New descriptions of the weighted Reed-Muller codes and the homogeneous Reed-Muller codes

Harinaivo ANDRIATAHINY
Mention: Mathematics and Computer Science,
Domain: Sciences and Technologies,
University of Antananarivo, Madagascar
e-mail: hariandriatahiny@gmail.com

Vololona Harinoro RAKOTOMALALA
Mention: Meteorology,
Domain: Sciences of the Engineer,
Higher Polytechnic School of Antananarivo (ESPA),
University of Antananarivo, Madagascar
e-mail: volhrakoto@gmail.com

January 5, 2017

Abstract
We give a description of the weighted Reed-Muller codes over a prime field in a modular algebra. A description of the homogeneous Reed-Muller codes in the same ambient space is presented for the binary case. A decoding procedure using the Landrock-Manz method is developed.

Keywords: weighted Reed-Muller codes, homogeneous Reed-Muller codes, modular algebra, Jennings basis, decoding.

MSC 2010: 94B05, 94B35, 12E05.

1 Introduction

It is well known that the Generalized Reed-Muller (GRM) codes of length $p^m$ over the prime field $\mathbb{F}_p$ can be viewed as the radical powers of the modular algebra $A = \mathbb{F}_p[X_0, \ldots, X_{m-1}]/(X_0^p - 1, \ldots, X_{m-1}^p - 1)$ ([1],[4],[5]). $A$ is isomorphic to the group algebra $\mathbb{F}_p[\mathbb{F}_p^m]$.

The weighted Reed-Muller codes and the homogeneous Reed-Muller codes are classes of codes in the Reed-Muller family. The Jennings basis are used to describe the GRM codes over $\mathbb{F}_p$. We utilize the elements of the Jennings basis for the description of the weighted Reed-Muller codes and the homogeneous Reed-Muller codes in $A$. P. Landrock and O. Manz developed a decoding algorithm...
for the binary Reed-Muller codes in [9]. We use here the same method for the binary homogeneous Reed-Muller codes.

The weighted Reed-Muller codes can be considered as a generalization of the GRM codes. Some classes of the weighted Reed-Muller codes are algebraic-geometric codes.

The homogeneous Reed-Muller codes are subcodes of the GRM codes. In general, they have a much better minimum distance than the GRM codes.

We give, in section 2, the definition and some properties of the weighted Reed-Muller codes. We consider here the affine case. In section 3, a description of the weighted Reed-Muller codes over \( \mathbb{F}_p \) in the quotient ring \( A \) is presented.

In section 4, we recall the definition and the parameters of the homogeneous Reed-Muller codes. In section 5, we describe the homogeneous Reed-Muller codes over the two elements field \( \mathbb{F}_2 \) (with \( p = 2 \)). In section 6, we use the Landrock-Manz method to construct a decoding procedure for the homogeneous Reed-Muller codes in the binary case. In section 7, an example is given.

## 2 Weighted Reed-Muller codes

The definition and the properties of the weighted Reed-Muller codes presented in this section are from [11]. Let \( \mathbb{F}_q \) the field of \( q \) elements where \( p \) is a prime number and \( r \geq 1 \) is an integer. Let \( (\mathbb{F}_q)^m \) be the \( m \)-dimensional affine space defined over \( \mathbb{F}_q \). \( \mathbb{F}_q[Y_0, Y_1, \ldots, Y_{m-1}] \) is the ring of polynomials in \( m \) variables with coefficients in \( \mathbb{F}_q \). If we attach to each variables \( Y_i \) a natural number \( w_i \), called weight of \( Y_i \), we speak about the ring of weighted polynomials, \( \mathbb{W}_q[Y_0, Y_1, \ldots, Y_{m-1}] \). The weighted degree of \( F \in \mathbb{W}_q[Y_0, Y_1, \ldots, Y_{m-1}] \), is defined as

\[
\deg_w(F) = \deg_w(F(Y_0, \ldots, Y_{m-1})) = \deg(F(Y_0^{w_0}, \ldots, Y_{m-1}^{w_{m-1}})),
\]

where \( \deg \) is the usual degree.

We will, without loss of generality, always assume that the weights are ordered \( w_0 \leq w_1 \leq \ldots \leq w_{m-1} \). Consider the evaluation map

\[
\phi : \mathbb{W}_q[Y_0, \ldots, Y_{m-1}] \longrightarrow (\mathbb{F}_q)^{q^m}
\]

\[
F \mapsto \phi(F) = (F(P_1), \ldots, F(P_n))
\]

(1)

where \( P_1, \ldots, P_n (n = q^m) \) is an arbitrary ordering of the elements of \( (\mathbb{F}_q)^m \).

For \( w_0 = w_1 = \ldots = w_{m-1} = 1 \) we have the following definition.

The Generalized Reed-Muller codes of order \( \nu \) (\( 1 \leq \nu \leq m(q - 1) \)) and length \( n = q^m \) is defined by

\[
C_{\nu}(m, q) = \phi(V(\nu)),
\]

where

\[
V(\nu) = \{ F \in \mathbb{F}_q[Y_0, \ldots, Y_{m-1}] \mid \deg(F) \leq \nu \}.
\]

Let \( \omega \) be a natural number and \( \{w_0, \ldots, w_{m-1}\} \) be weights corresponding to the ring of weighted polynomials \( \mathbb{W}_q[Y_0, \ldots, Y_{m-1}] \). The weighted Reed-Muller
codes $WRMC_\omega(m, q)$ of weighted order $\omega$ and length $n = q^m$, corresponding to the weights $\{w_0, \ldots, w_{m-1}\}$ is defined by

$$WRMC_\omega(m, q) = \phi(V_\omega),$$

(2)

where

$$V_\omega = \{F \in \mathbb{F}_q[Y_0, \ldots, Y_{m-1}] \mid \deg_\omega(F) \leq \omega \}.$$  \hspace{1cm} (3)

For a polynomial $F \in \mathbb{F}_q[Y_0, \ldots, Y_{m-1}]$, $\overline{F}$ denotes the reduced form of $F$, i.e. the polynomial of lowest degree equivalent to $F$ modulo the ideal $(Y_i^q - Y_i, i = 0, \ldots, m-1)$. For any subset $M$ of $\mathbb{F}_q[Y_0, \ldots, Y_{m-1}]$, the set $\overline{M}$ denotes the set of reduced elements of $M$.

2.1 Remark. For $F \in \mathbb{F}_q[Y_0, \ldots, Y_{m-1}]$, we have

1. for every $P \in (\mathbb{F}_q)^m : F(P) = \overline{F}(P)$.
2. if $F(P) = 0$ for all $P \in (\mathbb{F}_q)^m$, then $\overline{F} = 0$.

Given natural numbers $\omega, \nu$, and a set of weights $\{w_0, \ldots, w_{m-1}\}$ such that $1 \leq \nu \leq m(q - 1)$ and $1 \leq \omega \leq (q - 1) \sum_{i=1}^{m} w_i$.

Let

$$\nu_{\max}(\omega) = Q'(q - 1) + R'$$

where

$$Q' = \max\{Q \mid \omega \geq \sum_{i=0}^{Q} (q - 1) w_i\}$$

and

$$R' = \max\{R \mid \omega \geq \sum_{i=0}^{Q'} (q - 1) w_i + Rw_{Q'+1}\}.$$  \hspace{1cm} (4)

2.2 Theorem. Given a natural number $\omega$ and a set of ordered weights $\{w_0, \ldots, w_{m-1}\}$ such that $\omega \leq (q - 1) \sum_{i=1}^{m-1} w_i$. The code $WRMC_\omega(m, q)$ is an $\mathbb{F}_q$-linear $[q^m, k, d]$ code with

$$k = \text{card}\{(e_0, \ldots, e_{m-1}) \mid \sum_{i=0}^{m-1} w_i e_i \leq \omega, 0 \leq e_i < q\}$$

and

$$d = q^m - Q - 1(q - R)$$

where $Q$ and $R$ are given by

$$\nu_{\max}(\omega) = Q(q - 1) + R,$$

with $0 \leq R < q - 1$.

2.3 Remark. The set of monomials

$$\{ \prod_{i=0}^{m-1} Y_i^{e_i} \mid \sum_{i=0}^{m-1} w_i e_i \leq \omega, 0 \leq e_i < q\}$$

is a basis of $V_\omega$.  \hspace{1cm} (5)
3 Description of the weighted Reed-Muller codes in \( A \)

Consider the modular algebra

\[
A = \mathbb{F}_p[X_0, X_1, \ldots, X_{m-1}]/(X_0^p - 1, \ldots, X_{m-1}^p - 1)
\]

and the ideal

\[
I = (X_0^p - 1, \ldots, X_{m-1}^p - 1)
\]

of the polynomial ring \( \mathbb{F}_p[X_0, \ldots, X_{m-1}] \), where \( \mathbb{F}_p \) is the prime field of \( p \) (a prime number) elements.

Set \( x_0 = X_0 + I, \ldots, x_{m-1} = X_{m-1} + I \). Let us fix an order on the set of monomials

\[
\left\{ x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \mid 0 \leq i_0, \ldots, i_{m-1} \leq p - 1 \right\}.
\]

Then

\[
A = \left\{ \sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} a_{i_0 \cdots i_{m-1}} x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \mid a_{i_0 \cdots i_{m-1}} \in \mathbb{F}_p \right\}, \quad (4)
\]

And we have the following identification:

\[ A \ni \sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} a_{i_0 \cdots i_{m-1}} x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \leftrightarrow (a_{i_0 \cdots i_{m-1}})_{0 \leq i_0, \ldots, i_{m-1} \leq p - 1} \in (\mathbb{F}_p)^m. \]

Hence the modular algebra \( A \) is identified with \( (\mathbb{F}_p)^m \).

\( P(m, p) \) denotes the vector space of the reduced polynomials in \( m \) variables over \( \mathbb{F}_p \):

\[
\left\{ P(Y_0, \ldots, Y_{m-1}) = \sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} u_{i_0 \cdots i_{m-1}} Y_0^{i_0} \cdots Y_{m-1}^{i_{m-1}} \mid u_{i_0 \cdots i_{m-1}} \in \mathbb{F}_p \right\}.
\]

Consider a set of weights \( \{w_0, \ldots, w_{m-1}\} \) and let \( \omega \) be an integer such that

\[ 0 \leq \omega \leq (p - 1)(w_0 + \ldots + w_{m-1}). \]

When considering \( P(m, p) \) and \( A \) as vector spaces over \( \mathbb{F}_p \), we have the following isomorphism:

\[
\psi : \quad P(m, p) \rightarrow A
\]

\[
P(Y_0, \ldots, Y_{m-1}) \mapsto \sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} P(i_0, \ldots, i_{m-1}) x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}. \quad (5)
\]

The set

\[
B := \{(x_0 - 1)^{i_0} \cdots (x_{m-1} - 1)^{i_{m-1}} \mid 0 \leq i_0, \ldots, i_{m-1} \leq p - 1\} \quad (6)
\]
is called the Jennings basis of $A$.
Set $\{0, p^m - 1\} = \{0, 1, 2, \ldots, p^m - 1\}$.
Let $i \in [0, p^m - 1]$. Consider its $p$-adic expansion
\[ i = \sum_{k=0}^{m-1} i_k p^k \]
with $0 \leq i_k \leq p - 1$ for all $k = 0, \ldots, m - 1$.
We need the following notations and definitions:
\[ \mathbf{i} := (i_0, \ldots, i_{m-1}), \]
the $p$-weight of $i$ is defined by
\[ \text{wt}_p(i) := \sum_{k=0}^{m-1} i_k, \]
and the $p$-weight of $i$ with respect to the set of weights $\{w_0, \ldots, w_{m-1}\}$ is defined
by
\[ \text{Wwt}_p(i) := \sum_{k=0}^{m-1} i_k w_k. \] (7)
j \leq i if $j_l \leq i_l$ for all $l = 0, 1, \ldots, m - 1$ where
\[ j := (j_0, \ldots, j_{m-1}) \in ([0, p-1])^m, \]
x \[ := (x_0, \ldots, x_{m-1}), \]
xk \[ := x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}. \]
Consider the polynomial
\[ B_i(x) := (x_0 - 1)^{i_0} \cdots (x_{m-1} - 1)^{i_{m-1}} \in A. \] (8)

The following proposition is from [1].

3.1 Proposition. We have $H_i(Y) = \psi^{-1}(B_i(\mathbf{y}))$, where $\psi$ is the isomorphism defined in (2), i.e.
\[ B_i(\mathbf{x}) = \sum_{j \leq i} H_i(j) x^j \]
where
\[ H_i(Y) := \prod_{l=0}^{m-1} H_i(Y_l) \]
and
\[ H_i(Y) = \alpha_i \prod_{j=1}^{p-1-i} (Y + j), \]
with $\alpha_i = -i! \mod p$.

3.2 Corollary. We have
\[ \deg_{\omega}(H_i(Y)) = (p - 1) \sum_{l=0}^{m-1} w_l - \text{Wwt}_p(i). \]

We now present a description of the weighted Reed-Muller code $WRM{\omega}(m,p)$ in the algebra $A$. 5
3.3 Theorem. Consider a set of weights \( \{ w_0, \ldots, w_{m-1} \} \) and let \( \omega \) be an integer such that \( 0 \leq \omega \leq (p-1) \sum_{i=0}^{m-1} w_i \). Then, the set

\[
B_\omega := \{(x_0-1)^i \cdots (x_{m-1}-1)^{i_{m-1}} \mid 0 \leq i_k \leq p-1, \sum_{k=0}^{m-1} w_k i_k \geq (p-1) \sum_{k=0}^{m-1} w_k - \omega \}
\]

forms a linear basis of the weighted Reed-Muller code \( \text{WRMC}_\omega(m,p) \) over \( \mathbb{F}_p \) in \( A \).

Proof. It is clear that \( B_\omega \) is a set of linearly independent elements because \( B_\omega \subseteq B \).

Let \( B_2(\omega) := (x_0-1)^i \cdots (x_{m-1}-1)^{i_{m-1}} \in B_\omega \), i.e. \( 0 \leq i_k \leq p-1 \), for all \( k = 0, \ldots, m-1 \), and \( \sum_{k=0}^{m-1} w_k i_k \geq (p-1) \sum_{k=0}^{m-1} w_k - \omega \).

By the Proposition 3.1 and the Corollary 3.2, we have \( B_2(\omega) = \sum_{\omega \leq 1} H_\omega(j) x^j \)
with \( H_\omega(Y) = \prod_{i=0}^{m-1} H_i(Y), H_i(Y) = \alpha_i \prod_{j=1}^{m-1} (Y + j), \) and \( \alpha_i = -i \) mod \( p \).

We have \( \deg_{\omega}(H_\omega(Y)) = (p-1) \sum_{i=0}^{m-1} w_i - \text{wt}_p(i) \leq \omega \).

Thus \( B_2(\omega) \in \text{WRMC}_\omega(m,p) \).

Therefore, \( B_2(\omega) \in \text{WRMC}_\omega(m,p) \).

It is clear that \( \dim_{\mathbb{F}_p}(\text{WRMC}_\omega(m,p)) = \text{card}\{i \in [0, p^m-1] \mid \text{wt}_p(i) \leq \omega \} \).

On the other hand, we have \( \text{card}(B_\omega) = \text{card}\{i \in [0, p^m-1] \mid \text{wt}_p(i) \geq (p-1) \sum_{k=0}^{m-1} w_k - \omega \} \).

Consider the bijection

\[
\theta : [0, p^m-1] \rightarrow [0, p^m-1] \quad i = \sum_{k=0}^{m-1} i_k p^k \mapsto \theta(i) = \sum_{k=0}^{m-1} (p-1-i_k)p^k.
\]

We have \( \text{wt}_p(\theta(i)) = \sum_{k=0}^{m-1} w_k (p-1-i_k) = (p-1) \sum_{k=0}^{m-1} w_k - \text{wt}_p(i) \), i.e. \( \text{wt}_p(\theta(i)) = (p-1) \sum_{k=0}^{m-1} w_k - \text{wt}_p(i) \).

Thus, we have \( \text{wt}_p(i) \leq \omega \iff \text{wt}_p(\theta(i)) \geq (p-1) \sum_{k=0}^{m-1} w_k - \omega \).

Hence, \( \text{card}\{i \in [0, p^m-1] \mid \text{wt}_p(i) \leq \omega \} = \text{card}\{i \in [0, p^m-1] \mid \text{wt}_p(i) \geq (p-1) \sum_{k=0}^{m-1} w_k - \omega \} \).

The following Corollary is the famous result of Berman-Charpin ([1],[4],[5]).

3.4 Corollary. Consider the weights \( w_0 = \ldots = w_{m-1} = 1 \) and an integer \( \omega \) such that \( 0 \leq \omega \leq m(p-1) \). Then, the set

\[
B_\omega := \{(x_0-1)^i \cdots (x_{m-1}-1)^{i_{m-1}} \mid 0 \leq i_k \leq p-1, \sum_{k=0}^{m-1} i_k \geq m(p-1)-\omega \}
\]

forms a linear basis of the GRM code \( C_\omega(m,p) = P^{m(p-1)-\omega} \) over \( \mathbb{F}_p \), where \( P \) is the radical power of \( A \).
4 The homogeneous Reed-Muller codes

In this section, we recall the definition and some properties of the homogeneous Reed-Muller codes [3],[10]. \( \mathbb{F}_q \) denote the field of \( q = p^r \) elements with \( p \) a prime number and \( r \geq 1 \) an integer. For \( n = q^m - 1 \), let \( \{0, P_1, \ldots, P_n\} \) be the set of points in \( (\mathbb{F}_q)^m \) ordered in a fixed order.

Let \( \mathbb{F}_q[Y_0, \ldots, Y_{m-1}]_d^0 \) be the vector space of homogeneous polynomials in \( m \) variables over \( \mathbb{F}_q \) of degree \( d \).

Now \( d \) denote an integer such that \( 0 \leq d \leq m(q-1) \). The \( d \)th order homogeneous Reed-Muller (HRM) codes of length \( q^m \) over \( \mathbb{F}_q \) is defined as
\[
HRMC_d(m, q) := \{ (F(0), F(P_1), \ldots, F(P_n)) \mid F \in \mathbb{F}_q[Y_0, \ldots, Y_{m-1}]_d^0 \}. \quad (9)
\]

Thus \( HRMC_d(m, q) \) is a proper subcode of the GRM code \( C_d(m, q) \).

The following theorem can be found in [3].

4.1 Theorem. Let \( d \) such that \( 1 \leq d \leq (m - 1)(q - 1) \). The HRM code \( HRMC_d(m, q) \) is an \([n + 1, k, \delta]\) linear code with
\[
k = \sum_{t \equiv d \mod(q-1), 0 < t \leq d} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t - jq + m - 1}{t - jq},
\]
and
\[
\delta = (q - 1)(q - s)q^{m-r-2},
\]
where \( d - 1 = r(q - 1) + s \) and \( 0 \leq s < q - 1 \).

5 Description of the binary HRM codes in \( A \)

First, we recall some results in the Proposition 3.1 for the special case \( p = 2 \).

In this section, we consider the ambient space
\[
A = \mathbb{F}_2[X_0, \ldots, X_{m-1}]/(X_0^2 - 1, \ldots, X_{m-1}^2 - 1).
\]

We have
\[
B_d(x) = (x_0 - 1)^{i_0} \ldots (x_{m-1} - 1)^{i_{m-1}} = \sum_{j \leq i} H_d(j) x^j
\]
where \( 0 \leq i_k \leq 1 \), for all \( k \),
\[
H_d(Y) := \prod_{l=0}^{m-1} H_{i_l}(Y)
\]
and
\[
H_i(Y) = \alpha_i \prod_{j=1}^{1-i} (Y + j),
\]
\[
\delta = (q - 1)(q - s)q^{m-r-2},
\]
where \( d - 1 = r(q - 1) + s \) and \( 0 \leq s < q - 1 \).
with $\alpha_i = -i! \mod 2$.

Note that $B_{(1,1,\ldots,1)}(x) = (x_0 - 1)^1 \cdots (x_{m-1} - 1)^1 = \hat{1}$ is the "all one" word.

Let $d$ be an integer such that $0 \leq d \leq m$. The $d$th order homogeneous Reed-Muller (HRM) codes of length $2^m$ over $\mathbb{F}_2$ is defined as

$$HRMC_d(m, 2) := \{(F(0), F(P_1), \ldots, F(P_n)) | F \in \mathbb{F}_2[Y_0, \ldots, Y_{m-1}]^d\},$$

where $n = 2^m - 1$. We now give the description of the binary HRM code $HRMC_d(m, 2)$ in $A$.

**5.1 Theorem.** Let $d$ be an integer such that $1 \leq d \leq m$. The set

$$\{(x_0 - 1)^{i_0} \cdots (x_{m-1} - 1)^{i_{m-1}} + \hat{1} | 0 \leq i_k \leq 1, m > \sum_{k=0}^{m-1} i_k \geq m - d\}$$

forms a linear basis for the binary HRM code $HRMC_d(m, 2)$.

**Proof.** Let $d$ such that $1 \leq d \leq m$.

Consider the element

$$B_d(x) + \hat{1} = (x_0 - 1)^{i_0} \cdots (x_{m-1} - 1)^{i_{m-1}} + \hat{1},$$

where $0 \leq i_k \leq 1$ for all $k$ and $m > \sum_{k=0}^{m-1} i_k \geq m - d$.

Set $D(\hat{i}) := \{j \in (\{0, 1\})^m | j \leq \hat{i}\}$ and $C(\hat{i}) := (\{0, 1\})^m - D(\hat{i})$.

We have $H_{d}(\hat{j}) = 0$ for $\hat{j} \in C(\hat{i})$.

Thus

$$B_d(x) = \sum_{\hat{j} \leq \hat{i}} H_{d}(\hat{j})x^\hat{j} = \sum_{j \in (\{0, 1\})^m} H_{d}(\hat{j})x^j.$$

We have

$$H_{d}(Y) := \prod_{l=0}^{m-1} H_{l}(Y_l),$$

where

$$H_{1}(Y) = 1, H_{0}(Y) = Y + 1. \quad (10)$$

Since $\sum_{k=0}^{m-1} i_k \geq m - d$, then $B_d(x) \in P^{m-d}$ where $P$ is the radical of the modular algebra $A$.

And since $P^{m-d} = C_d(m, 2)$, then $H_{d}(Y) \in P_d(m, 2)$ where $P_d(m, 2)$ is a linear space generated by the set

$$\{Y_0^{i_0} \cdots Y_{m-1}^{i_{m-1}} | 0 \leq i_k \leq 1, 0 \leq \sum_{k=0}^{m-1} i_k \leq d\}. \quad (11)$$

We have

$$B_d(x) + \hat{1} = \sum_{j \in (\{0, 1\})^m} (H_{d}(\hat{j}) + 1)x^j.$$

8
By (10) and (11), we have $H_d(Y) + 1 \in \mathbb{F}_2[Y_0, \ldots, Y_{m-1}]_d^0$. Note that $\mathbb{F}_2[Y_0, \ldots, Y_{m-1}]_d^0$ is a linear space generated by the set

$$S := \{Y_0^{i_0} \cdots Y_{m-1}^{i_{m-1}} | 0 \leq i_k \leq 1, 0 < \sum_{k=0}^{m-1} i_k \leq d\}.$$ 

Thus $B_d(x) + \hat{1} \in HRMC_d(m, 2)$. Note also that $\sum_{k=0}^{m-1} i_k = m$ if and only if $i_k = 1$ for all $k = 0, \ldots, m - 1$.

Set $R := \{(x_0 - 1)^{i_0} \cdots (x_{m-1} - 1)^{i_{m-1}} + \hat{1} | 0 \leq i_k \leq 1, m > \sum_{k=0}^{m-1} i_k \geq m - d\}$. We will show that $\dim_{\mathbb{F}_2}(HRMC_d(m, 2)) = \text{card}(R)$.

We have $\dim_{\mathbb{F}_2}(HRMC_d(m, 2)) = \dim_{\mathbb{F}_2}(\mathbb{F}_2[Y_0, \ldots, Y_{m-1}]_d^0) = \text{card}(S)$. Consider the bijection

$$\beta : (\{0, 1\})^m \to (\{0, 1\})^m$$

$$(i_0, \ldots, i_{m-1}) \mapsto (1 - i_0, \ldots, 1 - i_{m-1})$$

Set $R' := \{\hat{1} = (i_0, \ldots, i_{m-1}) \in (\{0, 1\})^m | \sum_{k=0}^{m-1} i_k \geq m - d\}$ and $S' := \{\hat{1} = (i_0, \ldots, i_{m-1}) \in (\{0, 1\})^m | \sum_{k=0}^{m-1} i_k \leq d\}$. It is clear that $S' = \beta(R')$. Thus $\text{card}(R') = \text{card}(S')$. Since $\text{card}(R) = \text{card}(R') - 1$ and $\text{card}(S) = \text{card}(S') - 1$, then $\text{card}(R) = \text{card}(S)$. \hfill \Box

6 Decoding procedure for the binary HRM codes

In this section, we will follow Landrock-Manz as in [9].

Let $d$ be an integer such that $1 \leq d \leq m$. The HRM code $HRMC_d(m, 2)$ is of type $\left[2^m, \sum_{i=1}^{d} \binom{m}{i}, 2^{m-d}\right]$ over $\mathbb{F}_2$.

Set $b(\{i_1, \ldots, i_t\}) := (x_{i_1} - 1) \cdots (x_{i_t} - 1)$, where $\{i_1, \ldots, i_t\} \subseteq \{0, 1, \ldots, m - 1\}$.

$B_{m-d} := \{b(\eta) + \hat{1} | \eta \subseteq \{0, 1, \ldots, m - 1\}, m > \text{card}(\eta) \geq m - d\}$ is a linear basis of $HRMC_d(m, 2)$.

General results of the following Proposition can be found in [2].

6.1 Proposition. We have

1. $b(\{\}) = 1$.

2. $b(\eta) \cdot b(\kappa) = \begin{cases} 0 & \text{if } \eta \cap \kappa \neq \{\}, \\ b(\eta \cup \kappa) & \text{otherwise}. \end{cases}$

3. The weight of the codeword $w(b(\{i_1, \ldots, i_t\})) = 2^t$.

4. $b(\{0, 1, \ldots, m - 1\}) = \hat{1}$ the "all one" word.

5. $\hat{1} \cdot b(\{\eta\}) = 0$ if $\eta \neq \{\}$.
Set \( \eta^c := \{0,1,\ldots,m-1\} - \eta \).

Let \( c \in HRMC_d(m,2) \) be a transmitted codeword and \( v \in A \) the received vector, where

\[
A = F_2[X_0,\ldots,X_{m-1}]/(X_0^2 - 1,\ldots,X_{m-1}^2 - 1)
\]

Since \( HRMC_d(m,2) \) is \((2^{m-d-1} - 1)\)-error correcting, we write \( v = c + f \) with \( w(f) \leq 2^{m-d-1} - 1 \).

We have

\[
c = \sum_{m-d \leq \text{card}(\eta) < m, \eta \subseteq \{0,1,\ldots,m-1\}} \tau(\eta)(b(\eta) + \hat{1})
\]

with \( \tau(\eta) \in F_2 \).

We now present the decoding procedure to determine the coefficients \( \tau(\eta) \).

Step 1:

Let \( \kappa \) be a subset of \( \{0,1,\ldots,m-1\} \) such that \( \text{card}(\kappa) = m - d \). We have

\[
v.b(\kappa^c) = (c + f).b(\kappa^c) = \sum \tau(\eta)(b(\eta) + \hat{1}) + f.b(\kappa^c)
\]

\[
= \sum \tau(\eta)(b(\eta))b(\kappa^c) + \hat{1}.b(\kappa^c) + f.b(\kappa^c)
\]

\[
= \tau(\kappa).\hat{1} + f.b(\kappa^c)
\]

We have \( w(f.b(\kappa^c)) \leq w(f.w(b(\kappa^c))) \leq (2^{m-d-1} - 1).2^d = 2^m - 2^d < 2^{m-1} \leq \frac{1}{2}2^m \).

Then it is easy to see that

\[ \tau(\kappa) = 0 \text{ if and only if } w(v.b(\kappa^c)) < 2^{m-1}. \]

We next subtract \( \tau(\kappa).b(\kappa + \hat{1}) \) from \( v \) and obtain \( v' = v + \tau(\kappa).b(\kappa + \hat{1}) = c' + f \) where \( c' = c + \tau(\kappa).b(\kappa + \hat{1}) \in HRMC_d(m,2) \).

Consider another set \( \eta \) of cardinality \( \text{card}(\eta) = m - d \), multiply \( v' \) by \( b(\eta^c) \) and find so \( \tau(\eta) \). Having eventually run through all sets of cardinality \( m - d \), we end up with \( v'' = c'' + f \), where \( c'' \in HRMC_{d-1}(m,2) \).

Step 2:

We now fix a set \( \kappa \) of cardinality \( m - d + 1 \) and by using the same technique as in the first step, we can find the coefficient \( \tau(\kappa) \). We repeat the same treatment for all set \( \eta \) of cardinality \( m - d + 1 \). We eventually determine

\[
c = \sum_{m-d \leq \text{card}(\eta) < m, \eta \subseteq \{0,1,\ldots,m-1\}} \tau(\eta)(b(\eta) + \hat{1}).
\]

If another step is needed, we must pick a set \( \kappa \) of cardinality \( m - d + 2 \) and determine \( \tau(\kappa) \), and we continue in this way.
7 An example

Consider the binary HRM code \( HRMC_1(5, 2) \). This code is of type \([32, 5, 16]\).

Set \( \tilde{E}_l = \prod_{k \neq l} (x_k - 1) = b(\{l\}^c) \), where \( l \in \{0, 1, 2, 3, 4\} \).

The set \( \{\tilde{E}_l + \hat{1} \mid 0, 1, 2, 3, 4\} \) forms a linear basis for \( HRMC_1(5, 2) \).

Let \( c = \sum_{i=0}^{4} \tau_i(\tilde{E}_i + \hat{1}) \) be a transmitted codeword with \( \tau_i \in F_2 \) and \( v \in A = F_2[X_0, X_1, \ldots, X_4]/(X_0^2-1, \ldots, X_4^2-1) \) the received vector. Since \( HRMC_1(5, 2) \) is 7-error correcting, we write \( v = c + f \) with \( w(f) \leq 7 \).

We have

\[ v.(x_j - 1) = (c + f).(x_j - 1) = c.(x_j - 1) + f.(x_j - 1) = \tau_j \hat{1} + f.(x_j - 1) \text{ for } j = 0, 1, 2, 3, 4. \]

Since \( w(f.(x_j - 1)) \leq w(f).w((x_j - 1)) \leq 7 \ast 2 = 14 < 16 \), then we have the following Proposition

7.1 Proposition.

\[ \tau_j = 0 \text{ if and only if } w(v.(x_j - 1)) < 16 \]

By multiplying \( v \) with \( (x_j - 1) \) for \( j = 0, 1, 2, 3, 4 \) and utilizing the Proposition 7.1 we obtain the coefficients \( \tau_0, \tau_1, \tau_2, \tau_3, \tau_4 \) of \( c \).

References

[1] H. Andriatahiny, The Generalized Reed-Muller codes and the Radical Powers of a modular algebra, British Journal of Mathematics and Computer Science, 18(5):1-14, 2016.

[2] E. F. Assmus and J. D. Key, Polynomial codes and finite geometries, Handbook of Coding Theory, 1994.

[3] T.P. Berger, Automorphism Groups of Homogeneous and Projective Reed-Muller Codes, IEEE Transactions on Information Theory 48, no.5:1035-1045, 2002.

[4] S. D. Berman, On the theory of group codes, Kibernetika 3(1):31-39, 1967.

[5] P. Charpin, Une généralisation de la construction de Berman des codes de Reed et Muller p-aires, Communications in algebra 16:2231-2246, 1988.

[6] E. Coucelo, S. Gonzalez, VT. Markov, C. Martinez, AA. Nechaev, Ideal representation of Reed-Solomon and Reed-Muller codes, Algebra and Logic, vol.51, no.3, 2012.

[7] S.A. Jennings, The structure of the group ring of a p-group over a modular field, Trans.Amer.Math.Soc., 50:175-185, 1941.

[8] T. Kasami, S. Lin and W. W. Peterson, New generalizations of the Reed-Muller codes, IEEE Transactions on Information Theory 14, no.2:189-205, 1968.
[9] Landrock P. and Manz O., *Classical Codes as Ideals in Group Algebras*, Designs, Codes and Cryptography, 2:273-285, 1992.

[10] O. Moreno, I.M. Duursma, J.P. Cherdieu, A. Edouard, *Cyclic Subcodes of Generalized Reed-Muller Codes*, IEEE Transactions on Information Theory 44, no.1:307-311, 1998.

[11] A.B. Sorensen, *Weighted Reed-Muller Codes and Algebraic-Geometric Codes*, IEEE Transactions on Information Theory 38, no.6:1821-1826, 1992.

[12] J.H. Van Lint, *Introduction to Coding Theory*, 3rd ed., Springer, 1998.