International Journal of Pure and Applied Mathematics
Volume 107 No. 2 2016, 479-485
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v107i2.16

ON THE COVERING RADIUS OF MELAS CODES

Jingjing Gu[1 §], Xiwang Cao[2]
[1,2]College of Science
Nanjing University of Aeronautics and Astronautics
Jiangsu, 210016, P.R. CHINA

Abstract: Let $\mathbb{F}_q$ be the finite field of $q(=2^m)$ elements, $\mathcal{C}_{1,-1}$ the Melas code over $\mathbb{F}_q$. In this note, we show that the covering radius of $\mathcal{C}_{1,-1}$ is 3 if $q > 8$.

AMS Subject Classification: 94B15, 94B75
Key Words: covering radius, character sum, cyclic code, Melas code

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, $q = p^m$ be a prime power. Let $V = \mathbb{F}_q^n$ be a vector space of dimension n. A subspace of V with dimension k is called a *linear code* over $\mathbb{F}_q$ with parameter $[n, k]$. For $u = (x_1, \cdots, x_n), v = (y_1, \cdots, y_n) \in V$, the *(Hamming) distance* between u, v, denoted by $d(u, v)$ is defined by

$$d(u, v) = |\{i | x_i \neq y_i, 1 \leq i \leq n\}|.$$

The *minimum distance* of $\mathcal{C}$ is defined by

$$d(\mathcal{C}) = \min_{u,v \in \mathcal{C}} d(u, v).$$

The *(Hamming) weight* of a vector u is defined as the number of nonzero coordinates of u. If $\mathcal{C}$ is linear, then $d(\mathcal{C})$ is just the minimum weight of the codewords in $\mathcal{C}$. The *covering radius* of $\mathcal{C}$ is the least integer $R(\mathcal{C})$ such that the spheres of radius $R(\mathcal{C})$ around the codewords cover the entire space V.

Received: February 19, 2016
Published: April 11, 2016

url: www.acadpubl.eu
§Correspondence author

In coding theory, the covering radius is a fundamental parameter of a code and good covering codes have a number of applications and interconnections with other areas of mathematics [1] and [2]. Though the minimum distance plays a more central role in uses of codes for error-correction, the covering radius is also related to the error correction capability of the code, since if it is less than the distance, the code is maximal and no vector in the Hamming space can be added without worsening the codes distance [3]. Given an $[n, k]$ code $\mathcal{C}$, the problem to find the parameters of it is in general considered to be very difficult. Berlekamp, McEliece, and van Tilborg [4] have shown that the problem of finding the minimum distance of a general linear code is NP-complete. The problem of finding the covering radius of a general linear code seems to be an even more difficult problem [5], in fact, it is known to be both NP-hard and co-NP-hard, and hence strictly harder than any NP-complete problem unless NP = co-NP [3].

There are only a few classes of codes in which the covering radius are known. For example, Dougherty and Janwa [3] provide the covering radii of all binary cyclic codes of length ≤ 64. Downey and Sloane [6] give the covering radii of some cyclic codes of odd length < 31. Hou [7, 8, 9, 10, 11] investigates the covering radii of Reed-Muller codes systematically.

Let $\mathbb{F}_q$ be a finite field with $q(= p^m)$ elements. Let α be a primitive element of $\mathbb{F}_q$. Suppose that $m_\alpha(x)$ (resp. $m_{\alpha^{-1}}(x)$)$\in \mathbb{F}_p[x]$ is the minimal polynomial of α (resp. α^{-1}) over $\mathbb{F}_p$. The Melas code, $\mathcal{C}_{1,-1}$, is the cyclic code with generator polynomial $g(x) = m_\alpha(x)m_{\alpha^{-1}}(x)$. When $p = 2$, by making use of certain Hecke operators acting on spaces of cusp forms for the congruence subgroup $\Gamma_1(4) \subseteq SL_2(\mathbb{Z})$, Schoof and Vlugt [12] obtained the weight distribution of the Melas codes. If $m > 3$, and $d = 2^k + 1$ with $\gcd(k, m) = 1$, then it is known that the cyclic code with generator polynomial $g(x) = m_\alpha(x)m_{\alpha^d}(x)$ has covering radius 3, see [13]. When p is odd, Velikova and Bojilov [14] proved that the covering radius of $\mathcal{C}_{1,-1}$ is at most 3 if $q > 36$. In this note, we show that the covering radius of $\mathcal{C}_{1,-1}$ is 3 if $q > 8$.

2. Notations and Preliminaries

In this note, we fix q as 2^m and $\mathbb{F}_q$ is the finite field with q elements, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The absolute trace map tr_1^m is defined by

$$\mathrm{tr}_1^m(x) = x + x^2 + x^4 + \cdots + x^{2^{m-1}}, \quad \forall x \in \mathbb{F}_q.$$

For $a, b \in \mathbb{F}_q$, the Kloosterman sum $k_m(a, b)$ is defined by

$$k_m(a,b) = \sum_{x \in \mathbb{F}_q^*} (-1)^{\mathrm{tr}_1^m(ax+bx^{-1})}. \tag{1}$$

It is easy to check that $k_m(a, b) = k_m(1, ab) = k_m(ab, 1)$ holds for $a, b \in \mathbb{F}_q^*$, thus we simply denote $k_m(a)$ for $k_m(1, a) = k_m(a, 1)$. Also, $k_m(1, 0) = k_m(0, 1) = -1$, thus we define $k_m(0) = -1$. For the moments of Kloostrman sums, we have the following results, see [15]. For convenience, we define 0^{-1} as 0.

Lemma 1. (see [15]) *If $q = 2^m$, then*

$$\begin{aligned}
\sum_{a \in \mathbb{F}_q^*} k_m(a) &= 1; \\
\sum_{a \in \mathbb{F}_q^*} k_m(a)^2 &= q^2 - q - 1; \\
\sum_{a \in \mathbb{F}_q^*} k_m(a)^3 &= (-1)^m q^2 + 2q + 1; \\
\sum_{a \in \mathbb{F}_q^*} k_m(a)^4 &= 2q^3 - 2q^2 - 3q - 1.
\end{aligned}$$

Let $\mathcal{C}$ be a cyclic code with generator $g(x)$. In [5], Helleseth has the following result for computing the covering radius of $\mathcal{C}$.

Lemma 2. (see [6]) *Suppose that $\mathcal{C}$ is a cyclic code with generator*

$$g(x) = m_{i_1}(x) m_{i_2}(x) \cdots m_{i_t}(x),$$

$m_{i_j}(x)$ is the minimal polynomial of α^{i_j}, α is a primitive element of $\mathbb{F}_q$. Assume that $g(x)$ has no multiple roots. Then the covering radius is the least positive integer ρ such that for any $b_1, \cdots, b_t \in \mathbb{F}_q$ we can find $x_i \in \mathbb{F}_q$ for $1 \le i \le \rho$ where

$$\begin{cases}
x_1^{i_1} + \cdots + x_\rho^{i_1} &= b_1 \\
x_1^{i_2} + \cdots + x_\rho^{i_2} &= b_2 \\
\quad\vdots \qquad\qquad\quad &\vdots \quad \vdots \\
x_1^{i_t} + \cdots + x_\rho^{i_t} &= b_t.
\end{cases} \tag{2}$$

3. Main Result and the Proof

The main result of this note is the following theorem:

Theorem 1. *The covering radius of the Melas code is 3 if $q > 8$.*

Proof. By Lemma 2, we need to prove that there exists $\alpha, \beta \in \mathbb{F}_q$ such that the system of equations

$$\begin{cases} x_1 + x_2 &= \alpha \\ x_1^{-1} + x_2^{-1} &= \beta \end{cases} \tag{3}$$

has no solution x_1, x_2 in $\mathbb{F}_q$. Meanwhile for every pair of $\alpha, \beta \in \mathbb{F}_q$, the system of equations

$$\begin{cases} x_1 + x_2 + x_3 &= \alpha \\ x_1^{-1} + x_2^{-1} + x_3^{-1} &= \beta \end{cases} \tag{4}$$

has solutions $x_1, x_2, x_3 \in \mathbb{F}_q$.

Obviously, (3) has no solutions in $\mathbb{F}_q$ when $\alpha = 0$ and $\beta \neq 0$.

We denoted by $N_{\alpha,\beta}$ the number of solutions of the equation system (4) in $\mathbb{F}_q^n$ and by $N(f(x_1, ..., x_n) = c)$ the number of solutions of the equation $f(x_1, ..., x_n) = c$ in $\mathbb{F}_q^n$, where $f(x_1, ..., x_n) = c$ is a equation with coefficients in $\mathbb{F}_q^n$.

$$\begin{aligned} N_{\alpha,\beta} =& \frac{1}{q^2} \sum_{x_1,x_2,x_3 \in \mathbb{F}_q} \sum_{a,b \in \mathbb{F}_q} \chi_1 \left(b \left(x_1 + x_2 + x_3 - \alpha \right) \right) \\ & \times \chi_1 \left(a \left(x_1^{-1} + x_2^{-1} + x_3^{-1} - \beta \right) \right) \\ =& \frac{1}{q^2} \sum_{a,b \in \mathbb{F}_q} \chi_1 \left(\alpha b + \beta a \right) \left(\sum_{x \in \mathbb{F}_q} \chi_1 \left(a x^{-1} + b x \right) \right)^3 \\ =& \frac{1}{q^2} \left[\sum_{a \in \mathbb{F}_q} \chi_1 \left(\beta a \right) \left(\sum_{x \in \mathbb{F}_q} \chi_1 \left(a x^{-1} \right) \right)^3 \right. \\ & \left. + \sum_{ab \neq 0} \chi_1 \left(\alpha b + \beta a \right) \left(\sum_{x \in \mathbb{F}_q} \chi_1 \left(a x^{-1} + b x \right) \right)^3 \right]. \end{aligned}$$

Since

$$\sum_{a \in \mathbb{F}_q} \chi_1 \left(\beta a \right) \left(\sum_{x \in \mathbb{F}_q} \chi_1 \left(a x^{-1} \right) \right)^3 = q \cdot N(x_1^{-1} + x_2^{-1} + x_3^{-1} = \beta) = q^3$$

we have

$$\begin{aligned} N_{\alpha,\beta} &= \frac{1}{q^2}\left[q^3+\sum_{ab\neq 0}\chi_1(\alpha b+\beta a)\left(\sum_{x\in\mathbb{F}_q^*}\chi_1\left(ax^{-1}+bx\right)+1\right)^3\right] \\ &= q+\frac{1}{q^2}\sum_{t\neq 0}\sum_{b\neq 0}\chi_1\left(\alpha b+\beta t b^{-1}\right)\left(\sum_{x\in\mathbb{F}_q^*}\chi_1\left(t(bx)^{-1}+bx\right)+1\right)^3 \\ &= q+\frac{1}{q^2}\sum_{t\neq 0}\sum_{b\neq 0}\chi_1\left(\alpha b+\beta t b^{-1}\right)\left(K_m(t)+1\right)^3 \end{aligned}$$

Because $N_{1,0}=N_{0,1}=N_{\alpha,0}=N_{0,\beta}$, where $\alpha\neq 0$ and $\beta\neq 0$, we just need to consider the number of solutions of equations system (4) in the following three cases.

Case 1: $\alpha=0$, $\beta=0$.
In this case, we have

$$N_{0,0} = q+\frac{1}{q^2}\sum_{b\in\mathbb{F}_q^*}\sum_{t\in\mathbb{F}_q^*}(K_m(t)+1)^3$$

By Lemma 1, we obtain

$$\begin{aligned} N_{0,0} &= q+((-1)^m+3)(q-1) \\ &= \begin{cases} 3q-2, & \text{if } m \text{ is odd;} \\ 5q-4, & \text{if } m \text{ is even.} \end{cases} \end{aligned}$$

Case 2: $\alpha=1$, $\beta=0$.
Similarly, we can get the number of the solutions of the equations system (4) as in Case 1.

$$\begin{aligned} N_{1,0} &= q+\frac{1}{q^2}\sum_{b\in\mathbb{F}_q^*}\chi_1(b)\sum_{t\neq 0}\left(K_m(t)+1\right)^3 \\ &= q+((-1)^m+3)\sum_{b\in\mathbb{F}_q^*}\chi_1(b) \\ &= q+(-1)^{m+1}-3 \\ &= \begin{cases} q-2, & \text{if } m \text{ is odd;} \\ q-4, & \text{if } m \text{ is even.} \end{cases} \end{aligned}$$

Case 3: $\alpha = 1$, $\beta \neq 0$.

Now we consider the third condition that $\alpha = 1$, $\beta \neq 0$. As $z = 1-x-y$, the solutions of the equation system (4) are same as the solutions of the equation

$$x^{-1} + y^{-1} + (1 - x - y)^{-1} = \beta,$$

when $x \neq 0$, $y \neq 0$, $1 - x - y \neq 0$, we obtain

$$(\beta y + 1)x^2 + (\beta y + 1)(y + 1)x + y(y + 1) = 0. \tag{5}$$

when $y \neq \beta^{-1}$, $y \neq 1$, the equation (5) has a solution in $\mathbb{F}_q$ if and only if

$$\mathrm{tr}_1^m\left(\frac{(\beta y + 1)(y + 1)y}{(\beta y + 1)^2(y + 1)^2}\right) = \mathrm{tr}_1^m\left(\frac{y}{(\beta y + 1)(y + 1)}\right) = 0.$$

Let $f(y) = \frac{y}{(\beta y+1)(y+1)}$. If for $\forall y \in \mathbb{F}_q\backslash\{1, 0, \beta^{-1}\}$, $\mathrm{tr}_1^m(f(y)) = 1$, then we have

$$\left|\sum_{y\in\mathbb{F}_q\backslash\{1,0,\beta^{-1}\}} \chi_1(f(y))\right| = \left|\sum_{y\in\mathbb{F}_q\backslash\{1,0,\beta^{-1}\}} (-1)^{\mathrm{tr}_1^m(f(y))}\right| = q - 3.$$

However, by [16], one has

$$\left|\sum_{y\in\mathbb{F}_q\backslash\{1,0,\beta^{-1}\}} \chi_1(f(y))\right| \leq 2\sqrt{q} + 1.$$

This is a contradiction, thus there exists some $y \in \mathbb{F}_q\backslash\{1, 0, \beta^{-1}\}$, such that $\mathrm{tr}_1^m(f(y)) = 0$, and then the equation (4) has a solution in $\mathbb{F}_q$.

Therefore when $q > 8$, for any $\alpha \in \mathbb{F}_q^*$, $\exists y \in \mathbb{F}_q\backslash\{1, 0, \beta^{-1}\}$, such that the equation (5) have a solution.

In conclusion, for every pair of $\alpha, \beta \in \mathbb{F}_q$, the equation system (4) always has at least one solution in $\mathbb{F}_q$ if $q > 8$. □

Acknowledgements

Parts of this work were done during the second author was visiting Institute of Mathematics, Academia Sinica from May 2015 to August 2015 where he would like to express his grateful thankfulness to the financial support. X. Cao's work is also supported by the NNSF of China (11371011).

References

[1] R. Lidl, H. Niederriter, *Finite Fields*, Cambridge University Press, England (2008).

[2] Gèrard Cohen, Iiro Honkala, Simon Litsyn, Antoine Lobstein, *Covering Codes*, North-Holland Publishing Co., Holland (1997).

[3] R. Dougherty, H. Janwa, Covering radius computation for binary cyclic codes, *Math. Comp.*, **57**, No. 195 (1991), 415-434; **doi:** 10.1090/S0025-5718-1991-1079013-8.

[4] E.R. Berlekamp, R.J. McEliece, H.C.A. van Tilborg, On the inherent tractability of certain coding problems, *IEEE Trans. Inform. Theory*, **24**, No. 3 (1978), 384-386; **doi:** 10.1109/TIT.1978.1055873.

[5] T. Helleseth, On the covering radius of cyclic linear codes and arithmetic codes, *Discr. Appl. Math.*, **11**, No. 2 (1985), 157-173; **doi:** 10.1016/S0166-218X (85)80006-8.

[6] D. E. Downey, N. J. A. Sloane, The covering radius of cyclic codes of length up to 31, *IEEE Trans. Inform. Theory IT*, **31**, 3 (1985), 446-447; **doi:** 10.1109/TIT.1985.1057033.

[7] X. Hou, Some results on the covering radii of Reed-Muller codes, *IEEE Trans. Inform. Theory*, **39**, No. 2 (1993), 366-378; **doi:** 10.1109/18.212268.

[8] X. Hou, Further results on the covering radii of the Reed-Muller codes, *Des. Codes Cryptogr*, **3**, No. 2 (1993), 167-177; **doi:** 10.1007/BF01388415.

[9] X. Hou, On the covering radius of $R(1, m)$ in $R(3, m)$, *IEEE Trans. Inform. Theory*, **42**, No. 3 (1996), 1035-1037; **doi:** 10.1109/18.490572.

[10] X. Hou, Covering radius of the Reed-Muller code $R(1, 7)$-a simpler proof, *J. Combin. Theory A*, **74**, No. 0055 (1996), 337-341; **doi:** 10.1006/jcta.1996.0055.

[11] X. Hou, The covering radius of $R(1, 9)$ in $R(4, 9)$, *Des. Codes Cryptogr.* **8**, No. 3 (1996), 285-292; **doi:** 10.1023/A:1027399606196.

[12] R. Schoof, M. Van der Vlugt, Hecke operators and the weight distributions of certain codes, *J. Combin. Theory Ser. A.*, **57**, No. 2 (1991), 163-186; **doi:** 10.1016/0097-3165 (91)90016-A.

[13] O. Moreno, F. Castro, Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inf. Theory*, **49**, No. 12 (2003), 3299-3303; **doi:** 10.1109/TIT.2003.820033.

[14] E. Velikova, A. Bojilov, An upper bound on the covering radius of a class of cyclic codes1, *Eleventh International Workshop on Algebraic and Combinatorial Coding Theory*, Pamporovo, Bulgaria, June 16-22, 2008, 300-304.

[15] X. Cao, A note on the moments of Kloosterman sums, *Applicable Algebra in Engineering, Communication and Computing*, **20**, No. 5 (2009), 447-457; **doi:** 10.1007/s00200-009-0109-1.

[16] A.G. Shanbhag, P.V. Kumar, T. Helleseth, An upper bound for the extended Kloosterman sums over Galois rings, *Finite Fields Appl.*, **4**, No. 3 (1998), 218-238; **doi:** 10.1006/ffta.1998.0211.