Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-024-01392-z

Jacobi polynomials for the first-order generalized Reed–Muller codes

Ryosuke Yamaguchi[1]

Received: 5 September 2023 / Revised: 25 February 2024 / Accepted: 1 March 2024

Abstract
In this paper, we give the Jacobi polynomials for first-order generalized Reed–Muller codes. We show as a corollary the nonexistence of combinatorial 3-designs in these codes.

Keywords Generalized Reed–Muller code · Combinatorial t-design · Jacobi polynomial

Mathematics Subject Classification Primary 94B05 · Secondary 05B05

1 Introduction

There is growing interest in the designs derived from codes within the fields of coding theory and design theory. In [3, 9], a criterion was provided for determining whether a shell of a code constitutes a t-design, using Jacobi polynomials (see Proposition 2.2, the definition of the Jacobi polynomials will be given in Sect. 2.2). Using this criterion, in [3, 5], they presented t-designs derived from Type II, III, and IVcodes with short lengths. Additionaly, Miezaki and Munemasa [6] provided Jacobi polynomials for the first-order Reed–Muller codes. As a corollary, they showed the nonexistence of combinatorial 4-designs in these codes. The purpose of the present paper is to give a generalization of Miezaki and Munemasa's results.

Let m be a positive integer and q be a prime power, and set $V = \mathbb{F}_q^m$. The first-order generalized Reed–Muller (GRM) code $RM_q(1, m)$ is defined as the subspace of $\mathbb{F}_q^V$ consisting of affine linear functions:

$$RM_q(1, m) = \left\{(\lambda(x) + b)_{x \in V} \in \mathbb{F}_q^V \mid \lambda \in V^*, b \in \mathbb{F}_q\right\},$$

where $V^* = \mathrm{Hom}(V, \mathbb{F}_q)$. We remark that the weight enumerator of $RM_q(1, m)$ is

$$x^{q^m} + (q^{m+1} - q)x^{q^{m-1}} y^{(q-1)q^{m-1}} + (q-1)y^{q^m}. \tag{1.1}$$

Communicated by T. Feng.

✉ Ryosuke Yamaguchi
ryosuke.yama.821@fuji.waseda.jp

[1] School of Fundamental Science and Engineering, Waseda University, Tokyo 169–8555, Japan

Published online: 08 April 2024

Let $C = RM_q(1, m)$ and $C_\ell := \{c \in C \mid \mathrm{wt}(c) = \ell\}$. In this paper, we call C_ℓ a shell of the code C whenever it is non-empty. We show shells of C are combinatorial 2-designs but are not combinatorial 3-designs by using Jacobi polynomials. More precisely, the set $\mathcal{B}(C_\ell) := \{\mathrm{supp}(x) \mid x \in C_\ell\}$ forms the set of blocks of a combinatorial 2-design but does not form a 3-design. Herein, we always assume that a combinatorial t-design allows the existence of repeated blocks, and we exclude the trivial design $\mathcal{D} = (\Omega, \mathcal{B})$ where $\Omega = \{1, \ldots, n\}$ and $\mathcal{B} = \{\Omega, \ldots, \Omega\}$.

Remark In [7], Miezaki and Nakasora provided the first non-trivial examples of a code whose shells are t-designs for all weights and whose shells are t'-designs for some weights with some $t' > t$ (see also [1, 8]). Therefore, it is important to determine the value t such that all shells of a code are t-designs, and no shell is a $t+1$-design, if such a t exists.

First, we provide Jacobi polynomials for C with T, where $|T| = 2$.

Theorem 1.1 *Let $C = RM_q(1, m)$ and $T = \{0, u\} \in \binom{V}{2}$. Then,*

$$\begin{aligned} J_{C,T}(w, z, x, y) =& w^2 x^{q^m-2} + (q^{m-1} - 1) w^2 x^{q^{m-1}-2} y^{(q-1)q^{m-1}} \\ &+ 2(q-1)q^{m-1} wz x^{q^{m-1}-1} y^{(q-1)q^{m-1}-1} \\ &+ (q-1)(q^m - q^{m-1} - 1) z^2 x^{q^{m-1}} y^{(q-1)q^{m-1}-2} \\ &+ (q-1) z^2 y^{q^m-2}. \end{aligned}$$

Using this theorem, we show that the shells of $RM_q(1, m)$ and $RM_q(1, m)^\perp$ are 2-designs.

Corollary 1.2 *Let $C = RM_q(1, m)$. Then for any $\ell \in \mathbb{N}$, C_ℓ is a combinatorial 2-design. Similarly, $(C^\perp)_\ell$ is a combinatorial 2-design.*

Second, we provide Jacobi polnomials for C with T, where $|T| = 3$.

Theorem 1.3 *Let $C = RM_q(1, m)$, $T = \{0, u_1, u_2\} \in \binom{V}{3}$, and $A = {}^t[u_1\ u_2]$.*

1. *If* rank $A = 2$, *then*

$$\begin{aligned} J_{C,T}(w, z, x, y) =& w^3 x^{q^m-3} + (q^{m-2} - 1) w^3 x^{q^{m-1}-3} y^{(q-1)q^{m-1}} \\ &+ 3q^{m-2}(q-1) w^2 z x^{q^{m-1}-2} y^{(q-1)q^{m-1}-1} \\ &+ 3q^{m-2}(q-1)^2 w z^2 x^{q^{m-1}-1} y^{(q-1)q^{m-1}-2} \\ &+ (q-1)(q^m - 2q^{m-1} + q^{m-2} - 1) z^3 x^{q^{m-1}} y^{(q-1)q^{m-1}-3} \\ &+ (q-1) z^3 y^{q^m-3}. \end{aligned}$$

2. *If* rank $A = 1$, *then*

$$\begin{aligned} J_{C,T}(w, z, x, y) =& w^3 x^{q^m-3} + (q^{m-1} - 1) w^3 x^{q^{m-1}-3} y^{(q-1)q^{m-1}} \\ &+ 3q^{m-1}(q-1) w z^2 x^{q^{m-1}-1} y^{(q-1)q^{m-1}-2} \\ &+ (q-1)(q^m - 2q^{m-1} - 1) z^3 x^{q^{m-1}} y^{(q-1)q^{m-1}-3} \\ &+ (q-1) z^3 y^{q^m-3}. \end{aligned}$$

We show, as a corollary, the nonexistence of combinatorial 3-designs in these codes.

Corollary 1.4 *Let $C = RM_q(1,m)$. If $q \geq 3$ and $m \geq 2$, then for any $\ell \in \mathbb{N}$, C_ℓ is not a combinatorial 3-design.*

Using Theorem 1.3, we show that C_ℓ is a 3-$(v, k, (\lambda_1, \lambda_2))$-design (see Sect. 2.1).

Corollary 1.5 *Let $C = RM_q(1,m)$ and $\ell = (q-1)q^{m-1}$. Then, C_ℓ is a combinatorial 3-$(v, k, (\lambda_1, \lambda_2))$-design, where*

$$\begin{aligned}
v &= q^m,\ k = \ell = (q-1)q^{m-1},\\
\lambda_1 &= (q-1)(q^m - 2q^{m-1} + q^{m-2} - 1),\\
\lambda_2 &= (q-1)(q^m - 2q^{m-1} - 1).
\end{aligned}$$

Third, we provide Jacobi polnomials for C with T, where $|T| = 4$.

Theorem 1.6 *Let $C = RM_q(1,m)$, $T = \{0, u_1, u_2, u_3\} \in \binom{V}{4}$, and $A = {}^t[u_1\ u_2\ u_3]$.*

1. *If* rank $A = 3$ *then,*

$$\begin{aligned}
J_{C,T}(w,z,x,y) = &w^4 x^{q^m-4} + (q^{m-3}-1) w^4 x^{q^{m-1}-4} y^{(q-1)q^{m-1}}\\
&+ 4q^{m-3}(q-1) w^3 z x^{q^{m-1}-3} y^{(q-1)q^{m-1}-1}\\
&+ 6(q-1)^2 q^{m-3} w^2 z^2 x^{q^{m-1}-2} y^{(q-1)q^{m-1}-2}\\
&+ 4q^{m-3}(q-1)^3 w z^3 x^{q^{m-1}-1} y^{(q-1)q^{m-1}-3}\\
&+ (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - q^{m-3} - 1) z^4 x^{q^{m-1}} y^{(q-1)q^{m-1}-4}\\
&+ (q-1) z^4 y^{q^m-4}.
\end{aligned}$$

2. *If* rank $A = 2$ *then,*

$$\begin{aligned}
J_{C,T}(w,z,x,y) = &w^4 x^{q^m-4} + (q^{m-2}-1) w^4 x^{q^{m-1}-4} y^{(q-1)q^{m-1}}\\
&+ q^{m-2}(q-1) w^3 z x^{q^{m-1}-3} y^{(q-1)q^{m-1}-1}\\
&+ 3q^{m-2}(q-1) w^2 z^2 x^{q^{m-1}-2} y^{(q-1)q^{m-1}-2}\\
&+ q^{m-2}(q-1)(4q-5) w z^3 x^{q^{m-1}-1} y^{(q-1)q^{m-1}-3}\\
&+ (q-1)(q^m - 3q^{m-1} + 2q^{m-2} - 1) z^4 x^{q^{m-1}} y^{(q-1)q^{m-1}-4}\\
&+ (q-1) z^4 y^{q^m-4}
\end{aligned}$$

   or

$$\begin{aligned}
J_{C,T}(w,z,x,y) = &w^4 x^{q^m-4} + (q^{m-2}-1) w^4 x^{q^{m-1}-4} y^{(q-1)q^{m-1}}\\
&+ 6q^{m-2}(q-1) w^2 z^2 x^{q^{m-1}-2} y^{(q-1)q^{m-1}-2}\\
&+ q^{m-2}(q-1)(4q-8) w z^3 x^{q^{m-1}-1} y^{(q-1)q^{m-1}-3}\\
&+ (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - 1) z^4 x^{q^{m-1}} y^{(q-1)q^{m-1}-4}\\
&+ (q-1) z^4 y^{q^m-4}.
\end{aligned}$$

3. *If* rank $A = 1$ *then,*

$$\begin{aligned}J_{C,T}(w,z,x,y) =& w^4 x^{q^m-4} + (q^{m-1}-1)w^4 x^{q^{m-1}-4} y^{(q-1)q^{m-1}} \\ &+ 4q^{m-1}(q-1)wz^3 x^{q^{m-1}-1} y^{(q-1)q^{m-1}-3} \\ &+ (q-1)(q^m - 3q^{m-1} - 1)z^4 x^{q^{m-1}} y^{(q-1)q^{m-1}-4} \\ &+ (q-1)z^4 y^{q^m-4}.\end{aligned}$$

By this theorem, we show that C_ℓ is a combinatorial 4-$(v, k, (\lambda_1, \lambda_2, \lambda_3, \lambda_4))$-design.

Corollary 1.7 *Let* $C = RM_q(1, m)$ *and* $\ell = (q-1)q^{m-1}$*. Then* C_ℓ *is a* 4-$(v, k, (\lambda_1, \lambda_2, \lambda_3, \lambda_4))$-*design, where*

$$\begin{aligned}v &= q^m, \; k = \ell = (q-1)q^{m-1}, \\ \lambda_1 &= (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - q^{m-3} - 1), \\ \lambda_2 &= (q-1)(q^m - 3q^{m-1} + 2q^{m-2} - 1), \\ \lambda_3 &= (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - 1), \\ \lambda_4 &= (q-1)(q^m - 3q^{m-1} - 1).\end{aligned}$$

This paper is organized as follows. In Sect. 2, we define and give some basic properties of codes, combinatorial t-designs, and Jacobi polynomials used in this paper. In Sects. 3, 4, and 5, we show Theorems 1.1, 1.3, and 1.6, respectively.

All computer calculations reported in this paper were carried out using Magma [4] and Mathematica [10].

2 Preliminaries

In this section, we give definitions and some properties of codes, combinatorial designs, and Jacobi polynomials. We mainly refer to [6] and [5].

2.1 Codes and combinatorial *t*-designs

Let q be a prime power. A q-ary linear code C of length n is a linear subspace of $\mathbb{F}_q^n$. The dual code of C is the set of vectors which are orthogonal to any codewords in C: $C^\perp := \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C\}$. For $c \in \mathbb{F}_q^n$, the weight $\mathrm{wt}(c)$ is the number of its nonzero components. The shell of a weight-ℓ is the set of codewords whose weight is ℓ: $C_\ell := \{c \in C \mid \mathrm{wt}(c) = \ell\}$.

A combinatorial t-design is a pair $\mathcal{D} = (\Omega, \mathcal{B})$, where Ω is a set of points of cardinality v, and $\mathcal{B}$ is a collection of k-element subsets of Ω called blocks, with the property that any t-element subset of Ω is contained in precisely λ blocks. Recall [3] for the definitions of various types of designs. A pair $\mathcal{D} = (\Omega, \mathcal{B})$ is a combinatorial design with parameters t-$(v, k, (\lambda_1, \ldots, \lambda_N))$ if $\mathcal{B}$ is a collection of k-element subsets of Ω called blocks and every t-element subset of Ω is contained in λ_i blocks. Note that for $N = 1$, the design coincides exactly with a t-design.

The support of a vector $x := (x_1, \ldots, x_n)$, $x_i \in \mathbb{F}_q$, is the set of indices of its nonzero coordinates: $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$. Let $\Omega := \{1, \ldots, n\}$ and $\mathcal{B}(C_\ell) := \{\mathrm{supp}(x) \mid x \in C_\ell\}$. Then for a code C of length n, we say that the shell C_ℓ is a combinatorial t-design if

$(\Omega, \mathcal{B}(C_\ell))$ is a combinatorial t-design. Similarly, we say that the shell C_ℓ is a combinatorial t-$(v, k, (\lambda_1, \ldots, \lambda_N))$-design if $(\Omega, \mathcal{B}(C_\ell))$ is a combinatorial t-$(v, k, (\lambda_1, \ldots, \lambda_N))$-design.

2.2 Jacobi poynomials

Let C be a q-ary code of length n and $T \subset [n] := \{1, \ldots, n\}$. Then the Jacobi polynomial of C with T is defined as follows [9]:

$$J_{C,T}(w, z, x, y) := \sum_{c \in C} w^{m_0(c)} z^{m_1(c)} x^{n_0(c)} y^{n_1(c)},$$

where for $c = (c_1, \ldots, c_n)$,

$$\begin{aligned} m_0(c) &= |\{j \in T \mid c_j = 0\}|, \\ m_1(c) &= |\{j \in T \mid c_j \neq 0\}|, \\ n_0(c) &= |\{j \in [n] \setminus T \mid c_j = 0\}|, \\ n_1(c) &= |\{j \in [n] \setminus T \mid c_j \neq 0\}|. \end{aligned}$$

The Jacobi polynomial of the dual code is written as follows.

Theorem 2.1 [9, Theorem 4] *Let C be a q-ary code of length n and $T \subset [n]$. Then we have*

$$J_{C^\perp,T}(w, z, x, y) = \frac{1}{|C|} J_{C,T}(w + (q-1)z, w - z, x + (q-1)y, x - y).$$

Clearly, we have the following relation between Jacobi polynomials and combinatorial designs.

Proposition 2.2 *Let C be a linear code. C_ℓ is a combinatorial t-design if and only if the coefficient of $z^t x^{n-\ell} y^{\ell-t}$ in $J_{C,T}$ is independent of the choice of T with $|T| = t$.*

We remark that the Jacobi polynomials are invariant under the automorphisms of codes. In particular, for $C = RM_q(1, m)$, a map φ such that $\varphi(\lambda(x) + b') = \lambda(x) + b + b'$ is an automorphism on C. Then, we have the following result.

Proposition 2.3 *Let $C = RM_q(1, m)$, $T \subset V$, and $T' = T + v$, where $v \in V$. Then we have $J_{C,T} = J_{C,T'}$.*

This fact is useful because it suffices to consider the case that T contains zero.

2.3 Notation

We next introduce some notation. Let $C = RM_q(1, m)$, $T \subset V$, and $t = |T|$. For $c = (\lambda(x) + b)_{x \in V} \in C$ and $u \in V$, the evaluation of c at u is denoted by $c(u)$, which equals $\lambda(u) + b$. Let $i \in \{0, 1, \ldots, t\}$, $j \in \mathbb{F}_q$, we define

$$\begin{aligned} n_{j,T}(c) &:= |\{u \in T \mid c(u) = j\}|, \\ b_{i,j} &:= |\{c \in V^* \mid n_{j,T}(c) = i\}|, \end{aligned}$$

and

$$\begin{aligned} a_i &:= |\{c \in C \setminus \mathbb{F}_q\mathbf{1} \mid \mathrm{wt}(c|_T) = i\}|, \\ b_i &:= \sum_{j \in \mathbb{F}_q} b_{i,j} = \sum_{j \in \mathbb{F}_q} |\{c \in V^* \mid n_{j,T}(c) = i\}|. \end{aligned}$$

Then, the Jacobi polynomial of C with T is written as

$$\begin{aligned} J_{C,T}(w,z,x,y) =& w^t x^{q^m-t} \\ &+ \sum_{i=0}^{t} a_i w^{t-i} z^i x^{q^{m-1}-(t-i)} y^{(q-1)q^{m-1}-i} \\ &+ (q-1) z^t y^{q^m-t}. \end{aligned} \tag{2.1}$$

We have the following relation between a_i and b_i.

Lemma 2.4 *We have*

$$a_i = b_{t-i} - \delta_{i,0} - (q-1)\delta_{i,t}.$$

Proof Since

$$\begin{aligned} a_{t-i} &= |\{c \in C \setminus \mathbb{F}_q \mathbf{1} \mid n_{0,T}(c) = i\}| \\ &= \sum_{j \in \mathbb{F}_q} |\{c \in (V^* + j\mathbf{1}) \setminus \{j\mathbf{1}\} \mid n_{0,T}(c) = i\}| \\ &= \sum_{j \in \mathbb{F}_q} |\{c \in V^* \setminus \{0\} \mid n_{0,T}(c + j\mathbf{1}) = i\}| \\ &= \sum_{j \in \mathbb{F}_q} |\{c \in V^* \setminus \{0\} \mid n_{-j,T}(c) = i\}| \\ &= |\{c \in V^* \setminus \{0\} \mid n_{0,T}(c) = i\}| + \sum_{j \in \mathbb{F}_q \setminus \{0\}} |\{c \in V^* \setminus \{0\} \mid n_{-j,T}(c) = i\}| \\ &= b_{i,0} - \delta_{i,t} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} (b_{i,-j} - \delta_{i,0}) \\ &= \sum_{j \in \mathbb{F}_q} b_{i,-j} - \delta_{i,t} - (q-1)\delta_{i,0} \\ &= \sum_{j \in \mathbb{F}_q} b_{i,j} - \delta_{i,t} - (q-1)\delta_{i,0} \\ &= b_i - \delta_{i,t} - (q-1)\delta_{i,0}, \end{aligned}$$

we obtain

$$\begin{aligned} a_i &= b_{t-i} - \delta_{t-i,t} - (q-1)\delta_{t-i,0} \\ &= b_{t-i} - \delta_{i,0} - (q-1)\delta_{i,t}. \end{aligned}$$

□

Using this lemma, we obtain a_i by calculating b_i.

3 Proofs of Theorem 1.1 and Corollary 1.2

In this section, we give proofs of Theorem 1.1 and Corollary 1.2 using the notation introduced in Sect. 2.3. First, we give a lemma to show Theorem 1.1. Let $T = \{0, u\} \in \binom{V}{2}$.

Lemma 3.1 *We have*

$$b_0 = q^{m-1}(q-1)^2,$$
$$b_1 = 2q^{m-1}(q-1),$$
$$b_2 = q^{m-1}.$$

Proof Considering $u \in T$ as an element of V^{**}, u is a surjective linear map from V^* to $\mathbb{F}_q$ because $u \neq 0$. Then, for $j \in \mathbb{F}_q \backslash \{0\}$,

$$b_{0,0} = 0,\ b_{0,j} = \left| \bigcup_{a \in \mathbb{F}_q \backslash \{j\}} u^{-1}(a) \right| = (q-1)q^{m-1},$$
$$b_{1,0} = (q-1)q^{m-1},\ b_{1,j} = \left|u^{-1}(j)\right| = q^{m-1},$$
$$b_{2,0} = q^{m-1},\ b_{2,j} = 0.$$

Therefore,

$$b_0 = b_{0,0} + \sum_{j \in \mathbb{F}_q \backslash \{0\}} b_{0,j} = (q-1)^2 q^{m-1},$$
$$b_1 = b_{1,0} + \sum_{j \in \mathbb{F}_q \backslash \{0\}} b_{1,j} = 2(q-1)q^{m-1},$$
$$b_2 = b_{2,0} + \sum_{j \in \mathbb{F}_q \backslash \{0\}} b_{2,j} = q^{m-1}.$$

□

Using this Lemma, we show Theorem 1.1.

Proof of Theorem 1.1 Using Lemmas 2.4 and 3.1, we obtain

$$a_0 = b_2 - 1 = q^{m-1} - 1,$$
$$a_1 = b_1 = 2(q-1)q^{m-1},$$
$$a_2 = b_0 - (q-1) = (q-1)(q^m - q^{m-1} - 1).$$

Thus, we obtain coefficients of the Jacobi polynomial by (2.1). □

Finally, we give a proof of Corollary 1.2.

Proof of Corollary 1.2 By Proposition 2.3, it suffices to show that for any $T = \{0, u\} \subset \binom{V}{2}$, the coefficient of $z^2 x^{q^m - \ell} y^{\ell - 2}$ is the same value. This is true by using Theorem 1.1. In addition, we have the Jacobi polynomial of $RM_q(1, m)^{\perp}$ by using Theorem 2.1. Thus, we obtain the desired results. □

Remark Collorary 1.2 can be proved by 2-transitivity of the automorphism group of $RM_q(1, m)$, which is the general linear homogenious group [2].

4 Proofs of Theorem 1.3 and Corollary 1.4

In this section, we give proofs of Theorem 1.3 and Corollaries 1.4 and 1.5 using the notation introduced in Sect. 2.3. First, we give two lemmas to show Theorem 1.3. Let $T = \{0, u_1, u_2\} \in \binom{V}{3}$, $A = {}^t[u_1\ u_2]$.

Lemma 4.1 *If* rank $A = 2$, *then*

$$\begin{aligned} b_0 &= q^{m-2}(q-1)^3, \\ b_1 &= 3q^{m-2}(q-1)^2, \\ b_2 &= 3q^{m-2}(q-1), \\ b_3 &= q^{m-2}. \end{aligned}$$

Proof We remark that A is a surjective map from V to $\mathbb{F}_q^2$, and for all $a, b \in \mathbb{F}_q$, $|A^{-1}({}^t[a\ b])| = |\mathrm{Ker}\, A| = q^{m-2}$. Then, for $j \in \mathbb{F}_q \backslash \{0\}$,

$$\begin{aligned} b_{0,j} &= \left| \bigcup_{a,b \neq j} A^{-1}({}^t[a\ b]) \right| = \sum_{a,b \in \mathbb{F}_q \backslash \{j\}} \left| A^{-1}({}^t[a\ b]) \right| = (q-1)^2 q^{m-2}, \\ b_{1,j} &= 2 \times \left| \bigcup_{a \neq j} A^{-1}({}^t[j\ a]) \right| = 2(q-1)q^{m-2}, \\ b_{2,j} &= \left| A^{-1}({}^t[j\ j]) \right| = q^{m-2}, \\ b_{3,j} &= 0 \end{aligned}$$

and

$$\begin{aligned} b_{0,0} &= 0, \\ b_{1,0} &= \left| \bigcup_{a,b \neq 0} A^{-1}({}^t[a\ b]) \right| = \sum_{a,b \in \mathbb{F}_q \backslash \{0\}} \left| A^{-1}({}^t[a\ b]) \right| = (q-1)^2 q^{m-2}, \\ b_{2,0} &= 2 \times \left| \bigcup_{a \neq 0} A^{-1}({}^t[j\ a]) \right| = 2(q-1)q^{m-2}, \\ b_{3,0} &= |\mathrm{Ker}\, A| = q^{m-2}. \end{aligned}$$

Since

$$b_i = b_{i,0} + \sum_{j \in \mathbb{F}_q \backslash \{0\}} b_{i,j},$$

we obtain the desired results. □

Lemma 4.2 *If* rank $A = 1$, *then*

$$\begin{aligned} b_0 &= q^{m-1}(q-1)(q-2), \\ b_1 &= 3q^{m-1}(q-1), \\ b_2 &= 0, \\ b_3 &= q^{m-1}. \end{aligned}$$

Proof Because u_1 and u_2 are not equal to 0 or each other, there exist $a, b \in \mathbb{F}_q \setminus \{0\}$ such that $a \neq b$ and $\{{}^t[a\ b]\}$ is a basis of Im A. Hence, for any $v \in \text{Im } A$,

$$|A^{-1}(v)| = |\text{Ker } A| = q^{\dim \text{Ker } A} = q^{m - \text{rank } A} = q^{m-1}.$$

Then, for $j \in \mathbb{F}_q \setminus \{0\}$, we have

$$\begin{aligned} b_{1,j} &= |A^{-1}({}^t[j\ ja^{-1}b])| + |A^{-1}({}^t[jb^{-1}a\ j])| = 2q^{m-1}, \\ b_{2,j} &= b_{3,j} = 0, \\ b_{0,j} &= |V| - (b_{1,j} + b_{2,j} + b_{3,j}) = q^m - 2q^{m-1} \end{aligned}$$

and

$$\begin{aligned} b_{1,0} &= (q-1)q^{m-1}, \\ b_{0,0} &= b_{2,0} = 0, \\ b_{3,0} &= |\text{Ker } A| = q^{m-1}. \end{aligned}$$

Thus, since $b_i = \sum_{j \in \mathbb{F}_q} b_{i,j}$, we obtain the desired results. □

Using these lemmas, we give a proof of Theorem 1.3.

Proof of Theorem 1.3 By Lemmas 2.4 and (2.1), (1) follows from Lemma 4.1, and (2) follows from Lemma 4.2. □

Then, we show that the shells of $RM_q(1, m)$ are not 3-designs if $q \geq 3$ and $m \geq 2$.

Proof of Corollary 1.4 Let $C = RM_q(1, m)$. We give a proof relying on the properties of Jacobi polynomials. Let $T_1 = \{0, u_1, u_2\} \in \binom{V}{3}$, $T_2 = \{0, v_1, v_2\} \in \binom{V}{3}$, $A_1 = {}^t[u_1\ u_2]$, and $A_2 = {}^t[v_1\ v_2]$. We assume that rank $A_1 = 2$ and rank $A_2 = 1$. Indeed, if $q \geq 3$ and $m \geq 2$, there exist such T_1, T_2. By Theorem 1.3,

$$J_{C,T_1} - J_{C,T_2} = -q^{m-2}(q-1)x^{q^{m-1}-3}y^{(q-1)q^{m-1}-3}(wy - xz)^3.$$

Since the coefficient of $z^3 x^{q^m - \ell} y^{\ell - 3}$ in $J_{C,T_1} - J_{C,T_2}$ is non-zero whenever C_ℓ is non-empty, C_ℓ is not a 3-design. □

By using Theorem 2.1, we obtain

$$J_{C^\perp,T_1} - J_{C^\perp,T_2} = (q-1)\{x + (q-1)y\}^{q^{m-1}-3}(x-y)^{(q-1)q^{m-1}-3}(wy - xz)^3.$$

Based on this equation, we conjecture the following.

Conjecture 4.3 *Let $C = RM_q(1, m)$. If $q \geq 3$, then for any $\ell \in \mathbb{N}$, $(C^\perp)_\ell$ is not a combinatorial 3-design.*

We verified this conjecture for q, m which satisfying $q^{2m} < 10^9$. The computations were performed using the code available at GitHub.[1]

Finally, we claim that the shells of $RM_q(1, m)$ are 3-$(v, k, (\lambda_1, \lambda_2))$-designs.

Proof of Corollary 1.5 It is clear from Theorem 1.3.

[1] https://github.com/yama821/GRMJacobi-paper.

5 Proof of Theorem 1.6

In this section, we give proofs of Theorem 1.6 and Corollary 1.7 using the notation introduced in Sect. 2.3. Let $T = \{0, u_1, u_2, u_3\} \in \binom{V}{4}$, $A = {}^t[u_1\ u_2\ u_3]$.

Considering A as a linear map from V to $\mathbb{F}_q^3$, for all $j \in \mathbb{F}_q \setminus \{0\}$, we have

$$\begin{aligned} b_{i,j} &= |\{c \in V \mid i \text{ elements of } Ac \text{ are equal to } j\}| \\ &= q^{m-\operatorname{rank} A} \times |\{v \in \operatorname{Im} A \mid i \text{ elements of } v \text{ are equal to } j\}|, \end{aligned} \tag{5.1}$$

and for $j = 0$, we have

$$\begin{aligned} b_{i,0} &= |\{c \in V \mid i-1 \text{ elements of } Ac \text{ are equal to } 0\}| \\ &= q^{m-\operatorname{rank} A} \times |\{v \in \operatorname{Im} A \mid i-1 \text{ elements of } v \text{ are equal to } 0\}|. \end{aligned} \tag{5.2}$$

Next, we prepare three lemmas for proving Theorem 1.6.

Lemma 5.1 *If* rank $A = 3$,

$$\begin{aligned} &a_0 = q^{m-3} - 1,\ a_1 = 4(q-1)q^{m-3},\ a_2 = 6(q-1)^2 q^{m-3}, \\ &a_3 = 4(q-1)^3 q^{m-3},\ a_4 = (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - q^{m-3} - 1). \end{aligned}$$

Proof By (5.1) and (5.2),

$$\begin{aligned} b_0 &= b_{0,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{0,j} = (q-1) \times (q-1)^3 \times q^{m-3} = (q-1)^4 q^{m-3}, \\ b_1 &= b_{1,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{1,j} = (q-1)^3 q^{m-3} + 3(q-1)^3 q^{m-3} = 4(q-1)^3 q^{m-3}, \\ b_2 &= b_{2,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{2,j} = 3(q-1)^2 q^{m-3} + 3(q-1)^2 q^{m-3} = 6(q-1)^2 q^{m-3}, \\ b_3 &= b_{3,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{3,j} = 3(q-1) q^{m-3} + (q-1) q^{m-3} = 4(q-1) q^{m-3}, \\ b_4 &= b_{4,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{4,j} = q^{m-3}. \end{aligned}$$

Therefore, we obtain the desired results by Lemma 2.4. □

Lemma 5.2 *If* rank $A = 1$,

$$\begin{aligned} &a_0 = q^{m-1} - 1,\ a_1 = 0,\ a_2 = 0, \\ &a_3 = 4(q-1)q^{m-1},\ a_4 = (q-1)(q^m - 3q^{m-1} - 1). \end{aligned}$$

Proof Since u_1, u_2, u_3 are different from each other and not equal to 0, we take a basis $\{{}^t[a\ b\ c]\}$ of Im A, where $a, b, c \in \mathbb{F}_q \backslash \{0\}$ and are different from each other. If rank $A = 1$, then for all $v \in \operatorname{Im} A$, $|A^{-1}(v)| = q^{m-1}$. Then, for all $j \in \mathbb{F}_q \backslash \{0\}$,

$$\begin{aligned} b_{1,j} &= 3 \times q^{m-1} = 3q^{m-1}, \\ b_{2,j} &= b_{3,j} = b_{4,j} = 0, \\ b_{0,j} &= q^m - (b_{1,j} + b_{2,j} + b_{3,j} + b_{4,j}) = q^m - 3q^{m-1} \end{aligned}$$

and

$$b_{1,0} = (q-1) \times q^{m-1},$$
$$b_{0,0} = b_{2,0} = b_{3,0} = 0,$$
$$b_{4,0} = q^{m-1}.$$

Therefore, $b_0, \dots, b_4$ are written as follows:

$$b_0 = b_{0,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{0,j} = (q-1) \times (q^m - 3q^{m-1}) = (q-1)(q-3)q^{m-1},$$
$$b_1 = b_{1,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{1,j} = (q-1)q^{m-1} + (q-1) \times 3q^{m-1} = 4(q-1)q^{m-1},$$
$$b_2 = b_{2,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{2,j} = 0,$$
$$b_3 = b_{3,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{3,j} = 0,$$
$$b_4 = b_{4,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{4,j} = q^{m-1}.$$

Thus, we obtain $a_0, \dots, a_4$ by using Lemma 2.4. □

Before stating the lemma under the condition of rank $A = 2$, we give a basis of Im A. Since Im A is invariant under the right multiplication of an invertible matrix to A, we confine a basis of Im A to the following:

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ a \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ b \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 1 \\ a \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\},$$

where $a, b \in \mathbb{F}_q$. However, since u_1, u_2, u_3 are not equal to 0, the last one is excluded. Without loss of generality, we take the first one because $b_{i,j}$ is invariant under a permutation on indices of codewords. Note that we have $(a, b) \neq (0, 0), (1, 0), (0, 1)$ because $u_1, u_2, u_3 \neq 0$.

Lemma 5.3 *If* rank $A = 2$, *we have the following.*

1. *If* $a + b = 1$ *or* $ab = 0$, *then*

$$a_0 = q^{m-2} - 1,\ a_1 = q^{m-2}(q-1),\ a_2 = 3q^{m-2}(q-1),$$
$$a_3 = q^{m-2}(q-1)(4q-5),\ a_4 = (q-1)(q^m - 3q^{m-1} + 2q^{m-2} - 1).$$

2. *If* $a + b \neq 1$ *and* $ab \neq 0$, *then*

$$a_0 = q^{m-2} - 1,\ a_1 = 0,\ a_2 = 6q^{m-2}(q-1),$$
$$a_3 = q^{m-2}(q-1)(4q-8),\ a_4 = (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - 1).$$

Proof First, we give b_0. Clearly, $b_{0,0} = 0$. For all $j \in \mathbb{F}_q \setminus \{0\}$,

$$b_{0,j} = q^{m-\text{rank } A} \times |\{v \in \text{Im } A \mid \text{ zero elements of } v \text{ are equal to } j\}|$$
$$= q^{m-2} \times |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq j,\ c_2 \neq j,\ c_1 a + c_2 b \neq j\}|.$$

We have

$$\begin{aligned}
&|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq j, c_2 \neq j, c_1a + c_2b \neq j\}| \\
&= (q-1)^2 - |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq j, c_2 \neq j, c_1a + c_2b = j\}| \\
&= (q-1)^2 - (|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1a + c_2b = j\}| \\
&\quad - |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 = j, c_1a + c_2b = j\}| \\
&\quad - |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_2 = j, c_1a + c_2b = j\}| \\
&\quad + |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 = j, c_2 = j, c_1a + c_2b = j\}|).
\end{aligned}$$

If $a = 0$, then $b \neq 0, 1$, and if $b = 0$, then $a \neq 0, 1$. Thus,

$$\begin{aligned}
|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1a + c_2b = j\}| &= q, \\
|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 = j, c_1a + c_2b = j\}| &= \begin{cases} 1 \text{ if } b \neq 0, \\ 0 \text{ if } b = 0, \end{cases} \\
|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_2 = j, c_1a + c_2b = j\}| &= \begin{cases} 1 \text{ if } a \neq 0, \\ 0 \text{ if } a = 0, \end{cases} \\
|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 = j, c_2 = j, c_1a + c_2b = j\}| &= \begin{cases} 1 \text{ if } a + b = 1, \\ 0 \text{ otherwise.} \end{cases}
\end{aligned}$$

Therefore,

$$\begin{aligned}
&|\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq j, c_2 \neq j, c_1a + c_2b \neq j\}| \\
&= \begin{cases} (q-1)^2 - (q-1) \text{ if } ab = 0 \text{ or } a + b = 1, \\ (q-1)^2 - (q-2) \text{ otherwise.} \end{cases}
\end{aligned}$$

Hence,

$$\begin{aligned}
b_0 &= b_{0,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{0,j} \\
&= \begin{cases} \sum_{j \in \mathbb{F}_q \setminus \{0\}} q^{m-2}(q-1)(q-2) \text{ if } a + b = 1 \text{ or } ab = 0 \\ \sum_{j \in \mathbb{F}_q \setminus \{0\}} q^{m-2}(q^2 - 3q + 3) \quad \text{otherwise} \end{cases} \\
&= \begin{cases} q^{m-2}(q-1)^2(q-2) & \text{if } a + b = 1 \text{ or } ab = 0, \\ q^{m-2}(q-1)(q^2 - 3q + 3) & \text{otherwise.} \end{cases}
\end{aligned}$$

Second, we compute b_1. Similarly,

$$b_{1,0} = \begin{cases} q^{m-2}(q-1)^2 & \text{if } ab = 0, \\ q^{m-2}(q-1)(q-2) & \text{otherwise.} \end{cases}$$

Fix $j \in \mathbb{F}_q \setminus \{0\}$, and let I_1, I_2, and I_3 be non-negative numbers such that

$$\begin{aligned}
I_1 &= |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 = j, c_2 \neq j, ac_1 + bc_2 \neq j\}|, \\
I_2 &= |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq j, c_2 = j, ac_1 + bc_2 \neq j\}|, \\
I_3 &= |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq j, c_2 \neq j, ac_1 + bc_2 = j\}|.
\end{aligned}$$

Then, $b_{1,j} = q^{m-2} \times (I_1 + I_2 + I_3)$. We have

$$I_1 = \begin{cases} q-1 \text{ if } b=0 \text{ or } a+b=1, \\ q-2 \text{ otherwise,} \end{cases}$$

$$I_2 = \begin{cases} q-1 \text{ if } a=0 \text{ or } a+b=1, \\ q-2 \text{ otherwise,} \end{cases}$$

$$I_3 = \begin{cases} q-1 \text{ if } ab=0 \text{ or } a+b=1, \\ q-2 \text{ otherwise,} \end{cases}$$

$$I_1 + I_2 + I_3 = \begin{cases} 3q-3 \text{ if } a+b=1, \\ 3q-4 \text{ if } ab=0, \\ 3q-6 \text{ otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned} b_1 &= b_{1,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{1,j} \\ &= \begin{cases} q^{m-2}(q-1)(q-2) + \sum_j q^{m-2}(3q-3) & \text{if } a+b=1, \\ q^{m-2}(q-1)^2 + \sum_j q^{m-2}(3q-4) & \text{if } ab=0, \\ q^{m-2}(q-1)(q-2) + \sum_j q^{m-2}(3q-6) & \text{otherwise,} \end{cases} \\ &= \begin{cases} q^{m-2}(q-1)(q-2) + (q-1)q^{m-2}(3q-3) & \text{if } a+b=1, \\ q^{m-2}(q-1)^2 + (q-1)q^{m-2}(3q-4) & \text{if } ab=0, \\ q^{m-2}(q-1)(q-2) + (q-1)q^{m-2}(3q-6) & \text{otherwise,} \end{cases} \\ &= \begin{cases} q^{m-2}(q-1)(4q-5) \text{ if } a+b=1 \text{ or } ab=0, \\ q^{m-2}(q-1)(4q-8) \text{ otherwise.} \end{cases} \end{aligned}$$

Similarly, we give b_3. For all $j \in \mathbb{F}_q \setminus \{0\}$, we have

$$b_{3,j} = \begin{cases} q^{m-2} & \text{if } a+b=1, \\ 0 & \text{otherwise.} \end{cases}$$

Let J_1, J_2, and J_3 be non-negative integers such that

$$\begin{aligned} J_1 &= |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 = 0, c_2 \neq 0, ac_1 + bc_2 \neq 0\}|, \\ J_2 &= |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq 0, c_2 = 0, ac_1 + bc_2 \neq 0\}|, \\ J_3 &= |\{(c_1, c_2) \in \mathbb{F}_q^2 \mid c_1 \neq 0, c_2 \neq 0, ac_1 + bc_2 = 0\}|. \end{aligned}$$

Clearly, $J_3 = 0$. We have

$$J_1 = \begin{cases} q-1 & \text{if } a=0, \\ 0 & \text{otherwise,} \end{cases}$$

$$J_2 = \begin{cases} q-1 & \text{if } b=0, \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$b_{3,0} = q^{m-2} \times (J_1 + J_2 + J_3) = \begin{cases} q-1 & \text{if } ab=0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$b_3 = b_{3,0} + \sum_{j \in \mathbb{F}_q \setminus \{0\}} b_{3,j}$$
$$= \begin{cases} q^{m-2}(q-1) & \text{if } a+b=1 \text{ or } ab=0, \\ 0 & \text{otherwise,} \end{cases}$$

and we have $b_{4,j} = 0$, where $j \in \mathbb{F}_q \setminus \{0\}$, and $b_{4,0} = |\mathrm{Ker}\, A| = q^{m-2}$. Then we have

$$b_4 = q^{m-2}.$$

Finally, by using Lemma 2.4, we obtain $a_0, \ldots, a_4$ as follows:

$$\begin{aligned}
a_0 &= b_4 - 1 \\
&= q^{m-2} - 1, \\
a_1 &= b_3 \\
&= \begin{cases} q^{m-2}(q-1) & \text{if } a+b=1 \text{ or } ab=0, \\ 0 & \text{otherwise,} \end{cases} \\
a_3 &= b_1 \\
&= \begin{cases} q^{m-2}(q-1)(4q-5) & \text{if } a+b=1 \text{ or } ab=0, \\ q^{m-2}(q-1)(4q-8) & \text{otherwise,} \end{cases} \\
a_4 &= b_0 - (q-1) \\
&= \begin{cases} q^{m-2}(q-1)^2(q-2) - (q-1) & \text{if } a+b=1 \text{ or } ab=0, \\ q^{m-2}(q-1)(q^2-3q+3) - (q-1) & \text{otherwise,} \end{cases} \\
&= \begin{cases} (q-1)(q^m - 3q^{m-1} + 2q^{m-2} - 1) & \text{if } a+b=1 \text{ or } ab=0, \\ (q-1)(q^m - 3q^{m-1} + 3q^{m-2} - 1) & \text{otherwise,} \end{cases} \\
a_2 &= |C \setminus \mathbb{F}_q \mathbf{1}| - (a_0 + a_1 + a_3 + a_4) \\
&= q^{m+1} - q - (a_0 + a_1 + a_3 + a_4) \\
&= \begin{cases} 3q^{m-2}(q-1) & \text{if } a+b=1 \text{ or } ab=0, \\ 6q^{m-2}(q-1) & \text{otherwise.} \end{cases}
\end{aligned}$$

□

Proof of Theorem 1.6 and Corollary 1.7 Using Lemmas 5.1, 5.2, and 5.3, we obtain the desired results. □

Acknowledgements The authors would like to thank the anonymous reviewers for their beneficial comments on an earlier version of the manuscript. We are grateful to Professors Tsuyoshi Miezaki and Akihiro Munemasa for helpful discussions and comments on the manuscript.

Declarations

Conflict of interest The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript.

References

1. Assmus E.F. Jr., Mattson H.F. Jr.: New 5-designs. J. Comb. Theory **6**, 122–151 (1969).
2. Berger T., Charpin P.: The automorphism group of generalized Reed–Muller codes. Discret. Math. **117**, 1–17 (1993).
3. Bonnecaze A., Mourrain B., Solé P.: Jacobi polynomials, type II codes, and designs. Des. Codes Cryptogr. **16**(3), 215–234 (1999).
4. Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997).
5. Chakraborty H.S., Miezaki T., Oura M., Tanaka Y.: Jacobi polynomials and design theory I. Discret. Math. **346**, 113339 (2023).
6. Miezaki T., Munemasa A.: Jacobi polnomials and harmonic weight enumerators of the first-order Reed-Muller codes and the extended hamming codes, submitted (2023).
7. Miezaki T., Nakasora H.: The support designs of the triply even binary codes of length 48. J. Comb. Des. **27**, 673–681 (2019).
8. Miezaki T., Munemasa A., Nakasora H.: A note on Assmus-Mattson type theorems. Des. Codes Cryptogr. **89**, 843–858 (2021).
9. Ozeki M.: On the notion of Jacobi polynomials for codes. Math. Proc. Camb. Philos. Soc. **121**(1), 15–30 (1997).
10. Wolfram Research, Inc., Mathematica, Version 11.2, Champaign, IL (2017).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.