On the Structure of Optimal Linear Block Codes of Length a Multiple of 4 and $d = 4$

Morteza Esmaeili and T. Aaron Gulliver[1]

Abstract

A decomposition of optimal linear block codes with minimum distance $d = 4$ and length $4L$ into two subcodes is given such that one of the subcodes is an optimal length L code with minimum Hamming distance 4 and the other is a quasi-cyclic code of index 4. It is shown that the L-section minimal trellis diagram of the code is the product of the minimal trellis diagrams of the subcodes.

1 Introduction

In [3], the state complexity of the trellis diagram of a linear block code was analysed via atomic codewords. This approach was exploited in [1] and [2] to investigate the trellis complexity of quasi-cyclic and general linear block codes, respectively. In this paper, we apply the concepts presented in these papers to obtain a decomposition of optimal $[4L, k, 4]$, $L \geq 2$, binary linear block codes C into two subcodes C_1 and C_2 such that under a given coordinate ordering the minimal trellis diagram (MTD) of C is the product of the MTDs of C_1 and C_2. It turns out that C_1 is an optimal code of length L and minimum Hamming distance $d = 4$, and C_2 is a quasi-cyclic code of index 4 except for $L = 2$ for which C_2 is of index 2. Some background material which is required to obtain this decomposition is now presented.

Let C be an $[n, k]$ binary linear block code over F_2 (C is a subspace of F_2^n). The span of a nonzero codeword $\mathbf{c} = (c_1, \ldots, c_n) \in C$ is defined to be the smallest interval $[i, j]$, $1 \leq i \leq j \leq n$, containing all nonzero components of $\mathbf{c}$. The positions i and j are called the origin and terminus of $\mathbf{c}$, respectively. A codeword $\mathbf{c}$ with span $[i, j]$ is called active in the

[1]Morteza Esmaeili is with the Faculty of Mathematical Sciences, Isfahan University of Technology, Isfahan, Iran, emorteza@cc.iut.ac.ir. T. Aaron Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6, agullive@ece.uvic.ca.

interval $[i, j-1]$ and the number $j-i+1$ is referred to as the span length of c. A codeword is nowhere active if $i = j$.

Definition 1 (Atomic Codeword [3]) A codeword $c \in C$ is said to be an atomic codeword if it cannot be expressed as a linear combination of codewords of C with span lengths strictly smaller than that of c. The set of all atomic codewords with the same span is called an atomic class.

A linear block code C with a given coordinate ordering can be represented by a trellis diagram. A trellis representing C is an edge-labeled directed graph T with unique initial and final vertices v_o and v_n, such that every vertex lies on a path connecting v_0 to v_n and

1. each directed path connecting v_0 and v_n has length n and its edge-label sequence is a codeword of C;

2. the number of paths connecting v_0 and v_n is the number of codewords of C.

A trellis T representing C in a given ordering of coordinates is called minimal if the number of vertices of T at distance i, $1 \leq i \leq n-1$, from v_0 is the minimum possible. The vertices of T at distance i, $0 \leq i \leq n$, from v_0 are called the states at time index i. The number $S := \max\{S_0, S_1, \cdots, S_n\}$ is called the state complexity of a length n trellis T where 2^{S_i} is the number of vertices of T at time index i.

The product of two trellises T and T', denoted $T \times T'$, is defined in [3]. It is shown in [3] that if T_i, $1 \leq i \leq k$, is the MTD of atomic codeword $a^{(i)}$, where the $a^{(i)}$ are from k distinct atomic classes of an $[n, k]$ linear block code C, then the trellis $T := T_1 \times T_2 \times \ldots \times T_k$ is the MTD of C. Accordingly, any $k \times n$ generator matrix of an $[n, k]$ linear block code C whose rows are the representatives of the k distinct atomic classes of C is referred to as a trellis oriented generator matrix (TOGM) of C. It is shown in [3] that a generator matrix M of C is a TOGM iff no two spans of the rows of M either start or end in the same positions.

Let M be a generator matrix for a k-dimensional vector space $\mathcal{V} = \prod_{i=1}^{n} \mathcal{V}_i$ over a field F where the $\mathcal{V}_i$s are vector spaces over the same field. Let M_i (resp. M^i) denote the $k \times i$ submatrix of M consisting of the first (resp. last) columns of M. It has been shown in [2] that M is a minimal generator matrix, in the sense that the sum of the span lengths of the rows of M is minimal, if the nonzero rows of each element of $\{M_1, M_2, \cdots, M_n, M^1, M^2, \cdots, M^n\}$ are linearly independent. As a result this characterises the TOGM of mixed codes and of the generators representing the m-section MTD of linear block codes. As an example, the

matrix

$$M = \begin{bmatrix} 1111 & 0000 & 0000 & 0000 \\ 0000 & 1111 & 0000 & 0000 \\ 0000 & 0000 & 1111 & 0000 \\ 0000 & 0000 & 0000 & 1111 \\ 1100 & 1100 & 0000 & 0000 \\ 0000 & 1100 & 1100 & 0000 \\ 0000 & 0000 & 1100 & 1100 \\ 1010 & 1010 & 0000 & 0000 \\ 0000 & 1010 & 1010 & 0000 \\ 0000 & 0000 & 1010 & 1010 \end{bmatrix}, \tag{1}$$

considered as a 10×4 generator matrix over F_{16}, is minimal since the nonzero rows of each element of $\{M_1, M_2, M_3, M_4, M^1, M^2, M^3, M^4\}$ are linearly independent. As a generator matrix over F_2, (1) is a TOGM for the 4-section MTD of the corresponding $[16, 10]$ binary code.

A linear block code C of length n is called *quasi-cyclic* [4, 5] if it is invariant under Λ^m, a cyclic shift of m positions, where $m < n$ and Λ is the cyclic shift operator acting on the n-tuple $(c_1, c_2, \cdots, c_n)$ by $\Lambda(c_1, c_2, \cdots, c_n) = (c_n, c_1, c_2, \cdots, c_{n-1})$. The smallest positive such m is called the index of C. It turns out that m is a divisor of n and the code is cyclic iff $m = 1$. The direct sum of two codes C_1 and C_2 is defined by $C_1 + C_2 = \{\mathbf{c}_1 + \mathbf{c}_2 : \ \mathbf{c}_1 \in C_1 \ \text{ and } \ \mathbf{c}_2 \in C_2\}$.

2 Optimal $d = 4$ linear block codes

The binary Hamming code $\mathcal{H}_2(r)$ is a $[2^r - 1, 2^r - r - 1, 3]$ code. The columns of the parity check matrix $\mathcal{H}_2^r$ of this code are precisely the $2^r - 1$ distinct nonzero binary vectors of length r. A shortened Hamming code by i coordinates, denoted $s_i\mathcal{H}_2(r)$, is a $[2^r - i - 1, 2^r - r - i - 1, 3]$ code. Thus adding an overall parity check bit to $s_i\mathcal{H}_2(r)$ we obtain the $[2^r - i, 2^r - r - i - 1, 4]$ extended linear code $s_i\hat{\mathcal{H}}_2(r)$. Examples of the resulting $[16, 11, 4]$ and $[13, 8, 4]$ codes with $\mathbf{v} = 11101101001$, $\mathbf{u} = 11101101$ and $M(C)$ denotes a generator matrix for C are

$$s_0\mathcal{H}_2^4 = \begin{bmatrix} 1000000011111111 \\ 0100011100011111 \\ 0010101101100111 \\ 0001110110101011 \end{bmatrix} = [\mathbf{I}_4\mathbf{A}], \quad s_3\mathcal{H}_2^4 = \begin{bmatrix} 100000001111 \\ 010001110001 \\ 001010110110 \\ 000111011010 \end{bmatrix} = [\mathbf{I}_4\mathbf{B}],$$

$$M(s_0\hat{\mathcal{H}}_2(4)) = [\mathbf{A}^t\mathbf{I}_{11}\mathbf{v}^t] \quad \text{and} \quad M(s_3\hat{\mathcal{H}}_2(4)) = [\mathbf{B}^t\mathbf{I}_8\mathbf{u}^t],$$

respectively. The redundancy of these two codes $R = 16 - 11 = 13 - 8 = 5$ is equal. In general, optimal $d = 4$ linear block codes are shortened Hamming codes with an overall parity bit, and the redundancy of an $[n, k_{max}, 4]$ linear code with $2^{l-1} < n \leq 2^l$ is $R = n - k_{max} = l + 1$.

3 Optimal $d = 4$ codes of length a multiple of 4

A linear block code C of length n and minimum Hamming distance d is called optimal if it has maximum dimension among all codes of the same length and distance. In this section, we shall precisely describe the relationship between optimal linear block codes of length $4L$ and L with $d = 4$. In the sequel $\mathcal{C}(n, 4)$ stands for an optimal linear block code of length n and minimum Hamming distance $d = 4$. For $n < 4$ define $\mathcal{C}(n, 4) := \{\mathbf{0}\}$, the zero sequence of length n.

We shall show that there are subcodes C_1 and C_2 of $\mathcal{C}(4L, 4)$, $L \geq 2$, such that $\mathcal{C}(4L, 4)$ is the direct sum of C_1 and C_2; and

1. Ignoring the coordinates in which all codewords of C_1 are zero, C_1 is an optimal code $\mathcal{C}(L, 4)$. The subcode C_2 is a quasi-cyclic code of index 4.

2. Under a given coordinate ordering, the MTD of $\mathcal{C}(4L, 4)$ is the product of the MTDs of C_1 and C_2.

Let $\mathbf{c}_1$, $\mathbf{c}_2$, and $\mathbf{c}_3$ be binary words of weight 4 and length $4L$ such that the first 4 bits of $\mathbf{c}_1$ are nonzero; the first, second, fifth, and sixth bits of $\mathbf{c}_2$ are nonzero; and the first, third, fifth, and seventh positions of $\mathbf{c}_3$ are nonzero.

Define $\Lambda^j(\mathbf{c})$ as the cyclic shift of the word $\mathbf{c}$ by j positions to the right. Consider the matrix $G_L(1, 2)$ with rows consisting of the $4L$-tuples $\Lambda^{4i}(\mathbf{c}_1)$, $0 \leq i \leq L - 1$, and $\Lambda^{4i}(\mathbf{c}_j)$, $0 \leq i \leq L - 2$, $j = 2$ and 3. For instance, the matrix M given by (1) represents $G_4(1, 2)$.

The code with generator matrix $G_L(1, 2)$ is denoted by $\mathcal{R}_L(1, 2)$. In fact we have $\mathcal{R}_L(1, 2) = (L, L, 1) \otimes (4, 1, 4) + (L, L-1, 2) \otimes [1100] + (L, L-1, 2) \otimes [1100]$ where $\otimes$ stands for the Kronecker product operation. It is easy to see that $\mathcal{R}_2(1, 2)$ is a quasi-cyclic code of index 2 while $\mathcal{R}_L(1, 2)$ is a quasi-cyclic code of index 4 for $L \geq 3$.

Lemma 1 $\mathcal{R}_L(1, 2)$ is a $[4L, 3L - 2, 4]$ linear code.

Proof Consider $G_L(1, 2)$ as a $(3L - 2) \times L$ matrix with entries from F_2^4. For a given i, $1 \leq i \leq L$, let B_i denote the set of nonzero entries that are in the ith column such that each is the first nonzero element of a row of $G_L(1, 2)$. B_i is given by the independent set $\{1111, 1100, 1010\}$ for $1 \leq i \leq L - 1$, and $B_L = \{1111\}$. Since $\sum_{i=1}^{L} |B_i| = 3L - 2$, the rows of $G_L(1, 2)$ are independent and hence $\mathcal{R}_L(1, 2)$ has dimension $3L - 2$.

The row space of each column of $G_L(1, 2)$, viewed as a $(3L - 2) \times L$ matrix over F_2^4, is the set of all words of weights 0, 2, and 4. Let $\mathbf{c}$ be a

nonzero codeword of $\mathcal{R}_L(1,2)$, with c_i and c_j as the first and last nonzero components, where $1 \leq i \leq j \leq L$. If $i \neq j$, then both c_i and c_j are of weight at least two and hence c has weight at least four. Suppose $i = j$. This implies that all rows of $G_L(1,2)$ involved in the formation of $\mathbf{c}$ are nonzero only at their jth components. This means that $c_j = 1111$, and $\mathbf{c}$ has weight four. Therefore, $\mathcal{R}_L(1,2)$ has minimum distance four. ■

Let $k_{max}(n,4)$ denote the dimension of $\mathcal{C}(n,4)$. Define $\mathcal{C}_{n,4} := \mathcal{C}(n,4) \otimes [1000]$. Note that $\mathcal{R}_L(1,2) \bigcap \mathcal{C}_{L,4} = \{\mathbf{0}\}$, where $\mathbf{0}$ denotes the all zero codeword.

Lemma 2 $\mathcal{R}_L(1,2) + \mathcal{C}_{L,4}$ has minimum distance four.

Proof The statement trivially holds for $L < 4$ since by definition $\mathcal{C}(L,4) = \{\mathbf{0}\}$ for $L < 4$. Suppose $L \geq 4$. Let $\mathbf{c}$ and $\mathbf{c}'$ be nonzero codewords in $\mathcal{R}_L(1,2)$ and $\mathcal{C}_{L,4}$, respectively. Denote the first four nonzero block components of $\mathbf{c}'$ by c'_1, c'_2, c'_3, and c'_4. Let c_i, $1 \leq i \leq 4$, be the block components of $\mathbf{c}$ corresponding to c'_i. Since c_i is in the row space of $\{1111, 1100, 1010\}$, it has even weight, implying that $c_i + c'_i$ has odd weight and therefore is a nonzero block. It follows that $\mathbf{c} + \mathbf{c}'$ has weight at least four. ■

Theorem 1 Suppose T, T', and T'' are the m-section, $m \leq L$, MTDs of $\mathcal{C}(4L,4)$, $\mathcal{R}_L(1,2)$, and $\mathcal{C}_{L,4}$, respectively, considered as linear codes over F_2^4. Then

$$\mathcal{C}(4L,4) = \mathcal{R}_L(1,2) + \mathcal{C}_{L,4} \quad \text{and} \quad T = T' \times T''.$$

Proof If $2^{l-1} < 4L \leq 2^l$ then $4L - k_{\max}(4L,4) = l + 1$ and $L - k_{\max}(L,4) = l - 1$. Hence $k_{\max}(4L,4) - k_{\max}(L,4) = 3L - 2$. This equality and Lemma 2 result in $\mathcal{C}(4L,4) = \mathcal{R}_L(1,2) + \mathcal{C}_{L,4}$. Assume that M' and M'' are the TOGMs of the given $m-$section MTDs of $\mathcal{R}_L(1,2)$ and $\mathcal{C}_{L,4}$, respectively. The set consisting of the distinct nonzero entries of M' and M'', considered as matrices over F_2^4, is a linearly independent set. Therefore it follows from Theorem 4 in [2] that matrix M consisting of the rows of M' and M'' is a TOGM of the $m-$section MTD of $\mathcal{C}(4L,4)$, implying that $T = T' \times T''$. ■

Example 1 The doubly even self-orthogonal code specified by the following generator matrix is $\mathcal{C}(6,4)$

$$M' = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Therefore, the following is a TOGM for the 6-section MTD of the 18-dimensional linear code

$$\begin{aligned} \mathcal{C}(24,4) &= \mathcal{R}_6(1,2) + \mathcal{C}_{6,4} \\ &= \{(6,6,1) \otimes (4,1,4) + (6,5,2) \otimes [1100] + (6,5,2) \otimes [1010]\} \\ &\quad + \{(3,2,2) \otimes (2,1,2) \otimes [1000]\}, \end{aligned}$$

with generator matrix

$$M'' = \begin{bmatrix}
1111 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0000 & 1111 & 0000 & 0000 & 0000 & 0000 \\
0000 & 0000 & 1111 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 1111 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0000 & 1111 & 0000 \\
0000 & 0000 & 0000 & 0000 & 0000 & 1111 \\
1100 & 1100 & 0000 & 0000 & 0000 & 0000 \\
0000 & 1100 & 1100 & 0000 & 0000 & 0000 \\
0000 & 0000 & 1100 & 1100 & 0000 & 0000 \\
0000 & 0000 & 0000 & 1100 & 1100 & 0000 \\
0000 & 0000 & 0000 & 0000 & 1100 & 1100 \\
1010 & 1010 & 0000 & 0000 & 0000 & 0000 \\
0000 & 1010 & 1010 & 0000 & 0000 & 0000 \\
0000 & 0000 & 1010 & 1010 & 0000 & 0000 \\
0000 & 0000 & 0000 & 1010 & 1010 & 0000 \\
0000 & 0000 & 0000 & 0000 & 1010 & 1010 \\
1000 & 1000 & 1000 & 1000 & 0000 & 0000 \\
0000 & 0000 & 1000 & 1000 & 1000 & 1000
\end{bmatrix}.$$

For $L \geq 3$ each section of the L-section MTD of $\mathcal{R}_L(1,2)$ is a complete bipartite graph and except for the initial and final indices the trellis has 4 states at each time index. As a result $\mathcal{R}_L(1,2)$ has state complexity 2. Thus $S(4L) = S(L) + 2$, where $S(4L)$ and $S(L)$ are the state complexities of $\mathcal{C}(4L,4)$ and $\mathcal{C}(L,4)$, respectively.

It follows from the structure of the trellis diagram of $\mathcal{R}_L(1,2)$ that for $L \geq 4$, the number of parallel subtrellises in the $L-$section MTD of $\mathcal{C}(4L,4)$, denoted by $t(\mathcal{C}(4L,4))$, is at most two and is equal to that of $\mathcal{C}(L,4)$. Furthermore, if $t(\mathcal{C}(L,4)) = 2$ then $k_{\max}(L,4) = 1 + k_{\max}(L-2,4)$, which is true if $L = 2^l + 1$. Figure 1 presents the trellis structure of $\mathcal{C}(24,4)$.

ACKNOWLEDGMENT

The authors would like to thank Dr. Neil Sloane for his help with this paper.

References

[1] M. Esmaeili, T.A. Gulliver and N.P. Secord, "Quasi-cyclic structure of Reed-Muller codes and their smallest regular trellis diagram," *IEEE Trans. Inform. Theory*, vol. 43, May 1997, pp. 1040–1052.

[2] M. Esmaeili, T.A. Gulliver and N.P. Secord, "The minimal generator matrix of a vector space," *Applic. Algebra in Engin., Commun. and Comp.*, vol. 10, Aug. 1999, pp. 1–14.

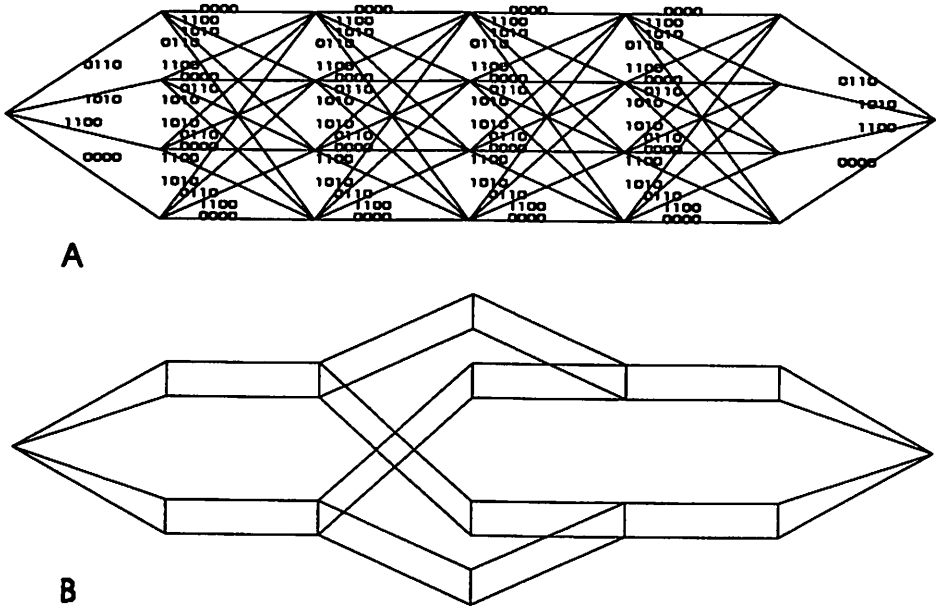

Figure 1: A: The 6-section MTD of $\mathcal{R}_5(1,2)$. B: An illustration of the 6-section MTD of $C(24,4)$.

[3] F.R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, Nov. 1995, pp. 1924–1937.

[4] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland:Amsterdam, 1977.

[5] G. E. Séguin and H. I. Huynh, *Quasi-Cyclic Codes: A Study*, Technical Report, Universite Laval, Quebec, Canada, 1985.