On the Pless-Construction and ML Decoding of the (48,24,12) Quadratic Residue Code

M. Esmaeili[⋆], T. A. Gulliver[†], and A. K. Khandani[‡]

[⋆]Dept. of Math. Sciences, Isfahan University of Technology, Isfahan, Iran

[†] Dept. of Elec. and Comp. Eng. Univ. of Victoria, Victoria, BC, V8W 3P6 Canada

[‡]Dept. of Elec. and Comp. Eng., Univ. of Waterloo, Waterloo, ON, N2L 3G1 Canada

Abstract: We present a method for maximum likelihood decoding of the $(48, 24, 12)$ quadratic residue code. This method is based on projecting the code onto a subcode with an acyclic Tanner graph, and representing the set of coset leaders by a trellis diagram. This results in a two level coset decoding which can be considered a systematic generalization of the Wagner rule. We show that unlike the $(24, 12, 8)$ Golay code, the $(48, 24, 12)$ code does not have a Pless-construction which has been an open question in the literature. It is determined that the highest minimum distance of a $(48, 24)$ binary code having a Pless-construction is 10, and up to equivalence there are three such codes.

1 Introduction

In the application of error-correcting codes to communication systems, one of the most important problems is to develop and implement an efficient decoding algorithm for a given code. Ideally, one would also like the algorithm to be universal or applicable over a wide range of code structures. It is well known that soft decision decoding results in a saving in required energy of about 25-50% over that for hard decision decoding. The main approaches for soft decision maximum likelihood (ML) decoding can be divided into two categories: (i) Trellis based decoding methods using Viterbi algorithm, and (ii) Coset decoding.

The Viterbi algorithm [10] provides a solution for decoding convolutional codes using the trellis diagram associated with the code. Bahl *et al.* [2] and Wolf [27] showed that one could also employ the Viterbi algorithm to decoding a block code. Forney [14] later gave a procedure for constructing *minimal* trellis diagrams (MTD) for Reed-Muller codes and the extended Golay code. Since then, there has been considerable interest in the minimal trellis of linear block codes [8, 15, 17, 19, 24]. Trellis based approaches have also been applied to the decoding of array codes [4, 16].

The work of Conway and Sloane [5] has addressed the decoding of binary codes containing geometrically simple subcodes such as the universe code $\mathcal{F}_n$ and the even weight code $\mathcal{E}_n$. A slightly different language and perspective has been independently applied to decoding of the extended Golay codes by Pless [21] using the hexacode H_6 and the $(4, 2, 3)$ tetracode. These approaches have been employed by several authors [22, 25, 26, 28] to produce many of the best known techniques for decoding linear block codes including the $(24, 12)$ Golay code [26], the $(32, 16)$ extended quadratic residue (QR) code [28], and the second order Reed-Muller codes [22]. The method of coset decoding has been also used in [11, 12, 13] in conjunction with other decoding techniques to provide a variety of tradeoffs between bit error performance and decoding complexity.

Coset decoding of the extended Golay codes has been addressed by Conway and Sloane [5] using subcodes with desirable properties such as even weight and universal codes, and by Pless [21] using the structure of the hexacode H_6 and the $(4, 2, 3)$ tetracode. The work of Pless was improved substantially first by Snyders and Be'ery [25] using the Wagner rule [23] together with coset decoding, and then by Vardy and Be'ery [26] applying the Wagner rule and Pless-construction of these codes.

The main techniques presented in [26] were later used in [28] to decode the extended $(32, 16, 8)$ QR code. The common approach in [26, 28] is the projection of these two extended QR codes onto quaternary codes. In these papers, it is left as a question whether the Pless-type projection can be applied to other block codes, particularly to the $(48, 24, 12)$ QR code.

It has been shown [7] that the decoding method used in [26, 28] lies in the framework of a systematic approach whose main ingredients, when decoding a code C, consist of an acyclic Tanner graph (ATG) of a subcode C_0 together with a trellis diagram of C/C_0. Here, we extend this method to the ML decoding of the $(48, 24, 12)$ QR code. This results in a decoding method which is 15% less complex than the best decoding method known for this code using a trellis based approach [20]. Note that codes with cycle-free TGs were completely characterized in [9].

We also show that unlike the $(24, 12, 8)$ Golay code, the $(48, 24, 12)$ code does not have a Pless-construction, which has been an open question in the literature [26, 28]. More generally, we show that the largest minimum distance of a $(48, 24)$ binary code with a Pless-construction is 10, and there are exactly three such codes up to equivalence.

A code C is said to be the sum of C_1 and C_2, denoted $C = C_1 + C_2$, if C_1 and C_2 are subcodes of C and $C_1 \bigcap C_2 = \{0\}$, and $C = \{c_1 + c_2 | \ c_1 \in C_1 \text{and } c_2 \in C_2\}$. The direct product (also called Kronecker product or simply product) operation is denoted by '$\otimes$'. The direct sum of two codes C_1 and C_2, denoted $C_1 \oplus C_2$, is defined to be $C_1 \oplus C_2 := \{c_1c_2 | \ c_1 \in C_1 \text{and } c_2 \in C_2\}$, where c_1c_2 is the concatenation of c_1 and c_2. The standard product of two matrices M_1 and M_2 is denoted by M_1M_2.

2 Background

In this section necessary results on the *Tanner-graph trellis* (TGT) representation, the Pless-type projection and their connection are given from [7, 21, 26, 28].

2.1 Tanner-graph Trellis Representation

A *Tanner graph* (TG) representing a linear block code C with parity check matrix $H = [h_{ij}]$ is a bipartite graph with parity nodes representing the rows of H and symbol nodes representing the columns of H. A symbol node v_i is adjacent to a parity node u_j iff $h_{ij} \neq 0$. The number of edges associated with a parity check matrix H is the number of nonzero entries in H. A TG representing C is referred to as the *minimal Tanner graph* (MTG) if it has the minimum number of edges among all such graphs. Although such a graph is not unique, all MTGs of C have the same cycle-space rank [6]. A cycle-free TG is called an *acyclic Tanner graph* (ATG) and a connected ATG is referred to as a *Tree Tanner graph* (TTG).

Example 1 Let C be the $(12, 7)$ binary linear code with generator and parity check matrices M and H, respectively, given below

$$M = \begin{bmatrix} 111100000000 \\ 001111000000 \\ 000011110000 \\ 000000111100 \\ 000000001111 \\ 101010110000 \\ 000010111010 \end{bmatrix}, \qquad H = \begin{bmatrix} 101010101010 \\ 111100000000 \\ 000000001111 \\ 000000110000 \\ 110011001100 \end{bmatrix}. \tag{1}$$

The TG associated with H is given in Fig. 1. This is a MTG since the check matrix H cannot be replaced by another check matrix with fewer nonzero entries.

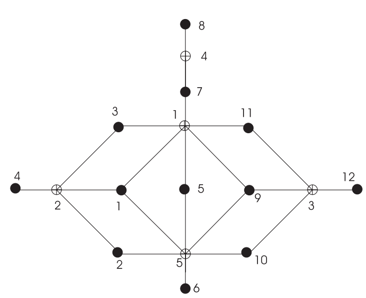

Figure 1: The minimal Tanner graph of linear block code C speccified by the generator and check matrices M and H, respectively, given by (1).

As the Wagner rule can only be applied to acyclic TGs, we choose the subcode C_0 of C with the following generator and parity check matrices M_0 and H_0, respectively

$$M_0 = \begin{bmatrix} 111100000000 \\ 001111000000 \\ 000011110000 \\ 000000111100 \\ 000000001111 \end{bmatrix}, \qquad H_0 = \begin{bmatrix} 101010101010 \\ 110000000000 \\ 001100000000 \\ 000011000000 \\ 000000110000 \\ 000000001100 \\ 000000000011 \end{bmatrix}. \tag{2}$$

The corresponding TG is shown in Fig. 2a. Following the method of [7], the code C is represented by four copies of this TTG with parity node values determined by the generator matrix $M_1 H_0^t$ denoted by

$$M_{PS} := M_1 H_0^t = \begin{bmatrix} 101010110000 \\ 000010111010 \end{bmatrix} \begin{bmatrix} 101010101010 \\ 110000000000 \\ 001100000000 \\ 000011000000 \\ 000000110000 \\ 000000001100 \\ 000000000011 \end{bmatrix}^t = \left[\begin{array}{ccccccc} p_r & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \\ \hline 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array} \right], \tag{3}$$

which is the generator of the parity space.

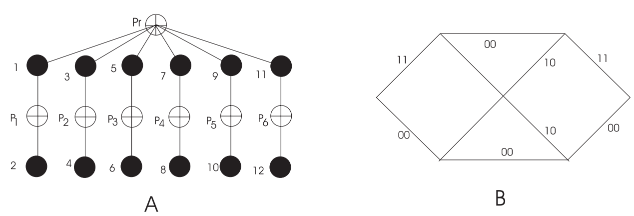

Figure 2: **A**- The minimal Tanner graph of linear block code C_0 with generator and check matrices M_0 and H_0, respectively, given by (2). **B**- The minimal 3-section trellis diagram of the parity space with generator matrix M_{PS} given by (3).

Ignoring the root parity p_r, this parity space is a $(6, 2)$ linear code and is represented by the 3-section minimal trellis diagram shown in Fig. 2b. This trellis together with the TG in Fig. 2a is called a *Tanner-graph trellis* (TG-T) representation of C.

The TG and the trellis should be in forms that allow low complexity implementation of the Wagner rule and the Viterbi algorithm, respectively. In this regard, the TTG should be similar to the MTG of the code $(n, n-1, 2) \otimes (m, 1, m)$ for some m and n. The MTG of the code $(n, n-1, 2) \otimes (m, 1, m)$ has n branches each of length m. Due to this property, these codes are called *uniform generalized single parity* (UGSP) codes [7]. The TG in Fig. 2 is the MTG of the $(6,5,2) \otimes (2,1,2)$ UGSP code.

A block code with a MTD such as the trellis shown inFig. 2b is called a multilevel parity code. To be precise, if $A_i, i = 1, \ldots, n$ is a sequence of matrices of rank r over F_q then the code C with the following generator matrix M is called an r-level parity check code,

$$M = \begin{bmatrix} A_1 & A_2 & & & & \\ & A_2 & A_3 & & & \\ & & \ddots & \ddots & & \\ & & & A_{n-2} & A_{n-1} & \\ & & & & A_{n-1} & A_n \end{bmatrix}. \quad (4)$$

For instance, the previous $(6,2)$ parity space code is a 1-level binary parity code. Although the Viterbi decoding algorithm is usually applied when decoding a code using its MTD, the multilevel parity codes can be decoded more efficiently by applying some elimination techniques on their MTDs [7, 22].

2.2 The $(24,12,8)$ and $(32,16,8)$ quadratic codes

In [26], the $(24,12,8)$ Golay Code $\mathcal{G}_{24}$, represented by generator matrix $M_{24} = [(6,5,2) \otimes (4,1,4)] + M_1$ with

$$M_1 = \begin{bmatrix} 1100 & 1100 & 1100 & 1100 & 0000 & 0000 \\ 1010 & 1010 & 1010 & 1010 & 0000 & 0000 \\ 0000 & 0000 & 1100 & 1100 & 1100 & 1100 \\ 0000 & 0000 & 1010 & 1010 & 1010 & 1010 \\ 0110 & 0000 & 0110 & 0000 & 1100 & 1010 \\ 0000 & 1100 & 0000 & 1100 & 0101 & 0110 \\ 1000 & 1000 & 1000 & 1000 & 1000 & 0111 \end{bmatrix} \quad (5)$$

was decoded by projecting $\mathcal{G}_{24}$ on the quaternary hexacode H_6 given by

$$H_6 = \begin{bmatrix} 1 & 0 & 0 & 1 & \bar{\omega} & \omega \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (6)$$

The 5-dimensional UGSP code $(6,5,2) \otimes (4,1,4)$ is a maximal acyclic subcode of $\mathcal{G}_{24}$ and has the MTG shown in Fig. 3a. The 3-section MTD of the corresponding parity space M_{PS} consists of eight structurally identical parallel trellises, one of which is given in Fig. 3b.

Following the work of Vardy and Be'ery [26], a similar two level decoding technique was presented by Yuan *et al.* [28] for decoding the $(32,16,8)$ QR code by projecting the code onto

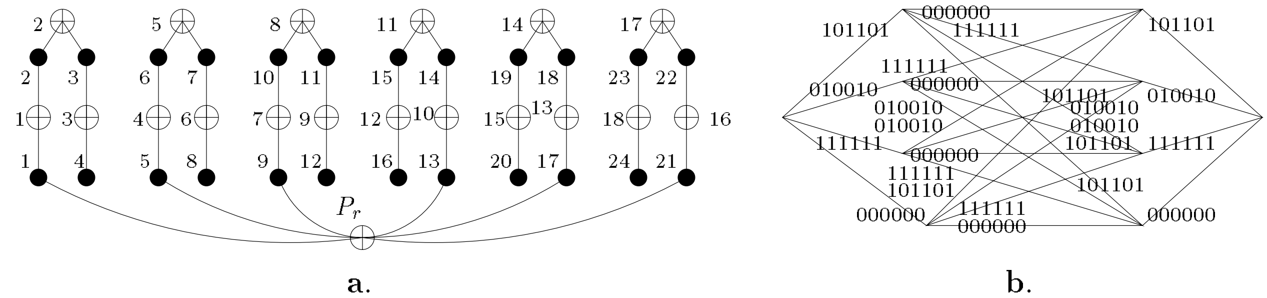

Figure 3: **a.** 5-dimensional acyclic subcode $(6,5,2) \otimes (4,1,4)$ of the Golay code $\mathcal{G}_{24}$. **b.** One of the 8 parallel 3-section regular subtrellises of the trellis associated with the corresponding parity space M_{PS}.

the $(8,4,4)$ quaternary code with generator matrix

$$G_b = \begin{bmatrix} 1 & 0 & 0 & 0 & \bar{\omega} & \omega & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & \bar{\omega} & 1 & \omega \\ 0 & 0 & 1 & 0 & \omega & 1 & \omega & 0 \\ 0 & 0 & 0 & 1 & \bar{\omega} & 0 & \bar{\omega} & 1 \end{bmatrix}. \tag{7}$$

In [28] the representation of the code specified by the generator matrix $M_{32} := [(8,7,2) \otimes (4,1,4)] + M_1$ was employed where

$$M_1 = \begin{bmatrix} 0101 & 0000 & 0110 & 1010 & 1100 & 0000 & 0000 & 0000 \\ 0011 & 0000 & 0101 & 0011 & 0110 & 0000 & 0000 & 0000 \\ 0000 & 0101 & 1111 & 1001 & 1010 & 1100 & 0000 & 0000 \\ 0000 & 0011 & 0000 & 1010 & 1100 & 0110 & 0000 & 0000 \\ 0000 & 0000 & 0110 & 0000 & 1100 & 0110 & 1100 & 0000 \\ 0000 & 0000 & 0011 & 0000 & 1010 & 0011 & 1010 & 0000 \\ 0000 & 0000 & 0000 & 0101 & 1100 & 0000 & 0011 & 1010 \\ 0000 & 0000 & 0000 & 0011 & 0110 & 0000 & 1001 & 1100 \\ 0001 & 1000 & 1000 & 0001 & 1000 & 1011 & 1101 & 1000 \end{bmatrix} \tag{8}$$

The UGSP code $(8,7,2) \otimes (4,1,4)$ is a maximal acyclic subcode of the $(32,16,8)$ QR code.

2.3 Pless-type projection

As mentioned previously, the $(24,12,8)$ and $(32,16,8)$ codes have been decoded by projecting them onto quaternary codes [21, 26, 28].

Each element of $F_4 = \{0,\ 1,\ \omega,\ \bar{\omega}\}$(where $\omega^2 = \bar{\omega}$, $\bar{\omega}^2 = \omega$, and $\omega + \bar{\omega} = 1$) can be expressed in four distinct ways as binary linear combinations of the elements of F_4. For instance

$$\begin{aligned} \omega &= 0 \times 0 + 0 \times 1 + 1 \times \omega + 0 \times \bar{\omega} \\ &= 1 \times 0 + 1 \times 1 + 0 \times \omega + 1 \times \bar{\omega} \\ &= 0 \times 0 + 1 \times 1 + 0 \times \omega + 1 \times \bar{\omega} \\ &= 1 \times 0 + 0 \times 1 + 1 \times \omega + 0 \times \bar{\omega}. \end{aligned}$$

Table 1: Even and odd interpretations of the elements of F_4.

0	01	10	10	10	0	10	01	01	01
1	01	10	01	01	1	01	10	01	01
ω	01	01	10	01	ω	01	01	10	01
$\bar{\omega}$	01	01	01	10	$\bar{\omega}$	01	01	01	10
	0	1	ω	$\bar{\omega}$		0	1	ω	$\bar{\omega}$
Even Interpretations					Odd Interpretations				

This induces an equally sized partition of F_2^4 which is shown below. A representations is called even or odd depending on the number of nonzero components of the associated binary 4-tuple. Each element of F_4 has two even interpretations and two odd, as shown in Table 1. In this way a binary sequence of length $4m$ may be considered as a quaternary sequence of length m.

Definition 1 (Pless-type projection) Let C_2 and C_4 be binary and quaternary linear codes of lengths $4m$ and m, respectively. According to [21, 26, 28], C_4 is called the Pless-type projection of the binary linear code C_2 if:
(1) The quaternary expression of any codeword of C_2 is a codeword of C_4;
(2) The components of any projection are all even or all odd interpretations;
(3) In the quaternary projection of a codeword of C_2, the number of nonzero coefficients of $0 \in F_4$ is even (odd) if the components of the corresponding projection are even (odd) interpretations.

For instance in the matrix M_1 given by (5) the last row is a quaternary sequence of length 6 all of whose components are odd, while the other rows are sequences of length 6 with even components. As for the third condition, the number of components starting with '1' in the last row is 5 (odd number) and for the other rows this number is even.

The projection of $\mathcal{G}_{24}$ on the hexacode H_6 satisfies the properties of Definition 1, but the projection of the $(32, 16, 8)$ QR code [28] on the quaternary code with generator matrix G_b does not satisfy the third condition. This can be noticed from the last row of matrix M_1 given by (8) derived from Theorem 1 of [28]. This does not significantly affect the decoding process. Due to this failure the root parity of the associated TG-T takes only '0' in contrast with that of $\mathcal{G}_{24}$ in which the root parity is '1' for half of the cosets and '0' for the other half.

As the first two conditions of Definition 1 are enough for implementation of the decoding method given in [21, 26, 28], we may remove the third condition and use the following definition.

Definition 2 (Projection) A linear code C_q, q a power of 2, over F_q is called the projection of the binary linear code C_2 if:

(1) The expression of any codeword of C_2 in terms of sequences over F_q is a codeword of C_q;

(2) The components of any projection are all even or all odd interpretation.

2.4 The Connection between the TG-T representation and the Pless-type projection

It has been shown in [7] that the decoding methods given in [21, 26, 28] lie in the framework of efficient use of the TG-T representation of the codes. When decoding using a TG-T representation of the code, both the maximal acyclic subcode and the MTD of the associated parity space have crucial roles. As shown in [7], the existence of the UGSP $(6,5,2) \otimes\ (4,1,4)$ and $(8,7,2) \otimes\ (4,1,4)$ codes in the $(24,12,8)$ and $(32,16,8)$ codes, respectively, have made it possible to define their Pless-type projections and to decode them efficiently.

The existence of a Pless-type projection for the $(48,24,12)$ QR code code has been an open problem in the literature [26, 28]. The remainder of this paper will consider the structure of this code and solve this problem.

3 The $(48, 24, 12)$ quadratic residue code

In this section we show that the $(48,24,12)$ QR code does not have a Pless-type projection and that there are three, up to equivalence, $(48,24,10)$ codes having this property. A decoding method for the $(48,24,12)$ code is provided which shows a 15% improvement compared to the trellis based decoding method presented in [20].

The $(48, 24, 12)$ QR code, denoted by C_{48}, has a generator matrix M_{48}, given by

$$\left[\begin{array}{cccc|cccc}
111111 & 111111 & 000000 & 000000 & 000000 & 000000 & 000000 & 000000 \\
000000 & 111111 & 111111 & 000000 & 000000 & 000000 & 000000 & 000000 \\
000000 & 000000 & 111111 & 111111 & 000000 & 000000 & 000000 & 000000 \\
000000 & 000000 & 000000 & 000000 & 111111 & 111111 & 000000 & 000000 \\
000000 & 000000 & 000000 & 000000 & 000000 & 111111 & 111111 & 000000 \\
000000 & 000000 & 000000 & 000000 & 000000 & 000000 & 111111 & 111111 \\
\hline
000111 & 111000 & 000111 & 111000 & & & & \\
 & & 100001 & 111001 & 010111 & 010010 & & \\
 & & 010010 & 111010 & 100111 & 100100 & & \\
 & & & & 000111 & 111000 & 000111 & 111000 \\
011100 & 011111 & 011010 & 011001 & 011000 & 000000 & & \\
001110 & 110111 & 010011 & 110010 & 110000 & 000000 & & \\
000011 & 011011 & 010001 & 001100 & 000011 & 000000 & & \\
000001 & 001110 & 001101 & 101001 & 000110 & 000000 & & \\
000000 & 010111 & 000101 & 100111 & 101110 & 110000 & & \\
000000 & 001111 & 000110 & 010111 & 110011 & 011000 & & \\
 & & 001001 & 010111 & 010100 & 010100 & 011000 & 000000 \\
 & & 000011 & 011110 & 001001 & 110011 & 010111 & 000000 \\
 & & 000000 & 110000 & 001100 & 010100 & 011011 & 110000 \\
 & & 000000 & 011000 & 011010 & 110010 & 001110 & 100000 \\
 & & 000000 & 000101 & 001010 & 110011 & 101000 & 010010 \\
 & & 000000 & 000011 & 010100 & 010001 & 001111 & 100100 \\
000000 & 000110 & 001010 & 010111 & 100111 & 000110 & 010100 & 000000 \\
000000 & 000011 & 100111 & 100111 & 111100 & 010111 & 000110 & 000000
\end{array}\right] \tag{9}$$

where the blank spaces denote zeros. The $(48, 6, 12)$ code C_{48}^6 with generator M_{48}^6, given by the first six rows of M_{48}, has parity matrix $H_{48}^6 := H \oplus H$ where

$$H = (4, 1, 4) \otimes [100000] + \mathcal{I}_4 \otimes (6, 5, 2).$$

M_{48} is divided into two halves by the vertical line, and each half generates the same $(24, 20, 2)$ code. It is clear that the 4 six-bit sections of any codeword of the $(24, 20, 2)$ code are either all of even weight or all of odd weight. Therefore, the $(24, 20, 2)$ satisfies the conditions of Definition 2. Accordingly, the structure of M_{48} is suitable for decoding C_{48} in a way similar to that given for the $(24, 12, 8)$ and $(32, 16, 8)$ QR codes. However, instead of F_4, we require F_{16} generated by $\alpha^4 + \alpha + 1 = 0$. The set F_2^6 is partitioned into 16 sets, each of which contains 4 elements, and each set is associated with an element of F_{16}, as shown below. Each element of F_{16} has four distinct representations as binary combination of the elements 0, 1, α, α^2, α^3, and α^{12}. Each element has two odd and two even interpretations, as shown in Table 2.

Let M_{48}^{18} denote the matrix with rows consisting of the last 18 rows of M_{48}. The parity space

Table 2: Even and odd interpretations of the elements of F_{16}.

	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	10	01	01	01	01	10	10	10	10	10	10	01	10	10	01	10
1	01	10	01	01	01	10	01	01	01	10	01	10	10	10	10	10
α	01	01	10	01	01	10	10	01	01	01	10	10	01	10	01	01
α^2	01	01	01	10	01	01	10	10	10	10	01	10	01	10	10	01
α^3	01	01	01	01	10	01	01	10	01	01	10	01	01	10	10	10
α^{12}	01	01	01	01	01	01	01	01	10	01	01	01	10	01	01	01

Odd Interpretations

	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	01	10	10	10	10	01	01	01	01	01	01	10	01	01	10	01
1	01	10	01	01	01	10	01	01	01	10	01	10	10	10	10	10
α	01	01	10	01	01	10	10	01	01	01	10	10	01	10	01	01
α^2	01	01	01	10	01	01	10	10	10	10	01	10	01	10	10	01
α^3	01	01	01	01	10	01	01	10	01	01	10	01	01	10	10	10
α^{12}	01	01	01	01	01	01	01	01	10	01	01	01	10	01	01	01

Even Interpretations

$H_{48}^{6} M_{48}^{18}$ is given by

P_{r1}	$P_{b1,1}$	$P_{b2,1}$	$P_{b3,1}$	$P_{b4,1}$	P_{r2}	$P_{b1,2}$	$P_{b2,2}$	$P_{b3,2}$	$P_{b4,2}$
0	00100	00100	00100	00100	0				
0			10001	00101	0	11100	11011		
1			11011	00111	0	10100	10110		
0					0	00100	00100	00100	00100
0	10010	10000	10111	10101	0	10100	00000		
0	01001	01100	11010	01011	1	01000	00000		
0	00010	10110	11001	01010	0	00010	00000		
1	00001	01001	01011	11101	0	00101	00000		
1	00000	11100	00111	10100	0	11001	01000		
0	00000	01000	00101	11100	1	01010	10100		
0			01101	11100	0	11110	11110	10100	00000
0			00010	10001	1	01101	01010	11100	00000
1			00000	01000	1	01010	11110	10110	01000
0			00000	10100	0	10111	01011	01001	10000
0			00000	00111	0	01111	01010	11100	11011
0			00000	00010	1	11110	11001	01000	10110
0	00000	00101	01111	11100	1	10100	00101	11110	00000
0	00000	00010	10100	10100	1	00010	11100	00101	00000

. (10)

The MTG of C_{48}^{6} is given in Fig. 4. P_{r1} and P_{r2} are the values of the two root parities, while the binary length 5 sequence $P_{bi,j}$ gives the values of the check nodes on the ith branch of the jth tree. In the decoding process, a Gray code with 32 elements is employed.

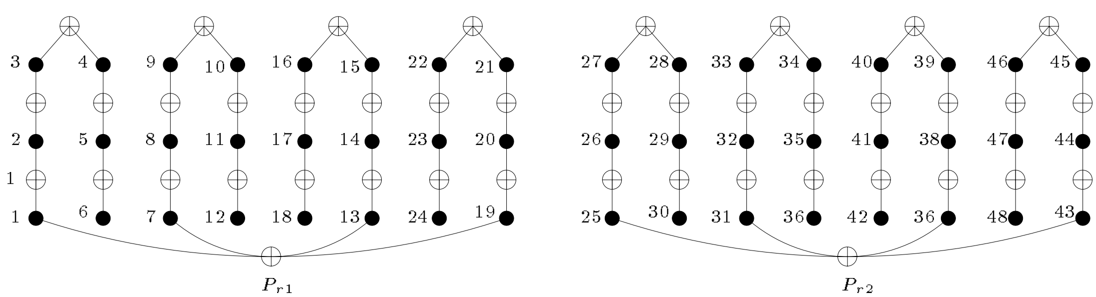

Figure 4: The minimal Tanner graph of the code with generator matrix M_{48}^{6}.

Since the two root parities P_{r1} and P_{r2} are not independent, the decoding process becomes complex when dealing with the parity space given by (10). As a result, we get only about a 15% improvement in complexity compared with trellis decoding of [20].

At this stage, we consider another interesting generator matrix of the $(48, 24, 12)$ code. The theory of tail-biting trellises has been given in [3]. A tail-biting 16-state trellis representation for the $(24, 12, 8)$ Golay code $\mathcal{G}_{24}$ was given in [3], and this can be used to construct a Type II convolutional code. Following this work, Koetter and Vardy constructed a tail-biting generator matrix G_{KV} for the $(48, 24, 12)$ code which appeared in [18]. This generator matrix has been used to construct a Type II convolutional code [18]. Although G_{KV} is important to the construction of Type II convolutional codes and tail-biting trellises, it is not better than M_{48} as far as decoding complexity is concerned. A 3-section trellis diagram representing G_{KV} consists of 256 distinct structurally identical subtrellises, each of which has 256 states at time indices 1 and 2. A 3-section trellis corresponding to generator M_{48} consists of only 64 structurally identical subtrellises each having 256 states at time indices 1 and 2. Thus the state complexity of M_{48} is less than that of G_{KV}. Another difference between these two matrices is that G_{KV} does not have a large subcode with a uniform acyclic Tanner graph. This is necessary for efficient decoding using the technique given in [7].

Suppose a version of the $(48, 24, 12)$ QR code includes the UGSP code $C_{48}^{7} := (8, 7, 2) \otimes (6, 1, 6)$ with generator matrix denoted by M_0. Denote the code given by this representation as C. Further, suppose that the projection of C on F_{16}^{8} produces a length 8 linear code B over F_{16} such that B is the projection of C in the sense of Definition 2. We show that B is an $(8, 4, 5)$ MDS code and the projection is not a Pless-type projection, in the sense of Definition 1. In other words, C does not have a Pless-type projection on F_{16}^{8}.

Lemma 1 The base code B has minimum Hamming distance 5.

Proof We show that the existence of a codeword of weight 4 results in a contradiction. Assume C has a generator matrix $M_0 + M_c$ where M_0 generates $(8, 7, 2) \otimes (6, 1, 6)$. To show that B has minimum Hamming distance 5, it is enough to show that no row of M_c may contain more than 3 blocks of zeros of length 6, considering the rows as sequences of blocks of length 8 with each block having 6 bits. Suppose there is a row, say r, in M_c consisting of 4 nonzero and 4 zero blocks. Since B has been assumed to be the projection of C (in the sense of Definition 2), the 4 nonzero blocks of r must have even binary Hamming weight. On the other hand, it follows from the minimum Hamming distance of C and the structure of M_0 that the row r must have Hamming weight 12. Therefore, the nonzero blocks of r have one of the 3 combinations

$$\{(6, 2, 2, 2), \quad (6, 4, 2), \quad (4, 4, 2, 2)\},$$

in terms of their Hamming binary weights. However, all these combinations result in a contradiction considering the structure of M_0 and the minimum Hamming distance of C. The same argument rejects the existence of any nonzero vector of weight $w < 4$ in the base code B. ■

Theorem 1 The base code B over F_{16} is an $(8, 4, 5)$ code.

Proof since F_{16} is a vector space of dimension 4 over F_2 with basis $\{1,\ \alpha,\ \alpha^2,\ \alpha^3\}$, any row of a generator matrix of B corresponds to 4 rows of M_c. The matrix M_c has 17 rows. One row is left to produce the codewords with blocks of odd binary Hamming weight. The remaining 16 rows have to be partitioned into groups of 4 rows, with each group associated with a row of the generator matrix of B. Therefore, B has dimension 4. ■

From Theorem 1, the base code B is an MDS code and hence has a generator matrix of the form $M = [I_4|A_{4\times4}]$, where any square sub-matrix of the 4×4 matrix $A_{4\times4}$ is nonsingular. We have already assumed that B is the projection of C in the sense of Definition 2. It is shown below that B is not the Pless-type projection of C.

Theorem 2 The base code B is not a Pless-type projection of C.

Proof Suppose to the contrary that B is a Pless-type projection. To determine the 4×4 matrix $A_{4\times4}$ consider the codewords of weight 5. Let

$$S_1 = \left\{1, \alpha, \alpha^2, \alpha^3, \alpha^{12}\right\},$$

and

$$S_2 = \left\{\alpha^4, \alpha^5, \cdots, \alpha^{11}, \alpha^{13}, \alpha^{14}\right\}.$$

Consider a codeword c of weight 5 in the base code B with nonzero components $S(c) = \{a_1, a_2, a_3, a_4, a_5\}$. Applying the even interpretation on this set and considering each component as a binary vector of length 6 and weight 2 (see the even and odd interpretations), the projection of c is a binary sequence of length 48 and Hamming weight 10, which is a contradiction. Therefore from Statement 3 of Definition 1, a necessary condition for c to be a codeword of C is

$$|S(c) \bigcap S_1| = 2k+1, \quad 0 \leq k \leq 2. \tag{11}$$

Under this condition, any binary representation of c satisfying statements $2-3$ of Definition 1 will result in a binary sequence of Hamming weight at least 12. Conversely, if $|S(c) \bigcap S_1| = 2k$ then there exists a binary representation for c of Hamming weight 10 that satisfies statements $2-3$ of Definition 1.

Each row of the matrix $M = [I_4|A_{4\times4}]$ has Hamming weight 5. It follows from the condition given by (11) that a row r of the matrix M with the set of nonzero components $S(v) = \{1, a_1, a_2, a_3, a_4\}$ must satisfy the condition

$$|S(\beta v) \bigcap S_1| = 2k+1, \quad 0 \leq k \leq 2, \tag{12}$$

where β is a nonzero element of F_{16} and $S(\beta v) = \{\beta, \beta a_1, \beta a_2, \beta a_3, \beta a_4\}$. Under the condition given by (12), a computer search shows that the set $\{a_1, a_2, a_3, a_4\}$ is precisely one of the following sets

$$\begin{array}{ll} 1. & \{\alpha,\ \alpha^2,\ \alpha^9,\ \alpha^{13}\} \\ 2. & \{\alpha,\ \alpha^8,\ \alpha^{12},\ \alpha^{14}\} \\ 3. & \{\alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^{11}\} \\ 4. & \{\alpha^3,\ \alpha^6,\ \alpha^9,\ \alpha^{12}\} \\ 5. & \{\alpha^4,\ \alpha^6,\ \alpha^7,\ \alpha^8\} \\ 6. & \{\alpha^7,\ \alpha^{11},\ \alpha^{13},\ \alpha^{14}\}\,. \end{array} \tag{13}$$

The best $(48,24)$ code obtained with this restriction has minimum Hamming distance 10, and hence B is not a Pless-type projection of C. ■

We now provide a combinatorial definition for the sets given by (13). Let X be a set with v elements, called points, and let Y be a set of subsets of X, called blocks. Following [1], the pair (X,Y) is called a $t-(v,k,\lambda)$ *design* if

(**a**) Every block in Y is of size k;

(**b**) Every t-subset of X is contained in precisely λ blocks.

According to this definition, the set $X := F_{16} - F_4$ (the set of points), together with the six sets given by (13) (the set of blocks), form a $1-(12,4,2)$ design. Note that $F_4 = \{0, 1, \alpha^5, \alpha^{10}\}$. A $1-(v,k,\lambda)$ design is called *tactical configuration* [1].

There are precisely forty-three $(8,4,5)$ codes, up to equivalence, over F_{16} generated by $[I_4|A_{4\times4}]$, where the rows of $A_{4\times4}$ are from $1-(12,4,2)$ design given by (13). Three of these codes generate $(48,24)$ binary codes of minimum distance 10, and the rest produce $(48,24)$ codes of minimum distance 8. These codes are the Pless-type projection of the corresponding $(48,24)$ binary codes. The generator matrices of the $(8,4,5)$ codes producing $(48,24,10)$ codes are $[I_4\ B_i]$ where

$$B_1 = \begin{bmatrix} \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} \\ \alpha^{11} & \alpha^7 & \alpha^{14} & \alpha^{13} \\ \alpha^{13} & \alpha^{14} & \alpha^7 & \alpha^{11} \\ \alpha^{14} & \alpha^{13} & \alpha^{11} & \alpha^7 \end{bmatrix} \quad B_2 = \begin{bmatrix} \alpha & \alpha^8 & \alpha^{12} & \alpha^{14} \\ \alpha^8 & \alpha & \alpha^{14} & \alpha^{12} \\ \alpha^{12} & \alpha^{14} & \alpha & \alpha^8 \\ \alpha^{14} & \alpha^{12} & \alpha^8 & \alpha \end{bmatrix} \quad B_3 = \begin{bmatrix} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^{11} \\ \alpha^3 & \alpha^2 & \alpha^{11} & \alpha^4 \\ \alpha^4 & \alpha^{11} & \alpha^2 & \alpha^3 \\ \alpha^{11} & \alpha^4 & \alpha^3 & \alpha^2 \end{bmatrix}. \tag{14}$$

The corresponding codes are MDS self-dual codes. The weight distributions of the corresponding binary codes are given in Table 3.

Table 3: Weight distributions of the (48,24,10) self-dual codes.

B_1		$B_2, \ B_3$	
Weight	Count	Weight	Count
$0, 48$	1	$0, 48$	1
$10, 38$	576	$10, 38$	768
$12, 36$	10000	$12, 36$	8848
$14, 34$	52416	$14, 34$	54528
$16, 32$	283959	$16, 32$	284727
$18, 30$	822336	$18, 30$	814848
$20, 28$	2116464	$20, 28$	2123760
$22, 26$	3056832	$22, 26$	3062016
24	4092048	24	4078224

The $(48, 24)$ code associated with B_1 has generator matrix $M_0 + M_1$, where M_1 is given by

$$\begin{bmatrix}
010001 & 001111 & 011011 & 011101 & 011000 & 000000 & 000000 & 000000 \\
001111 & 011000 & 000110 & 000101 & 010100 & 000000 & 000000 & 000000 \\
000101 & 010001 & 001001 & 101101 & 110000 & 000000 & 000000 & 000000 \\
000011 & 010010 & 010111 & 100100 & 100010 & 000000 & 000000 & 000000 \\
000000 & 010010 & 011101 & 001001 & 001010 & 001100 & 000000 & 000000 \\
000000 & 001010 & 001001 & 010100 & 100111 & 110000 & 000000 & 000000 \\
000000 & 000101 & 010001 & 000110 & 100100 & 110110 & 000000 & 000000 \\
000000 & 000011 & 010010 & 001010 & 110011 & 101000 & 000000 & 000000 \\
000000 & 000000 & 010111 & 001100 & 001010 & 101101 & 111100 & 000000 \\
000000 & 000000 & 001111 & 011000 & 010100 & 001001 & 001010 & 000000 \\
000000 & 000000 & 000110 & 000011 & 010010 & 100111 & 110000 & 000000 \\
000000 & 000000 & 000011 & 010010 & 011101 & 010100 & 011000 & 000000 \\
000000 & 000000 & 000000 & 010100 & 000101 & 000110 & 100111 & 110000 \\
000000 & 000000 & 000000 & 001010 & 010100 & 000101 & 110011 & 101000 \\
000000 & 000000 & 000000 & 000101 & 000110 & 001100 & 011101 & 010010 \\
000000 & 000000 & 000000 & 000011 & 001010 & 010100 & 111001 & 100100 \\
000001 & 011111 & 100000 & 111000 & 100101 & 101111 & 010011 & 100000
\end{bmatrix}. \tag{15}$$

For this code, the corresponding parity space is given by

$$M_{PS} = \begin{bmatrix} 0 & 11001 & 01000 & 10110 & 10011 & 10100 & 00000 & 00000 & 00000 \\ 0 & 01000 & 10100 & 00101 & 00111 & 11110 & 00000 & 00000 & 00000 \\ 0 & 00111 & 11001 & 01101 & 11011 & 01000 & 00000 & 00000 & 00000 \\ 0 & 00010 & 11011 & 11100 & 10110 & 10011 & 00000 & 00000 & 00000 \\ 0 & 00000 & 11011 & 10011 & 01101 & 01111 & 01010 & 00000 & 00000 \\ 0 & 00000 & 01111 & 01101 & 11110 & 10100 & 01000 & 00000 & 00000 \\ 0 & 00000 & 00111 & 11001 & 00101 & 10110 & 01101 & 00000 & 00000 \\ 0 & 00000 & 00010 & 11011 & 01111 & 01010 & 11100 & 00000 & 00000 \\ 0 & 00000 & 00000 & 11100 & 01010 & 01111 & 11011 & 00010 & 00000 \\ 0 & 00000 & 00000 & 01000 & 10100 & 11110 & 01101 & 01111 & 00000 \\ 0 & 00000 & 00000 & 00101 & 00010 & 11011 & 10100 & 01000 & 00000 \\ 0 & 00000 & 00000 & 00010 & 11011 & 10011 & 11110 & 10100 & 00000 \\ 0 & 00000 & 00000 & 00000 & 11110 & 00111 & 00101 & 10100 & 01000 \\ 0 & 00000 & 00000 & 00000 & 01111 & 11110 & 00111 & 01010 & 11100 \\ 0 & 00000 & 00000 & 00000 & 00111 & 00101 & 01010 & 10011 & 11011 \\ 0 & 00000 & 00000 & 00000 & 00010 & 01111 & 11110 & 00101 & 10110 \\ 1 & 00001 & 10000 & 10000 & 00100 & 10111 & 11000 & 11010 & 10000 \end{bmatrix}. \qquad (16)$$

Now we define a particular trellis form [7] which is useful in analyzing the structure of the parity space given above. Let $\{A_i\}_{i=1}^{6}$ be matrices of the same rank r such that

$$rank \begin{bmatrix} A_2 \\ A_6 \end{bmatrix} = rank \begin{bmatrix} A_3 \\ A_5 \end{bmatrix} = r$$

and

$$rank \begin{bmatrix} A_2 & A_3 \\ A_6 & A_5 \end{bmatrix} = 2r.$$

Consider the linear code C with generator matrix

$$\begin{bmatrix} A_1 & A_2 & A_3 & \\ & A_6 & A_5 & A_4 \end{bmatrix}. \qquad (17)$$

A 4-section MTD T of this code is a 3-section trellis as all rows of the generator are active at time index 2. All three sections of T are complete bipartite graphs and T has 2^r vertices at time indices 1 and 2. At section $1 \leq i \leq 4$, the edge labels of the trellis form $< A_i >$, the space generated by A_i. The main property of T is that any two distinct elements from any two spaces $< A_i >$ and $< A_j >$, $1 \leq i \neq j \leq 4$, determine a unique path of T. Let T be a 4-section trellis whose edge labels at the i-th section, $1 \leq i \leq 4$, form the set S_i. If any two distinct elements from any two sets S_i and S_j, $1 \leq i \neq j \leq 4$, define a unique path of T then we refer to T as a *3-section semi-regular* trellis.

Considering the $(48, 24)$ codes constructed previously, it is obvious from the parity space generator M_{PS} given in (16) that the space generated by the parities of any of the eight branches of the TG has dimension 5. Further, all eight spaces associated with $P_r = 0$ are identical and generated by

$$M = \begin{bmatrix} 10001 \\ 01000 \\ 00101 \\ 00010 \end{bmatrix}.$$

Inspection of M_{PS} with $P_r = 0$ shows that the parity space of any $i \leq 4$ consecutive branches of the TG is $\oplus_1^i M$. The MTD of the parity space consists of two parallel 3-section semi-regular sub-trellises, one for $P_r = 0$ and the other for $P_r = 1$.

Any generator matrix of the (48,24,12) QR code which contains C_{48}^7 can be represented by a uniform ATG with $P_r = 0$, as with the (32,16,8) QR code [7]. It would have a parity space with an MTD consisting of two disjoint 3-section semi-regular trellises, precisely as described above for the (48,24,10) codes. This is because according to Lemma 1 the base code will be an (8,4,5) code. This together with the rich structure of the edge spaces of the parity space of the (48,24,10) codes suggests that the decoding process and the decoding complexity of the three (48,24,10) codes given previously would be precisely the same as for any version of the (48,24,12) QR code which includes C_{48}^7 when the TG of C_{48}^7 is applied. Due to the size and 3-section semi-regular structure of the MTD of the parity space, the worst case decoding complexity of these (48,24,10) codes is about 399000 real operations. This is a 27% improvement over trellis decoding using optimal sectionalization [20].

4 Summary

We have presented a method for ML decoding of the $(48, 24, 12)$ Quadratic Residue Code based on projecting this code onto a subcode with an Acyclic Tanner Graph [7]. Using this projection, the code is represented by a combination of a trellis and a Tanner graph. The best maximum likelihood techniques applied to date in decoding the Hamming codes, Reed-Muller codes, hexacode, and the extended Golay codes are indeed based on this approach [7]. Unlike the $(24, 12, 8)$ Golay code, the $(48, 24, 12)$ code does not have a Pless-construction which has been an open question in the literature [26, 28]. More generally, an optimal $(48, 24)$ binary code having a Pless-type construction has minimum distance 10 and up to equivalence there are only 3 such codes.

Acknowledgment: We would like to thank Mr. A. R. Fazel for his valuable assistance in the computer programming required in Theorem 2.

References

[1] E. F. Assmus Jr, and J. D. Key, "Designs and Their Codes," *Cambridge University Press*, 1993.

[2] L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Infor. Theory*, Vol. 20, Mar. 1974, pp. 284–287.

[3] A. R. Calderbank, G. D. Forney, Jr., and A. Vardy, "Minimal tail-biting trellises: The Golay code and more," *IEEE Trans. Infor. Theory*, Vol. 45, July 1999, pp. 1435–1455.

[4] G. Charbit, H. Manoukian and B. Honary, "Array codes over rings and their trellis decoding," *IEE Proc. Commun.*, Vol. 143, No. 5, Oct. 1996, pp 241–246.

codes,"

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

[6] R. Diestel,"Graph Theory, Second Edition" Springer 2000.

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

[8] 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, No. 3, May 1997, pp. 1040–1052.

[9] T. Etzion, A. Trachtenberg and A. Vardy, "Which codes have cycle-free Tanner graphs?," *IEEE Trans. Inform. Theory*, Vol. 45, Sept. 1999, pp. 2173–2181.

[10] G. D. Forney Jr.,"The Viterbi algorithm," *Proc. IEEE*, Vol. 61, 1973,pp. 268–278.

[11] M. Fossorier and S. Lin, "Computationally efficient soft decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inform. Theory*, Vol. 42, 1996, pp. 738–750.

[12] M. Fossorier and S. Lin, "Generalized coset decoding," *IEEE Trans. Commun.*, Vol. 45, 1997, pp. 393–395.

[13] M. Fossorier and S. Lin, "Chase-type and GMD coset decodings," *IEEE Trans. Commun.*, Vol. 48, 2000, pp. 345–350.

[14] G.D. Forney, Jr., "Coset codes part II: binary lattices and related codes," *IEEE Trans. Inform. Theory*, Vol. 34, Sept. 1988, pp. 1152–1187.

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

[16] B. Honary, L. Kaya, G. Markarian, and M. Darnell, "Maximum-likelihood decoding of array codes with trellis structure," *IEE Proc. Commun,* Vol. 140, Oct. 1993, pp. 340–346.

[17] G.B. Horn and F.R. Kschischang, "On the intractability of permuting a block code to minimize trellis complexity," *IEEE Trans. Inform. Theory*, Vol. 42, Nov. 1996, pp. 2042–2047.

[18] R. Johannesson and P. Stahl, "A note on type II convolutional codes," *IEEE Trans. Inform. Theory*, Vol. 46, July 2000, pp. 1510–1514.

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

[20] A. Lafourcade and A. Vardy, "Optimal sectionalization of a trellis," *IEEE Trans. Inform. Theory*, Vol. 42, May 1996, pp. 689–703.

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

[22] M. Ran and J. Snyders, "Constrained designs for maximum likelihood soft decoding of RM(2,m) and the extended Golay codes," *IEEE Trans. Commun.,* Vol. 43, Feb./March/April 1995, pp. 812–820.

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

[24] V. Sidorenko, G. Markarian and B. Honary, "Minimal trellis design for linear codes based on the Shannon product," *IEEE Trans. Inform. Theory*, Vol. 42, Nov. 1996, pp. 2048–2053.

[25] 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, Sept. 1989, pp. 963–975.

[26] A. Vardy and Y. Be'ery, "More efficient soft decoding of the Golay codes," *IEEE Trans. Inform. Theory*, Vol. 37, May 1991, pp. 667–672.

1996.

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

[28] J. Yuan, C.S. Chen and S. Ma, "Two-level decoding of $(32, 16, 8)$ quadratic residue code," *IEE Proc. I,* Vol. 140, Dec. 1993, pp. 409–414.