Covering Radius of Melas Codes

Minjia Shi, Tor Helleseth, Ferruh Özbudak, Patrick Solé

Covering Radius of Melas Codes

Minjia Shi & Tor Helleseth & Ferruh Özbudak & Patrick Solé

***Abstract*—We prove that the covering radius of the Melas code $M(m,q)$ of length $n=q^m-1$ over $\mathbb{F}_q$ is 2 if $q>3$. We also prove that the covering radius of $M(m,3)$ is 3 is $m\geq 3$, the covering radius of $M(2,3)$ is 4, and the covering radii of $M(1,2)$ and $M(1,3)$ are 1.**

***Index Terms*—Melas code, covering radius, finite fields.**

I. Introduction

THE covering radius of a code is one of the fundamental properties of codes (see, for example, [6]). It has applications in data compression, testing, write-once memories, decoding of errors and erasures. It is also interesting for its own sake [2], [3], [4], and [5].

Let $\mathbb{F}_q$ be a finite field with q elements. Let n be a positive integer. Let $C\subseteq\mathbb{F}_q^n$ be a q-ary code of length n. The covering radius of C is the maximum distance of any vector $x\in\mathbb{F}_q^n$ to the code C. Here the distance of $x\in\mathbb{F}_q^n$ to C is $d(x,C)=\min\{w_H(x-c):c\in C\}$, where $w_H(\cdot)$ is the Hamming weight. Equivalently the covering radius of C is the smallest integer r such that the Hamming balls of radius r centered at the codewords of C cover $\mathbb{F}_q^n$, namely

$$\mathbb{F}_q^n\subseteq\bigcup_{c\in C}B(c;r),$$

where $B(c;r)=\left\{x\in\mathbb{F}_q^n:w_H(x-c)\leq r\right\}$.

The problem of finding the covering radius of a given code is very hard in general [8]. In general, most of the results give bounds on the covering radii rather than exact values [1], [11], [17], [18], [21]. There are only a few classes of codes in which the covering radii are known [8], [9].

For an integer $m\geq 1$, there exists a finite field $\mathbb{F}_{q^m}$ with q^m elements such that $\mathbb{F}_{q^m}$ is a field extension of degree m over $\mathbb{F}_q$. Moreover the multiplicative group of $\mathbb{F}_{q^m}$ has q^m-1 elements and this group is cyclic. A generator of this cyclic group is called a primitive element of order q^m-1. We refer, for example, to [13], for further background in finite fields.

The Melas codes were introduced by C. M. Melas [14]. Let α be a primitive element of order $n=q^m-1$. The Melas code $M(m,q)$ of length $n=q^m-1$ over $\mathbb{F}_q$ has parity check matrix

$$H=\begin{bmatrix}1 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-2}\\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(q^m-2)}\end{bmatrix}. \quad (1)$$

Here the representation of the parity check matrix is in short. In fact we choose an arbitrary $\mathbb{F}_q$-linear bijective map $\phi:\mathbb{F}_{q^m}^{2\times 1}\to\mathbb{F}_q^{2m\times 1}$ and we consider each column $\begin{bmatrix}\alpha^j\\ \alpha^{-j}\end{bmatrix}$ in H as $\phi\left(\begin{bmatrix}\alpha^j\\ \alpha^{-j}\end{bmatrix}\right)$ for $0\leq j\leq q^{m-2}$. Therefore $M(m,q)$ has dimension $n-2m$ except the degenerate cases that $M(1,2)$ and $M(1,3)$. In these degenerate cases the dimensions are 0 and 1, respectively.

It is well known that the covering radius $\rho(m,q)$ of the Melas code $M(m,q)$ can also be defined as follows: Let $H_1,H_2,\ldots,H_n\in\mathbb{F}_{q^m}^{2\times 1}$ be the column vectors of H in (1). The covering radius $\rho(m,q)$ is the smallest integer ρ such that every column vector in $\mathbb{F}_{q^m}^{2\times 1}$ is a linear combination of at most ρ of $H_1,H_2,\ldots,H_n$ (see, for example, [3, Theorem 2.1.9] for $q=2$, and [11, Lemma 1.1] for q arbitrary).

In [7, Theorem 2] (see also [16]), the covering radius of $M(m,2)$ is shown to be 3 if $m\geq 2$. Let

This research is supported by the National Natural Science Foundation of China (12071001), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20) and the Research Council of Norway under grant (247742/O70).

Minjia Shi is with Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China (e-mail: smjwcl.good@163.com)

Tor Helleseth is with Department of Informatics, University of Bergen, Bergen, Norway (e-mail: tor.helleseth@uib.no)

Ferruh Özbudak is with Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey (e-mail: ozbudak@metu.edu.tr)

Patrick Solé is with I2M, Aix Marseille Univ., Centrale Marseille, CNRS, Marseille, France (e-mail: sole@enst.fr)

p be an odd prime. In [22], the covering radius of $M(m,p)$ is shown to be at most 3 if $p^m > 36$ using methods from [17]. In the main result of [12], the authors stated that the covering radius of $M(m,q)$ is 3 if $\mathbb{F}_q$ is a finite field of characteristic 2, where $q > 8$. Unfortunately, in this paper we show that this statement of [12] is wrong.

In this paper we exactly determine the covering radii of Melas codes complementing all of the cases after [7, Theorem 2], i.e. all positive integers m and all finite fields $\mathbb{F}_q$. In particular we develop new techniques very different from the ones in [17]. We use rather different methods in the even and odd characteristics. We present a simple and beautiful proof in the case of even characteristic. The case of odd characteristic is much more involved. We first give a characterization result (see Theorem II.1 and Remark II.2). This gives a connection of the covering radius of $M(m,q)$ to evaluations over $\mathbb{F}_{q^m}$ of certain quadratic polynomials over $\mathbb{F}_q$ and quadratic residues in $\mathbb{F}_{q^m}$, when the characteristic is odd and $q > 3$. Then we develop further techniques involving detailed structure of some subsets of $\mathbb{F}_{q^m}$ related to certain quadratic polynomials over $\mathbb{F}_q$ and quadratic residues in $\mathbb{F}_{q^m}$. Our proofs for the remaining case $M(m,3)$ use some results on elliptic curves and Hasse-Weil inequality.

This paper is organized as follows. Section II gives an important characterization result for the odd characteristic, except $q = 3$. We obtain the covering radius of all Melas codes in even characteristic in Section III, except $q = 2$. The case of Melas codes over $\mathbb{F}_3$ requires different methods, which we present in Section IV. Using our characterization in Theorem II.1 and Remark II.2, we first complete the covering radius of all Melas codes over $\mathbb{F}_5$ using new methods in Section V. These methods do not generalize directly to all finite fields with $q > 5$. In particular we need some stronger results than the covering radius is 2 when $m = 1$ and $q > 5$. This is accomplished in Section VI. Using results of earlier sections we complete the covering radius problem for all Melas codes $M(m,q)$ with $m \geq 1$ and $q > 5$ in Section VII. Section 8 concludes the paper.

Throughout the paper the multiplicative group of $\mathbb{F}_q$ (resp. $\mathbb{F}_q^m$) is denoted as $\mathbb{F}_q^*$ (resp. $\mathbb{F}_{q^m}^*$).

II. A CHARACTERIZATION OF THE COVERING RADIUS IN ODD CHARACTERISTIC

In this section we give a necessary and sufficient condition that the covering radius is 2 if the characteristic of the field $\mathbb{F}_q$ is odd and $q > 3$. In Sections V and VII, using this characterization, we show that the covering radius is 2 if the characteristic of the field $\mathbb{F}_q$ is odd and $q > 3$. Note that this characterization gives a link of the covering radius of these codes to the solutions of certain quadratic polynomials over finite fields. Throughout this section we assume that $\mathbb{F}_q$ is a finite field of odd characteristic.

Recall that $A \in \mathbb{F}_q$ is a square if there exists $a \in \mathbb{F}_q$ such that $A = a^2$. Note that $A = 0$ is a square and hence the number of squares in $\mathbb{F}_q$ is exactly $(q+1)/2$. Similarly $z \in \mathbb{F}_{q^m}$ is a square if there exists $y \in \mathbb{F}_{q^m}$ such that $z = y^2$.

Theorem II.1. *Assume that* $\operatorname{char} \mathbb{F}_q$ *is odd and* $q > 3$*. Let* $m \geq 1$ *be an integer. Then the covering radius of* $M(m,q)$ *is* 2 *if and only if the following condition holds:*

$$\begin{array}{l}\textit{For each } z \in \mathbb{F}_{q^m} \setminus \{c^2 : c \in \mathbb{F}_q\}\textit{, there}\\ \textit{exist squares } A, B \textit{ in } \mathbb{F}_q \textit{ with } A \neq B \textit{ and}\\ (z-A)(z-B) \textit{ is a square in } \mathbb{F}_{q^m}.\end{array} \quad (2)$$

Proof: We need to show that given $\alpha, \beta \in \mathbb{F}_{q^m}$ there exist $x, y \in \mathbb{F}_{q^m}^*$ with $x \neq y$ and $a, b \in \mathbb{F}_q$ such that the system

$$\begin{array}{rcl} ax + by & = & \alpha, \\ a\dfrac{1}{x} + b\dfrac{1}{y} & = & \beta \end{array} \quad (3)$$

holds. If $(\alpha, \beta) = (0,0)$, then we can choose $a = b = 0$ and $x, y \in \mathbb{F}_{q^m}^*$ arbitrarily with $x \neq y$. Hence we assume that $(\alpha, \beta) \neq (0,0)$ from now on in this proof.

If $\alpha = 0$ and $\beta \neq 0$, then let $a, b \in \mathbb{F}_q^*$ with $a^2 \neq b^2$. Note that this is possible as $q > 3$. Moreover, put

$$x = \frac{a^2 - b^2}{a\beta} \text{ and } y = \frac{-a}{b}x.$$

Note that $x \neq y$, $x, y \in \mathbb{F}_{q^m}^*$ and the system in (3) is satisfied by these choices. Hence the covering radius statement is satisfied in this case as well.

If $\alpha \neq 0$ and $\beta = 0$, then the covering radius statement is satisfied by symmetry using the arguments of the previous paragraph.

Next we consider the case that $\alpha \neq 0$, $\beta \neq 0$ and $\alpha\beta$ is a square in $\mathbb{F}_q$ (hence $\alpha\beta \in \mathbb{F}_q$ in particular). We choose $a \in \mathbb{F}_q$ with $a^2 = \alpha\beta$. Put

$$x = \frac{\alpha}{a} \text{ and } b = 0.$$

By choosing $y \in \mathbb{F}_{q^m}^*$ anything with $x \neq y$ we observe that the system in (3) is satisfied by these choices. Hence the covering radius statement is satisfied in this case.

From now on we assume that $\alpha \neq 0$, $\beta \neq 0$ and $\alpha\beta \neq c^2$ for any $c \in \mathbb{F}_q$ in this proof. Note that if there exist $a, b \in \mathbb{F}_q$, $x, y \in \mathbb{F}_{q^m}^*$ such that the system in (3) holds, then the following holds:

- $a \neq 0$, $b \neq 0$ and $x \neq y$: Otherwise $\alpha\beta$ is a square in $\mathbb{F}_q$, which is a contradiction to the assumption above.

Assume that there exist $a, b \in \mathbb{F}_q$, $x, y \in \mathbb{F}_{q^m}^*$ such that the system in (3) holds. This implies that

$$y = \frac{-ax}{b} + \frac{\alpha}{b}.$$

Putting this value into the system (3) we obtain

$$x^2 + x\left(\frac{b^2}{a\beta} - \frac{\alpha}{a} - \frac{a}{\beta}\right) + \frac{\alpha}{\beta} = 0. \tag{4}$$

Note that $x \neq 0$ as $\alpha/\beta \neq 0$. As the characteristic is odd the equation in (4) is equivalent to

$$\left(x + \frac{1}{2}\left(\frac{b^2}{a\beta} - \frac{\alpha}{a} - \frac{a}{\beta}\right)\right)^2 = \frac{1}{4}\left(\left(\frac{b^2}{a\beta} - \frac{\alpha}{a} - \frac{a}{\beta}\right)^2 - 4\frac{\alpha}{\beta}\right). \tag{5}$$

Considering the right hand side of (5) we conclude that $x \in \mathbb{F}_{q^m}^*$ if and only if

$$\left(b^2 - \alpha\beta - a^2\right)^2 - 4\alpha\beta a^2$$

is a square in $\mathbb{F}_{q^m}$. Put $z = \alpha\beta \in \mathbb{F}_{q^m} \setminus \{c^2 : c \in \mathbb{F}_q\}$. Hence $x \in \mathbb{F}_{q^m}^*$ if and only if

$$(b^2 - z - a^2)^2 - 4za^2$$

is a square in $\mathbb{F}_{q^m}^*$. We observe that

$$\left(b^2 - z - a^2\right)^2 - 4za^2 = \left(z - (a-b)^2\right)\left(z - (a+b)^2\right).$$

Let $\psi : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$ be the map defined as $\psi(a, b) = (a - b, a + b)$. Note that ψ is bijective. Moreover if $\psi(a, b) = (\mu, \nu)$, then it is easy to observe that

$$a = 0 \iff \mu = -\nu$$

and

$$b = 0 \iff \mu = \nu.$$

Hence we have that

$$a \neq 0 \text{ and } b \neq 0 \iff \mu^2 \neq \nu^2.$$

Put $A = (a - b)^2$ and $B = (a + b)^2$. These arguments complete the proof. ∎

Remark II.2. Under the notation and assumptions of Theorem II.1, assume further that $z \in \{c^2 : c \in \mathbb{F}_q\}$. If $z = 0$, then choosing $A = 0$ and $B = 1$ we obtain that $(z - A)(z - B)$ is a square in $\mathbb{F}_{q^m}$. If $z = c^2$ with $c \in \mathbb{F}_q^*$, then choosing $A = 0$ and $B = c^2$ we obtain that $(z - A)(z - B)$ is a square in $\mathbb{F}_{q^m}$. Hence the condition (2) is equivalent to the following condition, which we will use in the proofs below:

For each $z \in \mathbb{F}_{q^m}$, there exist squares A, B in $\mathbb{F}_q$ with $A \neq B$ and $(z - A)(z - B)$ is a square in $\mathbb{F}_{q^m}$.

III. The covering radius in even characteristic

In this section we give a simple and beautiful proof that the covering radius is 2 if the characteristic of the field $\mathbb{F}_q$ is 2 and $q > 2$.

Theorem III.1. *Assume that* $\mathrm{char}\ \mathbb{F}_q$ *is* 2 *and* $q > 2$. *Let* $m \geq 1$ *be an integer. Then the covering radius of* $M(m, q)$ *is* 2.

Proof: The arguments in the beginning of the proof of Theorem II.1 is independent from characteristic. We need to show that given $\alpha, \beta \in \mathbb{F}_{q^m}$ there exist $x, y \in \mathbb{F}_{q^m}^*$ with $x \neq y$ and $a, b \in \mathbb{F}_q$ such that the system

$$\begin{aligned} ax + by &= \alpha, \\ a\frac{1}{x} + b\frac{1}{y} &= \beta \end{aligned} \tag{6}$$

holds. If $\alpha = 0$, $\beta = 0$ or $\alpha\beta = c^2$ for some $c \in \mathbb{F}_q$, then it is easy to show existence of $x, y \in \mathbb{F}_{q^m}^*$ with $x \neq y$ and $a, b, \in \mathbb{F}_q$ such that the system (6) holds as these arguments in the proof of Theorem II.1 hold in even characteristic as well. Hence we

assume that $\alpha \neq 0$, $\beta \neq 0$ and $\alpha\beta \neq c$ for any $c \in \mathbb{F}_q$ from now on in this proof.

Following the arguments in the beginning of the proof of Theorem II.1, it remains to show that the equation

$$x^2 + x\left(\frac{b^2}{a\beta} + \frac{\alpha}{a} + \frac{a}{\beta}\right) + \frac{\alpha}{\beta} = 0 \tag{7}$$

has a solution $x \in \mathbb{F}_{q^m}$. Put

$$A = \frac{b^2}{a\beta} + \frac{\alpha}{a} + \frac{a}{\beta} \text{ and } B = \frac{\alpha}{\beta}.$$

As $a^2 + b^2 = (a+b)^2$, by our assumption above in this proof, we have that $A \neq 0$. The equation in (7) is equivalent to the equation

$$\left(\frac{x}{A}\right)^2 + \frac{x}{A} = \frac{B}{A^2}. \tag{8}$$

Let $\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_2$ be the absolute trace map. Using Hilbert's Theorem 90 it remains to show that we can choose $a, b \in \mathbb{F}_q^*$ so that $\mathrm{Tr}\left(\frac{B}{A^2}\right) = 0$.

Note that

$$\frac{B}{A^2} = \frac{a^2\alpha\beta}{a^4 + b^4 + \alpha^2\beta^2}.$$

Put $z = \alpha\beta \in \mathbb{F}_{q^m}$, which is nonzero by our assumption in this proof above. Hence we need to show existence of $a, b \in \mathbb{F}_q^*$ such that

$$\mathrm{Tr}\left(\frac{z}{a^4 + b^4 + z^2}\right) = 0.$$

Firstly, we assume that there exist $a, b \in \mathbb{F}_q^*$ such that

$$a^4 + b^4 = 0. \tag{9}$$

Secondly, we assume that there exist $a, b \in \mathbb{F}_q^*$ such that

$$a^4 + b^4 = 1. \tag{10}$$

We will prove that these assumptions hold at the end of this proof.

If $\mathrm{Tr}\left(\frac{1}{z}\right) = 0$, then we choose $a, b \in \mathbb{F}_q^*$ satisfying $a^4 + b^4 = 0$. This implies that

$$\mathrm{Tr}\left(\frac{z}{a^4 + b^4 + z^2}\right) = \mathrm{Tr}\left(\frac{1}{z}\right) = 0.$$

If $\mathrm{Tr}\left(\frac{1}{z}\right) = 1$, then we choose $a, b \in \mathbb{F}_q^*$ satisfying $a^4 + b^4 = 1$. Note that $\mathrm{Tr}\left(\frac{1}{1+z}\right) = \mathrm{Tr}\left(\frac{1}{1+z^2}\right)$. These imply that

$$\begin{aligned}
\mathrm{Tr}\left(\frac{z}{a^4 + b^4 + z^2}\right) &= \mathrm{Tr}\left(\frac{z}{1 + z^2}\right) \\
&= \mathrm{Tr}\left(\frac{z}{1 + z^2}\right) \\
&+ \mathrm{Tr}\left(\frac{1}{1+z^2}\right) + \mathrm{Tr}\left(\frac{1}{1+z}\right) \\
&= \mathrm{Tr}\left(\frac{1+z}{1+z^2}\right) + \mathrm{Tr}\left(\frac{1}{1+z}\right) \\
&= \mathrm{Tr}\left(\frac{1}{1+z}\right) + \mathrm{Tr}\left(\frac{1}{1+z}\right) \\
&= 0.
\end{aligned}$$

Finally we show that the assumptions (9) and (10) hold. Choosing $a = b = 1$ we show that the assumption in (9) holds. Choosing $a \in \mathbb{F}_q \setminus \mathbb{F}_2$ and $b \in \mathbb{F}_q^m$ with $b^4 = a^4 + 1$ we show that the assumption in (10) holds. ∎

We consider the degenerate case of characteristic 2, which happens only when $q = 2$, in the following remark.

Remark III.2. For $m = 1$ and $q = 2$, the Melas code $M(1,2)$ is degenerate as the parity check matrix $H = [1]$ has rank 1. It is clear that for any given $a \in \mathbb{F}_2$, we have $a \cdot 1 = a$, and hence the covering radius of $M(1,2)$ is 1.

IV. The covering radius over $\mathbb{F}_3$

In this section we determine the covering radius of the Melas code $M(m,3)$, see Theorem IV.3 below. We prove that the covering radius of $M(m,3)$ is 3 if $m \geq 3$ and the covering radius of $M(2,3)$ is 4. We consider the degenerate case $M(1,3)$ in Remark IV.4 below.

We first consider a special case in the proof of Theorem IV.3.

Lemma IV.1. *For $m \geq 2$, there exist $x, y, z \in \mathbb{F}_{3^m} \setminus \{0\}$ which are mutually distinct and*

$$x + y + z = 0,$$

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1.$$

Proof: Let $\gamma \in \mathbb{F}_{3^m} \setminus \{0\}$ such that

$$\mathrm{Tr}\left(\frac{1}{\gamma}\right) = 0. \tag{11}$$

The equation

$$T^3 - T + \frac{1}{\gamma} = 0 \tag{12}$$

has 3 distinct nonzero solutions in $\mathbb{F}_{3^m}$ by Hilbert's Theorem 90 (see [13, Theorem 2.25]) and (11). Let $\frac{x}{\gamma}$, $\frac{y}{\gamma}$ and $\frac{z}{\gamma}$ be the roots of the equation in (12). Then we have

$$T^3 - T + \frac{1}{\gamma} = \left(T - \frac{x}{\gamma}\right)\left(T - \frac{y}{\gamma}\right)\left(T - \frac{z}{\gamma}\right).$$

Considering the coefficients of T^2, T and 1 in both sides we obtain that

$$\begin{aligned} x + y + z &= 0, \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= 1. \end{aligned}$$

Note that the polynomial $T^3 - T + \frac{1}{\gamma} \in \mathbb{F}_{3^m}[T]$ is square-free and hence the elements $x, y, z \in \mathbb{F}_{3^m} \setminus \{0\}$ are mutually distinct. ∎

The next proposition corresponds to another special case in the proof of Theorem IV.3. We use elliptic curves and Hasse-Weil bound in its proof.

Proposition IV.1. *Assume that $\beta \in \mathbb{F}_{3^m} \setminus \{0, 1\}$. If $m \geq 3$, then there exists $y \in \mathbb{F}_{3^m}$ such that*

$$y \notin \left\{0, \frac{1}{\beta}, 1\right\}, \quad y^2 + y + \frac{1}{\beta} \neq 0, \tag{13}$$

and the equation

$$w^2 = \frac{y}{(y-1)(\beta y - 1)} + 1 \tag{14}$$

has a solution $w \in \mathbb{F}_{3^m} \setminus \{0, -1, 1\}$.

Proof: Let $F = \mathbb{F}_{3^m}(y)(w)$ be the algebraic function field given by the Kummer extension

$$w^2 = \frac{y}{(y-1)(\beta y - 1)} + 1 = \frac{\beta\left(y^2 - y + \frac{1}{\beta}\right)}{(y-1)(\beta y - 1)}$$

of the rational function field $\mathbb{F}_{3^m}(y)$. Note that the polynomials $y^2 - y + \frac{1}{\beta}$ and $(y-1)(\beta y - 1)$ in $\mathbb{F}_{3^m}[y]$ are coprime. There are two rational places of $\mathbb{F}_{3^m}(y)$ corresponding to the zeroes of $y^2 - y + \frac{1}{\beta}$ if this polynomial splits in $\mathbb{F}_{3^m}$. Otherwise there is a unique place of degree 2 of $\mathbb{F}_{3^m}(y)$ corresponding to the zero of $y^2 - y + \frac{1}{\beta}$. Hence the genus of F is 1 by [19, Proposition 3.7.3].

The place of $\mathbb{F}_{3^m}(y)$ corresponding to the zero of $y - 1$ is totally ramified in $F/\mathbb{F}_{3^m}(y)$. Hence there is exactly one rational place of F with coefficients y, w such that $y = 1$.

The place of $\mathbb{F}_{3^m}(y)$ corresponding to the zero of $\beta y - 1$ is totally ramified in $F/\mathbb{F}_{3^m}(y)$. Hence there is exactly one rational place of F with coefficients y, w such that $y = \frac{1}{\beta}$.

If the polynomial $y^2 - y + \frac{1}{\beta}$ splits in $\mathbb{F}_{3^m}$, then there are exactly two rational places of F with coefficients y, w such that $w = 0$. Otherwise there is no rational place of F with coefficients y, w such that $w = 0$.

Next we consider the polynomial $y^2 + y + \frac{1}{\beta}$. There are at most 4 rational places of F with coefficients y, w such that $y^2 + y + \frac{1}{\beta} = 0$. This happens only if this polynomial splits in $\mathbb{F}_{3^m}$ and both of the places of $\mathbb{F}_{3^m}(y)$ corresponding to the zeroes of this polynomial totally split in the extension $F/\mathbb{F}_{3^m}(y)$.

Finally we consider the rational place P_∞ of $\mathbb{F}_{3^m}(y)$ corresponding to the pole of y. There are at most 2 rational places of F over P_∞. This happens if and only if $-\beta$ is a square in $\mathbb{F}_{3^m}$.

Let $N(F)$ denote the number of rational places of F. Combining the arguments in the previous paragraphs we conclude that if

$$N(F) > 1 + 1 + 2 + 4 + 2 = 10, \tag{15}$$

then there exists a rational place of F such that the corresponding coefficients $y, w \in \mathbb{F}_{3^m}$ satisfy (13) and (14).

It remains to prove (15). Using Hasse-Weil inequality [19, Theorem 5.2.3], as the genus of F is 1, we have

$$N(F) \geq 3^m + 1 - 2 \cdot 3^{m/2}. \tag{16}$$

Note that

$$3^m + 1 - 2 \cdot 3^{m/2} \geq 11 \tag{17}$$

for $m \geq 3$. Combining (16) and (17) we prove (15), which completes the proof. ∎

The next proposition is a continuation of Proposition IV.1.

Proposition IV.2. *Assume that $m \geq 3$ and $\beta \in \mathbb{F}_{3^m} \setminus \{0, 1\}$. Let $y, w \in \mathbb{F}_{3^m}$ obtained by Proposition IV.1 satisfy the conditions (13) and (14). Put $x, z \in \mathbb{F}_{3^m}$ defined as*

$$x = (y-1)(w+1) \text{ and } z = 1 - y - (y-1)(w+1).$$

Then the followings hold:

1) $x+y+z=1, \quad \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\beta.$
2) $xyz \neq 0.$
3) x, y, z *are mutually distinct.*

Proof: Note that

$$\begin{aligned} x+y+z &= (y-1)(w+1) \\ &+ y+1-y-(y-1)(w+1) \\ &= 1. \end{aligned}$$

Moreover we have

$$\begin{aligned} \frac{1}{x}+\frac{1}{y}+\frac{1}{z} &= \frac{1}{(y-1)(w+1)}+\frac{1}{y} \\ &+ \tfrac{1}{1-y-(y-1)(w+1)} \\ &= \frac{1}{(y-1)(w+1)} \\ &+ \tfrac{1}{y}+\tfrac{1}{(y-1)(1-w)} \\ &= \frac{1}{(y-1)(w^2-1)}+\frac{1}{y} \\ &= \frac{1}{(y-1)} \cdot \frac{(y-1)(\beta y-1)}{y}+\frac{1}{y} \\ &= \beta. \end{aligned}$$

Next we consider item 2). Note that $y \neq 0$, $y \neq 1$ and $w \neq -1$ by Proposition IV.1 and hence $xy \neq 0$. Assume that $z=0$. Then we get

$$1-y=(y-1)(w+1) \text{ and hence } w+1=-1.$$

As $w \neq 1$ by Proposition IV.1, we get a contradiction. This shows that $xyz \neq 0$.

Finally we prove item 3). Assume that $x=y$. Then $w+1=\frac{y}{y-1}$ and hence $w=\frac{1}{y-1}$. Using (14) we obtain that

$$\frac{1}{(y-1)^2}=\frac{y}{(y-1)(\beta y-1)}+1.$$

This implies that

$$\beta y^3+\beta y^2+y=0.$$

As $y \neq 0$ and $\beta \neq 0$ we conclude that

$$y^2+y+\frac{1}{\beta}=0,$$

which is a contradiction to (13). This shows that $x \neq y$.

Assume that $x=z$. Then $2x+y=1$. As $x=(y-1)(w+1)$ we obtain that

$$2(y-1)(w+1)+y=1.$$

This implies that either $y=1$ or $w=0$, both are contradictions to Proposition IV.1. This shows that $x \neq z$.

Assume that $y=z$. Then $x+2y=1$. As $x=(y-1)(w+1)$ we obtain that

$$(y-1)(w+1)+2y=1.$$

This implies that $w=\frac{1}{1-y}$. Using (14) we obtain that

$$\frac{1}{(1-y)^2}=\frac{y}{(y-1)(\beta y-1)}+1.$$

As $y \neq 0$ and $\beta \neq 0$ we conclude that

$$y^2+y+\frac{1}{\beta}=0,$$

which is a contradiction to (13). This shows that $y \neq z$. This completes the proof. ∎

The following example refers to the covering radius of $M(2,3)$, which is different from the covering radius of $M(m,3)$ for $m \geq 3$.

Example IV.2. For $m=2$, let $w \in \mathbb{F}_{3^2}$ be a primitive element with $w^2+2w+2=0$. For each $1 \leq i \leq 8$ with $i \neq 5$ and $i \neq 7$, there exist $1 \leq i_1 < i_2 < i_3 \leq 8$ such that $x=w^{i_1}$, $y=w^{i_2}$, $z=w^{i_3}$ and $a, b, c \in \mathbb{F}_3$ satisfying

$$ax+by+cz=1,$$

$$a\frac{1}{x}+b\frac{1}{y}+c\frac{1}{z}=w^i.$$

However for w^5 and w^7 there does not exist such three mutually distinct elements $x, y, z \in \mathbb{F}_{3^m}$ and $a, b, c \in \mathbb{F}_3$ satisfying these conditions. Instead for w^5 we have

$$x+y+z+t=1,$$

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{t}=w^5,$$

with $x = w^3$, $y = w^5$, $z = w^6$ and $t = 1$. Similarly for w^7 we have

$$x + y + z + t = 1,$$

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{t} = w^7,$$

with $x = w$, $y = w^2$, $z = w^7$ and $t = 1$.

Now we are ready for the main result of this section.

Theorem IV.3. *Let $q = 3$ and $m \geq 2$ be an integer. Then the covering radius of $M(m, 3)$ is 3 if $m \geq 3$. Moreover the covering radius of $M(2, 3)$ is 4.*

Proof: Recall that the covering radius of $M(m, 3)$ is the smallest integer ρ such that every column vector in $\mathbb{F}_{3^m}^{2\times 1}$ is an $\mathbb{F}_3$-linear combination at most ρ columns in the parity check matrix H of $M(m, 3)$ given in (1). Choosing an $\mathbb{F}_3$-linear combination of 3 columns of H with nonzero coefficients so that the linear combination is $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{F}_{3^m}^{2\times 1}$ means choosing mutually distinct $x, y, z \in \mathbb{F}_{3^m} \setminus \{0\}$ such that

$$\begin{aligned} x + y + z &= \alpha, \text{ and} \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= \beta. \end{aligned}$$

The methods in Section 2 show that the covering radius of $M(m, 3)$ is at least 3 for $m \geq 2$. We will use the following assertions:

i) There are mutually distinct $x, y, z \in \mathbb{F}_{3^m} \setminus \{0\}$ such that

$$\begin{aligned} x + y + z &= 1, \text{ and} \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= 0. \end{aligned}$$

ii) For given $\beta \in \mathbb{F}_{3^m} \setminus \{0\}$, there are mutually distinct $x, y, z \in \mathbb{F}_{3^m} \setminus \{0\}$ such that

$$\begin{aligned} x + y + z &= 1, \text{ and} \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= \beta. \end{aligned}$$

It is not difficult to observe that the proofs of items i) and ii) imply that the covering radius of $M(m, 3)$ is 3.

Note that item i) is equivalent to the following assertion:

iii) There are mutually distinct $x, y, z \in \mathbb{F}_{3^m} \setminus \{0\}$ such that

$$\begin{aligned} x + y + z &= 0, \text{ and} \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= 1. \end{aligned}$$

We prove item iii) for any $m \geq 2$ by Lemma IV.1. We prove item ii) for any $m \geq 3$ by Proposition IV.2. This completes the proof of the statement that the covering radius of $M(m, 3)$ is 3 for $m \geq 3$. For the case $M(2, 3)$ we also use Example IV.2. This completes the proof. ■

We consider the degenerate case of $\mathbb{F}_3$ in the following remark.

Remark IV.4. For $m = 1$, the Melas code $M(1, 3)$ is degenerate as the parity check matrix $H = [1 \ \ 2]$ has rank 1. It is clear that for any given $a \in \mathbb{F}_3$, we have $a \cdot 1 = a$, and hence the covering radius of $M(1, 3)$ is 1.

V. The covering radius over $\mathbb{F}_5$

In this section we prove that the covering radius of the Melas code is 2 if q is 5, see Theorem V.4 below. We use the characterization in Section 2 and rather detailed counting arguments using quadratic forms over finite fields.

Note that the set of squares in $\mathbb{F}_5$ is $\{0, 1, 4\}$. We define subsets $B(0, 1)$, $B(0, 4)$ and $B(1, 4)$ of $\mathbb{F}_{5^m}$ as follows:

- $B(0,1) = \{z \in \mathbb{F}_{5^m} : z(z-1) \text{ is a square in } \mathbb{F}_{5^m}\}$.
- $B(0,4) = \{z \in \mathbb{F}_{5^m} : z(z-4) \text{ is a square in } \mathbb{F}_{5^m}\}$.
- $B(1,4) = \{z \in \mathbb{F}_{5^m} : (z-1)(z-4) \text{ is a square in } \mathbb{F}_{5^m}\}$.

Note that using Theorem II.1 and Remark II.2 we obtain that the covering radius of the Melas code $M(m, 5)$ is 2 if and only if

$$\mathbb{F}_{5^m} = B(0, 1) \cup B(0, 4) \cup B(1, 4).$$

Note that

$$B(0,1)\cap\mathbb{F}_5=\{0,1,3\},$$
$$B(0,4)\cap\mathbb{F}_5=\{0,2,4\},$$
$$\text{and }\ B(1,4)\cap\mathbb{F}_5=\{0,1,4\}.$$

Let $B(0,1)^*=B(0,1)\setminus\mathbb{F}_5$, $B(0,4)^*=B(0,4)\setminus\mathbb{F}_5$ and $B(1,4)^*=B(1,4)\setminus\mathbb{F}_5$.

Hence it is enough to prove that the cardinality $|B(0,1)^*\cup B(0,4)^*\cup B(1,4)^*|=5^m-5$ in order to show that the covering radius is 2. We will use some inclusion-exclusion principle together with some counting arguments and quadratic forms over finite fields in the proof below.

We start with a simple but useful lemma.

Lemma V.1. *We have that*

$$(B(0,1)^*\cap B(0,4)^*)\setminus B(1,4)^*=\emptyset,$$
$$(B(0,1)^*\cap B(1,4)^*)\setminus B(0,4)^*=\emptyset,\ \textit{and}$$
$$(B(0,4)^*\cap B(1,4)^*)\setminus B(0,1)^*=\emptyset.$$

Proof: Let $x\in(B(0,1)^*\cap B(0,4)^*)$. Then there exist $y_1,y_2\in\mathbb{F}_{q^m}^*$ such that $x(x-1)=y_1^2$ and $x(x-4)=y_2^2$. Multiplying both sides we obtain that $(x-1)(x-4)=\left(\frac{y_1y_2}{x}\right)^2$. This completes the proof of the statement that $(B(0,1)^*\cap B(0,4)^*)\setminus B(1,4)^*=\emptyset$. The proofs of the other statements are similar. ∎

The proof of the following lemma uses, for example, the map $x\mapsto\frac{1}{x}$. This map is useful in order to decide whether images of quadratic map $x(x-1)$ are squares. Indeed after this bijective map on $\mathbb{F}_{5^m}\setminus\{0,1\}$, the image becomes image of a linear map, which is easy to decide.

Lemma V.2. *We have that*

$$|B(0,1)|=|B(0,4)|=|B(1,4)|=\frac{5^m+1}{2}.$$

Proof: We present the proof of the statement $|B(0,1)|=\frac{5^m+1}{2}$ and the proof of the other statements are similar. Let $\mu:\mathbb{F}_{5^m}\setminus\{0\}\to\mathbb{F}_{5^m}\setminus\{1\}$ be the bijective map $\mu(x)=1-\frac{1}{x}$. Note that the number of $y\in\mathbb{F}_{5^m}$ such that y is in the image of μ and y is a square in $\mathbb{F}_{5^m}$ is

$$1+\left(\frac{5^m-1}{2}-1\right)-1=\frac{5^m-1}{2}.$$

Here the first summand 1 refers to $y=0$ and the second summand $\left(\frac{5^m-1}{2}-1\right)-1$ refers to the number of all nonzero squares in $\mathbb{F}_{5^m}$ except 1, which is not in the image of μ. The cardinality $|B(0,1)|$ is given by

$$\begin{aligned}
&|\{x\in\mathbb{F}_{5^m}:x(x-1)\text{ is a square in }\mathbb{F}_{5^m}\}|\\
&=\left|\left\{x\in\mathbb{F}_{5^m}^*:\frac{x(x-1)}{x^2}\text{ is a square in }\mathbb{F}_{5^m}\right\}\right|+1\\
&=\left|\left\{x\in\mathbb{F}_{5^m}^*:\left(1-\frac{1}{x}\right)\text{ is a square in }\mathbb{F}_{5^m}\right\}\right|+1\\
&=|\{y\in\mathbb{F}_{5^m}\setminus\{1\}:y\in\mathrm{Im}\mu,\text{ and }y\text{ is a square in }\mathbb{F}_{5^m}\}|\\
&+1\\
&=\frac{5^m-1}{2}+1=\frac{5^m+1}{2}.
\end{aligned}$$

This completes the proof. ∎

The following lemma is used in the proof of Theorem V.4 below.

Lemma V.3. *We have that*

$$|B(0,1)^*\setminus B(0,4)^*|=|B(0,1)^*\cap B(0,4)^*|,$$
$$|B(0,4)^*\setminus B(1,4)^*|=|B(0,4)^*\cap B(1,4)^*|,\ \textit{and}$$
$$|B(1,4)^*\setminus B(0,1)^*|=|B(1,4)^*\cap B(0,1)^*|.$$

Proof: In this proof we use the following relation notation: For $\alpha,\beta\in\mathbb{F}_{5^m}\setminus\mathbb{F}_5$, the relation $\alpha\sim\beta$ means that α/β is a square in $\mathbb{F}_{5^m}$.

Let $\mu:\mathbb{F}_{5^m}\setminus\mathbb{F}_5\to\mathbb{F}_{5^m}\setminus\mathbb{F}_5$ be the bijection given by $\mu(x)=\frac{1}{x-1}$. As μ is a bijection, we have equivalent definitions

$$B(0,1)^*\setminus B(0,4)^*=\left\{\begin{array}{l}x\in\mathbb{F}_{5^m}\setminus\mathbb{F}_5:\\ \mu(x)\,(\mu(x)-1)\\ \text{is a square,}\\ \\ \text{and}\\ \\ \mu(x)\,(\mu(x)-4)\\ \text{is not a square}\end{array}\right\},\quad(18)$$

and

$$B(0,1)^*\cap B(0,4)^*=\left\{\begin{array}{l}x\in\mathbb{F}_{5^m}\setminus\mathbb{F}_5:\\ \mu(x)\,(\mu(x)-1)\\ \text{is a square,}\\ \\ \text{and}\\ \\ \mu(x)\,(\mu(x)-4)\\ \text{is a square}\end{array}\right\}.\quad(19)$$

For $x\in\mathbb{F}_{5^m}\setminus\mathbb{F}_5$ we have

$$\begin{aligned}\mu(x)\,(\mu(x)-1)&=\frac{1}{x-1}\left(\frac{1}{x-1}-1\right)\\&\sim 1-(x-1)\sim x-2,\end{aligned}\quad(20)$$

and

$$\mu(x)\left(\mu(x)-4\right) = \frac{1}{x-1}\left(\frac{1}{x-1}-4\right) \sim 1-4(x-1) \sim (x-1)-4 \sim x, \quad (21)$$

where we use that 4 is a square in $\mathbb{F}_{5^m}$.

Using (18) and (20) we obtain that

$$B(0,1)^* \setminus B(0,4)^* = \left\{ \begin{array}{l} x \in \mathbb{F}_{5^m} \setminus \mathbb{F}_5 : (x-2) \\ \text{is a square,and} \\ x \text{ is not a square} \end{array} \right\}.$$

Using (19) and (21) we obtain that

$$B(0,1)^* \cap B(0,4)^* = \left\{ \begin{array}{l} x \in \mathbb{F}_{5^m} \setminus \mathbb{F}_5 : (x-2) \\ \text{is a square, and} \\ x \text{ is a square} \end{array} \right\}.$$

For $x \in \mathbb{F}_{5^m}$, note that $x-2$ is a square and x is a square if and only if there exist $y_1, y_2 \in \mathbb{F}_{5^m}$ such that

$$x-2 = y_1^2 \text{ and } x = y_2^2.$$

This observation implies that

$$|\{x \in \mathbb{F}_{5^m} : (x-2) \text{ is a square and } x \text{ is a square}\}| = \frac{1}{4}\left|\left\{(y_1,y_2) \in \mathbb{F}_{5^m} \times \mathbb{F}_{5^m} : y_1^2+y_2^2 = 2\right\}\right|.$$

Moreover we observe that

$$\left\{(y_1,y_2) \in \mathbb{F}_5 \times \mathbb{F}_5 : y_1^2+y_2^2 = 2\right\} = \{(1,1),(1,-1),(-1,1),(-1,-1)\},$$

in particular its cardinality is 4. Let N be the number of $(y_1,y_2) \in \mathbb{F}_{5^m} \times \mathbb{F}_{5^m}$ such that

$$y_1^2+y_2^2 = 2.$$

These arguments imply that

$$|B(0,1)^* \cap B(0,4)^*| = \frac{N-4}{4}. \quad (22)$$

Moreover using Lemma V.2 and the fact that $B(0,1) \cap \mathbb{F}_5 = \{0,1,3\}$ we have

$$|B(0,1)^*| = |B(0,1)| - |B(0,1) \cap \mathbb{F}_5| = \frac{5^m+1}{2} - 3 = \frac{5^m-5}{2}. \quad (23)$$

Using [13, Theorem 6.26] we obtain that

$$N = 5^m - 1. \quad (24)$$

Combining (22),(23) and (24) we complete the proof. ∎

Now we are ready to present and to prove the main result of this section.

Theorem V.4. *Let $q = 5$. Let $m \geq 1$ be an integer. Then the covering radius of $M(m,q)$ is 2.*

Proof: Recall that using Theorem II.1, Remark II.2, and the arguments above it is enough to prove that $|B(0,1)^* \cup B(0,4)^* \cup B(1,4)^*| = 5^m - 5$. Using (18) and Lemma V.2 we obtain that

$$|B(0,1)^*| = |B(0,4)^*| = |B(1,4)^*| = \frac{5^m+1}{2} - 3 = \frac{5^m-5}{2}. \quad (25)$$

Using inclusion-exclusion principle and (25) we obtain that

$$\begin{aligned} &|B(0,1)^* \cup B(0,4)^* \cup B(1,4)^*| \\ &= 3\frac{5^m-5}{2} - |B(0,1)^* \cap B(0,4)^*| \\ &-|B(0,4)^* \cap B(1,4)^*| - |B(1,4)^* \cap B(0,1)^*| \\ &+|B(0,1)^* \cap B(0,4)^* \cap B(1,4)^*|. \end{aligned} \quad (26)$$

Using Lemma V.1 we conclude that

$$B(0,1)^* \cap B(0,4)^* = B(0,1)^* \cap B(1,4)^* = B(0,1)^* \cap B(0,4)^* \cap B(1,4)^*. \quad (27)$$

Combining Lemma V.3, (25) and (27) we conclude that

$$\begin{aligned} &B(0,1)^* \cap B(0,4)^* = B(0,1)^* \cap B(1,4)^* \\ &= B(0,1)^* \cap B(0,4)^* \cap B(1,4)^* \\ &= \tfrac{5^m-5}{4}. \end{aligned} \quad (28)$$

Similarly we have

$$B(0,4)^* \cap B(1,4)^* = \frac{5^m-5}{4}. \quad (29)$$

In summary we have the picture in Figure 1.

Combining (26), (28) and (29) we obtain that

$$\begin{aligned} &|B(0,1)^* \cup B(0,4)^* \cup B(1,4)^*| \\ &= 3\tfrac{5^m-5}{2} - 3\tfrac{5^m-5}{4} + \tfrac{5^m-5}{4} = 5^m - 5. \end{aligned}$$

This completes the proof. ∎

VI. Case $m = 1$ for $q > 5$ in odd characteristic

In this section we prove a result, namely Theorem VI.7, which is stronger than the statement that the covering radius of $M(1,q)$ is 2 for any finite field $\mathbb{F}_q$ of odd characteristic and $q > 5$. Theorem VI.7 is used in the next section in order to prove that the covering radius of $M(m,q)$ is 2 for any

$m \geq 1$ and any finite field $\mathbb{F}_q$ of odd characteristic such that $q > 5$.

Lemma VI.1. *Assume that* $\mathrm{char}\ \mathbb{F}_q$ *is odd and* $q > 5$. *There exists* $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ *such that both* α *and* $\alpha - 1$ *are squares in* $\mathbb{F}_q$.

Proof: Put $\alpha = x_1^2$ and $\alpha - 1 = x_2^2$. Then we get that

$$x_1^2 - x_2^2 = 1. \tag{30}$$

Note that the cardinality N of the set $S = \{(x_1, x_2) \in \mathbb{F}_q \times \mathbb{F}_q : x_1^2 - x_2^2 = 1\}$ is $q - 1$ by [13, Theorem 6.26]. Here we use the facts that the determinant of the quadratic form in (30) is -1 and $(-1)(-1) = 1$ is a square in $\mathbb{F}_q$. Considering the solutions with non-zero coordinates we obtain that the cardinality N^* of the set $S^* = \{(x_1, x_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : x_1^2 - x_2^2 = 1\}$ is

$$\begin{cases} q-4 & \text{if } q \equiv 1 \mod 4, \\ q-3 & \text{if } q \equiv 3 \mod 4. \end{cases}$$

This implies that $N^* \geq 1$ if $q > 5$ and $q \equiv 1 \mod 4$. Also this implies that $N^* \geq 1$ if $q > 3$ and $q \equiv 3 \mod 4$. Choosing an element of $(x_1, x_2) \in S^*$ we obtain that $\alpha = x_1^2$ satisfies the conditions. ∎

From now on we assume that $\mathrm{char}\ \mathbb{F}_q$ is odd and $q > 5$. Using Lemma VI.1 we choose and fix $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ such that both α and $\alpha - 1$ are squares in $\mathbb{F}_q$.

As in Section V we define the subsets $B(0, 1)$, $B(0, \alpha)$ and $B(1, \alpha)$ of $\mathbb{F}_q$ as follows:

$$\begin{aligned} &B(0,1) = \{z \in \mathbb{F}_q : z(z-1) \text{ is a square in } \mathbb{F}_q\}, \\ &B(0,\alpha) = \{z \in \mathbb{F}_q : z(z-\alpha) \text{ is a square in } \mathbb{F}_q\}, \\ &\text{and } B(1,\alpha) = \{z \in \mathbb{F}_q : (z-1)(z-\alpha) \\ &\text{is a square in } \mathbb{F}_q\}. \end{aligned} \tag{31}$$

We start with an analog of Lemma V.2.

Lemma VI.2. *We have that*

$$|B(0,1)| = |B(0,\alpha)| = |B(1,\alpha)| = \frac{q+1}{2}.$$

Proof: Note that the map $\mu : \mathbb{F}_q \setminus \{0\} \to \mathbb{F}_q \setminus \{0\}$ given by $x \mapsto 1/x$ is a bijection. Note also that

$$0 \in B(0, 1). \tag{32}$$

Using the bijection μ we observe that

$$\begin{aligned} B(0,1) \setminus \{0\} &= \{x \in \mathbb{F}_q^* : \tfrac{1}{x}(\tfrac{1}{x} - 1) \\ &\qquad \text{is a square in } \mathbb{F}_q\} \\ &= \{x \in \mathbb{F}_q^* : 1 - x \\ &\qquad \text{is a square in } \mathbb{F}_q\}. \end{aligned} \tag{33}$$

It is clear that $\mathbb{F}_q = \{1 - x : x \in \mathbb{F}_q\}$. As the number of squares in $\mathbb{F}_q$ is $\frac{q+1}{2}$ and $1 - x = 1$ is a square for $x = 0$, using (33) we conclude that

$$|B(0,1) \setminus \{0\}| = \frac{q+1}{2} - 1. \tag{34}$$

Combining (32) and (34) we obtain that $|B(0,1)| = \frac{q+1}{2}$. The proof of the statements $|B(0,\alpha)| = \frac{q+1}{2}$ and $|B(1,\alpha)| = \frac{q+1}{2}$ are similar. ∎

Under this choice of α, we have a complete analog of Lemma V.1 for $q \equiv 1 \mod 4$.

Lemma VI.3. *Assume that* $q \equiv 1 \mod 4$. *We have*

$$\begin{aligned} &(B(0,1) \cap B(0,\alpha)) \subseteq B(1,\alpha), \\ &(B(0,1) \cap B(1,\alpha)) \subseteq B(0,\alpha), \quad \textit{and} \\ &(B(0,\alpha) \cap B(1,\alpha)) \subseteq B(0,1). \end{aligned}$$

Proof: Note that $0 \in B(0,1) \cap B(0,\alpha)$ trivially. Also for $z = 0$ we have $(z-1)(z-\alpha) = (-1)(-\alpha) = \alpha$ is a square. Hence $0 \in B(1,\alpha)$ as well.

For $x \in \mathbb{F}_q^*$, if $x \in B(0,1) \cap B(0,\alpha)$, then $x(x-1)$ and $x(x-\alpha)$ are both squares. Multiplying these we get that $(x-1)(x-\alpha)$ is a square, or equivalently $x \in B(1,\alpha)$. This completes the proof of the statement that $(B(0,1) \cap B(0,\alpha)) \subseteq B(1,\alpha)$.

The proof of the statement $(B(0,1) \cap B(1,\alpha)) \subseteq B(0,\alpha)$ is similar. For $z = 1$ we have $z(z-\alpha) = 1(1-\alpha) = 1-\alpha$, which is a square as $(\alpha - 1)$ is a square by the choice of α and -1 is a square by the assumption $q \equiv 1 \mod 4$. If $x \neq 1$, $x(x-1)$ is a square and $(x-1)(x-\alpha)$ is a square, then $x(x-\alpha)$ is a square.

The proof of the statement $(B(0,\alpha) \cap B(1,\alpha)) \subseteq B(0,1)$ is also similar. For $z = \alpha$ we have $z(z-1) = \alpha(\alpha-1)$ is a square as both α and $(\alpha-1)$ are squares by the choice of α. The rest of the proof is similar. ∎

Under this choice of α, there is a difference in the following analog to Lemma V.1 for $q \equiv 3 \mod 4$. Namely we need to exclude $\{1\}$ in the second item of the following lemma.

Lemma VI.4. *Assume that* $q \equiv 3 \mod 4$. *We*

have

$$(B(0,1)\cap B(0,\alpha))\subseteq B(1,\alpha),$$
$$(B(0,1)\cap B(1,\alpha))\setminus\{1\}\subseteq B(0,\alpha),\ \textit{and}$$
$$(B(0,\alpha)\cap B(1,\alpha))\subseteq B(0,1).$$

Proof: Note that $1\notin B(0,\alpha)$. Indeed for $z=1$ we have $z(z-\alpha)=-(\alpha-1)$, $(\alpha-1)$ is a square by the choice of α and (-1) is not a square as $q\equiv 3 \mod 4$. The rest of the proof of the statement $(B(0,1)\cap B(1,\alpha))\setminus\{1\}\subseteq B(0,\alpha)$ is similar to the proof of the statement $(B(0,1)\cap B(1,\alpha))\subseteq B(0,\alpha)$ in Lemma VI.3.

The proofs of the statements $(B(0,1)\cap B(0,\alpha))\subseteq B(1,\alpha)$ and $(B(0,\alpha)\cap B(1,\alpha))\subseteq B(0,1)$ are the same as the proof of Lemma VI.3. ∎

We need the following lemma in the proof of Theorem V.4 when $q\equiv 1 \mod 4$.

Lemma VI.5. *Assume that* $q\equiv 1 \mod 4$. *We have*

$$|(B(0,1)\cap B(0,\alpha))|=\frac{q-1}{4}+1.$$

Proof: Note that $0\in B(0,1)\cap B(0,\alpha)$ and we need to show that the cardinality N of the set

$$\{x\in\mathbb{F}_q^*: x(x-1) \text{ is a square and } x(x-\alpha) \text{ is a square}\} \quad (35)$$

is $\frac{q-1}{4}$. The map $\mu:\mathbb{F}_q^*\to\mathbb{F}_q^*$ given by $x\mapsto 1/x$ is a bijection. For $x\in\mathbb{F}_q^*$ we have

$$\mu(x)\left(\mu(x)-1\right)=\frac{1}{x}\left(\frac{1}{x}-1\right)=\frac{1-x}{x^2},$$

$$\mu(x)\left(\mu(x)-\alpha\right)=\frac{1}{x}\left(\frac{1}{x}-\alpha\right)=\frac{1-\alpha x}{x^2}.$$

Hence N, which is the cardinality of the set in (35), is equal to the cardinality of the set

$$S^*=\{x\in\mathbb{F}_q^*: 1-x \text{ is a square and } 1-\alpha x \text{ is a square}\}.$$

Put $1-x=x_1^2$ and $1-\alpha x=x_2^2$. We obtain that

$$\alpha x_1^2-x_2^2=\alpha-1. \quad (36)$$

The determinant of the quadratic form in (36) is $-\alpha$ and $(-1)(-\alpha)=\alpha$ is a square in $\mathbb{F}_q$. Using [13, Theorem 6.26] we obtain that the number of solutions $(x_1,x_2)\in\mathbb{F}_q\times\mathbb{F}_q$ is $q-1$.

If $x_1=0$ (or equivalently $x=1$), then there are exactly two solutions in (36).

If $x_2=0$ (or equivalently $x=1/\alpha$), then there are exactly two solutions in (36).

Note that $1\in S^*$ and $1/\alpha\in S^*$.

If $x=0$, then each element $(x_1,x_2)\in\{(1,1),(1,-1),(-1,1),(-1,-1)\}$ gives a solution to (36).

There is a 4-to-1 correspondence between

$$T^*=\{(x_1,x_2)\in\mathbb{F}_q\setminus\{0,1,-1\}\times\mathbb{F}_q\setminus\{0,1,-1\}: \alpha x_1^2-x_2^2=\alpha-1\}$$

and $S^*\setminus\{1,1/\alpha\}$ given by $(x_1,x_2)\mapsto 1-x_1^2$.

The arguments above imply that $|T^*|=q-1-2-2-4$ and hence

$$N-2=\frac{q-1-8}{4}.$$

This completes the proof. ∎

We need the following lemma in the proof of Theorem V.4 when $q\equiv 3 \mod 4$.

Lemma VI.6. *Assume that* $q\equiv 3 \mod 4$. *We have*

$$|(B(0,1)\cap B(0,\alpha))|=\frac{q-3}{4}+1.$$

Proof: The proof is similar to the proof of Lemma VI.5. We use the same arguments. The first difference is the following:

If $x_1=0$ (or equivalently $x=1$), then there are no solutions in (36). Indeed $-(\alpha-1)$ is not a square as -1 is not a square when $q\equiv 3 \mod 4$.

This implies that $|T^*|=q-1-0-2-4$ and hence

$$N-2=\frac{q-1-4}{4} \text{ and } N=\frac{q+1}{4}=\frac{q-3}{4}+1.$$

This completes the proof. ∎

Now we are ready to prove the main result of this section.

Theorem VI.7. *Assume that* $\mathrm{char}\ \mathbb{F}_q$ *is odd and* $q>5$. *There exists* $\alpha\in\mathbb{F}_q\setminus\{0,1\}$ *such that both* α *and* $\alpha-1$ *are squares in* $\mathbb{F}_q$. *Let* $B(0,1)$, $B(0,\alpha)$ *and* $B(1,\alpha)$ *be the subsets of* $\mathbb{F}_q$ *defined as in (31). We have that*

$$\mathbb{F}_q=B(0,1)\cup B(0,\alpha)\cup B(1,\alpha).$$

In particular the covering radius of $M(1,q)$ *is* 2.

Proof: Assume that $q \equiv 1 \mod 4$. See Figure 2 for the details. Using Lemma VI.3 we obtain that

$$\begin{aligned} &B(0,1) \setminus (B(0,\alpha) \cup B(1,\alpha)) \\ &= B(0,1) \setminus \{B(0,1) \cap B(0,\alpha) \cap B(1,\alpha)\}. \end{aligned} \tag{37}$$

Hence using Lemma VI.5 we get that

$$|B(0,1) \cap B(0,\alpha) \cap B(1,\alpha)| = \frac{q-1}{4} + 1. \tag{38}$$

Combining Lemma VI.2, Lemma VI.3 and Lemma VI.5 we obtain that

$$\begin{aligned} &|B(0,1) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &= \frac{q+1}{2} - \left(\frac{q-1}{4} + 1\right) = \frac{q-1}{4}. \end{aligned} \tag{39}$$

Similarly we have

$$\begin{aligned} &|B(0,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &= \frac{q+1}{2} - \left(\frac{q-1}{4} + 1\right) = \frac{q-1}{4}, \end{aligned} \tag{40}$$

and

$$\begin{aligned} &|B(1,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &= \frac{q+1}{2} - \left(\frac{q-1}{4} + 1\right) = \frac{q-1}{4}. \end{aligned} \tag{41}$$

Combining Lemma VI.3, (38), (39), (40) and (41) we obtain that

$$\begin{aligned} &|B(0,1) \cup B(0,\alpha) \cup B(1,\alpha)| \\ &= |B(0,1) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &\quad + |B(0,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &\quad + |B(1,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &\quad + |B(0,1) \cap B(0,\alpha) \cap B(1,\alpha)| \\ &= 3\frac{q-1}{4} + \frac{q-1}{4} + 1 = q. \end{aligned}$$

This completes the proof of the case that $q \equiv 1 \mod 4$.

Assume next that $q \equiv 3 \mod 4$. See Figure 3 for the details. Using Lemma VI.4 we obtain that

$$\begin{aligned} &B(0,1) \setminus (B(0,\alpha) \cup B(1,\alpha)) \\ &= B(0,1) \setminus \{B(0,1) \cap B(0,\alpha) \cap B(1,\alpha)\}. \end{aligned} \tag{42}$$

Hence using Lemma VI.6 we get that

$$|B(0,1) \cap B(0,\alpha) \cap B(1,\alpha)| = \frac{q-3}{4} + 1. \tag{43}$$

Combining Lemma VI.2, Lemma VI.4 and Lemma VI.5 we obtain that

$$\begin{aligned} &|B(0,1) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &= \frac{q+1}{2} - \left(\frac{q-3}{4} + 1 + 1\right) = \frac{q-3}{4}. \end{aligned} \tag{44}$$

Similarly we have

$$\begin{aligned} &|B(0,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &= \frac{q+1}{2} - \left(\frac{q-3}{4} + 1\right) = \frac{q-3}{4} + 1, \end{aligned} \tag{45}$$

and

$$\begin{aligned} &|B(1,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &= \frac{q+1}{2} - \left(\frac{q-3}{4} + 1 + 1\right) = \frac{q-3}{4}. \end{aligned} \tag{46}$$

Combining Lemma VI.4, (43), (44), (45) and (46) we obtain that

$$\begin{aligned} &|B(0,1) \cup B(0,\alpha) \cup B(1,\alpha)| \\ &= 1 + |B(0,1) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &\quad + |B(0,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &\quad + |B(1,\alpha) \setminus (B(0,1) \cap B(0,\alpha) \cap B(1,\alpha))| \\ &\quad + |B(0,1) \cap B(0,\alpha) \cap B(1,\alpha)| \\ &= 1 + \frac{q-3}{4} + \left(\frac{q-3}{4} + 1\right) + \frac{q-3}{4} + \left(\frac{q-3}{4} + 1\right) \\ &= 4\frac{q-3}{4} + 3 = q. \end{aligned}$$

This completes the proof. ■

VII. Generalization to arbitrary m for $q > 5$ in odd characteristic

In this section, for any integer $m \geq 1$, we prove that the covering radius of $M(m,q)$ is 2 for any finite field $\mathbb{F}_q$ of odd characteristic and $q > 5$. Our proof is a generalization of Theorem V.4 in the following sense. First using Lemma VI.1 we choose $\alpha \in \mathbb{F}_q \setminus \{0,1\}$ such that both α and $\alpha - 1$ are squares in $\mathbb{F}_q$. Using this α we define the analogous subsets $B(0,1)$, $B(0,\alpha)$ and $B(1,\alpha)$ in $\mathbb{F}_{q^m}$. An important technical step is to show that the union of the sets $B(0,1) \cap \mathbb{F}_q$, $B(0,\alpha) \cap \mathbb{F}_q$ and $B(1,\alpha) \cap \mathbb{F}_q$ cover $\mathbb{F}_q$. This holds in $\mathbb{F}_5$ by direct observation. We use such a choice of α and Theorem VI.7 for an arbitrary finite field $\mathbb{F}_q$ of odd characteristic with $q > 5$. Then we use analogous arguments as in the proof of Theorem V.4 in order to show that the union of the subsets $B(0,1)$, $B(0,\alpha)$ and $B(1,\alpha)$ cover $\mathbb{F}_{q^m}$.

From now on we assume that $\mathrm{char}\ \mathbb{F}_q$ is odd and $q > 5$. Using Lemma VI.1 we choose and fix $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ such that both α and $\alpha - 1$ are squares in $\mathbb{F}_q$.

We define subsets $B(0,1)$, $B(0,\alpha)$ and $B(1,\alpha)$ of $\mathbb{F}_{q^m}$ as follows:

- $B(0,1) = \{z \in \mathbb{F}_{q^m} : z(z-1)$ is a square in $\mathbb{F}_{q^m}\}$.
- $B(0,\alpha) = \{z \in \mathbb{F}_{q^m} : z(z-\alpha)$ is a square in $\mathbb{F}_{q^m}\}$.
- $B(1,\alpha) = \{z \in \mathbb{F}_{q^m} : (z-1)(z-\alpha)$ is a square in $\mathbb{F}_{q^m}\}$.

Note that using Theorem II.1 and Remark II.2 we obtain that the covering radius of the Melas code $M(m,q)$ is 2 if and only if

$$\mathbb{F}_{q^m} = B(0,1) \cup B(0,\alpha) \cup B(1,\alpha).$$

Let $B(0,1)^* = B(0,1) \setminus \mathbb{F}_q$, $B(0,\alpha)^* = B(0,\alpha) \setminus \mathbb{F}_q$ and $B(1,\alpha)^* = B(1,\alpha) \setminus \mathbb{F}_q$.

It follows from Theorem VI.7 that

$$\mathbb{F}_q = (B(0,1) \cap \mathbb{F}_q) \cup (B(0,\alpha) \cap \mathbb{F}_q) \cup (B(1,\alpha) \cap \mathbb{F}_q).$$

Hence it is enough to prove that the cardinality $|B(0,1)^* \cup B(0,\alpha)^* \cup B(1,\alpha)^*| = q^m - q$ in order to show that the covering radius is 2.

We observe that the same methods of Section V hold here. In particular the analogous statements of Lemmas V.1, V.2 and V.3 obtained by replacing 4 to α and 5 to q hold.

The following is a completion of Theorems III.1 and V.4.

Theorem VII.1. *Assume that* $\mathrm{char}\ \mathbb{F}_q$ *is odd and* $q > 5$. *Let* $m \geq 1$ *be an integer. Then the covering radius of* $M(m,q)$ *is* 2.

Proof: The proof of Theorem V.4 holds after changing 4 to α and 5 to q. ∎

VIII. Conclusion

In this paper we have completed the problem of the determination of the covering radius for an arbitrary Melas code $M(m,q)$, where $m \geq 1$ is an arbitrary positive integer and $\mathbb{F}_q$ is an arbitrary finite field (see (1)). This was known exactly only for $q = 2$ and $m \geq 2$. We introduce new techniques especially when the characteristic is odd.

It seems the techniques we develop are closely related to connections of quadratic polynomials and quadratic residues over finite fields. It would be interesting to find analogs of these results to higher degree polynomials and higher reciprocity laws.

Of course, another open problem is the extension of these techniques to other classes of codes in order to determine the covering radii exactly. Some natural choices for further investigation would be Zetterberg codes and antiprimitive BCH codes, some of their generalizations (see, for example, [10], [15], [20],[23]) and the extensions of the codes in [7].

Acknowledgment

The authors extend thanks to the anonymous reviewers and the associate editor for their valuable comments and suggestions, which improved the quality and presentation of the manuscript.

References

[1] A. Ashikhmin, and A. Barg: Bounds on the covering radius of linear codes, Des. Codes Cryptogr. **27(3)** (2002), 261–269.

[2] R. A. Brualdi, S. Litsyn and V. S. Pless: Covering radius, in *Handbook of Coding Theory*, North-Holland, Amsterdam, (1998), 755–826.

[3] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein: *Covering Codes*, North-Holland Mathematical Library, **54** North-Holland Publishing Co., Amsterdam, (1997).

[4] D.G. Cohen, M.G. Karpovsky, H. F. Mattson Jr., and J. R. Schatz: Covering radius-survey and recent results, IEEE Trans. Inf. Theory **31(3)** (1986), 328–343.

[5] D.G. Cohen, S.N. Litsyn, A.C. Lobstein, and H. F. Mattson Jr.: Covering radius 1985-1994, Appl. Algebra Eng. Commun. Comput. **8(3)** (1997), 173–239.

[6] P. Delsarte: Four fundamental parameters of a code and their combinatorial significance, Inf. Control. **23** (1973), 407–438.

[7] S.M. Dodunekov: Some quasiperfect double error correcting codes, Probl. Control Inf. Theory/Probl. Upr. Teor. Inf. **15(5)** (1986), 367–375.

[8] R. Dougherty and H. Janwa: Covering radius computations for binary cyclic codes, Math. Comp. **57** (1991), 415–434.

[9] D. E. Downie and N. J. A. Sloane: The covering radius of cyclic codes of length up to 31, IEEE Trans. Inform. Theory **31(3)** (1985), 446–447.

[10] G. van der Geer and M. van der Vlugt: Trace codes and families of algebraic curves, Math. Z. **209(2)** (1992), 307–315.

[11] T. Helleseth: On the covering radius of cyclic linear codes and arithmetic codes, Discret. Appl. Math. **11(2)** (1985), 157–173.
[12] J. Gu, and X. Cao: On the covering radius of Melas codes, International Journal of Pure and Applied mathematics **107(2)** (2016), 479–485.
[13] R. Lidl, and H. Niederreiter: *Finite Fields*, 2nd ed. Cambridge Univ. Press, Cambridge (1997).
[14] C.M. Melas: A cyclic code for double error correction, IBM J. Res. Develop. **4** (1960), 364–366.
[15] M. Moisio: The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, IEEE Trans. Inf. Theory **53(2)** (2007), 843–847.
[16] O. Moreno: Further results on quasiperfect codes related to the Goppa codes, Congr. Numer. **40** (1983), 249–256.
[17] O. Moreno and N.F. Castro: Divisibility properties for covering radius of certain cyclic codes, IEEE Trans. Inf. Theory **49(12)** (2003), 3299–3303.
[18] P. Solé: Packing radius, covering radius, and dual distance, IEEE Trans. Inf. Theory **41(1)** (1995), 268–272.
[19] H. Stichtenoth: *Algebraic Function Fields and Codes*, Springer GTM, New York, **254** (2009).
[20] H. Stichtenoth and C. Voß,: Generalized Hamming weights of trace codes, IEEE Trans. Inform. Theory **40(2)** (1994), 554–558.
[21] A. Tietäväinen: On the covering radius of long binary BCH codes, Discret. Appl. Math. **16(1)** (1987), 75–77.
[22] E. Velikova, and A. Bojilov: An upper bound on the covering radius of a class of cyclic codes, in *Eleventh International Workshop on Algebraic and Combinatorial Coding Theory*, Pamporovo, Bulgaria, June 16-22, (2008), 300–304.
[23] H. Zhu, M. Shi, X. Wang, T. Helleseth, The q-ary antiprimitive BCH codes, IEEE Trans. Inform. Theory, DOI: 10.1109/TIT.2021.3131810.

Minjia Shi received the Ph.D. degree from the Institute of Computer Network Systems, Hefei University of Technology, China, in 2010. From August 2012 to August 2013, he was a Visiting Researcher with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. From July 2016 to August 2016, he was a Visiting Researcher with Telecom Paris Tech, Paris, France. Later, he visited the Sobolev Institute of Mathematics in 2020. He has been a Professor of School of Mathematical Sciences at Anhui University since 2017. He is the author of over 100 journal articles and two books. His research interests include algebraic coding theory and cryptography.

Tor Helleseth received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973 to 1980, he was a Research Assistant with the Department of Mathematics, University of Bergen. From 1981 to 1984, he was with the Chief Head Quarters of Defense in Norway. Since 1984, he has been a Professor with the Department of Informatics, University of Bergen. During the academic years, from 1977 to 1978 and from 1992 to 1993, he was on sabbatical leave with the University of Southern California, Los Angeles. From 1979 to 1980, he was a Research Fellow with the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology. In 1997, he was elected as an IEEE fellow for his contributions to coding theory and cryptography. In 2004, he was elected as a member of Det Norske Videnskaps-Akademi. He was the Program Chairman of Eurocrypt 1993 and the Information Theory Workshop in 1997, Longyearbyen, Norway. He was the Program Co-Chairman of SEquences and Their Applications (SETA) in 1998, 2001, 2004, 2006, 2012, 2018, and 2020, and the IEEE Information Theory Workshop in Solstrand, Norway, in 2007. From 2007 to 2009, he served on the Board of Governors for the IEEE Information Theory Society. He served as an Associate Editor for coding theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1991 to 1993 and from 2012 to 2014.

Ferruh Özbudak received the B.S. degree in electrical and electronics engineering and the Ph.D. degree in mathematics from Bilkent University, Ankara, Turkey, in 1993 and 1997, respectively. He is currently a Professor with Middle East Technical University, Ankara. His research interests include algebraic curves, codes, sequences, cryptography, finite fields, and finite rings.

Patrick Solé received the Ingénieur and Docteur-Ingénieur degrees from the Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1984 and 1987, respectively, and the Habilitation à Diriger Des Recherches from the Université de Nice-Sophia Antipolis, Sophia Antipolis, France, in 1993. He has held visiting positions at Syracuse University, Syracuse, NY, USA, from 1987 to 1989, Macquarie University, Sydney, NSW, Australia, from 1994 to 1996, and Lille University, Lille, France, from 1999 to 2000. Since 1989, he has been a Permanent Member of the CNRS and became a Directeur de Recherche, in 1996. He is currently a member of the CNRS lab I2M, Marseilles, France. He is the author of more than 200 journal articles and five books. His research interests include coding theory (codes over rings, quasi-cyclic codes), interconnection networks (graph spectra, expanders), vector quantization (lattices), and cryptography (Boolean functions, pseudo random sequences). He was a co-recipient of the Best Paper Award for Information Theory, in 1995, given by the Information Theory Chapter of the IEEE. He was an Associate Editor of the Transactions from 1996 to 1999.

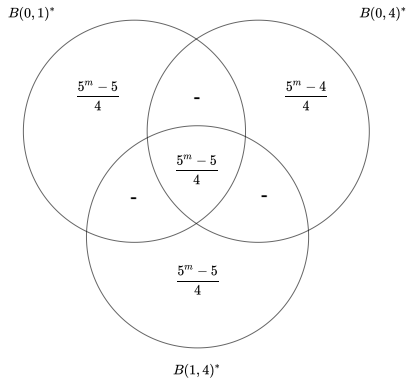

Fig. 1. The intersections of the sets in the proof of Theorem V.4

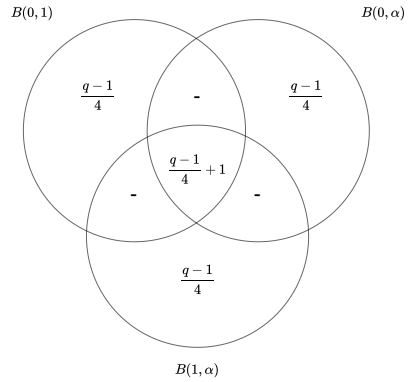

Fig. 2. The intersections of the sets in the proof of Theorem VI.7 for the case that $q \equiv 1 \mod 4$

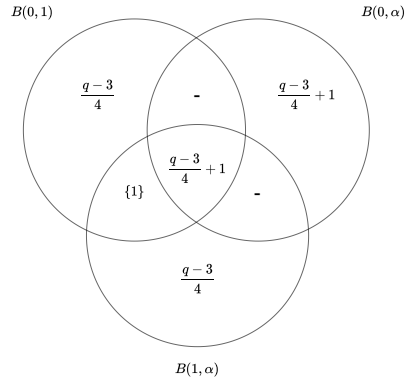

Fig. 3. The intersections of the sets in the proof of Theorem VI.7 for the case that $q \equiv 3 \mod 4$