Redundancies of Correction-Capability-Optimized Reed-Muller Codes

Maria Bras-Amorós* and Michael E. O'Sullivan†

February 1, 2008

Abstract

This article is focused on some variations of Reed-Muller codes that yield improvements to the rate for a prescribed decoding performance under the Berlekamp-Massey-Sakata algorithm with majority voting. Explicit formulas for the redundancies of the new codes are given.

Introduction

Reed-Muller codes belong to the family of evaluation codes, commonly defined on an order domain. The decoding algorithm widely used for evaluation codes is an adaptation of the Berlekamp-Massey-Sakata algorithm together with the majority voting algorithm of Feng-Rao-Duursma. By analyzing majority voting, one realizes that only some of the parity checks are really necessary to perform correction of a given number of errors. New codes can be defined with just these few checks, yielding larger dimensions while keeping the same correction capability as standard codes [4, 5]. These codes are often called Feng-Rao improved codes.

A different improvement to standard evaluation codes is given in [8]. The idea is that under the Berlekamp-Massey-Sakata algorithm with majority voting, error vectors whose weight is larger than half the minimum distance of the code are often correctable. In particular this occurs for *generic errors* (also called independent errors in [9, 6]), whose technical algebraic definition can be found in the mentioned references. Generic errors of weight t can be a very large proportion of all possible errors of weight t, as in the case of the examples worked out in [8]. This suggests that a code be designed to correct only *generic errors* of weight t rather than all error words of weight t. Using this restriction, one obtains new codes with much larger dimension than that of standard evaluation codes correcting the same number of errors.

*Universitat Autònoma de Barcelona, mbras@deic.uab.cat
†San Diego State University, mosulliv@sciences.sdsu.edu

In [2] both ideas are combined. Minimal order subsets are accurately designed in order to ensure correction capability of t generic errors, under the Berlekamp-Massey-Sakata algorithm with majority voting.

The scope of this work is to give explicit formulae for the redundancies of all the Reed-Muller improved codes. In Section 1 we recall the definitions of the correction-capability-optimized codes. In Section 2 we give formulas to find their redundancies.

1 Correction-capability-optimized Reed-Muller codes

Let $n = q^m$ and call $P_1, \ldots, P_n$ the n points in $\mathbb{F}_q^m$. Let $\mathbb{F}_q[x_1, \ldots, x_m]_{\leqslant s}$ be the subspace of $\mathbb{F}_q[x_1, \ldots, x_m]$ of polynomials with total degree $\leqslant s$ and let φ_s be the map $\mathbb{F}_q[x_1, \ldots, x_m]_{\leqslant s} \longrightarrow \mathbb{F}_q^n$, $f \longmapsto (f(P_1), \ldots, f(P_n))$. The *Reed-Muller code* $RM_q(s, m)$ is defined as the orthogonal space of the image of φ.

Let $A = \mathbb{F}_q[x_1, \ldots, x_m]$ and let $\varphi : f \mapsto (f(P_1), \ldots, f(P_n))$. Variations of Reed-Muller codes can be defined by means of a subset W of monomials in $\mathbb{F}_q[x_1, \ldots, x_m]$. The order-prescribed Reed-Muller code associated to W is

$$C_W = < \varphi(W) >^{\perp} .$$

Let $\ll$ be the graded lexicographic order on monomials in A with $x_m \ll x_{m-1} \ll \cdots \ll x_1$. Let z_i be the i-th monomial with respect to $\ll$, starting with $z_0 = 1$. Let j be such that $z_j = x_1^s$, then $z_{j+1} = x_m^{s+1}$ and $\mathbb{F}_q[x_1, \ldots, x_m]_{\leqslant s}$ is the space generated by $\{z_i : i \leqslant j\}$. Consequently we have

$$RM_q(s, m) = C_{\{z_i : i \leqslant j\}}.$$

More generally, one can define the *standard Reed-Muller code* for any given j to be $C_{\{z_i : i \leqslant j\}}$.

For $m \in \mathbb{N}_0$ let

$$\nu_m = |\{j \in \mathbb{N}_0 : z_j \text{ divides } z_m\}|.$$

The sequence given by the values ν_i with $i \in \mathbb{N}_0$ has two important applications. On the one hand, it is used to define bounds on the minimum distance of evaluation codes [3, 7, 5]. On the other hand it is used to design Feng-Rao improved codes [4, 5]. The main results used for defining correction-capability-optimized codes are the two following lemmas.

Lemma 1.1. *[4] All errors of weight t can be corrected by C_W if W contains all monomials z_i with $\nu_i < 2t + 1$.*

Lemma 1.2. *[2] All generic errors of weight t can be corrected by C_W if W contains all monomials z_i which are not a product $z_j z_k$ for any $j, k \geqslant t$.*

Standard Reed-Muller codes To design a standard Reed-Muller code which will correct t errors, let $m(t) = \max\{i \in \mathbb{N}_0 : \nu_i < 2t + 1\}$. Let $R(t) = \{z_i : i \leqslant m(t)\}$ and $r(t) = |R(t)|$. The code $C_{R(t)}$ has minimum distance at least $2t + 1$.

Feng-Rao improved codes To design an order-prescribed Reed-Muller code correcting t errors, we take $\widetilde{R}(t) = \{z_i : \nu_i < 2t+1\}$ and use the code $C_{\widetilde{R}(t)}$. Let $\widetilde{r}(t) = |\widetilde{R}(t)| = m(t) + 1$. The Feng-Rao improved Reed-Muller code correcting t errors requires $r(t) - \widetilde{r}(t)$ fewer check symbols than the standard Reed-Muller code correcting t errors.

Standard generic Reed-Muller codes To design a standard Reed-Muller code that will correct all generic errors of weight at most t, let $m^*(t) = \max\{i : z_i \neq z_j z_k \text{ for all } j, k \geqslant t\}$. Define $R^*(t) = \{z_i : i \leqslant m^*(t)\}$. The number of check symbols for the code $C_{R^*(t)}$ is $r^*(t) = |R^*(t)| = m^*(t) + 1$.

Improved generic Reed-Muller codes To design an order-prescribed Reed-Muller code correcting t generic errors, we use the code $C_{\widetilde{R}^*(t)}$ where $\widetilde{R}^*(t)$ is $\{z_i : z_i \neq z_j z_k \text{ for all } j, k \geqslant t\}$. Let $\widetilde{r}^*(t) = |\widetilde{R}^*(t)|$. Clearly $\widetilde{r}^*(t) \leqslant r^*(t)$.

2 Explicit formulae for the redundancies

Lemma 2.1. *Suppose* $z_i = x_1^{a_1} \cdot \cdots \cdot x_m^{a_m}$. *Then,* $\nu_i = \prod_{l=1}^{m}(a_l + 1)$.

Proof. It is obvious, since the monomial $x_1^{b_1} \cdot \cdots \cdot x_m^{b_m}$ divides $x_1^{a_1} \cdot \cdots \cdot x_m^{a_m}$ if and only if $0 \leqslant b_l \leqslant a_l$ for all $1 \leqslant l \leqslant m$. □

The next proposition quantifies the redundancy of non-generic codes.

Proposition 2.2. *For every* $t \in \mathbb{N}_0$,

(i) $r(t) = \binom{2t-1+m}{m}$,

(ii) $\tilde{r}(t) = |\{a \in \mathbb{N}_0^m : \prod_{l=1}^{m}(a_l + 1) < 2t + 1\}|$.

Proof.

(i) The monomial z_s of largest lexicographic order for which $\nu_s < 2t + 1$ is $z_s = x_1^{2t-1}$. Thus, $m(t) = s = \binom{2t-1+m}{m} - 1$ and $r(t) = \binom{2t-1+m}{m}$.

(ii) It is a direct consequence of Lemma 2.1.

□

We now give the redundancies for generic codes.

Proposition 2.3. *Suppose* $z_t = x_1^{a_1} \cdot \cdots \cdot x_m^{a_m}$ *and let* $\mathbf{a} = |a| = a_1 + a_2 + \cdots + a_m$.

(i) *If* $a_1 = a_2 = \cdots = a_{m-1} = 0$ *(hence* $a_m = \mathbf{a}$*), then*

- $r^*(t) = \binom{2\mathbf{a}-1+m}{m}$,
- $\tilde{r}^*(t) = r^*(t)$.

(ii) *Otherwise,*

- $r^*(t) = \binom{2\mathbf{a}+1+m}{m} - \sum_{k=1}^{m} \binom{2\mathbf{a}-\sum_{l=1}^{k} a_l+m-k}{m-k}$,
- $\tilde{r}^*(t) = r^*(t) - 1 - \sum_{k=1}^{m-1} \sum_{j=k}^{m-1} \binom{2\mathbf{a}-2-\sum_{i=1}^{j} a_i-\sum_{l=1}^{k} a_l+m-j}{m-j}$
  $- |\{k : \mathbf{a} - \sum_{i=1}^{k} a_i > 0\}|$.

Proof.

(i) If $z_t = x_m^{a_m}$ then $\{z_i : z_i = z_j z_k, j, k \geqslant t\} = \{z_i : \deg z_i \geqslant 2a_m\}$. So, $r^*(t) = \tilde{r}^*(t) = \binom{2a_m-1+m}{m}$.

(ii) Otherwise, $\{z_j : j \geqslant t\} = \{z_j : \deg(z_j) > \mathbf{a}\} \sqcup \{z_j : \deg(z_j) = \mathbf{a} \text{ and } j \geqslant t\}$. So,

$$\begin{aligned} \{z_j z_k : j, k \geqslant t\} &= \{z_j z_k : \deg(z_j z_k) > 2\mathbf{a}+1\} \\ &\quad \sqcup \{z_j z_k : \deg(z_j z_k) = 2\mathbf{a}+1 \text{ and } j, k \geqslant t\} \\ &\quad \sqcup \{z_j z_k : \deg(z_j z_k) = 2\mathbf{a} \text{ and } j, k \geqslant t\}. \end{aligned}$$

Let us introduce the following notation:

$$\begin{aligned} P_{2\mathbf{a}} &= \{z_j z_k : \deg(z_j z_k) = 2\mathbf{a} \text{ and } j, k \geqslant t\}, \\ P_{2\mathbf{a}+1} &= \{z_j z_k : \deg(z_j z_k) = 2\mathbf{a}+1 \text{ and } j, k \geqslant t\}. \end{aligned}$$

Then $\tilde{r}^*(t) = |\{z_i : \deg(z_i) \leqslant 2\mathbf{a}+1\}| - |P_{2\mathbf{a}}| - |P_{2\mathbf{a}+1}|$.

One may verify that the monomial $z_i = x_1^{b_1} \cdot \cdots \cdot x_m^{b_m}$ with $\deg(z_i) = 2\mathbf{a}$ is in $P_{2\mathbf{a}}$ if and only if it satisfies one of the following:

- $b_l = 2a_l$ for all $1 \leqslant l \leqslant m$,
- There exists $1 \leqslant k \leqslant m-1$ such that
  - $b_l = 2a_l$ for all $1 \leqslant l \leqslant k-1$,
  - $b_k \geqslant 2a_k + 2$
- There exists $1 \leqslant k < j \leqslant m-1$ such that
  - $b_l = 2a_l$ for all $1 \leqslant l \leqslant k-1$,
  - $b_k = 2a_k + 1$,
  - $b_l = a_l$ for all $k+1 \leqslant l \leqslant j-1$,
  - $b_j \geqslant a_j + 1$
- There exists $1 \leqslant k \leqslant m-1$ such that
  - $b_l = 2a_l$ for all $1 \leqslant l \leqslant k-1$,
  - $b_k = 2a_k + 1$,
  - $b_l = a_l$ for all $k+1 \leqslant l \leqslant m-1$,
  - $b_m \geqslant a_m$

Consequently,

$$\begin{aligned}
|P_{2\mathbf{a}}| &= 1+\sum_{k=1}^{m-1}\binom{2\mathbf{a}-2-2\sum_{l=1}^{k}a_l+m-k}{m-k} \\
&\quad +\sum_{k=1}^{m-1}\sum_{j=k+1}^{m-1}\binom{2\mathbf{a}-2-\sum_{l=1}^{j}a_l-\sum_{l=1}^{k}a_l+m-j}{m-j} \\
&\quad +|\{k:\mathbf{a}-\sum_{l=1}^{k}a_l>0\}| \\
&= 1+\sum_{k=1}^{m-1}\sum_{j=k}^{m-1}\binom{2\mathbf{a}-2-\sum_{l=1}^{j}a_l-\sum_{l=1}^{k}a_l+m-j}{m-j} \\
&\quad +|\{k:\mathbf{a}-\sum_{l=1}^{k}a_l>0\}|.
\end{aligned}$$

Similarly, the monomial $z_i = x_1^{b_1}\cdot\cdots\cdot x_m^{b_m}$ with $\deg(z_i) = 2\mathbf{a}+1$ is in $P_{2\mathbf{a}+1}$ if and only if there exists k, $1 \leqslant k \leqslant m$, such that

- $b_l = a_l$ for all $1 \leqslant l \leqslant k-1$,
- $b_k \geqslant a_k + 1$.

and thus, $|P_{2\mathbf{a}+1}| = \sum_{k=1}^{m}\binom{2\mathbf{a}-\sum_{l=1}^{k}a_l+m-k}{m-k}$.
The reader can easily prove that if $z_i \in P_{2\mathbf{a}+1}$ then for all $j > i$ with $\deg(z_j) = 2\mathbf{a}+1$ it holds $z_j \in P_{2\mathbf{a}+1}$. The details can be found in [1]. Thus, $r^*(t) = |\{z_i : \deg(z_i) \leqslant 2\mathbf{a}+1\}| - |P_{2\mathbf{a}+1}|$.

Now,

$$\begin{aligned}
r^*(t) &= \binom{2\mathbf{a}+1+m}{m} - |P_{2\mathbf{a}+1}| \\
&= \binom{2\mathbf{a}+1+m}{m} - \sum_{k=1}^{m}\binom{2\mathbf{a}-\sum_{l=1}^{k}a_l+m-k}{m-k}
\end{aligned}$$

and

$$\begin{aligned}
\tilde{r}^*(t) &= r^*(t) - |P_{2\mathbf{a}}| \\
&= r^*(t) - 1 - \sum_{k=1}^{m-1}\sum_{j=k}^{m-1}\binom{2\mathbf{a}-2-\sum_{l=1}^{j}a_l-\sum_{l=1}^{k}a_l+m-j}{m-j} \\
&\quad -|\{k:\mathbf{a}-\sum_{l=1}^{k}a_l>0\}|.
\end{aligned}$$

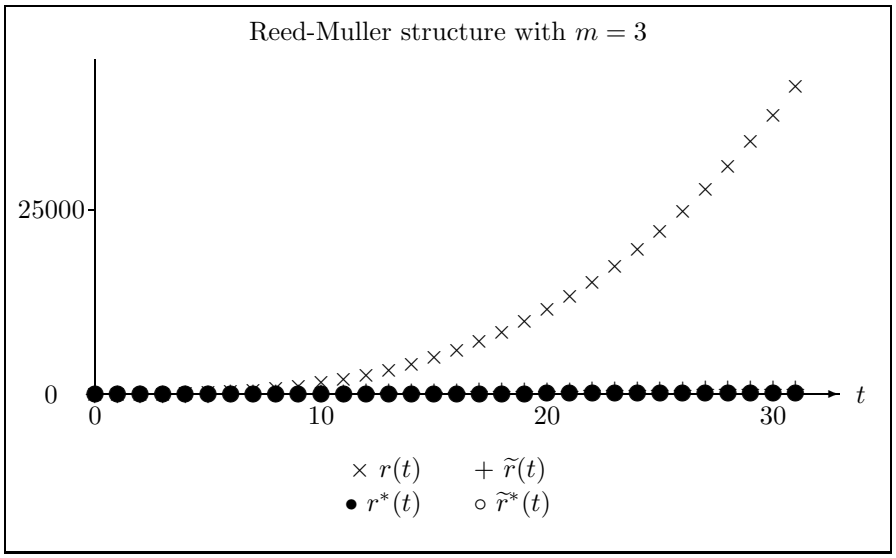

Figure 1: Redundancy values of Reed-Muller standard codes and all improved codes.

□

Remark 2.4. For $m \ll t$, $r(t)$ is $o(t^m)$, while $r^*(t)$ and $\tilde{r}^*(t)$ are $o(t)$. Indeed, notice that $\binom{a+b}{b} = \frac{a\cdot(a-1)\cdot\cdots\cdot(a-b+1)}{b!}$ is $o(a^b)$ if $a \gg b$. Now, for $m \ll t$, $r(t)$ is $o(t^m)$ while $r^*(t)$ and $\tilde{r}^*(t)$ are $o((\deg(z_t))^m)$. On the other hand, $\deg(z_t)$ is $o(t^{1/m})$, since all polynomials of degree k have order from $\binom{m+k-1}{m}$ to $\binom{m+k}{m}-1$.

Let $m = 3$. In Figure 2 we plot $r(t)$, $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$ as a function of t for the first values of t. Notice that for all t, $r(t)$ is $o(t^3)$ while $r^*(t)$ and $\tilde{r}^*(t)$ are $o(t)$. The function $\tilde{r}(t)$ seems to be also $o(t)$.

Since $r(t)$ is much larger than the other three functions, we cannot appreciate the differences between $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$. If we only plot $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$, (Figure 2) then the relative behavior of these functions becomes apparent. In particular, $\tilde{r}^*(t)$ behaves as a smooth version of $r^*(t)$.

References

[1] Maria Bras-Amorós. *Improving Evaluation Codes*. PhD thesis, Universitat Politècnica de Catalunya, Barcelona, 2003.

[2] Maria Bras-Amorós and Michael E. O'Sullivan. The correction capability of the Berlekamp-Massey-Sakata algorithm with majority voting. *Applicable Algebra in Engineering, Communication and Computing*, 2006.

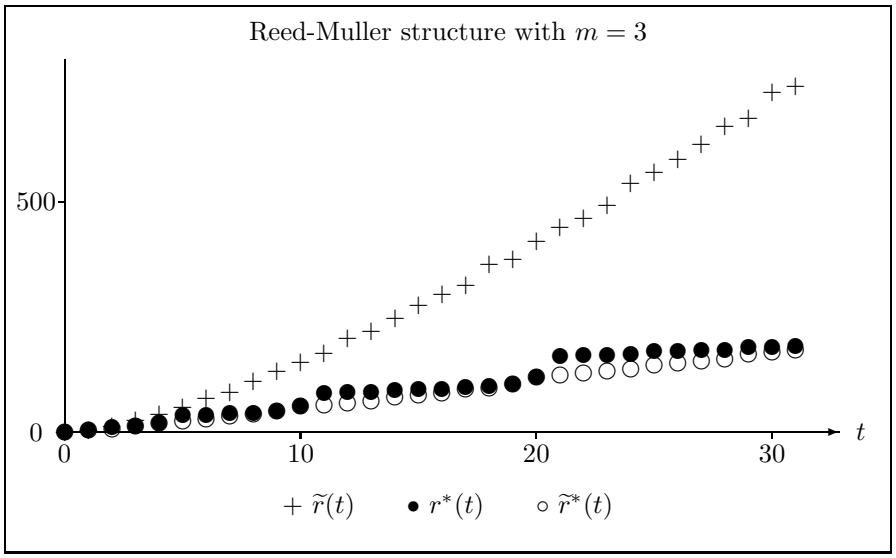

Figure 2: Redundancy values of all improved codes.

[3] Gui Liang Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.

[4] Gui-Liang Feng and T. R. N. Rao. Improved geometric Goppa codes. I. Basic theory. *IEEE Trans. Inform. Theory*, 41(6, part 1):1678–1693, 1995. Special issue on algebraic geometry codes.

[5] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. *Algebraic Geometry codes*, pages 871–961. North-Holland, Amsterdam, 1998.

[6] Helge Elbrønd Jensen, Rasmus Refslund Nielsen, and Tom Høholdt. Performance analysis of a decoding algorithm for algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(5):1712–1717, 1999.

[7] Christoph Kirfel and Ruud Pellikaan. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Trans. Inform. Theory*, 41(6, part 1):1720–1732, 1995. Special issue on algebraic geometry codes.

[8] Michael E. O'Sullivan. Decoding of Hermitian codes beyond $(d_{min} - 1)/2$. Proceedings of the IEEE International Symposium on Information Theory, Ulm, Germany, pp. 384, 1997.

[9] Ruud Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, 106/107:369–381, 1992. A collection of contributions in honour of Jack van Lint.