Bull. Aust. Math. Soc. **96** (2017), 513–518
doi:10.1017/S0004972717000636

A SPECIAL CLASS OF QUASI-CYCLIC CODES

MINJIA SHI✉, JIE TANG, MAORONG GE, LIN SOK and PATRICK SOLÉ

(Received 15 May 2017; accepted 29 May 2017; first published online 10 August 2017)

Abstract

We study a special class of quasi-cyclic codes, obtained from a cyclic code over an extension field of the alphabet field by taking its image on a basis. When the basis is equal to its dual, the dual code admits the same construction. We give some examples of self-dual codes and LCD codes obtained in this way.

2010 *Mathematics subject classification*: primary 94B05; secondary 94B15.

Keywords and phrases: quasi-cyclic codes, cyclic codes, self-dual codes, LCD codes.

1. Introduction

A quasi-cyclic code of length $n = \ell m$ and index ℓ over a finite field $\mathbb{F}_q$ is a linear code invariant under T^ℓ, where T denotes the shift operator. Quasi-cyclic codes contain cyclic codes as the case of index one. It has been known for some time that, unlike cyclic codes, quasi-cyclic codes are asymptotically good [1].

One approach to quasi-cyclic codes is to regard them as codes of length ℓ over a ring of size q^m [10]. Another approach is to view them as cyclic codes of length m over a field of size q^ℓ [9]. This is the approach we follow here. We consider cyclic codes over $\mathbb{F}_{q^\ell}$ and construct quasi-cyclic codes of index ℓ from them. Note that the map that takes a cyclic code over $\mathbb{F}_{q^\ell}$ to a quasi-cyclic code of index ℓ is just the projection on a basis of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$. This has been a celebrated operation in coding theory since Wolfmann's construction of the Golay code from a Reed–Solomon code over $\mathbb{F}_8$ [11]. It was used more recently to define the notion of Type II codes over $\mathbb{F}_4$ [6]. In particular, when the basis is self-dual, we can construct self-dual codes and LCD (linear codes with complementary dual) codes, which are a class of codes introduced by Massey [12]; these have recently found applications in the security of embedded electronics [2, 3].

The first and the last two authors were supported by NNSF of China (61672036), Technology Foundation for Selected Overseas Chinese Scholars, Ministry of Personnel of China (05015133), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11) and Key Projects of Support Program for Outstanding Young Talents in Colleges and Universities (gxyqZD2016008). The fourth author was supported by China Postdoctoral Science Foundation funded project (2016M601991).

© 2017 Australian Mathematical Publishing Association Inc. 0004-9727/2017 $16.00

https://doi.org/10.1017/S0004972717000636 Published online by Cambridge University Press

This note is organised as follows. In Section 2, we study the module structure of quasi-cyclic codes, introduce the special class of quasi-cyclic codes of interest to us and establish theoretical foundations for these codes. Section 3 contains some numerical examples. The concluding Section 4 presents some challenging open problems.

2. Module structure of quasi-cyclic codes

We define the shift map T from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ by $T(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$ for all $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$. A linear code C is called an ℓ-quasi-cyclic code if C is invariant under T^ℓ, that is, $T^\ell(C) = C$. In other words, a cyclic shift of any codeword by ℓ positions is still a codeword.

It is well known that a code is ℓ-quasi-cyclic if and only if it is (ℓ, n)-quasi-cyclic, where (ℓ, n) denotes the greatest common divisor of ℓ and n. We will therefore assume that $\ell \mid n$, so that $n = \ell m$ for some integer m. The special case of $\ell = 1$ gives the class of cyclic codes. The class of quasi-cyclic codes, which contains cyclic codes as a subclass, forms an important class of linear codes.

Let m be a positive integer such that $\gcd(m, q) = 1$. Let $\mathbb{F}_q[x]$ denote the ring of polynomials in the indeterminate x over $\mathbb{F}_q$ and define the ring $R_m = \mathbb{F}_q[x]/\langle x^m - 1\rangle$. We can represent a codeword of an $[n, k, d]_q$ ℓ-quasi-cyclic code as

$$c(x) = (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R_m^\ell,$$

where each entry is given by $c_i(x) = \sum_{j=0}^{m-1} c_{i,j}x^j$ and $c_{i,j} \in \mathbb{F}_q$ for $0 \le i \le \ell - 1$. Let $B = \{e_0, e_1, \ldots, e_{\ell-1}\}$ be a basis of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$ and, for a positive integer ℓ, define

$$\begin{aligned} \phi_B : R_m^\ell &\longrightarrow \mathbb{F}_{q^\ell}[x]/\langle x^m - 1\rangle, \\ (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) &\longmapsto \sum_{j=0}^{m-1} d_j x^j, \end{aligned}$$

where $d_j = \sum_{i=0}^{\ell-1} c_{i,j}e_i$.

We denote the minimum distance of a code C over the field F by $d_F(C)$.

Theorem 2.1. *If C is a cyclic code of length m over $\mathbb{F}_{q^\ell}$ then $\phi_B^{-1}(C)$ is an ℓ-quasi-cyclic code of length $n = \ell m$ over $\mathbb{F}_q$.*

Proof. Linearity of C over $\mathbb{F}_{q^\ell}$ entails linearity of the image $\phi_B^{-1}(C)$ over $\mathbb{F}_q$. Shifting symbols in $\mathbb{F}_{q^\ell}$ translates into shifting ℓ symbols of $\mathbb{F}_q$. Thus cyclicity of C over $\mathbb{F}_{q^\ell}$ entails ℓ-quasi-cyclicity of $\phi_B^{-1}(C)$ over $\mathbb{F}_q$. □

Theorem 2.2. *Let $\widetilde{C}$ be a quasi-cyclic code of length ℓm and index ℓ over $\mathbb{F}_q$ obtained from a cyclic code $C = \phi_B^{-1}(\widetilde{C})$ over $\mathbb{F}_{q^\ell}$ with respect to a basis $B = \{e_0, e_1, \ldots, e_{\ell-1}\}$ of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$. Then $d_{\mathbb{F}_q}(\widetilde{C}) \ge d_{\mathbb{F}_{q^\ell}}(C)$ and the equality holds if C has a minimum weight vector, the nonzero components of which are elements of B.*

https://doi.org/10.1017/S0004972717000636 Published online by Cambridge University Press

PROOF. Let $d(x) = \sum_{j=0}^{m-1} d_j x^j$ be a codeword of C. With the above notation, the weight of a component d_j of d is nonzero if and only if at least one of the $c_{i,j} \neq 0$. Thus the weight of d_j as a symbol of $\mathbb{F}_{q^\ell}$ is at most the weight of the vector $(c_{0,j}, \dots, c_{l-1,j})$ and equality holds if and only if just one of the $c_{i,j}$ is nonzero, that is, if and only if $d_j \in B$. The result follows by summation on j. □

The dual basis of $B = \{e_0, e_1, \dots, e_{\ell-1}\}$ has the form $B^* = \{e_0^*, e_1^*, \dots, e_{\ell-1}^*\}$, where $\mathrm{Tr}(e_i, e_j) = \delta_{i,j}$. Here, Tr denotes the trace from $\mathbb{F}_{q^\ell}$ to $\mathbb{F}_q$ and $\delta_{i,j}$ is the Kronecker symbol.

THEOREM 2.3. *Keep the above notation. If C is a cyclic code over $\mathbb{F}_{q^\ell}$ then*

$$\phi_{B^*}^{-1}(C^\perp) = \phi_B^{-1}(C)^\perp.$$

PROOF. The inclusion $\phi_{B^*}^{-1}(C^\perp) \subseteq \phi_B^{-1}(C)^\perp$ is immediate by comparing the scalar products over $\mathbb{F}_{q^\ell}^m$ and over $\mathbb{F}_q^{\ell m}$, using the definition of the dual basis. Equality follows from the fact that, since ϕ_B is a bijection, both sides have the same size. □

The following immediate consequences of Theorem 2.3 are useful in constructions.

COROLLARY 2.4. *If $B = B^*$ and C is self-dual, then $\phi_B^{-1}(C)$ is self-dual.*

Note that Corollary 2.4 can only be applied when self-dual cyclic codes over $\mathbb{F}_q$ exist, that is, in particular, when q is even [8].

COROLLARY 2.5. *If $B = B^*$ and C is LCD, then $\phi_B^{-1}(C)$ is LCD.*

This construction is mentioned in Dougherty *et al.* [4]. Criteria for the existence of LCD cyclic codes can be found in Yang and Massey [12].

3. Numerics

The following examples were obtained using an MDS Reed–Solomon code as the cyclic code. In most cases, the quasi-cyclic code that is obtained is almost optimal. The parameters for the corresponding best known linear code are given in the BKLC column of Table 1 (based on the code tables [7]).

In Tables 2 and 3, the coefficients of the generator polynomials for the cyclic codes (column 2) are arranged in descending order. For example, $11w^4w^4w^3w^3$ means $g(x) = x^5 + x^4 + w^4x^3 + w^4x^2 + w^3x + w^3$.

Using cyclic self-dual codes over $\mathbb{F}_8$ and $\mathbb{F}_{16}$, respectively, we obtain two quasi-cyclic codes that are optimal self-dual codes according to Gaborit's table of self-dual codes [5]. These are a [42, 21, 8] code C_{42} and a [40, 20, 8] code C_{40} with respective

https://doi.org/10.1017/S0004972717000636 Published online by Cambridge University Press

TABLE 1. Examples of quasi-cyclic codes.

q	Over $\mathbb{F}_q$	Over $\mathbb{F}_2$	BKLC
8	$[7,5,3]$	$[21,15,3]$	$[21,15,4]$
8	$[7,3,5]$	$[21,9,6]$	$[21,9,8]$
16	$[15,13,3]$	$[60,52,3]$	$[60,52,4]$
16	$[15,11,5]$	$[60,44,5]$	$[60,44,6]$
16	$[15,9,7]$	$[60,36,7]$	$[60,36,9]$
16	$[15,7,9]$	$[60,28,11]$	$[60,28,12]$
32	$[31,29,3]$	$[155,145,3]$	$[155,145,4]$
32	$[31,27,5]$	$[155,135,5]$	$[155,135,6]$
32	$[31,25,7]$	$[155,125,7]$	$[155,125,8]$

TABLE 2. Optimal self-dual quasi-cyclic codes.

q	Generator polynomials over $\mathbb{F}_q$	Over $\mathbb{F}_q$	Over $\mathbb{F}_2$
8	$11w^4w^411w^2w^2$	[14, 7, 5]	[42, 21, 8]
16	$11w^4w^4w^3w^3$	[10, 5, 4]	[40, 20, 8]

weight enumerators:

$$\begin{aligned} W_{C_{42}}(y) = {} & y^{42} + 420y^{34} + 441y^{32} + 9968y^{30} + 54960y^{28} + 157038y^{26} + 329140y^{24} \\ & + 496608y^{22} + 496608y^{20} + 329140y^{18} + 157038y^{16} \\ & + 54960y^{14} + 9968y^{12} + 441y^{10} + 420y^{8} + 1, \\ W_{C_{40}}(y) = {} & y^{40} + 285y^{32} + 1024y^{30} + 11040y^{28} + 46080y^{26} + 117090y^{24} \\ & + 215040y^{22} + 267456y^{20} + 215040y^{18} + 117090y^{16} \\ & + 46080y^{14} + 11040y^{12} + 1024y^{10} + 285y^{8} + 1. \end{aligned}$$

Using LCD cyclic codes over $\mathbb{F}_4, \mathbb{F}_8$ and $\mathbb{F}_{16}$ respectively, we obtain LCD quasi-cyclic codes that are optimal according to the code tables [7]. The parameters of the codes are summarised in Table 3.

4. Conclusion

In this note, we have studied a special class of quasi-cyclic codes obtained as the image of cyclic codes over an extension field with a given basis. To construct the full class of quasi-cyclic codes, it would be necessary to develop a theory of shift-invariant $\mathbb{F}_q$-linear cyclic codes over an extension of $\mathbb{F}_q$. Indeed, the classical definition of cyclic codes over a field assumes linearity over the alphabet field. There are shift-invariant codes that are $\mathbb{F}_q$-linear but not $\mathbb{F}_{q^\ell}$-linear over $\mathbb{F}_{q^\ell}$. Their image on a basis is still a *bona-fide* quasi-cyclic code over $\mathbb{F}_q$. While the subclass explored in this paper contains very good codes (as shown in Section 3), it is still desirable to have a general theory applicable to all quasi-cyclic codes. This is the main open problem of this research.

https://doi.org/10.1017/S0004972717000636 Published online by Cambridge University Press

TABLE 3. Optimal LCD quasi-cyclic codes.

q	Generator polynomials over $\mathbb{F}_q$	Over $\mathbb{F}_q$	Over $\mathbb{F}_2$
4	$1w1$	[5, 3, 3]	[10, 6, 3]
4	$1w^2w^21$	[5, 2, 4]	[10, 4, 4]
4	$1ww^2w1$	[13, 7, 5]	[26, 14, 6]
4	$1w^2ww^2w^2ww^21$	[13, 6, 6]	[26, 12, 8]
4	$1w^2ww^21$	[15, 11, 4]	[30, 22, 4]
4	$11w11$	[17, 13, 4]	[34, 26, 4]
4	$1www^2w^2ww1$	[17, 8, 8]	[34, 16, 8]
4	$1w^2w^2w1w^2w^21ww^2w^21$	[17, 4, 12]	[34, 8, 14]
4	$1w^211w^21$	[21, 14, 5]	[42, 28, 6]
4	$1w^2ww1ww11ww1www^21$	[29, 14, 12]	[58, 28, 12]
8	$1w^3w^31$	[9, 6, 4]	[27, 18, 4]
8	$1w^4w^3w^5w^5w^3w^41$	[9, 2, 8]	[27, 6, 12]
8	$1ww^2w^2w1$	[13, 8, 5]	[39, 24, 6]
8	$1ww^4w^4w1$	[19, 12, 6]	[57, 36, 8]
16	$1w^4w^41$	[17, 14, 4]	[68, 56, 4]

References

[1] C. L. Chen, W. W. Peterson and E. J. Weldon, 'Some results on quasi-cyclic codes', *Inform. Control* **5**(5) (1969), 407–423.

[2] C. Carlet and S. Guilley, 'Complementary dual codes for counter-measures to side-channel attacks', in: *Coding Theory and Applications*, CIM Series in Mathematical Sciences, 3 (eds. E. R. Pinto *et al.*) (Springer, Cham, Switzerland, 2014), 97–105.

[3] C. Carlet and S. Guilley, 'Complementary dual codes for counter-measures to side-channel attacks', *Adv. Math. Commun.* **10**(1) (2016), 131–150.

[4] S. T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok and P. Solé, 'The combinatorics of LCD codes: linear programming bound and orthogonal matrices', *Int. J. Inf. Coding Theory* **4**(2/3) (2017), 116–128.

[5] P. Gaborit, Tables of self-dual codes, available online at http://www.unilim.fr/pages_perso/philippe.gaborit/SD/GF2/GF2I.htm.

[6] P. Gaborit, V. Pless, P. Solé and O. Atkin, 'Type II codes over $\mathbb{F}_4$', *Finite Fields Appl.* **8**(2) (2002), 171–183.

[7] M. Grassi, Bounds on the minimum distance of linear codes and quantum codes, available online at http://www.codetables.de.

[8] Y. Jia, S. Ling and C. Xing, 'On self-dual cyclic codes over finite fields', *IEEE Trans. Inform. Theory* **57**(4) (2011), 2243–2251.

[9] K. Lally, 'Quasi-cyclic codes of index ℓ over $\mathbb{F}_q$ viewed as $\mathbb{F}_q[x]$-submodules', in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2003*, Lecture Notes in Computer Science, Vol. 2643 (eds. M. Fossorier *et al.*) (Springer, Berlin, Germany, 2003), 244–253.

[10] S. Ling and P. Solé, 'On the algebraic structure of quasi-cyclic codes. I. finite fields', *IEEE Trans. Inform. Theory* **47**(7) (2001), 2751–2760.

https://doi.org/10.1017/S0004972717000636 Published online by Cambridge University Press

[11] J. Wolfmann, 'A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field', *Discrete Math.* **31**(3) (1980), 337–338.

[12] X. Yang and J. L. Massey, 'The condition for a cyclic code to have a complementary dual', *J. Discrete Math.* **1**(26) (1994), 391–393.

MINJIA SHI,
Key Laboratory of Intelligent Computing and Signal Processing,
Anhui University, No. 3 Feixi Road, Hefei, Anhui Province 230039,
PR China
and
National Mobile Communications Research Laboratory,
Southeast University, Nanjing, 210096, PR China
and
School of Mathematical Sciences, Anhui University,
Hefei, Anhui, 230601, PR China
e-mail: smjwcl.good@163.com

JIE TANG, School of Mathematical Sciences, Anhui University,
Hefei, Anhui, 230601, PR China
e-mail: Lucytang1208@163.com

MAORONG GE, School of Mathematical Sciences, Anhui University,
Hefei, Anhui, 230601, PR China
e-mail: ge1968@163.com

LIN SOK, School of Mathematical Sciences, Anhui University,
Hefei, Anhui, 230601, PR China
and
Department of Mathematics,
Royal University of Phnom Penh, 12156 Phnom Penh, Cambodia
e-mail: sok.lin@rupp.edu.kh

PATRICK SOLÉ, CNRS/LAGA, Université Paris 8,
93 526 Saint-Denis, France
e-mail: sole@enst.fr

https://doi.org/10.1017/S0004972717000636 Published online by Cambridge University Press