6th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November. 17-18, 2021

On the weight distribution of generalized Reed-Muller codes

Somayyeh Golalizadeh[1]
Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University, Tehran, Iran.

Nasrin Soltankhah
Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University, Tehran, Iran.

Abstract

In this paper, we study on the weight distribution of generalized Reed-Muller codes. We will characterize the fourth weight of generalized Reed-Muller code $R_q(b,m)$ for $3 \leq b < \frac{q+4}{3}$.

Keywords: Generalized Reed-Muller codes, Fourth weight codewords, Affine subspace, Affine hyperplane.
Mathematics Subject Classification [2010]: 13D45, 39B42

1 Introduction

Let F_q be the finite field with q elements and $m \geq 1$ an integer. Let r be an integer such that $1 \leq r < m(q-1)$. The generalized Reed-Muller code of order r is the following subspace of the space $F_q^{q^m}$

$$R_q(r,m) = \Big\{(f(x))_{x \in F_q^m} | f \in F_q[X_1, \cdots, X_m] \ and \ \ deg(f) \leq r\Big\}$$

Two most important problems in generalized Reed-Muller code problems are determination of the weight distribution of generalized Reed-Muller codes and obtaining first minimum weights and corresponding codewords.

The minimum weight was given by Kasami et al. in [5]. It has been proved that the minimal weight of the generalized Reed-Muller code $R_q(r,m)$ is $(q-b)q^{m-a-1}$ where $r = a(q-1)+b$ and $0 \leq b < q-1$. The codewords reaching this bound were discribed by Delsarte et al. in [2] (see also [9]). The second weight problem of generalized Reed-Muller codes was studied by Geil using Gröbner basis in [3] for $r < q$ and $r > (m-1)(q-1)$ and it was almost completely solved by Rolland in [12]. Second weight codewords have been studied in [1, 13] and finally completely described in [7]. Leducq in [8] got a full description of the third weight and the third weight codewords of generalized Reed-Muller codes of order $r = a(q-1)+b$ for $3 \leq b < \frac{q+4}{3}$.

The weight distribution of $R_q(2,m)$ was given by McEliece in [11] for any q and due to some mistakes in the computation, Li in [10] provided a precise account for the weight distribution of second order generalized Reed-Muller codes. For $q = 2$, for all m and all r, the weight distribution is known in the range $[W_1, 2.5W_1]$ by a result of Kasami et al [6]. In this paper, we want to determine the fourth weight of generalized Reed-Muller codes. The main result of this article is characerization the fourth weight of $R_q(b,m)$, for $3 \leq b < \frac{q+4}{3}$

Throughout this article, we write $r = a(q-1)+b$, $0 \leq a \leq m-1$, $1 \leq b \leq q-1$ and by W_i we denote the ith minimum weight of $R_q(r,m)$.

[1] speaker

2 Preliminaries

2.1 Notation and preliminary remark

Let $f \in F_m^q$, $\lambda \in Fq$. We define $f_\lambda \in F_{m-1}^q$ by

$$\forall x = (x_2, ..., x_m) \in F_q^{m-1}, f_\lambda(x) = f(\lambda, x_2..., x_m)$$

. Let $0 \leq r \leq (m-1)(q-1)$ and $f \in R_q(r, m)$. We denote by S the support of f . Consider H an affine hyperplane in F_q^m, by an affine transformation, we can assume $x_1 = 0$ is an equation of H. Then $S \cap H$ is the support of $f_0 \in R_q(r, m-1)$ or the support of $(1 - x_1^{q-1})f \in R_q(r + (q-1), m)$.

2.2 Useful lemmas

The following lemmas are proved in [4]

Lemma 2.1. *Let $m \geq 1$, $q \geq 2$, $f \in B_m^q$ and $w \in F_q$. If for all $(x_2, \cdots, x_m)$ in F_q^{m-1}, $f(w, x_2, \cdots, x_m) = 0$, then for all $(x_1, x_2, \cdots, x_m) \in F_q^m$,*

$$f(x_1, \cdots, x_m) = (x_1 - w)g(x_1, \cdots, x_m)$$

with $deg_{x_1}(g) \leq deg_{x_1}(f) - 1$ and $deg(g) \leq deg(f) - 1$.

Lemma 2.2. *Let $m \geq 2$, $q \geq 3$, $0 \leq r \leq m(q-1)$. If $f \in R_q(r, m)$, $f \neq 0$ and there exists $y \in R_q(1, m)$ and $(\lambda_i)_{1 \leq i \leq n}$ n elements in F_q such that the hyperplanes of equation $y = \lambda_i$ do not meet the support of f, then*

$$|f| \geq (q-b)q^{m-a-1} + \begin{cases} n(b-n)q^{m-a-2} & \text{if} n < b, \\ (n-b)(q-1-n)q^{m-a-1} & \text{if} n \geq b. \end{cases}$$

where $r = a(q-1) + b$, $1 \leq b \leq q-1$.

Lemma 2.3. *If $f \in R_q(r, m)$ with $r \leq q-1$ and $|f| < (1 + \frac{1}{q})d_r^m$, then f is the product of r linear factors.*

Lemma 2.4. *Let $m \geq 2$, $q \geq 3$, $1 \leq b \leq q-1$. Assume $f \in R_q(b, m)$ is such that f depends only on x_1 and $g \in R_q(b-k, m)$, $1 \leq k \leq b$. Then either $f + g$ depends only on x_1 or $|f + g| \geq (q - b + k)q^{m-1}$.*

Lemma 2.5. *Let $m \geq 2$, $q \geq 3$, $1 \leq a \leq m-1$, $1 \leq b \leq q-2$. Assume $f \in R_q(a(q-1)+b, m)$ is such that $\forall x = (x_1, \cdots, x_m) \in F_q^m$,*

$$f(x) = (1 - x_1^{q-1})\widetilde{f}(x_2, \cdots, x_m)$$

and $g \in R_q(a(q-1) + b - k, m)$, $1 \leq k \leq q-1$, is such that $(1 - x_1^{q-1})$ does not divide g. Then either $|f + g| \geq (q - b + k)q^{m-a-1}$ or $k = 1$.

Lemma 2.6. *Let $m \geq 2$, $q \geq 3$, $1 \leq a \leq m-2$, $1 \leq b \leq q-2$ and $f \in R_q(a(q-1)+b, m)$. We set an order on the elements of F_q such that $|f_{\lambda_1}| \leq \cdots \leq |f_{\lambda_q}|$.*
If f has no linear factor and there exists $k \geq 1$ such that $(1 - x_2^{q-1})$ divides f_{λ_i} for $i \leq k$ but $(1 - x_2^{q-1})$ does not divide $f_{\lambda_{k+1}}$ then,

$$|f| \geq (q-b)q^{m-a-1} + k(q-k)q^{m-a-2}$$

Lemma 2.7. *Let $m \geq 2$, $q \geq 3$, $1 \leq a \leq m$ and $f \in R_q(a(q-1), m)$ such that $|f| = q^{m-a}$ and $g \in R_q(a(q-1) - k, m)$, $1 \leq k \leq q-1$, such that $g \neq 0$. Then, either $|f + g| = kq^{m-a}$ or $|f + g| \geq (k+1)q^{m-a}$.*

Lemma 2.8. *Let $m \geq 2$, $q \geq 3$, $1 \leq a \leq m-1$ and $f \in R_q(a(q-1), m)$. If for some $u, v \in F_q$, $|f_u| = |f_v| = q^{m-a-1}$, then there exists T an affine transformation fixing x_1 such that*

$$(f \circ T)_u = (f \circ T)_v$$

The following results can be found in [8].

Theorem 2.9. *Let $m \geq 2$, $q \geq 9$, $0 \leq a \leq m-2$ and $4 \leq b < \frac{q+4}{3}$. The third weight of $R_q(a(q-1)+b, m)$ is $W_3 = (q-2)(q-b+2)q^{m-a-2}$.*

Theorem 2.10. *Let $m \geq 3$, $q \geq 7$ and $0 \leq a \leq m-3$. The third weight of $R_q(a(q-1)+3, m)$ is $W_3 = (q-1)^3 q^{m-a-3}$.*

Theorem 2.11. *For $q \geq 7$, $m \geq 2$, $0 \leq a \leq m-2$, $4 \leq b < \frac{q+4}{3}$, up to affine transformation, the third weight codewords of $R_q(a(q-1)+b, m)$ are of the form:*

$$f(x) = \prod_{i=1}^{a}(1 - x_i^{q-1})g(x_{a+1}, x_{a+2}) \qquad \forall x = (x_1, \cdots, x_m) \in F_q^m$$

where $g \in R_q(b, 2)$ is such that $|g| = (q-2)(q-b+2)$.

Theorem 2.12. *For $q \geq 7$, $m \geq 3$, $0 \leq a \leq m-3$, up to affine transformation, the third weight codewords of $R_q(a(q-1)+3, m)$ are of the form:*

$$f(x) = \prod_{i=1}^{a}(1 - x_i^{q-1})x_{a+1}x_{a+2}x_{a+3} \qquad \forall x = (x_1, \cdots, x_m) \in F_q^m.$$

3 Main results

Lemma 3.1. *Let $f \in R_q(b, m)$ be the product of b linear factors. By an affine transformation suppose that $x_1 - \lambda_i$ for $i = 1, \cdots, k$ are of the linear factors. If for some $j_0 \notin \{1, \cdots, k\}$, $|f_{\lambda_{j_0}}| = (q-b+k)q^{m-2}$ then, for all $j \notin \{1, \cdots, k\}$, there is an integer t where $0 \leq t \leq b-k-1$ such that $|f_{\lambda_j}| = (q-b+k+t)q^{m-2}$.*

Proof. We denote by H_{λ_i} the hyperplane with the equation $x_1 = \lambda_i$ for $i = 1, \cdots, q$. Assume that S denotes the support of f. By the assumption of the lemma, S does not meet the hyperplanes H_{λ_i} for $i = 1, \cdots, k$. Denote by $H^{(i)}$ $i = 1, \cdots, b-k$ the other hyperplanes which do not meet S. Since for some $j_0 \notin \{1, \cdots, k\}$, $|f_{\lambda_{j_0}}| = (q-b+k)q^{m-2}$ then, $f_{\lambda_{j_0}}$ is a minimum weight codeword of $R_q(b-k, m-1)$. So $H_{\lambda_{j_0}} \cap H^{(i)} = P^{(i)}$ is an affine subspace of codimension 2 where $P^{(i)} \cap P^{(i')} = \emptyset$ for $i \neq i'$. We get that for each two hyperplanes $H^{(s)}$ and $H^{(s')}$, $H^{(s)} \cap H^{(s')}$ is either empty or an affine subspace of codimension 2 which is included in one of the hyperplanes H_{λ_i} for $i = 1, \cdots, q$. Denote by P^{ij} the affine subspace of codimension 2 $H_{\lambda_i} \cap H^{(j)}$ for $k+1 \leq i \leq q$ and $1 \leq j \leq b-k$ in which for $j \neq j'$, $P^{ij} \cap P^{ij'} = \emptyset$ or $P^{ij} = P^{ij'}$. So we get that $|f_{\lambda_i}| = q^{m-1} - (b-k-t)q^{m-2}$ in which $b-k-t$ is the number of distinct subspaces P^{ij} which is included in H_{λ_i}. □

Lemma 3.2. *Let $m \geq 3$, $q \geq 9$, $4 \leq b < \frac{q+4}{3}$ and $f \in R_q(b, m)$. If $|f| > (q-2)(q-b+2)q^{m-2}$, then $|f| \geq (q-1)^2(q-b+2)q^{m-3}$.*

Proof. Let $f \in R_q(b, m)$ such that $|f| > (q-2)(q-b+2)q^{m-2}$. Assume $|f| < (q-1)^2(q-b+2)q^{m-3}$. Since

$$(q-1)^2(q-b+2)q^{m-3} \leq (1 + \frac{1}{q})d_b^m = (1 + \frac{1}{q})(q-b)q^{m-1} \tag{1}$$

for $b < \frac{q+4}{3}$, by Lemma 2.3 f is the product of b linear factors. For $y \in R_q(1, m)$, denote by n the number of distinct $\lambda \in F_q$ such that $y - \lambda$ divides f. Since $n \leq b$ by Lemma 2.2

$$(q-b)q^{m-1} + n(b-n)q^{m-2} < (q-1)^2(q-b+2)q^{m-3}$$

we get that $n \in \{1, 2, b-2, b-1, b\}$.
By applying an affine transformation we can assume that $x_1 = \lambda_1$, $\lambda_1 \in F_q$ is one of the linear factors.
If $n = b$, then for all $x = (x_1, \cdots, x_m) \in F_q^m$, we have

$$f(x) = \alpha \prod_{i=1}^{b}(x_1 - \lambda_i)$$

with $\lambda_i \in F_q$, $\lambda_i \neq \lambda_j$ for $i \neq j$. In this case f is a minimum weight codeword of $R_q(b,m)$ which is absurd.
If $n = b-1$, then for all $x = (x_1, \cdots, x_m) \in F_q^m$, we have

$$f(x) = \prod_{i=1}^{b-1}(x_1 - \lambda_i)g(x)$$

with $\lambda_i \in F_q$, $\lambda_i \neq \lambda_j$ for $i \neq j$ and $g \in R_q(1,m)$. If $deg(g) = 0$, then f is a minimum weight codeword of $R_q(b-1,m)$. If $deg(g) = 1$, then f is a second minimum weight codeword of $R_q(b,m)$. Both cases give us a contradiction, since $(q-2)(q-b+2)q^{m-2} < |f| < (q-1)^2(q-b+2)q^{m-3}$.
If $n = b-2$, then for all $x = (x_1, \cdots, x_m) \in F_q^m$, we have

$$f(x) = \prod_{i=1}^{b-2}(x_1 - \lambda_i)g(x)$$

with $\lambda_i \in F_q$, $\lambda_i \neq \lambda_j$ for $i \neq j$ and $g \in R_q(2,m)$. If $deg(g) = 0$, then f is a minimum weight codeword of $R_q(b-2,m)$. If $deg(g) = 1$, then f is a second minimum weight codeword of $R_q(b-1,m)$. Both cases give a contradiction. So $deg(g) = 2$. For all $i \geq b-1$, $f_{\lambda_i} \in R_q(2, m-1)$ and $|f_{\lambda_i}| = |g_{\lambda_i}| \geq (q-2)q^{m-2}$. Denote by $N := \#\{i \geq b-1; |f_{\lambda_i}| = (q-2)q^{m-2}\}$. For $\lambda \in F_q$, if $|f_\lambda| > (q-2)q^{m-2}$, then $|f_\lambda| \geq (q-1)^2q^{m-3}$. Since $|f| < (q-1)^2(q-b+2)q^{m-3}$, we get that $N \geq 1$. So by Lemma 3.1 we conclude that for all $i \geq b-1$, $|f_{\lambda_i}| = (q-2)q^{m-2}$ or $|f_{\lambda_i}| = (q-1)q^{m-2}$. From

$$N(q-2)q^{m-2} + (q-b+2-N)(q-1)q^{m-2} < (q-1)^2(q-b+2)q^{m-3}$$

we get that $N = q-b+2$ that gives a third minimum weight codeword of $R_q(b,m)$ which is absurd.
If $n = 2$, then for all $x = (x_1, \cdots, x_m) \in F_q^m$, we have

$$f(x) = (x_1 - \lambda_1)(x_1 - \lambda_2)g(x)$$

with $\lambda_1, \lambda_2 \in F_q$, $\lambda_1 \neq \lambda_2$ and $g \in R_q(b-2,m)$. Then for all $i \geq 3$, $f_{\lambda_i} \in R_q(b-2, m-1)$ and $|f_{\lambda_i}| = |g_{\lambda_i}| \geq (q-b+2)q^{m-2}$. Denote by $N := \#\{i \geq 3; |f_{\lambda_i}| = (q-b+2)q^{m-2}\}$. For $\lambda \in F_q$, if $|f_\lambda| > (q-b+2)q^{m-2}$, then $|f_\lambda| \geq (q-1)(q-b+3)q^{m-3}$. Since

$$(q-2)(q-1)(q-b+3)q^{m-3} > (q-1)^2(q-b+2)q^{m-3}$$

we get that $N \geq 1$. So by Lemma 3.1 for all $i \geq 3$, $|f_{\lambda_i}| = (q-b+t)q^{m-2}$ where $2 \leq t \leq b-1$. Therefore we have

$$\begin{aligned} |f| &\geq N(q-b+2)q^{m-2} + (q-2-N)(q-b+3)q^{m-2} \\ &= \Big(q(q-2)(q-b+3) - Nq\Big)q^{m-3}. \end{aligned}$$

By considering $|f| < (q-1)^2(q-b+2)q^{m-3}$, we get that $N = q-2$ that gives a third minimum weight codeword of $R_q(b,m)$ which is absurd.
From now, assume $n = 1$. Then for all $x = (x_1, \cdots, x_m) \in F_q^m$, we have

$$f(x) = (x_1 - \lambda_1)g(x)$$

with $\lambda_1 \in F_q$ and $g \in R_q(b-1,m)$. Then for all $i \geq 2$, $f_{\lambda_i} \in R_q(b-1, m-1)$ and $|f_{\lambda_i}| = |g_{\lambda_i}| \geq (q-b+1)q^{m-2}$. Denote by $N := \#\{i \geq 2; |f_{\lambda_i}| = (q-b+1)q^{m-2}\}$. For $\lambda \in F_q$, if $|f_\lambda| > (q-b+1)q^{m-2}$, then $|f_\lambda| \geq (q-1)(q-b+2)q^{m-3}$. Since

$$(q-1)(q-1)(q-b+2)q^{m-3} \geq (q-1)^2(q-b+2)q^{m-3}$$

we get that $N \geq 1$. Assume H_0 is the hyperplane with the equation $x_1 = \lambda_1$. Let $\mathcal{H} = \{H_1, \cdots, H_{b-1}\}$ be the set of $(b-1)$ other hyperplanes which do not meet S. Denote by A the affine subspace of codimension

2 which is included in both of H_0 and H_1. Let $\mathcal{A} = \{H_i; i \geq 1, H_i \cap H_0 = A\}$. Since $n = 1$ and $N \geq 1$, for each pair $(H, H') \in \mathcal{A} \times (\mathcal{H} - \mathcal{A})$, $H \cap H'$ is an affine subspace of codimension 2 which is included in one of $H^{(i)}$ (the hyperplane with the equation $x_1 = \lambda_i$) for $2 \leq i \leq q$. Then we have

$$|f| \geq (q-1)(q-b+1)q^{m-2} + \#\mathcal{A}(b-1-\#\mathcal{A})q^{m-2}.$$

By considering $|f| < (q-1)^2(q-b+2)q^{m-3}$, we get that $|\mathcal{A}| = b-1$ that gives a second minimum weight codeword of $R_q(b,m)$ which is absurd. □

Lemma 3.3. *Let $q \geq 4$, $m \geq 3$. If $f \in R_q(3,m)$ and $|f| > (q-1)^3 q^{m-3}$ then, $|f| \geq ((q-1)^3+1)q^{m-3}$.*

Proof. We prove this lemma by induction on m. The case where $m = 3$ is an immediate result. Suppose that for some $m \geq 4$, if $f \in R_q(3, m-1)$ is such that $|f| > (q-1)^3 q^{m-4}$ then $|f| \geq ((q-1)^3+1)q^{m-4}$.
Let $f \in R_q(3,m)$ such that $|f| > (q-1)^3 q^{m-3}$. Assume $|f| < ((q-1)^3+1)q^{m-3}$. Denote by S the support of f.
Assume S meets all affine hyperplanes. Then for all H hyperplanes $\#(S \cap H) \geq (q-3)q^{m-2}$. Suppose that there exists H_1 such that $\#(S \cap H_1) = (q-3)q^{m-2}$. By applying an affine transformation, we can assume $x_1 = \alpha$ is an equation of H_1. Set an order on the elements of F_q such that $|f_{\lambda_1}| \leq \cdots \leq |f_{\lambda_q}|$. Then f_{λ_1} is a minimum weight codeword of $R_q(3, m-1)$. By applying an affine transformation, we can assume f_{λ_1} depends only on x_2. Let $k \geq 1$ be such that f_{λ_i} depends only on x_2 for all $i \leq k$ but $f_{\lambda_{k+1}}$ does not depend only on x_2. If $k > 3$, we can write for all $x = (x_1, \cdots, x_m) \in F_q^m$

$$f(x) = \sum_{i=0}^{3} f^{(i)}_{\lambda_{i+1}}(x_2, \cdots, x_m) \prod_{1 \leq j \leq i} (x_1 - \lambda_j)$$

Since for $i \leq 4$, f_{λ_i} depends only on x_2, then f depends only on x_1, x_2, Then $|f| \equiv 0 \pmod{q^{m-2}}$. Since $|f| > (q-1)^3 q^{m-3}$, then $|f| \geq ((q-1)^3+1)q^{m-3}$ which is absurd. So $k \leq 3$. Since $f_{\lambda_1}, \cdots, f_{\lambda_k}$ depend only on x_2, we can write for all $x_1, x_2 \in F_q$ and $\widehat{x} \in F_q^{m-2}$

$$f(x_1, x_2, \widehat{x}) = g(x_1, x_2) + \prod_{i=1}^{k} (x_1 - \lambda_i) h(x_1, x_2, \widehat{x})$$

where $deg(h) \leq 3 - k$. Then

$$f_{\lambda_{k+1}}(x_2, \widehat{x}) = g_{\lambda_{k+1}}(x_2) + \alpha h_{\lambda_{k+1}}(x_2, \widehat{x})$$

where $\alpha \in F_q^*$. So by Lemma 2.4 since $f_{\lambda_{k+1}}$ does not depend only on x_2, $|f_{\lambda_{k+1}}| \geq (q-3+k)q^{m-2}$. So

$$|f| \geq k(q-3)q^{m-2} + (q-k)(q-3+k)q^{m-2} = (q-3)q^{m-1} + k(q-k)q^{m-2}.$$

By considering $|f| < ((q-1)^3+1)q^{m-3}$, we get a contradiction.

So for all H hyperplane, $\#(S \cap H) \geq (q-1)(q-2)q^{m-3}$. By induction hypothesis, considering q parallel hyperplanes there esists a hyperplane H_0 such that $\#(S \cap H_0) = (q-1)(q-2)q^{m-3}$ or $\#(S \cap H_0) = (q-1)^3 q^{m-4}$. In both cases, we get that there exists A an affine subspace of codimension 2 included in H_0 which does not meet S. Considering all hyperplanes through A, since for all H hyperplanes, $\#(S \cap H) \geq (q-1)(q-2)q^{m-3}$, we get

$$(q+1)(q-1)(q-2)q^{m-3} < ((q-1)^3+1)q^{m-3}.$$

and this is absurd. So there exists an affine hyperplane H_1 which does not meet S. Denote by n the number of hyperplanes parallel to H_1 which do not meet S.

By applying an affine transformation, we can assume $x_1 = \lambda_1$ is an equation of H_1. We have $n \leq 3$.

If $n = 3$, then for all $x = (x_1, \cdots, x_m) \in F_q^m$ we can write

$$f(x) = (x_1 - \lambda_1)(x_1 - \lambda_2)(x_1 - \lambda_3)g(x)$$

where $\lambda_i \in F_q$, $\lambda_i \neq \lambda_j$ for all $i \neq j$, $deg(g) = 0$. So $|f| = (q-3)q^{m-1}$ that gives a minimum weight codeword of $R_q(3, m)$ which is absurd.

If $n = 2$, then for all $x = (x_1, \cdots, x_m) \in F_q^m$ we can write

$$f(x) = (x_1 - \lambda_1)(x_1 - \lambda_2)g(x)$$

where $\lambda_i \in F_q$, $\lambda_1 \neq \lambda_2$, $deg(g) \leq 1$. If $deg(g) = 0$, $|f| = (q-2)q^{m-1}$. If $deg(g) = 1$, $|f| = (q-2)(q-1)q^{m-2}$. We get a contradiction in both cases.

From now, assume $n = 1$. Then for all $x = (x_1, \cdots, x_m) \in F_q^m$ we have

$$f(x) = (x_1 - \lambda_1)g(x)$$

where $deg(g) \leq 2$. Then for $i \geq 2$, $deg(f_{\lambda_i}) \leq 2$ and so either $|f_{\lambda_i}| = (q-2)q^{m-2}$ or $|f_{\lambda_i}| = (q-1)^2q^{m-3}$ or $|f_{\lambda_i}| \geq (q^2 - q - 1)q^{m-3}$. Since

$$(q-1)(q^2 - q - 1)q^{m-3} \geq ((q-1)^3 + 1)q^{m-3},$$

is a contradiction, there exists $i \geq 2$ such that $|f_{\lambda_i}| = (q-2)q^{m-2}$ or $|f_{\lambda_i}| = (q-1)^2q^{m-3}$. Denote by H' a hyperplane such that $\#(S \cap H') = (q-2)q^{m-2}$ ($\#(S \cap H') = (q-1)^2q^{m-3}$). Then there exist P_1 and P_2 two parallel affine subspaces of codimension 2 (two affine subspaces of codimension 2 intersect in an affine subspace of codimension 3) included in H' not in S. Consider P an affine subspace of codimension 2 included in H' which intersect P_1 and P_2 (in two different subspace of codimension 3). Then $\#(S \cap P) = (q-2)q^{m-3}$. Then for all H hyperplane through P, $\#(S \cap H) \geq (q-1)(q-2)q^{m-3}$. We can apply the same argument to all affine subspaces of codimension 2 included in H' parallel to P. Now, consider a hyperplane through P and the $q-1$ parallel hyperplanes to this hyperplane. Since $|f| < ((q-1)^3+1)q^{m-3}$, by induction hypothesis one of these hyperplanes say H'' meets S either in $(q-2)(q-1)q^{m-3}$ or $(q-1)^3q^{m-4}$ points.

Denote by $(A_i)_{1 \leq i \leq 3}$ the 3 affine subspaces of codimension 2 included in H'' which do not meet S. Suppose that S meets all hyperplanes through A_i and consider H one of them. If all hyperplanes parallel to H meet S then as in the beginning of the proof of this lemma, we get that $\#(S \cap H) \geq (q-1)(q-2)q^{m-3}$. If there exists a hyperplane parallel to H which does not meet S then $\#(S \cap H) \geq (q-2)q^{m-2}$. In all cases we get a contradiction since $(q+1)(q-1)(q-2)q^{m-3} \geq ((q-1)^3 + 1)q^{m-3}$.

Then there exist three hyperplanes H_1 (with the equation $x_1 = \lambda_1$), H_2 and H_3 which do not meet S. Since $n = 1$, the intersection of H_2 and H_3 is an affine subspace of codimension 2 say $A_{2,3}$. There are three following cases:
If $A_{2,3}$ is contained in the hyperplane H_1, then for all $i \geq 2$ $|f_{\lambda_i}| = (q-2)q^{m-2}$. So $|f| = (q-1)(q-2)q^{m-2}$ which is absurd.
If $A_{2,3}$ is contained in one of the hyperplanes $x_1 = \lambda_j$ for $j \geq 2$, then $|f_{\lambda_j}| = (q-1)q^{m-2}$ and $|f_{\lambda_i}| = (q-2)q^{m-2}$ for $i \geq 2$ and $i \neq j$. So

$$\begin{aligned} |f| &= (q-2)(q-2)q^{m-2} + (q-1)q^{m-2} \\ &= (q^2 - 3q + 3)q^{m-2} \\ &= ((q-1)^3 + 1)q^{m-3}, \end{aligned}$$

we get a contradiction, since $|f| < ((q-1)^3 + 1)q^{m-3}$.
If $A_{2,3}$ meets the hyperplane $x_1 = \lambda_i$ in an affine subspace P_i of codimension 3 for all i, then $|f_{\lambda_i}| = (q-1)^2q^{m-3}$. So $|f| = (q-1)(q-1)^2q^{m-3} = (q-1)^3q^{m-3}$ which is absurd. □

Theorem 3.4. *Let $m \geq 3$, $q \geq 9$ and $4 \leq b < \frac{q+4}{3}$. The fourth weight of $R_q(b, m)$ is $W_4 = (q-1)^2(q-b+2)q^{m-3}$.*

Proof. By Lemma 3.2 we have $W_4 \geq (q-1)^2(q-b+2)q^{m-3}$. Define

$$g(x_1, x_2, x_3) = \prod_{i=1}^{b-2}(x_1 - \lambda_i)(x_2 - \alpha)(x_3 - \beta)$$

Then $g \in R_q(b, 3)$ and $|g| = (q-1)^2(q-b+2)$. For $x = (x_1, \cdots, x_m) \in F_q^m$, we define

$$f(x) = g(x_1, x_2, x_3).$$

Then $f \in R_q(b, m)$ and $|f| = |g|q^{m-3}$ which completes the proof. □

Theorem 3.5. *Let $m \geq 3$, $q \geq 7$. The fourth weight of $R_q(3, m)$ is $W_4 = ((q-1)^3 + 1)q^{m-3}$.*

Proof. By Lemmas 3.3 we have

$$W_4 \geq ((q-1)^3 + 1)q^{m-3}$$

For $x = (x_1, \cdots, x_m) \in F_q^m$, we define

$$f(x) = (x_1 - c)(x_2 - d)(\alpha x_1 + \beta x_2 - e)$$

with $c, d, e \in F_q$, $\alpha, \beta \in F_q^*$ and $e \neq \alpha c + \beta d$. Then, $f \in R_q(3, m)$ and $|f| = ((q-1)^3 + 1)q^{m-3}$ which proves $W_4 = ((q-1)^3 + 1)q^{m-3}$. □

References

[1] J.P. Cherdieu, R. Rolland, *On the number of points of some hypersurfaces in F_q^n*, Finite Fields Appl., **2(2)**(1996), 214–224.

[2] P. Delsarte , J.M. Goethals , F.J. MacWilliams, *On generalized Reed-Muller codes and their relatives*, Inf. Control., **16**(1970), 403–442.

[3] O. Geil, *On the second weight of generalized Reed–Muller codes*, Des. Codes Cryptogr., **48(3)**(2008), 323-330.

[4] D. Erickson, M. California *Institute of Technology. Division of Physics, Astronomy, Counting Zeros of Polynomials Over Finite Fields (CIT thesis)*, California Institute of Technology., (1974).

[5] T. Kasami, S. Lin, W. W. Peterson, *New generalizations of the Reed-Muller codes*, I. Primitive codes. IEEE Trans. Inf. Theory., **14**(1968), 189–199.

[6] T. Kasami, N. Tokura, S. Azumi, *On the Weight Enumeration of Weights Less than* $2.5d$ *of Reed-Muller Codes*, Faculty of Engineering Science, Osaka University, Osaka Japan (1974).

[7] E. Leducq, *Second weight codewords of generalized Reed–Muller codes*, Cryptogr. Commun., **5(4)**(2013), 241–276.

[8] E. Leducq, *On the third weight of generalized Reed–Muller codes*, Discrete Math., **338**(2015), 1515–1535.

[9] E. Leducq, *A new proof of Delsarte, Goethals and Mac Williams theorem on minimal weight codewords of generalized Reed–Muller codes*, Finite Fields Appl., **18(3)**(2012), 581–586.

[10] S. Li, *On the weight distribution of second order Reed–Muller codes and their relatives*, Des. Codes Cryptogr., **87**(2019), 2447–2460.

[11] R. McEliece, *Quadratic Forms over Finite Fields and Second-order Reed-Muller Codes*, JPL Space Programs Summary. Trans. Inf. Theory., **III**(1969), 37–58.

[12] R. Rolland, *The second weight of generalized Reed-Muller codes in most cases*, Cryptogr. Commun., **2(1)**(2010), 19–40.

[13] A. Sboui, *Second highest number of points of hypersurfaces in* F_q^n, Finite Fields Appl., **13(3)**(2007), 444–449.

Email: s.golalizade@alzahra.ac.ir
Email: soltan@alzahra.ac.ir