Optimum Distance Profiles of Linear Block Codes

A. J. Han Vinck, *IEEE Fellow*
Institute for Experimental Mathematics
Duisburg-Essen University
Ellernstr. 29, 45326 Essen, Germany
Email: vinck@iem.uni-due.de

Yuan Luo
Computer Science & Engineering Department
Shanghai Jiao Tong University
Shanghai 200240, China
Email: yuanluo@sjtu.edu.cn

***Abstract*— In this paper, two kinds of optimum distance profiles of linear block codes are introduced to study how to include or exclude some basis codewords one by one while keeping the minimum distances (of the generated subcodes) as large as possible. One application is to serve a suitable code for the realization of the transport format combination indicators (TFCI) of some CDMA systems.**

I. Introduction

The transport format combination indicators (TFCI) are widely used in CDMA systems, see [3][8], where some input TFCI bits are used to combine some basis codewords. When the number of the input TFCI bits increases or decreases, some basis codewords will be included or excluded, respectively. In this paper, we consider how to include or exclude the basis codewords of linear block codes one by one while keeping the minimum distances (of the generated subcodes) as large as possible.

Corresponding properties are investigated by introducing two kinds of optimum distance profiles of linear block codes in Section II. Then we provide some optimum distance profiles and related generator matrices in Section III, Section IV and Section V, which are about the generalized Reed-Solomon codes, the (binary, ternary and extended) Golay codes and some codes from the Hadamard matrices, respectively. The results on the generalized Reed-Solomon codes and the Hadamard matrices, are straightforward. But the optimum distance profiles of the Golay codes are not obvious, where the proofs are omitted because of the limitation of space.

Final conclusions are presented in Section VI including some preliminary ideas for the BCH codes.

II. Preliminary

Let C be an $[n,k]$ linear code over $GF(q)$ and denote $C_0 = C$. A sequence of linear subcodes

$$C_0 \supset C_1 \supset \cdots \supset C_{k-1} \tag{1}$$

is called a **subcode chain**, where $\dim[C_i] = k-i$. The increasing sequence

$$d[C_0] \leq d[C_1] \leq \cdots \leq d[C_{k-1}] \tag{2}$$

is called a **distance profile of the linear block code** C, where $d[C_i]$ is the minimum Hamming distance of the subcode C_i. For a given $[n,k]$ code C over $GF(q)$, the number of its subcode chains is

$$\prod_{t=2}^{k} Q[t,t-1] = \prod_{t=2}^{k} \frac{q^t-1}{q-1},$$

where $Q[t,r]$ is the $q-ary$ Gaussian binomial coefficient

$$\prod_{j=0}^{r-1} \frac{q^{t-j}-1}{q^{r-j}-1}.$$

We study the chains having the optimum distance profiles defined in the following paragraphs, and try to find a generator matrix G such that its first $k-i$ rows generate C_i.

For any two integer sequences of length k, $a_0,\ldots,a_{k-1}$ and $b_0,\ldots,b_{k-1}$, we say that $a_0,\ldots,a_{k-1}$ is an upper bound on $b_0,\ldots,b_{k-1}$ in the dictionary order if there is an integer t such that

$$\begin{aligned} a_i &= b_i \quad \text{for } 0 \leq i \leq t-1, \\ a_t &> b_t. \end{aligned}$$

We say that $a_0,\ldots,a_{k-1}$ is an upper bound on $b_0,\ldots,b_{k-1}$ in a inverse dictionary order if there is an integer t such that

$$\begin{aligned} a_i &= b_i \quad \text{for } k-1 \geq i \geq t+1, \\ a_t &> b_t. \end{aligned}$$

A distance profile of the linear block code C is called the **optimum distance profile in the dictionary order** ($ODPB[C]^{dic}$), which is denoted by a sequence

$$ODPB[C]^{dic}_0, ODPB[C]^{dic}_1, \cdots, ODPB[C]^{dic}_{k-1}, \tag{3}$$

if it is an upper bound on any other distance profile in the dictionary order. A definition of the **optimum distance profile in the inverse dictionary order** ($ODPB[C]^{inv}$), which is denoted by a sequence

$$ODPB[C]^{inv}_0, ODPB[C]^{inv}_1, \cdots, ODPB[C]^{inv}_{k-1}, \tag{4}$$

follows from similar arguments of (3) but in the inverse dictionary order.

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

It is easy to verify that $ODPB[C]_0^{dic} = ODPB[C]_0^{inv} = d_{min}$ and $ODPB[C]_{k-1}^{inv} = d_{max}$, where d_{min} is the minimum distance of C and d_{max} is the maximum weight of nonzero codewords.

The existence and uniqueness of the two kinds of optimum distance profiles of a linear block code, are obvious since any two distance profiles can compare with each other in the corresponding order.

Given a distance profile $d[C_0], d[C_1]$, ..., $d[C_{k-1}]$, there is a generator matrix G (not unique) of the code C such that its first $k-i$ rows generate the subcode C_i. This matrix G is called a **generator matrix with respect to the distance profile**. In this paper, we consider the **generator matrices with respect to the two kinds of optimum distance profiles** $ODPB^{dic}$ and $ODPB^{inv}$, respectively.

The structures of the generator matrices with respect to $ODPB^{dic}$ and $ODPB^{inv}$ respectively, imply how to exclude (from the last row of the matrix) and include (from the first row of the matrix) the basis codewords one by one, while keeping the minimum distance of the generated code as large as possible. These structures can be used for encoding a transport format combination indicator (TFCI) in some CDMA systems (see [8], pp.189), when the number of input TFCI bits are decreasing or increasing, respectively.

One example is about the Hamming code, see follows. More examples are presented in the following sections.

Let C be a binary $[7, 4, 3]$ Hamming code. Its weight enumerator $1 + 7z^3 + 7z^4 + z^7$ implies that all possible minimum distances of any subcode are 3, 4 or 7. We have $ODPB[C]_0^{dic} = 3$ and

$$ODPB[C]_1^{dic} = ODPB[C]_2^{dic} = ODPB[C]_3^{dic} = 4$$

since all even weight codewords generate a $[7, 3, 4]$ subcode and any $[7, 3, 4]$ subcode does not include the codeword (1111111). One generator matrix with respect to the $ODPB[C]^{dic}$ is:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Furthermore, it is easy to verify that $ODPB[C]_3^{inv} = 7$ and

$$ODPB[C]_2^{inv} = ODPB[C]_1^{inv} = ODPB[C]_0^{inv} = 3.$$

One generator matrix with respect to the $ODPB[C]^{inv}$ is:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

In addition, two linear codes are said to be equivalent (monomially equivalent) if they are the same up to:

- a uniform permutation of coordinate indices,
- a multiplication of the ith entry in each codeword by a nonzero constant α_i for each i.

For equivalent linear block codes, the properties about the Hamming weight, the Hamming distance and the distance profile, are the same.

III. The Optimum Distance Profiles of the Generalized Reed-Solomon Codes

Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $v = (v_1, v_2, \ldots, v_n)$ be two vectors over $GF(q)$, where $\alpha_i (1 \leq i \leq n)$ are distinct and $v_i \neq 0$. A generalized Reed-Solomon code $GRS_{n,k}(\alpha, v)$ with length $n \leq q$ and dimension $k \leq n$, is a set of vectors

$$\begin{aligned} \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) : \\ f(x) \in F_q[x], \deg f \leq k-1\}, \end{aligned} \tag{5}$$

see [6]. If $n = q - 1$, $v_i = 1$ and $\alpha_i = \gamma^i$ for $1 \leq i \leq n$, where γ is a primitive element of $GF(q)$, then the definition (5) is of a Reed-Solomon code.

It is known that $GRS_{n,k}(\alpha, v)$ is an $[n, k, n-k+1]$ maximum distance separable (MDS) code, and $GRS_{n,k-1}(\alpha, v)$ is a subcode of $GRS_{n,k}(\alpha, v)$. Then, by using the Singleton bound and the Vandermonde matrix, its optimum distance profiles $ODPB^{dic}$ and $ODPB^{inv}$ follow.

Proposition 1: For an $[n, k]$ generalized Reed-Solomon code, its optimum distance profiles $ODPB^{dic}$ and $ODPB^{inv}$, are both equal to

$$n-k+1, n-k+2, \ldots, n.$$

Furthermore, one generator matrix with respect to the profile is

$$\begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \ldots & v_n\alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{pmatrix},$$

where the arguments are from (5).

IV. The Optimum Distance Profiles of Some Codes from the Hadamard Matrices

The Hadamard matrix H_n considered in this section is a normalized Sylvester-type Hadamard matrix where $n = 2^k$. By replacing $+1$ and -1 with 0 and 1 respectively, H_n is changed into a binary Hadamard matrix A_n. The following codes are related to the matrix A_n, see [6].

- Type I: The rows of A_n with the first column deleted, form a $[2^k - 1, k, 2^{k-1}]$ simplex code, i.e. the dual of the binary Hamming code, which is equidistant.
- Type II: The codewords of the type I code and their complements form a $[2^k - 1, k+1, 2^{k-1} - 1]$ punctured Reed-Muller code with weight enumerator $1 + (2^k - 1)z^{2^{k-1}-1} + (2^k - 1)z^{2^{k-1}} + z^{2^k - 1}$.
- Type III: The rows of A_n and their complements form a $[2^k, k+1, 2^{k-1}]$ first order Reed-Muller code $RM(1, k)$ with weight enumerator $1 + (2^{k+1} - 2)z^{2^{k-1}} + z^{2^k}$.

By using the arguments of the three linear codes, it is easy to get the following optimum distant profiles.

Proposition 2: For the code of type I, its optimum distance profiles $ODPB^{dic}$ and $ODPB^{inv}$, are both equal to a sequence with length k: $2^{k-1}, \ldots, 2^{k-1}$. Any generator matrix is with respect to the profile.

For the code of type II, its optimum distance profile $ODPB^{dic}$ or $ODPB^{inv}$, is $2^{k-1}-1, 2^{k-1}, \ldots, 2^{k-1}$ or $2^{k-1}-1, \ldots, 2^{k-1}-1, 2^{k}-1$, respectively. One generator matrix with respect to $ODPB^{dic}$ or $ODPB^{inv}$, can be obatined by appending a row of weight 2^k-1 to the end or the start of any generator matrix of type I, respectively.

For the code of type III, its optimum distance profiles $ODPB^{dic}$ and $ODPB^{inv}$, are both equal to $2^{k-1}, \ldots, 2^{k-1}, 2^{k}$. The generator matrix with respect to the profile is any generator matrix such that the first row is of weight 2^k.

V. The Optimum Distance Profiles of the Golay Codes

The results of this section are obtained by using the weight enumerators and some tables on the maximum minimal distances of linear block codes [1][5].

A. $\mathcal{G}_{24}$

Let $\mathcal{G}_{24}$ be a $[24,12,8]$ extended binary Golay code given by the Turyn construction ([6], p. 588). Its optimum distance profiles follow from the unique $[24,5,12]$ subcode [4][9] which has a generator

$$\begin{pmatrix} 00000000 & 11111111 & 11111111 \\ 11111111 & 00000000 & 11111111 \\ 10100110 & 10100110 & 10100110 \\ 01001110 & 01001110 & 01001110 \\ 00111010 & 00111010 & 00111010 \end{pmatrix}. \qquad (6)$$

Proposition 3: The optimum distance profile $ODPB[\mathcal{G}_{24}]^{dic}$ is

$$\begin{aligned} ODPB[\mathcal{G}_{24}]_i^{dic} &= 8 \quad \text{for } 0 \le i \le 6, \\ ODPB[\mathcal{G}_{24}]_i^{dic} &= 12 \quad \text{for } 7 \le i \le 9, \\ ODPB[\mathcal{G}_{24}]_i^{dic} &= 16 \quad \text{for } i = 10, 11. \end{aligned}$$

A generator matrix with respect to the $ODPB[\mathcal{G}_{24}]^{dic}$ is:

- its first five rows are the rows of (6),
- its 6th row is (00011011 00000000 00011011),
- its last six rows can be constructed easily.

The optimum distance profile $ODPB[\mathcal{G}_{24}]^{inv}$ is

$$\begin{aligned} ODPB[\mathcal{G}_{24}]_i^{inv} &= 8 \quad \text{for } 0 \le i \le 7, \\ ODPB[\mathcal{G}_{24}]_i^{inv} &= 12 \quad \text{for } 8 \le i \le 10, \\ ODPB[\mathcal{G}_{24}]_i^{inv} &= 24 \quad \text{for } i = 11. \end{aligned}$$

A generator matrix with respect to the $ODPB[\mathcal{G}_{24}]^{inv}$ follows where

- its first five rows are

$$\begin{pmatrix} 11111111 & 11111111 & 11111111 \\ 10100110 & 10100110 & 10100110 \\ 01001110 & 01001110 & 01001110 \\ 00111010 & 00111010 & 00111010 \\ 00011011 & 00000000 & 00011011 \end{pmatrix},$$

- its last seven rows can be constructed easily.

B. $\mathcal{G}_{23}$

Deleting one column of $\mathcal{G}_{24}$, we have a $[23,12,7]$ binary Golay code $\mathcal{G}_{23}$.

Proposition 4: The optimum distance profile $ODPB[\mathcal{G}_{23}]^{dic}$ is

$$\begin{aligned} ODPB[\mathcal{G}_{23}]_0^{dic} &= 7, \\ ODPB[\mathcal{G}_{23}]_i^{dic} &= 8 \quad \text{for } 1 \le i \le 7, \\ ODPB[\mathcal{G}_{23}]_i^{dic} &= 12 \quad \text{for } 8 \le i \le 10, \\ ODPB[\mathcal{G}_{23}]_{11}^{dic} &= 16. \end{aligned}$$

A generator matrix with respect to the $ODPB[\mathcal{G}_{23}]^{dic}$ follows where

- its first four rows are from (6) but delete one row and one column

$$\begin{pmatrix} 11111111 & 0000000 & 11111111 \\ 10100110 & 1010011 & 10100110 \\ 01001110 & 0100111 & 01001110 \\ 00111010 & 0011101 & 00111010 \end{pmatrix}. \qquad (7)$$

- its 5th row is (00011011 0000000 00011011).
- its last seven rows can be generated easily.

C. $\mathcal{G}_{12}$

Let $\mathcal{G}_{12}$ be a $[12,6,6]$ extended ternary Golay code given by the generator ([6], pp.489, not full rank)

$$\begin{pmatrix} & 0 \\ \bar{G} & \vdots \\ & 0 \\ 11111111111 & 1 \end{pmatrix}_{12\times12}, \qquad (8)$$

where

$$\bar{G} = \begin{pmatrix} 10100011101 \\ 11010001110 \\ 01101000111 \\ 10110100011 \\ 11011010001 \\ 11101101000 \\ 01110110100 \\ 00111011010 \\ 00011101101 \\ 10001110110 \\ 01000111011 \end{pmatrix}_{11\times11}.$$

Proposition 5: The optimum distance profile $ODPB[\mathcal{G}_{12}]^{dic}$ is

$$\begin{aligned} ODPB[\mathcal{G}_{12}]_i^{dic} &= 6 \quad \text{for } 0 \le i \le 3, \\ ODPB[\mathcal{G}_{12}]_i^{dic} &= 9 \quad \text{for } 4 \le i \le 5. \end{aligned}$$

By using the construction (8), a generator matrix with respect to the $ODPB[\mathcal{G}_{12}]^{dic}$ is obtained, where

- its first three rows are

$$\begin{pmatrix} 111002012112 \\ 110120222220 \\ 101000111010 \end{pmatrix},$$

- its last three rows can be generated easily.

The optimum distance profile $ODPB[\mathcal{G}_{12}]^{inv}$ is

$$\begin{array}{rcl} ODPB[\mathcal{G}_{12}]_i^{inv} & = & 6 \quad \text{for } 0 \leq i \leq 4, \\ ODPB[\mathcal{G}_{12}]_i^{inv} & = & 12 \quad \text{for } i = 5. \end{array}$$

A generator matrix with respect to the $ODPB[\mathcal{G}_{12}]^{inv}$ follows where

- its first two rows are

$$\left(\begin{array}{c} 111111111111 \\ 110120222220 \end{array} \right),$$

- its last four rows can be generated easily.

D. $\mathcal{G}_{11}$

Let $\mathcal{G}_{11}$ be a $[11, 6, 5]$ ternary Golay code with generator ([6], pp.489, not full rank)

$$\left(\begin{array}{c} \bar{G} \\ 11111111111 \end{array} \right), \tag{9}$$

where $\bar{G}$ is in (8). By using some properties provided in [2][7][10], the optimum distance profiles $ODPB[\mathcal{G}_{11}]^{dic}$ and $ODPB[\mathcal{G}_{11}]^{inv}$, are obtained in Proposition 6.

Proposition 6: The optimum distance profile $ODPB[\mathcal{G}_{11}]^{dic}$ is

$$\begin{array}{rcl} ODPB[\mathcal{G}_{11}]_0^{dic} & = & 5, \\ ODPB[\mathcal{G}_{11}]_i^{dic} & = & 6 \quad \text{for } 1 \leq i \leq 4, \\ ODPB[\mathcal{G}_{11}]_5^{dic} & = & 9. \end{array}$$

For the construction (9), a generator matrix with respect to the $ODPB[\mathcal{G}_{11}]^{dic}$ is

$$\left(\begin{array}{c} 11012022222 \\ 01110110100 \\ 00111011010 \\ 00011101101 \\ 01101000111 \\ 11111111111 \end{array} \right).$$

The optimum distance profile $ODPB[\mathcal{G}_{11}]^{inv}$ is

$$\begin{array}{rcl} ODPB[\mathcal{G}_{11}]_i^{inv} & = & 5 \quad \text{for } 0 \leq i \leq 2, \\ ODPB[\mathcal{G}_{11}]_i^{inv} & = & 6 \quad \text{for } 3 \leq i \leq 4, \\ ODPB[\mathcal{G}_{11}]_5^{inv} & = & 11. \end{array}$$

For the construction (9), a generator matrix with respect to the $ODPB[\mathcal{G}_{11}]^{inv}$ is

$$\left(\begin{array}{c} 12212111222 \\ 01002102120 \\ 01000111011 \\ 11012022222 \\ 00111011010 \\ 00011101101 \end{array} \right).$$

VI. Conclusions

In this paper, we investigate two kinds of optimum distance profiles of some linear block codes, which include the generalized Reed-Solomon codes, the (binary, ternary and extended) Golay codes and some codes from the Hadamard matrices.

Corresponding problems about the BCH codes are more difficult because their subcodes may be not BCH and cyclic, and the minimum distances of the subcodes can not be determined easily. But by using the constructions of the parity check matrices and the generator polynomials, some lower bounds on the two optimum distance profiles can be obtained.

For example, let α be a primitive element of the field $GF(2^4) = F_2[x]_{1+x+x^4}$ such that $1+\alpha+\alpha^4 = 0$. The minimal polynomial of α, α^2 α^4 and α^8 is

$$m_1(x) = 1 + x + x^4.$$

The minimal polynomial of α^3, α^6, α^{12} and α^9 is

$$m_3(x) = 1 + x + x^2 + x^3 + x^4.$$

The minimal polynomial of α^5 and α^{10} is

$$m_5(x) = 1 + x + x^2.$$

The minimal polynomial of α^7, α^{14}, α^{13} and α^{11} is

$$m_7(x) = 1 + x^3 + x^4.$$

Let $C = C_0$ be the BCH code with length 15, designed distance 2 and generator polynomial $m_1(x)$. It is easy to see that C_0 is also a $[15, 11, 3]$ binary Hamming code. We have a subcode chain

$$C_0 \supset C_1 \supset \cdots \supset C_{10},$$

where C_4 is a BCH code with generator polynomial $m_1(x)m_3(x)$, C_6 is a BCH code with generator polynomial $m_1(x)m_3(x)m_5(x)$, C_{10} is a BCH code with generator polynomial $m_1(x)m_3(x)m_5(x)m_7(x)$. The corresponding distance profile is

$$d[C_0] \leq d[C_1] \leq \cdots \leq d[C_{10}], \tag{10}$$

where $d[C_0] = 3$, $d[C_4] = 5$, $d[C_6] = 7$ and $d[C_{10}] = 15$. Equation (10) is a lower bound on the optimum distance profiles in the dictionary order or inverse dictionary order.

Acknowledgment

This work was supported in part by the German Research Foundation DFG, the National High Technology Research and Development Program of China (863 Program) (Grant no. 2006AA01Z125), the Major State Basic Research Development Program of China (973 Program) (Grant no. 2007CB310900) and the National Natural Science Foundation of China (Grant no. 60402022).

The authors wish to thank the two anonymous reviewers for their comments and suggestions to improve this paper.

REFERENCES

[1] M. Grassl, Linear Block Codes, http://www. codetables.de/.

[2] R. Hill and D.E. Newton, “Optimal ternary linear codes,” *Designs, Codes and Cryptography*, vol.2 pp. 137-157, 1992.

[3] H. Holma and A. Toskala, *WCDMA for UMTS - HSPA Evolution and LTE*, 4th Edition, John Wiley & Sons, 2007.

[4] D. B. Jaffe, “Optimal binary linear codes of length $\leq$ 30,” *Discrete Mathematics*, vol.223 pp. 135-155, 2000.

[5] D. B. Jaffe, Coding Theory Database, http://www.math.unl.edu/ ∼djaffe2/.

[6] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error Corresting Codes*, 5th printing, Elsevier Science Publishers, The Netherlands, 1986.

[7] J. Olsson and W. Willems, “A characterization of certain Griesmer codes: MMD codes in a more general sense,” *IEEE Trans. Inform. Theory*, vol. 45, no.6, pp. 2138-2142, 1999.

[8] R. Tanner and J. Woodard, *WCDMA - Requirements and Practical Design*, John Wiley & Sons, 2004.

[9] H. van Tilborg, “On the uniqueness resp. nonexsitence of certain codes meeting the Griesmer bound,” *Information and Control*, vol.44, pp. 16-35, 1980.

[10] H. N. Ward, “Divisibility of codes meeting the Griesmer bound,” *Journal of Combinatorial Theory, Series A*, vol.83 pp. 79-93, 1998.