Des Codes Crypt (2007) 42:327–334
DOI 10.1007/s10623-007-9038-9

New classes of 2-weight cyclic codes

Gerardo Vega · Jacques Wolfmann

Received: 7 June 2006 / Revised: 29 December 2006 /
Accepted: 5 January 2007 / Published online: 23 February 2007

Abstract We introduce new classes of 2-weight cyclic codes which are direct sums of 1-weight irreducible cyclic codes

Keywords Cyclic codes · Irreducible cyclic codes · 2-weight projective cyclic codes

AMS Classifications 94B

1 Introduction

We assume that the reader is familiar with elementary definitions and results of the theory of linear and cyclic codes over finite fields (a reference could be [3] for codes and [4] for finite fields). First, we recall the useful definitions.

A linear code is said to be projective if the minimum weight of its dual code is at least 3. This means that the columns of a generator matrix are non-zero distinct representatives of the one-dimensional subspaces of $\mathbb{F}_q^k$ (the projective points) where k is the dimension of the code.

A linear code is a N-weight code if the number of non-zero weights of this code is N.

A cyclic code is irreducible if its check polynomial is irreducible (its polynomial representation is a minimal ideal).

Communicated by G. McGuire.

G. Vega
Dirección General de Servicios de Cómputo Académico, Universidad Nacional Autónoma de México, Mexico DF 04510, Mexico
e-mail: gerardo@servidor.unam.mx

J. Wolfmann (✉)
GRIM, Université du Sud Toulon-Var, 83957 La Garde cedex, France
e-mail: wolfmann@univ-tln.fr

When the length of such a code is $q^k - 1$ and the check polynomial is the minimal polynomial over $\mathbb{F}_q$ of a primitive root of $\mathbb{F}_{q^k}$, then the code is called a simplex code and this is a 1-weight code with $(q-1)q^{k-1}$ as unique non-zero weight.

In [6] it was proved that if C is a 2-weight projective cyclic code of dimension t over $\mathbb{F}_q$, then either

$(\mathcal{C}_1)$: C is irreducible

or,

$(\mathcal{C}_2)$: if $q \neq 2$, C is the direct sum of two 1-weight irreducible cyclic codes of length $n = \lambda(\frac{q^t-1}{q-1})$ where λ divides $q-1$ and $\lambda \neq 1$.

In this second case, the two non-zero weights of C are $(\lambda-1)q^{t-1}$ and λq^{t-1}. (direct sum here means direct sum as vector spaces).

An infinite class of 2-weight cyclic projective codes which are irreducible is known for any q (deduced from semi-primitive codes) but only numerical examples are known for the second case. An open problem was to find infinite classes in this case.

First, in order to construct codes satisfying $(\mathcal{C}_2)$, we need to know what are the possible 1-weight irreducible cyclic codes we can use. The condition for a code of dimension k over $\mathbb{F}_q$ to have a length equal to $n = \lambda(\frac{q^k-1}{q-1})$ where λ divides $q-1$ is not sufficient to be a 1-weight code, even if $\lambda = 1$. For example, the non-degenerate irreducible cyclic code over $\mathbb{F}_3$ of length $n = 40 = \frac{3^4-1}{3-1}$ and check polynomial $x^4 + x^2 + 2x + 1$, is a 2-weight code with non-zero weights 24 and 30 (this is a semi-primitive code).

In Sect. 2, we characterize the 1-weight codes of length $\lambda(\frac{q^k-1}{q-1})$ where λ divides $q-1$ and in Sect. 3, we introduce new classes of 2-weight cyclic codes satifying condition $(\mathcal{C}_2)$.

From now on, we assume $q \neq 2$. We consider cyclic codes of length n over $\mathbb{F}_q$ with $(n, q) = 1$ and we suppose that such a code is non trivial, that is, different from $\{0\}$. Because of the cyclicity, this implies that the weight of the dual code is at least 2.

Notation :

The weight of a vector x is denoted by $wt(x)$.

If $e \in \mathbb{F}_{q^k}$ then $tr(e)$ is the trace of e over $\mathbb{F}_q$.

We write (u, v) instead of $gcd(u, v)$.

2 1-Weight irreducible cyclic codes

Theorem 1 *Let C be a $[n, k]$ irreducible cyclic code over $\mathbb{F}_q$ with $n = \lambda(\frac{q^k-1}{q-1})$ where λ divides $q-1$.*
Let ρ be the order of the check polynomial of C, that is, the common order of its roots. The following assertions are equivalent:

(a) *C is a 1-weight code.*

(b) *C contains a word of weight $w = \lambda q^{k-1}$.*

(c) $\frac{\rho}{(\rho,q-1)} = \frac{q^k-1}{q-1}$.

In order to prove this theorem, we need the following three lemmas. The first one was proved in Proposition 10 of [6].

Lemma 2 *Let C be an irreducible cyclic code over $\mathbb{F}_q$ of length n such that $(n, q) = 1$. Let β in $\mathbb{F}_{q^k}$ be such that the check polynomial of C is the minimal polynomial of β^{-1} over $\mathbb{F}_q$.*

Let $m \in \mathbb{N}$ be the smallest non-zero integer such that $\beta^m \in \mathbb{F}_q$ and let e be in $\mathbb{F}_q$ such that $\beta^m = e$.
Then m divides n and :

$$(\Diamond) \qquad C = \{c_a = (|\, \overline{c}_a \mid e\,\overline{c}_a \mid \cdots \mid e^j\,\overline{c}_a \mid \cdots \mid e^{t-1}\,\overline{c}_a\, |) \mid a \in \mathbb{F}_{q^k}\}$$

with $n = mt$ and $\overline{c}_a = (tr(a), tr(a\beta), \ldots, tr(a\beta^{m-1}))$.
(The vertical bars denote concatenation)

Lemma 3 *With the previous definitions of β, C, and m, define :*

$$\overline{C} = \{\overline{c}_a = (tr(a), tr(a\beta), \ldots, tr(a\beta^{m-1})) \mid a \in \mathbb{F}_{q^k}\}.$$

(1) *$\overline{C}$ is a $[m, k]$ projective code of length m over $\mathbb{F}_q$.*

(2) *$\overline{C}$ is a N-weight code if and only if C is a N-weight code.*

Proof
(1) Obviously, the map $c_a \longrightarrow \overline{c}_a$ from C to $\overline{C}$ is a vector isomorphism. Consequently, $\overline{C}$ is a linear code of length m over $\mathbb{F}_q$ and both codes, $\overline{C}$ and C, have the same dimension.
From the theory of cyclic codes it is clear that there exists a word of weight 1 or 2 in the dual code of $\overline{C}$ if and only if there exists $(x_i, x_j) \in \mathbb{F}_q^2$ with $0 \leq i \leq m-1$, $0 \leq j \leq m-1$ and $x_i \neq x_j$ such that :

$x_i\beta^i + x_j\beta^j = 0$ or, equivalently:

$\beta^j = \epsilon\beta^i$ with $\epsilon \in \mathbb{F}_q$ that is to say: $\beta^{j-i} \in \mathbb{F}_q$.

This last condition is not possible because of the definitions of i, j and m. The minimal weight of the dual of $\overline{C}$ is at least 3 and then $\overline{C}$ is a projective code.

(2) Since the element e^j in $(\Diamond)$ of Lemma 2 is a non-zero element of $\mathbb{F}_q$, it follows that $wt(e^j\overline{c}_a) = wt(\overline{c}_a)$ and then $wt(c_a) = twt(\overline{c}_a)$ and this proves the expected result. □

Lemma 4 *Let β be a non-zero element of $\mathbb{F}_{q^k}$.*
Let ρ be the order of β in the multiplicative group of $\mathbb{F}_{q^k}$.

If $m \in \mathbb{N}$ is the smallest non-zero integer such that $\beta^m \in \mathbb{F}_q$ then $m = \frac{\rho}{(\rho, q-1)}$

Proof The order of $< \beta > \cap \mathbb{F}_q$ is $(\rho, q-1)$ and the image of β in the quotient group $< \beta > / < \beta > \cap \mathbb{F}_q$ has then the order $m = \rho/(\rho, q-1)$. □

We are now in position to prove Theorem 1.

Proof of Theorem 1
Step 1 : a)$\Longrightarrow$ b),
It is well known (see [1] or [6] for instance) that the length of a $[n, k]$ 1-weight linear code over $\mathbb{F}_q$ is of the form $n = \lambda(\frac{q^k-1}{q-1})$ and that the weight of every non-zero word of this code is λq^{k-1}.

Step 2 : b)$\Longrightarrow$ c) Let $\overline{C}$ be as defined in Lemma 3 and let a be in $\mathbb{F}_q^k$ such that $wt(c_a) = \lambda q^{k-1}$.
According to Lemma 2, let t be such that $n = mt$. As already mentioned in the proof of Lemma 3 : $wt(c_a) = twt(\overline{c}_a)$. This gives :

$\lambda(\frac{q^k-1}{q-1}) = tm$ and $\lambda q^{k-1} = t\overline{w}$ where $\overline{w} = wt(\overline{c}_a)$.

We easily deduce that $\lambda = t\theta$ with $\theta = q\overline{w} - m(q-1)$.
Thus, $t\theta(\frac{q^k-1}{q-1}) = tm$ and then $m = \theta(\frac{q^k-1}{q-1})$.
Since $\overline{C}$ is a projective code, its length is at most equal to the number of projective points : $m \leq \frac{q^k-1}{q-1}$.
This means $\theta = 1$ hence $m = \frac{q^k-1}{q-1}$. Observe that the order of the check polynomial of C is also the order of β and applying Lemma 4 we have $m = \frac{\rho}{(\rho,q-1)}$ and therefore $\frac{\rho}{(\rho,q-1)} = \frac{q^k-1}{q-1}$.

Step 3 : c)$\Longrightarrow$ a) Since $m = \frac{\rho}{(\rho,q-1)}$ and $\frac{\rho}{(\rho,q-1)} = \frac{q^k-1}{q-1}$, then $\overline{C}$ is a projective code of length $\frac{q^k-1}{q-1}$. It is well known that such a code is a 1-weight code (see [3]).
From Lemma 3, we deduce that C is also a 1-weight code. □

Remark If $\lambda = q-1$ and if the check polynomial is the minimal polynomial over $\mathbb{F}_q$ of a primitive root of $\mathbb{F}_{q^k}$, then applying Theorem 1 we obtain a simplex code.

3 2-Weight cyclic codes

The following result is a characterization of projective codes (cyclic or not) in the set of 2-weight codes.

Proposition 5 *Let C be a 2-weight code of length n and dimension k over $\mathbb{F}_q$ with non-zero weights w_1 and w_2. Assume that the minimum weight of the dual of C is at least 2.*
C is a projective code if and only if :

$$n^2(q-1) - [q(w_1+w_2)-1]n + \frac{(q^k-1)w_1w_2}{(q-1)q^{k-2}} = 0$$

Proof We just have to calulate the number B_2 of codewords of weight 2 in the dual of C.

We use the method of Proposition 5 in [5] by replacing the rigth side of Eq. (6) by $\{n(q-1)(n(q-1)+1)+2B_2\}q^{k-2}$ and this gives the Pless equation in the general case. We obtain:
$(q-1)\{n^2(q-1) - [q(w_1+w_2)-1]n + \frac{(q^k-1)w_1w_2}{(q-1)q^{k-2}}\} + 2B_2 = 0$
which shows that $B_2 = 0$ if and only if :
$n^2(q-1) - [q(w_1+w_2)-1]n + \frac{(q^k-1)w_1w_2}{(q-1)q^{k-2}} = 0.$ □

Corollary 6 *If C is a 2-weight cyclic code of length $n = \lambda(\frac{q^k-1}{q-1})$ and dimension $2k$ over $\mathbb{F}_q$ with $\lambda \neq 1$ and non-zero weights $w_1 = (\lambda-1)q^{k-1}$ and $w_2 = \lambda q^{k-1}$, then C is a projective code.*

Proof Use the remark on the minimum weight of the dual code of C, which appears at the end of the introduction, and apply Proposition 5. □

Theorem 7 *Let α be a primitive element of $\mathbb{F}_{q^k}$ with q and k odd numbers. The minimal polynomial over $\mathbb{F}_q$ of $\omega \in \mathbb{F}_{q^k}$ is denoted by $m_\omega(x)$.*

(1) *The cyclic code C of length $n = q^k - 1$ over $\mathbb{F}_q$ with check polynomial $h(x) = m_\alpha(x)m_{-\alpha}(x)$ is a 2-weight cyclic code of dimension $2k$ and the two non-zero weights are $(q-1)q^{k-1}$ and $(\frac{q-1}{2})q^{k-1}$.*

(2) *If $q = 3$, then C is a projective code.*

Proof The code C is the direct sum of the irreducible cyclic codes C_1 and C_2 with check polynomials $m_\alpha(x)$ and $m_{-\alpha}(x)$, respectively.

$$C_1 = \{c(a) = (tr(a), tr(a\alpha), \ldots, tr(a\alpha^i), \ldots, tr(a\alpha^{n-1})) \mid a \in \mathbb{F}_{q^k}\},$$

$$C_2 = \{d(b) = (tr(b), tr(-b\alpha), \ldots, tr(b(-1)^i\alpha^i), \ldots, tr(b(-1)^{n-1}\alpha^{n-1})) \mid b \in \mathbb{F}_{q^k}\}.$$

Oviously, for every b the words $c(b)$ and $d(b)$ have the same weight. Since C_1 is a simplex code then C_1 and C_2 are 1-weight codes with $(q-1)q^{k-1}$ as non-zero weight and a typical word in C is of the form:

$$m_{(a,b)} = (tr(a+b), tr((a-b)\alpha), \ldots, tr\big((a+(-1)^i b)\alpha^i\big), \ldots, tr((a+(-1)^{n-1}b)\alpha^{n-1})).$$

If $a = 0$ or $b = 0$ and except if $a = 0$ and $b = 0$, the weigth of $m_{(a,b)}$ is $(q-1)q^{k-1}$. From now on we assume $a \neq 0$ and $b \neq 0$.

For every word $m = (m_0, m_1, \ldots, m_i, \ldots, m_{n-1})$ in $\mathbb{F}_q^n$ now define two partial words, the even part and the odd part of m, as follows :

$m^{even} = (m_0, m_2, \ldots, m_{2t}, \ldots, m_{n-2})$, $m^{odd} = (m_1, m_3, \ldots, m_{2t+1}, \ldots, m_{n-1})$. Obviously:

$$(*) \quad wt(m_{(a,b)}) = wt(m^{\text{even}}_{(a,b)}) + wt(m^{\text{odd}}_{(a,b)}).$$

Let $M_u = (tr(u), tr(u\alpha), \ldots, tr(u\alpha^i), \ldots, tr(u\alpha^{n-1})$ be with u in $\mathbb{F}_{q^k}$. This is a word of a simplex code and if $u \neq 0$ then $wt(M_u) = (q-1)q^{k-1}$ and therefore:

$$(**) \quad (q-1)q^{k-1} = wt(M_u^{\text{even}}) + wt(M_u^{\text{odd}}).$$

Now remark that:

$$(***) \quad m^{\text{even}}_{(a,b)} = M^{\text{even}}_{a+b} \text{ and } m^{\text{odd}}_{(a,b)} = M^{\text{odd}}_{a-b}.$$

The following results are easy to check from (*), (**),(***):

(1) If $a + b = 0$ then $wt(m_{(a,b)}) = (q-1)q^{k-1} - wt(M^{\text{even}}_{2a})$.

(2) If $a - b = 0$ then $wt(m_{(a,b)}) = wt(M^{\text{even}}_{2a})$.

(3) If $a + b \neq 0$ and $a - b \neq 0$ then:

$$wt(m_{(a,b)}) = wt(M^{\text{even}}_{a+b}) + (q-1)q^{k-1} - wt(M^{\text{even}}_{a-b}).$$

Summarizing (1),(2),(3), all that remains is to calculate $wt(M^{\text{even}}_u)$
when $u \neq 0$.

Since $\theta = \alpha^{q^k-1/q-1} \in \mathbb{F}_q$ then :

$$\theta M^{\text{even}}_u = \left(tr(u\alpha^{q^k-1/q-1}), tr(u\alpha^{(q^k-1/q-1)+2}), \ldots, tr(u\alpha^{(q^k-1/q-1)+2t}), \ldots, tr(u\alpha^{(q^k-1/q-1)+n-2})\right).$$

Observe that, since q and k are odd numbers then $\frac{q^k-1}{q-1}$ also is odd. On the other hand, $q^k - 1$ is even . Hence, reducing modulo $q^k - 1$, the map $i \longrightarrow \frac{q^k-1}{q-1} + i$ send bijectively the set of even integers in the range $[0, n-1]$ onto the set of odd integers in the same range.

We deduce $wt(\theta M^{\text{even}}_u) = wt(M^{\text{odd}}_u)$. Now, because $wt(\theta M^{\text{even}}_u) = wt(M^{\text{even}}_u)$ and using (**) we obtain:

$$wt(M^{even}_u) = wt(M^{odd}_u) = (\frac{q-1}{2})q^{k-1}.$$

Applying this result to $u = 2a$ in (1) and (2), to $u = a+b$ and to $u = a-b$ in (3), and summarising all the possible cases we conclude that the non-zero weights of C are $(q-1)q^{k-1}$ and $(\frac{q-1}{2})q^{k-1}$.

(2) If $q = 3$, then C satisfy conditions of Corollary 6 with $\lambda = q - 1 = 2$. □

Theorem 8 *Let α be a primitive element of $\mathbb{F}_{4^k}$.*
The minimal polynomial over $\mathbb{F}_4$ of $\omega \in \mathbb{F}_{4^k}$ is denoted by $m_\omega(x)$.
The cyclic code C of length $n = 4^k - 1$ over $\mathbb{F}_4$ with check polynomial $m_\alpha(x)m_{\alpha^2}(x)$ is a 2-weight projective cyclic code of dimension $2k$. The two non-zero weights of this code are $3(4^{k-1})$ and $2(4^{k-1})$.

Proof As usual, the words of cyclic codes are represented by their polynomial representations.

It is easy to check that α^2 is not a $\mathbb{F}_4$-conjugate of α. This means that m_α and m_{α^2} are distinct irreducible divisors of $x^n - 1$ over $\mathbb{F}_4$. The roots of the check polynomial $h(x) = m_\alpha m_{\alpha^2}$ are the $\mathbb{F}_4$-conjugates of α and the $\mathbb{F}_4$-conjugates of α^2. Therefore, the roots of $h(x)$ are the $\mathbb{F}_2$-conjugates of α and then $h(x)$ is a polynomial in $\mathbb{F}_2[x]$. The generator $g(x)$ of C, defined by $x^n - 1 = g(x)h(x)$, also is in $\mathbb{F}_2[x]$ and its degree is $n - 2k$. This is the generator of a binary simplex code S of dimension $2k$.

A typical non-zero word of C is $c(x) = \tilde{c}(x)g(x)$ where $\tilde{c}(x)$ is a polynomial in $\mathbb{F}_4[x]$ with degree at most $2k - 1$. Let γ be a primitive root of $\mathbb{F}_4$. Since $\{1, \gamma\}$ is a $\mathbb{F}_2$-basis of $\mathbb{F}_4$, then $\tilde{c}(x)$ can be decomposed in $\tilde{c}(x) = r(x) + \gamma s(x)$ where $r(x)$ and $s(x)$ are polynomials in $\mathbb{F}_2[x]$, both with degree at most equal to $2k - 1$. We obtain : $c(x) = r(x)g(x) + \gamma s(x)g(x) = u(x) + \gamma v(x)$ where $u(x)$ and $v(x)$ are in S.

Let $\underline{u} = (u_1, u_2, \ldots, u_i, \ldots, u_n)$ and $\underline{v} = (v_1, v_2, \ldots, v_i, \ldots, v_n)$ be respectively the binary vectors which are represented by $u(x)$ and $v(x)$. The weight of $c(x)$ is the weight of $\underline{u} + \gamma\underline{v}$. Obviously, the number of zero components of this vector is the number z of i such that $u_i = 0$ and $v_i = 0$. We easily deduce that :

$$wt(\underline{u} + \gamma\underline{v}) = \frac{1}{2}[wt(\underline{u}) + wt(\underline{v}) + wt(\underline{u} + \underline{v})].$$

Since $\underline{u}$, $\underline{v}$, $\underline{u} + \underline{v}$ are in the polynomial representation of S then the weight of each is 0 or 2^{2k-1}. Considering the different cases, we see that the possible weights of $wt(\underline{u}+\gamma\underline{v})$ are 0, $2(4^{k-1})$, and $3(4^{k-1})$.

Finally we check that C is a projective code by applying Corollary 6 with $\lambda = 3$. □

Corollary 9 *A cyclic code over* $\mathbb{F}_4$ *generated over* $\mathbb{F}_4$ *by a binary cyclic simplex code of length* $2^{2k} - 1$ *is a 2-weight projective cyclic code and the two non-zero weights of this code are* $3(4^{k-1})$ *and* $2(4^{k-1})$.

Proof The check polynomial $h(x)$ of such a simplex code S is the minimal polynomial over $\mathbb{F}_2$ of a a primitive element α of $\mathbb{F}_{2^{2k}}$, which can be decomposed as $h(x) = m_\alpha(x)m_{\alpha^2}(x)$. Thus the code generated over $\mathbb{F}_4$ by S is a code described in the previous theorem. □

Remark The 2-weight codes obtained from Theorem 7 and Theorem 8 probably have the same length, dimension and weight distribution than codes which appear in the coding litterature. The new fact is that the codes of the two previous theorem are cyclic and direct sums of two 1-weight irreducible cyclic codes.

For example, the code of Theorem 8 has the same length, dimension and weights as the code obtained by the construction 4.2 in [5] (also mentioned in the survey [2] as example SU2) for $q = 4$ and $r = 3$. However, for a given set of projective subspaces arising in this construction, this gives several (dependent on the choice of representatives of the projective points) 2-weight projective codes with the same parameters, but this is not a construction of cyclic codes.

4 Conclusion

The purpose of this paper was to study 2-weight cyclic codes over $\mathbb{F}_q$ with $q \neq 2$, which are direct sum of two 1-weight irreducible cyclic codes. We have characterize 1-weight irreducible cyclic codes and introduced two special classes of 2-weight cyclic codes which are direct sums of 1-weight irreducible cyclic codes. The open problem now is to find all such codes.

Acknowledgments The authors would like to thank the anonymous referee who gave clever comments and suggestions to improve the proofs and the presentation of the paper. The second author wishes to thank the Universidad Nacional Autónoma de México, where part of this work was done during his visit.

References

1. Bonisoli A (1984) Every equidistant linear code is a sequence of dual Hamming codes. Ars Comb 18:181–186
2. Calderbank R, Kantor WM (1986) The geometry of two-weight codes. Bull. London Math. Soc 18:97–122

3. Huffman WC, Pless V (2003) Fundamental of error-correcting codes. Cambridge University Press, Cambridge
4. Lidl R, Niederreiter H (1983) Finite fields in encyclopedia of mathematics and its applications, Vol 20. Addison-Wesley, Reading MA
5. Wolfmann J (1977) Codes projectifs à deux poids “caps" complets et ensembles de différences. J Comb Theory Ser A 23:208–222
6. Wolfmann J (2005) Are two-weight projective cyclic codes irreducible? IEEE Trans. Inf Theory 51:733–737