Journal of Combinatorial Theory, Series A **93**, 168–172 (2001)
doi:10.1006/jcta.2000.3064, available online at http://www.idealibrary.com on IDEAL®

NOTE

Maximal Arcs in Projective Three-Spaces and Double-Error-Correcting Cyclic Codes

Henk D. L. Hollmann

Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands
E-mail: hollmann@natlab.research.philips.com

and

Qing Xiang[1]

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716
E-mail: xiang@math.udel.edu

Communicated by the Managing Editors

Received August 30, 1999

Using maximal arcs in $PG(3, 2^m)$, we give a new proof of the fact that the binary cyclic code $C^{(m)}_{1, 2^h-2^h+1}$, the code of length 2^m-1 with defining zeroes α and α^t, $t=2^{2h}-2^h+1$, where α is a primitive element in GF(2^m), is 2-error-correcting when $\gcd(m, h)=1$. © 2001 Academic Press

1. INTRODUCTION

Let $C^{(m)}_{1, t}$ denote the binary cyclic code of length 2^m-1 with defining zeroes α and α^t, where α is a primitive element in GF(2^m). For example, $C^{(m)}_{1, 3}$ is the 2-error-correcting binary BCH code of length $n=2^m-1$. It has minimum distance $\geqslant 5$ (and equal to 5 except when $m=3$, in which case the code has only two codewords, namely, the zero and all-one codewords; hence it has minimum distance 7). The problem of deciding when such a code $C^{(m)}_{1, t}$ is 2-error-correcting has been studied extensively in [6, 8–10]. One of the most interesting cases (sometimes called the *Kasami case*) arises when $t=2^{2h}-2^h+1$ with $\gcd(m, h)=1$. There are several proofs that these *Kasami codes* are 2-error-correcting [6, 8]. These proofs involve quite a bit

[1] Partially supported by NSA Grant MDA 904-99-1-0012.

0097-3165/01 $35.00

of computations, and one proof needs to distinguish between the cases where m is odd and m is even. In this note we give a short new proof by using maximal arcs in $PG(3, 2^m)$, the projective 3-space over $GF(2^m)$.

2. THE NEW PROOF

We first state the result we want to prove.

THEOREM 1. *Let* $m \geqslant 4$, $t = 2^{2h} - 2^h + 1$ *and* $\gcd(m, h) = 1$. *Then* $C_{1,t}^{(m)}$ *has minimum distance* 5.

We remind the reader that a set of k points in $PG(r, q)$, q a prime power, $k \geqslant r + 1$, is called a k-arc if no $r + 1$ of the k points are in some hyperplane. So in $PG(3, q)$, a k-arc is a set of k points no four of which are coplanar. It is known that in $PG(3, q)$, q any prime power, the maximum value of k for which k-arcs exist is $q + 1$ [3, 12]. The starting point of our proof is the following $(2^m + 1)$-arc in $PG(3, 2^m)$.

LEMMA 1. *For* $q = 2^m$, *the collection of points*

$$\mathscr{C}(2^h) = \{(1, x, x^{2^h}, x^{2^h+1}) \mid x \in GF(q)\} \cup \{(0, 0, 0, 1)\}$$

is a $(q + 1)$*-arc in* $PG(3, q)$ *if and only if* $\gcd(m, h) = 1$.

The proof of this lemma can be found in [7, p. 250; 11, p. 226]. The key point of the proof in [7, 11] is the fact that $PGL(2, q)$ leaves invariant the set $\mathscr{C}(2^h)$, hence acts triply transitively on $\mathscr{C}(2^h)$. To make this note self-contained, we offer the following simple proof.

Proof of Lemma 1. First, if $\mathscr{C}(2^h)$ is an arc in $PG(3, q)$, then for any $x \in GF(q)$, $x \neq 0, 1$, the four points $(1, 0, 0, 0)$, $(1, 1, 1, 1)$, $(0, 0, 0, 1)$, $(1, x, x^{2^h}, x^{2^h+1})$ are not coplanar. Hence

$$\det \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & x & x^{2^h} & x^{2^h+1} \end{vmatrix} = x + x^{2^h} \neq 0$$

for all $x \in GF(q)$, $x \neq 0, 1$. Therefore, $\gcd(m, h) = 1$.

Now, let $\tau = 2^h$ and $\gcd(m, h) = 1$. We want to show that $\mathscr{C}(\tau)$ is a $(q + 1)$-arc. Let $P(x) = (1, x, x^\tau, x^{\tau+1})$ for $x \in GF(q)$, and $P(\infty) = (0, 0, 0, 1)$. Then $\mathscr{C}(\tau) = \{P(x) \mid x \in GF(q) \cup \{\infty\}\}$. Let (c, d, a, b) be any

nonzero vector in $\mathrm{GF}(q)^4$. Then for $x \in \mathrm{GF}(q)$, we have that $P(x)$ is contained in the plane $H = (c, d, a, b)^\perp$ if and only if

$$c + dx + ax^\tau + bx^{\tau+1} = 0. \tag{1}$$

Now, putting

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we note that the equation (1) holds if and only if

$$A \begin{pmatrix} 1 \\ x \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ x^\tau \end{pmatrix} \tag{2}$$

for some $\lambda \in \mathrm{GF}(q)$. (Here λ depends on x.) Using the fact that the map $X \mapsto X^\tau$ is a field automorphism, from (2) we conclude that for each k,

$$A^{\tau^{k-1}} \begin{pmatrix} 1 \\ x^{\tau^{k-1}} \end{pmatrix} = \lambda^{\tau^{k-1}} \begin{pmatrix} 1 \\ x^{\tau^k} \end{pmatrix}. \tag{3}$$

Now since $\gcd(h, m) = 1$, there exists an integer h' such that $hh' \equiv 1 \bmod m$. Let

$$B = A^{\tau^{h'-1} + \cdots + \tau + 1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

for some $c', d', a', b' \in \mathrm{GF}(q)$. Since $x^{\tau^{h'}} = x^{2^{hh'}} = x^2$ for all $x \in \mathrm{GF}(q)$, from repeated applications of (3) we find that

$$B \begin{pmatrix} 1 \\ x \end{pmatrix} = \mu \begin{pmatrix} 1 \\ x^{\tau^{h'}} \end{pmatrix} = \mu \begin{pmatrix} 1 \\ x^2 \end{pmatrix}$$

with $\mu = \lambda^{\tau^{h'-1} + \cdots + \tau + 1}$, which in turn is equivalent to

$$c' + d'x + a'x^2 + b'x^3 = 0. \tag{4}$$

Now we distinguish two cases. If $\det A = ad - bc = 0$, we may assume that $d \neq 0$ (otherwise, it leads to trivial cases), then by multiplying (2) by d and using $ad = bc$, we see that (2) implies $(c + dx)(d + bx^\tau) = 0$, so in that case (2) has at most two solutions. On the other hand, if $\det A \neq 0$, then $B \neq 0$, hence x is a solution of the nontrivial cubic equation $c' + d'x + a'x^2 + b'x^3 = 0$, which has at most three solutions in $\mathrm{GF}(q)$. Moreover, we remark that $P(\infty)$ is contained in the plane H if and only if $b = 0$; in that case the matrix A, and hence also B, is lower-triangular, so that the equation (4) is quadratic and has at most two solutions in $\mathrm{GF}(q)$. In summary, we have shown that no four points of $\mathscr{C}(\tau)$ are coplanar. This completes the proof. ∎

We remark that Casse and Glynn [4] proved that in $PG(3, 2^m)$, $m > 2$, in fact every $(2^m + 1)$-arc is projectively equivalent to some $\mathscr{C}(2^h)$, $\gcd(m, h) = 1$.

Before starting the proof of Theorem 1, we introduce some notation. Let $\mathbf{F}$ be a finite field of characteristic 2, let α be an nth root of 1 in some extension of GF(2), and let $E \subseteq \mathbf{Z}_n$. We define

$$C(\mathbf{F}, n, E, \alpha) = \{c(x) \in \mathbf{F}[x] \bmod (x^n - 1) \mid c(\alpha^e) = 0, e \in E\}$$

to be the cyclic code of length n over $\mathbf{F}$ with zeroes α^e, $e \in E$.

Proof of Theorem 1. Let $n = 2^m - 1$. Since $\mathscr{C}(2^h)$ is an arc in $PG(3, 2^m)$, translating the arc property into coding language we see that the code $C_1 = C(\mathrm{GF}(2^m), n, \{0, 1, 2^h, 2^h + 1\}, \alpha)$ is an MDS code over $\mathrm{GF}(2^m)$, that is, C_1 has minimum distance 5. Since $\gcd(m, h) = 1$, replacing the primitive element α of $\mathrm{GF}(2^m)$ by $\alpha^{2^h - 1}$, we see that the code $C_2 = C(\mathrm{GF}(2^m), n, \{0, 2^h - 1, 2^{2h} - 2^h, 2^{2h} - 1\}, \alpha)$ also has minimum distance 5. Using the monomial transformation $(c_0, c_1, \cdots, c_{2^m - 2}) \mapsto (c_0, c_1 \alpha^{-1}, \cdots, c_{2^m - 2} \alpha^{-(2^m - 2)})$, we see that the code C_2 is equivalent to $C_3 = C(\mathrm{GF}(2^m), n, \{1, 2^h, 2^{2h} - 2^h + 1, 2^{2h}\}, \alpha)$. Therefore the code C_3 also has minimum distance 5. As a subfield subcode of C_3, the code $C = C(\mathrm{GF}(2), n, \{1, 2^h, 2^{2h} - 2^h + 1, 2^{2h}\}, \alpha)$ has minimum distance at least 5. A closer look reveals that the code C is nothing but the code $C_{1,t}^{(m)}$, $t = 2^{2h} - 2^h + 1$, therefore $C_{1,t}^{(m)}$ has minimum distance at least 5. Finally, it is well-known [1, 10] that $C_{1,t}^{(m)}$, $m \geqslant 4$, has minimum distance at most 5. The theorem now follows. ∎

Remarks. (1) We remark that it is known [2] that the code $C_{1,t}^{(m)}$ has minimum distance 5 if and only if the function $x^t + (x+1)^t : \mathrm{GF}(2^m) \to \mathrm{GF}(2^m)$ is two-to-one. Therefore the above proof of Theorem 1 also gives a new proof that the function

$$f(x) = 1 + x^{2^{2h} - 2^h + 1} + (1 + x)^{2^{2h} - 2^h + 1} : \mathrm{GF}(2^m) \to \mathrm{GF}(2^m),$$

$\gcd(m, h) = 1$, is two-to-one.

(2) We also remark that the function $f(x)$ is closely related to the Müller–Cohen–Matthews polynomials $P_h(x)$ defined as follows. Let h, m be two positive integers. Define

$$P_h(x) = x(1 + x + x^3 + x^7 + \cdots + x^{2^{h-1} - 1})^{2^h + 1}.$$

It is shown in [5] that when h is odd, $P_h(x)$ is a permutation polynomial on $\mathrm{GF}(2^m)$ for any m with $\gcd(h, m) = 1$. By direct computations, we see that as functions from $\mathrm{GF}(2^m)$ to itself, we have $f(x) = P_h(x + x^2)$. So the

above proof of Theorem 1 at least proves that the polynomial $P_h(x)$ is one-to-one on the trace zero hyperplane of $\mathrm{GF}(2^m)$, that is, for any $x, y \in \mathrm{GF}(2^m)$, $\mathrm{tr}(x) = \mathrm{tr}(y) = 0$, if $P_h(x) = P_h(y)$, then $x = y$. Here tr is the trace from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$.

(3) Another important case in which the cyclic codes $C_{1,t}^{(m)}$ are 2-error-correcting arises when $t = 2^h + 1$ with $\gcd(m, h) = 1$. We note that one can also prove these *Gold codes* to be 2-error-correcting in a similar way, now starting from the translation hyperoval $\{(1, x, x^{2^h}) \mid x \in \mathrm{GF}(2^m)\} \cup \{(0, 1, 0), (0, 0, 1)\}$ in $PG(2, 2^m)$. Indeed, this hyperoval gives an MDS code, now with minimum distance 4, and the Gold code $C_{1,2^h+1}^{(m)}$, being a subfield subcode of a code equivalent to this MDS code, has minimum distance at least four. Then we use the well-known and easily proved fact (see, e.g., [10]) that a Gold code has odd minimum distance.

REFERENCES

1. A. E. Brouwer and L. M. G. M. Tolhuizen, A sharpening of the Johnson bound for binary linear codes, *Des. Codes Cryptogr.* **3** (1991), 95–98.
2. C. Carlet and P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* **15** (1998), 125–156.
3. L. R. A. Casse, A Solution to B. Segre's problem $I_{r,q}$, *Atti Accad. Naz. Lincei Rend.* **46** (1969), 13–20.
4. L. R. A. Casse and D. G. Glynn, The solution to Beniamino Segre's problem $I_{r,q}$, $r = 3$, $q = 2^h$, *Geom. Dedicata* **13** (1982), 157–163.
5. S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, *Trans. Amer. Math. Soc.* **345** (1994), 897–909.
6. H. Dobbertin, Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: The Welch case, *IEEE Trans. Inform. Theory*, to appear.
7. J. W. P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Clarendon Press, Oxford, 1985.
8. H. Janwa and R. M. Wilson, Hyperlane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes, *in* "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes—Proceedings AAECC-10" (G. Cohen, T. Mora, and O. Moreno, Eds.), Lecture Notes in Computer Science, Vol. 673, Springer-Verlag, New York/Berlin, 1993.
9. H. Janwa, G. McGuire, and R. M. Wilson, Double error-correcting codes and absolutely irreducible polynomials over GF(2), *J. Algebra* **178** (1995), 665–676.
10. J. H. van Lint and R. M. Wilson, On the minimum distance of cyclic codes, *IEEE Trans. Inform. Theory*, **32** (1986), 23–40.
11. H. Lüneburg, Translation planes, Springer, Berlin/Heidelberg/New York, 1980.
12. B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* **39** (1955), 357–379.