Optimal Binary Linear Codes Containing the $[6,5,2] \otimes [3,1,3]$ Product Code

M. Esmaeili
Department of Mathematical Sciences
Isfahan University of Technology, Isfahan, Iran
emorteza@cc.iut.ac.ir

M. R. Yazdani
Dept. of Systems and Computer Engineering
Carleton University, Ottawa, Canada
ryazdani@sce.carleton.ca

T. A. Gulliver
Dept. of Electrical and Computer Engineering
University of Victoria, P.O. Box 3055, STN CSC
Victoria, B.C., Canada V8W 3P6
agullive@ece.uvic.ca

Abstract

Optimal binary linear codes of length 18 containing the $[6,5,2] \otimes [3,1,3]$ product code are presented. It is shown that these are $[18,9,5]$ and $[18,8,6]$ codes. The soft-decision maximum-likelihood decoding complexity of these codes is determined. From this point of view these codes are better than the $[18,9,6]$ code.

[1]The first author's contribution was supported in part by the Isfahan University of Technology under grant 1MAE831.

1 Introduction

Let $[n, k, d]$ be a binary linear code of length n, dimension k and minimum Hamming distance d. It is known that codes containing simple subcodes, such as $E_m = [m, m-1, 2]$, the length m single parity check code, can be decoded efficiently [2, 4, 9]. It is shown in [4] that if a code C of length tm includes the product code $E_m \otimes [t, 1, t]$, then one may employ the acyclic Tanner graph [13] of this product subcode and the minimal trellis diagram(MTD) [1, 5, 7, 8, 14] of the quotient code $C/(E_m \otimes [t, 1, t])$ to efficiently decode C. This method is in fact an extension of the Wagner rule [10] decoding algorithm. The efficiency of this approach is based on the fact that the subcode $E_m \otimes [t, 1, t]$ has the best form of an acyclic Tanner graph. The $[24, 12, 8]$ Golay code and the extended $[32, 16, 8]$ BCH code contain the acyclic codes $E_6 \otimes [4, 1, 4]$ and $E_8 \otimes [4, 1, 4]$, respectively [4]. We refer the interested reader to [4] for more details.

A Tanner graph representing a linear block code with parity check matrix $H = [h_{ij}]$ is a bipartite graph in which one of the two sets of vertices denote the parity nodes (rows of H), and the other set denote the symbol nodes (columns of H). A parity node u_i is connected to a symbol node v_j iff $h_{ij} \neq 0$. A cycle-free Tanner graph is called an acyclic Tanner graph (ATG).

Suppose $C = C_5 + C'$ where $C_5 := [6, 5, 2] \otimes [3, 1, 3]$. The values of the parity nodes of the Tanner graph of C_5 are zero. The cosets of C_5 in C have structurally the same Tanner graphs but with different values on the parity nodes. Let M_5 and $M_5^{\perp}$ denote generator matrices of C_5 and its dual code $C_5^{\perp}$, respectively. The space of the parity nodes, referred to as the *parity space* (PS), is generated by the matrix $M_{PS} := M_5^{\perp} M'^{t}$, where M'^{t} is the transpose of a generator matrix M' of C'. The ATG of C_5 together with the MTD of the associated PS are a graphical representation of C that can be employed in the decoding process (for a more detailed treatment of this area of research, we refer the reader to [4]). Figure 1 shows one such representation for an $[18, 9, 5]$ code containing C_5 (this will be described in more detail in Example 2).

In this paper we study optimal codes that contain C_5 as a subcode. In Section 2 we apply the results given in [11] to show that there is no $[18, 9, 6]$ code containing C_5. It is then shown in Section 3 that there are $[18, 9, 5]$ codes containing C_5 whose soft-decision maximum-likelihood decoding complexity is half that of the $[18, 9, 6]$ code. These codes are divided into three groups in terms of the MTD of the quotient code $[18, 9, 5]/C_5$. We also present $[18, 8, 6]$ codes whose average decoding complexity is 121 binary operations, which is about one-third the complexity for the $[18, 9, 6]$ code.

We now provide some necessary background material. Let C be an $[n, k]$ linear block code over F_2. For nonnegative integers i and j, the interval

$[i, j]$ is said to be the span interval, or simply the span, of the codeword $c = (c_1, \cdots, c_n) \in C$ if $c_i c_j \neq 0$, and $c_l = 0$ if $l < i$ or $j < l$. In this case the codeword c is said to be *active* in the interval $[i, j-1]$, and has span length $j - i + 1$. A codeword c is said to be nowhere active if either $i = j$ or c is zero. The span length of the zero codeword is defined to be 0.

Let M be a $k \times m$ matrix whose entries are in the vector space F_2^l. Consider the set

$$S = \{M_1,\ M_2,\ \cdots,\ M_m,\ M^1,\ M^2,\ \cdots,\ M^m\},$$

where M_i (resp. M^i), $1 \leq i \leq m$, is the $k \times i$ matrix formed from the first i (resp. last i) columns of M. Matrix M is said to be a minimal matrix if the nonzero rows of each element of S are linearly independent Suppose now that such a minimal matrix M is a generator matrix of a linear block code C of length $n = lm$ and dimension k. Then Theorem 5 of [5] states that T, the m-section MTD of C, consists of $2^{|A_{1m}|}$ identical (in terms of the graph structure) parallel subtrellises, where A_{1m} is the number of rows in M with support $[1, m-1]$ when M is considered over F_2^l.

2 Structure of the $[18, 9, 6]$ binary code

In this section we show that the class of optimal binary codes containing $[6, 5, 2] \otimes [3, 1, 3]$ does not include the $[18, 9, 6]$ binary code and hence we focus on the $[18, 9, 5]$ and $[18, 8, 6]$ codes.

Using enumeration and combinatorial methods it was shown in [6] that there is no $[18, 9, 6]$ code containing C_5 as a subcode. Here we present a simpler proof using the fact that Simonis [11] has shown that the $[18, 9, 6]$ code is unique. In Table 2 of [11], the weight distribution of the cosets of this code were given. We use this distribution to show that C_5 cannot be extended to the $[18, 9, 6]$ code.

Theorem 1 The $[18, 9, 6]$ code C does not contain C_5.

Proof. If C contains C_5 then the coset $r+C$, with $r = 111000000000000000$ contains at least 6 words of weight 3. However from the weight distribution given in Table 2 of [11], the number of weight 3 words in a coset does not exceed 4, which is a contradiction. ■

3 Optimal Codes Containing C_5

As mentioned previously, the existence of C_5 in a binary code of length 18 reduces the decoding complexity substantially. In this section we consider

codes containing C_5 that are optimal either in terms of dimension or minimum distance. In particular, we show that there exist $[18, 8, 6]$ and $[18, 9, 5]$ codes that contain C_5.

3.1 $[18, 8, 6]$ codes containing C_5

It is shown that the 3-section MTD of the parity space of any $[18, 8, 6]$ code with generator matrix

$$\mathbf{G}_1 = \begin{pmatrix} \mathbf{M}_5 \\ \mathbf{M}_3 \end{pmatrix},$$

consists of 8 parallel paths and the decoding process requires 117 to 125 binary operations. First we show that in order to extend the generator matrix $\mathbf{M}_5$ of C_5 into a generator matrix $\mathbf{M}$ representing an $[18, 8, 6]$ code it is enough to choose three additional words from a subclass $\mathbf{A}$ of the weight 6 and weight 7 words from which the trellis structure can be obtained.

3.1.1 Elimination of unnecessary words

For simplicity, a word of length 18 from $\mathbf{M}_5$ is divided into 6 blocks of length 3 denoted by b_1, b_2, $\cdots$, b_6 from left to right. It is obvious that C_5 is invariant under block column permutations. Therefore we have the following form for $\mathbf{M}_5$

$$\mathbf{M}_5 = \begin{pmatrix} 111 & 111 & 000 & 000 & 000 & 000 \\ 000 & 111 & 111 & 000 & 000 & 000 \\ 000 & 000 & 111 & 111 & 000 & 000 \\ 000 & 000 & 000 & 111 & 111 & 000 \\ 000 & 000 & 000 & 000 & 111 & 111 \end{pmatrix}.$$

Suppose there exists a binary 3×18 matrix $\mathbf{M}_3$ such that $\mathbf{G}_1$ represents an $[18, 8, 6]$ binary code denoted by C_8. The requirement for a minimum distance of 6 implies that the rows of $\mathbf{M}_3$ must be of Hamming weight at least 6. It is shown here that we can restrict the elements of $\mathbf{M}_3$ to a subclass of words of weights 6 and 7. Using C_5 and row operations one can easily verify the statements given in the following lemma.

Lemma 1 (1). A row $\mathbf{c} \in \mathbf{M}_3$ with an even number of blocks of weight 2 (and arbitrary weights in the other blocks), can be replaced with another word $\mathbf{c}'$ such that in the block positions that $\mathbf{c}$ has weight 2 the word $\mathbf{c}'$ is of weight 1 and in other blocks they are identical. (2). If a row $\mathbf{c}$ of $\mathbf{M}_3$ has some blocks b_i and b_j of weight 3 and 1, respectively, then $\mathbf{c}$ can be replaced by a row $\mathbf{c}'$ in which the blocks b_i and b_j have weight 0 and 2, respectively. (3). A row $\mathbf{c} \in \mathbf{M}_3$ having two blocks of weight 3 can be replaced with a word $\mathbf{c}'$ in which the corresponding blocks have weight 0. ■

3.1.2 Words of weight 6 and 7

Theorem 2.6 of [3] states "If C is an $[n,k,d]$ code of length $n = g_2(k,d)+t$ with t an integer, then C has a generator matrix G, every row of which has weight between d and $d+t$," where $g_2(k,d) := \sum_{j=0}^{k-1}\lceil d/2^j\rceil$. For a $[18,8,6]$ binary code we have $n = 18$ and $g_2(8,6) = \sum_{j=0}^{7}\lceil 6/2^j\rceil = 16$ and hence $d+t = 8$. Therefore, this theorem implies that such a code has a generator matrix G every row of which has weight 6, 7 or 8. In the following we show that a $[18,8,6]$ code containing C_5 has a generator matrix G every row of which has weight 6 or 7.

If a word $\mathbf{c}$ of weight 6 has two or three weight2 blocks then, by Lemma 1, $\mathbf{c}$ is equivalent to a word $\mathbf{c}'$ (i.e. it can be replaced with $\mathbf{c}'$) of weight less than 6. Hence these words are eliminated. Thus there are only two types of weight 6 words that can be used to extend $\mathbf{M}_5$. One type is the weight 6 words with exactly one block of weight 2 and four blocks of weight 1, and the other type is the set of weight 6 words each of which consists of six blocks of weight 1. A similar argument shows that the only useful words of weight 7 are those consisting of one block of weight 2 and five blocks of weight 1. The union of these three types of words is denoted by $\mathbf{A}$.

It is obvious that a word $\mathbf{c}$ of weight 8 has either at least two blocks of weight more than 1 or one block of weight 3 and five weight 1 blocks. According to Lemma 1 in either of these two cases $\mathbf{c}$ can be replaced with a word of weight at most 6. Thus there is no need to consider the set of weight 8 words. According to Theorem 2.6 of [3] we do not need to consider words of weight more than 8.

In summary, we may assume that the rows of $\mathbf{M}_3$ belong to $\mathbf{A}$. This together with Theorem 5 of [5], restated in the Introduction, results in the following corollary.

Corollary 1 The 3-section MTD of the parity space of any $[18,8,6]$ code containing C_5 consists of 8 parallel paths.

Based on this corollary and using the decoding method given in [4], these $[18,8,6]$ codes can be decoded using 117 to 125 binary operations.

Example 1 The following matrix $\mathbf{M}_3$ in an $[18,8,6]$ code that contains C_5 results in the weight distribution given below.

$$\mathbf{M}_3 = \begin{pmatrix} 000 & 110 & 001 & 100 & 010 & 001 \\ 110 & 010 & 000 & 001 & 010 & 010 \\ 100 & 100 & 100 & 100 & 100 & 010 \end{pmatrix}$$

Weight	0, 18	6, 12	8, 10
Count	1	46	81

3.2 $[18, 9, 5]$ codes containing C_5

In this section, we consider 9-dimensional binary codes containing C_5 with the largest minimum distance. Based on the previous results, these codes have minimum distance 5, and from the decoding complexity point of view they are divided into three classes. These codes can be partitioned according to the number of parallel subtrellises in the 3-section MTD of their associated parity spaces.

Lemma 2 The number of parallel subtrellises (NPS) of the 3-section MTD of the parity space of any $[18, 9, 5]$ binary code containing C_5 belongs to $\{4, 8, 16\}$.

Proof. Assume that

$$\mathbf{G}_2 = \begin{pmatrix} \mathbf{M}_5 \\ \mathbf{M}_4 \end{pmatrix},$$

is a generator matrix of a binary $[18, 9, 5]$ code C_9. By Theorem 5 of [5], NPS is a power of 2. If this number is at most 2 then the supports of at least 3 rows of the parity space lie in the interval $[1, 8]$ or $[5, 12]$. It follows then from $\mathbf{M}_{PS} = \mathbf{M}_5^{\perp}\mathbf{M}_4^t$ that the first or the last 6 bits of the corresponding rows of $\mathbf{M}_4$ are all zero. Without loss of generality we may assume that two rows of $\mathbf{M}_4$, say r_1 and r_2, are zero in their first 6 bits. We show that this results in a codeword with $d < 5$.

By Lemma 1 and the condition that $d \geq 5$ the rows r_1 and r_2 of $\mathbf{M}_4$ must have weight 5 in their last four blocks and none of these blocks can be of weight zero. It also follows from condition $d = 5$ that the number of bit positions of these last four blocks in which both r_1 and r_2 are nonzero is at most 2; but then $r_1 + r_2$ will be of weight 6, 8, or 10. This together with C_5 produce a codeword of weight less than 5, a contradiction. Hence NPS $\in \{4, 8, 16\}$. ■

Example 2 In this example we show that NPS can be any of the three numbers 4, 8 and 16. For each of these three sets of codes we provide an example. A code with NPS=i is given below by its corresponding 4-dimensional matrix $\mathbf{M}_4$, denoted $\mathbf{M}_4(i)$. The weight distributions are also listed.

$$\mathbf{M}_4(4) = \begin{pmatrix} 001 & 001 & 011 & 001 & 000 & 100 \\ 000 & 000 & 001 & 001 & 011 & 001 \\ 100 & 100 & 110 & 100 & 010 & 000 \\ 000 & 011 & 010 & 001 & 001 & 010 \end{pmatrix}$$

Weight	0, 18	5, 13	6, 12	7, 11	8, 10	9
Count	1	22	46	56	81	100

$$\mathbf{M}_4(8) = \begin{pmatrix} 001 & 010 & 010 & 010 & 010 & 001 \\ 000 & 000 & 001 & 001 & 011 & 001 \\ 100 & 100 & 110 & 100 & 010 & 000 \\ 000 & 011 & 010 & 001 & 001 & 010 \end{pmatrix}$$

Weight	0, 18	5, 13	6, 12	7, 11	8, 10	9
Count	1	20	46	64	81	88

$$\mathbf{M}_4(16) = \begin{pmatrix} 011 & 001 & 001 & 000 & 100 & 001 \\ 001 & 000 & 000 & 011 & 001 & 001 \\ 110 & 100 & 100 & 010 & 000 & 100 \\ 010 & 011 & 000 & 001 & 010 & 001 \end{pmatrix}$$

Weight	0, 18	5, 13	6, 12	7, 11	8, 10	9
Count	1	22	46	56	81	100

The Tanner graph of C_5 together with the 3-section MTD of the parity space generated by $\mathbf{M}_{PS} = \mathbf{M}_5^{\perp}\mathbf{M}_4(4)^t$ is shown in Figure 1.

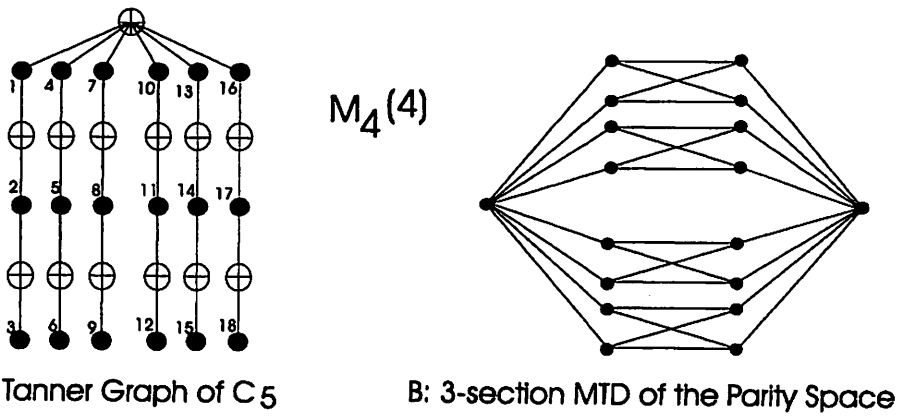

Figure 1: A: The Tanner graph of the product code C_5. B: The 3-section MTD of the parity space corresponding to the $[18, 9, 5]$ code represented by $\mathbf{M}_4(4)$.

The corresponding decoding complexities are given in Table 1. The average decoding complexity of the codes with NPS=4, using the decoding method given in [4], is 181 binary operations while the lowest reported decoding complexity for the $[18, 9, 6]$ code is 340 [12].

References

[1] L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, Optimal decoding of linear codes for minimising symbol error rate, IEEE Trans. Inform.

Table 1: Decoding complexities of [18,9,5] codes.

NPS	Min Operations	Max Operations
4	173	189
8	189	205
16	205	221

Theory, Vol. 20, pp. 284–287, Mar. 1974.

[2] J.H. Conway and N.J.A. Sloane, Decoding techniques for codes and lattices, including the Golay code and the Leech lattice, IEEE Trans. Inform. Theory, Vol. 32, pp. 41–50, Jan. 1986.

[3] S.M. Dodunekov and N.L. Manev, An improvement of the Griesmer bound for some small minimum distances, Discrete Applied Math., Vol. 12, pp. 103–114,1985.

[4] M. Esmaeili and A.K. Khandani, Acyclic Tanner graph and maximum-likelihood decoding of linear block codes, IEE Proc. Commun., Vol. 147, No. 6, pp. 322–332, Dec. 2000.

[5] M. Esmaeili, T.A. Gulliver and N.P. Secord, The minimal generator matrix of a vector space, Applic. Algebra in Eng., Commun. and Comp., Vol. 10, No. 1, pp. 1–14, Aug. 1999.

[6] M. Esmaeili, M.R. Yazdani and T.A. Gulliver, On the structure of the binary $(18, 9, 6)$ linear code, Proc. IEEE Inform. Theory Workshop, pp. 62–65, Mar. 2003.

[7] B. Honary, G. Markarian and M. Darnell, Low-complexity trellis decoding of linear block codes, IEE Proc. Commun., Vol. 142, pp. 201–209, Aug. 1995.

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

[9] V. Pless, Decoding the Golay code, IEEE Trans. Inform. Theory, Vol. 32, pp. 561–567, July 1986.

[10] R.A. Silverman and M. Balser, Coding for a constant data rate source, IRE Trans. Inform. Theory, Vol. 4, pp. 50–63, 1954.

[11] J. Simonis, The $[18, 9, 6]$ code is unique, Discrete Math., Vol. 106/107, pp. 439–448, 1992.

[12] J. Snyders and Y. Be'ery, Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes, IEEE Trans. Inform. Theory, Vol. 35, pp. 963–975, Sept. 1989.

[13] R.M. Tanner, A recursive approach to low complexity codes, IEEE Trans. Inform. Theory, Vol. 27, pp. 533–547, Sept. 1981.

[14] J.K. Wolf, Maximum likelihood decoding of linear block codes using a trellis, IEEE Trans. Inform. Theory, Vol. 24, pp. 76–80, Jan. 1978.