Acyclic Tanner Graphs and Maximum-Likelihood Decoding of Linear Block Codes

M. Esmaeili and A. K. Khandani

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1

Technical Report UW-E&CE#98-01

May 4, 1998

Abstract The maximum-likelihood decoding of linear block codes by the Wagner rule decoding is discussed. In this approach, the Wagner rule decoding which has been primarily applied to single parity check codes is employed on acyclic Tanner graphs. Accordingly, a coset decoding equipped with the Wagner rule decoding is applied to the decoding of a code C having a Tanner graph with cycles. A subcode C_1 of C with acyclic Tanner graph is chosen as the base subcode. All cosets of C_1 have the same Tanner graph and are distinguished by their values of parity nodes in the graph. The acyclic Tanner graph of C_1 together with a trellis representation of the space of the parity sequences represent the code C. Efficient use of this graphical presentation provides a unified and systematic approach to several ever best known maximum-likelihood decoding techniques of linear block codes. The hexacode H_6, ternary Golay code $\mathcal{G}_{12}$, Reed-Muller codes, Hamming codes, and the extended quadratic residue codes are discussed.

1 Introduction

The maximum likelihood (ML) soft-decoding complexity of a group code C is one of the main concerns in the application of C. It is believed that appropriate graphical representations of codes will contribute in this regard. The well known graphical models presented for linear codes are trellis diagram [1, 2, 3], Tanner graph (TG) [4], and Tanner-Wiberg-Loeliger graph [5, 6]. While the Viterbi algorithm works with trellis diagrams, there is not any known algorithm working on Tanner graphs (TGs) with cycles. However, the *forward-backward* algorithm [7], including the min-sum and the sum-product algorithms introduced in [4], work on any cycle-free TG, here called *acyclic Tanner graph* (ATG).

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

The single parity (SP) codes are easily decoded by using the Wagner rule [8]. The unique parity node of the corresponding ATG is adjacent with all symbol nodes. In this case, a bit-by-bit hard decision of the received channel output is considered as the transmitted codeword unless the parity is not satisfied in which case the least reliable bit is flipped (inversed). The Wagner rule decoding has been, explicitly or implicitly, applied and generalized by several authors including [9, 10, 11, 12, 13, 14, 15, 16, 17] to the ML decoding of block codes and lattices.

The work of Conway and Sloane [17] has addressed the decoding of binary codes and lattices 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 [18] using the hexacode H_6 and the $(4,2,3)$ tetracode. The general approaches given in these two works have been employed by several authors [19, 20, 21, 22] to introduce some of the ever best known techniques in decoding linear block codes including the $(24,12)$ Golay code [19], the $(32,16)$ extended quadratic residue (QR) code [20], and the second order Reed-Muller codes [22].

Snyders and Be'ery [21] introduced a generalization of the Wagner rule decoding for binary block codes including the Golay codes. Later, their work on the Golay codes was improved substantially by Vardy and Be'ery [19] using Pless construction [18] of these codes together with the Wagner rule. The same approach was taken for decoding of $(32,16)$ QR code [20].

It is natural to think of a generalization of the Wagner rule decoding on codes with connected ATGs by focusing on one of the parity nodes, to be called the root parity node, and then considering the branches leaving the root parity node as the symbol nodes. In short, we can say that any code with connected ATG may be decoded by the Wagner rule decoding. This, together with coset decoding techniques, lead us to the application of the Wagner rule decoding on codes having TGs with cycle.

There are obviously two main parameters involved in this approach. Given a linear block code C, one first needs to determine a relatively large subcode C_0 of C with ATG to reduce the number of cosets. Our experience has shown that always the largest subcode (with the minimum index) results in the minimum overall complexity. The method to deal with the cosets of C_0 for finding the most overall reliable codeword is another important issue. To illustrate this point, in the following, we compare the method of [21] and [19] for the decoding of the Golay codes. These references use the same 5-dimensional subcode of the Golay code $\mathcal{G}_{24}$. In [21], all cosets are decoded independently and then the most likely codeword is chosen while in [19], the final selected codeword is determined without decoding all the cosets. This is the main reason for the reduction in complexity in [19] with respect to [21]. This explains the fact that in any coset decoding of a linear code, the structure of the underlying subcode and the corresponding set of coset leaders have to be applied efficiently in order to achieve the lowest possible decoding complexity.

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 $C_1 \oplus C_2 := \{c_1 c_2 |\ c_1 \in C_1 \text{and } c_2 \in C_2\}$, where $c_1 c_2$ is the concatenation of c_1 and c_2. Ordinary product of two matrices M_1 and M_2 is denoted by $M_1 M_2$.

Consider a linear block code C where a subcode C_0 of C with ATG is used as the base subcode and $C = C_0 + C_c$. Let $M_0^\perp$ denotes a generator matrix of the dual code $C_0^\perp$. The space of the parity nodes, referred to as *the parity space* (PS), is given by generator matrix $M_{PS} := M_0^\perp M_c$, where M_c is a generator matrix of C_c. The ATG of C_0 together with Minimal Trellis Diagram (MTD) of the associated PS are considered as a graphical representation of the code C and are applied in the decoding process. We refer to this representation as a Tanner Graph-Trellis (TG-T) of C.

As it was mentioned the base code C_0 needs to be of high dimension to keep the index low. This refers to the importance of the maximal acyclic subcodes. We will see that although this is a crucial criteria for C_0 but is not enough. Another property of C_0, which has the same importance as the dimension has, is the structure of the corresponding minimal Tanner graph (MTG). To reduce the decoding complexity it is essential to have the number of branches leaving the root parity node as large as possible and that the branches be as similar as possible. That is roughly to say that the set of symbol nodes needs to be partitioned into as many subsets having almost the same cardinality as possible. We refer to this property as the uniformity of the Tanner graph. The class of product codes $(n, n-1, 2) \otimes\ (m, 1, m)$ satisfies this uniformity condition fully for which the corresponding ATG is composed of n branches of length m connected to the root parity.

In all the important cases examined in our work, the base sub-code is of the form $(n, n-$

$1, 2) \otimes\ (m, 1, m)$, $m = \lceil d_{\min}/2 \rceil$ where $d_{\min}$ is the minimum distance of the original code. This results in a minimum distance of $2\lceil d_{\min}/2 \rceil$ for the resulting subcode. This is the minimum possible value for the length of branches in extracting such a subcode from a code of minimum distance $d_{\min}$. Indeed, after this work was completed, we became aware of [23] which completely characterizes the kind of codes that have cycle-free Tanner graphs. Using the Theorem 5 of [23], we conclude that all the base subcodes used in our discussions are indeed maximal. We have an independent proof for the maximality of the extracted subcode for the case of the first order Reed-Muller code which is mentioned in our following discussions.

The structure of the paper is as follows: Section 2 is devoted to the concept of MTG of linear block codes. Some aspects of MTG together with a constructing algorithm is given. Connection between SP codes and ATGs is discussed in Section 3. The ML decoding of linear block codes by using acyclic subcodes and Wagner rule is given in Section 4. In this section, we also introduce a class of codes, to be called *multilevel parity* codes, together with a decoding method for them. Maximal acyclic subcodes and *Uniform Generalized Single Parity* (UGSP) codes are discussed in Section 5. The quaternary hexacode H_6 and the ternary Golay code $\mathcal{G}_{12}$ are presented in Section 6. Reed-Muller codes and Hamming codes are studied in Section 7. The extended QR codes, mainly the $(48, 24, 12)$ code, are examined in Section 8. As a side result, it is shown that the $(48, 24, 12)$ code does not have a Pless type construction.

2 Minimal Tanner Graphs

In this section, we first give a definition of TGs and MTGs. Noting that all MTGs of a code C have the same cycle space rank we will introduce the term *the minimal Tanner graph* for C. An algorithm is given for the construction of parity matrices corresponding with MTGs of C.

2.1 Tanner graph

Tanner graphs were first introduced in [4]. A TG of a linear code C is a bipartite graph obtained from a set of parity check equations representing C. The two sets of vertices are called variable nodes and check nodes. A variable node v is adjacent with a check node u iff the coefficient of the variable corresponding with v is not zero in the check equation corresponding to u.

Example 1 Two TGs of the (4,2) linear code C presented by the parity check matrices

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad H' = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \tag{1}$$

are given by Figure 1.

Note that the number of edges in a TG is the number of ones in the corresponding check matrix H, and the number of vertices is the sum of the rows and columns of H. Therefore, unlike the number of vertices of TGs of a code, the number of edges is not constant as it can be seen from Example 1.

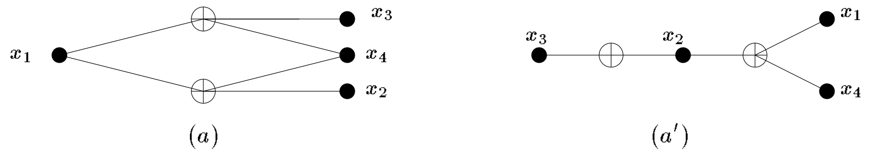

Fig. 1. Two Tanner graphs of the $(4,2)$ linear code C corresponding to the check matrices H and H' given by (1).

2.2 Minimal Tanner graph

Definition 1 (Minimal Tanner Graph) *A TG of a linear code C is called Minimal Tanner Graph (MTG) if the number of edges of TG is the minimum possible among all TGs representing C.*

For the $(4,2)$ code given above the check matrix H' contains the minimum possible ones and hence the TG given by Figure $1(a')$ is a MTG.

The self dual $(8,4,4)$ code C presented by the parity check matrices

$$H = \begin{bmatrix} 11110000 \\ 00111100 \\ 00001111 \\ 01011010 \end{bmatrix}, \quad H' = \begin{bmatrix} 10001110 \\ 01001101 \\ 00101011 \\ 00010111 \end{bmatrix}, \text{ and } \; H'' = \begin{bmatrix} 11001100 \\ 00111100 \\ 00001111 \\ 01011010 \end{bmatrix} \tag{2}$$

has the MTGs given in Figure 2. This shows that a linear code C may have several MTGs.

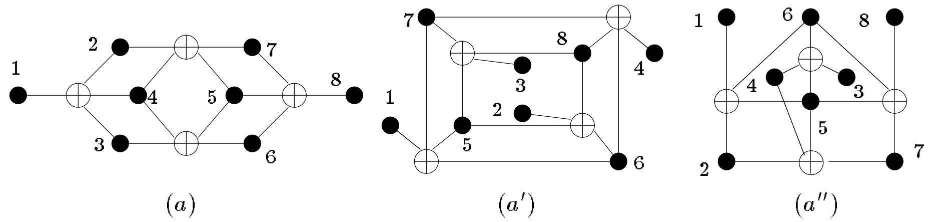

Fig. 2. Three Tanner graphs of the $(8,4,4)$ linear code C corresponding to the check matrices H, H' and H'' given by (2).

One of the matrices associated with a graph G, whose cycles and edges are labeled, is the cycle matrix and the generated space is called *the cycle space.* For a graph G with m cycles and n edges the cycle matrix $[c_{ij}]$ is a binary $m \times n$ binary matrix for which $c_{ij} = 1$ iff the jth edge lies on the ith cycle [24]. A graph G is called connected if any two vertices of G lie on a path.

If G is not connected then each maximal connected subgraph of G is called a component. A connected acyclic graph G is called a *tree* and an unconnected one is referred to as a *forest.* It is known that in a connected graph G with $v(G)$ vertices and $e(G)$ edges, the rank of the cycle matrix is $r(G) = e(G) - v(G) + 1$ [24]. Obviously, for a tree one should have $r(G) = 0$, resulting in $e(G) = v(G) + 1$.

As all MTGs of a linear code C have the same number of edges and vertices, it is followed that the associated cycle spaces have the same rank. For instance, the cycle spaces of three

TGs given in Figure 2 are of dimension $16-12+1=5$. This supports the idea to refer to any MTG of a linear code C as **the minimal Tanner graph** of C.

Let C be an (n,k) linear binary code with an $(n,n-k,d^{\perp})$ code $C^{\perp}$. A trivial lower bound on $e(MTG)$, the number of edges of MTG of C, is

$$e(MTG) := |H_{min}| \geq (n-k)d^{\perp}, \tag{3}$$

where H_{min} stands for any parity check matrix of C with minimum number of nonzero entries. This bound is met by the maximum distance separable (MDS) codes [25], Reed-Muller codes [25], Hamming codes [26], and extended quadratic residue codes.

2.3 Equivalent codes and their common minimal Tanner graphs

Presentation of a linear block code C by a trellis and the concept of MTD is well known in the literature of coding theory. One of the most important differences between the MTG and the MTD of a linear block code is the fact that all equivalent codes have the same MTG, while permutation of coordinates can result in reducing the complexity of a trellis diagram. Indeed, for any generator matrix M and any column permutation operation π on M, we have $\pi(M^{\perp}) = (\pi(M))^{\perp}$, where $\perp$ stands for the dual operation. Figure below is just a graphical expression of this statement.

$$\begin{tikzcd}
M \arrow[r, "\pi"] \arrow[d, "\perp"'] & \pi(M) \arrow[d, "\perp"] \\
M^{\perp} \arrow[r, "\pi"'] & (\pi(M))^{\perp}
\end{tikzcd}$$

Fig. 3. A permutation of coordinates of a linear code C is just a relabeling of the variable nodes of the Tanner graph of C.

2.4 Minimal Tanner basis algorithm

As it was noted the MTG of a linear block code C with the check matrix H corresponds to a version of H which has the minimum possible number of nonzero entries. It turns out, therefore, that only the row operations on H is needed to determine the MTG. In this connection, the main question addresses the existence of a possible algorithm to find the MTG of a given code C. The answer is positive and an algorithm is presented shortly. In parallel with this paper, the MTG of block codes and lattices have been independently addressed by Tarokh [27]. As a result, the two works overlap, ignoring the languages, in the statement of Theorem 1.

Definition 2 (Minimal Tanner Basis) *Let H_{min} denotes any version of the check matrix of C that generates the MTG of C. The set of rows of H_{min} will be referred to as a minimal Tanner basis of C.*

Let the integer sequence $0 = w_o < w_1 < \cdots < w_m$ be the Hamming weight sequence of C. Further, suppose A_i is the set of all codewords of C with Hamming weight w_i. Let C_i be the subcode of C generated by $\cup_{j=1}^{i} A_j$ and $l \leq m$ be the smallest number for which $C_l = C$. A minimal Tanner basis of $C^{\perp}$ may now be introduced.

Theorem 1 *If $B_i \subset \cup_{j=1}^{i} A_j$ is any basis of C_i such that $B_i \subset B_{i+1}$, then B_l is a minimal Tanner basis of $C^{\perp}$.*

Proof It is easy to see that any minimal Tanner basis of $C^{\perp}$ contains a subset of $\cup_{j=1}^{i} A_j$ as a basis of C_i. □

The Minimal Tanner Basis Algorithm: To construct H_{min} from a given check matrix H, we first determine the weight distribution of $C^{\perp}$. Any codeword of $C^{\perp}$ is a combination of the rows of H. One may start the construction of H_{min} by checking the weight of the codewords and taking the first observed codeword of weight w_1 as a matrix M of dimension 1. Suppose now that the dimension of M is increased to h, $1 \leq h < k(C^{\perp})$, where $k(C^{\perp})$ is the dimension of $C^{\perp}$, and there are still codewords of weight w_1 to be checked to see if they are in the row space of M or not. If a codeword c is of weight w_1 and is not in the row space of M then c is added to M as the $(h+1)$th row, otherwise the other unchecked codewords of weight w_1 are examined until either all such codewords are checked or the number of rows of M is reached to $k(C^{\perp})$. If the codewords of weight w_1 are checked and the row space of M is not $C^{\perp}$ then we consider codewords of weight w_2. A codeword of weight w_2 which is not in the row space of M is added to M as a row. Following this procedure and stopping when the rank of M is equal $k(C^{\perp})$ the rows of M is a minimal Tanner basis and $M = H_{min}$.

3 Acyclic Tanner Graphs and Single Parity Codes

A linear code C whose MTG is cycle-free will be referred to as an acyclic code. Since most of optimal codes are not acyclic, for a given code C, the acyclic subcodes are of especial interest. Therefore, we study the structure of acyclic codes in this section.

3.1 Single parity check codes

The $(n, n-1, 2)$ SP code $\mathcal{E}_n$, called also the even weight code, has the simplest nontrivial ATG. Its associated TG consists of one parity node and n symbol nodes all adjacent with the parity node. The SP code $\mathcal{E}_n$ is in fact the cyclic code of length n with generator polynomial $g(x) = 1 + x$. The generator matrix and TG of $\mathcal{E}_6$ are shown in Figure 4 as an example.

110000
011000
001100
000110
000011

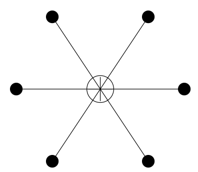

Fig. 4. Generator and Tanner graph of single parity check code $\mathcal{E}_6$.

3.2 Computing the generator matrix of a tree Tanner graph

Let C be an acyclic linear code. If the MTG is forest, then obviously each component of the TG represents a linear subcode of C such that C is the direct-sum of all such subcodes. Therefore, in characterizing acyclic linear codes we may consider only those with tree TG (TTG).

It is natural to think of a code C with TTG as a SP code by focusing on one of the parity nodes, to be called the root parity node, and then considering the branches leaving the root parity node as the symbol nodes. In this way, one can easily construct a generator matrix of C using the associated TTG and generator matrices of SP codes.

To construct the generator matrix of linear code C presented by a TTG, we first choose one of the parity nodes, say p_1. The parity node p_1 and the symbol nodes adjacent with p_1, say $\left\{x_1, \cdots, x_{d(p_1)}\right\}$, where $d(p_1)$ is degree of parity node p_1, form the single parity check code $\mathcal{E}_{d(p_1)}$. In the generator matrix of $\mathcal{E}_{d(p_1)}$ the nonzero entries of the i-th column, corresponding to symbol node x_i, $1 \leq i \leq d(p_1)$ are replaced by a string of ones of length $d(x_i)$, the number of parity nodes adjacent with x_i. The first element of such sequence together with each of the other $d(x_i)-1$ elements of the sequence are applied to construct $d(x_i)-1$ SP codes that may be considered as the shortened codes obtained from C. The construction of generator matrix of C is completed once no parity symbol is left. The resultant generator matrix is in the form that its columns corresponding to the symbol nodes adjacent with a given parity node p represent the SP code introduced by p.

Example 2 Consider the TTGs given in Figure 5. For the first graph the parity node p_1 represents $\mathcal{E}_4$. This corresponds to the first four columns of matrix M_1, ignoring the all zero rows. As the symbol node x_4 is adjacent also with p_2, the nonzero entry of the fourth column is replaced by a two tuple of ones to be used for the construction of $\mathcal{E}_3$, presented by parity node p_2. In this way, we obtain the fifth and the sixth columns of M_1. The resultant matrix M_1 has the property that its first four columns presents $\mathcal{E}_4$, while its last three columns presents $\mathcal{E}_3$.

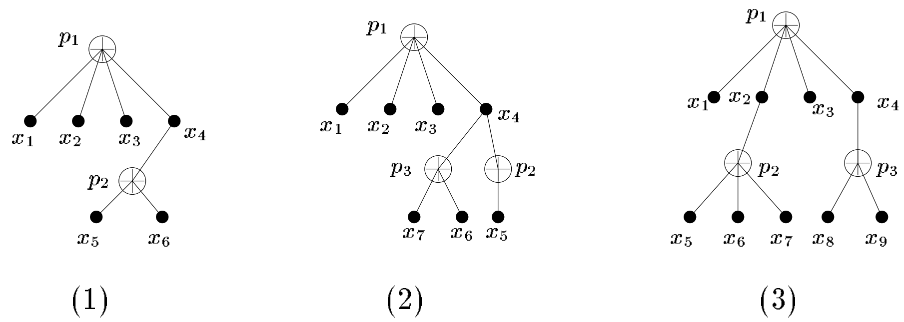

Fig. 5. Tree Tanner graphs illustrating Example 2.

With regard to the second graph, we first consider p_1 and construct the matrix consisting of the first four columns of M_2, ignoring the all zero rows. Then, the nonzero entry of the fourth column is replaced by a three tuple of ones as x_4 is adjacent with two more parity nodes. We now have the 3×6 matrix located at the left top corner of M_2. In this submatrix, the fourth and the fifth columns introduce $\mathcal{E}_2$ corresponding to p_2. Finally, the nonzero entries of the fourth and sixth column of the 3×6 matrix are used to construct $\mathcal{E}_3$ associated with parity node p_3. In doing so we need to add the last row and column to obtain M_2, in which the set of fourth, sixth, and seventh columns introduces $\mathcal{E}_3$.

$$M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad M_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad M_3 = \left[\begin{array}{ccccccccc} 1 & 2 & 5 & 6 & 7 & 3 & 4 & 8 & 9 \\ \hline 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

Similarly, we obtain M_3 the generator matrix of the third graph. First the columns labeled by 1, 2, 3, and 4 are formed. The nonzero entries of column 2 are replaced by a two tuple of ones. The added column is considered as the fifth column. Columns 2 and 5 are used to form $\mathcal{E}_4$ associated with p_2. Hence, we obtain columns 6 and 7. Finally, the nonzero entry of column 4 is used to form $\mathcal{E}_3$. This is done by adding the last two columns.

3.3 Generalized parity codes

Definition 3 (Generalized single parity code) A linear code C having tree Tanner graph G is defined to be a *generalized single parity* (GSP) code if at most one of the parity nodes of G is of degree $m \geq 3$. Such unique node is referred to as the *root parity.*

If all parity nodes of the TTG G are of degree 2 then C is a repetition code. In this case we say the root parity is of degree 2. It is said that G has $m \geq 2$ branches if the root parity is of degree m. The number of symbol nodes on a branch is called the length of the branch.

It is obvious that the generator matrix of a GSP code C with $m \geq 3$ branches is obtained from generator of $(m, m-1, 2)$ SP code $\mathcal{E}_m$ by replacing the nonzero entries of each column of $\mathcal{E}_m$ with a repetition code that has the same length as the corresponding branch of G.

If all the branches are of the same length then C is called a *Uniform Generalized Single Parity* (UGSP) code.

4 Acyclic Tanner Graphs and Maximum Likelihood Decoding

This section is concerned with ML soft-decoding of linear block codes by using acyclic subcodes and applying the Wagner rule. A general description of the method is provided in the first part and then we introduce a class of codes to be called multilevel parity codes. A soft-decoding technique is given for these codes which is more efficient than the Viterbi algorithm. An application of multilevel parity codes and their given decoding technique appears in the process of ML decoding of some well known codes such as quaternary hexacode H_6, (24,12) Golay code, and Reed-Muller codes.

4.1 Maximum likelihood decoding using an acyclic subcode and Wagner rule

Let C_0 with generator matrix M_0 be an acyclic subcode of a given linear code C. The matrix M_0 can be extended to a generator matrix M for C. Suppose $M = M_0 + M_c$ where M_c is a generator matrix for the space of coset representatives.

Let $M_0^\perp$ stands for a generator matrix of $C_0^\perp$, the dual of C_0. Hence $C_0 = \left\{x \mid M_0^\perp x = 0\right\}$. A coset $C_0 + c$ is specified by $C_0 + c = \left\{x + c \middle| \, M_0^\perp x = 0\right\}$. If $M_0^\perp c = b$, then $M_0^\perp(x + c) =$

$M_0^\perp x + M_0^\perp c = b$. Therefore, TG corresponding to the coset $C_0 + c$ is the same as that of C_0 except for the values of the parity nodes, i.e., the sequence of zeros for the parity nodes of C_0 has to be replaced by $b = M_0^\perp c$. It follows that any two cosets are distinguished by the values of their corresponding sequences of parity nodes. The set of all such parity node sequences is a vector space called *the parity space* corresponding to C_0 and is denoted by $PS(C_0)$.

The parity space is given by generator matrix $M_{PS} := M_0^\perp \times M_c$. The ATG of C_0, denoted $G_T(C_0)$, together with $T_{PS}(C)$, a MTD of the parity space in which the root parity is ignored, may be considered as a graphical representation of C, and we call it a Tanner graph-trellis (TG-T) of C. Figures 15, 16, 18, 19, and 20 are examples of such a representation. If C_0 is a maximal acyclic subcode, then the corresponding representation of C will be called *a minimal* TG-T of C, as the associated parity space has the minimum size.

In general, if the root parity in $G_T(C_0)$ is of degree m then we may think of T_{PS} as an m-section trellis diagram. The edge label set at each section of T_{PS} is generated by the parity sequences of the corresponding branch of $G_T(C_0)$. If C is over field F_q then any element of F_q can be the contribution of each edge e of T_{PS} to the root parity. Therefore, an edge e can be thought of as q-tuple $e := (e_1, e_2, \cdots, e_q)$ where e_i is the version of e which provides the root parity with contribution $i \in F_q$. To each version e_i of e, $1 \leq i \leq q$, a confidency value is associated. In the q-tuple of confidency values the maximum confidency and the differences between that and the other values are determined. The differences are referred to as the confidency deviations.

All the edges lying on a path of T_{PS} are originally considered with their preferred version, the version with maximum confidency, unless the root parity is not satisfied in which case a group of edges of the path are changed with their other versions so that the changes causes the least total confidency deviation and satisfies the root parity.

One way to implement the forgoing process is to substitute each edge of T_{PS} by q-tuple $e = (e_1, e_2, \cdots, e_q)$ and then ignore the paths that do not satisfy the root parity. The so obtained trellis, denoted $TT_{PS}(C)$ or simply TT_{PS}, is referred to as the *twisted trellis* of parity space. The trellises shown by Figure 10(c) and Figure 20 are examples of twisted trellises.

One can simply apply the Viterbi algorithm on TT_{PS} and find the optimal path. Depending on the structure of TT_{PS}, however, it may be possible to find the optimal path in a more efficient technique than the Viterbi algorithm. For instance if TT_{PS} consists of disjoint regular subtrellises, to be defined in the next subsection, then it can be decoded efficiently.

4.2 Multilevel parity codes

Definition 4 Let $\{A_i\}_{i=1}^n$ be a sequence of nonzero matrices of rank r over field F_q. The code C over F_q with generator matrix

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

is called an *r-level parity check code.*

Example 3 The following matrices represent two 1-level and 2-level binary parity codes.

$$M = \begin{bmatrix} 11 & 10 & 00 \\ 00 & 10 & 11 \end{bmatrix} \quad M' = \begin{bmatrix} 111 & 100 & \\ 001 & 001 & \\ & 100 & 111 \\ & 001 & 001 \end{bmatrix} \tag{5}$$

Definition 5 [Regular Trellis Diagram] An n-section trellis diagram T is called regular if:

1. The number of vertices of T is the same for all time indices, except for the initial and final time indices that have a single vertex.

2. Each section of the trellis is a complete bipartite graph.

3. The set of label of edges leaving or entering any vertex of a section of T, except for the first and last sections, is the whole set of edge labels of that section.

The trellises shown by Figures 6(a), 17(a), and 22 are regular quaternary, ternary, and binary trellises, respectively.

The MTD of a SP code of length n over F_q is regular with q states at each time index, except for the initial and final vertices. In general, an r-level parity code over F_q, specified by matrix sequence $\{A_i\}_{i=1}^n$, has an n-section regular trellis diagram with q^r vertices at each time index. This has been indeed the motivation to introduce the term *multilevel parity code.*

4.3 Maximum likelihood soft-decoding of linear block codes containing a multilevel parity code

The Viterbi algorithm is a common tool when decoding a code using a trellis. For multilevel parity codes, however, we can apply a much more efficient technique. A linear block code C containing an r-level parity code has a trellis diagram consisting of structurally identical parallel subtrellises each of which is a regular trellis. In each of the regular trellises an optimal path is found and then a comparison among the obtained paths determines the decoder output. Therefore, we may just focus on the decoding process of a given r-level parity code C over F_q.

At each section of the n-section regular trellis T of C there are q^r distinct edge labels. The corresponding q^r confidency values are determined and sorted. If the edges with maximum confidency constitute a path in T then that path is the optimal path. If this is not the case then all n paths containing $n-1$ edges with maximum confidency are determined and among them the best is specified. After that, all the n nonmaximal edges of these n paths are deleted from T as the best paths containing such edges are indeed the obtained paths containing $n-1$ edges with maximum confidency values. The second step is to find the paths containing $n-2$ edges with maximum confidency among the remained paths after the deletions in step one. The best path among the so obtained paths is determined. If e_1 and e_2 are the two nonmaximal edges of one of such paths then all other paths containing these two edges are deleted. The third step is to deal with the remaining paths that have $n-3$ edges with maximum confidency. This process is continued till no path is left. A comparison among the candidates of the mentioned groups of paths gives the decoder output.

Example 4 Consider the single parity code C over F_4 given by generator matrix

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \tag{6}$$

It has regular trellis diagram shown in Figure 6. We have to find a path of the trellis with the

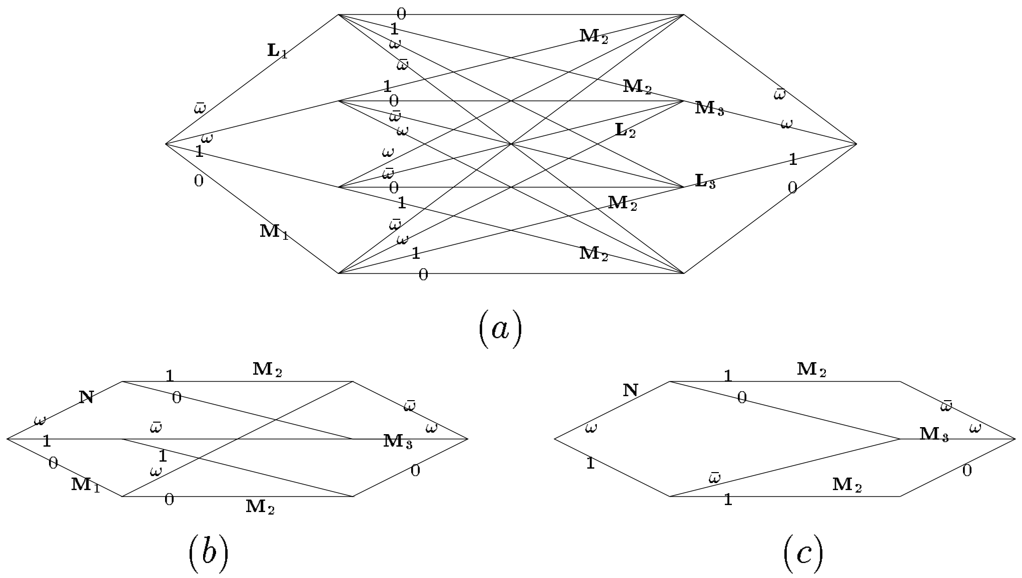

Fig. 6. (a)- A regular trellis diagram representing the 2-dimensional single parity code C over F_4 with generator matrix given by (6). (b)- The trellis obtained from trellis (a) by deleting the edges labeled with X_1, X_2, and X_3. (c)- The trellis obtained from trellis (b) by deleting paths containing the edge labeled with M_1.

maximum possible of confidency. Let M_i and M'_i denote the maximum and second maximum values, not necessarily distinct, among the four confidency numbers associated with the i-th section of the trellis.

The computations of finding M_i and M'_i along with the differences between M_i and the other three confidency numbers of the same section requires at most 5 real operations. Therefore, the complexity of this step is 15 real operations. If the edges corresponding with M_1, M_2, and M_3 form a path in the trellis then it is the best choice. Suppose this is not the case and consider the paths of the trellis including two edges with maximum confidency, say the edges with confidency labels $L_1M_2M_3$, $M_1L_2M_3$, and $M_1M_2L_3$. Two real operations is required to determine the winner of these three paths based on the difference between their total confidency and the number $M := M_1+M_2+M_3$. These three paths are the best among the paths including any edge with confidency labels L_1, L_2, and L_3. Therefore, the paths including such edges are deleted from the trellis and this results in the trellis shown by Figure 6(b).

Now consider $N := max\,\{M'_1,\ M'_2,\ M'_3\}$ and without loss of generality suppose $N = M'_1$. This requires 2 real operations. If $N = L_1$ then the path with confidency label $L_1M_2M_3$ would be the best. Assume $N \neq L_1$. It is easy to see that in this case the paths including the edge with confidency label M_1 could be deleted and we are left with the trellis shown by Figure 6(c).

In this trellis 5 real operations is required to determine the winner based on total confidency deviation from $M = M_1 + M_2 + M_3$. Between the two survived paths one operation is needed to find the winner. Hence C is decoded by at most $15 + 2 + 2 + 5 + 1 = 25$ real operations. Decoding of C by the Viterbi algorithm requires 35 real operations.

4.4 3-Section semiregular trellis

In dealing with decoding of ternary $(12, 6, 6)$ Golay code, $(32, 16, 8)$ and $(48, 24, 12)$ QR codes we encounter a special form of trellis which is worth to describe at this point.

Let $\{A_i\}_{i=1}^{6}$ be matrices of the same rank r such that

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

Consider linear code C with generator matrix

$$\begin{bmatrix} A_1 & A_2 & A_3 & \\ & A_6 & A_5 & A_4 \end{bmatrix} \tag{7}$$

A 4-section MTD T of this code is indeed 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 q^r vertices at time indices 1 and 2.

At section $1 \le i \le 4$ 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 $< A_j >$, $1 \le i \ne j \le 4$, determine a unique path of T.

Let in general T be a 4-section trellis whose edge labels at the i-th section, $1 \le i \le 4$, form set S_i. If any two distinct elements from any two sets S_i and S_j, $1 \le i \ne j \le 4$, define a unique path of T then we refer to T as a *3-section semiregular* trellis.

Example 5 The ternary generator matrix below

$$\begin{bmatrix} 22 & 22 & 22 & 00 \\ 00 & 22 & 11 & 11 \\ 20 & 21 & 21 & 20 \end{bmatrix}$$

has a MTD consisting of three structurally identical parallel subtrellises each of which is a 3-section semiregular trellis. The trellis corresponding to the subcode specified by the first two rows of the generator is given in Figure 16(b).

5 Maximal Acyclic Subcodes

5.1 Distinct maximal acyclic subcodes

The maximal acyclic subcode of a code have the advantage of minimizing the number of cosets. However, the number of cosets does not necessarily reflect the decoding complexity. Another involved factor is the structure of the chosen acyclic subcode. If the TG has a poor structure, from the decoding complexity point of view, then the non-maximal acyclic subcodes might worth to be examined. In general, the more well structured the Tanner graph the lower

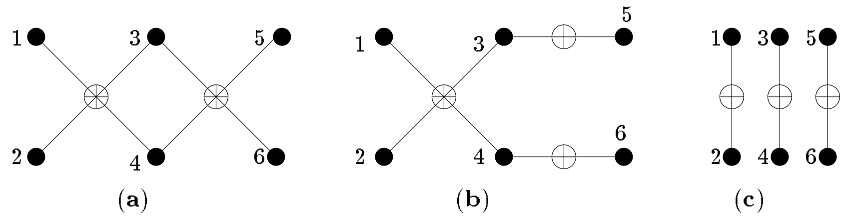

Fig. 7. (a)- A minimal tanner graph; (b),(c)- Two maximal acyclic subcodes of the code with specified by graph (a).

the decoding complexity.

A (6,4,2) code. The code with MTG displayed by Figure 7(a) have two distinct maximal subcodes with TGs shown in Figure 7(b) and Figure 7(c). The code C represented by Figure 7(a) can be decoded by either of the two given ATGs. While decoding complexity, the total required real operations, associated with Figure 7(c) is 11 for any input sequence for decoder, there exist nine cases with decoding complexities 7,9,13,9,13,12,10,14, and 14 if C is decoded using the other graph. The average decoding complexity of C by applying Figure 7(b) is $101/9 = 11.22$. This shows that, from both the top complexity and the average complexity point of view, the uniform maximal subcode is superior to the nonuniform maximal one.

A (12,8,3) code. The (12,8,3) code C_{12} specified by parity matrix H has MTG given in Figure 8.

$$H = \begin{bmatrix} 111011001000 \\ 110100110100 \\ 101110100010 \\ 011101010001 \end{bmatrix} \tag{8}$$

A 5-dimensional maximal acyclic subcode C' of C_{12} is given by parity matrix H'. This subcode has $G_T(C')$ shown by Figure 9.

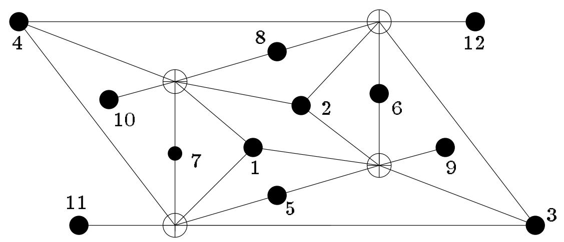

Fig. 8. The minimal Tanner graph of (12,8,3) code with parity matrix H given in (8).

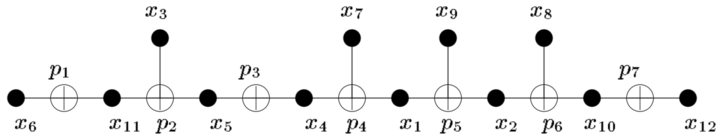

Fig. 9. Tanner graph associated with parity matrix H'.

As it is apparent from the graph, the parity node p_4 is the best option to be considered as the root parity. Applying this graph and considering p_4 as the root parity, the code C_{12} is decoded by about 150 real operations. The main problem with this graph is the fact that from three branches leaving p_4 one branch is too short compared with the other two branches.

$$H' = \begin{bmatrix} 000110000000 \\ 001010000010 \\ 100100100000 \\ 110000001000 \\ 010000010100 \\ 000001000010 \\ 000000000101 \end{bmatrix} \qquad H'' = \begin{bmatrix} 001011001011 \\ 010000000001 \\ 001100000000 \\ 000010100000 \\ 000001010000 \\ 000000001100 \\ 100000000010 \end{bmatrix}$$

On the other hand, the parity check matrix H'' presents a 5-dimensional UGSP subcode C'' of C_{12}. It has $G_T(C'')$ given in Figure 10(a). The corresponding parity space is

$$M_{PS} = \left[\begin{array}{cccc} P_r & P_{1,2} & P_{3,4} & P_{5,6} \\ \hline 1 & 11 & 10 & 00 \\ 0 & 01 & 11 & 10 \\ 1 & 00 & 10 & 11 \end{array}\right]$$

The trellis $T_{PS}(C'')$ given by Figure 10(b) represents the space of parities $\{P_1, \cdots, P_6\}$. The impact of the root parity P_r has changed trellis (b) into the twisted trellis (c). The twisted trellis (c) consists of two disjoint regular subtrellises. Using this trellis and applying the decoding technique given for regular trellises, C_{12} is decoded by at most 48 real operations.

Comparing with the 5-dimensional subcode given by the check matrix H', we see that it is indeed the number of branches leaving the root parity P_r and the uniformity of those branches that has reduced the decoding complexity substantially.

5.2 The maximal acyclic subcode problem

The determination of maximal subcodes with ATGs of a given code C seems to be a quite challenging problem. To find such a subcode, the dual space of C has to be extended which in turn results in the removal of the cycles of the MTG of C by adding new constraints to the parity check matrix. Few observations are presented in the following:

Consider the MTG given in Figure 11. To remove the cycles, one may add two new constraints $x_1 + x_{10} = 0$ and $x_3 + x_{12} = 0$, displayed by the two dot-lines in the figure. However, the cycles can be removed by only one extra constraint, for instance $x_8 + x_9 = 0$. In this MTG, the removal of any of the three parities located in the right and left side of the graph results in a graph with cycle space of rank 1 while the removal of any of the two parities located in the center part leads to a cycle free graph. It seems natural to work with the parities whose removal has the most decrement effect on the rank of the cycle space. However, as it is observed, the two displayed cuts on the two central parities have different impacts on opening the cycles. While the upper cut opens a cycle of length 6, the other one opens a cycle of length 8. By opening the latter cycle from either of the two central parities, the shorter cycle is affected consequently, but the larger cycle is not opened when the cut originally opens the short cycle. This trend seems to be general and starting from a parity node with the most impact on the cycle space, one should try to find a cut with the most possible immediate impact on the longer cycles incident with that parity node.

A vertex v of a connected graph G is called a cut-node if $G - v$, the graph obtained from G by removing vertex v and the edges adjacent with v, is a disconnected graph. A

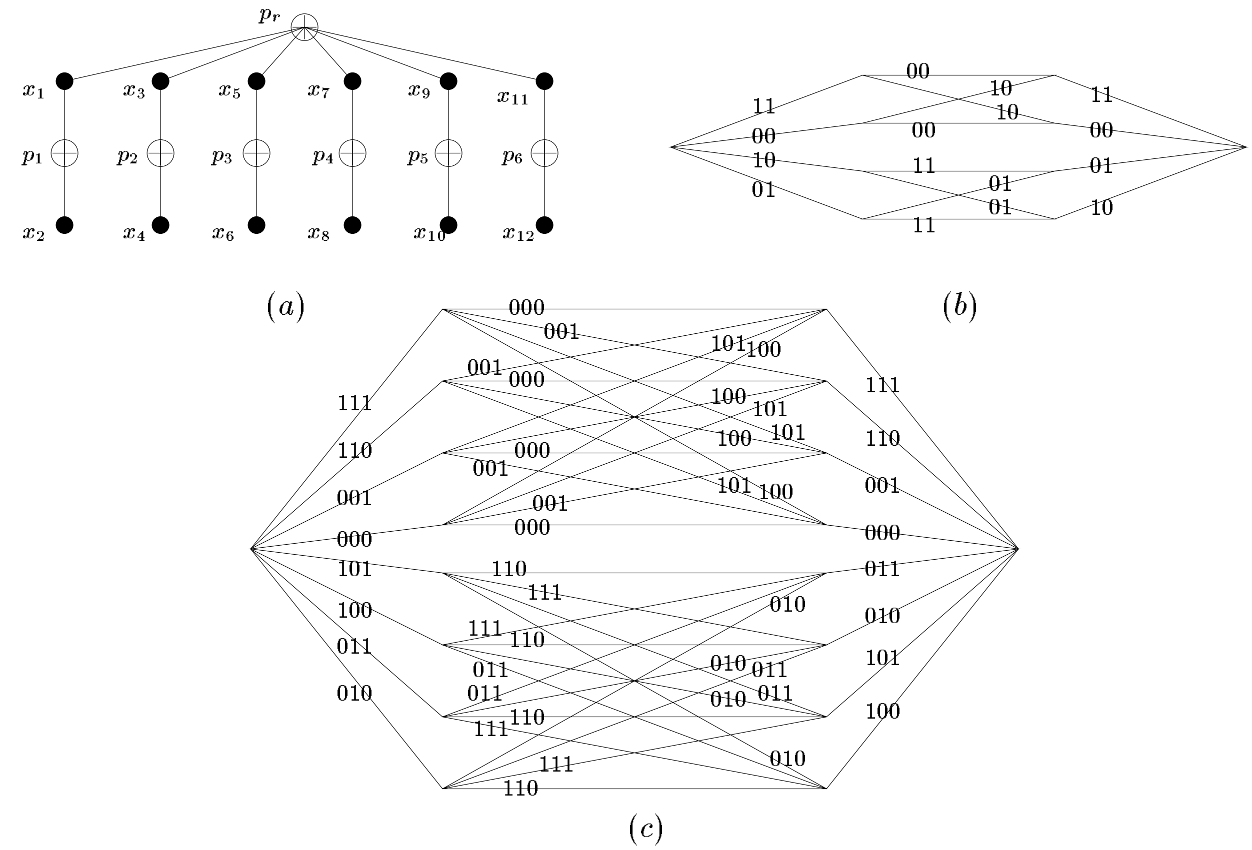

Fig. 10. (a)- Tanner graphs associated with parity matrix H''. (b)- Minimal trellis diagram of parity space when the root parity P_r is ignored. (c)- Twisted regular trellis diagram representing paths satisfying the root parity.

schematic representation in both matrix and graphical forms is given by Figure 12 for parity and symbol cut-nodes in a MTG. The blank parts of the matrices are covered by zeros and each large submatrix is referred to as a block of the associated cut-node. The thin submatrices, representing a row in part (a) and a column in part (b), display the associated parity and symbol cut-nodes, respectively.

The matrices clearly explain that any two cycles in two distinct blocks do not annihilate each other. Therefore, if there are t non-tree blocks among the blocks corresponding to a parity cut-node then at least $t-1$ new parities are required for opening the cycles. These new parities could be obtained by partitioning the row presenting the parity cut-node. Consider, for instance, the MTG given by Figure 13 that includes a parity cut-node with two non-tree blocks. In this case, even separation of the blocks is not enough and two new parities are required. It should be mentioned here that the parity nodes of degree 2, such as $x_1 + x_2 = 0$ in Figure 13, have no impact on the cycle space and are ignored.

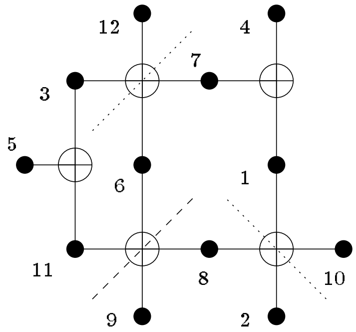

Fig. 11. A minimal Tanner graph whose cycles are removed by adding one parity to the check parities.

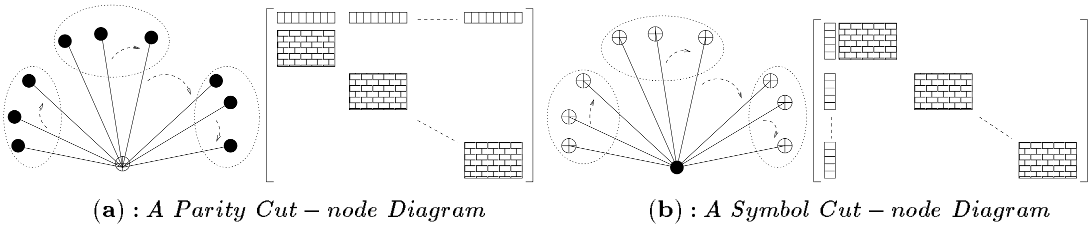

Fig. 12. A matrix and graph representation of parity and symbol cut-nodes in a Tanner graph.

6 The Hexacode H_6 and $(12, 6, 6)$ Ternary Golay Code

6.1 The hexacode H_6

The $(6, 3, 4)$ quaternary hexacode H_6 has generator matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \bar{\omega} & \omega \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Interchanging the last two columns of the matrix, we obtain the generator matrix of the dual code. Based on this and the fact that the code is MDS, we obtain the MTG of H_6 given in Figure 14. The edge labels are the variable coefficients. For instance, for the variables touching the second parity equation, we have $x_2 + x_4 + \bar{\omega}x_5 + \omega x_6 = 0$.
Consider the 2-dimensional UGSP subcode of the hexacode with generator and parity matrices M_0 and $M_0^{\perp}$, respectively.

$$M_0 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad M_0^{\perp} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

The corresponding MTG is a tree, shown in Figure 15 in which $P_r P_1 P_2 P_3 = 0000$ and the edge labels are 1.
The hexacode is the union of 4 cosets of the given subcode and the corresponding four sequences of $P_r P_1 P_2 P_3$ are the elements of the 1-dimensional space generated by $\omega 111$, i.e.:

$$P_r P_1 P_2 P_3 \in \{0000, \omega 111, \bar{\omega}\omega\omega\omega, 1\bar{\omega}\bar{\omega}\bar{\omega}\}\,.$$

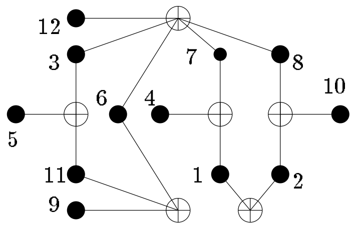

Fig. 13. A MTG with a parity cut-node introducing two non-tree blocks.

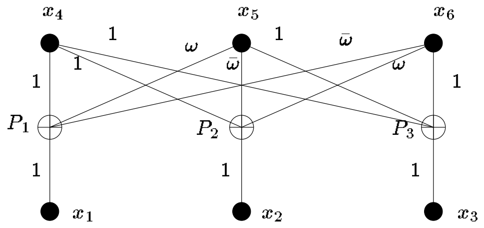

Fig. 14. The minimal Tanner graph of the hexacode H_6.

These 4 cosets are applied in a maximum likelihood soft-decoding technique of the code. Let $(r_1, r_2, r_3, r_4, r_5, r_6)$ be the received output channel. Four real numbers $p(r_i|\alpha_j)$, $\alpha_j \in GF(4)$, are associated with each r_i, $1 \le i \le 6$, and hence a sequence of 24 real numbers is the input of the decoder.

In each of the 4 cosets the best candidate is selected and then a comparison among the 4 candidates determines the decoder output. We briefly discuss the process of finding the best candidate of one of the cosets, for instance $P_r P_1 P_2 P_3 = 0000$. For this coset, we have $x_i = x_{2i}$, $1 \le i \le 3$, and $x_2 + x_4 + x_6 = 0$. Therefore, 12 operations is required to determine the confidency accumulation of all possible choices of (x_i, x_{2i}), $1 \le i \le 3$. The symbol x_{2i} hereafter is denoted by X_{2i} equipped with the total confidency of the couple (x_i, x_{2i}). Thus X_{2i} corresponds with 4 total confidency values, one confidency for each value of X_{2i}, and we are left with the condition $X_2 + X_4 + X_6 = 0$. All 16 possible solutions of this equation are represented by the trellis shown in Figure 6(a).

According to our discussion in Example 4, at most $12 + 25 + 2 = 39$ real operations are required to determine the confidency the winner path of this coset. The final winner, therefore, is found by at most $39 \times 4 + 3 = 159$ operations.

6.2 The ternary Golay code $\mathcal{G}_{12}$

The ternary $(12, 6, 6)$ Golay code $\mathcal{G}_{12}$ has generator matrix M_{12} given by (9).

$$M_{12} = \begin{bmatrix} 111 & 111 & 000 & 000 \\ 000 & 111 & 222 & 000 \\ 000 & 000 & 111 & 111 \\ 020 & 001 & 010 & 221 \\ 020 & 121 & 001 & 020 \\ 002 & 211 & 010 & 020 \end{bmatrix} \qquad M_{PS} = \begin{bmatrix} P_r & P_{1,2} & P_{3,4} & P_{5,6} & P_{7,8} \\ \hline 1 & 22 & 22 & 22 & 00 \\ 0 & 20 & 21 & 21 & 20 \\ 0 & 00 & 22 & 11 & 11 \end{bmatrix} \tag{9}$$

The 3-dimensional UGSP subcode C_0 generated by the first three rows of M_{12} has dual space presented by TTG shown in Figure 16 in which all parity nodes are zero. The corresponding

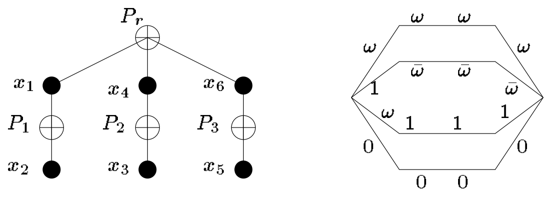

Fig. 15. A minimal Tanner graph-trellis of the hexacode H_6.

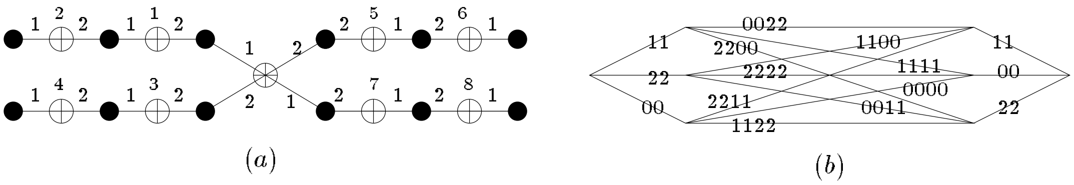

Fig. 16. A Tanner graph-trellis representation of the the ternary Golay code. (a): The minimal Tanner graph of C_0; (b): One of three parallel semiregular subtrellises of the parity space.

parity space is given by the generator matrix M_{PS}. Let r be a received channel output. One approach in decoding the code is to find a closest codeword to r in each coset and then choose the best one among the 27 obtained codewords. We briefly discuss this approach in finding the winner codeword in the coset C_0. For this coset, we may consider the TTG as parity $X_1 + 2X_2 + 2X_3 + X_4 = 0$, where X_i represents three symbol nodes of the ith branch of the TTG. Therefore, X_i is an element of $\{000,\ 111,\ 222\}$. The computation of confidency of X_is for all 27 cosets requires $(9 + 9 \times 3)4 = 144$ real operations. Among the three confidency values of X_i the maximum M_i and the second maximum, M_i', are determined by 2 operations and a total of 8 operations in each coset. Thus, such computations requires a total of $8 \times 27 = 216$ real operations. The codewords of the coset C_0, that is the solutions of $X_1 + 2X_2 + 2X_3 + X_4 = 0$, are specified by generator matrix

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

and are shown by Figure 17(a). If the edges labeled by M_1, M_2, M_3, and M_4 form a path of

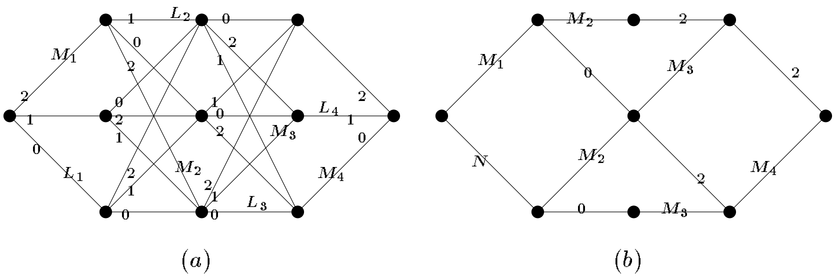

Fig. 17. A regular trellis representation of 3-dimensional UGSP subcode C_0 of $\mathcal{G}_{12}$.

the trellis then it is the winner one, otherwise, there are four paths in the trellis each of which contains three of such edges. Suppose such paths are labeled by $M_1M_2M_3L_4$, $M_1M_2L_3M_4$,

$M_1L_2M_3M_4$, and $L_1M_2M_3M_4$. We may then ignore all paths containing any edge labeled by L_i, $1 \le i \le 4$. This gives the trellis of Figure 17(b). Let $N := max\,\{M_1',\ M_2',\ M_3',\ M_4'\}$, and without loss of generality suppose $N = M_1'$. It is easy to see that the paths containing the edge labeled by M_1 may be deleted and we just need to consider the labeled paths NM_2M_32, $N0M_3M_4$, and NM_22M_4. The total confidency of the winner of these 7 remaining paths is determined by at most 10 real operations. Therefore, the code is decoded by at most $144 + 216 + 270 + 26 = 656$ real operations, as reported in [21].

Instead of working on each coset and then choosing the best codeword, we could apply the MTD of the parity space M_{PS} to work on all cosets simultaneously and come up with less operations. This is the same method as implicitly used in [19]. The corresponding trellis consists of four parallel subtrellises one of which is given in Figure 16. In this trellis, the paths beginning with edges labeled by 00, 22, and 11 correspond to the root parity values 0, 1, and 2, respectively.

7 Reed-Muller codes and Hamming codes

In this section, we show that the maximal acyclic subcodes of first order Reed-Muller code, $\mathcal{R}(1,m)$, are of dimension 3. For the general case of $\mathcal{R}(r,m)$ a $(2^{r+1}-1)$-dimensional UGSP subcode is presented. This is a maximal acyclic subcode of $\mathcal{R}(r,m)$.

Let $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ be two n-tuples. The Boolean product of a and b is defined as $ab := (a_1b_1, a_2b_2, \ldots, a_nb_n)$. The product of i n-tuples is called a Boolean product of degree i. For a nonnegative integer m, consider the 2^m-tuples v_0, v_1, …, and v_m such that v_0 has Hamming weight 2^m, and v_i, $1 \le i \le m$, is the concatenation of 2^{m-i} identical blocks of length 2^i, each of which is divided into 2 sub-blocks of length 2^{i-1} such that the first sub-block is the string of all ones, and the second sub-block is the string of all zeros.

Let $0 \le r \le m$, and A be the set consisting of v_0 and all the Boolean products of the elements of $D = \{v_1, v_2, \ldots, v_m\}$ up to degree r. The subspace of $F_{2^{2^m}}$, generated by A is defined as the r-th order Reed-Muller code of length 2^m, and is denoted by $\mathcal{R}(r,m)$.

7.1 First order Reed-Muller codes

Let $\mathcal{R}'(1,m)$ denote the $(m-2)$-dimensional subcode of $\mathcal{R}(1,m)$ generated by $[v_1, v_2, \cdots, v_{m-2}]^t$, where $[\,.\,]^t$ stands for the transpose operation. The matrix G_m^1, the generator matrix of $\mathcal{R}(1,m)$, may be represented by

$$G_m^1 = \begin{bmatrix} G_0(1,m) \\ G_c(1,m) \end{bmatrix} := \begin{bmatrix} (4,3,2) \otimes \mathcal{R}(0,m-2) \\ \mathcal{R}'(1,m) \end{bmatrix}.$$

The dual of $G_0(1,m)$ is $H_0(1,m)$

$$H_0(1,m) := (4,4,1) \otimes \mathcal{R}(m-1,m-2) + \mathcal{R}(0,2) \otimes 10^{2^{m-2}-1}.$$

The parity space is given by generator $M_{PS}(1,m)$

$$M_{PS}(1,m) := H_0(1,m)\mathcal{R}'(1,m) = 0\mathcal{R}(0,2) \otimes M_m,$$

where the 0 beside $\mathcal{R}(0,2)$ denotes a zero column and M_m is defined by

$$M_m := \left[\begin{array}{ccc} 0 & 1 & 0 \\ M_{m-1} & 0 & M_{m-1} \end{array}\right] \quad \text{and} \quad M_3 = 1.$$

It will be shown that $G_0(1,m)$ is a maximal acyclic subcode of $\mathcal{R}(1,m)$.

Example 6 For $m = 4$, we have

$$G_4^1 = \left[\begin{array}{c} G_0(1,4) \\ G_c(1,4) \end{array}\right] = \left[\begin{array}{cccc} 1111 & 1111 & 0000 & 0000 \\ 0000 & 1111 & 1111 & 0000 \\ 0000 & 0000 & 1111 & 1111 \\ \hline 1100 & 1100 & 1100 & 1100 \\ 1010 & 1010 & 1010 & 1010 \end{array}\right];$$

$$H_0(1,4) = [1111] \otimes [1000] + (4,4,1) \otimes \mathcal{R}(1,2);$$

$$M_{PS}(1,4) = \left[\begin{array}{ccccc} P_r & P_{1,2,3} & P_{4,5,6} & P_{7,8,9} & P_{10,11,12} \\ \hline 0 & 010 & 010 & 010 & 010 \\ 0 & 101 & 101 & 101 & 101 \end{array}\right].$$

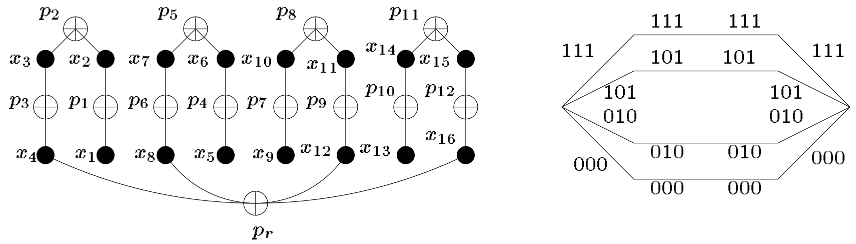

Fig. 18. A minimal Tanner graph-trellis of the $(16,5,8)$ Reed-Muller code.

In the followings, we apply the criteria that a connected graph G with v vertices and e edges is tree iff $e = v - 1$. By *a MTG of a matrix M*, we mean a MTG of a linear code having generator matrix M. The number of edges of MTG of such a code is denoted by $e(M^\perp)$.

Theorem 2 *For any $(n-k)\times n$ matrix M, the MTG of M is acyclic iff the MTG of $(2,1,2)\otimes M$ is acyclic.*

Proof We may assume that M does not present a direct sum code. Hence, we show that the MTG of M is tree iff the MTG of $(2,1,2) \otimes M$ is tree.

$M^\perp$, the dual of M, may be expressed by $M^\perp = X_{k\times k} Y_{k\times(n-k)}$, where $X_{k\times k}$ is invertible. Denoting the square n-dimensional identity matrix by $\mathcal{I}_n$, it is easy to check that

$$[(2,1,2)\otimes M]^\perp = \left[\begin{array}{cccc} 0 & \mathcal{I}_{n-k} & 0 & \mathcal{I}_{n-k} \\ X & Y & 0 & 0 \\ 0 & 0 & X & Y \end{array}\right].$$

It follows that

$$\begin{aligned} [(2,1,2)\otimes M]^\perp &= \left[\begin{array}{cccc} 0 & \mathcal{I}_{n-k} & 0 & \mathcal{I}_{n-k} \\ X & Y & X & Y \\ 0 & 0 & X & Y \end{array}\right] = \left[\begin{array}{cccc} 0 & \mathcal{I}_{n-k} & 0 & \mathcal{I}_{n-k} \\ X & 0 & X & 0 \\ 0 & 0 & X & Y \end{array}\right] \\ &= \left[\begin{array}{cccc} 0 & \mathcal{I}_{n-k} & 0 & \mathcal{I}_{n-k} \\ \mathcal{I}_k & 0 & \mathcal{I}_k & 0 \\ 0 & 0 & X & Y \end{array}\right] = \left[\begin{array}{cc} \mathcal{I}_n & \mathcal{I}_n \\ 0 & M^\perp = XY \end{array}\right]. \end{aligned} \tag{10}$$

It implies that $e([(2,1,2)\otimes M]^\perp) = 2n + e(M^\perp)$ and $e([(2,1,2)\otimes M]^\perp) = 4n-k-1$ iff $e(M^\perp) = 2n-k-1$. $\Box$

The set of Boolean polynomials of degree one given by $D = \{v_1, v_2, \ldots, v_m\}$ defines the simplex code [25], denoted herein by $\mathcal{B}(1,m)$. For instance

$$\mathcal{B}(1,3) = \begin{bmatrix} 11110000 \\ 11001100 \\ 10101010 \end{bmatrix} \equiv \begin{bmatrix} 1111000 \\ 1100110 \\ 1010101 \end{bmatrix}.$$

Lemma 1 *The simplex code $\mathcal{B}(1,m)$ is not acyclic.*

Proof $\mathcal{B}(1,m)$ is the dual of the $(2^m-1, 2^m-m-1, 3)$ Hamming code $\mathcal{H}_m$. Hence, in any matrix H representing $(\mathcal{B}(1,m))^\perp = \mathcal{H}_m$, we have

$$e(H) \geq 3(2^m-m-1) > (2^m-1) + (2^m-m-1) - 1 = \nu - 1, \quad \text{for} \quad m \geq 3,$$

where ν is the number of vertices of the MTG of $\mathcal{B}(1,m)$. It follows that the MTG of $\mathcal{B}(1,m)$, $m \geq 3$, is not a tree. Therefore, $\mathcal{B}(1,m)$ is not acyclic as this code is not a direct sum code $\Box$

Theorem 3 *The maximal acyclic subcodes of $\mathcal{R}(1,m)$ are of dimension three.*

Proof $\mathcal{R}(0,m-2)\otimes\mathcal{R}(1,2)$ is a subcode of $\mathcal{R}(1,m)$ of dimension 3 and its associated MTG is a tree. We show that this dimension may not be increased.

Let C_3 denote any subcode of $\mathcal{B}(1,m)$, $m \geq 3$, of dimension 3. $C_3 + < v_0 >$ is of dimension 4 and is equivalent with $\mathcal{R}(0,m-3)\otimes\mathcal{R}(1,3)$. Since $\mathcal{R}(1,3)$, and hence according to Theorem 2 $\mathcal{R}(0,m-3)\otimes\mathcal{R}(1,3)$, is not acyclic, the same is true $C_3 + < v_0 >$. Suppose C_4 is any subcode of $\mathcal{B}(1,m)$, $m \geq 4$, of dimension 4. C_4 and $C_4 + < v_0 >$ may be expressed by

$$\begin{aligned} C_4 \equiv\ & \mathcal{R}(0,m-4)\otimes\mathcal{B}(1,4) \\ C_4 + < v_0 > \equiv\ & \mathcal{R}(0,m-4)\otimes\mathcal{R}(1,4) \end{aligned} \tag{11}$$

Therefore, C_4 and $C_4 + < v_0 >$ are not acyclic $\mathcal{B}(1,4)$ and $\mathcal{R}(1,4)$ are not acyclic.

The same argument shows that C_n and $C_n + < v_0 >$ are not acyclic, implying that the maximum dimension for any acyclic subcode C of $\mathcal{R}(1,m)$ is 3. $\Box$

Applying the presented minimal TG-T for the first order Reed-Muller codes, the codes $\mathcal{R}(1,3)$, $\mathcal{R}(1,4)$, $\mathcal{R}(1,5)$, and $\mathcal{R}(1,6)$ are decoded by at most 21, 59, 183, and 623 real operations, respectively, versus 23, 94, 278, and 806 operations required in trellis decoding under optimal sectionalizations [28]. Note that in the mentioned minimal TG-T of $\mathcal{R}(1,m)$, the trellis representing the parity space consists of parallel paths as it was the case with the hexacode H_6. In this case, one requires to perform an exhaustive search over all the trellis paths. This means that the trellis can not be exploited for further reduction of the decoding complexity.

7.2 The rth order Reed-Muller codes

The results given for the first order Reed-Muller codes may be generalized. We can now show that the second order Reed-Muller code $\mathcal{R}(2,m)$, $m \geq 3$, includes acyclic subcodes of dimension 7, and the third order Reed-Muller code $\mathcal{R}(3,m)$, $m \geq 4$, includes acyclic subcodes of dimension 15, and in general the rth order Reed-Muller code $\mathcal{R}(r,m)$, $m \geq r+1$, includes acyclic subcodes of dimension $2^{r+1}-1$. The existence of such subcodes are shown below and using Theorem 5 of [23] it can be shown that the presented subcodes are maximal acyclic subcodes.

The code $\mathcal{R}(m-1,m)$ is the dual of $\mathcal{R}(0,m)$ and hence the MTG of $\mathcal{R}(m-1,m)$ is a tree. The code $\mathcal{R}(r,m)$ may be expressed by

$$\mathcal{R}(r,m) = \begin{bmatrix} \mathcal{R}(r-1,m-1) & 0 \\ \mathcal{R}(r,m-1) & \mathcal{R}(r,m-1) \end{bmatrix}.$$

It is followed that $\mathcal{R}(r,m)$ includes $G_0(r,m) := \mathcal{R}(0,m-r-1) \otimes \mathcal{R}(r,r+1)$ as a subcode. This subcode is of dimension $2^{r+1}-1$ and, according to Theorem 2, is acyclic.

Let $H_0(r,m)$ denotes the dual of $G_0(r,m)$ and $PS(r,m)$ stands for the associated parity space. From the foregoing argument and the relation given by (10) the followings are easily derived.

Theorem 4 *For the Reed-Muller code $\mathcal{R}(r,m)$ we have:*

$$H_0(r,m) = \begin{bmatrix} \mathcal{I}_{2^{m-1}} & \mathcal{I}_{2^{m-1}} \\ 0 & H_0(r,m-1) \end{bmatrix}, \quad \text{where} \quad H_0(r,r+1) = \mathcal{R}(0,r+1); \qquad (12)$$

$$M_{PS}(r,m) = \begin{bmatrix} \mathcal{R}(r-1,m-1) & 0 \\ 0 & M_{PS}(r,m-1) \end{bmatrix}, \quad \text{where} \quad M_{PS}(r,r+2) = \mathcal{R}(r-1,r+1)0. \qquad (13)$$

Example 7

$$H_0(2,4) = \begin{bmatrix} \mathcal{I}_8 & \mathcal{I}_8 \\ 0 & 11111111 \end{bmatrix}, \quad \text{and} \quad M_{PS}(2,4) = \mathcal{R}(1,3)0.$$

The associated TTG is shown by Figure 19. The root parity P_r is always zero and the space of the other 8 parities is $\mathcal{R}(1,3)$ as shown by a trellis.

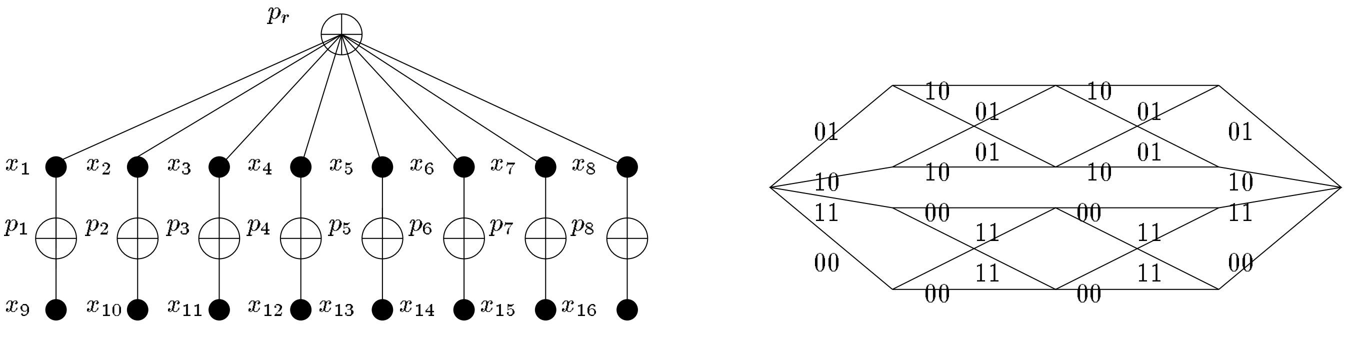

Fig. 19. A Tanner graph-trellis of the $(16,11,4)$ Reed-Muller code.

The trellis in Figure 19 expresses the relation among the set of parities $\{p_1, p_2, \cdots, p_8\}$ and does not reflect the role of the root parity p_r in the TTG of the code. Therefore, it is replaced by a trellis illustrating the role of all parities including the root parity.

Define $P_i := (p_{2i-1}, p_{2i})$ or simply $P_i = p_{2i-1}p_{2i}$, $1 \leq i \leq 4$, and $X_i := x_{2i-1} + x_{2i}$, $1 \leq i \leq 8$. We say $P_i = 0$ (resp. 1) iff $p_{2i-1} + p_{2i} = 0$ (resp. 1)mod 2. By this convention, the $(16, 11, 4)$ code is represented by two copies of the TTG shown by Figure 20, one with $P_i = 0$ and $\sum_{j=1}^{4} X_j = 0$, $1 \leq i \leq 4$, and the other one with $P_i = 1$, and $\sum_{j=1}^{4} X_j = 0$, $1 \leq i \leq 4$. The so obtained TTG, given by Figure 20, will be referred to as a *twisted tree Tanner graph* (TTTG). This graph expresses the TTG of $(16, 11, 4)$ code in terms of the TTG of $(8, 4, 4)$ RM code.

For a fixed value of P_i, X_i has two values, 0 and 1, meaning that

$$\begin{aligned} \{(P_i, X_i)\} &= \{\{(0,0),(0,1)\},\{(1,0),(1,1)\}\} \\ &= \{\{(00,0),(00,1),(11,0),(11,1)\},\{(10,0),(10,1),(01,0),(01,1)\}\}. \end{aligned} \tag{14}$$

For P_i, $1 \leq i \leq 4$, the value of X_i affects the root parity and thus a desirable trellis is a trellis expressing the system $\{P_i X_i\}_{i=1}^{4}$ with $\sum_{i=1}^{4} X_i = 0$. This is the twisted trellis given in Figure 20. The value of X_i is the contribution of P_i to the root parity.

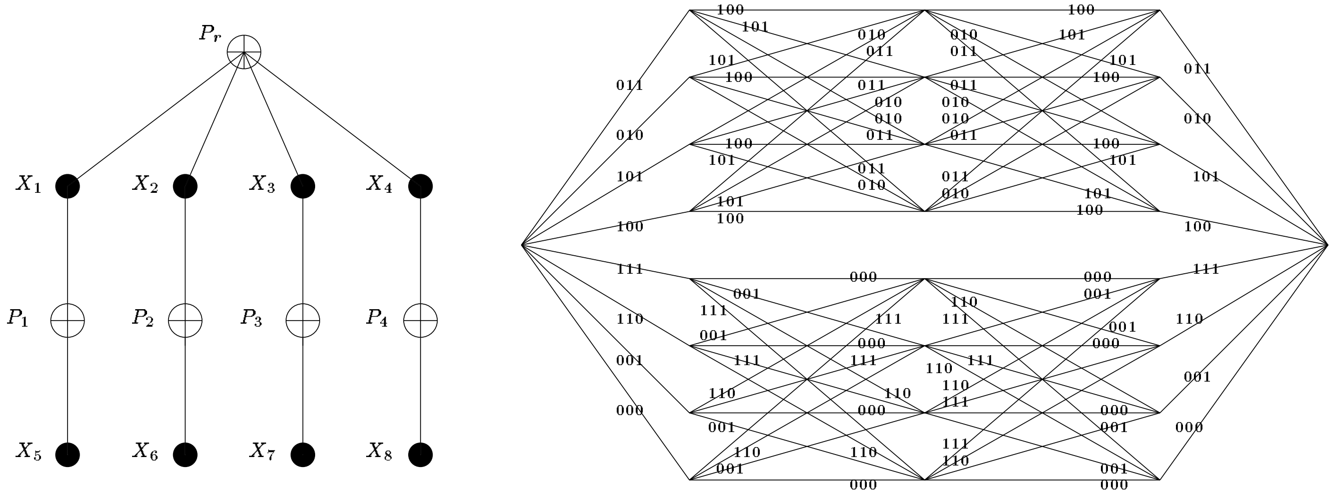

Fig. 20. A twisted Tanner graph-trellis representation of the $(16, 11, 4)$ Reed-Muller code.

The twisted trellis consists of two disjoint regular subtrellises and hence the decoding technique given for the multilevel codes can be applied on this trellis. This trellis has been applied in [22] in the language of design theory. As a result the two works give the same decoding complexity.

7.3 Hamming codes

If a code is obtained by shortening of another code, then it inherits many of the properties of the original code. As an example of such inheritance, an ATG for the shortened code can be obtained by shortening the ATG of the original code.

The $(2^r - 1, 2^r - 1 - r, 3)$ Hamming code $\mathcal{H}_r$, the shortened Reed-Muller code, is obtained from $\mathcal{R}(r-2, r)$ by deleting the last column of the corresponding generator matrix. Therefore, one may apply the results of the previous section to find maximal acyclic subcodes of $\mathcal{H}_r$.
Let $r = 3$. The code $\mathcal{R}(1, 3)$ contains $\mathcal{R}(1, 2)\mathcal{R}(1, 2)$ as a subcode. Deletion of the last column

of the matrix

$$(2,1,2) \otimes \mathcal{R}(1,2) = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

results in the matrix

$$\mathcal{I}_3 1 \mathcal{I}_3 := \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

where the "1" in $\mathcal{I}_3 1 \mathcal{I}_3$ stands for a column of 1's. $\mathcal{I}_3 1 \mathcal{I}_3$ is a subcode of the (7,4,3) Hamming code and its dual code is

$$(\mathcal{I}_3 1 \mathcal{I}_3)^{\perp} = \begin{bmatrix} \mathcal{I}_3 & 0 & \mathcal{I}_3 \\ 0 & 1 & 111 \end{bmatrix}.$$

This shows that the MTG of $\mathcal{I}_3 1 \mathcal{I}_3$ is a tree. The method may be applied to introduce $\mathcal{I}_{2^{r-1}-1} 1 \mathcal{I}_{2^{r-1}-1}$ as an acyclic subcode of $\mathcal{H}_r$.

8 Quadratic residue codes

The extended QR codes seem to be decodable efficiently by determining their maximal acyclic subcodes. We will show that the best techniques which have been applied to decode the $(24,12,8)$ and $(32,16,8)$ extended QR codes [19, 20, 18] are essentially based on the application of TG-T representation of these codes. A discussion on the $(48,24,12)$ QR code is then provided.

In the mentioned works the $(24,12,8)$ and $(32,16,8)$ extended QR codes have been projected on the quaternary codes. There are 16 binary sequences of length 4 and this set is partitioned into 4 subsets of the same cardinality and each subset is associated with an element of the field $F_4 = \{0,\ 1,\ \omega,\ \bar{\omega}\}$, where $\omega^2 = \bar{\omega}$, $\bar{\omega}^2 = \omega$, and $\omega + \bar{\omega} = 1$. In other words, any element of F_4 may be expressed in 4 distinct ways as a binary combination of the elements of F_4. This produces the aforementioned partition. The following gives the partition.

	0	1	ω	$\bar{\omega}$
0	01	10	10	10
1	01	10	01	01
ω	01	01	10	01
$\bar{\omega}$	01	01	01	10

Even interpretation

	0	1	ω	$\bar{\omega}$
0	10	01	01	01
1	01	10	01	01
ω	01	01	10	01
$\bar{\omega}$	01	01	01	10

Odd interpretation

For any element of F_4 an expression is called an even or odd interpretation depending on the number of nonzero coefficients of the expression.

Based on the given correspondence, any binary sequence of length a multiple of 4, say $4m$, may be considered as a quaternary sequence of length m and this leads to projecting of binary codes onto quaternary codes. Let C_2 and C_4 be two binary and quaternary linear codes of length $4m$ and m, respectively. According to [18], we have the following definition as has been given in [19, 20].

Definition 6 (Pless-type projection) The quaternary linear code 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 in even or all in odd interpretation;
(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 in even (odd) interpretation.

8.1 The $(24,12,8)$ Golay code $\mathcal{G}_{24}$

The $(24,12,8)$ Golay Code $\mathcal{G}_{24}$ has generator matrix M_{24} given below. The UGSP code $(6,5,2)\otimes\ (4,1,4)$, the 5-dimensional subcode generated by the first five rows of M_{24}, is a maximal acyclic subcode of $\mathcal{G}_{24}$. The associated TG is given in Figure 21.

$$
M_{24} = \begin{bmatrix}
1111 & 1111 & 0000 & 0000 & 0000 & 0000 \\
0000 & 1111 & 1111 & 0000 & 0000 & 0000 \\
0000 & 0000 & 1111 & 1111 & 0000 & 0000 \\
0000 & 0000 & 0000 & 1111 & 1111 & 0000 \\
0000 & 0000 & 0000 & 0000 & 1111 & 1111 \\
1100 & 1100 & 1100 & 1100 & 0000 & 0000 \\
1010 & 1010 & 1010 & 1010 & 0000 & 0000 \\
0000 & 0000 & 1100 & 1100 & 1100 & 1100 \\
0000 & 0000 & 1010 & 1010 & 1010 & 1010 \\
0110 & 0000 & 0110 & 0000 & 1100 & 1010 \\
0000 & 1100 & 0000 & 1100 & 0101 & 0110 \\
1000 & 1000 & 1000 & 1000 & 1000 & 0111
\end{bmatrix}
$$

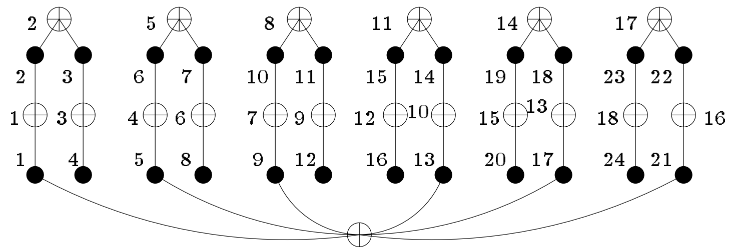

Fig. 21. A 5-dimensional acyclic subcode of the Golay code $\mathcal{G}_{24}$.

The parity space is given by M_{PS}.

$$
M_{PS} = \left[\begin{array}{ccccccc}
P_r & P_{1,2,3} & P_{4,5,6} & P_{7,8,9} & P_{10,11,12} & P_{13,14,15} & P_{16,17,18} \\
\hline
0 & 010 & 010 & 010 & 010 & 000 & 000 \\
0 & 111 & 111 & 111 & 111 & 000 & 000 \\
0 & 000 & 000 & 010 & 010 & 010 & 010 \\
0 & 000 & 000 & 111 & 111 & 111 & 111 \\
0 & 101 & 010 & 101 & 010 & 101 & 010 \\
0 & 000 & 010 & 000 & 010 & 111 & 101 \\
1 & 100 & 100 & 100 & 100 & 100 & 100
\end{array}\right] \tag{15}
$$

The matrix M_{PS} together with TTG in Fig. 21 display the code $\mathcal{G}_{24}$. For $i \in \{1,4,7,10,13,16\}$, the domain of $P_{i,i+1,i+2}$ is the set of all binary 3-tuples. For each value of $P_{i,i+1,i+2}$, two complement solutions are associated to the corresponding 4-tuple variable. For instance, with $P_{1,2,3} = 110$ we have $(x_1,x_2,x_3,x_4) = 0100$, or 1011. These two 4-tuples are the odd interpretations of 1 [19].

Ignoring the root parity P_r, the parity space with generator M_{PS} is represented by a 3-section trellis diagram consisting of 8 parallel regular subtrellises 4 of which correspond to the odd codewords, $P_r = 1$, and the other 4 correspond to the even codewords, $P_r = 0$. One of the subtrellises associated with the first 4 rows of M_{PS} is shown by Figure 22. The decoding steps is as follows:

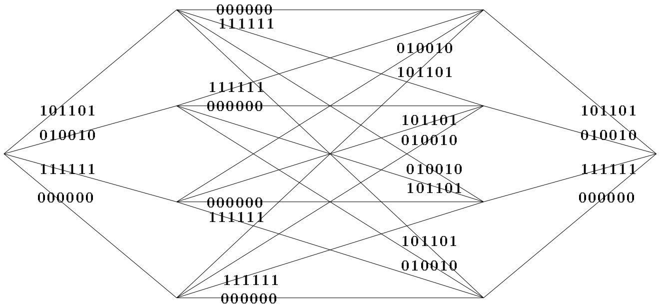

Fig. 22. One of the 8 parallel 3-section regular subtrellises of the trellis associated with the parity space M_{PS} given by (15).

1- For the 4-tuple variable associated with $P_{i,i+1,i+2}$, the eight corresponding confidence values are determined.

2- The confidence value of each path of the trellis is determined by adding the confidence values of its corresponding edges. If the associated codeword does not satisfy the root parity, then the 4-tuple variable with the least confidence value is complemented.

3- Among 128 obtained codewords, the best is chosen. Note that the trellis is applied for finding the best path without computing the confidence values of all 128 codewords.

Applying the same computational techniques used in [19], we come up with the same decoding complexity. This shows that the *decoding of* $\mathcal{G}_{24}$ *by means of its projection on hexacode* H_6 is just another expression of the *decoding by projection of the code on its maximal UGSP subcodes.*

8.2 The $(32, 16, 8)$ quadratic residue code

A two level decoding technique has been presented for the $(32, 16, 8)$ QR code [20]. In [20], the $(8, 4, 4)$ quaternary code B with generator matrix

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

has been considered as the base code.

From the permutation given in Theorem 1 of [20], we have derived generator matrix $M_{32} := [(8,7,2) \otimes (4,1,4)] + M_1$ where M_1 is given below.

$$M_1 = \begin{bmatrix} 0101 & 0000 & 0110 & 1010 & 1100 & 0000 & 0000 & 0000 \\ 0011 & 0000 & 0101 & 0011 & 0110 & 0000 & 0000 & 0000 \\ 0000 & 0101 & 1111 & 1001 & 1010 & 1100 & 0000 & 0000 \\ 0000 & 0011 & 0000 & 1010 & 1100 & 0110 & 0000 & 0000 \\ 0000 & 0000 & 0110 & 0000 & 1100 & 0110 & 1100 & 0000 \\ 0000 & 0000 & 0011 & 0000 & 1010 & 0011 & 1010 & 0000 \\ 0000 & 0000 & 0000 & 0101 & 1100 & 0000 & 0011 & 1010 \\ 0000 & 0000 & 0000 & 0011 & 0110 & 0000 & 1001 & 1100 \\ 0001 & 1000 & 1000 & 0001 & 1000 & 1011 & 1101 & 1000 \end{bmatrix} \quad (16)$$

The last row of this matrix does NOT satisfy the third condition of Definition 6, contrary to the claim made by the authors. The matrix M_{32}, however, satisfies the first two conditions of the definition. From this, we give the following as our definition for projection. Indeed, we remove the third condition from Definition 6.

Definition 7 (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 in even or all in odd interpretation.

By this definition, the quaternary code B with generator matrix G_b is the projection of the $(32, 16, 8)$ QR code. This definition of projection seems to be applicable to any extended (n, k, d) QR code if n is divisible by $d/2$. In fact we conjecture that such a code includes the UGSP code $(2n/d, 2n/d - 1, 2) \otimes\ (d/2, 1, d/2)$.

The UGSP code $(8, 7, 2) \otimes\ (4, 1, 4)$, presenting the first seven rows of M_{32}, has parity matrix H_{32}^7 is as follows:

$$H_{32}^7 := (8, 1, 8) \otimes [1000] + \mathcal{I}_8 \otimes (4, 3, 2).$$

The parity space has generator matrix $M_{PS} := H_{32}^7 M_1$:

$$M_{PS} = \begin{bmatrix} 0 & 111 & 000 & 101 & 111 & 010 & 000 & 000 & 000 \\ 0 & 010 & 000 & 111 & 010 & 101 & 000 & 000 & 000 \\ 0 & 000 & 111 & 000 & 101 & 111 & 010 & 000 & 000 \\ 0 & 000 & 010 & 000 & 111 & 010 & 101 & 000 & 000 \\ 0 & 000 & 000 & 101 & 000 & 010 & 101 & 010 & 000 \\ 0 & 000 & 000 & 010 & 000 & 111 & 010 & 111 & 000 \\ 0 & 000 & 000 & 000 & 111 & 010 & 000 & 010 & 111 \\ 0 & 000 & 000 & 000 & 010 & 101 & 000 & 101 & 010 \\ 0 & 001 & 100 & 100 & 001 & 100 & 110 & 011 & 100 \end{bmatrix} \tag{17}$$

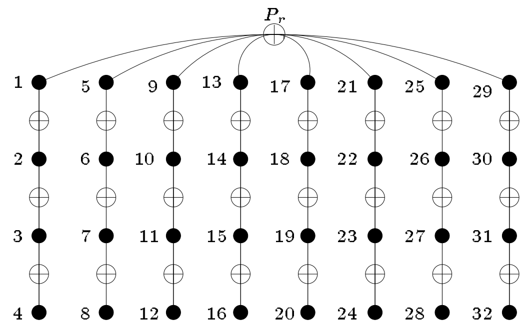

Fig. 23. The minimal Tanner graph of UGSP code $(8, 7, 2) \otimes (4, 1, 4)$.

The corresponding TTG is shown by Figure 23 in which the root parity P_r is always zero, contrary to the TTG of the Golay code $\mathcal{G}_{24}$. This is indeed due to the fact that M_{32} does not satisfy the third condition. From this point of view, this code is the same as the $(32, 16, 8)$ Reed-Muller code that has graphically the same TTG with zero root parity for all cosets.

Ignoring the root parity we see that the parity space has a 3-section trellis consisting of two disjoint semiregular trellises. This is because the deletion of the root parity and the last row of M_{PS} results in generator matrix

$$\begin{bmatrix} A_1 & A_2 & A_3 & \\ & A_6 & A_5 & A_4 \end{bmatrix}$$

where A_i, $1 \leq i \leq 6$, is a 4×6 matrix row-equivalent with matrix

$$\left[\begin{array}{cc} 111 & 000 \\ 010 & 000 \\ 000 & 111 \\ 000 & 010 \end{array}\right]$$

and

$$rank \left[\begin{array}{c} A_2 \\ A_6 \end{array}\right] = rank \left[\begin{array}{c} A_3 \\ A_5 \end{array}\right] = 4 \quad \text{and} \quad rank \left[\begin{array}{cc} A_2 & A_3 \\ A_6 & A_5 \end{array}\right] = 8.$$

The main portion of the decoding complexity is concerned with this 3-section semiregular trellises. Once again our conclusion is that the decoding technique given in [20] for the $(32, 16, 8)$ QR code is in fact nothing but the application of the TG-T of this code with the UGSP subcode $(8, 7, 2) \otimes\ (4, 1, 4)$ as the base code.

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

The generator matrix M_{48}, given by (18), in which the blank spaces are zeros is a presentation of the extended $(48, 24, 12)$ QR code, denoted by C_{48}. The $(48, 6, 12)$ code C_{48}^6 with generator M_{48}^6, the first six rows in M_{48}, have parity matrix $H_{48}^6 := H \oplus H$ where $H = (4, 1, 4) \otimes 100000 + \mathcal{I}_4 \otimes (6, 5, 2)$.

$$\left[\begin{array}{cccc|cccc}
111111 & 111111 & 000000 & 000000 & 000000 & 000000 & 000000 & 000000 \\
000000 & 111111 & 111111 & 000000 & 000000 & 000000 & 000000 & 000000 \\
000000 & 000000 & 111111 & 111111 & 000000 & 000000 & 000000 & 000000 \\
000000 & 000000 & 000000 & 000000 & 111111 & 111111 & 000000 & 000000 \\
000000 & 000000 & 000000 & 000000 & 000000 & 111111 & 111111 & 000000 \\
000000 & 000000 & 000000 & 000000 & 000000 & 000000 & 111111 & 111111 \\
\hline
000111 & 111000 & 000111 & 111000 & & & & \\
 & & 100100 & 111001 & 010111 & 010010 & & \\
 & & 010010 & 111010 & 100111 & 100100 & & \\
 & & & & 000111 & 111000 & 000111 & 111000 \\
011100 & 011111 & 011010 & 011001 & 011000 & 000000 & & \\
001110 & 110111 & 010110 & 110010 & 110000 & 000000 & & \\
000011 & 011011 & 010100 & 001100 & 000011 & 000000 & & \\
000001 & 001110 & 001101 & 101001 & 000110 & 000000 & & \\
000000 & 010111 & 000101 & 100111 & 101110 & 110000 & & \\
000000 & 001111 & 000011 & 010111 & 110011 & 011000 & & \\
 & & 001100 & 010111 & 010100 & 010100 & 011000 & 000000 \\
 & & 000110 & 011110 & 001001 & 110011 & 010111 & 000000 \\
 & & 000000 & 110000 & 001100 & 010100 & 011011 & 110000 \\
 & & 000000 & 011000 & 011010 & 110010 & 001110 & 100000 \\
 & & 000000 & 000101 & 001010 & 110011 & 101000 & 010010 \\
 & & 000000 & 000011 & 010100 & 010001 & 001111 & 100100 \\
000000 & 000110 & 001010 & 010111 & 100111 & 000110 & 010100 & 000000 \\
000000 & 000011 & 100111 & 100111 & 111100 & 010111 & 000110 & 000000
\end{array}\right] \qquad (18)$$

The M_{48} is divided into two parts by the vertical line. The two sides introduce the same $(24, 20, 2)$ code with the generator matrix given by (19). It is clear from this generator matrix that the 4 six-digits 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 conditions of Definition 7. Accordingly, the structure of M_{48} is applicable for decoding C_{48} in a way similar to the $(24, 12, 8)$ and

(32, 16, 8) QR codes.

$$\begin{bmatrix}
110000 & 000000 & 000000 & 000000 \\
011000 & 000000 & 000000 & 000000 \\
001100 & 001100 & 000000 & 000000 \\
000110 & 000000 & 000000 & 000000 \\
000011 & 000000 & 000000 & 000000 \\
000000 & 110000 & 000000 & 000000 \\
000000 & 011000 & 000000 & 000000 \\
000000 & 001100 & 001100 & 000000 \\
000000 & 000110 & 000000 & 000000 \\
000000 & 000011 & 000000 & 000000 \\
000000 & 000000 & 110000 & 000000 \\
000000 & 000000 & 011000 & 000000 \\
000000 & 000000 & 001100 & 001100 \\
000000 & 000000 & 000110 & 000000 \\
000000 & 000000 & 000011 & 000000 \\
000000 & 000000 & 000000 & 110000 \\
000000 & 000000 & 000000 & 011000 \\
000000 & 000000 & 000000 & 000110 \\
000000 & 000000 & 000000 & 000011 \\
000001 & 001110 & 000001 & 100000
\end{bmatrix} \tag{19}$$

Instead of F_4, here, we need F_{16} generated by $\alpha^4 + \alpha + 1 = 0$. The set $(F_2)^6$ is partitioned into 16 sets, each of which containing 4 elements, and each set is associated with an element of F_{16}, as shown below.

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
	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}

Odd Interpretations

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
	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}

Even Interpretations

Let M_{48}^{18} denotes the matrix with the rows consisting of the last 18 rows of M_{48}. The parity space $H_{48}^{6} M_{48}^{18}$ is given by (20).

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			10110	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	11101	01011	1	01000	00000		
0	00010	10110	11110	01010	0	00010	00000		
1	00001	01001	01011	11101	0	00101	00000		
1	00000	11100	00111	10100	0	11001	01000		
0	00000	01000	00010	11100	1	01010	10100		
0			01010	11100	0	11110	11110	10100	00000
0			00101	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

(20)

The MTG of C_{48}^6 is given by Figure 24. 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. The gray code required in the decoding process is given by (21).

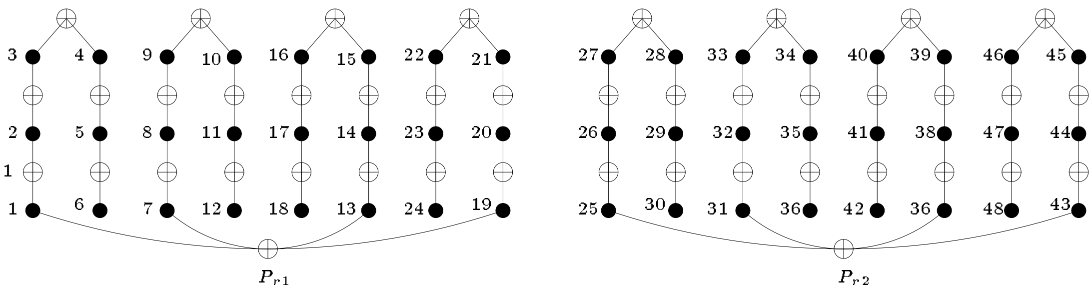

Fig. 24. The minimal Tanner graph of the code with generator matrix M_{48}^6.

1.	$++++++$	9.	$++--++$	17.	$+++--+$	25.	$++-+-+$
2.	$-+++++$	10.	$-+--++$	18.	$-++--+$	26.	$-+-+-+$
3.	$--++++$	11.	$----++$	19.	$--+--+$	27.	$---+-+$
4.	$+-++++$	12.	$+---++$	20.	$+-+--+$	28.	$+--+-+$
5.	$+--+++$	13.	$+-+-++$	21.	$+----+$	29.	$+-++-+$
6.	$---+++$	14.	$--+-++$	22.	$-----+$	30.	$--++-+$
7.	$-+-+++$	15.	$-++-++$	23.	$-+---+$	31.	$-+++-+$
8.	$++-+++$	16.	$+++-++$	24.	$++---+$	32.	$++++-+$

(21)

Since the two root parities P_{r1} and P_{r2} are not independent, the decoding process becomes complex when dealing with parity space given by (20). As a result, we get only about %15 improvement compared with optimal trellis decoding complexity [28].

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 M_0:

$$M_0 := \begin{bmatrix} 111111 & 111111 & 000000 & 000000 & 000000 & 000000 & 000000 & 000000 \\ 000000 & 111111 & 111111 & 000000 & 000000 & 000000 & 000000 & 000000 \\ 000000 & 000000 & 111111 & 111111 & 000000 & 000000 & 000000 & 000000 \\ 000000 & 000000 & 000000 & 111111 & 111111 & 000000 & 000000 & 000000 \\ 000000 & 000000 & 000000 & 000000 & 111111 & 111111 & 000000 & 000000 \\ 000000 & 000000 & 000000 & 000000 & 000000 & 111111 & 111111 & 000000 \\ 000000 & 000000 & 000000 & 000000 & 000000 & 000000 & 111111 & 111111 \end{bmatrix}. \qquad (22)$$

Under such a possible presentation, we denote the code by 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 7. 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 6. In other words, C does not have a Pless-type projection on $(F_{16})^8$.

Lemma 2 *The base code B is of minimum Hamming distance 5.*

Proof We show that the existence of a codeword of weight 4 results in a contradiction. Assume C have generator matrix $M_0 + M_c$ where M_0 is given by (22). To show that B is of 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 block-length 8 and each block of binary length 6. Suppose there is a row, say r, in M_c consisting of 4 nonzero and 4 zero blocks. As B has been assumed to be the projection of C, in the sense of Def. 7, all the 4 nonzero blocks of r must be of 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 is of Hamming weight 12. Therefore, the nonzero blocks of r have one of the 3 combinations $\{(6, 2, 2, 2),\ \ (6, 4, 2),\ \ (4, 4, 2, 2)\}$ in terms of their Hamming binary weights. However, all these three combinations result in contradiction considering the structure of M_0 and 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 5 *The base code B over F_{16} is a $(8, 4, 5)$ code.*

Proof As F_{16} is a vector space of dimension 4 over F_2, with the basis $\{1,\ \alpha,\ \alpha^2,\ \alpha^3\}$, any row of a generator matrix of B corresponds with 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 each group associated with a row of the generator matrix of B. Therefore, B is of dimension 4.□

From Theorem 5 the base code B is a MDS code and hence has a generator matrix of the form $M = [I_4|A_{4\times4}]$, where any square submatrix 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 Def. 7. It is shown that B is not the Pless-type projection of C.

Theorem 6 *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 $A_{4\times4}$ we put a restriction on the codewords of weight 5. Let

$$\begin{aligned} S_1 &= \{1, \alpha, \alpha^2, \alpha^3, \alpha^{12}\}, \\ S_2 &= \{\alpha^4, \alpha^5, \cdots, \alpha^{11}, \alpha^{13}, \alpha^{14}\}. \end{aligned}$$

Consider a codeword c of weight 5 in the base code B with the set of 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 codeword c is given Hamming binary weight 10, i.e. the reflection of c, as a binary sequence of length 48, has Hamming weight 10, which is a contradiction. Therefore, a necessary condition for c to be a codeword of C is:

$$|S(c)\bigcap S_1| = 2k+1, \quad 0 \leq k \leq 2. \tag{23}$$

Each row of the matrix $M = [I_4|A_{4\times 4}]$ has Hamming weight 5. It follows from the condition given by (23) 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:

$$|S(\beta v)\bigcap S_1| = 2k+1, \quad 0 \leq k \leq 2, \tag{24}$$

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 (24), a computer search shows that the set $\{a_1, a_2, a_3, a_4\}$ is precisely one of the following sets:

$$\begin{array}{ll} 1. & \{\alpha,\ \alpha^2,\ \alpha^9,\ \alpha^{13}\} \\ 2. & \{\alpha,\ \alpha^8,\ \alpha^{12},\ \alpha^{14}\} \\ 3. & \{\alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^{11}\} \\ 4. & \{\alpha^3,\ \alpha^6,\ \alpha^9,\ \alpha^{12}\} \\ 5. & \{\alpha^4,\ \alpha^6,\ \alpha^7,\ \alpha^8\} \\ 6. & \{\alpha^7,\ \alpha^{11},\ \alpha^{13},\ \alpha^{14}\}. \end{array} \tag{25}$$

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

It is worth to mention that the sets given by (25) introduce a $1-(12,6,2)$ design and that the elements of F_4, i.e. 1, α^5, and α^{10}, are not appeared in this design.

There are precisely forty three $(8,4,5)$ codes, up to equivalence, over F_{16} with generator $[I_4|A_{4\times 4}]$ where the rows of $A_{4\times 4}$ are from $1-(12,6,2)$ design given by (25). Three of these codes generate $(48,24)$ binary codes of minimum distance 10, and the rest produce $(48,24)$ codes of minimum distance 8. All these codes are the Pless-type projection of their associated $(48,24)$ binary codes. Here are the ones producing $(48,24,10)$ codes:

$$B_1 = \left[I_4 \left| \begin{array}{cccc} \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} \\ \alpha^{11} & \alpha^7 & \alpha^{14} & \alpha^{13} \\ \alpha^{13} & \alpha^{14} & \alpha^7 & \alpha^{11} \\ \alpha^{14} & \alpha^{13} & \alpha^{11} & \alpha^7 \end{array} \right.\right] \quad B_2 = \left[I_4 \left| \begin{array}{cccc} \alpha & \alpha^8 & \alpha^{12} & \alpha^{14} \\ \alpha^8 & \alpha & \alpha^{14} & \alpha^{12} \\ \alpha^{12} & \alpha^{14} & \alpha & \alpha^8 \\ \alpha^{14} & \alpha^{12} & \alpha^8 & \alpha \end{array} \right.\right] \quad B_3 = \left[I_4 \left| \begin{array}{cccc} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^{11} \\ \alpha^3 & \alpha^2 & \alpha^{11} & \alpha^4 \\ \alpha^4 & \alpha^{11} & \alpha^2 & \alpha^3 \\ \alpha^{11} & \alpha^4 & \alpha^3 & \alpha^2 \end{array} \right.\right] \tag{26}$$

These codes are MDS self dual codes. B_2 and B_3 generate $(48,24,10)$ codes having the same weight distributions. The weight distribution of the corresponding codes is given below:

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 (27).

$$\begin{bmatrix}
010001 & 001111 & 011011 & 011101 & 011000 & 000000 & 000000 & 000000 \\
001111 & 011000 & 000110 & 000101 & 010100 & 000000 & 000000 & 000000 \\
000101 & 010001 & 001001 & 101101 & 110000 & 000000 & 000000 & 000000 \\
000011 & 010010 & 010111 & 100100 & 100010 & 000000 & 000000 & 000000 \\
000000 & 010010 & 011101 & 001001 & 001010 & 001100 & 000000 & 000000 \\
000000 & 001010 & 001001 & 010100 & 100111 & 110000 & 000000 & 000000 \\
000000 & 000101 & 010001 & 000110 & 100100 & 110110 & 000000 & 000000 \\
000000 & 000011 & 010010 & 001010 & 110011 & 101000 & 000000 & 000000 \\
000000 & 000000 & 010111 & 001100 & 001010 & 101101 & 111100 & 000000 \\
000000 & 000000 & 001111 & 011000 & 010100 & 001001 & 001010 & 000000 \\
000000 & 000000 & 000110 & 000011 & 010010 & 100111 & 110000 & 000000 \\
000000 & 000000 & 000011 & 010010 & 011101 & 010100 & 011000 & 000000 \\
000000 & 000000 & 000000 & 010100 & 000101 & 000110 & 100111 & 110000 \\
000000 & 000000 & 000000 & 001010 & 010100 & 000101 & 110011 & 101000 \\
000000 & 000000 & 000000 & 000101 & 000110 & 001100 & 011101 & 010010 \\
000000 & 000000 & 000000 & 000011 & 001010 & 010100 & 111001 & 100100 \\
000001 & 011111 & 100000 & 111000 & 100101 & 101111 & 010011 & 100000
\end{bmatrix} \tag{27}$$

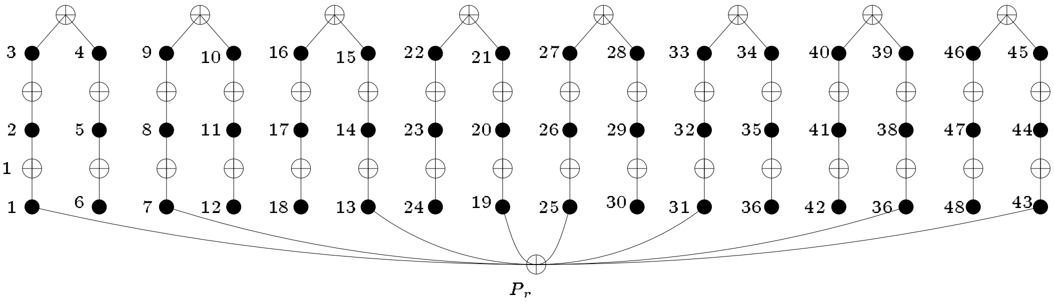

Fig. 25. A minimal Tanner graph of $(8, 7, 2) \otimes (6, 1, 6)$ code.

For this code the ATG given by Figure 25 has a single root parity. The corresponding parity space is given by M_{PS}:

$$M_{PS} = \begin{bmatrix}
0 & 11001 & 01000 & 10110 & 10011 & 10100 & 00000 & 00000 & 00000 \\
0 & 01000 & 10100 & 00101 & 00111 & 11110 & 00000 & 00000 & 00000 \\
0 & 00111 & 11001 & 01101 & 11011 & 01000 & 00000 & 00000 & 00000 \\
0 & 00010 & 11011 & 11100 & 10110 & 10011 & 00000 & 00000 & 00000 \\
0 & 00000 & 11011 & 10011 & 01101 & 01111 & 01010 & 00000 & 00000 \\
0 & 00000 & 01111 & 01101 & 11110 & 10100 & 01000 & 00000 & 00000 \\
0 & 00000 & 00111 & 11001 & 00101 & 10110 & 01101 & 00000 & 00000 \\
0 & 00000 & 00010 & 11011 & 01111 & 01010 & 11100 & 00000 & 00000 \\
0 & 00000 & 00000 & 11100 & 01010 & 01111 & 11011 & 00010 & 00000 \\
0 & 00000 & 00000 & 01000 & 10100 & 11110 & 01101 & 01111 & 00000 \\
0 & 00000 & 00000 & 00101 & 00010 & 11011 & 10100 & 01000 & 00000 \\
0 & 00000 & 00000 & 00010 & 11011 & 10011 & 11110 & 10100 & 00000 \\
0 & 00000 & 00000 & 00000 & 11110 & 00111 & 00101 & 10100 & 01000 \\
0 & 00000 & 00000 & 00000 & 01111 & 11110 & 00111 & 01010 & 11100 \\
0 & 00000 & 00000 & 00000 & 00111 & 00101 & 01010 & 10011 & 11011 \\
0 & 00000 & 00000 & 00000 & 00010 & 01111 & 11110 & 00101 & 10110 \\
1 & 00001 & 10000 & 10000 & 00100 & 10111 & 11000 & 11010 & 10000
\end{bmatrix} \tag{28}$$

It is obvious from this generator matrix that the space generated by the parities of any of eight branches of the TG is of dimension 5. Further, all eight spaces associated with $P_r = 0$ are also the same and generated by M

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

More inspection of M_{PS}, with $P_r = 0$, shows that the space of the parities of any $i \leq 4$ consecutive branches of the TG is the direct sum space $\oplus_1^i M$. The MTD of the parity space consists of two parallel 3-section semiregular subtrellises, one for $P_r = 0$ and the other one for $P_r = 1$.

Any possible version of the (48,24,12) QR code that contains C_{48}^7 can be presented by TG given in Figure 25 with $P_r = 0$, as it has been the case for (32,16,8) QR code with parity space given by (17). It would have a parity space with a MTD consisting of two disjoint 3-section semiregular trellises, precisely the same as that described above for the (48,24,10) codes. This is because according to Lemma 5 the base code will be an (8,4,5) code. This together with considering the rich structure of the edge spaces of parity space of (48,24,10) code suggest that the decoding process and decoding complexity of three presented (48,24, 10) codes would be precisely the same as those of any version of (48,24,12) QR code which includes C_{48}^7 when TG given by Figure 25 is applied.

Due to the size and 3-section semiregular structure of the MTD of parity space, the worst case decoding complexity of the given (48,24,10) codes is about 399000 real operations. This shows %27 improvement over trellis decoding using optimal sectionalization [28].

Acknowledgment: We would like to thank Mr. A. R. Fazel for his valuable assistance in the computer programming required in Theorem 6.

References

[1] G.D. Forney, Jr., "Coset codes part II: binary lattices and related codes," *IEEE Trans. Infor. Theory*, vol. IT-34, Sept. 1988, pp. 1152-1187.

[2] J.K. Wolf, "Maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Infor. Theory,* vol. IT-24, Jan. 1978, pp.76-80.

[3] 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. IT-20, Mar. 1974, pp. 284-287.

[4] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Infor. Theory*, vol. IT-27, Sept. 1981, pp. 533-547.

[5] N. Wiberg, H.-A. Loeliger and R. Kotter, "Codes and iterative decoding on general graphs," *Euro. Trans. Telecommun.,* vol.6 , pp. 513-526, Sep. 1995.

[6] N. Wiberg, "Codes and decoding on general graphs," Ph.D. dissertation, Dept. Elec. Engg., U. Linkoping, Sweden, Apr. 1996.

[7] G.D. Forney, Jr., "The forward-backward algorithm," *The Proceedings of the Thirty-Fourth annual Allerton conference on communication, control and computing*, Oct. 1997, pp. 432-446.

[8] R. A. Silverman and M. Balser, "Coding for a constant data rate source," *IRE Trans. Infor. Theory,* vol. PG IT-4, pp. 50-63, 1954.

[9] A. D. Abbaszadeh and C. K. Rushforth, "Efficient maximum-likelihood decoding of the extended Nordstrom-Robinson code," *Proc. 25th Annu. Allerton Conf.*, 1987, pp. 598-599.

[10] D. Chase, "A class of algorithms for decoding block codes with channel measurment information," *IEEE Trans. Infor. Theory*, vol. IT-18, 1972, pp. 170-182.

[11] E. R. Berlekamp, "The technology of error correctiong codes," *Proc. IEEE*, vol. 68, Sept. 1980, pp. 574-593.

[12] E. R. Berlekamp, "The construction of fast, high-rate, soft decision block decoders," *IEEE Trans. Infor. Theory*, vol. IT-29, 1983, pp. 372-377.

[13] G.D. Forney, Jr., "Concatenated Codes," Cambridge, MA: MIT Press, 1966, pp. 61-62.

[14] G.D. Forney, Jr., "Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference," *IEEE Trans. Infor. Theory*, vol. IT-18, Sept. 1972, pp. 363-378.

[15] G.D. Forney, Jr., "Coset codes part III: ternary codes, lattices, and trellis codes," *IEEE Unpublished paper*, 1987 .

[16] J. H. Conway and N. J. A. Sloane, "Fast quantizing and decoding algorithms for lattice quantizers and codes," *IEEE Trans. Infor. Theory,* vol. IT-28, 1982, pp. 227-232.

[17] 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. IT-32, Jan. 1986, pp.41-50.

[18] V. Pless, "Decoding the Golay code," *IEEE Trans. Infor. Theory,* vol. IT-32, July 1986, pp. 561-567.

[19] A. Vardy and Yair Be'ery, "More Efficient Soft Decoding of the Golay Codes," *IEEE Trans. Infor. Theory*, vol. IT-37, May 1991, pp. 667-672.

[20] J.Yuan, C.S. Chen, S. Ma, "Two-level decoding of $(32,16,8)$ quadratic residue code," *IEE PROCEEDINGS-I,* vol. 140, No. 6, Dec. 1993, pp.409-414.

[21] Jakov Snyders and Yair Be'ery, "Maximum likelihood Soft Decoding of Binary Block Codes and Decoders for the Golay Codes," *IEEE Trans. Infor. Theory,* vol. 35, No. 5, Sept. 1989, pp.963-975.

[22] Moshe Ran and Jakov Snyders, "Constrained Designs for Maximum Likelihood Soft Decoding of RM(2,m) and the Extended Golay Codes," *IEEE Trans. on Communications,* vol. 43, NO. 2/3/4, Feb./March/April 1995, pp. 812-820.

[23] T. Etzion, A. Trachtenberg, A. Vardy, "Which codes have cycle-free Tanner graphs?," Preprint, Nov. 1997.

[24] F. Harary, *Graph Theory*, Addison-Wesley:New York, 1972.

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

[26] Lin Shu, Costello Daniel, *Error Control Coding*, Prentice-Hall, 1983.

[27] V. Tarokh, "Minimal Tanner graphs for block codes and lattices," *Proceedings of the 5th Canadian Workshop on Information Theory,* June 3-6, 1997.

[28] Alec Lafourcade and Alexander Vardy, "Optimal Sectionalization of a Trellis," *IEEE Trans. Infor. Theory*, vol. 42, No. 3, May 1996, pp. 689-703.

[29] A. Poli and L. Huguet, *Error Correcting Codes, Theory and Application*, Masson and Prentice Hall:UK, 1992.