Projective Reed-Muller Codes Revisited

Sudhir R. Ghorpade

Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400076, India
http://www.math.iitb.ac.in/∼srg/

Based on joint work with Rati Ludhani

ALgebraic and combinatorial methods for COding and CRYPTography
CIRM, Luminy, France
February 23, 2023

Reed-Muller codes : A Brief History

- Reed-Muller codes constitute a widely studied and fairly well-understood class of linear codes. These codes were introduced, in the binary case, by David Muller, and further studied by Irving Reed in the following papers, both published in September 1954.
  - D. E. Muller, Application of Boolean algebra to switching circuit design and to error detection, *IRE Trans. Electron. Comput.* **EC-3** (1954), 6–12
  - I. S. Reed, A class of multiple-error-correcting codes and the decoding scheme, *IRE Trans. Inform. Theory* **4** (1954), 38–49.
- Generalizations to the q-ary case were considered and extensively studied in the following papers.
  - T. Kasami, S. Lin, and W. W. Peterson, New Generalization of the Reed-Muller Codes–Part I: Primitive Codes, *IEEE Trans. Inform. Theory* **IT-14** (1968), 189–199.
  - P. Delsarte, J. M. Goethals, and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Inform. Control*, **16** (1970), 403–442.

(Generalized) Reed-Muller code

Definition

Let $m, \nu \in \mathbb{Z}$ with $m \geq 1$ and $\nu \geq 0$. Write $\mathbb{F}_q^m = \{P_1, \ldots, P_{q^m}\}$. Consider

$$\text{ev} : \mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu} \to \mathbb{F}_q^{q^m} \quad \text{defined by} \quad f \mapsto c_f := (f(P_1), \ldots, f(P_{q^m})).$$

Then (generalized or affine) Reed-Muller code of order ν and length q^m is

$$\mathrm{RM}_q(\nu, m) = \text{im}(\text{ev}) = \text{ev}\left(\mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu}\right).$$

(Generalized) Reed-Muller code

Definition

Let $m, \nu \in \mathbb{Z}$ with $m \geq 1$ and $\nu \geq 0$. Write $\mathbb{F}_q^m = \{P_1, \ldots, P_{q^m}\}$. Consider

$$\text{ev} : \mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu} \to \mathbb{F}_q^{q^m} \quad \text{defined by} \quad f \mapsto c_f := (f(P_1), \ldots, f(P_{q^m})).$$

Then (generalized or affine) Reed-Muller code of order ν and length q^m is

$$\mathrm{RM}_q(\nu, m) = \text{im}(\text{ev}) = \text{ev}\left(\mathbb{F}_q[X_1, \ldots, X_m]_{\leq \nu}\right).$$

Simple Observations.

- $\mathrm{RM}_q(\nu, m)$ is a nondegenerate q-ary linear code of length q^m.
- When $\nu < q$, the map ev is injective and so $\dim \mathrm{RM}_q(\nu, m) = \binom{m+\nu}{\nu}$.
- When $\nu \geq m(q-1)$, the map ev is surjective and so $\mathrm{RM}_q(\nu, m) = \mathbb{F}_q^{q^m}$.
- If $\nu < q$, then $d\left(\mathrm{RM}_q(\nu, m)\right) = q^m - \nu q^{m-1} = (q - \nu q^{m-1}$, thanks to:

  Ore's bound: If $0 \neq f \in \mathbb{F}_q[X_1, \ldots, X_m]$ has degree $\nu < q$, then it has at most νq^{m-1} zeros in $\mathbb{F}_q^m$.

Summary of Known Results about Reed-Muller codes

Fix $m \geq 1$ and $0 \leq \nu \leq m(q-1)$ and let $C = \mathrm{RM}_q(\nu, m)$. Then

- $\dim C = \sum_{s=0}^{\nu} \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{s - iq + m - 1}{s - iq} = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{m + \nu - iq}{m}.$
- [Kasami-Lin-Peterson] Write $\nu = t(q-1) + s$ with $t \geq 0$ and $0 \leq s < q - 1$. Then $d(C) = (q-s)q^{m-t-1}$.
- [Delsarte-Goethals-MacWilliams] Let t, s be as above. Then $c \in \mathrm{RM}_q(\nu, m)$ is a minimum weight codeword if and only if $c = \mathrm{ev}(f)$, where $f = \omega_0 \left(\prod_{i=1}^{t} (1 - L_i^{q-1}) \right) \prod_{j=1}^{s} (L_{t+1} - \omega_j)$ for some lin. indep. linear $L_1, \ldots, L_{t+1} \in \mathbb{F}_q[X_1, \ldots, X_m]$, $0 \neq \omega_0 \in \mathbb{F}_q$, and distinct $\omega_1, \ldots, \omega_s \in \mathbb{F}_q$.
- [Delsarte-Goethals-MacWilliams] $C^\perp = \mathrm{RM}_q(m(q-1) - \nu - 1, m)$.
- [Berger-Charpin] $\mathrm{Aut}(C)$ is the affine general linear group $\mathrm{AGL}(m, \mathbb{F}_q)$.
- [Heijnen–Pellikaan] All generalized Hamming weights of C are known.

Projective Reed-Muller codes : A Brief History

- Projective Reed-Muller codes were introduced[1] by Gilles Lachaud and further studied by Anders Bjært Sørensen, in the following papers.
  - G. Lachaud, Projective Reed-Muller codes, in; "Coding Theory and Applications" (Cachan, 1986), pp. 125–129, *Lecture Notes in Comput. Sci.,* **311**, Springer, Berlin, 1988.
  - G. Lachaud, The parameters of projective Reed-Muller codes, *Discrete Math.* **81** (1990), 217–221.
  - A. B. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* **37** (1991), 1567–1576.
- Questions about the minimum distance of these codes are related to:

  Tsfasman's Conjecture: If $0 \neq F \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]$ is homogeneous of degree $d \leq q$, then it has at most $dq^{m-1} + p_{m-2}$ zeros in $\mathbb{P}^m(\mathbb{F}_q)$.

  This was proved in the affirmative by J.-P. Serre and A. B. Sørensen.

[1] S. Ghorpade, C. Ritzenthaler, F. Rodier and M. Tsfasman, Arithmetic, Geometry, and Coding Theory: Homage to Gilles Lachaud, *Contemp. Math.* **770** (2021), 131–150.

Another Geometric Viewpoint

The study of the projective Reed-Muller code $\mathrm{PRM}_q(\nu, m)$ is closely related to that of the Veronese variety, which is the image of the ν-ple embedding

$$\mathbb{P}^m \hookrightarrow \mathbb{P}^{\binom{m+\nu}{\nu}-1}$$

and the $\mathbb{F}_q$-rational points of its hyperplane sections as well as linear sections. In this set-up the study is also related to linear authentication schemes.

Remark: A good reference for Veroneseans, over $\mathbb{F}_q$, is:
W. M. Kantor and E. E. Shult, Veroneseans, power subspaces and independence, *Adv. Geom.* **13** (2013), 511–531.
Here they remark that their first main theorem can be viewed as a statement about a certain code C having a check matrix whose columns consist of one nonzero vector in each Veronesean point. Then they write:
We have not been able to find any reference to this code in the literature. It is probably worth studying, at least from a geometric perspective.

Projective Reed-Muller codes

For $j \geq 0$, define $p_j := |\mathbb{P}^j(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^j$. Set $p_j := 0$ if $j < 0$.

Definition (Lachaud, 1988; Sørensen, 1991)

Let $m, \nu \in \mathbb{Z}$ with $m \geq 1$ and $\nu \geq 0$. Fix unique representatives $\mathsf{P}_1, \ldots, \mathsf{P}_{p_m}$ of points of $\mathbb{P}^m(\mathbb{F}_q)$ in $\mathbb{F}_q^{m+1}$ having last nonzero coordinate 1. Consider

$$\mathrm{Ev} : \mathbb{F}_q[X_0, \ldots, X_m]_\nu \to \mathbb{F}_q^{p_m} \quad \text{defined by} \quad f \mapsto c_f := (f(\mathsf{P}_1), \ldots, f(\mathsf{P}_{p_m})).$$

Then projective Reed-Muller code of order ν and length p_m is

$$\mathrm{PRM}_q(\nu, m) = \mathrm{im}(\mathrm{Ev}) = \mathrm{Ev}(\mathbb{F}_q[X_0, \ldots, X_m])_\nu.$$

Projective Reed-Muller codes

For $j \geq 0$, define $p_j := |\mathbb{P}^j(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^j$. Set $p_j := 0$ if $j < 0$.

Definition (Lachaud, 1988; Sørensen, 1991)

Let $m, \nu \in \mathbb{Z}$ with $m \geq 1$ and $\nu \geq 0$. Fix unique representatives $\mathsf{P}_1, ..., \mathsf{P}_{p_m}$ of points of $\mathbb{P}^m(\mathbb{F}_q)$ in $\mathbb{F}_q^{m+1}$ having last nonzero coordinate 1. Consider

$$\mathrm{Ev} : \mathbb{F}_q[X_0, \ldots, X_m]_\nu \to \mathbb{F}_q^{p_m} \quad \text{defined by} \quad f \mapsto c_f := (f(\mathsf{P}_1), \ldots, f(\mathsf{P}_{p_m})).$$

Then projective Reed-Muller code of order ν and length p_m is

$$\mathrm{PRM}_q(\nu, m) = \mathrm{im}(\mathrm{Ev}) = \mathrm{Ev}(\mathbb{F}_q[X_0, \ldots, X_m])_\nu.$$

Observations.

- $\mathrm{PRM}_q(\nu, m)$ is a nondegenerate q-ary linear code of length p_m.
- When $\nu \leq q$, the map Ev is injective and so $\dim \mathrm{PRM}_q(\nu, m) = \binom{m+\nu}{\nu}$.
- When $\nu \geq m(q-1)+1$, the map Ev is surjective and so $\mathrm{PRM}_q(\nu, m) = \mathbb{F}_q^{p_m}$.
- If $\nu \leq q$, then affirmative answer to Tsfasman's conjecture shows that $d\left(\mathrm{PRM}_q(\nu, m)\right) = (q - \nu + 1)q^{m-1}$.

Known Results about Projective Reed-Muller codes

Fix $m \geq 1$ and $1 \leq \nu \leq m(q-1)+1$ and let $C = \mathrm{PRM}_q(\nu, m)$. Then

- [Sørensen] $\dim C = \displaystyle\sum_{\substack{i=1 \\ i \equiv \nu \pmod{q-1}}}^{\nu} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{i-jq+m}{i-jq} \right),$
- [Mercier-Rolland (1998)]
$$\dim C = \binom{m+\nu}{\nu} - \sum_{j=2}^{m+1} (-1)^j \binom{m+1}{j} \sum_{i=0}^{j-2} \binom{\nu+(i+1)(q-1)-jq+m}{\nu+(i+1)(q-1)-jq}.$$
- [Sørensen] Write $\nu - 1 = t(q-1) + s$ with $t \geq 0$ and $0 \leq s < q-1$. Then
$$d(C) = (q-s)q^{m-t-1}$$
- [Sørensen] Suppose $\mathbf{1}$ denotes that all-1 vector in $\mathbb{F}_q^{p_m}$. Then
$$C^{\perp} = \begin{cases} \mathrm{PRM}_q(m(q-1)-\nu, m) & \text{if } \nu \not\equiv 0 \pmod{(q-1)}, \\ \mathrm{PRM}_q(m(q-1)-\nu, m) + \langle \mathbf{1} \rangle & \text{if } \nu \equiv 0 \pmod{(q-1)}. \end{cases}$$
- [Berger (2002)] $\mathrm{Aut}(C)$ is known explicitly.

What is Not Known about PRM codes?

- A characterization of minimum weight codewords does not appear to be known in the literature.
- Generalized Hamming weights of projective Reed-Muller codes are not known, in general, and this has been a topic of considerable investigation. When $\nu \leq q$, this is equivalent to the following geometric

  Question: What is the maximum possible number of $\mathbb{F}_q$-rational points on a projective algebraic variety in $\mathbb{P}^m$ defined by r linearly independent homogeneous polynomial equations of degree $\nu \leq q$ in $m+1$ variables with coefficients in $\mathbb{F}_q$?

  Answer to this question are known in many cases, and one may refer to the following paper for the current state of the art.

  P. Beelen, M. Datta, and S. R. Ghorpade, A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields, *Moscow Math J.* **22** (2022), 565–593.

Sørensen’s paper and its impact

Sørensen’s paper was published in 1991 and it has a large number of citations.

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 37, NO. 6, NOVEMBER 1991 1567

Projective Reed–Muller Codes

Anders Bjært Sørensen

Abstract—**A class of codes in the Reed–Muller family, the projective Reed–Muller codes, are studied. The exact parameters of the codes are derived and the duals are characterized. It is shown that a subclass of the projective Reed–Muller codes are cyclic and the generator polynomial is characterized. Tables over parameters of the codes are given.**

Index Terms—**Error-correcting codes, Reed–Muller codes, cyclic codes, finite projective geometry.**

I. Introduction

THE GENERALIZED Reed–Muller codes (GRM codes) were introduced by Kasami, Lin, and Peterson [1] and Weldon [2]. They showed that GRM codes are cyclic and thereby determined the minimum distance. Kasami, Lin, and Peterson [3] introduced the polynomial codes as a generalization of GRM codes (and of other codes as well) based on the multivariable approach. Delsarte, Goethals, and MacWilliams [4] studied in detail the connection between the multivariable and one-variable approach to GRM codes. All these classical works appeared about 1970.

It seems that Manin and Vlăduţ in a paper on algebraic geometric codes [5] are the first to mention the very natural projective parallel of the multivariable GRM construction, which leads to the projective Reed–Muller codes (PRM codes). They obtained bounds on the minimum distance of PRM codes over $\mathbb{F}_q$ of order ν for $\nu < q$, q a prime power. Lachaud [6] is the first to introduce the notation of projective Reed–Muller codes and studies PRM codes of order 1 and 2.

This paper defines, in Section II, the PRM codes of all orders and discusses their relation to polynomial codes. In Section III the exact parameters of PRM codes are given. The duals are characterized in Section IV and in parallel to the classical works on GRM codes the cyclic properties are studied in Section V. It is shown that a subclass of PRM codes is cyclic. A number of examples are shown in detail and tables over codeparameters are listed.

Manuscript received January 2, 1990; revised November 11, 1990. This work was supported by the Danish Natural Science Research Council. This work was presented at the Fourth Nordic Symposium in Discrete Mathematics, Frederikshavn, Denmark, June 14–16, 1990.

The author is with the Department of Mathematics, University of Aarhus, DK-8000, Aarhus C, Denmark.

IEEE Log Number 9102343.

II. Definition of Projective Reed–Muller Codes

We introduce some useful concepts and necessary notation.

A. Nomenclature

$\mathbb{F}_q$	Finite field with q elements, q a prime power. $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.
$\mathbb{F}_q[X_0, X_1, \cdots, X_m]$	Ring of polynomials in $X_0, X_1, \cdots, X_m$ with coefficients in $\mathbb{F}_q$.
$\mathbb{F}_q[X_0, X_1, \cdots, X_m]^\nu \cup \{0\}$	Vectorspace of polynomials in $X_0, X_1, \cdots, X_m$ with coefficients in $\mathbb{F}_q$ and of degree ν.
$\mathbb{F}_q[X_0, X_1, \cdots, X_m]_h \cup \{0\}$	Vectorspace of homogeneous polynomials in $X_0, X_1, \cdots, X_m$ with coefficients in $\mathbb{F}_q$.
$\mathbb{F}_q[X_0, X_1, \cdots, X_m]_h^\nu \cup \{0\}$	Vectorspace of homogeneous polynomials in $X_0, X_1, \cdots, X_m$ with coefficients in $\mathbb{F}_q$ and of degree ν.
$\mathbb{A}^m(\mathbb{F}_q)$	m-dimensional affine space over $\mathbb{F}_q$ $(= \mathbb{F}_q^m)$.
$\mathbb{P}^m(\mathbb{F}_q)$	m-dimensional projective space over $\mathbb{F}_q$.

We will often use the abbreviations $\mathbb{A}^m$ for $\mathbb{A}^m(\mathbb{F}_q)$, $\mathbb{P}^m$ for $\mathbb{P}^m(\mathbb{F}_q)$ and $X = X_1, \cdots, X_m$ or $X = X_0, X_1, \cdots, X_m$.

If $F(X) \in \mathbb{F}_q[X_0, X_1, \cdots, X_m]$ and $P \in \mathbb{P}^m(\mathbb{F}_q)$, then $F(P)$ means F evaluated in some representative $(a_0 : a_1 : \cdots : a_m)$ for P. Therefore $F(P)$ is in general dependent on the choice of representative for P. The standard representation for projective points is on the form $(0 : \cdots : 0 : 1 : a_j : \cdots : a_m)$, that is zeros to the left and the first nonzero entry equal to 1. Unless explicit stated otherwise the standard representation will be used.

It is well known, cf. [4], that the GRM codes $C_\nu(m,q)$ over $\mathbb{F}_q$ of order ν, $1 \le \nu \le m(q-1)$ and of length q^m can be defined as

$$C_\nu(m,q) = \Big\{ \big(F(\mathbf{0}), F(P_1), \cdots, F(P_{q^m-1})\big) \,\Big|\, F(X_1, \cdots, X_m) \in \mathbb{F}_q[X_1, \cdots, X_m],\ \deg(F) \le \nu \Big\},$$

where $P_i \in \mathbb{A}^m(\mathbb{F}_q)$ runs through $\mathbb{A}^m(\mathbb{F}_q) \setminus \{\mathbf{0}\}$ for $i =$

AMERICAN MATHEMATICAL SOCIETY
MathSciNet
Mathematical Reviews

Previous | Up | Next

Citations	From References: 67	From Reviews: 3

MR1134296 (92g:94018) 94B15
Sørensen, Anders Bjært (DK-ARHS)
Projective Reed-Muller codes.
IEEE Trans. Inform. Theory **37** (1991), *no. 6,* 1567–1576.

Summary: “A class of codes in the Reed-Muller family, the projective Reed-Muller codes, are studied. The exact parameters of the codes are derived and the duals are characterized. It is shown that a subclass of the projective Reed-Muller codes are cyclic and the generator polynomial is characterized. Tables over parameters of the codes are given.”

Why revisit PRM codes and Sørensen's paper?

Unfortunately, the proof of Theorem 1 (which is about the minimum distance of $\mathrm{PRM}_q(\nu, m)$) in Sørensen's paper appears to have a gap.

More precisely, in the case when $\nu - 1 = (m-1)(q-1) + s$, where $0 \leq s \leq (q-1)$, Sørensen, on p. 1569 of his paper, considers the complement $\mathbb{P}^m(\mathbb{F}_q) \setminus X$ of the set $X = V(F)$ of zeros in $\mathbb{P}^m(\mathbb{F}_q)$ of the homogeneous polynomial F of degree ν and writes this complement as $\{P_1, \ldots, P_t\}$. He then goes on to say that we can find linear homogeneous polynomials $G_i(\mathbf{X})$, $i = 1, \ldots, t-1$ such that

$$G_i(P_j) = \delta_{ij} \quad \text{for } i = 1, \ldots, t-1 \text{ and } j = 1, \ldots, t.$$

However, this may not be true since it is possible that some P_j is a linear combination of other points P_i. Furthermore, his claim that the polynomial

$$H(\mathbf{X}) = F(\mathbf{X}) \prod_{i=1}^{t-1} G_i(\mathbf{X})$$

satisfies $V(H) = \mathbb{P}^m(\mathbb{F}_q) \setminus \{P_t\}$, seems erroneous as well.

Our contribution

Thankfully, Sørensen's result about the minimum distance of the projective Reed-Muller code $\mathrm{PRM}_q(\nu, m)$ is correct (and even the proof can be fixed). But while trying to understand his result, we have been able to:

- Give a new proof of the formula

$$d\left(\mathrm{PRM}_q(\nu, m)\right) = (q-s)q^{m-t-1}$$

  where $t, s \in \mathbb{Z}$ are determined by the equation $\nu - 1 = t(q-1) + s$ and the conditions $t \geq 0$ and $0 \leq s < q-1$.
  [For this new proof, we essentially follow the idea of Serre in his resolution of Tsfasman's conjecture, but also combine it with the results and techniques of Delsarte, Goethals and MacWilliams.]

- Given a characterization of minimum weight codewords of $\mathrm{PRM}_q(\nu, m)$.

Minimum weight codewords of PRM codes

More precisely, we prove the following.

Theorem

Assume that $1 \le \nu \le m(q-1)+1$ *and let* $c \in \mathrm{PRM}_q(d,m)$. *Write*

$$\nu - 1 = t(q-1) + s,$$

where $t, s \in \mathbb{Z}$ *are such that* $t \ge 0$ *and* $0 \le s < q-1$. *Then* c *is a minimum weight codeword of* $\mathrm{PRM}_q(\nu, m)$ *if and only if* $c = c_F = \mathrm{Ev}(F)$ *for some* $F \in \mathbb{F}_q[X_0, \ldots, X_m]_\nu$ *of the form*

$$L_t \prod_{i=0}^{t-1} \left(L_i^{q-1} - L_t^{q-1} \right) \prod_{j=1}^{s} (L_{t+1} - \omega_j L_t)$$

where $L_0, L_1, \ldots, L_{t+1}$ *are linearly independent linear homogeneous polynomials over* $\mathbb{F}_q$ *and* $\omega_1, \ldots, \omega_s$ *are distinct elements of* $\mathbb{F}_q$.

Thank you for your attention!