On the generalized Hamming weigths of Hyperelliptic codes

Domingo Ramirez-Alzola *

Abstract – Motivated by cryptographical applications, we study the generalized Hamming weights of Hyperelliptic codes.

Index Terms – Linear codes, generalized Hamming weights, Hyperelliptic codes.

1 Introduction

The *generalized Hamming weights* of linear codes are the generalization of the minimum distance. They were first motivated by applications from cryptography, namely the wire-tap channel of type II and the t-resilient functions, see [17]. The generalized Hamming weights completely characterize the performance of a linear code when it is used on the type II wire-tap channel. It is also useful in trellis coding (lower bounding the number of trellis states, see [11] and [12]) and in truncating a linear block code, see [6]. Later on, another apparently different concept, the Dimension/length Profiles (DLP) of a linear code, was proved to be equivalent to its generalized Hamming weights, see [3]. The close and deep connections between these two concepts make this topic more interesting and active.

Let $\mathbf{F}_q$ be the finite field with q elements. The *support* of a linear code $\mathcal{C}$ over $\mathbf{F}_q$ is defined as

$$\mathrm{supp}(\mathcal{C}) = \{i \mid x_i \neq 0 \text{ for some } \mathbf{x} \in \mathcal{C}\}.$$

If $\mathcal{C}$ is an $[n,k]$ code, for $1 \leq r \leq k$, the rth *generalized Hamming weight* of $\mathcal{C}$ is defined by

$$d_r(\mathcal{C}) = \min\{\#\mathrm{supp}(D) \mid D \text{ is a linear subcode of } \mathcal{C} \text{ with } \dim(D) = r\}.$$

The sequence of generalized Hamming weights, or *weight hierarchy* of $\mathcal{C}$, was introduced by Helleseth, Kløve and Mykkleveit, [7], and rediscovered by Wei, [17]. Nowadays, the weight hierarchy plays a central role in coding theory, and much is known about it for several classes of codes: Hamming codes, Golay codes, Reed-Muller codes, algebraic geometric codes, etc.

Recently, Heijnen and Pellikaan, [10], have given a new bound for higher Hamming weights. This so called *order bound*, which is a generalization of the Feng-Rao bound on the minimum distance, allowed the determination of the complete hierarchy of q-ary Reed-Muller codes. Using this bound, we study the weight hierarchy of hyperelliptic codes.

The organization of the paper is as follows: Hyperelliptic codes are defined in Section 2 where some known results are also included. The generalized Hamming weights are computed using the order bound in Section 3. In Section 4, we deal with the special case. We give a construction method of hyperelliptic curves so that the associated algebraic geometric codes have the weight hierarchy fully determinated. To show that examples of such curves exist, we will construct a class of them.

*The author is with University of Basque Country, Department of Mathematics, Apartado 644, 48080 Bilbao, Spain; E-mail mtpraald@lg.ehu.es

2 Hyperelliptic codes and known results

C. Munuera proved, [13], the next result.

Theorem 1 *Let $C(D,G)$ be a code with dimension k and abundance α. Then, for every $1 \leq r \leq k$*

$$\begin{aligned} d_r(C(D,G)) &= \min\{\deg(D^{'}) \mid 0 \leq D^{'} \leq D, l(G-D+D^{'}) \geq r+\alpha\} \\ &= n - \max\{\deg(D^{''}) \mid 0 \leq D^{''} \leq D, l(G-D^{''}) \geq r+\alpha\}. \end{aligned}$$

An absolutely irreducible smooth curve $\mathcal{X}$ is hyperelliptic if and only if its genus is at least two and there exists a morphism of degree two from $\mathcal{X}$ to the projective line or if its genus is at least two and there exists a rational divisor H with $l(H) = \deg(H) = 2$. $\mathcal{X}$ allows a unique involution (conjugation), the hyperelliptic involution, denoted by σ. The fixed points of σ are called hyperelliptic points, for this kind of points the rth pole number is γ_r, the rth gonality of the curve. The next result related to this fact is known.

$$\gamma_r = \begin{cases} 2r-2 & \text{if } r \leq g, \\ r+g-1 & \text{if } r > g. \end{cases}$$

Then if Q is a hyperelliptic point, its Weierstrass semigroup is generated by 2 and $2g-1$.

For rational points P, $\{P, \sigma(P)\}$ are called hyperelliptic (conjugated) pairs.

In this paper we consider algebraic geometric codes $C(D,G)$ arising from hyperelliptic curves with the property that, if $\mathrm{supp}D = \{P_1, ..., P_n\} \subseteq \mathcal{X}(\mathbf{F}_q)$, then for every P_i, $\sigma(P_i) \in \mathrm{supp}D$. Let π be the number of conjugated pairs in $\mathrm{supp}D$. We consider $G = mQ$, with $Q \notin \mathrm{supp}D$ and Q a hyperelliptic point. We denote the algebraic geometric code by $\mathcal{C}(m)$ and the rth generalized Hamming weigth by $d_r(m)$.

For this kind of codes we have the next known results. First of all, we have an estimate for the generalized Hamming weights proved by C. Munuera, [13].

Proposition 1 *Let $\mathcal{C}(m)$ be a $[n,k]$ hyperelliptic code with abundance $\alpha > 0$. For $1 \leq r \leq \min\{\pi, g-\alpha, k\}$ we have*

$$n - m + 2(r+\alpha-1) \leq d_r(m) \leq 2r.$$

Moreover, when $G - D$ is a hyperelliptic divisor we get the equality

In the case $m < n$ and even, we have the next result by De Boer, [2]

Proposition 2 *Let $\mathcal{C}(m)$ be a hyperelliptic code with $m = 2l < n$. We denote $\Delta = l - \pi$,*

$$d_r(m) = \begin{cases} n - 2l + \gamma_r + \min\{\Delta - r + 1, 2g+1-w\} & \text{if } 1 \leq r \leq \min\{l-g, \Delta\}, \\ n - 2l + r - 1 + \Delta & \text{if } l-g+1 \leq r \leq \Delta, \\ n - 2l + \gamma_r & \text{if } \Delta + 1 \leq r \leq g, \\ n - k + r & \text{if } r \geq g+1. \end{cases}$$

3 The order bound for the generalized Hamming weights

The order bound for the generalized Hamming weights has been introduced by P. Heijnen and R. Pellikaan, [10]. It is a generalization of the Feng-Rao bound for the minimum distance. For the reader's convenience we shall explain it briefly in this section.

Let $\mathcal{L} = \cup_{t=0}^{\infty}\mathcal{L}(tQ)$ and let $\{f_1, f_2, \cdots\}$ be a basis of $\mathcal{L}$ such that $-v_Q(f_i) < -v_Q(f_{i+1})$ for all i, where v_Q is the valuation at Q. Note that $\{-v_Q(f) \mid f \in \mathcal{L}\} = S$.

For every positive integer l let us consider the code

$$C_l = \langle ev(f_1), \cdots, ev(f_l)\rangle^{\perp}$$

and the set

$$A(l) = \{p_i \in S \mid p_i + p_j = p_{l+1} \text{ for some } p_j \in S\}.$$

Furthermore, for $l_1 < \cdots < l_r$, let us define the set $A(l_1, \cdots, l_r)$ by

$$A(l_1, \cdots, l_r) = A(l_1) \cup \cdots \cup A(l_r).$$

Definition 1 Let l be a positive integer. The number

$$d_r^{ORD}(l) = \min\{\#A(l_1, \cdots, l_r) \mid l \leq l_1 < \cdots < l_r\}$$

is called the *order bound* for the rth generalized weight of C_l.

Theorem 2 *For $1 \leq l \leq n+g$, we have*

$$d_r(C_l) \geq d_r^{ORD}(l).$$

The proof of this theorem can be found in the article by Heijnen and Pellikaan ([10], Theorem 3.14). Note that $C_l = (0)$ for $l > n+g$.

Let us compute the value of l. It is known that $\mathcal{C}_{\mathcal{L}}(D, mQ) = C_l$ with $l = l(D + W - mQ)$. We suppose $D \sim nQ$ and hence $l = l((n + 2g - 2 - m)Q)$ (we observe that $(2g-2)Q$ is a canonical divisor).

Proposition 3

$$l(D + (2g-2)Q - mQ) = \begin{cases} n - m + g - 1 & \text{if } \ m < n. \\ [n - m/2] + g & \text{if } \ m \geq n. \end{cases}$$

Proof. The case $m < n$ is a direct consequence of Riemann-Roch theorem. In the other case, we can write $n - m = 2s$ and then $n - m + 2g - 2 = 2(g+s) - 2$ is a pole number in Q and for this $l((n - m + 2g - 2)Q) = g + s$. ∎

To compute the order bound we must study the $A(l)$ sets.

Proposition 4 *We have that*

(i) **[Type I]** *If $1 \leq l \leq g-1$, then*

$$A(l) = \{2i - 2 \mid 1 \leq i \leq l+1\}.$$

(ii) **[Type II]** *For $g \leq l \leq 3g-1$,*

(ii.a) If $l+g$ is even, then

$$A(l) = \{2i-2 \mid 1 \leq i \leq g\} \cup \{i+g-1 \mid g+1 \leq i \leq l+1, l-i \ odd\}.$$

(ii.b) If $l+g$ is odd, then

$$A(l) = \{2i-2 \mid 1 \leq i \leq (l-g+1)/2\} \cup \{i+g-1 \mid g+1 \leq i \leq l+1, \ l-i \ odd\}.$$

(iii) **[Type III]** *For $l \geq 3g$*

$$\begin{aligned} A(l) = & \{ \ 2i-2 \mid 1 \leq i \leq g\} \cup \{i+g-1 \mid g+1 \leq i \leq l-2g+1\} \\ \cup & \ \{i+g-1 \mid l-2g+3 \leq i \leq l+1 \ , l-i \ \ odd\}. \end{aligned}$$

We can now calculate the order bound. In the case $1 \leq m < n$, the order bound does not give relevant information. When $m \geq n$, we get the next result.

Proposition 5 *For $n \leq m$ we have*

$$d_r^{ORD}([n-m/2]+g) = 2r.$$

Proof. a.- If every l is of type I, $\#A(l_1,\ldots,l_r) = \#A(l_r) \geq [n-m/2]+g+r$.

b.- If every l is of type II, we have the minimun and the equality with $l_i = g+1+2i-2$, $1 \leq i \leq r$.

c.- If every l is of type III, $\#A(l_1,\ldots,l_r) \geq l_r - g + 1 \geq 3g + 2(r-1) - g + 1 \geq 2r$.

Finally when, $l_1,\ldots,l_s$ are of type I, $l_{s+1},\ldots,l_{s+t}$ of type II and the rest of type III, it is easy to see that $\#A(l_1,\ldots,l_r) \geq l_r - g + 1 \geq 3g + 2(r-s-t-1) \geq 2g+1 \geq 2r$. ■

We obtain the next corollary

Corollary 1 *For $m \geq n$ we have $d_r(m) = 2r$ while $1 \leq r \leq \min\{\pi, g-\alpha, k\}$.*

4 Weight Hierarchy of odd and non abundant codes

To finish, we must compute the weight hierarchy of $\mathcal{C}(m)$ with $m < n$ and odd.

We could write $\text{supp}D = \{W_1,...,W_w,Q_1,\sigma(Q_1),...,Q_\pi,\sigma(Q_\pi)\}$, with W_i hyperelliptic for every $i = 1,...,w$.

The number of conjugated pairs is related to the weight hierarchy as can be seen in the De Boer theorem. We use the techniques by De Boer in our case,[2].

4.1 Divisors on Hyperelliptic curves

The main property that we use is the **unique reduction property (or URP)**. Let D be an effective divisor. By replacing all conjugated pairs in D by $2Q$ we can write $D \sim F + mQ$ with F such that $\sigma(P) \notin \text{supp}(F)$ if $P \in \text{supp}(F)$. In this case, we say that D is reduced to F and we call F a **semi-reduced** divisor. From Riemman-Roch theorem, it follows that every effective divisor can be reduced uniquely to a semi-reduced divisor of degree less than or equal to g; such divisors are called reduced divisors.

Let $\mathcal{C}(m)$ be a code with $m = 2l-1 < n$. Then, for $r \leq g$, we can write $d_r(m) = n - m + \gamma_r + \delta$ with $0 \leq \delta \leq g-r+1$. We have the next result.

Proposition 6 *Let $m = 2l - 1$, then*

$$\begin{array}{lll} \pi & \geq & l - r + 1 - \delta \qquad\qquad \text{if } q \text{ is even or } \deg G - \gamma_r \leq 2g - 1, \\ \pi & \geq & l - r + 1 - \delta \text{ or } \delta + w \geq 2g + 1 \qquad \text{in other case.} \end{array}$$

We analyse the inverse of the last proposition when $\delta = 0$.

Proposition 7 *If $\pi \geq l - r + 1$ then*

$$n - m + \gamma_r \leq d_r(m) \leq n - m + \gamma_r + 1.$$

Proof. The first inequality is a known result. To prove the other one we take $D' = P_1 + \sigma(P_1) + \ldots + P_{(m-1-\gamma_r)/2} + \sigma(P_{(m-1-\gamma_r)/2})$ so that $l(G - D') \geq r$ and, from theorem 1, $d_r(m) \leq n - m + \gamma_r + 1$. ■

As a consequence of the previous result we get the next theorem.

Theorem 3 *Let $\mathcal{C}(m)$ be a hyperelliptic code with $m = 2l-1 < n$ and let us denote $\Delta = l - \pi$. Then,*

$$d_r(m) = \begin{cases} n - 2l + 1 + \gamma_r + \min\{\Delta - r + 1, 2g + 1 - w\} & \text{if } 1 \leq r \leq \min\{l - g, \Delta\}, \\ n - l + r - \Delta & \text{if } l - g + 1 \leq r \leq \Delta, \\ n - 2l + 1 + \gamma_r \text{ or } n - 2l + 1 + \gamma_r + 1 & \text{if } \Delta + 1 \leq r \leq g, \\ n - k + r & \text{if } r \geq g + 1. \end{cases}$$

Proof. We can suppose that $1 \leq r \leq g$. When $\deg G - 2\pi \leq \gamma_r \leq 2g - 2$ we can use the previous proposition.

For $\deg G - 2g + 1 \leq \gamma_r \leq \deg G - 2\pi - 1$, we have that $\delta \geq (\deg G - \gamma_r - 2\pi + 1)/2$ and we get one inequality. For the equality we take $D' = P_1 + \sigma(P_1) + ... + P_\pi + \sigma(P_\pi) + W_1 + ... + W_{(\deg G - 2\pi - \gamma_r - 1)/2}$ and we can see that $G \sim P_1 + \sigma(P_1) + ... + P_\pi + \sigma(P_\pi) + 2W_1 + ... + 2W_{(\deg G - 2\pi - 1)/2} + Q$. Hence, therefore

$$l(G - D') \geq l(2W_{(\deg G - 2\pi - \gamma_r + 1)/2} + ... + 2W_{(\deg G - 2\pi - 1)/2}) \geq r.$$

From theorem 1, we get the equality.

With the same techniques we demostrate that for $0 \leq \gamma_r \leq \min\{\deg G - 2g - 1, \deg G - 2\pi - 1\}$

$$d_r(m) = n - \deg G + \gamma_r + \min\{(\deg G - 2\pi - \gamma_r + 1)/2, 2g + 1 - w\}.$$

■

Taking this result into account we see that for $\Delta + 1 \leq r \leq g$ we have two possible values for $d_r(m)$.

We observe that $d_r(m) = n - m + \gamma_r$ if and only if there exists an effective divisor $D' \leq D$ with $D' \sim (m - \gamma_r)Q$. In the last section, we give a construction method of hyperelliptic codes such that the generalized Hamming weights are fully determinated.

5 Construction of examples

We know that if $\mathcal{X}$ is a hyperelliptic curve over K, we can represent $\mathcal{X}$ in the form $K(x, y)$ where, if $\mathrm{char}(K) = 2$, the equation of the curve is $y^2 + y = r(x)$ with $r(x) \in K(x)$.

Let $\mathcal{X}$ be a hyperelliptic curve over K with characteristic equal to 2. We suppose that the equation associated to the curve is $y^2 + y = f(x)$ with $f(T) + y^2 + y \in \mathbf{F}_q(y)[T]$ irreducible and there exists $\alpha \in \mathbf{F}_q$ with the property that $f(T) + \alpha^2 + \alpha$ has $\deg f$ distinct roots in $\mathbf{F}_q$. From Kummer's theorem, exist $P_1, ..., P_{degf}$ rational points with $(y - \alpha) = P_1 + ... + P_{\deg f} - (\deg f)Q$.

The rational points of this curve are

$$\mathcal{X}(\mathbf{F}_q) = \{Q, P_1, \sigma(P_1), ..., P_{\deg f}, \sigma(P_{\deg f}), M_1, \sigma(M_1)..., M_t, \sigma(M_t)\}.$$

Proposition 8 *In the previous conditions, there exists an effective divisor $D' \leq D$ linearly equivalent to hQ if and only if h is even or h is odd in the interval* $[\deg f, \deg f + 2t]$.

Proof. The even case is obvious. Let h be odd. If there exists such divisor then h is a pole number and hence $h \geq degf = 2g + 1$. Moreover, with the conjugated pairs we have $P_1 + ... + P_{\deg f} + M_1 + N_1 + ... + M_t + N_t \sim (\deg f + 2t)Q$. We suppose that $h > \deg f + 2t$. If exists $D' \sim hQ$, the number of conjugated pairs in $\mathrm{supp} D'$ would be at least $h - \deg f - t$. Let δ be the number of conjugated pairs. Then there exists $D'' \sim (h - 2\delta)Q$, with $h - 2\delta \leq 2\deg f + 2t - h < \deg f$ but it is impossible. ∎

After this result we conclude the following.

Corollary 2 *Let $\mathcal{X}$ be a hyperelliptic curve over a finite field of characteristic equal to 2. We assume that the curve has associated the equation $y^2 + y = f(x)$ with two properties. $f(T) + y^2 + y \in \mathbf{F}_q(y)[T]$ is irreducible and there exists $\alpha \in \mathbf{F}_q$ where $f(T) + \alpha^2 + \alpha$ has* $\deg(f)$ *distinct roots. Let $\mathcal{C}(m) = \mathcal{C}_{\mathcal{L}}(D, mQ)$ be the algebraic geometric code. Then*

$$d_r(m) = \begin{cases} n - m + \gamma_r & m - \gamma_r \text{ is even or is odd in } [degf, degf + 2t]. \\ n - m + \gamma_r + 1 & \text{in other case.} \end{cases}$$

An equivalent construction can be given in the case $\mathrm{char}(\mathbf{F}_q) \neq 2$.

5.1 Example

We consider the equation $y^2 + y = x^s + 1$ where s is a divisor of $q - 1$.

The number of rational points of the curve $y^2 + y = x^{q-1} + 1$ is $2q + 1$ if q is an even power of two and $2q - 1$ in other case.

For the curve $y^2 + y = x^s + 1$, the rational points are $P_i = ((\alpha^i)^{q-1/s} : 0 : 1), Q_i = ((\alpha^i)^{q-1/s} : 1 : 1)$ with $0 \leq i \leq s - 1$ and the infinity point Q and, when q is an even power of two, we have two other points $M = (0 : \beta : 1)$ and $N = (0 : \beta + 1 : 1)$.

From Hilbert's theorem, we have

Theorem 4 *Let $y^2 + y = x^s + 1$ be the equation of the curve considered, with $q = 2^{2h}$ and $\frac{(q-1)}{(\sqrt{q}-1)} \mid s \mid q - 1$. There exists an effective divisor $D' \sim mQ$ if and only if m is even or $m = s, s + 2, ..., 2q - s$.*

Proof. When $(q-1)/(\sqrt{q}-1)|s$, we have $\beta^{\sqrt{q}s}=\beta^s$. So $\mathrm{Tr}((\beta)^s+1)=2\beta^s+2\beta^{2s}+...+2\beta^{2^{(h-1)}s}=0$. Let $\{P_1,Q_1,...,P_s,Q_s,M_1,\ N_1,...,M_t,N_t\}$ be the rational points different from the infinity point. From proposition 8 $P_1+...+P_s\sim sQ$, $P_1+...+P_s+M_1+N_1\sim(s+2)Q$, $\ldots$, $P_1+...+P_s+M_1+N_1+...+M_t+N_t\sim(s+2t)Q$. ■

We conclude the next result

Corollary 3 *Let $\mathcal{C}(m)$ be the AG code associated to the curve $y^2+y=x^s+1$ over $\mathbf{F}_q$. If q is a square and $s\in\mathbf{Z}$ with $(q-1)/(\sqrt{q}-1)|s|q-1$, then,*

$$d_r(m)=\begin{cases} n-m+\gamma_r & \text{if } m-\gamma_r \text{ is even or equal to } s,s+2,\ldots,2q\text{-}s. \\ n-m+\gamma_r+1 & \text{in other case.}\end{cases}$$

References

[1] A. Barbero y C. Munuera, "The weight hierarchy of Hermitian codes" *SIAM J. Discrete Math.* vol. 13, pp.79-104, 2000.

[2] M. A. de Boer, "The Generalized Hamming Weights of some Hyperelliptic Codes", *J. Pure Appl. Algebra* vol. 123, pp. 153-163, 1998.

[3] G.D. Forney, Jr., "Dimension/Length Profiles and Trellis Complexity of Linear Block Codes", *IEEE Trans. Inform. Theory,* vol. IT-40, pp. 1741-1752, Nov., 1994.

[4] G.L. Feng, K.K. Tzeng y V.K. Wei, "On the generalized Hamming weights of several classes of cyclic codes ", *IEEE Trans. Inform. Theory,* vol. IT-38, pp.1125-1130, May 1992.

[5] G.L. Feng, J. Zhu, X-W. Wu y T.R.N. Rao, "The generalized Hamming weights of Algebraic Geometry codes from Type I curves", preprint del año 2000.

[6] T. Helleseth y P.V. Kumar, "The weight Hierarchy of the Kasami codes", *Discrete Math.,*

[7] T. Helleseth, T. Kløve y J. Mykkeleveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$", *Discrete Math.* vol. 18, pp. 179-211, 1977.

[8] T. Helleseth, T. Kløve y O.Ytreus, "Generalized Hamming weights of linear codes", *IEEE Trans. Inform. Theory,* vol. 38, pp. 1133-1140, 1992.

[9] T. Høholdt, J.H. van Lint y R. Pellikaan, "Algebraic Geometry Codes", to appear in *Handbook of Coding Theory*, R.A. Brualdi, W.C. Huffman, V. Pless (Eds.), Elsevier.

[10] P. Heijnen y R. Pellikaan, "Generalized Hamming weights of q-ary Reed-Muller codes". *IEEE Trans. Inform. Theory*, vol. IT-44. pp. 181-197, January 1998.

[11] T. Kasami, T. Tanaka, T. Fujiwara y S.Lin "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary codes", *IEEE Trans. Inform. Theory,* vol. IT-39, pp. 242-245, Jan., 1993.

[12] T. Kasami, T. Tanaka, T. Fujiwara y S.Lin "On complexity of trellis structure of linear block codes", *IEEE Trans. Inform. Theory,* vol. IT-39, pp. 1057-1064, May, 1993.

[13] C. Munuera, "On the Generalized Hamming Weights of Geometric Goppa Codes", *IEEE Trans. Inform. Theory*, vol.IT-40, pp. 2092-2099, November 1994.

[14] C. Munuera y D. Ramirez-Alzola, "The Second and The Third Generalized Hamming Weigths on Hermitian Codes". *IEEE Transactions on Information Theory*, Vol.45,N0.2, March 1999.

[15] D. Ramirez-Alzola, "On the State Complexity of Hyperelliptic Codes". Submitted to *IEEE Transactions on Information Theory*, November 2002.

[16] M. Tsfasman y S.G. Vlăduţ, "Geometric approach to higher weights", *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1564-1588, November 1995.

[17] V.K. Wei, "Generalized Hamming weights for linear codes", *IEEE Trans. Inform. Theory,* vol. IT-37, pp. 1412-1418, May 1991.

[18] V.K. Wei y K. Yang, "On the generalized Hamming weights of products codes", *IEEE Trans. Inform. Theory,* vol. IT-39, pp. 1709-1713, Sept. 1993.

[19] K. Yang, P.V. Kumar y H. Stichtenoth, "On the weight hierarchy of Geometric Goppa Codes", *IEEE Trans. Inform. Theory,* vol. IT-40, pp. 913-920, 1994.