On th Minimum-Weight Trellis Diagrams of Reed-Muller codes

T.Kasami and S.Lin

Abstract

The structure of the minimal 4-section trellis diagram for the set of minimum weight codewords of Reed-Muller codes is presented. The number of states at the end of each section is $2 + \Pi_{i=1}^{m-r-1}(2^{m-i}-1)/\Pi_{i=1}^{m-r-1}(2^{m-r-i}-1)$ except for the last section.

Keywords: minimal trellis diagram, Reed-Muller codes

1. Minimal trellis diagram

For a binary j-tuple $\mathbf{u} = (u_1, u_2, \ldots, u_j)$ and $1 \leq i_1 < i_2 \leq j$, let $p_{i_1,i_2}\mathbf{u}$ denote the $(i_2 - i_1 + 1)$-tuple $(u_{i_1}, u_{i_1+1}, \ldots, u_{i_2})$ and let $|\mathbf{u}|$ denote the weight of $\mathbf{u}$. Let C denote a binary block code of length n, and for $1 \leq i_1 < i_2 \leq n$, let $p_{i_1,i_2}C$ be defined as

$$p_{i_1,i_2}C \stackrel{\triangle}{=} \{p_{i_1,i_2}\mathbf{u} : \mathbf{u} \in C\}. \tag{1.1}$$

For $\mathbf{u}_1$ and $\mathbf{u_2}$ in $p_{1,i}C$ with $1 \leq i < n$, we write

$$\mathbf{u}_1 \approx_i \mathbf{u}_2, \tag{1.2}$$

if and only if for any binary $(n-i)$-tuple $\mathbf{v}$,

$$\mathbf{u}_1 \circ \mathbf{v} \in C \Longleftrightarrow \mathbf{u}_2 \circ \mathbf{v} \in C,$$

where "$\circ$" denotes the concatenation of two tuples. Suppose that the above relation (1.2) holds. For $0 \leq i < j \leq n$ and a binary $(j-i)$-tuple $\mathbf{v}$, if $\mathbf{u}_1 \circ \mathbf{v} \in p_{1,j}C$, then

$$\mathbf{u}_1 \circ \mathbf{v} \approx_j \mathbf{u}_2 \circ \mathbf{v}. \tag{1.3}$$

For $\mathbf{u}$ and $\mathbf{v}$ in C, we simply write

$$\mathbf{u} \approx_i \mathbf{v}, \tag{1.4}$$

in place of $p_{1,i}\mathbf{u} \approx_i p_{1,i}\mathbf{v}$. Note that "$\approx_i$" in (1.4) is an equivalent relation on C. C can be partitioned into equivalent blocks by the relation "$\approx_i$". Let N_i denote the number of blocks.

Let T be a trellis diagram with the minimum number of states for C. T is known to be unique [1] and said to be minimal. For $0 \leq i \leq n$, let S_i denote the set of states at the i-th bit position (just after the i-th bit position) in T. Then $|S_i|$, the number of states in S_i, is equal to N_i. Let s_0 denote the initial state of T and for $s \in S_i$ and $s' \in S_j$ with $0 \leq i < j \leq n$, let $L(s, s')$ denote the set of all label sequences of paths from s to s'. Hereafter a binary sequence of length j is regarded as a binary j-tuple and vice versa.

2. Key lemmas

For a positive integer m and a nonnegative integer r not greater than m, let B_m^r denote the set of all Boolean polynomials of degree r or less with m variables. For $f \in B_m^m$, let $V_m(f)$

denote the following binary 2^m-tuple:

$$V_m(f) \stackrel{\triangle}{=} (f(0,0,\ldots,0), f(1,0,\ldots,0), \ldots, f(1,1,\ldots,1)), \tag{2.1}$$

and let $|f|_m$ denote the weight of $V_m(f)$, and let $s_m(f)$ be defined as

$$s_m(f) \stackrel{\triangle}{=} \{(a_1, a_2, \ldots, a_m) \in \{0,1\}^m : f(a_1, a_2, \ldots, a_m) = 1\}. \tag{2.2}$$

For $f \in B_m^m$ and binary constants a and b, $f^{(a)}$ denotes $f' \in B_{m-1}^{m-1}$ such that

$$f'(x_1, x_2, \ldots, x_{m-1}) = f(x_1, x_2, \ldots, x_{m-1}, a), \tag{2.3}$$

and $f^{(a,b)}$ denotes $f'' \in B_{m-2}^{m-2}$ such that

$$f''(x_1, x_2, \ldots, x_{m-2}) = f(x_1, x_2, \ldots, x_{m-2}, a, b). \tag{2.4}$$

Then, for $\mathbf{u} = V_m(f)$,

$$p_{1+a2^{m-1}, 2^{m-1}+a2^{m-1}}\mathbf{u} = V_{m-1}(f^{(a)}), \tag{2.5}$$

$$p_{1+a2^{m-2}+b2^{m-1}, 2^{m-2}+a2^{m-2}+b2^{m-1}}\mathbf{u} = V_{m-2}(f^{(a,b)}), \tag{2.6}$$

$$|\mathbf{u}| = |f|_m = |f^{(0)}|_{m-1} + |f^{(1)}|_{m-1} \tag{2.7}$$

$$= |f^{(0,0)}|_{m-2} + |f^{(0,1)}|_{m-2} + |f^{(1,0)}|_{m-2} + |f^{(1,1)}|_{m-2}. \tag{2.8}$$

It is known [2] that for $f \in B_m^r$, $|f|_m = 2^{m-r}$ if and only if f is a product of linearly independent r polynomials $f_1, f_2, \ldots, f_r$ of degree one. Polynomials $f_i \stackrel{\triangle}{=} a_{i,0} + \sum_{j=1}^m a_{i,j}x_j$ with $1 \le i \le r$ are said to be linearly independent if and only if their coefficient vectors $\mathbf{a}_i \stackrel{\triangle}{=} (a_{i,1}, a_{i,2} \ldots, a_{i,m})$ with $1 \le i \le r$ are linearly independent. Since $f = f_1 \cdots f_{i-1}(1 + f_j + f_i)f_{i+1} \cdots f_r$, for $i \ne j$ (this is called a row operation), there is no loss of generality in assuming that

$$a_{i,m-1} = 0, \qquad \text{for } i \ne r-1, \tag{2.9}$$

$$a_{i,m} = 0, \qquad \text{for } i \ne r. \tag{2.10}$$

In case that (2.9) and (2.10) are satisfied, f is said to be of standard form, and if $a_{r-1,m-1} = 0$, then $f^{(0,b)} = f^{(1,b)}$ for $b \in \{0,1\}$ and if $a_{r,m} = 0$, then $f^{(0)} = f^{(1)}$.

Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-r}$ be a basis of the dual space of the linear subspace spanned by $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r$ in $[\mathrm{GF}(2)]^m$. Then there exists a vector $\mathbf{b}$ in $[\mathrm{GF}(2)]^m$ such that

$$s_m(f) = \{\mathbf{b} + \sum_{i=1}^{m-r} \mathbf{b}_i y_i : y_i \in \{0,1\} \text{ for } 1 \le i \le m-r\}. \tag{2.11}$$

That is, $s_m(f)$ is an $(m-r)$-flat in $[\mathrm{GF}(2)]^m$. Conversely, if $s_m(f)$ is an $(m-r)$-flat in $[\mathrm{GF}(2)]^m$, then f is a product of linearly independent r polynomials of degree one. The following fact will be used.

(F) Suppose that $f \in B_m^r$ is a product of linearly independent r polynomials $f_1, f_2, \ldots, f_r$ of degree one. Then, for $f' \in B_m^r$ different from f, there exist binary constants $c_1, c_2, \ldots, c_r$ such that

$$f' = (f_1 + c_1)(f_2 + c_2)\cdots(f_r + c_r), \tag{2.12}$$

if and only if $s_m(f)$ and $s_m(f')$ are parallel r-flats in $[\mathrm{GF}(2)]^m$.

We have the following two lemmas.

Lemma 1: Let f be a Boolean polynomial in B_m^r with $1 \le r < m-1$ such that $|f|_m = 2^{m-r}$.

(i) For $f^{(0)}$ and $f^{(1)}$, one of the following three cases holds:

Case 1: $f^{(0)} = 0$,

Case 2: $|f^{(0)}|_{m-1} = 2^{m-r}$ and $f^{(1)} = 0$,

Case 3: $|f^{(0)}|_{m-1} = |f^{(1)}|_{m-1} = 2^{m-1-r}$, and either $f^{(0)} = f^{(1)}$ or $s_{m-1}(f^{(0)})$ and $s_{m-1}(f^{(1)})$ are parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-1}$.

(ii) For $f^{(a,b)}$ with (a,b) in $\{0,1\}^2$, one of the following three cases holds:

Case 1′: One of $|f^{(a,b)}|_{m-2}$ with (a,b) in $\{0,1\}^2$ is 2^{m-r}.

Case 2′: Two of $|f^{(a,b)}|_{m-2}$ with (a,b) in $\{0,1\}^2$ is 2^{m-r-1}, and nonzero $f^{(a,b)}$ and $f^{(a',b')}$ are the same or $s_{m-2}(f^{(a,b)})$ and $s_{m-2}(f^{(a',b')})$ are parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-2}$.

Case 3′: $|f^{(a,b)}|_{m-2} = 2^{m-r-2}$ for (a,b) in $\{0,1\}^2$, and either $f^{(0,0)} = f^{(1,0)}$ or $s_{m-2}(f^{(0,0)})$ and $s_{m-2}(f^{(1,0)})$ are parallel $(m-r-2)$-flats in $[\mathrm{GF}(2)]^{m-2}$.

(Proof) As stated before, f is a product of linearly independent r polynomials $f_i = a_{i,0} + \sum_{j=1}^{m} a_{i,j}x_j$ with $1 \le i \le r$. For a and b in$\{0,1\}$, we have that for $1 \le i \le r$,

$$f^{(a)} = f_1^{(a)} f_2^{(a)} \cdots f_r^{(a)}, \tag{2.13}$$

$$f_i^{(a)} = a_{i,0} + a_{i,m}a + \sum_{j=1}^{m-1} a_{i,j}x_j, \tag{2.14}$$

$$f^{(a,b)} = f_1^{(a,b)} f_2^{(a,b)} \cdots f_r^{(a,b)}, \tag{2.15}$$

$$f_i^{(a,b)} = a_{i,0} + a_{i,m-1}a + a_{i,m}b + \sum_{j=1}^{m-2} a_{i,j}x_j. \tag{2.16}$$

For $1 \le i \le r$, let $\mathbf{a}_i$, $\mathbf{a}'_i$ and $\mathbf{a}''_i$ denote $(a_{i,1}, a_{i,2} \ldots, a_{i,m})$, $(a_{i,1}, a_{i,2} \ldots, a_{i,m-1})$, $(a_{i,1}, a_{i,2} \ldots, a_{i,m-2})$, respectively, and let r' and r'' denote the numbers of linearly independent vectors in $\{\mathbf{a}'_1, \mathbf{a}'_2, \ldots, \mathbf{a}'_r\}$ and $\{\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_r\}$, respectively. Since $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r\}$ are linearly independent,

$$r - 1 \le r' \le r, \tag{2.17}$$

$$r - 2 \le r'' \le r. \tag{2.18}$$

Assume that f is of standard form. Then $\mathbf{a}'_1, \mathbf{a}'_2, \ldots, \mathbf{a}'_{r-1}$ are linearly independent, and $\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_{r-2}$ are also linearly independent.

(A.i) Suppose that $r' = r$. Then, for $a \in \{0,1\}$, $f_i^{(a)}$ with $1 \le i \le r$ are linearly independent and from (F), (2.13), and (2.14), Case 3 holds.

(A.ii) Suppose that $r' = r-1$. Since $\mathbf{a}'_1, \mathbf{a}'_2, \ldots, \mathbf{a}'_{r-1}$ are linearly independent, $\mathbf{a}'_r$ is a linear sum of $\mathbf{a}'_1, \mathbf{a}'_2, \ldots, \mathbf{a}'_{r-1}$, denoted $\sum_{i=1}^{r-1} b_i \mathbf{a}'_i$. Since $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r$ are linearly independent, $a_{r,m} = 1$. By row operations, f can be expressed as

$$f = f_1 f_2 \cdots f_{r-1}(a_{r,0} + \sum_{i=1}^{r-1} b_i(a_{i,0} + 1) + x_m).$$

Hence, $f^{(0)}$ or $f^{(1)}$ is zero.

(B.i) Suppose that $r'' = r$. Then, for $(a,b) \in \{0,1\}^2$, $f_i^{(a,b)}$ with $1 \le i \le r$ are linearly independent, and from (F), (2.15), and (2.16), Case 3′ holds.

(B.ii) Suppose that $r'' = r-1$. Since $\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_{r-2}$ are linearly independent, by exchanging indices $r-1$ and r, if necessary, we can assume that (1) $\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_{r-1}$ are linearly independent, (2) $\mathbf{a}''_r$ is a linear sum of $\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_{r-1}$ and (3) $a_{r,m} = 1$. Then, $f_i^{(a,b)}$ with $1 \le i \le r-1$ and $(a,b) \in \{0,1\}^2$ are independent and f can be expressed as $f_1 f_2 \cdots f_{r-1}(c + c'x_{m-1} + x_m)$, where c and c' are binary constants. Hence Case 2′ holds.

(B.iii) Suppose that $r'' = r-2$. Then (1) $f_i^{(a,b)}$ with $1 \le i \le r-2$ and $(a,b) \in \{0,1\}^2$ are linearly independent, (2) $\mathbf{a}''_{r-1}$ and $\mathbf{a}''_r$ are linear sums of $\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_{r-2}$ and (3) $a_{r-1,m-1} = a_{r,m} = 1$. Hence f can be expressed as $f_1 f_2 \cdots f_{r-2}(c_{r-1} + x_{m-1})(c_r + x_m)$ by row operations, where c_{r-1} and c_r are binary constants. Consequently, Case 1′ holds. $\Delta\Delta$

The inverses of Case 3 and Case 2′ hold as shown in the following lemma.

Lemma 2: (1) Let g and h be Boolean polynomials of degree r with variables $x_1, x_2, \ldots, x_{m-1}$ such that $s_{m-1}(g)$ and $s_{m-1}(h)$ are the same or parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-1}$. Then there is a polynomial f of degree r with variables $x_1, x_2, \ldots, x_m$ such that

$$|f|_m = 2^{m-r}, \tag{2.19}$$

$$f^{(0)} = g, \tag{2.20}$$

$$f^{(1)} = h. \tag{2.21}$$

(2) Let g and h be Boolean polynomials of degree $r-1$ with variables $x_1, x_2, \ldots, x_{m-2}$ such that $s_{m-2}(g)$ and $s_{m-2}(h)$ are the same or parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-2}$. Then, for any two pairs (a,b) and (a',b') in $\{0,1\}^2$, there is a polynomial f of degree r with variables $x_1, x_2, \ldots, x_m$ such that

$$|f|_m = 2^{m-r}, \tag{2.22}$$

$$f^{(a,b)} = g, \tag{2.23}$$

$$f^{(a',b')} = h, \tag{2.24}$$

$$f^{(a'',b'')} = 0, \quad \text{for } (a'',b'') \in \{0,1\}^2 - \{(a,b),(a',b')\}. \tag{2.25}$$

(Proof) (1) If $g = h$, let $f = g$ and regard f as a polynomial in B_m^r. Consider the case where $s_{m-1}(g)$ and $s_{m-1}(b)$ are parallel $(m-r-1)$-flats. Then it follows from (F) that there exist linearly independent r polynomials of degree one, $g_i = a_{i,0} + \sum_{j=1}^{m-1} a_{i,j} x_j$ with $1 \le i \le r$, and binary constants $c_1, c_2, \ldots, c_r$ such that

$$\begin{aligned} g &= g_1 g_2 \cdots g_r, \\ h &= (g_1 + c_1)(g_2 + c_2) \cdots (g_r + c_r). \end{aligned}$$

Let f be defined as $f = f_1 f_2 \cdots f_r$, where

$$f_i = g_i + c_i x_m, \qquad \text{for } 1 \le i \le r.$$

Since $f_1, f_2, \ldots, f_r$ are linearly independent, f meets the conditions (2.19) to (2.21).
(2) There is a polynomial $f_r = a_{r,0} + a_{r,m-1}x_{m-1} + a_{r,m}x_m$ such that $f_r = 1$ if and only if $(x_{m-1}, x_m) \in \{(a,b),(a',b')\}$. If $g = h$, then let $f \stackrel{\triangle}{=} gf_r$. Otherwise, there are linearly independent $r-1$ polynomials of degree one, $g_i = a_{i,0} + \sum_{j=1}^{m-2} a_{i,j}x_j$ with $1 \le i \le r-1$, and binary constants $c_1, c_2, \ldots, c_{r-1}$ such that

$$\begin{aligned} g &= g_1 g_2 \cdots g_{r-1}, \\ h &= (g_1 + c_1)(g_2 + c_2) \cdots (g_{r-1} + c_{r-1}). \end{aligned}$$

Without loss of generality, assume that $a \neq a'$. Let f be defined as

$$f = \left(\prod_{i=1}^{r-1} [g_i + c_i(a + x_{m-1})] \right) f_r.$$

Then f meets the conditions (2.22) to (2.25). $\Delta\Delta$

3. Minimal 4-section trellis diagram for the set of minimum weight codewords of $\mathrm{RM}_{m,r}$

For a positive integer i and a nonnegative integer j not greater than i, let $\begin{bmatrix} i \\ j \end{bmatrix}$ be defined as

$$\begin{bmatrix} i \\ 0 \end{bmatrix} \stackrel{\triangle}{=} 1, \tag{3.1}$$

$$\begin{bmatrix} i \\ j \end{bmatrix} \stackrel{\triangle}{=} \frac{(2^i - 1)(2^{i-1} - 1) \cdots (2^{i-j+1} - 1)}{(2^j - 1)(2^{j-1} - 1) \cdots (2 - 1)}. \tag{3.2}$$

In $[\mathrm{GF}(2)]^i$, there are $2^{i-j}\begin{bmatrix} i \\ j \end{bmatrix}$ j-flats. Let F_i^j denotes the set of all j-flats in $[\mathrm{GF}(2)]^i$, and let $F_{i,0}^j$ denote the set of those j-flats which pass through the origin $\mathbf{0}_i$, where $\mathbf{0}_i$ denotes the zero i-tuple. F_i^j is partitioned into $\begin{bmatrix} i \\ j \end{bmatrix}$ blocks of size 2^{i-j} in such a way that two j-flats are in the same block if and only if they are parallel. For $\alpha \in F_i^j$, let $P(\alpha)$ denote the set consisting of α and all j-flats parallel to α. For a subset β of $[\mathrm{GF}(2)]^i$, $\mathbf{v}_i(\beta)$ denotes the binary 2^i-tuple $(a_1, a_2, \ldots, a_{2^i})$ such that $a_j = 1$ if and only if $j - 1 = \sum_{h=1}^{i} b_h 2^{h-1}$ and $(b_1, b_2, \ldots, b_i) \in \beta$. For subsets α and β of $[\mathrm{GF}(2)]^i$, let $\alpha \bullet \beta$ be defined as the following subset of $[\mathrm{GF}(2)]^{i+1}$:

$$\begin{aligned} \alpha \bullet \beta \stackrel{\triangle}{=} & \{(a_1, a_2, \ldots, a_i, 0) : (a_1, a_2, \ldots, a_i) \in \alpha\} \\ & \cup \{(b_1, b_2, \ldots, b_i, 1) : (b_1, b_2, \ldots, b_i) \in \beta\} \end{aligned} \tag{3.3}$$

Let C be defined as

$$C = \{\mathbf{0}\} \cup \{V_m(f) : f \in B_m^r \text{ and } |f|_m = 2^{m-r}\}. \tag{3.4}$$

Let $\mathbf{u} = V_m(f)$ and $\mathbf{v} = V_m(g)$ be two codewords in C. For $1 \le i \le n$,

$$\mathbf{u} \approx_i \mathbf{v}, \tag{3.5}$$

only if $|p_{1,i}\mathbf{u}| = |p_{1,i}\mathbf{v}|$.

First, for $1 \le i < m$, consider the relation "$\approx_{2^{m-1}}$" on C.

(C.i) If $f^{(0)} = g^{(0)} = 0$, then $\mathbf{u} \approx_{2^{m-1}} \mathbf{v}$.

(C.ii) If $|f^{(0)}|_{m-1} = |g^{(0)}|_{m-1} = 2^{m-r}$, then $\mathbf{u} \approx_{2^{m-1}} \mathbf{v}$.

By Lemma 1, there remains only Case 3, for which Lemmas 1 and 2 imply the following.

(C.iii) Suppose that $|f^{(0)}|_{m-1} = |g^{(0)}|_{m-1} = 2^{m-r-1}$. Then, $\mathbf{u} \approx_{2^{m-1}} \mathbf{v}$, if and only if $s_{m-1}(f^{(0)})$ and $s_{m-1}(g^{(0)})$ are the same or parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-1}$. For this case, the number of equivalent blocks in $\begin{bmatrix} m-1 \\ m-r-1 \end{bmatrix}$.

Consequently, $S_{2^{m-1}}$ consists of $2 + \begin{bmatrix} m-1 \\ m-r-1 \end{bmatrix}$ states, denoted $s_{2^{m-1},\mathrm{i}}$, $s_{2^{m-1},\mathrm{ii}}$, $s_{2^{m-1},\mathrm{iii}}(\alpha)$ with $\alpha \in F_{m-1,0}^{m-r-1}$, such that

(i) $L(s_0, s_{2^{m-1},\mathrm{i}}) = \{\mathbf{0}_{2^{m-1}}\}$,

(ii) $L(s_0, s_{2^{m-1},\mathrm{ii}}) = \{\mathbf{v}_{m-1}(\beta) : \beta \in F_{m-1}^{m-r}\}$,

(iii) $L(s_0, s_{2^{m-1},\mathrm{iii}}(\alpha)) = \{\mathbf{v}_{m-1}(\beta) : \beta \in P(\alpha)\}$.

For $\alpha \in F_{m-1,0}^{m-r-1}$, there are the following two cases:

(a) $\alpha = \alpha_1 \bullet \alpha_2$, where $\alpha_1 \in F_{m-2,0}^{m-r-2}$ and $\alpha_2 \in P(\alpha_1)$.

(b) $\alpha = \beta \bullet \{\mathbf{0}_{2^{m-2}}\}$, where $\beta \in F_{m-2,0}^{m-r-1}$.

For convenience, we write $s_{2^{m-1},0}$ for $s_{2^{m-1},\mathrm{i}}$, $s_{2^{m-1},1.1}(\alpha_1 \bullet \alpha_2)$ for $s_{2^{m-1},\mathrm{iii}}(\alpha_1 \bullet \alpha_2)$ with $\alpha_1 \in F_{m-2,0}^{m-r-2}$ and $\alpha_2 \in P(\alpha_1)$, $s_{2^{m-1},2}(\beta)$ for $s_{2^{m-1},\mathrm{iii}}(\beta \bullet \{\mathbf{0}_{2^{m-2}}\})$ with $\beta \in F_{m-2,0}^{m-r-1}$, and $s_{2^{m-1},4}$ for $s_{2^{m-1},\mathrm{ii}}$.

Next, for $2 \le r \le m-2$, consider the relation "$\approx_{2^{m-2}}$" on C. From Lemma 1, there are the following four cases to be considered.

(D.i) If $f^{(0,0)} = g^{(0,0)} = 0$, then $\mathbf{u} \approx_{2^{m-2}} \mathbf{v}$.

(D.ii) If $|f^{(0,0)}|_{m-2} = |g^{(0,0)}|_{m-2} = 2^{m-r}$, then $\mathbf{u} \approx_{2^{m-2}} \mathbf{v}$.

By Lemma 1, there remain the following two cases:

(D.iii) $|f^{(0,0)}|_{m-2} = |g^{(0,0)}|_{m-2} = 2^{m-r-1}$.

From Lemmas 1 and 2, $\mathbf{u} \approx_{2^{m-2}} \mathbf{v}$ if and only if $s_{m-2}(f^{(0,0)})$ and $s_{m-2}(g^{(0,0)})$ are the same or parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-2}$. For this case, the number of equivalent blocks is $\begin{bmatrix} m-2 \\ m-r-1 \end{bmatrix}$.

(D.iv) $|f^{(0,0)}|_{m-2} = |g^{(0,0)}|_{m-2} = 2^{m-r-2}$ and $f^{(0,0)} \neq g^{(0,0)}$.

Assume that $\mathbf{u} \approx_{2^{m-2}} \mathbf{v}$. There must be a polynomial h in B_m^r such that $|h|_m = 2^{m-r}$, $h^{(0,0)} = g^{(0,0)}$ and $h^{(1,0)} = f^{(1,0)}$.

Let $\mathbf{w} \stackrel{\triangle}{=} V_m(h)$. Then, it follows from (1.3) and (2.6) that

$$\mathbf{u} \approx_{2^{m-1}} \mathbf{w}. \tag{3.6}$$

It follows from (C.iii) and (3.6) that $s_{m-1}(f^{(0)})$ and $s_{m-1}(h^{(0)})$ are the same or parallel $(m-r-1)$-flats in $[\mathrm{GF}(2)]^{m-1}$. Since $h^{(1,0)} = f^{(1,0)}$, it follows from (2.5) and (2.6) that $s_{m-1}(f^{(0)})$ and $s_{m-1}(h^{(0)})$ intersect and therefore they are not parallel. Hence, $s_{m-1}(f^{(0)}) = s_{m-1}(h^{(0)})$, which contradicts the assumption that $f^{(0,0)} \neq g^{(0,0)} = h^{(0,0)}$. That is,

$$\mathbf{u} \not\approx_{2^{m-1}} \mathbf{w}. \tag{3.7}$$

For this case, the number of equivalent blocks is $2^r \begin{bmatrix} m-2 \\ m-r-2 \end{bmatrix}$.

Consequently, for $2 \leq r \leq m-2$, $S_{2^{m-2}}$ consists of the following $2 + \begin{bmatrix} m-2 \\ m-r-1 \end{bmatrix} + 2^r \begin{bmatrix} m-2 \\ m-r-2 \end{bmatrix} = 2 + \begin{bmatrix} m-1 \\ m-r-1 \end{bmatrix}$ states, denoted $s_{2^{m-2},0}$, $s_{2^{m-2},1}(\alpha)$ with $\alpha \in F_{m-2}^{m-r-2}$, $s_{2^{m-2},2}(\alpha')$ with $\alpha' \in F_{m-2,0}^{m-r-1}$, and $s_{2^{m-2},4}$ such that

(0-0) $L(s_0, s_{2^{m-2},0}) = \{\mathbf{0}_{2^{m-2}}\}$.

(0-1) $L(s_0, s_{2^{m-2},1}(\alpha)) = \{\mathbf{v}_{m-2}(\alpha)\}$.

(0-2) $L(s_0, s_{2^{m-2},2}(\alpha')) = \{\mathbf{v}_{m-2}(\beta) : \beta \in P(\alpha')\}$.

(0-4) $L(s_0, s_{2^{m-2},4}) = \{\mathbf{v}_{m-2}(\beta) : \beta \in F_{m-2}^{m-r}\}$.

(1-0,0) $L(s_{2^{m-2},0}, s_{2^{m-1},0}) = \{\mathbf{0}_{2^{m-2}}\}$.

(1-0,2) For $\beta \in F_{m-2,0}^{m-r-1}$, $L(s_{2^{m-2},0}, s_{2^{m-1},2}(\beta)) = \{\mathbf{v}_{m-2}(\gamma) : \gamma \in P(\beta)\}$.

(1-0,4) $L(s_{2^{m-2},0}, s_{2^{m-1},4}) = \{\mathbf{v}_{m-2}(\beta) : \beta \in F_{m-2}^{m-r}\}$.

(1-1) $L(s_{2^{m-2},1}(\alpha), s) = \emptyset$, for $s \in S_{2^{m-1}} - \{s_{2^{m-1},1.1}(\beta \bullet \gamma)\}$.

(1-1,1.1) for $\beta \in F_{m-2,0}^{m-r-2}$ and α and $\gamma \in P(\beta)$, $L(s_{2^{m-2},1}(\alpha), s_{2^{m-1},1.1}(\beta \bullet \gamma)) = \{\mathbf{v}_{m-2}(\delta) : \alpha \bullet \delta \in P(\beta \bullet \gamma)\}$.

(1-2) $L(s_{2^{m-2},2}(\alpha'), s) = \emptyset$, for $s \in S_{2^{m-1}} - \{s_{2^{m-1},4}, s_{2^{m-1},2}(\alpha')\}$.

(1-2,2) $L(s_{2^{m-2},2}(\alpha'), s_{2^{m-1},2}(\alpha')) = \{\mathbf{0}_{2^{m-2}}\}$.

(1-2,4) $L(s_{2^{m-2},2}(\alpha'), s_{2^{m-1},4}) = \{\mathbf{v}_{m-2}(\beta) : \beta \in P(\alpha')\}$.

(1-4) $L(s_{2^{m-2},4}, s) = \emptyset$, for $s \in S_{2^{m-1}} - \{s_{2^{m-1},4}\}$.

(1-4,4) $L(s_{2^{m-2},4}, s_{2^{m-1},4}) = \{\mathbf{0}_{2^{m-2}}\}$.

By the symmetry of $\mathrm{RM}_{m,r}$, $S_{2^{m-1}+2^{m-2}}$ consists of the following $2 + \begin{bmatrix} m-2 \\ m-r-1 \end{bmatrix} + 2^r \begin{bmatrix} m-2 \\ m-r-2 \end{bmatrix} = 2 + \begin{bmatrix} m-1 \\ m-r-1 \end{bmatrix}$ states, denoted $s_{2^{m-1}+2^{m-2},0}$, $s_{2^{m-1}+2^{m-2},1}(\alpha)$ with $\alpha \in F_{m-2}^{m-r-2}$, $s_{2^{m-1}+2^{m-2},2}(\alpha')$ with $\alpha' \in F_{m-2,0}^{m-r-1}$, and $s_{2^{m-1}+2^{m-2},4}$ such that

(2-0) $L(s_{2^{m-1},0}, s) = \emptyset$, for $s \in S_{2^{m-1}+2^{m-2}} - \{s_{2^{m-1}+2^{m-2},0}, s_{2^{m-1}+2^{m-2},2}(\alpha'), s_{2^{m-1}+2^{m-2},4}\}$.

(2-0,0) $L(s_{2^{m-1},0}, s_{2^{m-1}+2^{m-2},0}) = \{\mathbf{0}_{2^{m-2}}\}$.

(2-0,2) $L(s_{2^{m-1},0}, s_{2^{m-1}+2^{m-2},2}(\alpha')) = \{\mathbf{v}_{m-2}(\beta) : \beta \in P(\alpha')\}$.

(2-0,4) $L(s_{2^{m-1},0}, s_{2^{m-1}+2^{m-2},4}) = \{\mathbf{v}_{m-2}(\beta) : \beta \in F_{m-2}^{m-r}\}$.

(2-1.1) For $\alpha_1 \bullet \alpha_2 \in F_{m-1,0}^{m-r-1}$,

$$L(s_{2^{m-1},1.1}(\alpha_1 \bullet \alpha_2), s) = \emptyset,$$

for $s \in S_{2^{m-1}+2^{m-2}} - \{s_{2^{m-1}+2^{m-2},1}(\beta)$ with $\beta \in P(\alpha_1)\}$.

(2-1.1,1) $L(s_{2^{m-1},1.1}(\alpha_1 \bullet \alpha_2), s_{2^{m-1}+2^{m-2},1}(\beta_2)) = \{\mathbf{v}_{m-2}(\beta_1) : \beta_1 \bullet \beta_2 \in P(\alpha_1 \bullet \alpha_2)\}$.

(2-2) $L(s_{2^{m-1},2}(\beta), s) = \emptyset$, for $s \in S_{2^{m-1}+2^{m-2}} - \{s_{2^{m-1}+2^{m-2},2}(\beta), s_{2^{m-1}+2^{m-2},4}\}$.

(2-2,2) $L(s_{2^{m-1},2}(\beta), s_{2^{m-1}+2^{m-2},2}(\beta)) = \{\mathbf{0}_{2^{m-2}}\}$.

(2-2,4) $L(s_{2^{m-1},2}(\beta), s_{2^{m-1}+2^{m-2},4}) = \{\mathbf{v}_{m-2}(\gamma) : \gamma \in P(\beta)\}$.

(2-4) $L(s_{2^{m-1},4}, s) = \emptyset$, for $s \in S_{2^{m-1}+2^{m-2}} - \{s_{2^{m-1}+2^{m-2},4}\}$.

(2-4,4) $L(s_{2^{m-1},4}, s_{2^{m-1}+2^{m-2},4}) = \{\mathbf{0}_{2^{m-2}}\}$.

(3-0,f) $L(s_{2^{m-1}+2^{m-2},0}, s_f) = \{\mathbf{0}_{2^{m-2}}\} \cup \{\mathbf{v}_{m-2}(\beta) : \beta \in F_{m-2}^{m-r}\}$.

(3-1,f) $L(s_{2^{m-1}+2^{m-2},1}(\alpha), s_f) = \{\mathbf{v}_{m-2}(\alpha)\}$.

(3-2,f) $L(s_{2^{m-1}+2^{m-2},2}(\alpha'), s_f) = \{\mathbf{v}_{m-2}(\beta) : \beta \in P(\alpha')\}$.

(3-4,f) $L(s_{2^{m-1}+2^{m-2},4}, s_f) = \{\mathbf{0}_{2^{m-2}}\}$.

T consists of the following subtrellis diagrams without cross connections between them whose set of states are as follows:

(1) $\{s_{i.0}, s_{i,2}(\alpha)$ with $\alpha \in F_{m-2}^{m-r-1}, s_{i,4} :$ for $i = 2^{m-2}, 2^{m-1}, 2^{m-1} + 2^{m-2}\}$.

(2) for each $\alpha_1 \bullet \alpha_2 \in F_{m-1,0}^{m-r-1}$ such that $\alpha_2 \in P(\alpha_1)$,

$$\{s_{2^{m-2}}(\beta), s_{2^{m-1}}(\alpha_1 \bullet \alpha_2), s_{2^{m-1}+2^{m-2}}(\gamma) : \beta \text{ and } \gamma \in P(\alpha_1)\}.$$

For applications of minimum-weight trellis diagram to decoding of a block code, refer to [3,4,5].

References

[1] D.J.Muder, "Minimal Trellises for Block Codes," *IEEE Trans. Information Theory*, Vol.34,5, pp.1049–1053, September 1988.

[2] F.J.MacWilliams and N.J.A.Sloane., "The Theory of Error Correcting Codes," North–Holland, 1977.

[3] H.T.Moorthy, S.Lin and T.Kasami, "Soft-Decision Decoding of Binary Linear Block Codes Based on an Iterative Search Algorithm," submitted to *IEEE Trans. Information Theory*, 1995.

[4] S.Lin, H.T.Moorthy and T.Kasami, "An Efficient Soft-Decision Decoding Scheme for Binary Linear Block Codes," to appear in *Proc. of the 3rd International Symposium on Communication Theory & Applications*, 10–14 July 1995, Charlotte Mason Colledge, Ambleside, Lake District, UK.

[5] T.Koumoto, H.Nagano, T.Takata, T.Fujiwara, T.Kasami and S.Lin, "A New Iterative Soft-Decision Decoding Algorithm," *Technical Report of IEICE*, IT95-28 The Inst. of Electronics, Information and Communication Engineers, Japan, July 1995.