolutely irreducible smooth curve $\mathscr{X}$ is hyperelliptic if and only if its genus is at least two and there exists a morphism of degree two from $\mathscr{X}$ to the projective line. $\mathscr{X}$ allows a unique involution (conjugation), the hyperelliptic involution, denoted by σ. The fixed points of σ are called hyperelliptic points. For rational points P, both divisors of the form $P + \sigma(P)$ and sets of the form $\{P, \sigma(P)\}$ are called hyperelliptic (conjugated) pairs. In this paper P_∞ is a fixed hyperelliptic point and $\mathscr{H} = \{H_1, H_2, \ldots, H_h\}$ is the set of all (not necessarily $\mathbb{F}_q$-rational) hyperelliptic points on $\mathscr{X}$ different from P_∞. In the case q odd we have that $h = 2g + 1$ and $\sum_{i=1}^{2g+1} H_i \sim (2g+1)P_\infty$. In the case q even we have $h \le g$. As a general reference on hyperelliptic curves we refer the reader to [3] or [5].

In this paper we consider algebraic geometric codes $C(\mathscr{P}, G)$ arising from hyperelliptic curves, with the properties that for any rational point $P \in \mathscr{P}$ we have that $\sigma(P) \in \mathscr{P}$, and G is a hyperelliptic divisor (which means $G \sim lP_\infty$ for some l) of degree $\deg(G) < n$. From Clifford's theorem and the Riemann–Roch theorem we find

that the dimension of these codes is $k = l+1$ if $l \leq g-1$ and $k = 2l+1-g$ if $l > g-1$. Remark that this class of codes includes the most studied form of algebraic geometric code: codes $C(\mathscr{P}, G)$ with $G = mP_\infty$ and $\mathscr{P}$ all rational points on $\mathscr{X}$ except P_∞.

Using the fact that for a hyperelliptic curve the gonality sequence is known, Munuera proved (see [4])

$$\begin{cases} d_r \geq n - \deg G + 2(r-1) & \text{if } 1 \leq r \leq \min\{k, g\}, \\ d_r = n - k + r & \text{if } r > g. \end{cases}$$

Munuera could even prove equality in the first equation if $\mathscr{P}$ contains enough conjugated pairs. In this paper we will prove a converse to Munuera's results which allows us to determine all generalized Hamming weights. This also generalizes [8], in which Xing determines the minimum distance of these codes in the case $l > g-1$ and q odd. For $l = g$ we will show that Xing's result is not exact, and we will correct it. Our approach differs completely from Xing's proof.

2. Results on divisors of hyperelliptic curves

In this section we will prove the facts on hyperelliptic curves that we will need in the next section to prove the main result. The main ingredient is the fact that for a hyperelliptic curve we have the unique reduction property (URP) (see [2]). Let D be an effective divisor. By replacing all conjugated pairs in D by $2P_\infty$ we can write $D \sim D' + mP_\infty$ with D' such that $\sigma(P) \notin \operatorname{supp}(D')$ if $P \in \operatorname{supp}(D')$. We say that D reduces to D' and call D' semi-reduced. From the Riemann–Roch theorem it follows that every effective divisor can be reduced uniquely to a semi-reduced divisor of degree $\leq g$; such divisors are called reduced divisors. Thus, the URP yields that every effective divisor D is equivalent to a unique divisor of the form $D' + cP_\infty$, with D' an effective divisor of degree at most g with neither conjugated pairs nor P_∞ in $\operatorname{supp}(D')$ (in [2] Cantor describes an algorithm that reduces divisors).

Now we prove some useful lemmas. The first is a generalization of a lemma proved by the author in [1]. It also shows that the reduction of a divisor is unique.

Lemma 2.1. *Let $\mathscr{X}$ be a hyperelliptic curve of genus g. Let D be an effective divisor of the form*

$$D = T + sP_\infty$$

of degree $t+s$ with T a semi-reduced divisor of degree t. Then we have

$$l(D) = \begin{cases} \lfloor \frac{s}{2} \rfloor + 1 & \text{if } 2t + s \leq 2g-2, \\ t + s + 1 - g & \text{if } 2t + s > 2g-2. \end{cases}$$

Proof. Since the dimension of the vectorspace $L(D)$ does not change if we extend the ground field $\mathbb{F}_q$, we will prove the lemma in the case of the algebraically closed field

$\overline{\mathbb{F}}_q$. In this case we can write $T \sim P_1 + \cdots + P_t$ with $P_i \neq P_\infty$ and $P_i \neq \sigma(P_j)$ for $i \neq j$. Suppose $P_i \neq P_j$ for $i \neq j$.

We prove the case s even, the case s odd being quite similar. Let $D' = P_1 + \cdots + P_t + P_{t-1} + \sigma(P_{t+1}) + \cdots + P_{t+s/2} + \sigma(P_{t+s/2}) \sim D$. Set $D'' = P_1 + \sigma(P_1) + \cdots + P_t + \sigma(P_t) + P_{t+1} + \sigma(P_{t-1}) + \cdots + P_{t+s/2} + \sigma(P_{t+s/2})$. Let f_i for $i = 1, \ldots, t + s/2$ be such that $(f_i) = 2P_\infty - P_i - \sigma(P_i)$. First suppose that $2t + s \leq 2g - 2$. Then $L(D') \subset L(D'') = \langle 1, f_1, \ldots, f_{t+s/2} \rangle$. Since $\langle f_1, \ldots, f_t \rangle \cap L(D') = \{0\}$ we find $l(D) = l(D') \leq s/2 + 1$. The equality follows from $l(D) \geq l(sP_\infty) = s/2 + 1$.

Now let $2t + s > 2g - 2$. Then $L(D') \subset L(D'') = \langle 1, f_1, \ldots, f_{t+(s/2)}, h_1, \ldots, h_{t+(s/2)-g} \rangle$ for some rational functions $h_1, \ldots, h_{t+(s/2)-g}$. Again we have $L(D') \cap \langle f_1, \ldots, f_t \rangle = \{0\}$, so $l(D) = l(D') \leq t + s + 1 - g$. From the Riemann–Roch theorem we have that $l(D) \geq t + s + 1 - g$ which completes the proof.

If some of the P_i coincide, say $P_1 = P_2 = \cdots = P_s$, then the proof proceeds as above but with $(f_1) = 2P_\infty - P_1 - \sigma(P_1)$ and $f_2 = f_1^2, f_3 = f_1^3, \ldots, f_s = f_1^s$. □

Lemma 2.2. *Let $W_i \in \mathscr{H}$ be such that $\sum_{i=1}^{r} W_i \sim rP_\infty$ with every W_i appearing at most twice in the sum. Then either every W_i appears exactly twice in the sum, or $r = 2g + 1$ and every W_i appears exactly once in the sum (in this case $\{W_i \mid i = 1, \ldots, 2g + 1\} = \mathscr{H}$). The last case cannot occur if q is even.*

Proof. Replacing all the points that appear twice in the sum $\sum W_i$ by $2P_\infty$ (reduction) yields

$$W_{i_1} + \cdots + W_{i_l} \sim lP_\infty,$$

for some l, $0 \leq l \leq 2g+1$ if q is odd, and $0 \leq l \leq g$ if q is even. First suppose $l \leq g$. By the URP this is impossible unless $l = 0$, i.e. every point appears twice in the original sum.

Now suppose $l \geq g + 1$. Then q is odd and as stated in the previous section we have

$$\sum_{i=1}^{2g+1} H_i \sim (2g + 1)P_\infty,$$

so we find

$$\sum_{j=1}^{2g+1} H_j - W_{i_1} - \cdots - W_{i_l} \sim (2g + 1 - l)P_\infty.$$

Now $2g + 1 - l \leq g$. Using the URP this is impossible, unless $l = 2g + 1$, i.e. every point appears exactly once in the original sum. □

The following lemma gives a lower bound on the degree of a divisor that reduces to a sum of hyperelliptic points and that is itself not a sum of hyperelliptic points.

Lemma 2.3. *Let E be an effective divisor of degree e with $P \in \mathrm{supp}(E)$ and $\sigma(P) \notin \mathrm{supp}(E)$ for some point P. Suppose for hyperelliptic points $H_1, \ldots, H_u$, $0 \le u \le g$ we have*

$$E \sim H_1 + \cdots + H_u + (e-u)P_\infty.$$

Then $e \ge 2g + 1 - u$.

Proof. Replacing all hyperelliptic pairs in the support of E by $2P_\infty$ yields a divisor E' of degree $e' \le e$ with $E \sim E' + (e-e')P_\infty$. The property of E that there is a point $P \in \mathrm{supp}(E)$ with $\sigma(P) \notin \mathrm{supp}(E)$ also holds for E'. We can write

$$E' \sim H_1 + \cdots + H_u + (e'-u)P_\infty. \tag{1}$$

First note that $e' \ge g$. Indeed, if e' were smaller than g the URP would imply that there is a divisor $A \sim (|u-e'|)P_\infty$ such that either $E' + A = H_1 + \cdots + H_u$ or $E' = H_1 + \cdots + H_u + A$. This is impossible since not all conjugates of points in $\mathrm{supp}(E')$ are in $\mathrm{supp}(E')$. Hence $e' \ge g$.

Now suppose that $e' + u \le 2g - 2$. From the proof of Lemma 2.1 we find that there is a divisor $A \sim (e'-u)P_\infty$ such that $E' = H_1 + \cdots + H_u + A$, which is again impossible since not all conjugates of points in $\mathrm{supp}(E')$ are in $\mathrm{supp}(E')$.

So we can assume $e' + u \ge 2g - 1$. Lemma 2.1 gives $l(E') = e' + 1 - g$. Suppose $e \le 2g - u$, so $e' \le 2g - u$. Then $l((e'-u)P_\infty) \ge l((2e'-2g)P_\infty) = e' - g + 1$ (Clifford's theorem). This shows that the number of effective divisors that are equivalent to $(e'-u)P_\infty$ is at least the number of effective divisors that are equivalent to E'. Together with Eq. (1) this implies that these numbers must be equal and we again find $E' = H_1 + \cdots + H_u + A$ for some effective divisor $A \sim (e'-u)P_\infty$, which is impossible for the same reason as above. Hence, $e \ge 2g + 1 - u$ and the proof is finished. □

The next lemma gives bounds on the generalized Hamming weights d_r for $1 \le r \le g$.

Lemma 2.4. *Let $\mathscr{P}$ be a set of n distinct rational points on a hyperelliptic curve $\mathscr{X}$ of genus g. Let $G \sim 2lP_\infty$ with $2l < n$. Let $1 \le r \le g$. Then the rth generalized Hamming weight is $d_r = n - 2l + 2(r-1) + \delta$ for some δ, $0 \le \delta \le g - r + 1$.*

Proof. The lower bound $\delta \ge 0$ was proved by Munuera in [4]. The upper bound follows from the generalized Singleton bound (see [7]): $d_r \le n - k + r$. We distinguish between two cases. First suppose $l \ge g$. Then $k = 2l + 1 - g$ and we find $d_r = n - 2l + 2(r-1) + \delta \le n - 2l - 1 + g + r$ from which the lemma follows.

In the case $l \le g-1$ we have $k = l+1$ and we find $d_r = n - 2l + 2(r-1) + \delta \le n - l - 1 + r$ and the lemma also follows immediately. □

Lemma 2.5. *Let S be a divisor with $\deg(S) \le g + r - 2$ and $l(S) = r$, with $S \sim F + mP_\infty$ for some semi-reduced divisor F of degree f. Then $2f + m \le 2g - 2$ and $m = 2r - 1$ or $2r - 2$.*

Proof. First suppose $2f+m>2g-2$. Then Lemma 2.1 yields $r=l(S)=l(F+mP_\infty)=f+m+1-g\leq r-1$ which is a contradiction.

Hence, $2f+m\leq 2g-2$ and Lemma 2.1 gives $r=l(S)=l(F+mP_\infty)=\lfloor m/2\rfloor+1$ which proves the lemma. □

3. The generalized Hamming weights

In this section we state and prove the main result.

Let $W_1,\ldots,W_\omega\in\mathscr{H}$ be $\mathbb{F}_q$-rational hyperelliptic points and let $P_i,\sigma(P_i)$, $i=1,\ldots,\pi$ be pairs of distinct conjugated $\mathbb{F}_q$-rational points of $\mathscr{X}$. Then we have the following proposition.

Proposition 3.1. *Let* $\mathscr{P}=\{W_1,\ldots,W_\omega,P_1,\sigma(P_1),\ldots,P_\pi,\sigma(P_\pi)\}$ *and* $G\sim 2lP_\infty$ *with* $2l<n=2\pi+\omega$. *Suppose the code* $C(\mathscr{P},G)$ *has rth generalized Hamming weight* $d_r=n-2l+2(r-1)+\delta$ *for some* $\delta\geq 0$. *Then* $\pi\geq l-r+1-\delta$ *in any of the following cases*:

1. $\delta+\omega<2g+2$;
2. $l\leq r+g-1$.

Proof. Suppose $d_r=n-2l+2(r-1)+\delta$. Then, after reindexing the points of $\mathscr{P}$, there is a divisor

$$D=W_1+\cdots+W_m+P_1+\sigma(P_1)+\cdots+P_s+\sigma(P_s)+Q_1+\cdots+Q_t$$

with $W_i,P_i,Q_i\in\mathscr{P}$, $\sigma(Q_i)\neq Q_j$ for all i,j, and $\deg(D)=2l-2r+2-\delta$, such that $l(G-D)=r$. From Lemma 2.4 we find $\delta\leq g-r+1$. If $\delta=g-r+1$ the proof is finished, since in this case $2\pi+2g+1\geq 2\pi+\omega=n>2l$ implies that $\pi\geq l-g=l-r+1-\delta$. Hence, from now on we can assume $\delta\leq g-r$.

Since $\deg(G-D)=2(r-1)+\delta\leq g+r-2$ we can apply Lemma 2.5 to the divisor $G-D$ to find that $G\sim D+2(r-1)P_\infty+F$ for some effective divisor F of degree δ. Hence, we can write

$$(2l-2r+2)P_\infty\sim W_1+\cdots+W_m+P_1+\sigma(P_1)+\cdots+P_s+\sigma(P_s)+Q_1+\cdots+Q_t+F. \tag{2}$$

Since $\mathscr{P}$ contains all conjugates of its points we have $\pi\geq s+t$. We want to give a lower bound on $s+t$.

Comparing Eq. (2) with its conjugate yields

$$Q_1+\cdots+Q_t+F\sim\sigma(Q_1)+\cdots+\sigma(Q_t)+\sigma(F).$$

Since the reduced divisor of $Q_1+\cdots+Q_t+F$ must also be equivalent to its conjugate we have by the URP

$$Q_1+\cdots+Q_t+F\sim H_{i_1}+\cdots+H_{i_u}+(t+\delta-u)P_\infty,$$

with $0 \leq u \leq g$ and $H_{i_j} \in \mathscr{H}$. Substitution in Eq. (2) yields

$$W_1 + \cdots + W_m + H_{i_1} + \cdots + H_{i_u} \sim (m+u)P_\infty.$$

Since the W_i are pairwise distinct and the H_{i_j} are pairwise distinct (reduction), we can apply Lemma 2.2. We are left with two cases. The first case is the case in which $\{W_1, \ldots, W_m\} = \{H_{i_1}, \ldots, H_{i_u}\}$. In the second case $m+u = 2g+1$ and $\{W_1, \ldots, W_m\} \cup \{H_{i_1}, \ldots, H_{i_u}\} = \mathscr{H}$.

1. Suppose $\{W_1, \ldots, W_m\} = \{H_{i_1}, \ldots, H_{i_u}\}$. Then $m = u$ and since $t + \delta \geq u$ we find, comparing degrees in Eq. (2), that $2l - 2r + 2 = m + 2s + t + \delta \leq 2s + 2t + 2\delta$, and so $\pi \geq s + t \geq l - r + 1 - \delta$. This finishes the proof in this case.

2. Suppose $m + u = 2g + 1$ and $\{W_1, \ldots, W_m\} \cup \{H_{i_1}, \ldots, H_{i_u}\} = \mathscr{H}$. We again distinguish between two cases.

(a) Suppose $m + u = 2g + 1$ and $t > 0$. Lemma 2.3 implies that $t + \delta \geq 2g + 1 - u$. We again find that $t + \delta \geq m$, and the result follows as in case 1.

(b) Suppose $m + u = 2g + 1$ and $t = 0$. Now $\delta \geq u$ and $m \leq \omega$. If we note that $m + \delta$ is even by comparing degrees in Eq. (2) for $t = 0$, this yields $\delta + \omega \geq 2g + 2$. This possibility cannot occur if any of the two conditions of the proposition is satisfied. Indeed, the contradiction is immediate in the case $\delta + \omega < 2g + 2$. For the other case, assume that $l \leq r + g - 1$. Then the degree of the equivalent divisors in Eq. (2) is at most $2g$. This is only possible if $m = u$ which contradicts with $m + u = 2g + 1$. □

Remark 3.2. The first condition in Proposition 3.1 is always satisfied if q is even. Indeed, if q is even, then $\omega \leq g$. From Lemma 2.4 we find that $\delta \leq g$, so that $\delta + \omega \leq 2g$.

We can use Proposition 3.1 to prove the following converse of a proposition by Munuera [4].

Proposition 3.3. *Let* $\mathscr{P} = \{W_1, \ldots, W_\omega, P_1, \sigma(P_1), \ldots, P_\pi, \sigma(P_\pi)\}$ *and* $G \sim 2lP_\infty$ *with* $2l < n = 2\pi + \omega$. *Let* $1 \leq r \leq g$. *Then the code* $C(\mathscr{P}, G)$ *has rth generalized Hamming weight* d_r, *with*

$$d_r = n - 2l + 2(r-1) \Leftrightarrow \pi \geq l - r + 1.$$

Proof. Suppose $\pi \geq l - r + 1$ and let

$$D = P_1 + \sigma(P_1) + \cdots + P_{l-r-1} + \sigma(P_{l-r-1}).$$

Then $l(G - D) = l(2(r-1)P_\infty) = r$ and we find $d_r \leq n - \deg(D) = n - 2l + 2(r-1)$. Equality follows from Lemma 2.4.

Now suppose $d_r = n - 2l + 2(r-1)$. Then Proposition 3.1 implies $\pi \geq l - r + 1$ (note that $\omega \leq 2g + 1$). □

In the case where $\pi \geq l$ Proposition 3.3 determines all generalized Hamming weights. We will now determine the generalized Hamming weights in the general case.

Theorem 3.4. *Let* $\mathscr{P}=\{W_1,\dots,W_\omega,P_1,\sigma(P_1),\dots,P_\pi,\sigma(P_\pi)\}$ *and* $G\sim 2lP_\infty$ *with* $2l<n=2\pi+\omega$. *Let* $\Delta=\max\{l-\pi,0\}$. *Then the code* $C(\mathscr{P},G)$ *has generalized Hamming weights*

$$d_r=\begin{cases} n-2l+2(r-1)+\min\{\Delta-r+1,2g+2-\omega\} & \text{if } 1\le r\le \min\{l-g,\Delta\},\\ n-2l+r-1+\Delta & \text{if } l-g+1\le r\le \Delta,\\ n-2l+2(r-1) & \text{if } \Delta+1\le r\le g,\\ n-k+r & \text{if } g+1\le r\le k.\end{cases}$$

Here $k=l+1$ *if* $l\le g-1$ *and* $k=2l+1-g$ *if* $l\ge g$.

Proof. The case $r\ge\Delta+1$ follows from Proposition 3.3 for $r\le g$ and from the results of Munuera [4] for $r>g$. From now on we can assume $r\le\Delta$, and $l\ge\pi$.

We will first prove the lower bounds of the theorem. Suppose $r\le l-g$. Take $\delta<\min\{\Delta-r+1,2g+2-\omega\}$. Then $\pi<l-r+1-\delta$ and $\delta+\omega<2g+2$. Proposition 3.1 implies that $d_r\ne n-2l+2(r-1)+\delta$. Hence, $d_r\ge n-2l+2(r-1)+\min\{\Delta-r+1,2g+2-\omega\}$.

Now suppose $r\ge l-g+1$. In this case take $\delta<\Delta-r+1$, and again Proposition 3.1 implies that $d_r\ne n-2l+2(r-1)+\delta$, so $d_r\ge n-2l+r-1+\Delta$.

To prove equality, first note that $n=2\pi+\omega=2l-2\Delta+\omega>2l$ and so $\omega>2\Delta$. We distinguish between two cases. We first show that $d_r\le n-2l+r-1+\Delta$. Since $\omega>\Delta$ we can write

$$G\sim P_1+\sigma(P_1)+\cdots+P_{l-\Delta}+\sigma(P_{l-\Delta})+2W_1+\cdots+2W_\Delta,$$

and define the divisor

$$D=P_1+\sigma(P_1)+\cdots+P_{l-\Delta}+\sigma(P_{l-\Delta})+W_1+\cdots+W_{\Delta-r+1},$$

with $P_i,\sigma(P_i),W_i\in\mathscr{P}$. Now $l(G-D)\ge l(2W_{\Delta-r+2}+\cdots+2W_\Delta)=r$ and we find $d_r\le n-\deg(D)=n-2l+r-1+\Delta$.

Now, for $r\le l-g$, we show $d_r\le n-2l+2r+2g-\omega$. Note that $2\Delta<\omega\le 2g+1$ and so $\pi=l-\Delta\ge l-g-1$. Hence, we can write

$$G\sim H_1+\cdots+H_{2g+1}+P_1+\sigma(P_1)+\cdots+P_{l-g-1}+\sigma(P_{l-g-1})+P_\infty,$$

and define

$$D=W_1+\cdots+W_\omega+P_1+\sigma(P_1)+\cdots+P_{l-r-g}+\sigma(P_{l-r-g}).$$

Again we find that $l(G-D)\ge l((2r-2)P_\infty)=r$ and the proof is complete. □

Setting $r=1$ in Theorem 3.4 gives the minimum distance of the codes.

Corollary 3.5. *The code* $C=C(\mathscr{P},G)$ *as in Theorem* 3.4 *has minimum distance*

$$d=\begin{cases} n-2l+\Delta & \text{if } l\le g,\\ n-2l+\min\{\Delta,2g+2-\omega\} & \text{if } l\ge g+1.\end{cases}$$

In the case $l = g$, Corollary 3.5 differs from the result by Xing in [8]. Going through a specific example yields that Corollary 3.5 gives the correct value for the minimum distance. Indeed, take a hyperelliptic curve of genus g over a field $\mathbb{F}_q$ that has $2g+2$ $\mathbb{F}_q$-rational hyperelliptic points. Take $\Delta = l = g$ and $\omega = 2g+1$. Then the resulting code is a Reed Solomon code with parameters $[2g+1, g+1, g+1]$, whereas Xing's result would yield $d = 2$.

Using the relation between the generalized Hamming weights of a code and its dual code [7, Theorem 3], we can in particular determine the minimum distance of the dual code of $C(\mathscr{P}, G)$.

Corollary 3.6. *Let $C = C(\mathscr{P}, G)$ be defined as in Theorem* 3.4. *Then the minimum distance of the dual code is*

$$d^{\perp} = \begin{cases} 2 & \text{if } \Delta < l \text{ and } l \leq g-1, \\ l+2 & \text{if } \Delta = l \text{ and } l \leq g-1, \\ 2l-2g+2 & \text{if } l \geq g. \end{cases}$$

4. Examples: a class of maximal hyperelliptic curves

In order to construct long codes of the type that we are considering in this paper, we need hyperelliptic curves with both many $\mathbb{F}_q$-rational points and many hyperelliptic points. This seems contradictive, and it is so if the genus of the curve is small compared with the size of the ground field. In this section we will give examples of curves that attain the Weil bound and have the maximal possible number of hyperelliptic points.

Let q be odd. Then a hyperelliptic curve $\mathscr{X}$ of genus g has a (singular) plane model of the form $y^2 = f(x)$, with f a square-free polynomial of degree $2g+1$ or $2g+2$. The finite hyperelliptic points of $\mathscr{X}$ are in one–one correspondence with the zeros of $f(x)$. If f has degree $2g+1$, $\mathscr{X}$ also has an infinite hyperelliptic point. For N, the number of $\mathbb{F}_q$-rational points on $\mathscr{X}$, we have two well-known bounds:

$$N \leq \begin{cases} 2q+2 & \text{trivial bound,} \\ q+1+2g\sqrt{q} & \text{Weil bound.} \end{cases}$$

If $g > (q+1)/2\sqrt{q}$, the trivial bound is stronger that the Weil bound. The following proposition establishes equality in the Weil bound if the genus is just below $(q+1)/2\sqrt{q}$.

Proposition 4.1. *Let $g \geq 2$ such that $p = 2g+1$ is a prime power. Set $q = p^2$. Let N be the number of $\mathbb{F}_q$-rational points on the hyperelliptic curve $\mathscr{X}$ with plane model*

$$y^2 = x^p + x.$$

Then $\mathscr{X}$ has genus g, contains $2g+2$ $\mathbb{F}_q$-rational hyperelliptic points and $N = q+1+2g\sqrt{q}$.

Proof. Let α be a primitive element in $\mathbb{F}_q$. Then $(x^p + x)$ splits as

$$(x^p + x) = x \prod_{i=0}^{2g-1} (x - \alpha^{(p+1)(i+1/2)}).$$

Hence, $\mathscr{X}$ has $2g + 1$ finite hyperelliptic points. The infinite point brings the total number to $2g + 2$.

Let $f(x) = x^p + x$ and $\beta \in \mathbb{F}_q$. Then $f(\beta) = \mathrm{Tr}(\beta) \in \mathbb{F}_p$, where Tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Since $\mathbb{F}_p$ consists of the set of $p+1$ powers of elements in $\mathbb{F}_q$ we find that $f(\beta)$ is either 0 or a square in $\mathbb{F}_q$. The zeros of $f(x)$ correspond to the $p+1$ hyperelliptic points, and the $x \in \mathbb{F}_q$ for which $f(x)$ is a square correspond to pairs of conjugated points. This gives a total number of points of $N = p + 1 + 2(q - p) = q + 1 + (q - p) = q + 1 + (p - 1)p = q + 1 + 2gp = q + 1 + 2g\sqrt{q}$. □

Remark 4.2. The class of curves given in Proposition 4.1 is a subclass of a more general class of maximal curves that also includes the Hermitian curves. These can be found in Example VI.4.2. of [5].

To end this section we will give the parameters of some codes that arise from this construction and that have a minimum distance that exceeds the Goppa lower bound. From Proposition 3.3, which shows that in this case we have $\pi \leq l - 1$, we see that this can only occur for comparatively small minimum distances. Indeed, $d = n - 2l + \min\{\Delta, 2g+2-\omega\} = 2\pi + \omega - 2l + \min\{\Delta, 2g+2-\omega\} \leq 2l - 2 + \omega - 2l + 2g + 2 - \omega = 2g$.

Example. Codes with the parameters shown in Table 1 can be obtained from the curves of Proposition 4.1.

Table 1

Field	Genus	Example of code
$\mathbb{F}_{25}$	2	[45, 41, 4]
$\mathbb{F}_{49}$	3	[91, 86, 4]
	3	[91, 84, 6]
$\mathbb{F}_{81}$	4	[151, 147, 4]
	4	[152, 145, 6]
	4	[153, 143, 8]
$\mathbb{F}_{121}$	5	[229, 224, 4]
	5	[229, 222, 6]
	5	[229, 220, 7]
	5	[231, 220, 8]
	5	[231, 218, 10]

References

[1] M.A. de Boer, MDS codes from hyperelliptic curves, in: R. Pellikaan, M. Perret, S.G. Vlăduţ (Eds.), Arithmetic, Geometry and Coding Theory, Walter de Gruyter, Berlin, 1996, pp. 23–34.
[2] D.G. Cantor, Computing in the Jacobian of a hyperelliptic curve, Math. Comput. 48 (1987) 95–101.
[3] R. Hartshorne, Algebraic Geometry, Springer, New York, 1977.
[4] C. Munuera, On the generalized Hamming weights of geometric Goppa codes, IEEE Trans. Inform. Theory 40 (1994) 2092–2099.
[5] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1991.
[6] M.A. Tsfasman, S.G. Vlăduţ, Algebraic-Geometric Codes, Kluwer Academic Publishers, Dordrecht, 1991.
[7] V.K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412–1418.
[8] C.-P. Xing, Hyperelliptic function fields and codes, J. Pure Appl. Algebra 74 (1991) 109–118.
[9] K. Yang, P.V. Kumar, H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, IEEE Trans. Inform. Theory 40 (1994) 913–920.