On the trellis structure of $\mathcal{GRM}$—codes

Tim Blackmore and Graham Norton*

Introduction We look at the structure of the minimal trellises of generalised Reed–Muller ($\mathcal{GRM}$)–codes. We determine how these trellis behave locally and use this to determine their state complexity. We give minimal span generator matrices (MSGMs) for these codes with an application to parallelism in uniform sectionalisations of their minimal trellises. The results generalise some of those in [2].

Generalised Reed–Muller codes We denote the finite field with q elements by $\mathbb{F}_q$. We put $P_q(m)$ equal to those polynomials in $\mathbb{F}_q[X_1, \ldots, X_m]$ of degree no more than $q-1$ in each variable and for $0 \leq \nu \leq m(q-1)-1$ we put $P_q(\nu, m)$ equal to those P in $P_q(m)$ of total degree no more than ν. For a fixed ordering $\alpha_0 < \alpha_1 < \ldots < \alpha_{q^m-1}$ of $\mathbb{F}_q^m$ and $P \in P_q(\nu, m)$ we put $ev(P) = (P(\alpha_0), P(\alpha_1), \ldots, P(\alpha_{q^m-1}))$. Then $\mathcal{GRM}_q(\nu, m)$ or just $\mathcal{GRM}(\nu, m)$ is $\{ev(P) : P \in P_q(\nu, m)\}$. We put $k(\nu, m) = \dim(\mathcal{GRM}(\nu, m))$.

Trellises A trellis for a length n code C is a graph whose vertices are placed at $n+1$ depths, here labelled -1 to $n-1$. There is a single root vertex at depth -1 and a single final vertex at depth $n-1$. Paths through the trellis, passing through one vertex at each depth, are in one–to–one correspondence with the codewords.

Trellis structure determines the speed of Viterbi decoding. Trellis complexities, such as state complexity (SC), give measures of decoding complexity. Parallel structure in a trellis can lead to quicker decoding using parallel processing.

When C is linear it has a *minimal trellis* $T(C)$ which minimises many trellises complexities. The SC of a code is the SC of its minimal trellis and is considered a fourth code parameter. Unlike the other code parameters equivalent codes can have different SC.

Local behaviour of $T(\mathcal{GRM}(\nu, m))$ For $-1 \leq i \leq n-1$ we put $s_i(C) = \log_q |V_i|$ where V_i is the set of vertices at depth i of $T(C)$. The SC of C is then $s(C) = \max\{s_i(C) : -1 \leq i \leq n-1\}$. Also we write $b_{i,j}(C)$ for $\log_q |B_{i,j}|$ where $B_{i,j}$ is the set of branches between depths i and j in $T(C)$. With $C_i^- = \{c \in C : c = (c_0, \ldots, c_i, 0, \ldots, 0)\}$ and $C_i^+ = \{c \in C : c = (0, \ldots, 0, c_{i+1}, \ldots, c_{n-1})\}$ it is well–known that

$$s_i(C) = \dim(C) - \dim(C_i^-) - \dim(C_i^+) \text{ and } b_{i,j}(C) = \dim(C) - \dim(C_i^-) - \dim(C_j^+).$$

We refer to an i where $\dim(C_i^-) = \dim(C_{i-1}^-) + 1$ as a *point of fall (PofF)* and an i where $\dim(C_i^+) = \dim(C_{i-1}^+) - 1$ as a *point of gain (PofG)*. Knowledge of where the

*Research supported by the U.K. Engineering and Physical Sciences Research Council under grant K27728

PsofF and PsofG are gives a local description of the trellis of C. We write $\delta_i(C)$ and $\gamma_i(C)$ respectively for the number of PsofF and PsofG before and including i. Thus $s_i(C) = \gamma_i(C) - \delta_i(C)$ and $b_{i,j}(C) = \gamma_j(C) - \delta_i(C)$.

We identify $\mathbb{F}_q$ with $\{0, \ldots, q-1\}$. For $\alpha_i = (i_1, \ldots, i_m) \in \mathbb{F}_q^m$ we put $|\alpha_i| = \sum_{k=1}^m i_k$. The ordering of the codewords of $\mathcal{GRM}(\nu, m)$ is determined by an ordering $\alpha_0 < \ldots < \alpha_{q^m-1}$ of $\mathbb{F}_q^m$. This ordering is a monomial ordering if $i_1 \leq j_1, \ldots, i_m \leq j_m$ implies that $\alpha_i \leq \alpha_j$. Then we say that $\mathcal{GRM}(\nu, m)$ is monomially ordered. Our characterisation of the PsofF and PsofG of $\mathcal{GRM}(\nu, m)$ generalises [2, Proposition1.1]

Proposition 1 *If $\mathcal{GRM}(\nu, m)$ is monomially ordered then i is a PofG of $\mathcal{GRM}(\nu, m)$ if and only if $|\alpha_i| \leq \nu$ and i is a PofF of $\mathcal{GRM}(\nu, m)$ if and only if $|\alpha_i| \geq m(q-1) - \nu$.*

Thus as for $\mathcal{RM}$–codes if $\mathcal{GRM}(\nu, m)$ has a total degree ordering then its SC attains the Wolf upper bound, $\min\{k(\nu, m), k(m(q-1) - nu - 1, m)\}$ (as it does with its extended cyclic ordering). In fact as for $\mathcal{RM}$–codes it is known that the SC of $\mathcal{GRM}$–codes is minimised with lexicographical ordering, [3], which is a monomial ordering. *From now on we take $\mathcal{GRM}(\nu, m)$ with lexicographic ordering* which we refer to as standard ordering. Thus $\alpha_i = (i_1, \ldots, i_m)$ if and only if $i = \sum_{j=1}^m i_j q^{j-1}$ is the q–ary expansion of i. We just write i for α_i.

SC of $\mathcal{GRM}(\nu, m)$. For a trellis function $f \in \{s, b, s_i, b_{i,j}, \gamma, \delta, T\})$ we write $f(\nu, m)$ for $f(\mathcal{GRM}(\nu, m))$. The following symmetry property of $T(\nu, m)$ is well–known for $\mathcal{RM}$–codes with standard ordering.

Proposition 2 *For $-1 \leq i \leq j \leq q^m - 1$, $b_{i,j}(\nu, m) = b_{q^m-j-2, q^m-i-2}(\nu, m)$. In particular $s_i(\nu, m) = s_{q^m-i-2}(\nu, m)$.*

The SC of $\mathcal{RM}$–codes is known, [1], and is perhaps most simply determined using the recurrence relation of [4], as in [2]. We do not have a generalisation of this recurrence relation. Instead we use that for $aq^{m-1} \leq i \leq (a+1)q^{m-1} - 1$

$$s_i(\nu, m) = \gamma_{i-aq^{m-1}}(\nu - a, m-1) - \delta_{i-aq^{m-1}}(\nu + a - q + 1, m-1) + s_{aq^{m-1}-1}(\nu, m).$$

Thus we put $\sigma_u(\nu, a, m-1) := \gamma_u(\nu - a, m-1) - \delta_u(\nu + a - q + 1, m-1)$ and note that it is straightforward to determine from Proposition 1 that

$$s_{aq^{m-1}-1}(\nu, m) = \sum_{l=0}^{a-1} \left(k(\nu - l, m-1) - k(\nu + l - q + 1), m-1)\right). \tag{1}$$

We put $Q = \lfloor q/2 \rfloor$. Then for q odd we have $\sigma_u(\nu, Q, m-1) = s_u(\nu - Q, m-1)$. Fortunately SC is attained in the range $Qq^{m-1} \leq i \leq (a+1)q^{m-1} - 1$. So we get by induction

Proposition 3 *For q odd the SC of $\mathcal{GRM}_q(\nu, m)$ is attained at $(Q, \ldots, Q)$ and $s(\nu, m) = \sum_{j=0}^{m-1} s_{Qq^{m-j-1}-1}(\nu - jQ, m-j)$, where $s_{Qq^{m-j-1}-1}(\nu - jQ, m-j)$ is given by (1).*

For even q we get that for $bq^{m-2} \leq u \leq (b+1)q^{m-2}-1$, $\sigma_u(\nu, a, m-1)$ is equal to

$$\gamma_{u-bq^{m-2}}(\nu - a - b, m-2) - \delta_{u-bq^{m-2}}(\nu + a + b - 2(q-1), m-2) + \sigma_{bq^{m-2}-1}(\nu, a, m).$$

Thus for $(Q-1)q^{m-2} \leq u \leq Qq^{m-2}-1$, $\sigma_u(\nu, Q, m-1) = s_{u-(Q-1)q^{m-2}}(\nu - q + 1, m - 2) + \sigma_{(Q-1)q^m-2}(\nu, Q, m)$. Fortunately $s_i(\nu, m)$ is maximised in the range $Qq^{m-1} \leq i \leq Qq^{m-1} + (Q-1)q^{m-2} - 1$.

Proposition 4 *For q even the SC of $\mathcal{GRM}_q(\nu, m)$ is attained at $(\ldots, Q-1, Q, \ldots, Q-1, Q)$ (and hence at $(\ldots, Q, Q-1, \ldots, Q, Q-1)$) and*

$$\begin{aligned} s(\nu, m) &= \sum_{j=0}^{(m-1)/2} s_{Qq^{m-2j-1}-1}(\nu - j(q-1), m-2j) \\ &+ \sum_{j=0}^{(m-3)/2} \sigma_{(Q-1)q^{m-2j-2}-1}(\nu - j(q-1), Q, m-2j-1). \end{aligned} \qquad (2)$$

As in Proposition 3 the first term in the right–hand side of (2) is given by (1). A similar identity holds for the second term. For $q = 2$ this second term disappears and we get the known result $s(\nu, m) = \sum_{j=0}^{(m-1)/2} \left(k(\nu - j, m-2j-1) - k(\nu - j - 1, m - 2j - 1)\right)$.

For $\nu \leq m(q-1)/2$ total degree or cyclic ordering of $\mathcal{GRM}(\nu, m)$ gives SC equal to $k(\nu, m)$ which for q odd can be shown by induction to be equal to

$$\sum_{j=0}^{m-1} \sum_{l=0}^{Q-1} \left(k(\nu - jQ - l, m - j - 1) + k(\nu - jQ + l - q + 1, m - j - 1)\right).$$

Thus the saving in SC of using standard ordering in this case is $2\sum_{j=0}^{m-1}\sum_{l=0}^{Q-1} k(\nu - jQ + l - q + 1, m - j - 1)$. Similar calculations can be done for the other cases.

Minimal Span Generator Matrices for $\mathcal{GRM}$–codes A generator matrix of a linear code can be used to construct a trellis for the code. An MSGM is a generator matrix which gives the minimal trellis. As for any linear code it is possible to determine an MSGM for a *given* $\mathcal{GRM}$–code from any generator matrix for the code. Here we give a general form MSGM for the family of $\mathcal{GRM}$–codes.

For $0 \leq a \leq q-1$ we put $r_a(X) = X(X-1)\cdots(X-q+1)/(X-a)$ and for $1 \leq n \leq m$ we put $R(n+1)$ equal to the set of those polynomials of the form $r_{a(n+1)}(X_{n+1})\cdots r_{a(m)}(X_m)$ for some $0 \leq a(n+1), \ldots, a(m) \leq q-1$. Also for $S_{q-1} \subseteq \ldots \subseteq S_1 \subseteq \{1, \ldots, n-1\}$ and $0 \leq r \leq t \leq q-2$ we put $q_1(S_1, \ldots, S_{q-1}, r, t)(X_1, \ldots, X_n)$ equal to

$$\prod_{i \in S_1} X_i \cdots \prod_{i \in S_{q-1}} (X - q + 2) \left(\frac{X_n \cdots (X_n - q + 1)}{(X_n - r) \cdots (X_n - q + 2 + t - r)} \right)$$

and $q_2(S_1, \ldots, S_{q-1}, r, t)(X_1, \ldots, X_n)$ equal to

$$\prod_{i \in S_1} (X - i - q + 1) \cdots \prod_{i \in S_{q-1}} (X_i - 1) \left(\frac{X_n \cdots (X_n - q + 1)}{(X_n - r - 1) \cdots (X_n - q + 1 + t - r)} \right).$$

For $0 \leq l \leq m(q-1)-1$, $Q(l, n-1)$ is the set of those polynomials of the form $q_1 - q_2$ for some $0 \leq r \leq q-2$, $r \leq t \leq q-2$ and $S_{q-1} \subseteq \ldots \subseteq S_1 \subseteq \{1, \ldots, n-1\}$ such that $|S_1| + \ldots + |S_{q-1}| = l - t$. Then with $R \cdot Q = \{r \cdot q : r \in R, q \in Q\}$,

THEOREM 5 *For $m \geq 1$ and $0 \leq \nu \leq m(q-1)-1$*

$$G(\nu, m) = \left[ev \left(\bigcup_{s=0}^{\nu/(q-1)} Q(\nu - s(q-1), m-s-1) \cdot R(m-s+1) \right) \right]$$

is an MSGM for $\mathcal{GRM}(\nu, m)$.

Theorem 5 gives generalisations of [2, Propositions 3.3 and 3.10]. A q^u–way sectionalisation is one in which each section has length q^{m-u}. Writing $||\nu, m, q^u||$ for the number of parallel subtrellises and $< \nu, m, q^u, l >$ for the number of branches between connected states at depths $(l-1)q^{m-u} - 1$ and $lq^{m-u} - 1$ $(0 \leq l \leq q^u)$ in a q^u–way sectionalisation of $T(\nu, m)$ we get

COROLLARY 6 *For $1 \leq u \leq m$, $\log_q ||\nu, m, q^u|| = k(\nu, m-u) - k(\nu-1, m-u)$ and $\log_q < \nu, m, q^u, l >= k(\nu - (q-1)u, m-u)$.*

It is known that $< \nu, m, q^u, l >$ is independent of l for $\mathcal{RM}$–codes. It follows from Corollary 6.2 that this is true for all q. It is stated in [5] that sectionalisations of trellises for binary codes with more than two branches between adjacent connected states are disadvantageous. From Corollary 6 we have $||\nu, m, q^u|| > 1$ and $< \nu, m, q^u, l > \leq q$ if and only if $\nu/(q-1) \leq u \leq m - \nu/(q-1)$.

References

[1] Yuval Berger and Yair Be'ery (1993) *Bounds on the trellis size of linear block codes.* IEEE Trans. Information Theory **39**, 203–209.

[2] Tim Blackmore and Graham Norton (1998) *On trellis structures for Reed–Muller codes.* Submitted for publication.

[3] Petra Heijnen and Ruud Pellikaan *Generalized Hamming weights of q–ary Reed–Muller codes.*

[4] Chung-Chin Lu and Sy–Hann Huang (1995) *On bit–level trellis complexity of Reed–Muller codes.* IEEE Trans. Information Theory **41**, 2061–2064.

[5] Hari T. Moorthy, Shu Lin and Gregory T. Uehara (1997) *Good trellises for IC implementation of Viterbi decoders for linear block codes.* IEEE Trans. Communications **45**, 52–63.