THE ART OF DISCRETE AND APPLIED MATHEMATICS

ISSN 2590-9770
The Art of Discrete and Applied Mathematics
https://doi.org/10.26493/2590-9770.1417.02a
(Also available at http://adam-journal.eu)

On algebraic structure of the Reed-Muller codes

Harinaivo Andriatahiny

Department of Mathematics and Computer Science, Faculty of Sciences, University of Antananarivo, Madagascar

Received 20 May 2021, accepted 16 August 2021

Abstract

It is known that the Reed-Muller codes over a prime field may be described as the radical powers of a modular group algebra. In this paper, we give a new proof of the same result in a quotient of a polynomial ring. Special elements in a prime field are studied. An interpolation polynomial is introduced in order to characterize the coefficients of the Jennings polynomials.

Keywords: Reed-Muller codes, finite field, interpolation polynomial, Jennings basis.

Math. Subj. Class.: 94B05, 16N40, 12E05, 12E20

1 Introduction

Reed-Muller codes are among the oldest known families of codes. They were discovered by I.S. Reed and D.E. Muller in 1954. These codes were initially given as binary codes, but generalizations to q-ary were provided with q a prime power. Reed-Muller codes were studied by many authors (see, e.g. [3, 5, 9, 7, 8, 11, 12]).

These codes form a class of practically important codes. They have found widespread applications. A powerful Reed-Muller code was used by Mariner 9 to send back clear pictures from Mars to Earth in 1972.

A great advantage of the Reed-Muller codes is that they are relatively easy to decode by using majority logic decoding.

One of the interesting properties of the Reed-Muller codes is that there are several ways to describe them. They may be described by using finite geometries [2]. Group algebra approach can be used to characterize the Reed-Muller codes. This approach enables Berman and Charpin to identify the Reed-Muller codes with the radical powers in a suitable modular group algebra for the binary and p-ary cases. This is the famous theorem of Berman for the binary case [4]. The p-ary case was treated by Charpin [6]. Many authors (see, e.g. [1, 9, 10]) have studied this property of Reed-Muller codes.

E-mail address: hariandriatahiny@gmail.com (Harinaivo Andriatahiny)

In this paper, we utilize the quotient algebra $B = \mathbb{F}_p[X_0, \ldots, X_{m-1}]/\langle X_0^p - 1, \ldots, X_{m-1}^p - 1\rangle$ as the ambient space of the codes. The radical powers of B are linearly generated by the Jennings bases. We give some properties of special elements of the finite field $\mathbb{F}_p$. Then, we obtain the coefficients of the Jennings polynomials by means of an appropriate interpolation function. We can apply this fact to show that the radical powers of B are the Reed-Muller codes of length p^m over $\mathbb{F}_p$.

2 Preliminary results

In this section, we give some properties of the following special elements of the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots p-1\}$

$$a_{i,d} := \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} j^d \tag{2.1}$$

where i and d are integers such that $0 \le i, d \le p-1$.

Proposition 2.1. *We have*

$$a_{i,d} \;=\; i \sum_{k=0}^{d-1} \binom{d-1}{k} a_{i-1,k}$$

for all integers d *and* i *such that* $1 \le i, d \le p-1$.

Proof. We have

$$\sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} j^d \;=\; \sum_{j=1}^{i} (-1)^{i-j} \binom{i}{j} j^d \;=\; \sum_{j=1}^{i} (-1)^{i-j} \cdot j \cdot \binom{i}{j} j^{d-1}.$$

Since

$$\binom{i}{j} = \frac{i}{j} \binom{i-1}{j-1},$$

the last expression become

$$i \sum_{j=1}^{i} (-1)^{i-1-(j-1)} \binom{i-1}{j-1} ((j-1)+1)^{d-1}.$$

By using the relation

$$((j-1)+1)^{d-1} = \sum_{k=0}^{d-1} \binom{d-1}{k} (j-1)^k,$$

and introducing $J = j-1$, the last expression become

$$i \sum_{k=0}^{d-1} \binom{d-1}{k} (\sum_{J=0}^{i-1} (-1)^{i-1-J} \binom{i-1}{J} J^k).$$

□

Proposition 2.2. *Let* i *be an integer such that* $1 \leq i \leq p-1$. *We have*

$$a_{i,d} = 0$$

for $d = 0, 1, ..., i-1$.

Proof. By induction on i:

- for $i = 1$: thus $d = 0$, we have, by convention $0^0 = 1$,

$$(-1)^1 \cdot \binom{1}{0} \cdot 0^0 + (-1)^0 \cdot \binom{1}{1} \cdot 1^0 = -1 + 1 = 0$$

- suppose the assertion is true for $i-1$, i.e.

$$\sum_{j=0}^{i-1} (-1)^{i-1-j} \binom{i-1}{j} j^d = 0 \ , \ for \ \ d = 0, 1, ..., i-2$$

and let us prove that it is also true for i.

• For $d = 0$,

$$\sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} = 0.$$

• Let d be such that $1 \leq d \leq i-1$, thus $0 \leq d-1 \leq i-2$; according to Proposition 2.1,

$$\begin{aligned}\sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} j^d &= i \sum_{k=0}^{d-1} \binom{d-1}{k} (\sum_{j=0}^{i-1} (-1)^{i-1-j} \binom{i-1}{j} j^k) \\ &= i \sum_{k=0}^{d-1} \binom{d-1}{k} \cdot 0 = 0\end{aligned}$$

□

Proposition 2.3. *Let* i *be an integer such that* $1 \leq i \leq p-1$. *Thus*

$$a_{i,i} \neq 0.$$

Proof. By induction on i.

- For $i = 1$,

$$(-1)^1 \binom{1}{0} 0^1 + (-1)^0 \binom{1}{1} 1^1 = 0 + 1 \neq 0$$

- Assume that the assertion holds for $i-1$ with $1 \leq i-1 \leq p-2$ (therefore, $2 \leq i \leq p-1$), i.e.

$$\sum_{j=0}^{i-1} (-1)^{i-1-j} \binom{i-1}{j} j^{i-1} \neq 0$$

And we have to show that the assertion is also true for i.

Using Proposition 2.1 and Proposition 2.2, we have

$$\sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} j^i = i \sum_{k=0}^{i-2} \binom{i-1}{k} \cdot 0 + i \sum_{j=0}^{i-1} (-1)^{i-1-j} \binom{i-1}{j} j^{i-1} \neq 0.$$

□

3 Interpolation polynomial

In this section, we study the following interpolation polynomial.

Definition 3.1. Taking account of (2.1), we define

$$H_i(Y) = (a_{i,0} - a_{i,p-1}) - \sum_{d=0}^{p-2} a_{i,d}\, Y^{p-1-d} \quad \in \mathbb{F}_p[Y]. \tag{3.1}$$

Theorem 3.2. *We have*

$$\deg(H_i(Y)) = p - 1 - i \tag{3.2}$$

where deg *denotes the degree of the polynomial.*

Proof. This is clear by using Proposition 2.2 and Proposition 2.3 in (3.1). □

Recall the following well known Lemmas.

Lemma 3.3. *We have*

$$\binom{p-1}{d} = (-1)^d \mod p$$

for $d = 0, 1, \ldots, p-1$.

Proof. It can be proved by induction on d. □

Lemma 3.4. *For* $a \in \mathbb{F}_p$, *we have*

$$a^{p-1} = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \neq 0. \end{cases}$$

Proof. It is clear that $0^{p-1} = 0$, because $p \geq 2$.
For the second case, note that $\mathbb{F}_p - \{0\}$ is a multiplicative group of order $p-1$. □

Theorem 3.5. *For an integer* k *such that* $0 \leq k \leq i$, *we have*

$$H_i(k) = (-1)^{i-k}\binom{i}{k}.$$

Proof. By using (3.1), (2.1) and the Lemma 3.3, we have

$$\begin{aligned}
H_i(Y) &= (a_{i,0} - a_{i,p-1}) - \sum_{d=0}^{p-2} a_{i,d}\, Y^{p-1-d} \\
&= a_{i,0} - \sum_{d=0}^{p-1} a_{i,d}\, Y^{p-1-d} \\
&= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j} - \sum_{d=0}^{p-1}\Big(\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j} j^d\Big)\, Y^{p-1-d} \\
&= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j} - \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}\Big[\sum_{d=0}^{p-1} j^d\, Y^{p-1-d}\Big] \\
&= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j} - \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}\Big[\sum_{d=0}^{p-1} (-1)^d(-j)^d\, Y^{p-1-d}\Big] \\
&= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j} - \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}\Big[\sum_{d=0}^{p-1} \binom{p-1}{d}(-j)^d\, Y^{p-1-d}\Big] \\
&= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j} - \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}(Y-j)^{p-1} \\
&= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j}\big[1-(Y-j)^{p-1}\big].
\end{aligned}$$

And by Lemma 3.4, we have the result. □

Remark 3.6. For an integer k such that $i < k \leq p-1$, we have

$$H_i(k) \;= 0.$$

4 Application to Reed-Muller codes

In this section, we give a new proof of the theorem of Berman and Charpin. Recall that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ is the field of p elements with p a prime number. Let m be a positive integer.

Definition 4.1. A linear code of length p^m over $\mathbb{F}_p$ is a linear subspace of the vector space

$$(\mathbb{F}_p)^{p^m} = \{(c_0, c_1, \ldots, c_{p^m-1}) \mid c_t \in \mathbb{F}_p, \text{ for all } t\}.$$

We consider the quotient algebra

$$B = \mathbb{F}_p[X_0, \ldots, X_{m-1}]/\langle X_0^p - 1, \ldots, X_{m-1}^p - 1\rangle \tag{4.1}$$

where $I = \langle X_0^p - 1, \ldots, X_{m-1}^p - 1\rangle$ is the ideal of the polynomial ring $\mathbb{F}_p[X_0, \ldots, X_{m-1}]$ generated by $X_0^p - 1, \ldots, X_{m-1}^p - 1$.

We denote

$$x_0 = X_0 + I, \ldots, x_{m-1} = X_{m-1} + I. \tag{4.2}$$

Remark 4.2. Note that $x_t^p = 1 = x_t^0$ for $t = 0, \dots, m-1$. Then, the exponent i_t in $x_t^{i_t}$ can be viewed as an integer in $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$.

We have

$$B = \left\{ \sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} c_{i_0,\dots,i_{m-1}} x_0^{i_0} \dots x_{m-1}^{i_{m-1}} \mid c_{i_0,\dots,i_{m-1}} \in \mathbb{F}_p \right\}. \tag{4.3}$$

Let us fix an order on the set of monomials

$$\left\{ x_0^{i_0} \dots x_{m-1}^{i_{m-1}} \mid i_t \in \mathbb{Z}/p\mathbb{Z}, \text{ for all } t \right\}.$$

Then, we can consider the isomorphism of vector spaces

$$\begin{array}{rcccl} \Phi & : & B & \longrightarrow & (\mathbb{F}_p)^{p^m} \\ \sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} c_{i_0,\dots,i_{m-1}} x_0^{i_0} \dots x_{m-1}^{i_{m-1}} & \longmapsto & (c_{i_0,\dots,i_{m-1}})_{0 \le i_0,\dots,i_{m-1} \le p-1}. \end{array} \tag{4.4}$$

Therefore, B can be considered as the ambient space for the linear codes of length p^m over $\mathbb{F}_p$, and the polynomial $\sum_{i_0=0}^{p-1} \cdots \sum_{i_{m-1}=0}^{p-1} c_{i_0,\dots,i_{m-1}} x_0^{i_0} \dots x_{m-1}^{i_{m-1}}$ of B can be identified with the vector $(c_{i_0,\dots,i_{m-1}})_{0 \le i_0,\dots,i_{m-1} \le p-1}$ of $(\mathbb{F}_p)^{p^m}$ and vice-versa.

B is a local ring with maximal ideal R which is the radical of B, i.e.

$$R = \mathrm{rad}(B). \tag{4.5}$$

Let d be an integer such that $0 \le d \le m(p-1)$. Consider the powers R^d of R. We have the following sequence of ideals:

$$\{0\} \subset R^{m(p-1)} \subset \cdots \subset R^2 \subset R \subset B.$$

For simplicity, in virtue of (4.2) and Remark 4.2, we use the following notations

$\mathbf{x} := (x_0, ..., x_{m-1})$,
$\mathbf{Y} := (Y_0, ..., Y_{m-1})$,
$\mathbf{i} := (i_0, \dots, i_{m-1}) \in (\mathbb{Z}/p\mathbb{Z})^m$,
$\mathbf{j} \le \mathbf{i}$ if $j_t \le i_t$, for all t, with $\mathbf{i}, \mathbf{j} \in (\mathbb{Z}/p\mathbb{Z})^m$,
$\mathbf{x}^{\mathbf{i}} := x_0^{i_0} \cdot \ldots \cdot x_{m-1}^{i_{m-1}}$ and
$\lfloor \mathbf{i} \rfloor := i_0 + \ldots + i_{m-1}$.

Definition 4.3. The Jennings polynomial is defined by

$$J_{\mathbf{i}}(\mathbf{x}) := (x_0 - 1)^{i_0} \cdot \ldots \cdot (x_{m-1} - 1)^{i_{m-1}}$$

with $\mathbf{i} := (i_0, \dots, i_{m-1}) \in (\mathbb{Z}/p\mathbb{Z})^m$.

Remark 4.4. (i) A linear basis of R^d over $\mathbb{F}_p$ called the Jennings basis of R^d is

$$E_d := \{ J_{\mathbf{i}}(\mathbf{x}) \mid \mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m, \ \lfloor \mathbf{i} \rfloor \ge d \}.$$

(ii) We have

$$\dim_{\mathbb{F}_p}(R^d) = \text{card}\,\{\mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m \mid \lfloor \mathbf{i} \rfloor \geq d\,\} \tag{4.6}$$

where $\dim_{\mathbb{F}_p}$ denotes the dimension of the vector space over $\mathbb{F}_p$ and card means the number of elements in the set.

By taking account of the relation (3.1), we have the following definition.

Definition 4.5. For $\mathbf{i} := (i_0, \ldots, i_{m-1}) \in (\mathbb{Z}/p\mathbb{Z})^m$, we define the interpolation polynomial

$$H_{\mathbf{i}}(\mathbf{Y}) := H_{i_0}(Y_0) \cdot \ldots \cdot H_{i_{m-1}}(Y_{m-1}) \quad \in \mathbb{F}_p[Y_0, \ldots, Y_{m-1}].$$

Theorem 4.6. *For* $\mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m$, *we have*

$$\deg(H_{\mathbf{i}}(\mathbf{Y})) = m(p-1) - \lfloor \mathbf{i} \rfloor. \tag{4.7}$$

Proof. It is obvious by (3.2). □

Theorem 4.7. *For* $\mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m$, *we have*

$$J_{\mathbf{i}}(\mathbf{x}) = \sum_{\mathbf{j} \leq \mathbf{i}} H_{\mathbf{i}}(\mathbf{j})\mathbf{x}^{\mathbf{j}}.$$

Proof. By Theorem 3.5, we have

$$\begin{aligned} J_{\mathbf{i}}(\mathbf{x}) &= \prod_{t=0}^{m-1} (x_t - 1)^{i_t} \\ &= \prod_{t=0}^{m-1} \Big(\sum_{j_t=0}^{i_t} (-1)^{i_t - j_t} \binom{i_t}{j_t} x_t^{j_t}\Big) \\ &= \prod_{t=0}^{m-1} \Big(\sum_{j_t=0}^{i_t} H_{i_t}(j_t) x_t^{j_t}\Big) \\ &= \sum_{\mathbf{j} \leq \mathbf{i}} \Big(\prod_{t=0}^{m-1} H_{i_t}(j_t)\Big)\mathbf{x}^{\mathbf{j}} \\ &= \sum_{\mathbf{j} \leq \mathbf{i}} H_{\mathbf{i}}(\mathbf{j})\mathbf{x}^{\mathbf{j}}. \end{aligned}$$

□

Remark 4.8. (i) If there is a t such that $j_t > i_t$, then $H_{\mathbf{i}}(\mathbf{j}) = 0$.

(ii) The polynomial $J_{\mathbf{i}}(\mathbf{x})$ can be identified with the vector $(H_{\mathbf{i}}(\mathbf{j}))_{\mathbf{j} \in (\mathbb{Z}/p\mathbb{Z})^m}$.

Recall that $\mathbf{Y} := (Y_0, ..., Y_{m-1})$. Consider the vector space of the reduced polynomials in m variables over $\mathbb{F}_p$

$$P(m,p) := \big\{P(\mathbf{Y}) \in \mathbb{F}_p[Y_0, ..., Y_{m-1}] \mid \deg_{Y_t}(P) \leq p-1, \text{ for all } t\big\}$$

where $\deg_{Y_t}(P)$ is the degree of the polynomial $P(\mathbf{Y})$ with respect to the variable Y_t.

Let ω be an integer such that $0 \leq \omega \leq m(p-1)$. Consider the subspace of $P(m,p)$ defined by

$$P_\omega(m,p) := \{P(\mathbf{Y}) \in P(m,p) \mid \deg(P) \leq \omega\}$$

where $\deg(P)$ is the total degree of the polynomial $P(\mathbf{Y})$.

We have the following isomorphism of vector spaces:

$$\begin{array}{rccc} \Psi: & P(m,p) & \longrightarrow & B \\ & P(\mathbf{Y}) & \longmapsto & \displaystyle\sum_{\mathbf{j}\in(\mathbb{Z}/p\mathbb{Z})^m} P(\mathbf{j})\mathbf{x}^{\mathbf{j}} \end{array} \tag{4.8}$$

Definition 4.9. The Reed-Muller code of length p^m over $\mathbb{F}_p$ and of order ω $(0 \leq \omega \leq m(p-1))$ is the subspace of $(\mathbb{F}_p)^{p^m}$ defined by

$$RM_{\mathbb{F}_p}(m,\omega) := \left\{(P(\mathbf{j}))_{\mathbf{j}\in(\mathbb{Z}/p\mathbb{Z})^m} \in (\mathbb{F}_p)^{p^m} \mid P(\mathbf{Y}) \in P_\omega(m,p)\right\}. \tag{4.9}$$

Remark 4.10. (i)- According to the isomorphisms (4.4) and (4.8), the Reed-Muller code $RM_{\mathbb{F}_p}(m,\omega)$ is isomorphic to $P_\omega(m,p)$.

(ii)- We have

$$\dim_{\mathbb{F}_p}(RM_{\mathbb{F}_p}(m,\omega)) = \mathrm{card}\left\{ \prod_{t=0}^{m-1} Y_t^{e_t} \mid 0 \leq e_t \leq p-1\,,\ \sum_{t=0}^{m-1} e_t \leq \omega \right\} \tag{4.10}$$

We know give a new proof of the following theorem

Theorem 4.11 (Berman-Charpin)**.** *Let ω be an integer such that $0 \leq \omega \leq m(p-1)$. We have*

$$RM_{\mathbb{F}_p}(m,\omega) \ = \ R^{m(p-1)-\omega}$$

where R is defined in (4.5).

Proof. For simplicity, let $d = m(p-1)-\omega$. By (4.7), we have $\deg(H_{\mathbf{i}}(\mathbf{Y})) \leq \omega$, for $\lfloor \mathbf{i} \rfloor \geq d$. And it follows from Remark 4.4 (i), Remark 4.8 (ii) and (4.9) that

$$R^d \subseteq RM_{\mathbb{F}_p}(m,\omega).$$

It remains to show that $\dim_{\mathbb{F}_p}(RM_{\mathbb{F}_p}(m,\omega)) = \dim_{\mathbb{F}_p}(R^d)$.

By (4.10), we have

$$\dim_{\mathbb{F}_p}(RM_{\mathbb{F}_p}(m,\omega)) = \mathrm{card}\,\{\, \mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m \mid \lfloor \mathbf{i} \rfloor \leq \omega \,\}$$

and by (4.6), we have

$$\dim_{\mathbb{F}_p}(R^d) = \mathrm{card}\,\{\, \mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m \mid \lfloor \mathbf{i} \rfloor \geq d \,\}.$$

It is clear that the map

$$\begin{array}{rccc} \theta: & (\mathbb{Z}/p\mathbb{Z})^m & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^m \\ & \mathbf{i} = (i_0, ..., i_{m-1}) & \longmapsto & \theta(\mathbf{i}) = (p-1-i_0, ..., p-1-i_{m-1}) \end{array}$$

is a bijection with $\theta^{-1} = \theta$. And we obtain

$$\lfloor \theta(\mathbf{i}) \rfloor \;=\; \sum_{t=0}^{m-1} p - 1 - i_t \;=\; m(p-1) - \lfloor \mathbf{i} \rfloor.$$

It follows that $\lfloor \mathbf{i} \rfloor \;=\; m(p-1) - \lfloor \theta(\mathbf{i}) \rfloor$.

Thus, we have the following equivalence

$$\lfloor \mathbf{i} \rfloor \;\leq \omega \quad\Longleftrightarrow\quad \lfloor \theta(\mathbf{i}) \rfloor \;\geq m(p-1) - \omega.$$

This implies that

$$\operatorname{card}\{\, \mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m \mid \lfloor \mathbf{i} \rfloor \;\leq \omega \,\} \;=\; \operatorname{card}\{\, \mathbf{i} \in (\mathbb{Z}/p\mathbb{Z})^m \mid \lfloor \mathbf{i} \rfloor \geq m(p-1) - \omega \,\}.$$

□

ORCID iDs

Harinaivo Andriatahiny https://orcid.org/0000-0003-4847-3854

References

[1] E. F. Assmus, Jr., On Berman's characterization of the Reed-Muller codes, *J. Statist. Plann. Inference* **56** (1996), 17–21, doi:10.1016/s0378-3758(96)00004-3, special issue on orthogonal arrays and affine designs, Part I.

[2] E. F. Assmus, Jr. and J. D. Key, Polynomial codes and finite geometries, in: *Handbook of coding theory, Vol. I, II*, North-Holland, Amsterdam, pp. 1269–1343, 1998.

[3] T. Berger and P. Charpin, The automorphism group of generalized Reed-Muller codes, *Discrete Math.* **117** (1993), 1–17, doi:10.1016/0012-365x(93)90321-j.

[4] S. D. Berman, On the theory of group codes, *Cybernetics* **3** (1967), 25–31, doi:10.1007/bf01072842.

[5] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1975, doi:10.1016/c2013-0-10384-4.

[6] P. Charpin, Une generalisation de la construction de berman des codes de reed et muller p-aires, *Commun. Algebra* **16** (1988), 2231–2246, doi:10.1080/00927878808823689.

[7] P. Delsarte, J.-M. Goethals and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control* **16** (1970), 403–442, doi:10.1016/s0019-9958(70)90214-7.

[8] T. Kasami, S. Lin and W. Peterson, New generalizations of the reed-muller codes–i: Primitive codes, *IEEE Trans. Inf. Theory* **14** (1968), 189–199, doi:10.1109/tit.1968.1054127.

[9] E. Kouselo, S. Gonsales, V. T. Markov, K. Martines and A. A. Nechaev, Ideal representations of Reed-Solomon and Reed-Muller codes, *Algebra Logic* **51** (2012), 297–320, 414, 417, doi:10.1007/s10469-012-9183-8.

[10] P. Landrock and O. Manz, Classical codes as ideals in group algebras, *Des. Codes Cryptogr.* **2** (1992), 273–285, doi:10.1007/bf00141972.

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

[12] A. Poli, Codes stables sous le groupe des automorphismes isométriques de $A = \mathbf{F}_p[X_1, \cdots, X_n]/(X_1^p - 1, \cdots, X_n^p - 1)$, *C. R. Acad. Sci. Paris Sér. A-B* **290** (1980), A1029–A1032.