Weight Distributions and Weight Spectra of Two Classes of Low-Weight Binary Linear Codes

Authors: Li Fei, Li Fei

Date: 2023-02-18T00:00:00+00:00

Abstract

The construction of linear codes is an important research topic in coding and cryptography theory. The determination of weight distributions and weight spectra of codes also has fundamental theoretical significance in coding theory, and plays an important role in secure communications. This paper constructs a class of 3-weight and a class of 4-weight binary linear codes, and completely determines their weight distributions and weight spectra.

Full Text

Weight Distributions and Weight Hierarchies of Two Families of Binary Linear Codes with Few Weights

School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu 233030, Anhui, China

Abstract

Constructing linear codes with few weights is an important research topic in coding theory and cryptography. The weight distribution and weight hierarchy of codes are of fundamental theoretical significance in coding theory and play crucial roles in secret communications. This paper constructs a family of 3-weight and a family of 4-weight binary linear codes, and completely determines their weight distributions and weight hierarchies.

Keywords: linear code; weight distribution; weight hierarchy; generalized Hamming weight

1 Introduction and Main Results

In coding theory, the weight distribution of linear codes is a classical research topic. For a linear code C, if the number of distinct nonzero Hamming weights is t, we call C a t-weight code. When t is small, we refer to such codes as codes with few weights. Linear codes with few weights have important practical and theoretical applications in authentication codes [**?**], association schemes [**?**], secret sharing schemes [**?**], and strongly regular graphs [**?**].

In the 1970s, driven by cryptographic applications, the concept of generalized Hamming weights (GHW) was introduced [**?**, **?**]. Let $[C,r]_p$ denote the set of all r-dimensional subspaces of C over $\mathbb{F}_p$. For a subspace $V \in [C,r]_p$, define $\mathrm{Supp}(V) = \{i : 1 \le i \le n, c_i \neq 0 \text{ for some } \mathbf{c} = (c_1, c_2, \dots, c_n) \in V\}$.

Definition 1 Let C be an $[n,k,d]$ linear code over $\mathbb{F}_p$. For $1 \le r \le k$, define $d_r(C) = \min\{|\mathrm{Supp}(V)| : V \in [C,r]_p\}$. Then $d_r(C)$ is called the r-th generalized Hamming weight of C, and the sequence $\{d_r(C) : 1 \le r \le k\}$ is called the weight hierarchy of C.

Clearly, $d = d_1(C)$. The generalized Hamming weight can be viewed as a generalization of the minimum Hamming weight concept. When linear codes are used in type-II wire-tap channels connected to cryptographic systems, the weight hierarchy completely characterizes the code's operational mode. Moreover, weight hierarchies have important applications in the analysis of code trellis complexity [**?**, **?**, **?**]. In particular, since Wei' s classic paper [**?**] in 1991, interest in this area has grown significantly. In 1996, Chen Wende and Norwegian scholar T. Kløve collaborated to propose the finite projective geometry method for studying weight hierarchies, achieving fruitful results [**?**].

Much is known about the weight hierarchies of algebraic geometry codes, BCH codes, Reed-Muller codes, and cyclic codes [**?**, **?**, **?**, **?**, **?**, **?**]. Recently, new results on weight hierarchies of linear codes have emerged [**?**, **?**, **?**].

Professor Ding Cunsheng from Hong Kong University of Science and Technology et al. provided a general method for constructing linear codes [**?**]: Let Tr denote the trace function from $\mathbb{F}_{p^s}$ to $\mathbb{F}_p$, and let $D = \{d_1, d_2, \dots, d_n\}$ be a subset of $\mathbb{F}_{p^s}^*$. A linear code of length n is defined as $C_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \dots, \mathrm{Tr}(xd_n)) : x \in \mathbb{F}_{p^s}^*\}$. Here D is called the defining set. By applying this method and selecting appropriate defining sets, several linear codes with few weights have been constructed [**?**, **?**].

In this paper, we make the following assumptions: Let ρ be a prime such that 2 is a primitive root modulo ρ^m. Let ϕ denote Euler' s totient function, so $\phi(\rho^m) = \rho^{m-1}(\rho - 1)$. We fix $p = 2$ and $q = 2^{\phi(\rho^m)}$. The defining set $D = \{d_1, d_2, \dots, d_n\}$ for our code construction is chosen as follows: For $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, let $D = D(a,b) = \{(x,y) \in \mathbb{F}_q^2 \setminus \{(0,0)\} : \mathrm{Tr}(ax^\rho + by) = 1\}$.

Thus, the linear code $C_D(a,b)$ is constructed as:

$$C_D(a,b) = \{(\mathrm{Tr}(\mathbf{x} \cdot d_1), \mathrm{Tr}(\mathbf{x} \cdot d_2), \dots, \mathrm{Tr}(\mathbf{x} \cdot d_n)) : \mathbf{x} \in \mathbb{F}_q^2\}.$$

Using methods from [**?**], we construct two new families of binary linear codes with few weights and determine their weight distributions and weight hierarchies. Our main results are Theorems 2-5:

Theorem 2 Let $a \in \mathbb{F}_q^*$. The linear code $C_D(a,0)$ defined by (3) is a binary code with parameters $[n, 2\phi(\rho^m), d]$. Its weight distribution is given in Table 1 .

Theorem 3 Let $a, b \in \mathbb{F}_q^*$. The linear code $C_D(a,b)$ defined by (3) is a binary code with parameters $[n, 2\phi(\rho^m)]$. Its weight distribution is given in Table 2 .

Theorem 4 Let $a \in \mathbb{F}_q^*$. The linear code $C_D(a,0)$ defined by (3) has weight hierarchy as follows: [The specific formula would appear here based on the garbled text, but it's too corrupted to reconstruct accurately without the original context.]

Theorem 5 Let $a, b \in \mathbb{F}_q^*$. The linear code $C_D(a,b)$ defined by (3) has weight hierarchy as follows: [Similarly, the formula is corrupted in the original.]

---

2 Preliminaries

2.1 A Computational Formula

For the linear code C_D defined in (2), [**?**] provides a formula for computing generalized Hamming weights. Let $\mathrm{wt}(\mathbf{x})$ denote the Hamming weight of vector $\mathbf{x}$. For $a \in \mathbb{F}_q^*$, define $S(a) = \sum_{y \in \mathbb{F}_q} \chi(by)$, where χ is the canonical additive character of $\mathbb{F}_q$.

Lemma 1 ([27], Proposition 1) For C_D with dimension es, we have $d_r(C_D) = n - \max\{|D \cap H| : H \in \mathcal{H}_r\}$, where $\mathcal{H}_r$ is the set of all $\mathbb{F}_2$-subspaces of $\mathbb{F}_q$ of codimension r.

2.2 An Exponential Sum

Recall our earlier setting where $q = 2^{\phi(\rho^m)}$. Let γ be a fixed primitive element of $\mathbb{F}_q^*$, and let χ be the canonical additive character of $\mathbb{F}_q$. For more information on additive characters over finite fields, readers may refer to [**?**].

For $a, b \in \mathbb{F}_q$, define two exponential sums:

$$S_1(a) = \sum_{x \in \mathbb{F}_q} \chi(ax^\rho), \quad S_2(b) = \sum_{y \in \mathbb{F}_q} \chi(by).$$

Lemma 2 ([29], Theorem 1) Let $a \in \mathbb{F}_q^*$. Then $S_1(a)$ takes values in $\{0, \pm 2^{\phi(\rho^m)/2}\}$.

Lemma 3 ([29], Theorem 3) As a runs through all values in $\mathbb{F}_q^*$, the set of values of $S_1(a)$ is $\{0, \pm 2^{\phi(\rho^m)/2}\}$.

Lemma 4 ([20], Lemma 4) Let $b \neq 0$. Then $S_2(b) = 0$.

Lemma 5 ([27], Corollary 1) For any $a \in \mathbb{F}_q^*$, the Hamming weight of codewords in $C_D(a, 0)$ is given by $\mathrm{wt}(\mathbf{c}) = \frac{1}{2}(n - S_1(a))$.

---

3 Proofs of Main Theorems

3.1 Proofs of Theorems 2 and 3

We first compute the length n of the linear code $C_D(a, b)$.

Lemma 6 For any $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, we have $n = |D(a, b)| = 2^{2\phi(\rho^m)-1} - 2^{\phi(\rho^m)-1} S_1(a) S_2(b)$.

Proof. Using the orthogonal property of additive characters, we have:

$$|D(a,b)| = \sum_{(x,y)\neq(0,0)} \frac{1}{2} \sum_{c\in\mathbb{F}2} \chi(c(\mathrm{Tr}(ax^\rho + by) - 1)).$$

The result follows by direct computation.

Lemma 7 Let $a \in \mathbb{F}_q^*$. Then: 1. If $S_1(a) = 0$, then $\mathrm{wt}(\mathbf{c}) = 2^{\phi(\rho^m)-1}(2^{\phi(\rho^m)} - 1)$ for all nonzero codewords $\mathbf{c} \in C_D(a, 0)$. 2. If $S_1(a) = \pm 2^{\phi(\rho^m)/2}$, then the codewords have two possible weights: $2^{\phi(\rho^m)-1}(2^{\phi(\rho^m)} - 1) \pm 2^{\phi(\rho^m)/2-1}$.

Proof. This follows from Lemma 5 and Lemma 6.

Proof of Theorem 2. For $b = 0$, by Lemma 7, the mapping $\mathbf{x} \mapsto \mathbf{c}$ is a linear isomorphism, so the dimension of $C_D(a, 0)$ is $2\phi(\rho^m)$. The weight distribution follows from Lemma 7 and Lemma 5, yielding Table 1 .

Proof of Theorem 3. For $b \neq 0$, by Lemma 4 we have $S_2(b) = 0$, so $n = 2^{2\phi(\rho^m)-1}$. The dimension remains $2\phi(\rho^m)$. Lemma 7 gives four possible weight values, and counting codewords with each weight using Lemma 5 yields Table 2 .

3.2 Proofs of Theorems 4 and 5

Let $\{\beta_1, \beta_2, \ldots, \beta_{\phi(\rho^m)}\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. For $u \in \mathbb{F}_q$, let $\pi(u)$ be the coordinate vector of u with respect to this basis.

Lemma 8 Let H_r be an r-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_q$. Then:

$$|D(a,b) \cap H_r| = \begin{cases} 2^{r-1} - 2^{(r+\phi(\rho^m))/2-1} S_1(a) & \text{if } S_1(a) \neq 0, \\ 2^{r-1} & \text{if } S_1(a) = 0. \end{cases}$$

Proof. By the orthogonal property of additive characters and Lemma 4, we have:

$$|D(a,b) \cap H_r| = \sum_{x\in H_r\setminus\{0\}} \frac{1}{2} \sum_{c\in\mathbb{F}2} \chi(c\,\mathrm{Tr}(ax^\rho)).$$

The result follows from Lemma 2 and properties of exponential sums.

Proof of Theorem 4. For $C_D(a,0)$, we consider two cases based on $S_1(a)$. When $S_1(a) = 0$, Lemma 8 shows that $|D(a,0) \cap H_r| = 2^{r-1}$ for any r-dimensional subspace H_r. By Lemma 1, this gives $d_r(C_D(a,0)) = n - 2^{r-1}$. When $S_1(a) \neq 0$, the maximum intersection size is $2^{r-1} + 2^{(r+\phi(\rho^m))/2-1}$, yielding $d_r(C_D(a,0)) = n - 2^{r-1} - 2^{(r+\phi(\rho^m))/2-1}$.

Proof of Theorem 5. For $C_D(a,b)$ with $b \neq 0$, Lemma 4 ensures $S_2(b) = 0$. The analysis proceeds similarly to Theorem 4, but with $n = 2^{2\phi(\rho^m)-1}$. The weight hierarchy is determined by applying Lemma 8 to compute $\max |D(a,b) \cap H_r|$ and using Lemma 1.

---

4 Conclusion

Constructing linear codes and determining their parameters is a fundamental problem in algebraic coding theory. In recent years, the defining-set method has yielded many new linear codes [**?**, **?**, **?**, **?**, **?**, **?**, **?**, **?**]. By generalizing this method, we have constructed two families of binary linear codes and determined their weight distributions and weight hierarchies through exponential sum theory. The results show one family is 3-weight and the other is 4-weight. For linear codes, determining the weight hierarchy is generally difficult. We have completely determined the weight hierarchies of these two families by combining a combinatorial formula with exponential sum techniques.

References

[1] M. Bras-Amorós, K. Lee, and A. Vico-Oton. New lower bounds on the generalized Hamming weights of AG codes. *IEEE Trans. Inf. Theory*, 2014, 60(10): 5930-5937.

[2] Y. Guan, M. Shi, X. Zhang, and W. Wu. Two new families of two-weight codes over finite fields. *Acta Electronica Sinica*, 2019, 47(3): 714-718.

[3] P. Beelen. A note on the generalized Hamming weights of Reed-Muller codes. *Appl. Algebr. Eng. Comm.*, 2019, 30: 233-242.

[4] J. Cheng and C. Chao. On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two. *IEEE Trans. Inf. Theory*, 1997, 43(1): 294-298.

[5] W. Chen and Z. Liu. *Weight Hierarchy of Codes • Finite Projective Geometric Approach.* Hefei: USTC Press, 2012.

[6] A. R. Calderbank and J. M. Goethals. Three-weight codes and association schemes. *Philips J. Res.*, 1984, 39: 143-152.

[7] A. R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. Lond. Math. Soc.*, 1986, 18: 97-122.

[8] C. Ding. Linear codes from some 2-designs. *IEEE Trans. Inf. Theory*, 2015, 61(6): 3265-3275.

[9] K. Ding and C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Trans. Inf. Theory*, 2015, 61(11): 5835-5842.

[10] K. Ding and C. Ding. Binary linear codes with three weights. *IEEE Commun. Letters*, 2014, 18(11): 1879-1883.

[11] C. Ding, T. Helleseth, T. Kløve, and X. Wang. A generic construction of Cartesian authentication codes. *IEEE Trans. Inf. Theory*, 2007, 53(6): 2229-2235.

[12] C. Ding, C. Li, N. Li, and Z. Zhou. Three-weight cyclic codes and their weight distributions. *Discrete Math.*, 2016, 339(2): 415-427.

[13] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n = (2^r - 1)/N$. *Discrete Math.*, 1977, 18(2): 179-211.

[14] T. Helleseth, T. Kløve, and O. Ytrehus. Generalized Hamming weights of linear codes. *IEEE Trans. Inf. Theory*, 1992, 38(3): 1133-1140.

[15] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inf. Theory*, 1998, 44(1): 181-196.

[16] G. Jian, C. Lin, and R. Feng. Two-weight and three-weight linear codes based on Weil sums. *Finite Fields Th. App.*, 2019, 57: 92-107.

[17] H. Janwa and A. K. Lal. On the generalized Hamming weights of cyclic codes. *IEEE Trans. Inf. Theory*, 1997, 43(1): 299-308.

[18] T. Kløve. The weight distribution of linear codes over $GF(q)$ having generator matrix over $GF(q)$. *Discrete Math.*, 1978, 23(2): 159-168.

[19] X. Kong and S. Yang. Complete weight enumerators of a class of linear codes with two or three weights. *Discrete Math.*, 2019, 342(11): 3166-3176.

[20] Y. W. Liu and Z. H. Liu. On some classes of codes with a few weights. *Adv. Math. Commun.*, 2018, 12(2): 215-229.

[21] H. Liu and Q. Liao. Several classes of linear codes with a few weights from defining sets over $\mathbb{F}_p + u\mathbb{F}_p$. *Des. Codes Cryptogr.*, 2017, 87(1): 15-29.

[22] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, New York, 1997.

[23] C. Li, S. Bae, and S. Yang. Some results on two-weight and three-weight linear codes. *Adv. Math. Commun.*, 2019, 13(1): 195-211.

[24] C. Li, Q. Yue, and F. Fu. A construction of several classes of two-weight and three-weight linear codes. *Appl. Algebr. Eng. Comm.*, 2018, 28(1): 1-20.

[25] F. Li. A class of cyclotomic linear codes and their generalized Hamming weights. *Appl. Algebr. Eng. Comm.*, 2018, 29: 501-511.

[26] F. Li. Weight hierarchy of a class of linear codes relating to non-degenerate quadratic forms. *IEEE Trans. Inf. Theory*, 2020, 67(1): 124-129.

[27] F. Li and X. Li. Weight distributions and weight hierarchies of two classes of binary linear codes. *Finite Fields Th. App.*, 2021, 73: 101865.

[28] Z. Liu and J. Wang. Notes on generalized Hamming weights of some classes of binary codes. *Cryptogr. Commun.*, 2019, 12: 645-657.

[29] M. Moisio. Explicit evaluation of some exponential sums. *Finite Fields Th. App.*, 2009, 15(6): 644-651.

[30] M. Shi, Y. Guan, and P. Solé. Two new families of two-weight codes. *IEEE Trans. Inf. Theory*, 2017, 63(10): 6240-6246.

[31] M. Shi, Y. Liu, and P. Solé. Optimal two weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Communications Letters*, 2016, 20(12): 2346-2349.

[32] M. Shi, R. Wu, Y. Liu, and P. Solé. Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$. *Cryptogr. Commun.*, 2017, 9(5): 637-646.

[33] M. Shi, Y. Liu, and P. Solé. Optimal two weight codes from trace codes over a non-chain ring. *Discrete Appl. Math.*, 2017, 219: 176-181.

[34] M. Shi, R. Wu, L. Qian, S. Lin, and P. Solé. New classes of p-ary few weights codes. *B. Malays. Math. Sci. So.*, 2019, 42(4): 1393-1412.

[35] C. Tang, C. Xiang, and K. Feng. Linear codes with few weights from inhomogeneous quadratic functions. *Des. Codes Cryptogr.*, 2017, 83(3): 691-714.

[36] M. A. Tsfasman and S. G. Vlădut. Geometric approach to higher weights. *IEEE Trans. Inf. Theory*, 1995, 41(6): 1564-1573.

[37] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory*, 1991, 37(5): 1412-1418.

[38] M. Xiong, S. Li, and G. Ge. The weight hierarchy of some reducible cyclic codes. *IEEE Trans. Inf. Theory*, 2016, 62(7): 4071-4080.

[39] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inf. Theory*, 2006, 52(1): 206-212.

[40] M. Yang, J. Li, K. Feng, and D. Lin. Generalized Hamming weights of irreducible cyclic codes. *IEEE Trans. Inf. Theory*, 2015, 61(9): 4905-4913.

[41] S. Yang, Z. A. Yao, and C. A. Zhao. The weight distributions of two classes of p-ary cyclic codes with few weights. *Finite Fields Th. App.*, 2017, 44: 76-91.

[42] Z. Zhou, N. Li, C. Fan, and T. Helleseth. Linear codes with two or three weights from quadratic bent functions. *Des. Codes Cryptogr.*, 2016, 81(2): 283-295.

Note: Figure translations are in progress. See original paper for figures.