SCIENCE CHINA
Information Sciences

• LETTER •

July 2020, Vol. 63 179103:1–179103:3
https://doi.org/10.1007/s11432-018-9610-9

Weight distribution of two classes of linear codes with a few weights

Yuanlong SONG & Jing YANG*

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, *China*

Received 30 May 2018/Accepted 5 September 2018/Published online 19 May 2020

Citation Song Y L, Yang J. Weight distribution of two classes of linear codes with a few weights. Sci China Inf Sci, 2020, 63(7): 179103, https://doi.org/10.1007/s11432-018-9610-9

Dear editor,

Linear codes have been widely studied in coding theory and have extensive applications due to their good properties. In this study, p denotes an odd prime and $q = p^m$ for a positive integers $m \geqslant 2$. $\mathbb{F}_q$ means a finite field with q elements. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ means a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum (Hamming) distance d (see [1]).

For each $i \in \{0, 1, \ldots, n\}$, A_i denotes the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

$$A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n,$$

where $A_0 = 1$. In particular, the sequence $(A_0, A_1, \ldots, A_n)$ is called the weight distribution of the code $\mathcal{C}$. Here, we call $\mathcal{C}$ a t-weight code if $|\{1 \leqslant i \leqslant n : A_i \neq 0\}| = t$.

The study of the weight distribution of linear codes has played an important role in both theory and applications for the following reasons:

- The weight distribution of a code induces the minimum distance of the code, which helps to obtain the error correcting capability.
- The weight distribution of a code enables the computation of the error probability of error detection in terms of error correction algorithms.

Recently, the linear codes with a few weights have become a hot research topic, since they are applied widely in communication systems, data storage systems and consumer electronics. If we know the weight distribution of a series of linear codes, we can choose the ones with a few weights. Therefore, the weight distribution of a linear code is significant and has been paid a lot of attention by many researchers. However, learning the weight distribution of linear codes is an intractable and complicated problem, and it still remains open.

Ding et al. [2,3] gave the generic construction of linear codes, which is the so-called "Defining set". Let the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathbb{F}_q$ and Tr denote the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. A linear code $\mathcal{C}_D$ of length n over $\mathbb{F}_p$ is defined by

$$\mathcal{C}_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) : x \in \mathbb{F}_q\}.$$

The set D is called the defining set of $\mathcal{C}_D$. Ding et al. [3] presented certain two-weight and three-weight codes by choosing defining set $D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x^2) = 0\}$. Many linear codes with good parameters can be obtained by choosing the defining set D properly. Most of them constructed the defining sets by a certain quadratic Bent function. Recently, Li et al. [4] studied the linear codes with the defining sets $D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x^2 + x) = 0\}$ rather than quadratic Bent function, they presented a class of three-weight and five-weight linear codes over $\mathbb{F}_p$ and obtained the detailed information on the weight distribution of the codes for all four subcases.

Motivated by the construction methods mentioned above and the idea of [4], we define linear codes $\mathcal{C}_{D_0}$ and $\mathcal{C}_{D_1}$ by

$$\mathcal{C}_{D_i} = \{\boldsymbol{c}_b = (\mathrm{Tr}(bx))_{x \in D_i} : b \in \mathbb{F}_q\}, \quad i \in \{0, 1\}, \tag{1}$$

* Corresponding author (email: y-j@tsinghua.edu.cn)

where

$$D_i = \{x \in \mathbb{F}_q : \mathrm{Tr}(x^2 + x) \in C_i^{(2,p)}\} = \{x_1, x_2, \ldots, x_{n_i}\}, \quad i \in \{0, 1\}, \tag{2}$$

where $C_0^{(2,p)}$ and $C_1^{(2,p)}$ denote the sets of all squares and non-squares in $\mathbb{F}_p^*$, respectively.

For such linear codes, we studied their weight distribution and proved that they just have three, four, five or six weights. In addition, each nonzero codeword of $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$ constructed in this study is minimal if $m \geqslant 5$, which indicates that such linear codes can be applied to secret sharing schemes [5] with nice access structures. The more information about the application is in [3].

We proposed a new method to calculate the weight distribution of the linear codes $\mathcal{C}_{D_i}$ ($i \in \{0, 1\}$), including Gauss sum, Gaussian period and two lemmas (see [6] Theorem 5.33 and [7] Theorem 6.3.1). In particular, it is the first time to calculate the weight distribution of linear codes by using the lemma in [7]. Therefore, we can calculate the weight distribution completely by using this method. Our approach has universal significance in the corresponding domain. Here we list the main results and omit the proof process for the space limitations.

Theorem 1. If m is even and $p \mid m$, then $\mathcal{C}_{D_i}$ ($i = 0, 1$) defined in (1) and (2) are at most four-weight linear codes with parameters $[\frac{p-1}{2}p^{m-1} - \frac{p-1}{2p}G, m]$, whose weight enumerator is

$$\begin{aligned} &1 + \left(\frac{p+1}{2}p^{m-2} + \frac{p-1}{2p}G - 1\right) z^{\frac{(p-1)^2}{2}p^{m-2}} \\ &+ \frac{(p-1)^2}{2}p^{m-2} z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-3}{2p}G} \\ &+ \frac{p^2-1}{2}p^{m-2} z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-1}{2p}G} \\ &+ \left(\frac{p-1}{2}p^{m-2} \right. \\ &\left. - \frac{p-1}{2p}G\right) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-1}{p}G}, \end{aligned} \tag{3}$$

where G denotes the quadratic Gauss sum over $\mathbb{F}_q$ for short and $G = -(-1)^{\frac{m(p-1)}{4}}p^{\frac{m}{2}}$.

Theorem 2. If m is even and $(\frac{-m}{p}) = (-1)^i$, where $(\frac{\cdot}{\cdot})$ is the Legendre symbol, then $\mathcal{C}_{D_i}$ ($i = 0, 1$) defined in (1) and (2) are at most five-weight linear codes with parameters $[\frac{p-1}{2}p^{m-1} + \frac{p+1}{2p}G, m]$, whose weight enumerator is

$$\begin{aligned} &1 + (p^{m-2} - 1) z^{\frac{(p-1)^2}{2}p^{m-2}} \\ &+ (p-1)p^{m-2} z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{1}{p}G} \\ &+ \left(\frac{p^2-1}{4}p^{m-2} - \frac{p^2-1}{4p}G\right) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p-1}{2p}G} \\ &+ \left(\frac{p^2-1}{2}p^{m-2} + \frac{p-1}{p}G\right) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p+1}{2p}G} \\ &+ \left(\frac{(p-1)(p-3)}{4}p^{m-2} \right. \\ &\left. + \frac{(p-1)(p-3)}{4p}G\right) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p+3}{2p}G}, \end{aligned} \tag{4}$$

where G denotes the quadratic Gauss sum over $\mathbb{F}_q$ for short and $G = -(-1)^{\frac{m(p-1)}{4}}p^{\frac{m}{2}}$.

Theorem 3. If m is even and $(\frac{-m}{p}) = (-1)^{1-i}$, where $(\frac{\cdot}{\cdot})$ is the Legendre symbol, then $\mathcal{C}_{D_i}$ ($i = 0, 1$) defined in (1) and (2) are at most four-weight linear code with parameters $[\frac{p-1}{2}p^{m-1} - \frac{p-1}{2p}G, m]$, whose weight enumerator is

$$\begin{aligned} &1 + (p^{m-1} - 1) z^{\frac{(p-1)^2}{2}p^{m-2}} + \left(\frac{(p-1)^2}{4}p^{m-2} \right. \\ &\left. + \frac{(p-1)^2}{4p}G\right) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-3}{2p}G} \\ &+ \frac{p^2-1}{2}p^{m-2} z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-1}{2p}G} \\ &+ \left(\frac{(p-1)^2}{4}p^{m-2} \right. \\ &\left. - \frac{(p-1)^2}{4p}G\right) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p+1}{2p}G}, \end{aligned} \tag{5}$$

where G denotes the quadratic Gauss sum over $\mathbb{F}_q$ for short and $G = -(-1)^{\frac{m(p-1)}{4}}p^{\frac{m}{2}}$.

Theorem 4. If m is odd and $p \mid m$, then $\mathcal{C}_{D_i}$ ($i = 0, 1$) defined in (1) and (2) are at most five-weight linear codes with parameters $[\frac{p-1}{2}p^{m-1} + \frac{p-1}{2p}H, m]$, whose weight enumerator is

$$\begin{aligned} &1 + (p^{m-2} - 1) z^{\frac{(p-1)^2}{2}p^{m-2}} \\ &+ \frac{(p-1)^2}{2}p^{m-2} z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p^2-2p-1}{2p^2}H} \\ &+ \left(\frac{p-1}{2}p^{m-1} - \frac{p-1}{2p}H\right) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{(p-1)^2}{2p^2}H} \\ &+ (p-1)p^{m-2} z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p-1}{2p}H} \\ &+ \left(\frac{p-1}{2}p^{m-2} + \frac{p-1}{2p}H\right) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p^2-1}{2p^2}H}, \end{aligned} \tag{6}$$

where $H = (-1)^i(\frac{-1}{p})GG_p = (-1)^{i+\frac{(m+3)(p-1)}{4}}p^{\frac{m+1}{2}}$, here $(\frac{\cdot}{\cdot})$ is the Legendre symbol, G and G_p denote the quadratic Gauss sum over $\mathbb{F}_q$ and $\mathbb{F}_p$ respectively and $GG_p = (-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m+1}{2}}$.

Theorem 5. If m is odd and $(\frac{m}{p}) = (-1)^i$, where $(\frac{\cdot}{\cdot})$ is the Legendre symbol, then $\mathcal{C}_{D_i}$ $(i = 0, 1)$ defined in (1) and (2) are at most six-weight linear codes with parameters $[\frac{p-1}{2}p^{m-1} - \frac{1}{p}H, m]$, whose weight enumerator is

$$\begin{aligned}
&1 + \left(p^{m-2} + \frac{p-1}{p^2}H - 1\right) z^{\frac{(p-1)^2}{2}p^{m-2}} \\
&+ \left(\frac{p^2-1}{4}p^{m-2} - \frac{p^2-1}{4p^2}H\right) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-1}{2p^2}H} \\
&+ \Bigg(\frac{(p-1)(p+3)}{4}p^{m-2} \\
&+ \frac{3(p-1)^2}{4p^2}H\Bigg) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p+1}{2p^2}H} \\
&+ \left((p-1)p^{m-2} - \frac{p-1}{p^2}H\right) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{1}{p}H} \\
&+ \Bigg(\frac{(p-1)^2}{4}p^{m-2} \\
&- \frac{(p-1)^2}{4p^2}H\Bigg) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{3p-1}{2p^2}H} \\
&+ \Bigg(\frac{(p-1)(p-3)}{4}p^{m-2} \\
&- \frac{(p-1)(p-3)}{4p^2}H\Bigg) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{3p+1}{2p^2}H}, \qquad (7)
\end{aligned}$$

where $H = (-1)^i(\frac{-1}{p})GG_p = (-1)^{i+\frac{(m+3)(p-1)}{4}}p^{\frac{m+1}{2}}$, here G and G_p denote the quadratic Gauss sum over $\mathbb{F}_q$ and $\mathbb{F}_p$ respectively and $GG_p = (-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m+1}{2}}$.

Theorem 6. If m is odd and $(\frac{m}{p}) = (-1)^{1-i}$, where $(\frac{\cdot}{\cdot})$ is the Legendre symbol, then $\mathcal{C}_{D_i}$ $(i = 0, 1)$ defined in (1) and (2) are five-weight linear codes with parameters $[\frac{p-1}{2}p^{m-1}, m]$, whose weight enumerator is

$$\begin{aligned}
&1 + \left(\frac{(p-1)^2}{4}p^{m-2} + \frac{(p-1)^2}{4p^2}H\right) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p+1}{2p^2}H} \\
&+ \Bigg(\frac{p^2-1}{4}p^{m-2} \\
&- \frac{(p-1)(3p-1)}{4p^2}H\Bigg) z^{\frac{(p-1)^2}{2}p^{m-2} - \frac{p-1}{2p^2}H} \\
&+ (p^{m-1} - 1) z^{\frac{(p-1)^2}{2}p^{m-2}} + \Bigg(\frac{p^2-1}{4}p^{m-2} \\
&+ \frac{p^2-1}{4p^2}H\Bigg) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p-1}{2p^2}H} \\
&+ \left(\frac{(p-1)^2}{4}p^{m-2} + \frac{(p-1)^2}{4p^2}H\right) z^{\frac{(p-1)^2}{2}p^{m-2} + \frac{p+1}{2p^2}H}, \qquad (8)
\end{aligned}$$

where $H = (-1)^i(\frac{-1}{p})GG_p = (-1)^{i+\frac{(m+3)(p-1)}{4}}p^{\frac{m+1}{2}}$, here G and G_p denote the quadratic Gauss sum over $\mathbb{F}_q$ and $\mathbb{F}_p$ respectively and $GG_p = (-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m+1}{2}}$.

Remark 1. In the above six theorems, there are some special cases, such as the case of $p = 3$, in which codes $\mathcal{C}_{D_i}$ may have less number of non-zero weights.

Remark 2. For all of the above theorems, we have been using software Magma for example verification. And some of the examples are optimal linear codes according to the codetables in [8].

To sum up, we present two classes of linear codes $\mathcal{C}_{D_i}$ $(i = 0, 1)$ by properly chosen defining sets with at most six weights. Moreover, such linear codes can be used to construct secret sharing schemes [9]. Let $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weight of a linear code $\mathcal{C}$. We recall that if

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p},$$

then all nonzero codewords of code $\mathcal{C}$ are minimal and the linear code $\mathcal{C}$ can be used to construct a secret sharing scheme with interesting access structures. It can be checked that for linear codes $\mathcal{C}_{D_i}$ for each $i \in \{0, 1\}$ defined in (1) and (2) with $m \geqslant 5$, we have

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}.$$

Therefore linear codes $\mathcal{C}_{D_i}$ $(i = 0, 1)$ defined in (1) and (2) with $m \geqslant 5$ can be employed to get secret sharing schemes.

Acknowledgements This work was partly supported by National Natural Science Foundation of China (Grant Nos. 11471178, 11571007).

References

1 MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977
2 Ding K, Ding C. Binary linear codes with three weights. IEEE Commun Lett, 2014, 18: 1879–1882
3 Ding K, Ding C. A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans Inform Theor, 2015, 61: 5835–5842
4 Li F, Wang Q, Lin D. A class of three-weight and five-weight linear codes. Discrete Appl Math, 2018, 241: 25–38
5 Carlet C, Ding C, Yuan J. Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans Inform Theor, 2005, 51: 2089–2102
6 Lidl R, Niederreiter H. Finite Fields. New York: Cambridge University Press, 1997
7 Berndt B C, Evans R J, Williams K S. Gauss and Jacobi Sums. New York: John Wiley & Sons Company, 1997
8 Grassl M. Bounds on the minimum distance of linear codes and quantum codes. 2007 http://www.codetables.de
9 Yuan J, Ding C S. Secret sharing schemes from three classes of linear codes. IEEE Trans Inform Theor, 2006, 52: 206–212