ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **11** (2022), no.9, 803–816
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.11.9.5

DECODING BINARY REED-MULLER CODES VIA GROEBNER BASES

Irrish Parker Ramahazosoa[1], Harinaivo Andriatahiny, and J.J. Ferdinand Randriamiarampanahy

ABSTRACT. The binary Reed-Muller codes can be characterized as the radical powers of a modular group algebra. In this paper, we deal with the Groebner bases to decode these codes.

INTRODUCTION

Several authors have studied the Reed-Muller codes (see e.g. [4], [5], [7], [8]). S.D. Berman [3] showed that the binary Reed-Muller codes can be described as the radical powers of the group algebra $\mathbb{F}_2[G]$ where $\mathbb{F}_2$ is the field of two elements and G is the additive group of the field $\mathbb{F}_{2^m}$ of 2^m elements with $m \geq 1$ an integer. $\mathbb{F}_2[G]$ is isomorphic to the quotient ring $\mathcal{A} = \mathbb{F}_2[X_1, \ldots, X_m]/\langle X_1^2 - 1, \ldots, X_m^2 - 1\rangle$. If M is the radical of $\mathcal{A}$, then the Jennings basis of M^ℓ is a linear basis of M^ℓ over $\mathbb{F}_2$. Moreover, it is well-known that the Groebner basis is an efficient algebraic tool to solve a large range of problems (see e.g. [1], [6], [9]). In this paper, using the fact that from the Jennings basis of M^ℓ, one can construct a basis for the ideal M^ℓ and dealing with Groebner bases properties, we give an algorithm for decoding the binary Reed-Muller codes.

[1] *corresponding author*
2020 *Mathematics Subject Classification.* 94B05, 12E05, 13P10, 94B35.
Key words and phrases. Reed-Muller code, Polynomial Ideal, Groebner Basis.
Submitted: 29.08.2022; *Accepted:* 15.09.2022; *Published:* 30.09.2022.

1. GROEBNER BASIS

In this section, we introduce some background about Groebner bases (see [1], [6]) and Reed-Muller codes which are useful to our results.

Definition 1.1. *Let k be a field and $\mathbb{N}$ the set of non negative integers. A monomial in the polynomial ring $k[X_1, \ldots, X_m]$ is a product of the form $X^\alpha = X_1^{\alpha_1} \ldots X_m^{\alpha_m}$ with $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$. Let $\mid \alpha \mid = \alpha_1 + \cdots + \alpha_m$ be the total degree of the monomial X^α.*

A monomial order in $k[X_1, \ldots, X_m]$ is a relation denoted $>$ on $\mathbb{N}^m$ satisfying for $\alpha, \beta \in \mathbb{N}^m$:

(i) *$>$ is a linear order on $\mathbb{N}^m$,*
(ii) *if $\alpha > \beta$ and $\gamma \in \mathbb{N}^m$, then $\alpha + \gamma > \beta + \gamma$,*
(iii) *$>$ is a well-ordering on $\mathbb{N}^m$.*

We will write $\alpha > \beta$ in $\mathbb{N}^m$ if and only if $X^\alpha > X^\beta$ in $k[X_1, \ldots, X_m]$.

Example 1.

- *Lexicographic order $>_{lex}$:*

  $\alpha >_{lex} \beta$ if, and only if, the left-most non zero entry of $\alpha - \beta$ is positive.

- *Graded lexicographic order $>_{grlex}$:*

  $\alpha >_{grlex} \beta$ if, and only if, $\mid \alpha \mid > \mid \beta \mid$ or $\mid \alpha \mid = \mid \beta \mid$ and $\alpha >_{lex} \beta$.

Definition 1.2. *A polynomial $f \in k[X_1, \ldots, X_m]$ is a linear combination of monomials with coefficients in k : $f = \sum_\alpha a_\alpha X^\alpha$.*

Let $>$ be a monomial order on $k[X_1, \ldots, X_m]$.

The multidegree of f is defined as $\operatorname{multideg}(f) = \max_>(\alpha | a_\alpha \neq 0)$. We call

- *leading coefficient of f: $\operatorname{lc}(f) = a_{\operatorname{multideg}(f)}$*
- *leading monomial of f: $\operatorname{lm}(f) = X^\alpha$ where $\alpha = \operatorname{multideg}(f)$.*
- *initial term of f: $\operatorname{in}(f) = a_\alpha X^\alpha$ where $\alpha = \operatorname{multideg}(f)$.*

Theorem 1.1. *Let $>$ be a monomial order and $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[X_1, \ldots, X_m]$. Then, every polynomial $f \in k[X_1, \ldots, X_m]$ can be written as $f = a_1 f_1 + \cdots + a_s f_s + r$ with $a_i, r \in k[X_1, \ldots, X_m]$ where $r = 0$ or r is a linear combination of monomials with coefficients in k none of which is divisible by any of $\operatorname{in}(f_1), \ldots, \operatorname{in}(f_s)$. The polynomial r is called the remainder on division of f by F. Furthermore, if $a_i f_i \neq 0$ then $\operatorname{multideg}(f) \geq \operatorname{multideg}(a_i f_i)$.*

Remark 1.1. *The operation of computing the remainders on division by $F = (f_1, \ldots, f_s)$ is linear over k. In fact, if r_i ($i = 1, 2$) is the remainder on division of g_i by F, then for any $c_1, c_2 \in k$, the remainder on division of $c_1 g_1 + c_2 g_2$ by F is $c_1 r_1 + c_2 r_2$.*

Definition 1.3. *Fix a monomial order and let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal, $I \neq \{0\}$. We call initial ideal of I the ideal of $k[X_1, \ldots, X_m]$ generated by all initial terms $\mathrm{in}(f), f \in I$, i.e. $\mathrm{in}(I) = \langle \mathrm{in}(f) | f \in I \rangle$.*

A finite set $G = \{g_1, \ldots, g_s\}$ is a Groebner basis for I if the initial terms $\mathrm{in}(g_1), \ldots, \mathrm{in}(g_s)$ generate $\mathrm{in}(I)$, i.e. $\mathrm{in}(I) = \langle \mathrm{in}(g_1), \ldots, \mathrm{in}(g_s) \rangle$.

Theorem 1.2. *Fix a monomial order. Every ideal I in $k[X_1, \ldots, X_m]$, $I \neq \{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is a basis for I.*

Proof. cf [6] p.75 □

Proposition 1.1. *Let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis for an ideal $I \subseteq k[X_1, \ldots, X_m]$. For $f \in k[X_1, \ldots, X_m]$ there is a unique remainder r on division of f by G with the following properties:*

(1) *no term of r is divisible by any of $\mathrm{in}(g_1), \ldots, \mathrm{in}(g_s)$,*
(2) *there is $g \in I$ such that $f = g + r$.*

The remainder r is unique up to how the elements of G are listed in the division by G. We will write $r = \mathrm{rem}_G(f)$ or simply $\mathrm{rem}(f)$ if confusion does not happen.

Corollary 1.1. *Let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis for an ideal $I \subseteq k[X_1, \ldots, X_m]$ and let $f \in k[X_1, \ldots, X_m]$. Then, $\quad f \in I \Longleftrightarrow \mathrm{rem}_G(f) = 0$.*

Definition 1.4. *Let X^α, X^β be two monomials with $\alpha = (\alpha_1, \ldots, \alpha_m)$ and $\beta = (\beta_1, \ldots, \beta_m)$. The least common multiple of X^α* and *X^β is the monomial $X^\gamma = \mathrm{lcm}(X^\alpha, X^\beta)$ where $\gamma = (\gamma_1, \ldots, \gamma_m)$ with $\gamma_i = \max(\alpha_i, \beta_i)$ for $i = 1, \ldots, m$.*

For $f, g \in k[X_1, \ldots, X_m]$, we call the S-polynomial of f and g the polynomial

$$S(f, g) = \frac{X^\gamma}{\mathrm{in}(f)} \cdot f - \frac{X^\gamma}{\mathrm{in}(g)} \cdot g$$

where $\gamma = \mathrm{lcm}(\mathrm{multideg}(f), \mathrm{multideg}(g))$.

Theorem 1.3. *Let I be a polynomial ideal and $G = \{g_1, \cdots, g_s\}$ a basis for I. Then, G is a Groebner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero (G listed in some order).*

Definition 1.5. *A Groebner basis G for a polynomial ideal I is said reduced if*

(1) $\mathrm{lc}(g) = 1$ *for all* $g \in G$.
(2) *For all* $g \in G$ *no monomial of* g *lies in* $\langle \mathrm{in}(f) \mid f \in G \setminus \{g\} \rangle$.

Proposition 1.2. *Fix a monomial order. Every polynomial ideal of the ring* $k[X_1, \dots, X_m]$ *has a unique reduced Groebner basis.*

2. Reed-Muller codes

In this section, we recall some properties of the Reed-Muller codes of length 2^m over $\mathbb{F}_2$. Let us consider the set in the polynomial ring $\mathbb{F}_2[X_1, \dots, X_m]$

$$H = \{X_1^2 - 1, \dots, X_m^2 - 1\}$$

and the quotient ring $\mathcal{A} = \mathbb{F}_2[X_1, \dots, X_m]/\langle H \rangle$ where $\langle H \rangle$ is the ideal generated by H. We will denote respectively by $x_1, \dots, x_m$ the equivalence classes $\mod \langle H \rangle$ of the variables $X_1, \dots, X_m$ i.e.

$$x_i = X_i + \langle H \rangle \quad \text{for} \quad i = 1, \dots, m,$$

Then, every element of $\mathcal{A}$ can be written as

$$a(x) = \sum_{i \in \{0,1\}^m} a_i x^i = \sum_{i_1=0}^{1} \cdots \sum_{i_m=0}^{1} a_{i_1,\dots,i_m} x_1^{i_1} \cdots x_m^{i_m}$$

with $i = (i_1, \dots, i_m) \in \{0,1\}^m$, $x^i = x_1^{i_1} \cdots x_m^{i_m}$ and $a_i = a_{i_1,\dots,i_m} \in \mathbb{F}_2$.

We always consider the corresponding standard representative

$$a(X) = \sum_{i \in \{0,1\}^m} a_i X^i = \sum_{i_1=0}^{1} \cdots \sum_{i_m=0}^{1} a_{i_1,\dots,i_m} X_1^{i_1} \cdots X_m^{i_m} \in \mathbb{F}_2[X_1, \dots, X_m]$$

with $X^i = X_1^{i_1} \cdots X_m^{i_m}$. It is clear that $a(x) = a(X) + \langle H \rangle$.

Let us fix an order on the set of monomials $\{x^i \mid i \in \{0,1\}^m\}$. Then we have the following isomorphism:

$$\begin{array}{cccc} \phi & : & \mathcal{A} & \longrightarrow & (\mathbb{F}_2)^{2^m} \\ & & a(x) = \displaystyle\sum_{i=(i_1,\dots,i_m) \in \{0,1\}^m} a_i x^i & \longmapsto & a = (a_i)_{i=(i_1,\dots,i_m) \in \{0,1\}^m} \end{array} \tag{2.1}$$

A linear code of length 2^m over $\mathbb{F}_2$ is a linear subspace of $(\mathbb{F}_2)^{2^m}$. By the isomorphism ϕ, $\mathcal{A}$ can be considered as the ambient space for the codes and the codeword $a = (a_i)_{i=(i_1,\ldots,i_m)\in\{0,1\}^m}$ can be identified with the polynomial $a(x) = \sum_{i=(i_1,\ldots,i_m)\in\{0,1\}^m} a_i x^i$.

We have the following well-known result.

Theorem 2.1. *The ring $\mathcal{A}$ is a local ring and its maximal ideal is the radical of $\mathcal{A}$ denoted $\mathcal{M} = rad(\mathcal{A})$. Moreover, for each integer $0 \le \ell \le m$, the set*

$$\mathcal{J}_\ell = \left\{ (x_1-1)^{i_1}\cdots(x_m-1)^{i_m} \in \mathcal{A} \mid 0 \le i_1,\ldots,i_m \le 1,\ \sum_{k=1}^{m} i_k \ge \ell \right\} \tag{2.2}$$

is a linear basis for the radical power $\mathcal{M}^\ell$ over $\mathbb{F}_2$. It is known as the Jennings basis of $\mathcal{M}^\ell$, and we have the following ascending chain of ideals

$$\{0\} \subset \mathcal{M}^m \subset \mathcal{M}^{m-1} \subset \cdots \subset \mathcal{M} \subset \mathcal{A}.$$

Corollary 2.1. *For all integer ℓ with $0 \le \ell \le m$, we have*

$$\dim_{\mathbb{F}_2}(\mathcal{M}^\ell) = \binom{m}{\ell} + \binom{m}{\ell+1} + \cdots + \binom{m}{m}.$$

From now on, let denote $P(m,2)$ the set of all polynomials in reduced form in m variables $Y_1,\ldots,Y_m$ over $\mathbb{F}_2$ i.e.

$$P(m,2) = \left\{ P(Y_1,\ldots,Y_m) = \sum_{i_1=0}^{1}\cdots\sum_{i_m=0}^{1} u_{i_1\ldots i_m}\, Y_1^{i_1}\ldots Y_m^{i_m} \mid u_{i_1\ldots i_m} \in \mathbb{F}_2 \right\}.$$

Let r be an integer such that $0 \le r \le m$ and denote $P_r(m,2)$ the vector subspace of $P(m,2)$ generated by the monomials of total degree at most equal to r:

$$P_r(m,2) = \{P(Y_1,\ldots,Y_m) \in P(m,2) \ \mid\ \deg(P) \le r\}.$$

Definition 2.1. *The r-th order Reed-Muller code of length 2^m over $\mathbb{F}_2$ is defined as*

$$C_r(m,2) = \{(P(i_1,\ldots,i_m))_{0\le i_1,\ldots,i_m\le 1} \in (\mathbb{F}_2)^{2^m} |\ P \in P_r(m,2)\}.$$

$C_r(m,2)$ are subspaces of $(\mathbb{F}_2)^{2^m}$ and we have the following ascending sequence :

$$\{0\} \subset C_0(m,2) \subset C_1(m,2) \subset \cdots \subset C_m(m,2) = (\mathbb{F}_2)^{2^m}.$$

Theorem 2.2 (Berman)**.** *For every integer $0 \le \ell \le m$, we have $\mathcal{M}^\ell = C_{m-\ell}(m,2)$.*

The weight of the vector $v = (v_1, \dots, v_{2^m}) \in (\mathbb{F}_2)^{2^m}$ is $\omega t(v) = \mathrm{card}(\{\ i \mid v_i \neq 0\})$, where card denotes the number of elements in the set.

Theorem 2.3. *The Reed-Muller code $\mathcal{M}^\ell$ has minimum weight $d_{min}(\mathcal{M}^\ell) = 2^\ell$ where $0 \leq \ell \leq m$.*

Remark 2.1. *$\mathcal{M}^\ell$ is a t-error correcting code where t is the greatest integer such that $2t + 1 \leq 2^\ell$.*

3. Main results

In this section will be presented the main results and a decoding algorithm. Let us fix an integer ℓ such that $0 \leq \ell \leq m$ and by taking account of (2.2), consider

$$\mathcal{G}_\ell = \left\{ (x_1 - 1)^{i_1} \cdots (x_m - 1)^{i_m} \in \mathcal{A} \mid 0 \leq i_1, \dots, i_m \leq 1, \sum_{k=1}^{m} i_k = \ell \right\}.$$

Proposition 3.1. *$\mathcal{G}_\ell$ is a basis for the ideal $\mathcal{M}^\ell$.*

Proof. Since $\mathcal{M}^\ell$ is an ideal and $\mathcal{G}_\ell \subset \mathcal{M}^\ell$, then for all $g \in \mathcal{G}_\ell$, we get $\mathcal{A}g \subseteq \mathcal{M}^\ell$. Therefore, $\sum_{g \in \mathcal{G}_\ell} \mathcal{A}g \subseteq \mathcal{M}^\ell$. Conversely, since $\mathcal{J}_\ell$ is a linear basis for $\mathcal{M}^\ell$ over $\mathbb{F}_2$, then every element of $\mathcal{M}^\ell$ is a linear combination of elements in $\mathcal{J}_\ell$. Moreover, every element of $\mathcal{J}_\ell$ can be written as a product ag with $a \in \mathcal{A}$ and $g \in \mathcal{G}_\ell$. Thus, we have $\mathcal{M}^\ell \subseteq \sum_{g \in \mathcal{G}_\ell} \mathcal{A}g$. □

Definition 3.1. *For each integer ℓ such that $0 \leq \ell \leq m$, we denote G_ℓ the subset of $\mathbb{F}_2[X_1, \dots, X_m]$ defined by*

$$G_\ell = \left\{ (X_1 - 1)^{i_1} \cdots (X_m - 1)^{i_m} \ \mid \ 0 \leq i_1, \dots, i_m \leq 1, \ \sum_{k=1}^{m} i_k = \ell \right\}$$

and $\langle G_\ell \rangle$ the ideal of $\mathbb{F}_2[X_1, \dots, X_m]$ generated by G_ℓ.

We denote $E = \{1, \dots, m\}$ and for every subset $I \subseteq E$, we set

$$X_I = \prod_{i \in I} X_i, \qquad \textit{with} \quad X_\emptyset = 1,$$
$$g_I = \prod_{i \in I} (X_i - 1) \quad \textit{with} \quad g_\emptyset = 1.$$

In the same manner, we define in $\mathcal{A}$,

$$x_I = \prod_{i \in I} x_i \quad \textit{with} \quad x_\emptyset = 1 \;\; \textit{and} \;\; x_i = X_i + < H > .$$

Remark 3.1. *We can write*

$$G_\ell = \{g_I \mid I \in \mathcal{P}(E),\ \operatorname{card}(I) = \ell\} \quad \textit{where} \quad \mathcal{P}(E) = \{I \mid I \subseteq E\}$$

It follows that $\operatorname{card}(G_\ell) = \binom{m}{\ell}$. *Moreover, by expanding all factors in g_I, we get*

$$g_I = \sum_{L \in \mathcal{P}(I)} X_L = X_I + \sum_{L \in \mathcal{P}(I) \setminus \{I\}} X_L \tag{3.1}$$

Furthermore, with respect to grlex order $>_{grlex}$, we have $\operatorname{in}(g_I) = X_I$. So, the initial ideal of G_ℓ is given by $\operatorname{in}(G_\ell) = \langle \operatorname{in}(g) \mid g \in G_\ell \rangle = \langle X_I \mid I \in \mathcal{P}(E),\ \operatorname{card}(I) = \ell \rangle$.

We recall that $\langle G_\ell \rangle + \langle H \rangle$ is the ideal of $\mathbb{F}_2[X_1, \ldots, X_m]$ generated by $G_\ell \cup H$, i.e. $\langle G_\ell \rangle + \langle H \rangle = \langle G_\ell \cup H \rangle$.

We give a new proof for the following proposition.

Proposition 3.2. *We consider grlex order. For each integer ℓ such that $0 \le \ell \le m$,*

(1) *G_ℓ is a reduced Groebner basis for the ideal $\langle G_\ell \rangle$,*
(2) *$H = \{X_1^2 - 1, \ldots, X_m^2 - 1\}$ is a reduced Groebner basis for $\langle H \rangle$,*
(3) *$G_\ell \cup H$ is a reduced Groebner basis for the ideal $\langle G_\ell \rangle + \langle H \rangle$.*

Proof. (1) Let $I, J \subseteq E$ be subsets with $\operatorname{card}(I) = \operatorname{card}(J) = \ell$. So

$$\begin{aligned}
S(g_I, g_J) &= \frac{X^\gamma}{\operatorname{in}(g_I)} g_I - \frac{X^\gamma}{\operatorname{in}(g_J)} g_J \\
&= \frac{X^\gamma}{X_I} g_I - \frac{X^\gamma}{X_J} g_J \\
&= (X_{(I \cup J) \setminus I}) g_I - (X_{(I \cup J) \setminus J}) g_J \\
&= (X_{J \setminus I}) g_I - (X_{I \setminus J}) g_J \\
&= (\prod_{i \in J \setminus I} [(X_i - 1) + 1]) g_I - (\prod_{i \in I \setminus J} [(X_i - 1) + 1]) g_J \\
&= (\sum_{K \in \mathcal{P}(J \setminus I)} g_K) g_I - (\sum_{K \in \mathcal{P}(I \setminus J)} g_K) g_J \\
&= \sum_{K \in \mathcal{P}(J \setminus I)} g_K g_I - \sum_{K \in \mathcal{P}(I \setminus J)} g_K g_J,
\end{aligned}$$

where $X^{\gamma} = \mathrm{lcm}(\mathrm{lm}(g_I), \mathrm{lm}(g_J)) = \mathrm{lcm}(X_I, X_J) = X_{I \cup J}$. It is obvious that $\mathrm{rem}_{G_\ell}(g_K g_I) = 0$ for all $K \in \mathcal{P}(J \setminus I)$ and similarly $\mathrm{rem}_{G_\ell}(g_K g_J) = 0$ for all $K \in \mathcal{P}(I \setminus J)$. Furthermore, by the Remark 1.1, it follows that $\mathrm{rem}_{G_\ell}(S(g_I, g_J)) = 0$. Then, by the Theorem 1.3, we conclude the expected result.

Using similar way as in (1), one can prove (2) and (3). $\square$

Proposition 3.3. *For every integer ℓ such that $0 \leq \ell \leq m$, we have*

$$\mathcal{M}^{\ell} = (< G_\ell > + < H >)/ < H >$$

Proof. The morphism

$$\begin{aligned} \psi \ : \ \langle G_\ell \rangle + \langle H \rangle &\longrightarrow \mathcal{M}^{\ell} \\ g + h \ &\longmapsto g + < H > \end{aligned}$$

is surjective by Proposition 3.1 and the fact that $\mathcal{G}_\ell = \{g_I + < H >, \ g_I \in G_\ell\}$. Moreover, it is clear that $\ker(\psi) = \langle H \rangle$. $\square$

Corollary 3.1. *For every integer ℓ such that $0 \leq \ell \leq m$, we have*

$$\mathcal{M}^{\ell} \simeq < G_\ell > /(< G_\ell > \cap < H >)$$

Proof. From [2] p.491 we have $(\langle G_\ell \rangle + \langle H \rangle)/\langle H \rangle \simeq \langle G_\ell \rangle/(\langle G_\ell \rangle \cap \langle H \rangle)$ and the expected result follows from Proposition 3.3. $\square$

Remark 3.2. *Generally, for $0 \leq \ell \leq m$, $\langle G_\ell \rangle \cap \langle H \rangle \neq \{0\}$.*

In the particular case where $\ell = 1$, we have $G_1 = \{X_1 - 1, \ldots, X_m - 1\}$ and $H = \{X_1^2 - 1, \ldots, X_m^2 - 1\} = \{(X_1 - 1)^2, \ldots, (X_m - 1)^2\}$. Thus, $\langle H \rangle \subseteq \langle G_1 \rangle$ and $\mathcal{M} \simeq \langle G_1 \rangle / \langle H \rangle$.

For $\ell > 1$, as example consider the case $m = 3$ and $\ell = 2$. In the polynomial ring $\mathbb{F}_2[X, Y, Z]$, we have

$$\begin{aligned} G_2 &= \{(X-1)^i (Y-1)^j (Z-1)^k \mid 0 \leq i, j, k \leq 1, \ i + j + k = 2\} \\ &= \{(X-1)(Y-1), (X-1)(Z-1), (Y-1)(Z-1)\} \end{aligned}$$

and $H = \{X^2 - 1, Y^2 - 1, Z^2 - 1\}$. The polynomial of the ideal $\langle H \rangle$, $f(X, Y, Z) = (Y+1)(X^2 - 1) + (X-1)(Y^2 - 1)$ can be written as $f(X, Y, Z) = (Y+1)(X-1)(X+1) + (X-1)(Y-1)(Y+1) = (X+Y)(X-1)(Y-1)$ which belongs to the ideal $\langle G_2 \rangle$. Then $\langle G_2 \rangle \cap \langle H \rangle \neq \{0\}$.

From now on, if $c(x) \in \mathcal{M}^\ell$, by Proposition 3.1, we can write

$$c(x) = \sum_{\substack{i=(i_1,\dots,i_m)\in\{0,1\}^m \\ |i|=\ell}} c_{i_1,\dots,i_m}(x_1-1)^{i_1}\dots(x_m-1)^{i_m},$$

and we always consider the corresponding standard representative

$$c(X) = \sum_{\substack{i=(i_1,\dots,i_m)\in\{0,1\}^m \\ |i|=\ell}} c_{i_1,\dots,i_m}(X_1-1)^{i_1}\dots(X_m-1)^{i_m} \in < G_\ell > .$$

It is clear that $c(x) = c(X) + \langle H\rangle$.

For the remainder of the section, we always consider the graded lexicographic order $>_{grlex}$ such that $X_1 >_{grlex} X_2 >_{grlex} \cdots >_{grlex} X_m$.

Remark 3.3. *If $a(x) = b(x)$ in $\mathcal{A}$, then $a(X) - b(X) \in \langle H\rangle$. Therefore $\mathrm{rem}_H(a(X) - b(X)) = 0$. So $\mathrm{rem}_H(a(X)) = \mathrm{rem}_H(b(X))$. Since $a(X)$ and $b(X)$ are standard representatives of $a(x)$ and $b(x)$, then $\mathrm{rem}_H(a(X)) = a(X)$ and $\mathrm{rem}_H(b(X)) = b(X)$. It follows that $a(X) = b(X)$ in $\mathbb{F}_2[X_1,\dots,X_m]$.*

Definition 3.2. *Let $\ell \in \mathbb{N}$ with $1 \le \ell \le m$. For every subset $I \subseteq E = \{1,\dots,m\}$, we denote by $\sigma(I)$ the subset of $\mathcal{P}(I) = \{L \mid L \subseteq I\}$ such that*

$$\mathrm{rem}_{G_\ell}(X_I) = \sum_{L\in\sigma(I)} X_L$$

Definition 3.3. *We define the operator Δ as $A \,\Delta\, B = (A \setminus B) \cup (B \setminus A)$, where $A, B \subseteq E$. Generally, we have $\quad A \,\Delta\, B \,\Delta\, C = (A \,\Delta\, B) \,\Delta\, C$.*

Proposition 3.4. *Let $m, \ell \in \mathbb{N}$ with $1 \le \ell \le m$. For every subsets $I, J \subseteq E$, $I \ne J$, we have $\quad \mathrm{rem}_{G_\ell}(X_I + X_J) = \sum_{L \,\in\, \sigma(I)\,\Delta\,\sigma(J)} X_L$.*

Proof. By the Remark 1.1, we get

$$\begin{aligned}\mathrm{rem}_{G_\ell}(X_I + X_J) = \mathrm{rem}_{G_\ell}(X_I) + \mathrm{rem}_{G_\ell}(X_J) &= \sum_{L\in\sigma(I)} X_L + \sum_{L\in\sigma(J)} X_L \\ &= \sum_{L\in\sigma(I)\setminus\sigma(J)} X_L + \sum_{L\in\sigma(J)\setminus\sigma(I)} X_L + 2\sum_{L\in\sigma(I)\cap\sigma(J)} X_L \\ &= \sum_{L\in\sigma(I)\,\Delta\,\sigma(J)} X_L.\end{aligned}$$

$\square$

Proposition 3.5. *Let $I \subseteq E = \{1, \ldots, m\}$, $\ell \in \mathbb{N}$ with $1 \leq \ell \leq m$, and t the greatest integer such that $2t + 1 \leq 2^l$. Then,*

(1) *if* $\mathrm{card}(I) < \ell$ *then* $\sigma(I) = \{I\}$*;*
(2) *if* $\mathrm{card}(I) = \ell$ *then* $\sigma(I) = \mathcal{P}(I) \setminus \{I\}$.

Proof. (1)- Suppose that $\mathrm{card}(I) < \ell$, then X_I contains less than ℓ factors X_i, and no initial term $\mathrm{in}(g_J)$ of every $g_J \in G_\ell$ divides X_I. Therefore, $\mathrm{rem}_{G_\ell}(X_I) = X_I$ and hence $\sigma(I) = \{I\}$.
(2)- Now assume that $\mathrm{card}(I) = \ell$. Then, $g_I \in G_\ell$ and we can write $X_I = g_I + \sum_{L \in \mathcal{P}(I) \setminus \{I\}} X_L$ by equality (3.1), where $\mathrm{card}(L) < \ell$ for every $L \in \mathcal{P}(I) \setminus \{I\}$. It follows that, $\mathrm{rem}_{G_\ell}(X_I) = \sum_{L \in \mathcal{P}(I) \setminus \{I\}} X_L$ and so $\sigma(I) = \mathcal{P}(I) \setminus \{I\}$. □

Corollary 3.2. *For each $I \subseteq E$ such that $\mathrm{card}(I) = \ell \geq 1$, we have $\omega t(\mathrm{rem}_{G_\ell}(X_I)) > t$ where t is the greatest integer such that $2t + 1 < 2^\ell$.*

Proof. Let I be a subset of $E = \{1, \ldots, m\}$. By Proposition 3.5 (2), if $\mathrm{card}(I) = \ell$, then $\omega t(\mathrm{rem}_{G_\ell}(X_I)) = \mathrm{card}(\sigma(I)) = \mathrm{card}(\mathcal{P}(I) \setminus \{I\}) = 2^{\mathrm{card}(I)} - 1 = 2^\ell - 1$. As t is the greatest integer such that $2t + 1 \leq 2^\ell$, we have $2t \leq 2^\ell - 1$. Thus, $\omega t(\mathrm{rem}_{G_\ell}(X_I)) > t$. □

Theorem 3.1. *Let $m, \ell \in \mathbb{N}$ with $2 \leq \ell \leq m$. Let $c(x) \in \mathcal{M}^\ell$ be a transmitted codeword and $v(x) \in \mathcal{A}$ the received word, i.e. $v(x) = c(x) + e(x)$ with $\omega t(e(x)) \leq t$ where t is the greatest integer such that $2t + 1 \leq 2^\ell$. Then, $\mathrm{rem}_{G_\ell}(v(X)) = \mathrm{rem}_{G_\ell}(e(X))$ and*

(1)- *if* $\mathrm{rem}_{G_\ell}(v(X)) = 0$ *then* $c(x) = v(x)$*;*
(2)- *if* $\mathrm{rem}_{G_\ell}(v(X)) = \displaystyle\sum_{L \in \sigma(I_1) \Delta \cdots \Delta \sigma(I_k)} X_L$ *for some $k \leq t$ and pairwise distinct subsets $I_1, \ldots, I_k \subseteq E$, then $e(x) = x_{I_1} + \cdots + x_{I_k}$ which means that $v(x)$ contains k errors located at $x_{I_1}, \ldots, x_{I_k}$.*

Proof. Let $c(x) \in \mathcal{M}^\ell$ and $c(X) \in \langle G_\ell \rangle$ be its standard representative. Since G_ℓ is a Groebner basis for $\langle G_\ell \rangle$, then $\mathrm{rem}_{G_\ell}(c(X)) = 0$ and therefore $\mathrm{rem}_{G_\ell}(v(X)) = \mathrm{rem}_{G_\ell}(e(X))$. Moreover,
(1)- if $\mathrm{rem}_{G_\ell}(v(X)) = 0$, then $\mathrm{rem}_{G_\ell}(e(X)) = 0$ i.e. $e(x) \in \mathcal{M}^\ell$. In addition, by assumption, $\omega t(e(x)) \leq t < 2^\ell = d_{min}(\mathcal{M}^\ell)$, then $e(x) = 0$ and $v(x) = c(x)$.
(2)- if $\mathrm{rem}_{G_\ell}(v(X)) \neq 0$ with $\mathrm{rem}_{G_\ell}(v(X)) = \sum_{L \in \sigma(I_1) \Delta \cdots \Delta \sigma(I_k)} X_L$ for some integer $k \leq t$ and pairwise distinct subsets $I_1, \ldots, I_k \subseteq E$, then by Proposition 3.4, we have

$\mathrm{rem}_{G_\ell}(v(X)) = \mathrm{rem}_{G_\ell}(X_{I_1} + \cdots + X_{I_k})$. Setting $c'(X) = v(X) - (X_{I_1} + \cdots + X_{I_k})$ implies that $\mathrm{rem}_{G_\ell}(c'(X)) = 0$. Then, $c'(X) \in \langle G_\ell \rangle$ and hence $c'(x) \in \mathcal{M}^\ell$. As a result, we can write $v(x) = c'(x) + e'(x)$ with $e'(x) = x_{I_1} + \cdots + x_{I_k}$. However, by assupmtion $v(x) = c(x)+e(x)$ then, $e'(x)-e(x) = c(x)-c'(x) \in \mathcal{M}^\ell$. Furthermore, $\omega t(e'(x) - e(x)) \leq \omega t(e'(x)) + \omega t(e(x)) \leq k + t \leq 2t < 2^\ell = d_{min}(\mathcal{M}^\ell)$. It follows that, $e'(x) = e(x)$ and $c'(x) = c(x)$. Thus, $v(x) = c(x) + e(x)$ with $e(x) = x_{I_1} + \cdots + x_{I_k}$. □

Theorem 3.2. *Let $m, \ell \in \mathbb{N}$ with $2 \leq \ell \leq m$. Let $c(x) \in \mathcal{M}^\ell$ be a transmitted codeword and $v(x) \in \mathcal{A}$ the received word, i.e. $v(x) = c(x) + e(x)$ with $\omega t(e(x)) \leq t$ where t is the greatest integer such that $2t + 1 \leq 2^\ell$. Then, $\omega t(\mathrm{rem}_{G_\ell}(v(X))) \leq t$ if, and only if, $\mathrm{rem}_{G_\ell}(v(X)) = e(X)$ and $e(x) = 0$ or $e(x) = x_{I_1} + \cdots + x_{I_k}$ for some $k \leq t$ and pairwise distinct subsets $I_1, \ldots, I_k \subseteq E$ such that $\mathrm{card}(I_i) < \ell$ for all $i = 1, \ldots, k$.*

Proof. Assume that $\omega t(\mathrm{rem}_{G_\ell}(v(X))) \leq t$. Denote $r(X) = \mathrm{rem}_{G_\ell}(v(X))$ the remainder on the division of $v(X)$ by G_ℓ. Then, we can write $v(X)$ as $v(X) = c'(X)+r(X)$ with $c'(X) \in \langle G_\ell \rangle$ and $r(X) = 0$ or every term in $r(X)$ is divisible by none of $\mathrm{in}(g)$, $g \in G_\ell$ and $\omega t(r(X)) \leq t$. Then, $v(x) = c(x) + e(x) = c'(x) + r(x)$, so $r(x)-e(x) = c(x)-c'(x) \in \mathcal{M}^\ell$. In addition, $\omega t(r(x)-e(x)) \leq \omega t(r(x))+\omega t(e(x)) \leq 2t < 2^\ell = d_{min}(\mathcal{M}^\ell)$. It follows that, $r(x) = e(x)$ and $c'(x) = c(x)$. Thus, $v(x) = c(x) + e(x)$ with $e(x) = r(x)$. In other terms, $\mathrm{rem}_{G_\ell}(v(X)) = r(X) = e(X)$. And if $r(X) = 0$ then $e(X) = 0$. If $r(X) \neq 0$, there are $k \in \mathbb{N}$ and pairwise distinct subsets $I_1, \ldots, I_k \subseteq E$ such that $r(X) = X_{I_1} + \cdots + X_{I_k}$. The assumption $\omega t(r(X)) \leq t$ implies that $k \leq t$. Moreover, since no term in $r(X)$ is divisible by any of $\mathrm{in}(g)$, $g \in G_\ell$, it follows that $\mathrm{card}(I_i) < \ell$ for all $i = 1, \ldots, k$. Hence, $e(x) = x_{I_1} + \cdots + x_{I_k}$ for some $k \leq t$ with $\mathrm{card}(I_i) < \ell$ for all $i = 1, \ldots, k$.

Conversely, suppose that $\mathrm{rem}_{G_\ell}(v(X)) = e(X)$. Hence, if $e(x) = 0$ then we have $\mathrm{rem}_{G_\ell}(v(X)) = 0$ and so, $\omega t(\mathrm{rem}_{G_\ell}(v(X))) = 0 \leq t$. On the other hand, if $e(X) = X_{I_1} + \cdots + X_{I_k}$ for some $k \leq t$ and pairwise distinct subsets $I_1, \ldots, I_k \subseteq E$, then $\omega t(\mathrm{rem}_{G_\ell}(v(X))) = k \leq t$. □

By taking into account the above discussion, we have the following result

Theorem 3.3. *Let $m, \ell \in \mathbb{N}$ with $2 \leq \ell \leq m$. Let $v(x) \in \mathcal{A}$ be a received word containing at most t errors, where t is the greatest integer such that $2t + 1 \leq 2^\ell$.*

Then, $v(x)$ can be decoded by the following algorithm:
Input:

- v
- G_ℓ *a Groebner basis for* $\langle G_\ell \rangle$
- $\Omega = \{S \subseteq \mathcal{P}(\{1,\dots,m\}) \mid \operatorname{card}(I) \geq \ell$ *for all* $I \in S\}$

Output: a codeword $c(x) \in M^\ell$

Begin

- *Compute* $\operatorname{rem}_{G_\ell}(v(X))$.
- *If* $\omega t(\operatorname{rem}_{G_\ell}(v(X))) \leq t$*, then* $c(X) = v(X) - \operatorname{rem}_{G_\ell}(v(X))$.
  Else find the element $S \in \Omega$ *such that*

$$\omega t(\operatorname{rem}_{G_\ell}(v(X) - \sum_{I \in S} X_I)) \leq t - \operatorname{card}(S)$$

and we obtain

$$c(X) = v(X) - \sum_{I \in S} X_I - \operatorname{rem}_{G_\ell}(v(X) - \sum_{I \in S} X_I).$$

End

Corollary 3.3. *Consider the Reed-Muller code $\mathcal{M}^2$. Let $v \in (\mathbb{F}_2)^{2^m}$ be a received vector containing at most one error. We denote $v(x)$ the polynomial in $\mathcal{A}$ corresponding to v. We have $v(x) = c(x) + e(x)$ with $c(x) \in \mathcal{M}^2$ and $\omega t(e) \leq 1$.*

- *If* $\operatorname{rem}_{G_2}(v(X)) = 0$ *then* $c(x) = v(x)$.
- *If* $\operatorname{rem}_{G_2}(v(X)) = \sum_{i \in I} X_i$ *or* $\operatorname{rem}_{G_2}(v(X)) = \sum_{i \in I} X_i + 1$ *with* $I \subseteq E$*, then* $e(x) = \prod_{i \in I} x_i$.

In the practice, by using standard representatives, we can indifferently use the variable x for X.

Example 2. *Decoding Reed-Muller Code $C_1(3,2) = \mathcal{M}^2$, a 1-error correcting code. Consider $g_1 = xy + x + y + 1, g_2 = xz + x + z + 1$, $g_3 = yz + y + z + 1 \in \mathbb{F}_2[x,y,z]$ and set $G_2 = \{g_1, g_2, g_3\}$. Then, G_2 is a Groebner basis for the ideal $\langle G_2 \rangle$. Let $v = (1,0,0,0,0,1,0,1)$ be a received word, so $v(x) = xyz + y + 1$ by correspondance (2.1). Using the grlex order we have $\operatorname{rem}_{G_2}(v(x)) = x+z+1$. Then, $e(x) = xz$ and we get the codeword $c = (1,0,0,0,0,1,0,1) + (0,0,1,0,0,0,0,0) = (1,0,1,0,0,1,0,1) \in \mathcal{M}^2 = C_1(3,2)$.*

Example 3. *Decoding Reed-Muller Code $C_1(4,2)=\mathcal{M}^3$, which is a 3-error correcting code. In $\mathbb{F}_2[x_1,x_2,x_3,x_4]$ consider $G_3=\{g_1,g_2,g_3,g_4\}$ with*

$g_1 = x_1x_2x_3 + x_1x_2 + x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 + 1$

$g_2 = x_1x_2x_4 + x_1x_2 + x_1x_4 + x_1 + x_2x_4 + x_2 + x_4 + 1$

$g_3 = x_1x_3x_4 + x_1x_3 + x_1x_4 + x_1 + x_3x_4 + x_3 + x_4 + 1$

$g_4 = x_2x_3x_4 + x_2x_3 + x_2x_4 + x_2 + x_3x_4 + x_3 + x_4 + 1.$

Then, G_3 is a Groebner basis for the ideal $< G_3 >$. Let v_0 be a received word, $v_0=(0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0)\in(\mathbb{F}_2)^{2^4}$. The code $C_1(4,2)=\mathcal{M}^3$ has as minimum distance $d=2^3=8$, it is a 3-error correcting code. By correspondance (2.1), we can write $v_0(x)=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_1+x_2x_3x_4+x_2+x_3+x_4\in\mathcal{A}$. Then, $v_0(x)=g_1(x)+g_2(x)+g_3(x)+g_4(x)$. Consequently, $\mathrm{rem}_{G_3}(v_0(x))=0$ and hence $c=v_0\in C_1(4,2)$. Let us reconsider now another the received word $v_1=(0,1,1,0,1,\boldsymbol{1},0,\boldsymbol{0},1,0,0,\boldsymbol{0},0,1,1,0)$ obtained from v_0 by adding errors on its sixth, eigth and twelth entries. It means that $v_1(x)=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_1x_3+x_2x_3x_4+x_3+x_4$, then we have $v_1(x)=g_1(x)+g_2(x)+g_3(x)+g_4(x)+x_1x_3+x_1+x_2$. As a result $\mathrm{rem}_{G_3}(v_1(x))=x_1x_3+x_1+x_2$. As $\omega t(\mathrm{rem}_{G_3}(v_1(x)))=3\leq t=3$ then $c(x)=v_1(x)+\mathrm{rem}_{G_3}(v_1(x))=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_1+x_2x_3x_4+x_2+x_3+x_4$. In other terms, after decoding of the received word v_1, we get the word $c=(0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0)=v_0$. All of three errors have been corrected.

Finally, let introduce this time only one error into v_0 on its second entry and denote v_2 the corresponding received word,

$$v_2=(0,\boldsymbol{0},1,0,1,0,0,1,1,0,0,1,0,1,1,0).$$

Equivalently, $v_2(x)=x_1x_2x_4+x_1x_3x_4+x_1+x_2x_3x_4+x_2+x_3+x_4$. We can write, $v_2(x)=g_2(x)+g_3(x)+g_4(x)+x_1x_2+x_1x_3+x_1+x_2x_3+x_2+x_3+1$. As a result $\mathrm{rem}_{G_3}(v_2(x))=x_1x_2+x_1x_3+x_1+x_2x_3+x_2+x_3+1$. Since $\omega t(\mathrm{rem}_{G_3}(v_2(x)))=7>3=t$, then it suffices to choose a set $S\in\Omega$ which saisfies the conditions of the algorithm. For $S=\{I\}$ with $I=\{1,2,3\}$, we have $x_I=x_1x_2x_3$. We can write $x_I=g_1(x)+x_1x_2+x_1x_3+x_1+x_2x_3+x_2+x_3+1$ and so $v_2(x)=g_2(x)+g_3(x)+g_4(x)+g_1(x)+x_I$. Hence, $v_2(x)-x_I\in\langle G_3\rangle$ and $\mathrm{rem}_{G_3}(v_2(x)-x_I)=0$. As a result $\omega t(\mathrm{rem}_{G_3}(v_2(x)-x_I))=0\leq t-\mathrm{card}(s)=2$. Thus, the decoding of $v_2(x)$ gives $c(x)=(v_2(x)-x_I)+\mathrm{rem}_{G_3}(v_2(x)-x_I)=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_1+x_2x_3x_4+x_2+x_3+x_4$. Hence, we have found the initial codeword $c=(0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0)=v_0$.

ACKNOWLEDGMENT

The authors would like to thank the referee for careful reading.

REFERENCES

[1] W. ADAMS, P. LOUSTAUNAU: *An introduction to Groebner Bases*, Amer. Math. Society, **3** (1994).

[2] AVIVA SZPIRGLAS ET AL: *Mathématiques L3 Algèbre*, Pearson Education France (2009).

[3] S.D. BERMAN: *On the theory of group codes*, kibernetika **3**(1) (1967), 31–39.

[4] I.F. BLAKE AND R.C. MULLIN: *The mathematical theory of coding*, Academic Press, 1975.

[5] P. CHARPIN: *Une généralisation de la construction de Berman des codes de Reed et Muller p-aires*, Comm. algebra, **16** (1988), 2231–2246.

[6] D. COX, J. LITTLE, D. O'SHEA: *Ideals, Varieties and Algorithms*, Springer, 1996.

[7] T. KASAMI, S. LIN, W.W. PETERSON: *New generalizations of the Reed-Muller codes*, IEEE Trans. Inform. Theory, **14**(2) (1968), 189–205.

[8] P. LANDROCK, O. MANZ: *Classical codes as ideals in group algebras*, Des. Codes Cryptogr., **2** (1992), 273–285.

[9] M. SALEEMI: *Coding Theory via Groebner Bases*, Thesis, 2012.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF ANTANANARIVO
ANTANANARIVO II,
MADAGASCAR.
Email address: ramahazos@yahoo.fr

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF ANTANANARIVO
ANTANANARIVO II,
MADAGASCAR.
Email address: hariandriatahiny@gmail.com

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF ANTANANARIVO
ANTANANARIVO II,
MADAGASCAR.
Email address: randriamiferdinand@gmail.com