Designs, Codes and Cryptography, 4, 171–175 (1994)

A Counter-Example to a Recent Result on the q-ary Image of a q^s-ary Cyclic Code

GÉRALD E. SÉGUIN
Department of Electrical and Computer Engineering, Royal Military College of Canada, Kingston, Ontario, Canada K7K 5L0

Communicated by S. Vanstone
Received September 9, 1992.

Abstract. We show, by means of a counter-example, that the necessary and sufficient conditions given in a recent paper [3] in order for the q-ary image of a q^s-ary cyclic code to be cyclic are incorrect.

1. Introduction

Let C be an $[v, k]$ cyclic code defined over $\mathbf{F}_{q^s}$ and let $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{s-1})$ be a basis for $\mathbf{F}_{q^s}$ over $\mathbf{F}_q$. If $a(x) = \Sigma_0^{v-1} a_i x^i$ is a polynomial over $\mathbf{F}_{q^s}$ we define $\phi_\beta(a(x))$ by setting:

$$\phi_\beta(a(x)) = \sum_0^{v-1} \phi_\beta(a_i) Y^{is} \tag{1}$$

where

$$\phi_\beta(a_i) = \sum_{j=0}^{s-1} a_{i,j} Y^j \tag{2}$$

and where

$$a_i = \sum_{j=0}^{s-1} a_{i,j}\beta_j, \qquad 0 \le i < v, \quad a_{i,j} \in F_q \tag{3}$$

Finally, the q-ary image of C with respect to the basis $\underline{\beta}$ is:

$$\phi_\beta(C) = \{\phi_\beta(a(x)) \mid a(x) \in C\}. \tag{4}$$

The problem is to find simple necessary and sufficient conditions on C and $\underline{\beta}$ in order for $\phi_\beta(C)$ to be a q-ary cyclic code. This problem was originally considered by Hanan and Palermo [1] and subsequently by MacWilliams [2]. Recently, Leonard [3] published a solution to this problem. In the next section, we provide a counter-example to Leonard's theorem, hence showing that it is incorrect.

2. A Counter-Example

First we reproduce Leonard's theorem as given in reference [3]:

THEOREM (*Leonard*): *Let* $g(x) \in \mathbf{F}_{q^s}[x]$ *be a canonic generator of a* $[v, k]$ *cyclic code over* $\mathbf{F}_{q^s}$. *Let* $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{s-1})$ *be a basis for* $\mathbf{F}_{q^s}$ *over* $\mathbf{F}_q$ *(with* $\beta_0 = 1$*) and define* $\beta(x) = \Sigma_0^{s-1} \overline{\beta}_{s-1-j} X^j$. *Then* $\phi_\beta(C)$, ϕ_β *as defined in the introduction, is a cyclic code over* $\mathbf{F}_q$ *of length sv if, and only if,* $g(x) = d(x)h(x)$, $h(x) \in \mathbf{F}_q[x]$ *and there exists an* $\alpha \in \mathbf{F}_{q^s}$, $t = \deg m_\alpha(x)$, $m_\alpha(x)$ *is the minimal polynomial of* α *over* $\mathbf{F}_q$ *such that either:*

$$d(x) = x - \alpha^t,\ d'(x) = m_{\alpha^t}(x)/x - \alpha^t,\ \beta(x) = \frac{x^t - \alpha^t}{x - \alpha} B(x),$$

$$\phi_\beta(d(x)) = m_\alpha(Y),\ \beta'(x) = \frac{m_\alpha(x)}{x - \alpha} B(x), \tag{1}$$

or,

$$d'(x) = x - \alpha^t,\ d(x) = m_{\alpha^t}(x)/x - \alpha^t,\ \beta'(x) = \frac{x^t - \alpha^t}{x - \alpha} B(x),$$

$$\phi(d(x)) = m_{\alpha^t}(Y),\ \beta'(x) = \frac{m_\alpha(x)}{x - \alpha} B(x), \tag{2}$$

Remark. We have stated the above theorem as it appears in [3], but clearly case (2) contains errors since (1) and (2) should be duals of each other. In the sequel, we use case (1) only.

Counter-example. Using the techniques presented in [4], it is possible to construct any number of counter-examples to the above-stated result, one of which we now give.

In this example, $v = 7$, $q = 2$, $s = 6$ and C is the 64-ary (7, 2) cyclic code generated by $g(x) = x^7 - 1/(x + \rho^{27})(x + \rho^{54}) = (x + \rho^{45})(x + 1)(x^3 + x^2 + 1) = \rho^{45} + \rho^9 x + \rho^9 x^2 + x^3 + \rho^{45} x^4 + x^5$ where ρ is a zero of the primitive polynomial $1 + x + x^6$. The elements of $\mathbf{F}_{64}$ may be found on page 562 of Lin and Costello [5].

Next, consider $\underline{\beta} = (1, \rho^{44}, \rho^{43}, \rho^{54}, \rho^{35}, \rho^{34})$. Using the table in [5], we may express β_i as a binary linear combination of $1, \rho, \ldots, \rho^5$ obtaining the corresponding 6×6 binary matrix:

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

and it may be verified that,

$$B^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

is indeed its inverse. This confirms that β is a basis for $\mathbf{F}_{64}$ over $\mathbf{F}_2$.

It now follows that $d(x) = \boldsymbol{\rho}^{45} + x$, $\overline{h(x)} = (1 + x)(1 + x^2 + x^3)$, $g(x) = d(x)h(x)$ and so $\alpha^t = \boldsymbol{\rho}^{45}$. We compute $\phi_\beta(d(x))$ to be

$$\phi_\beta(d(x)) = 1 + Y^2 + Y^4 + Y^5 + Y^6 \tag{5}$$

and it may be verified that

$$\phi_\beta(d(x)) = m_{\rho^{60}}(Y) \tag{6}$$

and so $\alpha = \boldsymbol{\rho}^{60}$ and $t = 6$. As a check, we have that $\alpha^t = (\boldsymbol{\rho}^{60})^6 = \boldsymbol{\rho}^{45}$. Next we compute $x^t - \alpha^t/x - \alpha = x^6 - \boldsymbol{\rho}^{45}/x - \boldsymbol{\rho}^{60}$ to be

$$\boldsymbol{\rho}^{48} + \boldsymbol{\rho}^{51}x + \boldsymbol{\rho}^{54}x^2 + \boldsymbol{\rho}^{57}x^3 + \boldsymbol{\rho}^{60}x^4 + x^5 \tag{7}$$

The basis polynomial $\beta(x)$ is

$$\beta(x) = \boldsymbol{\rho}^{34} + \boldsymbol{\rho}^{35}x + \boldsymbol{\rho}^{54}x^2 + \boldsymbol{\rho}^{43}x^3 + \boldsymbol{\rho}^{44}x^4 + x^5 \tag{8}$$

which is clearly not divisible by $x^t - \alpha^t/x - \alpha$. Hence, according to Leonard's theorem $\phi_\beta(C)$ is *not* cyclic.

We now show, by direct computation, that $\phi_\beta(C)$ is indeed a binary [42, 12] cyclic code. Representing $\beta_i g(x)$ by corresponding vector of exponents of $\boldsymbol{\rho}$ which figure as the coefficients, we obtain,

$$\begin{array}{ll} (45,\ 9,\ 9,\ 0,\ 45,\ 0,\ -\infty) & \leftrightarrow\ g(x) \\ (26,\ 53,\ 53,\ 44,\ 26,\ 44,\ -\infty) & \leftrightarrow\ \beta_1 g(x) \\ (25,\ 52,\ 52,\ 43,\ 25,\ 43,\ -\infty) & \cdot \\ (36,\ 0,\ 0,\ 54,\ 36,\ 54,\ -\infty) & \cdot \\ (17,\ 44,\ 44,\ 35,\ 17,\ 35,\ -\infty) & \cdot \\ (16,\ 43,\ 43,\ 34,\ 16,\ 34,\ -\infty) & \leftrightarrow\ \beta_5 g(x). \end{array} \tag{9}$$

We may now easily compute $\phi_\beta(\beta_i g(x))$ using the matrix B^{-1} and the table in [5] obtaining:

$$\begin{array}{l} (101011\ \ 001011\ \ 001011\ \ 100000\ \ 101011\ \ 100000\ \ 000000) \\ (111110\ \ 101110\ \ 101110\ \ 010000\ \ 111110\ \ 010000\ \ 000000) \\ (011111\ \ 010111\ \ 010111\ \ 001000\ \ 011111\ \ 001000\ \ 000000) \\ (100100\ \ 100000\ \ 100000\ \ 000100\ \ 100100\ \ 000100\ \ 000000) \\ (010010\ \ 010000\ \ 010000\ \ 000010\ \ 010010\ \ 000010\ \ 000000) \\ (001001\ \ 001000\ \ 001000\ \ 000001\ \ 001001\ \ 000001\ \ 000000) \end{array} \tag{10}$$

These, along with the 6 vectors obtained by cyclically shifting each of these by 6 positions to the right, will form a generator matrix for $\phi_\beta(C)$. Setting $G(Y) = \phi_\beta(g(x))$ we have:[1]

$$G(Y) = 1 + Y^2 + Y^4 + Y^5 + Y^8 + Y^{10} + Y^{11} + Y^{14} + Y^{16} + Y^{17} + Y^{18} + Y^{24} + Y^{26} + Y^{28} + Y^{29} + Y^{30} = (1 + Y)^2(1 + Y + Y^3)^2(1 + Y + Y^2)^2 (1 + Y + Y^2 + Y^4 + Y^6)^2(1 + Y^2 + Y^4 + Y^5 + Y^6)$$

and since,

$$Y^{42} + 1 = [(1 + Y)(1 + Y + Y^2)(1 + Y + Y^3)(1 + Y^2 + Y^3)(1 + Y + Y^2 + Y^4 + Y^6) (1 + Y^2 + Y^4 + Y^5 + Y^6)]^2$$

we see that $G(Y)$ divides $Y^{42} + 1$.

It is now easily verified that the array (10) corresponds to:

$$\begin{aligned} \phi_\beta(g(x)) &= G(Y) \\ \phi_\beta(\beta_1 g(x)) &= (1 + Y)G(Y) \\ \phi_\beta(\beta_2 g(x)) &= Y(1 + Y)G(Y) \\ \phi_\beta(\beta_3 g(x)) &= (1 + Y^2 + Y^3)G(Y) \\ \phi_\beta(\beta_4 g(x)) &= Y(1 + Y^2 + Y^3)G(Y) \\ \phi_\beta(B_5 g(x)) &= Y^2(1 + Y^2 + Y^3)G(Y). \end{aligned} \tag{11}$$

Hence, all the vectors in array (10), along with their cyclic shifts by 6 positions, are divisible by $G(Y)$, $G(Y)$ divides $Y^{42} + 1$ and has degree 30. Consequently, $\phi_\beta(C)$ is the binary (42, 12) cyclic code generated by $G(Y)$.

3. Conclusion

We have shown, by means of a counter-example, that the necessary and sufficient conditions presented by Leonard in order for the q-ary image of a q^s-ary cyclic code to be cyclic are incorrect. Hence, this problem remains an open problem.

Notes

1. The factorization may be easily obtained using the software package Maple.

References

1. M. Hanan and F.P. Palermo, On cyclic codes for multi-phase data transmission systems, *SIAM J. Appl. Math.*, Vol. 12, pp. 794–804, (1964).
2. F.J. MacWilliams, On binary cyclic codes which are also cyclic codes over $GF(2^S)$, *SIAM J. Appl. Math.*, Vol. 19, pp. 75–95, (1970).
3. D.G. Leonard, Linear cyclic codes of wordlength v over $GF(q^s)$ which are also cyclic codes of wordlength sv over $GF(q)$, *Designs, Codes and Cryptography*, Kluwer Academic Publishers, Vol. 1, pp. 183–189, (1991).
4. G.E. Séguin, The q-ary Image of a q^m-ary Cyclic Code, presented at the 16th Biennial Symposium on Communications held at Queen's University, Kingston, Ontario, May 27–29, (1992).
5. S. Lin and D.J. Costello, *Error Control Coding: Fundamentals and Applications*, Englewood Cliffs, NJ: Prentice-Hall, Inc., (1983).