The weight hierarchy of Ham(r, q)

F. Farhang Baftani
Department of Mathematics
Science and Research Branch
Islamic Azad University (IAU)
Tehran
Iran
far-farhang2007@yahoo.com

A. Tehranian*
Department of Mathematics
Science and Research Branch
Islamic Azad University (IAU)
Tehran
Iran
tehranian@srbiau.ac.ir

H.R. Maimani
Mathematics Section
Department of Basic Sciences
Shahid Rajaee Teacher Training University
P.O. Box 16785-163, Tehran
Iran
maimani@ipm.ir

Abstract. Calculation of the weight hierarchy for codes, is an attractive and applicable topic in coding theory and cryptography. In this paper, we obtain the weight hierarchy of Hamming codes over F_q. As a result of weight hierarchy of Hamming codes, we compute the weight hierarchy of simplex codes.
Keywords: generalized Hamming weight, weight hierarchy, MDS code, simplex code.

1. Introduction

In this paper, we denote $\mathbb{F}_q$ as a field of order q. Let C be a $[n, k, d]$ linear code over F_q, with parity check matrix, H. For a subspace D of C, the *support* of D is denoted by *supp*(D) and is defined as follows

$$\mathrm{supp}(D) = \{i : \exists(v_1, v_2, \cdots, v_n) \in D; v_i \neq 0\}.$$

The $r-th$ *generalized Hamming wight* for code C, denoted by $d_r(C)$, is defined as follows

$$d_r = d_r(c) = \min\{\|D\| : D \subset C, \dim(D) = r\},$$

∗. Corresponding author

where $\|D\| = |\text{supp}(D)|$. It is not difficult to see that $d_1(C) = d(C)$.

The concept of generalized Hamming weights (GHWs) were introduced by Wei [7] in 1990. In [5], Ozarow and Wyner had introduced a linear coding scheme on the wire-tap channel of Type II in connection with Cryptography. Wei [7] has shown that the generalized Hamming weights completely characterize the performance of a linear code when it is used on the above channel.

An $[n, k, d]$ linear code ,C, over F_q is called *Maximum Distance Separable*, (MDS), code if $d = n - k + 1$ and we call that C as $r-th$ *Maximum Distance Separable*,($r-$MDS), code when $d_r(C) = n - k + r$. Also, we say that C is a *proper* r *-MDS*(or P_r-MDS) code, where C is an r-MDS code and it is not an $(r-1)$-MDS code.

One may find known theorems about MDS and r- MDS codes in [3, 6].

Consider the $r \times (q^r - 1/q - 1)$ matrix H, where each column of H is a nonzero vector of each 1-dimensional subspace of F_q^r. The linear code which H is a parity check matrix, is called Hamming code and it is denoted by $Ham(r, q)$. For $q = 2$, the weight hierarchy of code was found by Wei [7]. In this paper we calculate the weight hierarchy for any q, where q is a power of a prime.

Suppose that C is a linear code over F_q. The *dual code* of C, denoted by $C^\perp$, is the orthogonal complement of C.

Remember that two vectors x and y are orthogonal when the inner product of them is equal to 0. Also, for a nonempty subset D of F_q^n, the orthogonal complement of D, denoted by $D^\perp$, is defined as follows $D^\perp = \{x \in F_q^n : x.y = 0, \forall y \in D\}$.

The dual of $q-$ary Hamming code$Ham(r, q)$ is called a $q-$array simplex code. We denote it by $S(r, q)$ (see [4]).

2. Main result

In this section, we give the generalized Hamming weights of Hamming codes over $\mathbb{F}_q$. At first we stat some properties of generalized Hamming weights which help us to computing the generalized Hamming weights of Hamming codes.

Theorem 2.1 ([7]). *Suppose that C is an $[n, k, d]-$ code over F_q with parity check matrix H. Then:*

(a) $\{d_r(C) : 1 \le r \le k\} = \{1, 2, ..., n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \le r \le n - k\}$,

(b) $1 \le d_1(C) < d_2(C) < ... < d_k(C) \le n$,

(c) If H_i's are columns of H for $1 \le i \le n$, then

$$d_r(C) = \min\{|X| : |X| - rank(< H_i : i \in X >) = r\}.$$

Theorem 2.2 ([1]). *If C is a linear $[n, k, d]$ code over F_q, then*

$$d_r \le n - k + r, 1 \le r \le k.$$

The following theorem shows a relation between the columns of H and $d(C)$.

Theorem 2.3 ([4]). *Let C be a linear code and H denote its parity-check matrix. Then the following statements are equivalent:*

(i) $d_1(C) = d$;

(ii) Any $d-1$ columns of H are linearly independent and H has d linearly dependent columns.

Theorem 2.4 ([1]). *Let C be an $[n, k, d]$ code over F_q and $C^\perp$ be an $[n, n-k, d^\perp]$ code. Then, we have:*

(a) If C is an r- MDS code over F_q, then C is an r_1- MDS code for all $r \le r_1 \le k$,

(b) If $d^\perp = 1$, then C is not a P_r-MDS code for any $1 \le r \le k$,

(c) If $d^\perp > 1$, then C is a $P_{k-d^\perp+2}$-MDS code.

The following theorem states the properties of $Ham(r, q)$

Theorem 2.5 ([4]). *Suppose that $Ham(r, q)$ is the Hamming code over the field $\mathbb{F}_q$. Then:*

(i) $Ham(r, q)$ is a $[(q^r-1)/(q-1), (q^r-1)/(q-1)-r, 3]$- code.

(ii) $Ham(r, q)$ is a perfect exactly single-error-correcting code.

Now we compute the generalized Hamming weights of Hamming codes over the field $\mathbb{F}_q$.

Theorem 2.6. *Let C be the Hamming code over the field $\mathbb{F}_q$ and $d_l(C)$ be the l-th generalized Hamming weight of C. Then*

$$d_l(C) = \begin{cases} l+2 & 1 \le l \le q-1, \\ l+3 & (T_2 =) q \le l \le q^2+q-2 (= T_3 - 3), \\ l+4 & (T_3 - 2 =) q^2+q-1 \le l \le q^3+q^2+q-3 (= T_4 - 4) \\ \vdots & \\ l+r & T_{r-1} - (r-2) \le l \le T_r - r \end{cases}$$

where $T_i = (q^i - 1)/(q-1)$

Proof. From Theorem 2.5, we know that $Ham(r, q)$ is a $[(q^r-1)/(q-1), (q^r-1)/(q-1)-r, 3]$ code. Hence $d = d_1 = 3$. By Theorems 2.1(b) and 2.2, we have $4 \le d_2 \le r+2$. For computing these generalized Hamming weights, we use Theorem 2.1(c). Let H denote the parity check matrix of $Ham(r, q)$ and H_i denote the i-th column of H. Since $d = 3$, by Theorem 2.4, every two columns of H are independent. Let H_t, H_s be two independent columns of H. Consider two columns H_s and H_t. The subspace $< H_s, H_t >$ has dimension two, and has $(q^2-1)/(q-1) = q+1$ subspaces of dimension 1. Except H_s and H_t, we have $q-1$ subspaces of dimension 1 in $< H_s, H_t >$. We denote these subspaces by $H_1, H_2, \cdots H_{q-1}$. For any $S \subseteq \{H_1, H_2, \cdots, H_{q-1}\}$, $< H_s, H_t >= < H_s, H_t, S >$. Hence by Theorem 2.1 (c), we have

$$d_l = l+2, 1 \le l \le (q-1).$$

For d_q we should use three independent columns of H (Note that since H is a matrix of rank r, then H has r independent columns). By Theorems 2.1(b) and 2.2, we have $q+2 \leq d_q \leq r+q$. We claim that $d_q = q+3$. Consider three independent columns H_{i_1}, H_{i_2} and H_{i_3}. The space generated by these three columns has $(q^3-1)/(q-1) = (q^2+q+1)$ subspaces of dimension 1. Except H_{i_1}, H_{i_2} and H_{i_3}, we have q^2+q-2 subspaces of dimension 1 in $< H_{i_1}, H_{i_2}, H_{i_3} >$. Call them $H_1, H_2, \cdots, H_{q^2+q-2}$. For any $S \subseteq \{H_1, H_2, \cdots, H_{q^2+q-2}\}$, we have $< H_{i_1}, H_{i_2}, H_{i_3} >= < H_{i_1}, H_{i_2}, H_{i_3}, S >$. Hence by Theorem 2.1 (c), we conclude that

$$d_l = l+3, (((q^2-1)/(q-1))-2) = q \leq l \leq q^2+q+1 = (((q^3-1)/(q-1))-3).$$

For the rest of prove, we continued this process and the result is obtained. □

Corollary 2.1. *The weight hierarchy for $S(r,q)$ is as follows* $\{q^{r-1}, q^{r-1}+q^{r-2}, q^{r-1}+q^{r-2}+q^{r-3}, ..., q^{r-1}+q^{r-2}+q^{r-3}+...+q, q^{r-1}+q^{r-2}+q^{r-3}+...+q+1\}$

Proof. Use Theorems 2.1 and 2.6. □

Corollary 2.2. *The code $Ham(r,q)$ is an P_s- MDS code for $s \geq ((q^r-1)/q-1) - q^{r-1} - (r-2)$.*

Let C be a code over $\mathbb{F}_q$. The *extended code* of C, which is denoted by $\bar{C}$, is defined as follows

$$\bar{C} = \{(c_1, c_2, ..., c_n, -\sum_{i=1}^{n} c_i) : (c_1, c_2, \cdots, c_n) \in C\}.$$

The code $\bar{C}$ is an $(n+1, M, \bar{d})$ code over F_q and $d \leq \bar{d} \leq d+1$. If C is linear, then $\overline{C}$ is linear too and if H is parity check matrix of C, then $\overline{H}$ the parity check matrix for $\overline{C}$, is as follows

$$\bar{H} = \left[\begin{array}{cccc|c} & & H & & 0 \\ - & - & - & - & - \\ 1 & 1 & 1 & \cdots & 1 \end{array}\right].$$

In the following we find generalized hamming weights for extended code of Hamming code over $GF(3)$.

Let $C = Ham(m,3)$ and $\bar{C} = \overline{Ham(m,3)}$. Let d_r and $\bar{d_r}$ denote the $r-$th generalized Hamming weight for C and $\bar{C}$, respectively. Also, H and $\bar{H}$ denote the parity check matrices for C and $\bar{C}$, respectively. Let H_i and $\bar{H}_i$ be the $i-$th columns of C and $\bar{C}$, respectively.

We know that

$$\bar{H} = \left[\begin{array}{cccc|c} & & H & & 0 \\ - & - & - & - & - \\ 1 & 1 & 1 & \cdots & 1 \end{array}\right].$$

The construction of $\bar{H}$ shows that it contains columns $(1,1,1,0,...,0)$ and $(1,0,1,0,...,0)$ and $(1,2,1,0,...,0)$. It is clear the element $\bar{x}$ whose coordinates are 1 in the corresponding columns to these vectors and 0 in other columns, is belonging to $\bar{C}$. Note that $wt(\bar{x}) = 3$, so by theorem (2.5) we conclude that $\bar{d_1} = 3$.

Remember that $\overline{d_2} = \min\{|X| : |X| - rank(< \bar{H}_i : i \in X >) = 2\}$. It is impossible to use $rank(< \bar{H}_i : i \in X >) = 2$ to calculate $\bar{d_2}$. For this, suppose that there exists $X = \{\bar{H}_{i_1}, \bar{H}_{i_2}, \bar{H}_{i_3}, \bar{H}_{i_4}\}$ such that $rank(< \bar{H}_{i_1}, \bar{H}_{i_2} >) = 2$. Now, $\bar{H}_{i_3}$ is a linear combination of $\bar{H}_{i_1}, \bar{H}_{i_2}$. Hence there are c_1, c_2 belonging to F_3 such that $c_1\bar{H}_{i_1} + c_2\bar{H}_{i_2} = \bar{H}_{i_3}$. Regarding that all the coordinates in the last row of $\bar{H}$ is 1, we have $c_1 + c_2 = 1$. Hence $c_1 = 1$ or $c_2 = 1$ and in particular $\bar{H}_{i_3} = \bar{H}_{i_1}$ or $\bar{H}_{i_3} = \bar{H}_{i_2}$. Then $H_{i_3} = H_{i_1}$ or $H_{i_3} = H_{i_2}$. This is a contradiction to the definition of H. So, we should use $rank3$ to calculate $\bar{d_2}$. Hence $\bar{d_2} = 5$.

Suppose that $rank(< \bar{H}_{j_1}, \bar{H}_{j_2}, \bar{H}_{j_3} >) = 3$. Now, we can add columns to these columns without changing the rank of this subspace. To calculate the number of these columns, we should solve the the equation $c_1\bar{H}_{j_1} + c_2\bar{H}_{j_2} + c_3\bar{H}_{j_3} = \bar{H}_{j_4}$ in particular we should solve the equation $c_1 + c_2 + c_3 = 1$ in F_3. The set

$$\{(2,2,0),(1,1,2),(2,0,2),(0,2,2),(1,2,1),(2,1,1)\}$$

contains the whole solutions of this equation. Then we can use $rank3$ to calculate the higher weights till $\bar{d_6}$. It is clear that $\bar{d_6} = 9$.

For $\bar{d_7}$, we should use $rank4$ and solve the equation $c_1 + c_2 + c_3 + c_4 = 1$ in F_3. This equation has 23 solution and we can use $rank4$ to calculate $\bar{d_{23}}$. By continuing this process, we can find the other values of $\bar{d_r}$'s.

Acknowledgments

The authors would like to thank the referee for his/her helpful remarks which have contributed to improve the presentation of the article.

References

[1] S. T. Dougherty, S. Han, *Higher weights and generalized MDS codes*, Korean Math. Soc., 6 (2010), 1167-1182.

[2] S.T. Dougherty, S. Han, H. Liu, *Higher weights for codes over rings*, Springer-Verlag, 2011.

[3] W. C. Huffman, V. S. Pless , *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[4] S.Ling, C.Xing, *Coding theory a first course*, Cambridge University Press, 2004.

[5] L.H Ozarow, A.D. Wyner, *Wire-tap channel-II*, AT and T Bell Labs. Tech. J., 63 (1984), 2135-2157.

[6] L. R. Vermani, *Elements of algebric coding theory*, Chapman and Hall Mathematics Series, Chapman and Hall Ltd., London, 1996.

[7] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory., 37 (1991), 1412-1418.

Accepted: 13.06.2019