On the second and third minimum weights of projective Reed-Muller codes

Mrinmoy Datta

Department of Mathematics Indian Institute of Technology Hyderabad Hyderabad, India

mrinmoy.datta@math.iith.ac.in



Notations:

The following notations will be used throughout the presentation.

- $\mathbb{A}^k(\mathbb{F}_q)$ = affine space of dimension k over \mathbb{F}_q .
- $\mathbb{P}^k(\mathbb{F}_q)$ = projective space of dimension k over \mathbb{F}_q .
- For $k \geq 0$, we define $p_k := |\mathbb{P}^k(\mathbb{F}_q)| = 1 + q + \cdots + q^k$.
- A k-dimensional linear subspace C of \mathbb{F}_q^n is called an $[n,k]_q$ linear code. The parameter n is called the length of the C. An element of a code C is called a codeword.
- For an element $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_q^n$, (expressed in terms of the usual basis of \mathbb{F}_q^n), we define the Hamming weight of \mathbf{a} , denoted by $\mathrm{wt}(\mathbf{a})$, as follows:

$$wt(\mathbf{a}) := \#\{i : a_i \neq 0\}.$$

Reed-Muller Codes

Throughout, m and d are positive integers with $d \le q - 1$.

Definition: Reed-Muller codes Let $n = q^m$. We define an evaluation map

$$\operatorname{ev}:R_{\leq d}\to \mathbb{F}_q^n$$
 given by $f\mapsto (f(P_1),\ldots,f(P_n)),$

where P_1, \ldots, P_n are a fixed enumeration of all the points in $\mathbb{A}^m(\mathbb{F}_q)$. Note that $R_{\leq d}$ is a vector space over \mathbb{F}_q and the map ev is an \mathbb{F}_q -linear transformation. We define the Reed-Muller code, denoted by $\mathrm{RM}(d,m)$, as

$$RM(d,m) = ev(R_{\leq d}).$$

We also note that the evaluation map is injective, thanks to the underlying hypothesis $d \le q - 1$. It follows that RM(d, m) is a linear code of

- length $n = q^m$,
- dimension $\binom{m+d}{d}$.

Projective Reed-Muller Codes

Definition: Projective Reed-Muller Codes As before, we fix positive integers m and d. Let $N=p_m$. Each point of $\mathbb{P}^m(\mathbb{F}_q)$ admits a unique representative in \mathbb{F}_q^{m+1} in which the first nonzero coordinate is 1. Let P_1,\ldots,P_N be an ordered listing of such representatives in \mathbb{F}_q^{m+1} of points of $\mathbb{P}^m(\mathbb{F}_q)$. The Projective Reed-Muller code of order d and length N, denoted by $\mathrm{PRM}(d,m)$, is defined by the image of the Evaluation map,

$$\text{Ev}: S_d \to \mathbb{F}_q^N$$
 given by $F \mapsto (F(P_1), \dots, F(P_N)).$

That is,

$$PRM(d, m) := \{(F(P_1), \dots, F(P_N)) : F \in S_d\}.$$

As in the case of Reed-Muller codes, the Evaluation map is an \mathbb{F}_q -linear transformation. Moreover, it is injective, thanks to the assumption that $d \leq q-1$. Thus PRM(d,m) is a linear code of

- length $N = p_m$,
- dimension $\binom{m+d}{d}$.

Hamming weights of codewords and \mathbb{F}_q -rational points on Hypersurfaces

Note that an codeword of RM(d, m) is uniquely given by ev(f) for some $f \in R_{\leq d}$, where

$$\operatorname{ev}(f) = (f(P_1), \dots, f(P_n)).$$

Thus, the Hamming weight of (ev(f)) is given by

$$wt(ev(f)) = |\{P \in \mathbb{A}^m(\mathbb{F}_q) : f(P) \neq 0\}| = q^m - |Z(f)|,$$

where Z(f) is the set of zeroes of f in $\mathbb{A}^m(\mathbb{F}_q)$. In particular, the determination of the minimum weight of $\mathrm{RM}(d,m)$ is equivalent to the determination of the maximum number of \mathbb{F}_q -rational zeroes of a polynomial in $R_{\leq d}$ of degree at most d.

- In algebro-geometric terminology, we see that the determination of the minimum weight of $\mathrm{RM}(d,m)$ is equivalent to the determination of the maximum number of \mathbb{F}_q -rational points on an affine hypersurface in \mathbb{A}^m of degree d defined over \mathbb{F}_q .
- Similarly, the determination of the minimum weight of PRM(d, m) is equivalent to the determination of the maximum number of \mathbb{F}_q -rational points on an projective hypersurface in \mathbb{P}^m of degree d defined over \mathbb{F}_q .

Minimum weight of (projective) Reed-Muller codes and the main question

As mentioned, we fix positive integers m, d with $d \le q - 1$.

- (Ore's Inequality) If $f \in R_{\leq d}$, and $f \neq 0$, then $|Z(f)| \leq dq^{m-1}$.
- (Serre's Inequality) If $f \in S_d$, and $F \neq 0$, then $|V(F)| \leq dq^{m-1} + p_{m-2}$.

Thus, the minimum weight of RM(d, m) and PRM(d, m), denoted by d(RM(d, m)) and d(PRM(d, m)) respectively, are given by

$$d(RM(d,m)) = q^m - dq^{m-1}$$
 and $d(PRM(d,m)) = p_m - dq^{m-1} - p_{m-2}$.

Minimum weight of (projective) Reed-Muller codes and the main question

As mentioned, we fix positive integers m, d with $d \le q - 1$.

- (Ore's Inequality) If $f \in R_{\leq d}$, and $f \neq 0$, then $|Z(f)| \leq dq^{m-1}$.
- (Serre's Inequality) If $f \in S_d$, and $F \neq 0$, then $|V(F)| \leq dq^{m-1} + p_{m-2}$.

Thus, the minimum weight of RM(d, m) and PRM(d, m), denoted by d(RM(d, m)) and d(PRM(d, m)) respectively, are given by

$$d(RM(d,m)) = q^m - dq^{m-1}$$
 and $d(PRM(d,m)) = p_m - dq^{m-1} - p_{m-2}$.

Question: Determine the weight distributions of RM(d, m) and PRM(d, m).

Broader goal

To complete the following "frequency tables":

Reed-Muller codes

w	$\mathcal{X}\subset\mathbb{A}^m$ affine hypersurface of degree $d,$ $ \mathcal{X}(\mathbb{F}_q) =w$
dq^{m-1}	Union of d parallel hyperplanes in \mathbb{A}^m each defined over \mathbb{F}_q
?	?

Projective Reed-Muller codes

w	$\mathcal{X}\subset\mathbb{P}^m$ projective hypersurface of degree $d,$ $ \mathcal{X}(\mathbb{F}_q) =w$		
$dq^{m-1} + p_{m-2}$	Union of d hyperplanes in \mathbb{P}^m each defined over \mathbb{F}_q , contain-		
	ing a codimension 2 linear subspace in common		
?	?		

Broader goal

To complete the following "frequency tables":

Reed-Muller codes

w	$\mathcal{X}\subset \mathbb{A}^m$ affine hypersurface of degree $d,$ $ \mathcal{X}(\mathbb{F}_q) =w$
dq^{m-1}	Union of d parallel hyperplanes in \mathbb{A}^m each defined over \mathbb{F}_q
?	?

Projective Reed-Muller codes

w	$\mathcal{X} \subset \mathbb{P}^m$ projective hypersurface of degree $d, \mathcal{X}(\mathbb{F}_q) = w$		
$dq^{m-1} + p_{m-2}$	Union of d hyperplanes in \mathbb{P}^m each defined over \mathbb{F}_q , contain-		
	ing a codimension 2 linear subspace in common		
?	?		

Remarks: These problems are easy when either m=1 or d=1. On the other hand, when d=2, the tables can be completed using the well-known classification of quadrics over finite fields. We will thus assume from now on that $m \ge 2$ and $d \ge 3$.

Second minimum weight of Reed-Muller codes

- **●** (Cherdieu and Rolland, 1996) If $f \in R_{\leq d}$ is given by a product of d linear polynomials defined over \mathbb{F}_q and $|Z(f)| < dq^{m-1}$, then $|Z(f)| \leq dq^{m-1} (d-1)q^{m-2}$. Moreover, if $|Z(f)| = dq^{m-1} (d-1)q^{m-2}$ and f is a product of d linear polynomials defined over \mathbb{F}_q , then Z(f) is given by one of the following configurations:
 - (a) **Type I:** Z(f) is a union of d affine hyperplanes passing through a common codimension 2 affine subspace in \mathbb{A}^m , or
 - (b) Type II: Z(f) is a union of d − 1 parallel hyperplanes and another hyperplane intersecting each of the d − 1 hyperplanes at distinct codimension 2 affine subspaces.

Second minimum weight of Reed-Muller codes

- ① (Cherdieu and Rolland, 1996) If $f \in R_{\leq d}$ is given by a product of d linear polynomials defined over \mathbb{F}_q and $|Z(f)| < dq^{m-1}$, then $|Z(f)| \leq dq^{m-1} (d-1)q^{m-2}$. Moreover, if $|Z(f)| = dq^{m-1} (d-1)q^{m-2}$ and f is a product of d linear polynomials defined over \mathbb{F}_q , then Z(f) is given by one of the following configurations:
 - (a) **Type I:** Z(f) is a union of d affine hyperplanes passing through a common codimension 2 affine subspace in \mathbb{A}^m , or
 - (b) **Type II:** Z(f) is a union of d-1 parallel hyperplanes and another hyperplane intersecting each of the d-1 hyperplanes at distinct codimension 2 affine subspaces.
- ② (Geil, 2008) If $f \in R_{\leq d}$ and $|Z(f)| < dq^{m-1}$, then $|Z(f)| \leq dq^{m-1} (d-1)q^{m-2}$.

Second minimum weight of Reed-Muller codes

- ① (Cherdieu and Rolland, 1996) If $f \in R_{\leq d}$ is given by a product of d linear polynomials defined over \mathbb{F}_q and $|Z(f)| < dq^{m-1}$, then $|Z(f)| \leq dq^{m-1} (d-1)q^{m-2}$. Moreover, if $|Z(f)| = dq^{m-1} (d-1)q^{m-2}$ and f is a product of d linear polynomials defined over \mathbb{F}_q , then Z(f) is given by one of the following configurations:
 - (a) Type I: Z(f) is a union of d affine hyperplanes passing through a common codimension 2 affine subspace in A^m, or
 - (b) **Type II:** Z(f) is a union of d-1 parallel hyperplanes and another hyperplane intersecting each of the d-1 hyperplanes at distinct codimension 2 affine subspaces.
- ② (Geil, 2008) If $f \in R_{\leq d}$ and $|Z(f)| < dq^{m-1}$, then $|Z(f)| \leq dq^{m-1} (d-1)q^{m-2}$.
- **③** (Leducq, 2012) If $q \ge 3$ and $f \in R_{\le d}$ with $|Z(f)| = dq^{m-1} (d-1)q^{m-2}$, then f is a product of d linear polynomials defined over \mathbb{F}_q .

Summary

Reed-Muller codes

w	$\mathcal{X}\subset\mathbb{A}^m$ affine hypersurface of degree $d, \mathcal{X}(\mathbb{F}_q) =w$
dq^{m-1}	Union of d parallel hyperplanes in \mathbb{A}^m each defined over
	\mathbb{F}_q
$dq^{m-1} - (d-1)q^{m-2}$	Type I or Type II
?	?

Question: Determine $N_2 = \max\{|V(F)| : F \in S_d, |V(F)| < dq^{m-1} + p_{m-2}\}$. As mentioned, we will assume that $m \ge 2$ and $d \ge 3$.

Question: Determine $N_2 = \max\{|V(F)| : F \in S_d, |V(F)| < dq^{m-1} + p_{m-2}\}$. As mentioned, we will assume that $m \ge 2$ and $d \ge 3$.

Known results:

- Rodier and Sboui, (2008) If $d \leq \frac{q}{2} + 1$, then $N_2 = dq^{m-1} + p_{m-2} (d-2)q^{m-2}$.
- Rodier and Sboui, (2008) If m = 2 and q is a prime, then $N_2 = dq d + 3$.

Question: Determine $N_2 = \max\{|V(F)| : F \in S_d, |V(F)| < dq^{m-1} + p_{m-2}\}$. As mentioned, we will assume that $m \ge 2$ and $d \ge 3$.

Known results:

- Rodier and Sboui, (2008) If $d \leq \frac{q}{2} + 1$, then $N_2 = dq^{m-1} + p_{m-2} (d-2)q^{m-2}$.
- Rodier and Sboui, (2008) If m = 2 and q is a prime, then $N_2 = dq d + 3$.

Basic inequality: Suppose $F \in S_d$ containing at least one linear polynomial defined over \mathbb{F}_q as a linear factor defined over \mathbb{F}_q , and $|V(F)| < dq^{m-1} + p_{m-2}$, then

$$|V(F)| \le dq^{m-1} + p_{m-2} - (d-1)q^{m-2}.$$

The equality is attained by V(F) if and only if V(F) contains a hyperplane Π and $V(F)\setminus \Pi$ is an affine hypersurface of degree d-1 with

$$|V(F) \setminus \Pi| = (d-1)q^{m-1} - (d-2)q^{m-2}.$$

Question: Determine $N_2 = \max\{|V(F)| : F \in S_d, |V(F)| < dq^{m-1} + p_{m-2}\}$. As mentioned, we will assume that $m \ge 2$ and $d \ge 3$.

Known results:

- Rodier and Sboui, (2008) If $d \leq \frac{q}{2} + 1$, then $N_2 = dq^{m-1} + p_{m-2} (d-2)q^{m-2}$.
- Rodier and Sboui, (2008) If m = 2 and q is a prime, then $N_2 = dq d + 3$.

Basic inequality: Suppose $F \in S_d$ containing at least one linear polynomial defined over \mathbb{F}_q as a linear factor defined over \mathbb{F}_q , and $|V(F)| < dq^{m-1} + p_{m-2}$, then

$$|V(F)| \le dq^{m-1} + p_{m-2} - (d-1)q^{m-2}.$$

The equality is attained by V(F) if and only if V(F) contains a hyperplane Π and $V(F)\setminus \Pi$ is an affine hypersurface of degree d-1 with

$$|V(F) \setminus \Pi| = (d-1)q^{m-1} - (d-2)q^{m-2}.$$

Question: What happens when F does not contain any linear factor defined over \mathbb{F}_q ?

Homma-Kim elementary bound

(Homma-Kim elementary bound, 2012) If $X \subset \mathbb{P}^m$ is a projective hypersurface of degree $d \leq q+1$ not containing any \mathbb{F}_q -linear component, then

$$|\mathcal{X}(\mathbb{F}_q)| \le (d-1)q^{m-1} + dq^{m-2} + p_{m-3}.$$

Remark: This bound was also obtained by Carvalho and Neumann, although in a different avatar, in 2016.

Now, a direct comparison shows that

$$(d-1)q^{m-1} + dq^{m-2} + p_{m-3} < dq^{m-1} + p_{m-2} - (d-2)q^{m-2} \iff d < \frac{q+3}{2}.$$

(Carvalho and Neumann, 2018) If $d \leq \frac{q+2}{2}$, then $N_2 = dq^{m-1} + p_{m-2} - (d-2)q^{m-2}$.

Remark: Combining everything above and the result by Leducq, we can get the geometric structure of V(F) where $|V(F)|=dq^{m-1}+p_{m-2}-(d-2)q^{m-2}$ in the case when $d\leq \frac{q+1}{2}$.

An elementary improvement of Homma-Kim elementary bound

(Homma-Kim elementary bound, 2012) If $X \subset \mathbb{P}^m$ is a projective hypersurface of degree $d \leq q+1$ not containing any \mathbb{F}_q -linear component, then

$$|\mathcal{X}(\mathbb{F}_q)| \le (d-1)q^{m-1} + dq^{m-2} + p_{m-3}.$$

(Tironi, 2017) Let $\mathcal{X} \subset \mathbb{P}^m$ be a projective hypersurface of degree $d \leq q+1$, not containing any \mathbb{F}_q -linear component, and $|\mathcal{X}(\mathbb{F}_q)| = (d-1)q^{m-1} + dq^{m-2} + p_{m-3}$, then $d=2, \sqrt{q}+1$ (in this case q must be a perfect square) or q+1.

An elementary improvement of Homma-Kim elementary bound

(Homma-Kim elementary bound, 2012) If $X \subset \mathbb{P}^m$ is a projective hypersurface of degree $d \leq q+1$ not containing any \mathbb{F}_q -linear component, then

$$|\mathcal{X}(\mathbb{F}_q)| \le (d-1)q^{m-1} + dq^{m-2} + p_{m-3}.$$

(Tironi, 2017) Let $\mathcal{X} \subset \mathbb{P}^m$ be a projective hypersurface of degree $d \leq q+1$, not containing any \mathbb{F}_q -linear component, and $|\mathcal{X}(\mathbb{F}_q)| = (d-1)q^{m-1} + dq^{m-2} + p_{m-3}$, then $d=2, \sqrt{q}+1$ (in this case q must be a perfect square) or q+1.

(Datta, 2024) If $d \neq 2, \sqrt{q} + 1$, and $\mathcal{X} \subset \mathbb{P}^m$ is a projective hypersurface of degree $d \leq q$ not containing any \mathbb{F}_q -linear component, then

$$|\mathcal{X}(\mathbb{F}_q)| \le (d-1)q^{m-1} + dq^{m-2} + p_{m-3} - (d-2)q^{m-3}.$$

Remark: With the new bound mentioned above, and observing that $\sqrt{q}+1<\frac{q+3}{2}$, now we can show that for $d\leq \frac{q+3}{2}$, we have $N_2=dq^{m-1}+p_{m-2}-(d-2)q^{m-2}$ and obtain the geometric classification of all hypersurfaces of degree $\leq \frac{q+3}{2}$ achieving N_2 .

Unfortunately, nothing more about N_2 is known when m > 3 yet!!

The case m=2

From now on, let $\mathcal{C} \subset \mathbb{P}^2$ denote a plane curve of degree $d \leq q$ defined over \mathbb{F}_q .

- **⑤** Serre's inequality shows that $|\mathcal{C}(\mathbb{F}_q)| \leq dq + 1$.
- ② Previously mentioned results on N_2 show that if $d \leq \frac{q+3}{2}$ and $|\mathcal{C}(\mathbb{F}_q)| < dq + 1$, then

$$|\mathcal{C}(\mathbb{F}_q)| \le dq - d + 3.$$

We can also classify the curves of degree *d* attaining the bound.

1 The basic inequality shows that if $\mathcal C$ contains a line defined over $\mathbb F_q$, then $|\mathcal C(\mathbb F_q)| \leq dq - d + 3$.

What can we say about plane curves that do not contain a line defined over \mathbb{F}_q ?

Homma-Kim-Sziklai bound

(Conjecture, P. Sziklai, 2008) Let $\mathcal{C} \subset \mathbb{P}^2$ be a plane curve of degree $d \leq q+1$ not containing any lines defined over \mathbb{F}_q . Then $|\mathcal{C}(\mathbb{F}_q)| \leq (d-1)q+1$.

(Homma-Kim, 2009-10) The conjecture is true, except when d=q=4. Moreover, when d=q=4, then up to projective equivalence, there is exactly one curve $\mathcal C$ for which the conjecture is false.

The bound is known to be attained in the following cases:

- 0 d = 2: hyperbolic quadric
- ② q is a square and $d=\sqrt{q}+1$: nonsingular Hermitian curve (in this case, Hermitian curves are the only curves attaining this bound, which is known thanks to (Hirschfeld, Storme, Thas and Voloch, 1991)

$$\alpha X^{q-1} + \beta Y^{q-1} + \gamma Z^{q-1} = 0,$$

where $\alpha, \beta, \gamma \in \mathbb{F}_q^{\times}$, and $\alpha + \beta + \gamma = 0$. This classification was obtained by Ferreira and Speziali in 2023.

 $\mathbf{Q} \quad d = q, q + 1$. Some examples are known.

Back to N_2 when m=2

Note that (d-1)q+1 < dq-d+3, whenever $d \le q+1$.

(Datta, 2024) For m=2, and $d \leq q$, we have $N_2=dq-d+3$. Moreover, if $\mathcal C$ is a plane curve of degree d defined over $\mathbb F_q$ such that $|\mathcal C(\mathbb F_q)|=dq-d+3$, then $\mathcal C$ is a union of d distinct lines, say ℓ_1,\ldots,ℓ_d satisfying the following condition:

 $\ell_1, \dots, \ell_{d-1}$ intersect at a common point P and ℓ_d intersect each of $\ell_1, \dots, \ell_{d-1}$ at a point different from P.

N_3 : One more step

Question: Determine $N_3 = \max\{|\mathcal{C}(\mathbb{F}_q)| : \mathcal{C} \text{ a plane curve}, \ \deg \mathcal{C} = d, |\mathcal{C}(\mathbb{F}_q)| < dq - d + 3\}.$ Known results:

- Sboui, 2009 If $\mathcal C$ is a union of d distinct lines and $|\mathcal C(\mathbb F_q)| < dq d + 3$, then $|\mathcal C(\mathbb F_q)| \le dq + 1 2(d-3)$.
- Sboui, 2009 For $d \le \frac{q}{3} + 2$, we have $N_3 = dq + 1 2(d 3)$.
- Rodier and Sboui, 2008 If q is a prime and 2 < d < q 2, then $N_3 = dq + 1 2(d 3)$.

Remark: The last result is wrong. Note that the curve $\mathcal C$ defined over $\mathbb F_q$, given by a union of d-1 lines passing through a common point, with one of the lines repeated twice, has degree d and satisfies $|\mathcal C(\mathbb F_q)|=(d-1)q+1$.

But one can easily check that

$$dq + 1 - 2(d - 3) < (d - 1)q + 1 < dq - d + 3,$$

the first inequality holds when $d>rac{q+6}{2}$ and, as observed before, the second one is always true.

Theorem (Datta, 2024)

For $5 \le d \le q-1$ and m=2, we have

$$N_3 = \begin{cases} dq + 1 - 2(d-3) & \text{if } d \leq \frac{q+5}{2} \\ \leq (d-1)q + 2 & \text{if } d \geq \frac{q+6}{2}. \end{cases}$$

Remarks:

- In fact, we proved that for $d \ge \frac{q+6}{2}$, we have $N_3 = (d-1)q + 1$ or (d-1)q + 2.
- A classification of degree curves d attaining the bound is still open. For example, let $\mathcal C$ be a curve of degree d. Write $\mathcal C = \mathcal L \cup \mathcal N$, where $\mathcal L$ consists of the union of all lines defined over $\mathbb F_q$ contained in $\mathcal C$, and $\mathcal N$ is the "line-free" part of $\mathcal C$. Suppose $\deg \mathcal N = s$. Then $|\mathcal C(\mathbb F_q)| = (d-1)q + 2$ if and only if
 - \triangleright \mathcal{L} is a union of d-s lines passing through a common point,
 - $|\mathcal{N}(\mathbb{F}_q)| = (s-1)q + 1$, and
 - $(\mathcal{L} \cap \mathcal{N})(\mathbb{F}_a) = \emptyset$
- Datta, 2024 When q = p or p^2 , where p is a prime, and $\frac{q+6}{2} \le d \le q-1$, then $N_3 = (d-1)q+1$.

Open Questions:

- **1** Determination for N_2 for $m \ge 3$.
- ② Determination of N_3 for $m \ge 2$.

Our approach essentially suggests investigations on the following questions:

- lacktriangle Classify all the plane curves not containing a line defined over \mathbb{F}_q that attain the Homma-Kim-Sziklai bound.
- ② Find the best possible upper bounds on the number of possible \mathbb{F}_q -rational points on absolutely irreducible hypersurfaces of degree d defined over \mathbb{F}_q .

These problems are known to be very difficult problems.

Thank you for your attention!