Acyclic Tanner graphs and maximum-likelihood decoding of linear block codes

M.Esmaeili and A.K.Khandani

Abstract: The maximum-likelihood decoding of linear block codes by 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 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. This graphical representation provides a unified and systematic approach to search for an efficient method for the maximum-likelihood decoding of a given linear block code. It is shown that the proposed method covers the most efficient techniques known for the decoding of some important block codes, including the hexacode H_6, extended Golay codes, Reed–Muller codes, Hamming codes and (32, 16, 8) quadratic residue code. The generalisation to the decoding of lattices is briefly explained.

1 Introduction

The maximum-likelihood (ML) 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 [1–3], Tanner graph (TG) [4], and Tanner–Wiberg–Loeliger graph [5, 6].

Bahl [1] and Wolf [3] demonstrated that one could construct a trellis diagram for a block code, and hence employ the Viterbi algorithm for its decoding. Wolf also gave a simple algorithm for the construction of the trellis diagram. Forney [2] later gave a procedure for the construction of the minimal trellis diagrams [Note 1] for the class of Reed–Muller codes and the extended Golay code. In most instances, the code was found to have far fewer states than the method originally given by Wolf in [3]. In the same year, Muder [7] rephrased the work of Forney in graph theoretic terms. Since then, several authors have studied the problem of finding minimal trellises for linear block codes [8–11]. Trellis-based approaches have also been successfully applied to the decoding of array codes [12, 13].

The work of Conway and Sloane [14] 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 [15] 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 [16–19] to introduce some of the best known techniques in decoding linear block codes, including the (24, 12) Golay code [18], the (32, 16) extended quadratic residue (QR) code [19], and the second order Reed–Muller codes [16].

The methods of coset decoding have been developed during many years by some of the best known coding theorists, and are mainly due to the intuitive understanding of their inventors with respect to the structure of the specific code considered. Unfortunately, however, the techniques developed usually do not follow a unified framework and the results cannot be easily understood or generalised from one instance to the other. The present work provides a unified and systematic approach to searching for an efficient coset decoding method of a given linear block code. It is shown that the proposed method covers the best decoding technique known for many of the important codes.

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 denotes the parity nodes, the rows of H, and the other set denotes the symbol nodes, the columns of H. A parity node u_i is connected to a symbol node v_j iff $h_{ij} \neq 0$. A cycle-free TG will be referred to as an acyclic TG (ATG).

The single parity (SP) codes are easily decoded by using the Wagner rule [20]. In this case, a bit-by-bit hard decision of the received channel output is considered 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 generalised by several authors including [14, 21–28] to the ML decoding of block codes and lattices.

Snyders and Be'ery [17] introduced a generalisation of the Wagner rule decoding for binary block codes, including

© IEE, 2000

IEE Proceedings online no. 20000663

DOI: 10.1049/ip-com:20000663

Paper first received 1st October 1998 and in revised form 16th December 1999

The authors are with the Department of Electronic and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Note 1: A minimal trellis diagram is the trellis having the least number of states among all trellis diagrams representing the code.

the Golay codes. Later, their work on the Golay codes was improved substantially by Vardy and Be'ery [18] using Pless construction [15] of these codes together with the Wagner rule. The same approach was taken for decoding of the (32, 16) QR code [19]. The method of coset decoding has been used in [34–36] in conjunction with various other decoding techniques to provide a variety of tradeoffs between bit error performance and decoding complexity.

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

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 the largest subcode (with the minimum index) always 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, we compare the method of [17, 18] for the decoding of the Golay code. These references use the same five-dimensional subcode of the Golay code $\mathcal{G}_{24}$. In [17], all cosets are decoded independently and then the most likely codeword is chosen, while in [18], the final selected codeword is determined without decoding all the cosets. This is the main reason for the reduction in complexity in [18] with respect to [17]. 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 $C_1 \cap C_2 = \{0\}$, and $C = \{c_1 + c_2 | c_1 \in C_1 \text{ and } c_2 \in C_2\}$. The direct product (also called the Kronecker product, or simply the product) operation is denoted by '$\otimes$'. The direct sum of two codes C_1 and C_2, denoted $C_1 \oplus C_2$, is defined to be $C_1 \oplus C_2 := \{c_1c_2 | c_1 \in C_1 \text{ and } c_2 \in C_2\}$, where c_1c_2 is the concatenation of c_1 and c_2. The ordinary product of two matrices M_1 and M_2 is denoted by M_1M_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 $M_0^{\perp}$ denote a generator matrix of the dual code $C_0^{\perp}$. The space of the parity nodes, referred to as the parity space (PS), is generated by the matrix $M_{PS} := M_0^{\perp}M_c$, where M_c is a generator of C_c. The ATG of C_0, together with the 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.

The base code C_0 needs to be of high dimension to keep the index (number of cosets) low. Another important feature of C_0 is the structure of the corresponding TG. To reduce the decoding complexity, it is essential to have the number of branches leaving the root parity large, and for the branches to be as similar 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.

In all the important cases examined, 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 [29], which completely characterises the codes with cycle-free TGs. Using the results of [29], we conclude that all the base subcodes used in our discussions are indeed maximal. We will present an independent proof for the maximality of the extracted subcode for the case of the first order Reed–Muller code.

2 Tanner graphs

2.1 Minimal 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 and H' are given in Fig. 1.

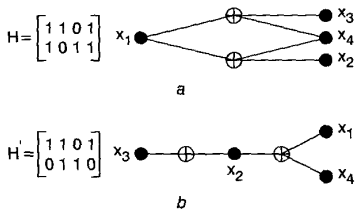

Fig. 1 *Two Tanner graphs of (4, 2) linear code C corresponding to H and H'*

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, the number of edges is not constant, as can be seen from example 1.

Definition 1 (minimal Tanner graph): A TG of a linear code C is called minimal Tanner graph (MTG) if it has the minimum number of edges 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 Fig. 1*b* is a MTG.

One of the matrices associated with a graph G, whose cycles and edges are labelled, 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 [30].

As all MTGs of a linear code C have the same number of edges and vertices, it follows that the associated cycle spaces have the same rank. This supports the idea of referring to any MTG of a linear code C as the minimal Tanner graph of C.

Definition 2 (minimal Tanner basis): Let $H_{\min}$ denote 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.

In [31], we have given an algorithm to construct $H_{\min}$ from a given check matrix H.

2.2 Acyclic Tanner graphs and single parity codes

A linear code C whose MTG is cycle-free will be referred to as an acyclic code. The class of linear block codes with ATGs is characterised in [29]. Since most of the important

codes are not acyclic, for a given code C, the acyclic subcodes are of special interest.

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.

Let C be an acyclic linear code. If the MTG is a forest (a disconnected acyclic graph), 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 characterising acyclic linear codes we may consider only those with connected ATG to be called 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 [31].

Definition 3 (generalised single parity code): A linear code C having tree Tanner graph G is defined to be a generalised single parity (GSP) code if at most one of the parity nodes of G is of degree $m \geq 3$. Such a 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 the generator of the $(m, m-1, 2)$ 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 generalised single parity (UGSP) code.

3 Acyclic Tanner graphs and maximum-likelihood decoding

3.1 Maximum-likelihood decoding using acyclic subcode and Wagner rule

3.1.1 Maximum likelihood decoding: Let C be an (n, k) linear block code over a field F_q. Assume that a codeword of C is transmitted over a noisy memoryless channel with discrete output alphabet Y and transition probability functions $f(y|x)$; that is, the probability of receiving symbol y given that x is transmitted is $f(y|x)$. Further, suppose the sequence $\boldsymbol{y} = (y_1, ..., y_n)$ is received as the channel output. The maximum-likelihood decoding consists of finding codeword $\boldsymbol{c} = (c_1, ..., c_n)$ that maximises $P(\boldsymbol{c}|\boldsymbol{y})$, the likelihood that $\boldsymbol{c}$ is transmitted provided that $\boldsymbol{y}$ is received. Assuming that all codewords of C are transmitted with equal probability q^{-k}, we see that maximisation of $P(\boldsymbol{c}|\boldsymbol{y})$ is equivalent to maximisation of $P(\boldsymbol{y}|\boldsymbol{c})$, the probability of receiving $\boldsymbol{y}$ given that $\boldsymbol{c}$ is transmitted. The channel is memoryless, and hence we have $P(\boldsymbol{y}|\boldsymbol{c}) = \Pi_{i=1}^{n} P(y_i|c_i) = \Pi_{i=1}^{n} f(y_i|c_i)$. Consequently $\boldsymbol{c} = (c_1, ..., c_n)$ is the most likely transmitted codeword if and only if it minimises

$$W_c := \sum_{i=1}^{n} -\log f(y_i|c_i) \tag{1}$$

Assume that C is an (n, k) binary code with BPSK, $x \in \{-1, 1\}$, modulation transmitted over a memoryless channel. Let $\mu_i := \ln(p(y_i|1)/p(y_i|-1))$ and $\mu := (\mu_1, ..., \mu_n)$. We refer to μ_i as the 'confidency value' of the ith bit. By considering C as a subset of the Euclidean space R^n, under projection $g(c_i) : (-1)^{c_i}$, the maximum-likelihood problem is to minimise the Euclidean norm $\|\mu - \boldsymbol{c}\|^2 := \|\mu\|^2 - 2<\mu, \boldsymbol{c}> + \|\boldsymbol{c}\|^2$. That is to say $\boldsymbol{c}$ must maximise the inner product $<\mu, \boldsymbol{c}> = \Sigma_{i=1}^{n} (-1)^{c_i}\mu_i$.

3.1.2 Tanner graph-trellis representation: 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, $C_0 = \{x|M_0^{\perp}x = 0\}$. A coset $C_0 + c$ is specified by $C_0 + c = \{x + c|M_0^{\perp}x = 0\}$. 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 $b = M_0^{\perp}c$. 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. Figs. 5–7, 9*b*, 9*c* and 10 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 $e := (e_1, e_2, ..., e_q)$, 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 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 change causes the least total confidency deviation and satisfies the root parity.

3.1.3 Twisted trellis representation: One way to implement the foregoing process is to substitute each edge of T_{PS} by q-tuple $e = (e_1, e_2, ..., e_q)$ and then to 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 Figs. 4*c* and 7 are examples of twisted trellises.

From the generator matrix point of view, the generator corresponding to a twisted trellis is easily obtained from that associated with the underlying trellis T_{PS}. The transformation process is given here for the binary case.

We consider the root parity column in the generator matrix of parity space as the contribution of a section, say the first section, of the trellis T_{PS} to the root parity, and provide other sections of the trellis with zero contributions. This, for instance, transfers parity matrix M_{PS} to M':

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

$$M' = \begin{bmatrix} 111 & 100 & 000 \\ 010 & 110 & 100 \\ 001 & 100 & 110 \end{bmatrix}$$

The generator matrix so obtained introduces only a linear subcode of the code corresponding to the twisted trellis. In the coset associated with the all-zero parity sequence, we may replace the all-zero sequence of contributions to the root parity by any even weight binary sequence. As a result, M_{TT}, the generator of the twisted trellis, is obtained by adjoining matrix M'' to M', where the columns of M'' corresponding to the contributions to the root parity form a SP code, and the rest of the entries are all zero. The following illustrates the process. The associated trellises are given in Figs. 4*b* and *c*, respectively.

$$M_{TT} = \begin{bmatrix} M' \\ M'' \end{bmatrix} = \begin{bmatrix} 111 & 100 & 000 \\ 010 & 110 & 100 \\ 001 & 100 & 110 \\ \hline 001 & 001 & 000 \\ 000 & 001 & 001 \end{bmatrix}$$

$$M_{PS} = \begin{bmatrix} P_r & P_{1,2} & P_{3,4} & P_{5,6} \\ \hline 1 & 11 & 10 & 00 \\ 0 & 01 & 11 & 10 \\ 1 & 00 & 10 & 11 \end{bmatrix} \quad (2)$$

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 manner. For instance, if TT_{PS} consists of disjoint regular sub-trellises, to be defined in the next subsection, then it can be decoded more efficiently.

3.2 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

$$\begin{bmatrix} A_1 & A_2 & & & & \\ & A_2 & A_3 & & & \\ & & \ddots & \ddots & & \\ & & & A_{n-2} & A_{n-1} & \\ & & & & A_{n-1} & A_n \end{bmatrix} \quad (3)$$

is referred to as an r-level parity check code.

Example 2: The following matrices represent two one-level and two-level binary parity codes.

$$M = \begin{bmatrix} 11 & 10 & 00 \\ 00 & 10 & 11 \end{bmatrix} \quad M' = \begin{bmatrix} 111 & 100 & \\ 001 & 001 & \\ & 100 & 111 \\ & 001 & 001 \end{bmatrix} \quad (4)$$

Definition 5 (regular trellis diagram): An n-section trellis diagram T is called regular if:

(i) 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;

(ii) each section of the trellis is a complete bipartite graph;

(iii) the set of labels 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 Figs. 2*a* and 8*b* are regular quaternary 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 indeed been the motivation for introducing the term multilevel parity code.

3.3 Maximum likelihood 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 constrained design representation of second order Reed–Muller codes and the (24, 12) Golay code is given in [16]. A layer of the constrained design does indeed present a regular trellis diagram. It is therefore natural to extend the elimination techniques given in [16] on the multilevel parity codes.

A linear block code C containing an r-level parity code has a trellis diagram consisting of structurally identical parallel sub-trellises, 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 the best among them is specified. After that, all the n non-maximal 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 the first step. The best path among the obtained paths is determined. If e_1 and e_2 are the two non-maximal edges of one such path, 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 until no path is left. A comparison among the candidates of the mentioned groups of paths gives the decoder output.

Example 3: Consider the single parity code C over F_4 given by the generator matrix

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad (5)$$

The corresponding trellis, which is regular, is shown in Fig. 2*a*. We have to find a path of the trellis with the maximum possible value 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 ith 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 five 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 are 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 Fig. 2*b*.

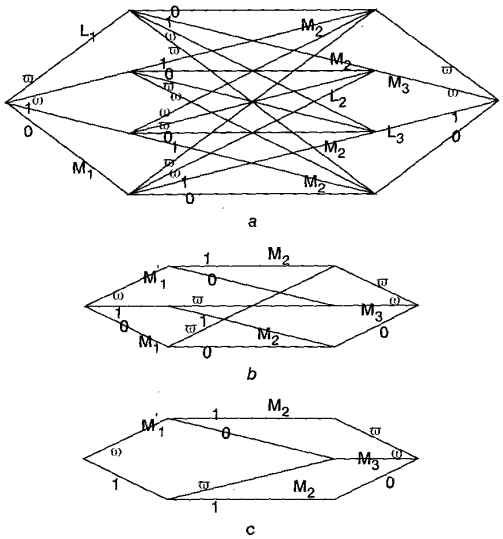

Fig. 2 *Regular trellis diagram representing 2-D single parity code, and derived trellises*
a Regular trellis diagram representing 2-D single parity code C over F_4 with generator matrix given by eqn. 5
b Trellis obtained from trellis a by deleting the edges labelled X_1, X_2 and X_3
c Trellis obtained from trellis *b* by deleting paths containing the edge labelled M_1

Now consider $N := \min\{M_1 - M_1', M_2 - M_2', M_3 - M_3'\}$ and without loss of generality suppose $N = M_1 - M_1'$. This requires two real operations. If $M_1' = L_1$ then the path with confidency label $L_1M_2M_3$ would be the best. Assume $M_1' \neq L_1$. It is easy to see that in this case the total confidency of the paths $M_1\bar{\omega}\bar{\omega}$ and $M_1\mathbf{00}$ is not larger than that of $M_1'M_2\bar{\omega}$ and $M_1'\mathbf{0}M_3$, respectively. Accordingly, the paths including the edge with confidency label M_1 could be deleted and we are left with the trellis shown in Fig. 2*c*. In this trellis five real operations are required to determine the winner based on total confidency deviation from $M = M_1 + M_2 + M_3$. Between the two surviving 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.

3.4 Three-section semi-regular trellis

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

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

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

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

Consider the linear code C with generator matrix

$$\begin{bmatrix} A_1 & A_2 & A_3 & \\ & A_6 & A_5 & A_4 \end{bmatrix} \tag{6}$$

A four-section MTD T of this code is indeed a three-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 $1 \leq i \leq 4$, the edge labels of the trellis form $<A_i>$, the space generated by A_i. The main property of T is that any two distinct elements from any two spaces $<A_i>$ and $<A_j>$, $1 \leq i \neq j \leq 4$, determine a unique path of T.

Let T in general be a four-section trellis whose edge labels at the ith section $1 \leq i \leq 4$, form set S_i. If any two distinct elements from any two sets S_i and S_j, $1 \leq i \neq j \leq 4$, define a unique path of T, then we refer to T as a three-section semi-regular trellis.

Example 4: The ternary generator matrix

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

has a MTD consisting of three structurally identical parallel sub-trellises, each of which is a three-section semi-regular trellis. The trellis corresponding to the subcode specified by the first two rows of the generator is given in Fig. 10*b*.

4 Maximal acyclic subcodes

Distinct maximal acyclic subcodes: The maximal acyclic subcode of a code has the advantage of minimising the number of cosets. However, the number of cosets does not necessarily reflect the decoding complexity. Another 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 be worth examining. In general, the more well structured the Tanner graph the lower the decoding complexity.

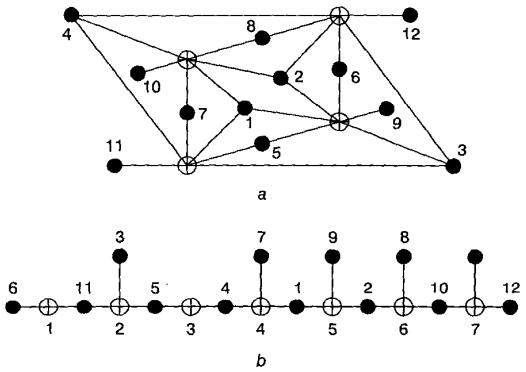

Fig. 3 *Tanner graphs associated with matrices H and H'*
a Minimal Tanner graph of (12, 8, 3) code with parity matrix H given in eqn. 7
b Tanner graph associated with parity matrix H'

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

$$H = \begin{bmatrix} 111011001000 \\ 110100110100 \\ 101110100010 \\ 011101010001 \end{bmatrix} \quad H' = \begin{bmatrix} 000110000000 \\ 001010000010 \\ 100100100000 \\ 110000001000 \\ 010000010100 \\ 000001000010 \\ 000000000101 \end{bmatrix}$$

$$H'' = \begin{bmatrix} 001011001011 \\ 010000000001 \\ 001100000000 \\ 000010100000 \\ 000001010000 \\ 000000001100 \\ 100000000010 \end{bmatrix} \tag{7}$$

A five-dimensional maximal acyclic subcode C' of C_{12} is given by the parity matrix H'. This subcode has $G_T(C')$ shown by Fig. 3*b*.

As 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.

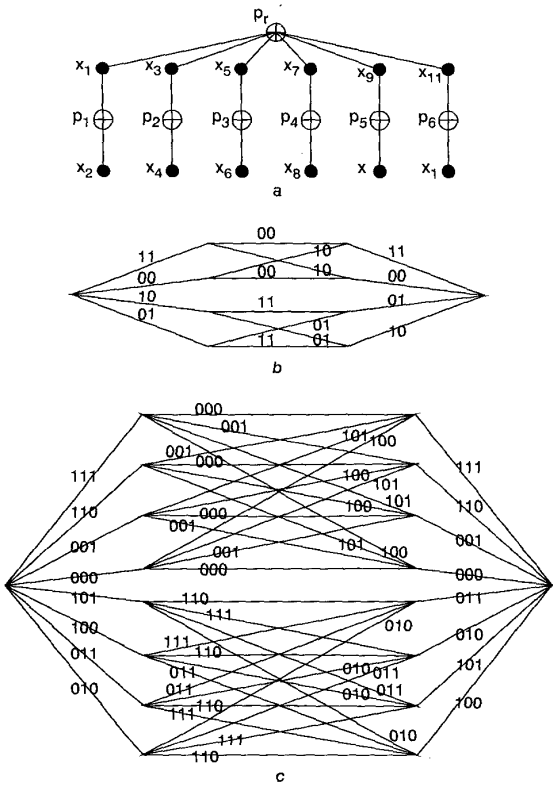

Fig. 4 *Tanner graphs assocoated with H" and trellis diagrams*
a Tanner graphs associated with parity matrix H''
b Minimal trellis diagram of parity space when the root parity P_r is ignored
c Twisted regular trellis diagram representing paths satisfying the root parity

On the other hand, the parity check matrix H'' represents a five-dimensional UGSP subcode C'' of C_{12}. It has $G_T(C'')$ given in Fig. 4*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 Fig. 4*b*. represents the space of parities $\{P_1, ..., P_6\}$. The impact of the root parity P_r has changed the trellis in Fig. 4*b* into the twisted trellis in Fig. 4*c*, which consists of two disjoint regular sub-trellises. 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 five-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.

The determination of maximal subcodes with ATGs of a given code C seems to be quite a 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. A few observations are given in [31].

5 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 three. 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 $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n)$ be two n-tuples. The Boolean product of a and b is defined as $ab := (a_1b_1, a_2b_2, ..., a_nb_n)$. The product of i n-tuples is called a Boolean product of degree i. For a nonnegative integer m, consider the 2^m-tuples $v_0, v_1, ..., v_m$ 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 two 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 $D = \{v_1, v_2, ..., v_m\}$ up to degree r. The subspace of $F_{2^{2^m}}$, generated by A is defined as the rth order Reed–Muller code of length 2^m, and is denoted by $\mathcal{R}(r, m)$.

5.1 First order Reed–Muller codes

Let $\mathcal{R}'(1, m)$ denote the $(m - 2)$-dimensional subcode of $\mathcal{R}(1, m)$ generated by $[v_1, v_2, ..., v_{m-2}]'$, where $[\cdot]'$ stands for the transpose operation. The matrix G_m^1, the generator matrix of $\mathcal{R}(1, m)$, may be represented by

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

The dual of $G_0(1, m)$ is $H_0(1, m) := (4, 4, 1) \otimes \mathcal{R}(m - 1, m - 2) + \mathcal{R}(0, 2) \otimes 10^{2^{m-2}-1}$. The parity space is given by generator $M_{PS}(1, m) := H_0(1, m)\mathcal{R}'(1, m) = 0\mathcal{R}(0, 2) \otimes M_m$, where the 0 beside $\mathcal{R}(0, 2)$ denotes a zero column, and M_m is defined by

$$M_m := \begin{bmatrix} 0 & 1 & 0 \\ M_{m-1} & 0 & M_{m-1} \end{bmatrix} \text{ and } M_3 = 1$$

It is obvious that $G_0(1, m)$ is a three-dimensional acyclic subcode of $\mathcal{R}(1, m)$. The following theorem shows that $G_0(1, m)$ is a maximal UGSP subcode of $\mathcal{R}(1, m)$. In this theorem, by the expression 'a MTG of a matrix M', we mean a MTG of a linear code having generator matrix M.

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

Proof: The proof is based on the fact that 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, and the simplex code $\mathcal{B}(1, m)$ (the code generated by the set of Boolean polynomials of degree one given by $D = \{v_1, v_2, ..., v_m\}$ [32]) is not acyclic. The details of the proof are given in [31]. □

Example 5: For $m = 4$, we have

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

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

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

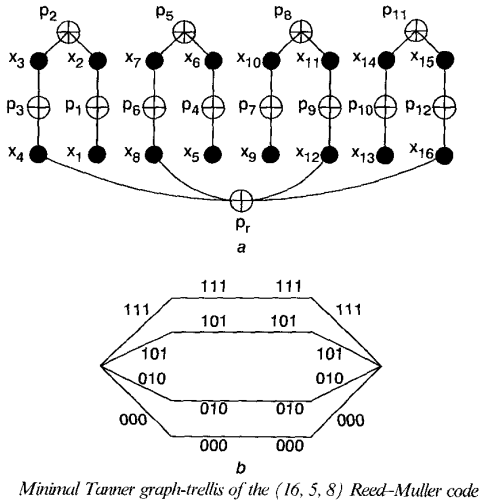

Fig. 5 *Minimal Tanner graph-trellis of the (16, 5, 8) Reed–Muller code*

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 sectionalisations [33]. Note that in the mentioned minimal TG-T of $\mathcal{R}(1, m)$, the trellis representing the parity space consists of parallel paths, as was the case with the hexacode H_6. In this case, one is required to perform an exhaustive search over all the trellis paths. This means that the trellis cannot be exploited for further reduction of the decoding complexity.

5.2 The rth order Reed–Muller codes

The results given for the first order Reed–Muller codes may be generalised. We can now show that the second order Reed–Muller code $\mathcal{R}(2, m)$, $m \geq 3$, includes acyclic subcodes of dimension seven, 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 is demonstrated, and using theorem 5 of [29], it can be shown that the subcodes presented 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 follows 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 is acyclic by the fact that 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.

Let $H_0(r, m)$ denote the dual of $G_0(r, m)$ and $PS(r, m)$ stand for the associated parity space. From the foregoing argument the following are easily derived.

Theorem 2: For the Reed–Muller code $\mathcal{R}(r, m)$ we have:

$$H_0(r,m) = \begin{bmatrix} \mathcal{I}_{2^{m-1}} & \mathcal{I}_{2^{m-1}} \\ 0 & H_0(r,m-1) \end{bmatrix}$$

$$\text{where } H_0(r,r+1) = \mathcal{R}(0,r+1) \tag{8}$$

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

$$\text{where } M_{PS}(r,r+2) = \mathcal{R}(r-1,r+1)0 \tag{9}$$

Example 6:

$$H_0(2,4) = \begin{bmatrix} \mathcal{I}_8 & \mathcal{I}_8 \\ 0 & 11111111 \end{bmatrix} \quad \text{and}$$

$$M_{PS}(2,4) = \mathcal{R}(1,3)0$$

The associated TTG is shown in Fig. 6. The root parity P_r is always zero and the space of the other eight parities is $\mathcal{R}(1, 3)$ as shown by a trellis. The trellis in Fig. 6 expresses the relation among the set of parities $\{p_1, p_2, ..., p_8\}$, and does not reflect the role of the root parity p_r in the TTG of the code. Therefore, it is replaced by the twisted trellis given in Fig. 7.

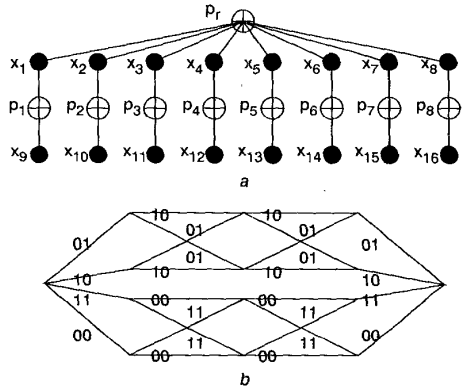

Fig. 6 *Tanner graph-trellis of the (16, 11, 4) Reed–Muller code*

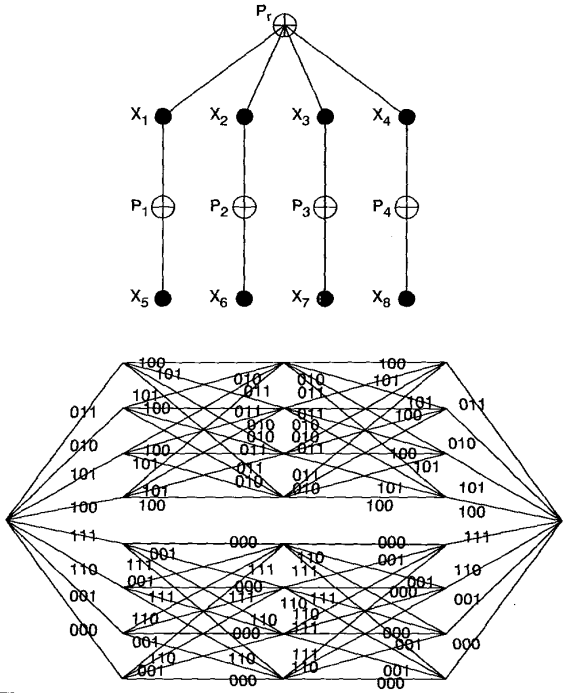

Fig. 7 *Twisted Tanner graph-trellis representation of the (16, 11, 4) Reed–Muller code*

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. A similar method has been implicitly used in [16] in the language of design theory. As a result the two works give the same decoding complexity.

5.3 Hamming codes

If a code is obtained by the 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 1s. $\mathcal{I}_3 1 \mathcal{I}_3$ 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 $\mathcal{H}_r$

6 Quadratic residue codes

We will show that the best techniques which have been applied to decode the (24, 12, 8) and (32, 16, 8) extended QR codes [15, 18, 19] are essentially based on the application of the TG-T representation of these codes.

In the mentioned works the (24, 12, 8) and (32, 16, 8) extended QR codes have been projected (refer to definition 6) on the quaternary codes. There are 16 binary sequences of length 4, and this set is partitioned into four 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 four distinct ways as a binary combination of the elements of F_4. This produces the aforementioned partition. 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.

Let C_2 and C_4 be two binary and quaternary linear codes of length $4m$ and m, respectively. According to [15], we have the following definition (also used in [18, 19]).

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:

(i) The quaternary expression of any codeword of C_2 is a codeword of C_4.

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

(iii) 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.

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

The (24, 12, 8) Golay code $\mathcal{G}_{24}$ has a generator matrix $M_{24} = [(6, 5, 2) \otimes (4, 1, 4)] + M_1$, where M_1 is given below. The five-dimensional UGSP code $(6, 5, 2) \otimes (4, 1, 4)$ is a maximal acyclic subcode of $\mathcal{G}_{24}$. The associated TG is given in Fig. 8*a*. The parity space is given by M_{PS}.

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

$M_{PS}(1, 4) =$

P_r	$P_{1,2,3}$	$P_{4,5,6}$	$P_{7,8,9}$	$P_{10,11,12}$	$P_{13,14,15}$	$P_{16,17,18}$
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

(10)

Ignoring the root parity P_r, the parity space with generator *MPS* is represented by a three-section trellis diagram consisting of eight parallel regular sub-trellises, four of which correspond to the odd codewords, $P_r = 1$, and the other four correspond to the even codewords, $P_r = 0$. One of the sub-trellises associated with the first four rows of M_{PS} is shown in Fig. 8.

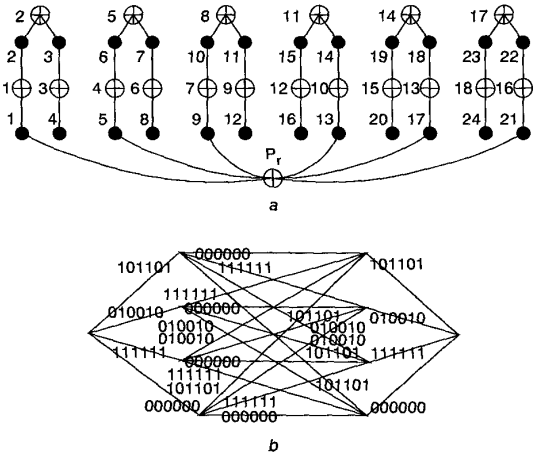

Fig. 8 *5-dimensional acyclic subcode and 3-section regular sub-trellis*
a 5-dimensional acyclic subcode (6, 5, 2) ⊗ (4, 1, 4) of the Golay code $\mathcal{G}_{24}$
b One of the 8 parallel 3-section regular sub-trellises of the trellis associated with the parity space MPS given by eqn. 10

Applying the eight parallel three-section regular sub-trellises representing the parity space M_{PS}, along with the same computational techniques used in [18], we come up with the same decoding complexity. This shows that the decoding of $\mathcal{G}_{24}$ by means of its projection on the hexacode H_6 is just another expression of the decoding by projection of the code on its maximal UGSP subcode.

6.2 The (32,16, 8) quadratic residue code

A two-level decoding technique has been presented for the (32, 16, 8) QR code [19]. In [19], the (8, 4, 4) quaternary code B with generator matrix G_b given in eqn. 11 has been

considered as the base code. From the permutation given in theorem 1 of [19], we have derived generator matrix $M_{32} := [(8, 7, 2) \otimes (4, 1, 4)] + M_1$, where M_1 is given below.

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

$$M_1 = \begin{bmatrix} 0101 & 0000 & 0110 & 1010 & 1100 & 0000 & 0000 & 0000 \\ 0011 & 0000 & 0101 & 0011 & 0110 & 0000 & 0000 & 0000 \\ 0000 & 0101 & 1111 & 1001 & 1100 & 1100 & 0000 & 0000 \\ 0000 & 0011 & 0000 & 1010 & 1100 & 0110 & 0000 & 0000 \\ 0000 & 0000 & 0110 & 0000 & 1100 & 0110 & 1100 & 0000 \\ 0000 & 0000 & 0011 & 0000 & 1010 & 0011 & 1010 & 0000 \\ 0000 & 0000 & 0000 & 0101 & 1100 & 0000 & 0011 & 1010 \\ 0000 & 0000 & 0000 & 0011 & 0110 & 0000 & 1001 & 1100 \\ 0001 & 1000 & 1000 & 0001 & 1000 & 1011 & 1101 & 1000 \end{bmatrix} \quad (11)$$

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.

The UGSP code (8, 7, 2) ⊗ (4, 1, 4), presenting the first seven rows of M_{32}, has parity matrix H_{32}^7:

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

The parity space has the generator matrix $M_{PS} := H_{32}^7 M_1$ given below (M'_{PS} will be defined later):

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

$$M'_{PS} = \begin{bmatrix} 0 & 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 0 & 010 & 010 & 010 & 010 & 000 & 000 & 000 & 000 \\ 0 & 000 & 000 & 010 & 010 & 010 & 010 & 000 & 000 \\ 0 & 000 & 000 & 000 & 000 & 010 & 010 & 010 & 010 \\ 0 & 010 & 000 & 010 & 000 & 010 & 000 & 010 & 000 \\ 0 & 111 & 111 & 111 & 111 & 000 & 000 & 000 & 000 \\ 0 & 000 & 000 & 111 & 111 & 111 & 111 & 000 & 000 \\ 0 & 000 & 000 & 000 & 000 & 111 & 111 & 111 & 111 \\ 0 & 111 & 000 & 111 & 000 & 111 & 000 & 111 & 000 \end{bmatrix} \quad (12)$$

The corresponding TTG is a uniform connected graph with eight branches, each of length 4. 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. The generator matrix M'_{PS} in eqn. 12 is the parity space of the (32, 16, 8) Reed–Muller code.

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

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

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

$$\begin{bmatrix} 111 & 000 \\ 010 & 000 \\ 000 & 111 \\ 000 & 010 \end{bmatrix}$$

and

$$rank \begin{bmatrix} A_2 \\ A_6 \end{bmatrix} = rank \begin{bmatrix} A_3 \\ A_5 \end{bmatrix} = 4$$

$$\text{and} \quad rank \begin{bmatrix} A_2 & A_3 \\ A_6 & A_5 \end{bmatrix} = 8$$

The main portion of the decoding complexity, 1599 operations out of 2059 operations, is concerned with this three-section semi-regular trellis. Due to the multilevel parity structure of M'_{PS} the (32, 16, 8) Reed–Muller code, unlike the (32, 16, 8) QR code, is decoded by only 1183 real operations, reported first in [16].

Once again our conclusion here is that the decoding technique given in [19] for the (32, 16, 8) QR code is in fact nothing but the application of the TG-T of this code with the maximal UGSP subcode (8, 7, 2) ⊗ (4, 1, 4) as the base code.

7 Hexacode H_6 and (12, 6, 6) ternary Golay code

7.1 Hexacode H_6

The (6, 3, 4) quaternary hexacode H_6 has a generator matrix M given in eqn. 13. 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 Fig. 9*a*. 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 two-dimensional UGSP subcode of the hexacode with generator and parity matrices M_0 and $M_0^\perp$, respectively.

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

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

$$M_0^\perp = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (13)$$

The corresponding MTG is a tree, shown in Fig. 9*b*, in which $P_rP_1P_2P_3 = 0000$, and the edge labels are 1. The hexacode is the union of four cosets of the given subcode, and the corresponding four sequences of $P_rP_1P_2P_3$ are the elements of the one-dimensional space generated by $\omega 111$, i.e.

$$P_rP_1P_2P_3 \in \{000, \omega 111, \bar{\omega}\omega\omega\omega, 1\bar{\omega}\bar{\omega}\bar{\omega}\}$$

These four cosets are applied in a maximum likelihood 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.

It can be easily verified that at most 39 real operations are required to determine the best candidate in each coset, and hence the code is decoded by at most $39 \times 4 + 3 = 159$ operations [31].

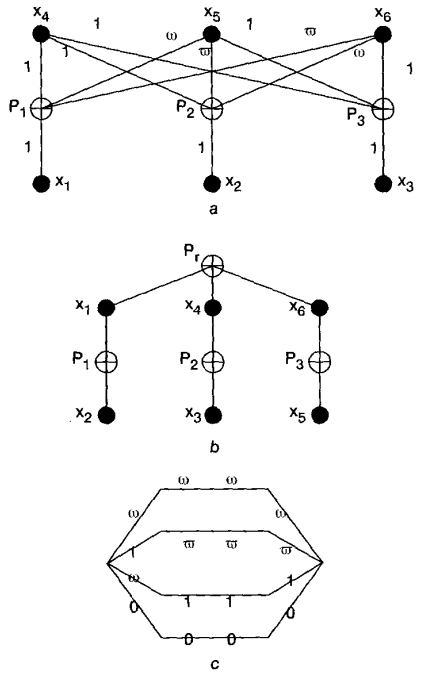

Fig. 9 *Minimal Tanner graph and graph-trellis of hexacode H_6*
a Minimal Tanner graph of the hexacode H_6
b, c Minimal Tanner graph-trellis of the hexacode H_6

7.2 Ternary Golay code $\mathcal{G}_{12}$

The ternary (12, 6, 6) Golay code $\mathcal{G}_{12}$ has a generator matrix M_{12} given by eqn. 14.

$$M_{12} = \begin{bmatrix} 111 & 111 & 000 & 000 \\ 000 & 111 & 222 & 000 \\ 000 & 000 & 111 & 111 \\ 020 & 001 & 010 & 221 \\ 020 & 121 & 001 & 020 \\ 002 & 211 & 010 & 020 \end{bmatrix}$$

$$M_{PS}(1,4) = \left[\begin{array}{ccccc} P_r & P_{1,2} & P_{3,4} & P_{5,6} & P_{7,8} \\ \hline 1 & 22 & 22 & 22 & 00 \\ 0 & 20 & 21 & 21 & 20 \\ 0 & 00 & 22 & 11 & 11 \end{array}\right] \quad (14)$$

The three-dimensional UGSP subcode C_0 generated by the first three rows of M_{12} has dual space

$$(4,4,1) \otimes \begin{bmatrix} 210 \\ 021 \end{bmatrix} + [100200200100]$$

presented by TG shown in Fig. 10*a*, in which the value of all parity nodes is zero. The edge labels are the coefficients of the corresponding variables, symbol nodes, forming a parity check equation. For instance, $2x_1 + x_2 = 0$, and $x_1 + 2x_4 + 2x_7 + x_{10} = 0$.

The corresponding 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. Applying this approach, a total of at most 656 real operations is required to decode the code in [31], as reported in [17].

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 [18]. The corresponding trellis consists of four parallel sub-trellises, one of which is given in Fig. 10. In this trellis, the paths beginning with edges labelled by 00, 22 and 11 correspond to the root parity values 0, 1 and 2, respectively.

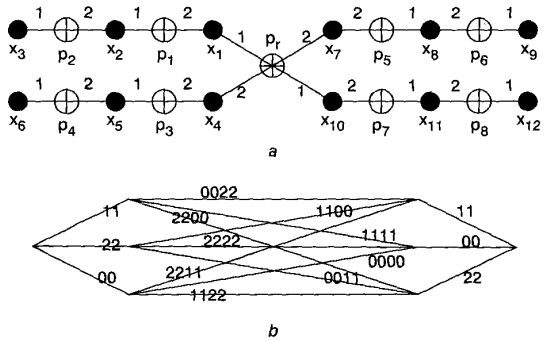

Fig. 10 *Tanner graph-trellis representation of the the ternary Golay code*
a Minimal Tanner graph of C_0
b One of three parallel semi-regular sub-trellises of the parity space

8 Summary and conclusion

Projection of linear block codes on maximal acyclic Tanner graphs provides the basis for the application of the Wagner rule to develop an efficient soft decision decoding algorithm. Using this projection, a given linear block code is represented by a combination of a trellis and a Tanner graph, where the efficiency of the decoding algorithm lies in the ability to exploit the structure of the underlying trellis diagram. It has been shown that the best maximum likelihood techniques known so far for the decoding of many important codes such as Hamming codes, Reed–Muller codes, hexacode, the extended Golay codes, and the (32, 16, 8) QR code are in fact based on this kind of projection.

The application of this approach on an arbitrary linear block code depends on the identification of relatively uniform acyclic subcodes of the code. Introduction of a method to find such a subcodes is left as an open problem.

The technique developed can be easily extended to the decoding of an integer lattice Λ with the partition chain $Z^n/\Lambda/KZ^n$, where Z^n is the set of the n-tuple integers. In this case, the role of the UGSP sub-code is replaced by the lattice KD_n, where the lattice D_n, defined as $D_n = \{(x_1, ..., x_n), x_i \in Z, \Sigma_i x_i \text{ even}\}$ is the counterpart to a single parity check code.

9 Acknowledgment

This work is financially supported by Communications and Information Technology Ontario (CITO), Research in Motion (RIM) Ltd. and the Natural Sciences and Engineering Research Council of Canada (NSERC).

10 References

1 BAHL, L.R., COCKE, J., JELINEK, F., and RAVIV, J.: 'Optimal decoding of linear codes for minimizing symbol error rate', *IEEE Trans. Inf. Theory*, 1974, **IT-20**, pp. 284–287
2 FORNEY, G.D.: 'Coset codes part II: binary lattices and related codes', *IEEE Trans. Inf. Theory*, 1988, **IT-34**, pp. 1152–1187
3 WOLF, J.K.: 'Maximum likelihood decoding of linear block codes using a trellis', *IEEE Trans. Inf. Theory*, 1978, **IT-24**, pp. 76–80

4 TANNER, R.M.: 'A recursive approach to low complexity codes', *IEEE Trans. Inf. Theory*, 1981, **IT-27**, pp. 533–547
5 WIBERG, N., LOELIGER, H.-A., and KOTTER, R.: 'Codes and iterative decoding on general graphs', *Eur. Trans. Telecommun.*, 1995, **6**, pp. 513–526
6 WIBERG, N.: 'Codes and decoding on general graphs'. PhD thesis, University of Linkoping, Sweden, 1996
7 MUDER, D.: 'Minimal trellises for block codes', *IEEE Trans. Inf. Theory*, 1988, **IT-34**, (5), pp. 1049–1053
8 HONARY, B., MARKARIAN, G., and DARNELL, M.: 'Low-complexity trellis decoding of linear block codes', *IEE Proc. Commun.*, 1995, **142**, (4), pp. 201–209
9 HORN, G.B., and KSCHISCHANG, F.R.: 'On the intractability of permuting a block code to minimize trellis complexity', *IEEE Trans. Inf. Theory*, 1996, **42**, (6), pp.
10 KSCHISCHANG, F.R., and SOROKINE, V.: 'On the trellis structure of block codes', *IEEE Trans. Inf. Theory*, 1995, **41**, (6), pp. 1924–1937
11 SIDORENKO, G., MARKARIAN, , and HONARY, B.: 'Minimal trellis design for linear codes based on the Shannon product', *IEEE Trans. Inf. Theory*, 1996, **42**, (6), pp. 2048–2053
12 CHARBIT, G., MANOUKIAN, H., and HONARY, B.: 'Array codes over rings and their trellis decoding', *IEE Proc. Commun.*, 1996, **143**, (5), pp. 241–246
13 HONARY, B., KAYA, L., MARKARIAN, G., and DARNELL, M.: 'Maximum-likelihood decoding of array codes with trellis structure', *IEE Proc. I*, 1993, **140**, (5), pp. 340–346
14 CONWAY, J.H., and SLOANE, N.J.A.: 'Decoding techniques for codes and lattices, including the Golay code and the Leech lattice', *IEEE Trans. Inf. Theory*, 1986, **IT-32**, pp. 41–50
15 PLESS, V.: 'Decoding the Golay code', *IEEE Trans. Inf. Theory*, 1986, **IT-32**, pp. 561–567
16 RAN, M., and SNYDERS, J.: 'Constrained designs for maximum likelihood soft decoding of RM(2,m) and the extended Golay codes', *IEEE Trans. Commun.*, 1995, **43**, (2–4), pp. 812–820
17 SNYDERS, J., and BE'ERY, Y.: 'Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes', *IEEE Trans. Inf. Theory*, 1989, **35**, (5), pp. 963–975
18 VARDY, A., and BE'ERY, Y.: 'More efficient soft decoding of the Golay codes', *IEEE Trans. Inf. Theory*, 1991, **IT-37**, pp. 667–672
19 YUAN, J., CHEN, C.S., and MA, S.: 'Two-level decoding of (32,16,8) quadratic residue code', *IEE Proc. I*, 1993, **140**, (6), pp. 409–414
20 SILVERMAN, R.A., and BALSER, M.: 'Coding for a constant data rate source', *IRE Trans. Inf. Theory*, 1954, **PG IT-4**, pp. 50–63
21 ABBASZADEH, A.D., and RUSHFORTH, C.K.: 'Efficient maximum-likelihood decoding of the extended Nordstrom-Robinson code'. Proceedings of 25th annual Allerton conference, 1987, pp. 598–599
22 BERLEKAMP, E.R.: 'The technology of error correcting codes', *Proc. IEEE*, 1980, **68**, pp. 564–593
23 BERLEKAMP, E.R.: 'The construction of fast, high-rate, soft decision block decoders', *IEEE Trans. Inf. Theory*, 1983, **IT-29**, pp. 372–377
24 CHASE, D.: 'A class of algorithms for decoding block codes with channel measurement information', *IEEE Trans. Inf. Theory*, 1972, **IT-18**, pp. 170–182
25 CONWAY, J.H., and SLOANE, N.J.A.: 'Fast quantizing and decoding algorithms for lattice quantizers and codes', *IEEE Trans. Inf. Theory*, 1982, **IT-28**, pp. 227–232
26 FORNEY, G.D. Jr.: 'Concatenated codes' (MIT Press, Cambridge, MA, 1966), pp. 61–62
27 FORNEY, G.D.: 'Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference', *IEEE Trans. Inf. Theory*, 1972, **IT-18**, pp. 363–378
28 FORNEY, G.D.: 'Coset codes part III: ternary codes, lattices, and trellis codes', *IEEE unpublished paper*, 1987
29 ETZION, T., TRACHTENBERG, A., and VARDY, A.: 'Which codes have cycle-free Tanner graphs?', 1997, (Preprint)
30 HARARY, F.: 'Graph theory' (Addison-Wesley, New York, 1972)
31 ESMAEILI, M., and KHANDANI, A.K.: 'Acyclic Tanner graphs and maximum-likelihood decoding of linear block codes'. Technical Report UW-E&CE#98-01, Department of Electrical and Computer Engineering; University of Waterloo, Waterloo, Canada, 1998
32 MACWILLIAMS, F.J., and SLOANE, N.J.A.: 'The theory of error-correcting codes' (North Holland, Amsterdam, 1977)
33 LAFOURCADE, A., and VARDY, A.: 'Optimal sectionalization of a trellis', *IEEE Trans. Inf. Theory*, 1996, **42**, (3), pp. 689–703
34 FOSSORIER, M.P.C., and LIN, S.: 'Computationally efficient soft-decision decoding of linear block codes based on ordered statistics', *IEEE Trans. Inf. Theory*, 1996, **42**, pp. 738–750
35 FOSSORIER, M.P.C., and LIN, S.: 'Generalized coset decoding', *IEEE Trans. Commun.*, 1997, **45**, pp. 393–395
36 FOSSORIER, M.P.C., and LIN, S.: 'Chase-type and GMD coset decodings', *IEEE Trans. Commun.*, 2000, **48**, pp. 345–350