Binary cyclic codes generated by m_1m_7

Citation for published version (APA):

van Lint, J. H., & Wilson, R. M. (1986). Binary cyclic codes generated by m_1m_7 . *IEEE Transactions on Information Theory*, 32(2), 283-283. <https://doi.org/10.1109/TIT.1986.1057166>

DOI:

[10.1109/TIT.1986.1057166](https://doi.org/10.1109/TIT.1986.1057166)

Document status and date:

Published: 01/01/1986

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Binary Cyclic Codes Generated by $m_1 m_7$

J. H. VAN LINT AND R. M. WILSON

Abstract—We show that binary cyclic codes of length $n = 2^m - 1$ with generator $g(x) = m_1(x)m_7(x)$ have minimum distance < 5 unless $m = 5$ (and possibly $m = 11, 13$, or 17).

I. INTRODUCTION

In [1] the authors studied the minimum distance of cyclic codes. It turned out that several codes of length $n = 2^m - 1$ with generator $m_1(x)m_i(x)$, where $m_s(x)$ denotes the minimal polynomial of ω^s (and ω is a primitive n th root of unity), have minimum distance five. For example, this is the case for m odd and $i = 13$ [1, ex. 9]. For several values of m we found by hand that the code with generator $m_1(x)m_7(x)$ is bad (i.e., $d = 3$ or 4). The aim of this correspondence is to show that this is always the case unless $m = 5$ (in which case, it is known that $d = 5$) and possibly $m \in \{11, 13, 17\}$, which could be checked by a computer search. Of course, this result itself is not very exciting. However, not many values of i exist for which such a result can be proved, except if it is trivial. The deep theorem which is used to prove our result makes the proof interesting.

Let us first consider some simple cases. The code C with generator $m_1(x)m_7(x)$ has zeros ω and ω^7 , that is, the code consists of the words $c(x)$ with $c(\omega) = c(\omega^7) = 0$. As usual, we indicate the position x^i by the element $\omega^i \in \mathbb{F} = \mathbb{F}_{2^m}$. If m is even, then an element $\zeta \neq 1$ exists in $\mathbb{F}$ such that $\zeta^3 = 1$. Then $1 + \zeta^7 + (\zeta + 1)^7 = 0$, and hence the positions $1, \zeta, \zeta + 1$ correspond to a codeword of weight three in C . This is the trivial part. If m is odd, then $3 \nmid 2^m - 1$. We apply the Hartmann–Tzeng bound (cf. [1, theorem 2]). Since each codeword has zeros $\omega, \omega^2, \omega^7, \omega^8$, the minimum distance of C is at least four. The cases $m = 3, m = 9$, and $m = 15$ are easily treated by hand because $\mathbb{F}$ contains $\mathbb{F}_8$ as a subfield. Let $\tau \in \mathbb{F}_8 \setminus \{1\}$ be such that $\text{tr}(\tau) = 1$. Then for $S := \{1, \tau, \tau^2, \tau^4\}$ we have $\sum_{x \in S} x = \sum_{x \in S} x^7 = 0$. Therefore, $d = 4$ for $m = 3, 9$, and 15 . As stated earlier, the cases $m = 5$ and $m = 7$ were treated in [1], and $m \in \{11, 13, 17\}$ still remain to be done. Our main result concerns $m \geq 18$.

Theorem 1: Let $n = 2^m - 1$, $m \geq 18$. The binary cyclic code C of length n with zeros ω^1, ω^7 (where ω is a primitive element of $\mathbb{F}_{2^m}$) has minimum distance $d \leq 4$.

Proof: In Section II we shall show that elements $\alpha, \beta \in \mathbb{F}$ exist such that $\alpha \notin \{\beta, \beta + 1\}$, $\{\alpha, \beta\} \cap \{0, 1\} = \emptyset$, and furthermore $a := \alpha^2 + \alpha$, $b := \beta^2 + \beta$ satisfy

$$a^2 + ab + b^2 = 1. \quad (1.1)$$

Let $S := \{\alpha, \beta, \alpha + 1, \beta + 1\}$. Note that $S \subset \mathbb{F}^*$, $|S| = 4$. Let

$\gamma := \alpha + \beta$. We have

$$\begin{aligned} (x + \alpha)(x + \alpha + 1)(x + \beta)(x + \beta + 1)(x + \gamma)(x + \gamma + 1) \\ = (x^2 + x + a)(x^2 + x + b)(x^2 + x + a + b) \\ = x^6 + x^5 + x^4 + x^3 + x^2 + x + ab(a + b). \end{aligned} \quad (1.2)$$

From (1.1) and (1.2) we find that $x \in S$ implies that

$$x^7 = 1 + (x + 1)(1 + ab(a + b)). \quad (1.3)$$

Since $\sum_{x \in S} x^0 = \sum_{x \in S} x = 0$ we find from (1.3) that also $\sum_{x \in S} x^7 = 0$. Therefore, the elements of S correspond to the positions of a codeword of weight four in C .

II. EXISTENCE OF THE PAIR $\{\alpha, \beta\}$

The hard part of our proof is showing that a pair $\{\alpha, \beta\}$ as used in the proof of Theorem 1 exists. This is a consequence of a deep result in algebraic geometry (Theorem 2 to follow), for which we need the following lemma.

Lemma 1: Let

$$\begin{aligned} f(X, Y) := Y^4 + (X^2 + X + 1)Y^2 + (X^2 + X)Y \\ + (X^4 + X^2 + 1). \end{aligned} \quad (2.1)$$

Then $f(X, Y)$ is *absolutely irreducible* over $\mathbb{F}$ (i.e., irreducible over every algebraic extension of $\mathbb{F}$).

Proof: Suppose $f(X, Y) = a(X, Y)b(X, Y)$ over the algebraic closure of $\mathbb{F}$. Then points (X, Y) exist such that $f, \partial f/\partial X$, and $\partial f/\partial Y$ vanish at (X, Y) . Now $\partial f/\partial X = Y(Y + 1)$ and $\partial f/\partial Y = X(X + 1)$ are both zero if and only if X and Y are both zero or one. However, at each of the corresponding four points (X, Y) the function f has value one.

For the proof of Theorem 1 we need a pair of elements $(\alpha, \beta) \in \mathbb{F}^2$ which satisfy (1.1), i.e., $f(\alpha, \beta) = 0$. The remaining conditions on α, β are satisfied if α, β are not elements of $\mathbb{F}_4$. We now apply the following modification of Weil's theorem, due to Schmidt (cf. [2], [3, III, theorem IA]).

Theorem 2: Suppose $f(X, Y) \in \mathbb{F}_q[X, Y]$ is absolutely irreducible and of total degree $d > 0$. Let N be the number of zeros of f in $\mathbb{F}_q^2$. If $q > 250d^5$, then $|N - q| < \sqrt{2}d^{5/2}q^{1/2}$.

In our case $q = 2^m$ ($m \geq 18$), and f is absolutely irreducible by Lemma 1. The total degree of f is four, so $q > 250d^5$. In all cases there are obviously many pairs satisfying the conditions of Theorem 1.

ACKNOWLEDGMENT

We thank A. E. Brouwer for valuable remarks.

REFERENCES

- [1] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-32, no. 1, pp. 23–40, Jan. 1986.
- [2] W. M. Schmidt, "Zur Methode von Stepanov," *Acta Arith.*, vol. 24, pp. 347–367, 1973.
- [3] —, *Equations Over Finite Fields*, Springer Lecture Notes in Math., vol. 536. Berlin, Germany: Springer-Verlag, 1976.

Manuscript received June 19, 1985; revised August 27, 1985.

J. H. van Lint is with the Department of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, The Netherlands.

R. M. Wilson is with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA.

IEEE Log Number 8406628.