Finite Fields and Their Applications 20 (2013) 1–14

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A q-polynomial approach to cyclic codes

Cunsheng Ding [a,*], San Ling [b]

[a] *Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China*
[b] *Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore*

ARTICLE INFO

Article history:
Received 27 August 2012
Revised 26 November 2012
Accepted 14 December 2012
Available online xxxx
Communicated by Simeon Ball

MSC:
94B15
94B05
05B50

Keywords:
Cyclic codes
Linear codes
Linearized polynomials
q-polynomials

ABSTRACT

Cyclic codes have been an interesting topic of both mathematics and engineering for decades. They are prominently used in consumer electronics, data transmission technologies, broadcast systems, and computer applications. Three classical approaches to the study and construction of cyclic codes are those based on the generator matrix, the generator polynomial and the idempotent. The objective of this paper is to develop another approach – the q-polynomial approach. Fundamental theory of this approach will be developed, and will be employed to construct a new family of cyclic codes in this paper.

1. Introduction

Let q be a power of a prime. A linear $[n, k, d; q]$ code is a k-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum nonzero (Hamming) weight d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by

$$1 + A_1 y + A_2 y^2 + \cdots + A_n y^n.$$

[*] Corresponding author.
E-mail addresses: cding@ust.hk (C. Ding), lingsan@ntu.edu.sg (S. Ling).

1071-5797/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ffa.2012.12.005

A linear $[n,k]$ code $\mathcal{C}$ over $\mathrm{GF}(q)$ is called *cyclic* if $(c_0,c_1,\dots,c_{n-1})\in\mathcal{C}$ implies $(c_{n-1},c_0,c_1,\dots,c_{n-2})\in\mathcal{C}$. By identifying any vector $(c_0,c_1,\dots,c_{n-1})\in\mathrm{GF}(q)^n$ with

$$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in\mathrm{GF}(q)[x]/\bigl(x^n-1\bigr),$$

any code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$ corresponds to a subset of the quotient ring $\mathrm{GF}(q)[x]/(x^n-1)$. A linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset in $\mathrm{GF}(q)[x]/(x^n-1)$ is an ideal of the ring $\mathrm{GF}(q)[x]/(x^n-1)$.

Note that every ideal of $\mathrm{GF}(q)[x]/(x^n-1)$ is principal. Let $\mathcal{C}=(g(x))$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of $\mathcal{C}$. Then $g(x)$ is unique and called the *generator polynomial*, and $h(x)=(x^n-1)/g(x)$ is referred to as the *parity-check* polynomial of $\mathcal{C}$.

The error-correcting capability of cyclic codes may not be as good as other linear codes in general. However, some cyclic codes are optimal in the sense that they meet some bounds on linear codes. Furthermore, cyclic codes have applications in storage and communication systems because they have efficient encoding and decoding algorithms [6,9,10,14,15]. For example, Reed–Solomon codes have found important applications from deep-space communication to consumer electronics. They are prominently used in consumer electronics such as CDs, DVDs, Blu-ray Discs, in data transmission technologies such as DSL & WiMAX, in broadcast systems such as DVB and ATSC, and in computer applications such as RAID 6 systems.

Cyclic codes have been studied for decades and a lot of progress has been made (see, for example, [6,7,10,11,13,16] and the references therein). Three general approaches to the design and analysis of cyclic codes are based on generator matrices, generator polynomials and idempotents. These approaches have their advantages and disadvantages in dealing with cyclic codes. The objectives of this paper are to introduce a q-polynomial approach to the study of cyclic codes, lay the foundations of this approach, and construct new ones with this approach.

This paper is organized as follows. Section 2 fixes some notations for this paper. Section 3 introduces some necessary notations and results about sequences. Section 4 defines the q-polynomial codes over $\mathrm{GF}(q)$ and establishes theoretical foundations for these codes. Section 5 defines a class of almost optimal q-polynomial codes. The relationship between q-polynomial codes and some other known types of codes are briefly discussed in Section 6. Section 7 summarizes this paper.

2. Some notations fixed throughout this paper

Throughout this paper, we adopt the following notations unless otherwise stated:

- p is a prime.
- q is a positive power of p.
- n is a positive integer, and is used to denote the length of a cyclic code over $\mathrm{GF}(q)$ and also the period of a periodic sequence over $\mathrm{GF}(q)$.
- $r=q^n$.
- $\mathbb{Z}_M=\{0,1,\dots,M-1\}$ denotes the residue class ring modulo M.
- $\mathrm{Tr}_{q^t/q}(x)$ is the trace function from $\mathrm{GF}(q^t)$ to $\mathrm{GF}(q)$.
- By the Database we mean the collection of the tables of best linear codes known maintained by Markus Grassl at http://www.codetables.de/.

3. The linear span and the dual of sequences

3.1. The linear span of sequences

Let $s^\infty=(s_i)_{i=0}^\infty$ be a sequence of period n over $\mathrm{GF}(q)$. A monic polynomial $c(x)=c_0x^\ell+c_1x^{\ell-1}+\cdots+c_\ell$ over $\mathrm{GF}(q)$, where $c_0=1$, is called a *characteristic polynomial* of the sequence s^∞ if

$$-c_0s_i=c_1s_{i-1}+c_2s_{i-2}+\cdots+c_\ell s_{i-\ell}\quad\text{for all } i\geqslant\ell. \tag{1}$$

The characteristic polynomial of s^∞ with the smallest degree is referred to as the *minimal polynomial* of s^∞. The *linear span* (also called *linear complexity*) of s^∞ is the degree of the minimal polynomial of this sequence.

There are a few ways to determine the linear span and minimal polynomial of periodic sequences. The first one is given in the following lemma [12].

Lemma 3.1. *(See [12].) Let s^∞ be a sequence of period n over* GF(q). *Define*

$$S^n(x) = s_0 + s_1 x + \cdots + s_{n-1}x^{n-1} \in \mathrm{GF}(q)[x].$$

Then the minimal polynomial $m_s(x)$ of s^∞ is given by

$$m_s(x) = \frac{x^n - 1}{\gcd(x^n - 1, x^{n-1}S^n(\frac{1}{x}))}; \tag{2}$$

and the linear span $\mathbb{L}_s$ of s^∞ is given by

$$\mathbb{L}_s = n - \deg\left(\gcd\left(x^n - 1, x^{n-1}S^n\left(\frac{1}{x}\right)\right)\right). \tag{3}$$

The second way to compute the minimal polynomial and linear span is described in the following lemma.

Lemma 3.2. *(See [1].) Every periodic sequence s^∞ over* GF(q) *of period $q^t - 1$, where t is a positive integer, has a unique expansion of the form*

$$s_i = \sum_{j=0}^{q^t-2} c_j \zeta^{ij}, \quad \textit{for all } i,$$

where ζ is a generator of GF$(q^t)^*$ *and $c_j \in$* GF(q^t) *for $0 \leqslant j \leqslant q^t - 2$. Let the* index set *be $J = \{0 \leqslant j \leqslant q^t - 2\colon\ c_j \neq 0\}$, then the minimal polynomial $m_s(x)$ of s^∞ is*

$$m_s(x) = \prod_{j\in J}(x - \zeta^j),$$

and the linear span $\mathbb{L}_s$ of s^∞ is the cardinality $|J|$.

The following lemma will be needed later when we deal with two classes of cyclic codes.

Lemma 3.3. *Let t be a positive integer, and let N be a positive divisor of $q^t - 1$. Define $n = (q^t - 1)/N$ and*

$$\lambda_i = \mathrm{Tr}_{q^t/q}(\eta^i)$$

for all $i \geqslant 0$, where $\eta = \zeta^N$ and ζ is a generator of GF$(q^t)^*$. *Then the sequence λ^∞ has period n.*

If

$$(q^t - 1) \nmid N(q^j - 1) \tag{4}$$

for all j with $1 \leqslant j \leqslant t-1$, *then the linear span of the sequence* λ^∞ *is equal to t, and the minimal polynomial of the sequence* λ^∞ *is given by*

$$m_\lambda(x) = \prod_{j=0}^{t-1}\left(x - \eta^{q^j}\right).$$

Proof. By the definition of the sequence λ^∞,

$$\lambda_i = \mathrm{Tr}_{q^t/q}\left(\eta^i\right) = \sum_{j=0}^{t-1} \eta^{iq^j},$$

where $\eta = \zeta^N$ and ζ is a generator of $\mathrm{GF}(q^t)^*$. Then we have

$$\lambda_i = \sum_{j=0}^{t-1} \zeta^{iNq^j}. \tag{5}$$

Under the conditions of (4), we now prove that all the exponents of ζ^i in (5) are pairwise distinct. Suppose that there exist j_1 and j_2 such that $0 \leqslant j_1 < j_2 \leqslant t-1$ and $Nq^{j_1} \equiv Nq^{j_2} \pmod{q^t - 1}$. We have then

$$\left(q^t - 1\right) \mid N\left(q^{j_2 - j_1} - 1\right),$$

which is contradictory to the conditions of (4). The desired conclusions of this lemma then follow from Lemma 3.2. □

The following lemma will also be frequently employed in this paper, and can be easily proved (see [16]).

Lemma 3.4. *Let* s^∞ *be a sequence of period n over* GF(q). *Then the linear span of this sequence is equal to the rank of the following circulant matrix*:

$$B_s = \begin{bmatrix} s_0 & s_{n-1} & s_{n-2} & \cdots & s_2 & s_1 \\ s_1 & s_0 & s_{n-1} & \cdots & s_3 & s_2 \\ s_2 & s_1 & s_0 & \cdots & s_4 & s_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ s_{n-1} & s_{n-2} & s_{n-3} & \cdots & s_1 & s_0 \end{bmatrix}.$$

We are interested in the linear span of sequences, as it determines the dimension of cyclic codes associated with these sequences.

3.2. The dual of sequences

Let GF($\tilde{r}$) be the splitting field of $x^n - 1 \in \mathrm{GF}(q)[x]$. Let s^∞ be a sequence of period n over GF(q). The *dual sequence* of s^∞, denoted by $\bar{s}^\infty$, is defined by

$$\bar{S}^n(x) := \sum_{i=0}^{n-1} \bar{s}_i x^i := \left(S^n(x)\right)^{\tilde{r}-1} - 1 \mod x^n - 1, \tag{6}$$

where $S^n(x)=\sum_{i=0}^{n-1} s_i x^i$ and $(S^n(x))^{\tilde{r}-1}-1 \bmod x^n-1$ denotes the remainder when $(S^n(x))^{\tilde{r}-1}-1$ is divided by x^n-1.

By definition, the dual $\bar{s}^\infty$ of any sequence s^∞ of period n over $\mathrm{GF}(q)$ is a sequence of period n over $\mathrm{GF}(q)$, and is unique.

Theorem 3.5. *For any sequence s^∞ of period n over $\mathrm{GF}(q)$, we have*

$$\gcd\bigl(m_s(x), m_{\bar{s}}(x)\bigr)=1 \quad \textit{and} \quad m_s(x)m_{\bar{s}}(x)=x^n-1, \tag{7}$$

where $m_{\bar{s}}(x)$ is the minimal polynomial of the dual sequence $\bar{s}^\infty$ of s^∞.

Proof. Let

$$\bar{S}^n(x)=\sum_{i=0}^{n-1}\bar{s}_i x^i \in \mathrm{GF}(q)[x].$$

By the definition of the dual sequence, for any nth root of unity $\mu \in \mathrm{GF}(\tilde{r})$, $\bar{S}^n(\mu)=0$ if and only if $S^n(\mu)\neq 0$, and $\bar{S}^n(\mu)\neq 0$ if and only if $S^n(\mu)=0$. The desired conclusions then follow from Lemma 3.1. □

We call the sequence $\bar{s}^\infty$ defined in (6) the dual sequence of s^∞ because of the properties of Theorem 3.5. We will need this theorem later when we deal with cyclic codes.

A polynomial $p(x)\in \mathrm{GF}(q)[x]$ is called an *idempotent* modulo x^n-1 if

$$p(x)^2 \equiv p(x) \pmod{x^n-1}.$$

The following lemma follows from the definitions of idempotents and dual sequences.

Lemma 3.6. *Let s^∞ be a sequence of period n over $\mathrm{GF}(q)$. If $S^n(x)=\sum_{i=0}^{n-1}s_i x^i$ is an idempotent modulo x^n-1, the dual sequence is given by $\bar{s}_0=s_0-1$ and*

$$\bar{s}_i=s_i \quad \textit{for } 1\leqslant i\leqslant n-1.$$

4. *q*-polynomial codes over GF(*q*)

A q-polynomial, or a linearized polynomial, over $\mathrm{GF}(q)$ is a polynomial of the form $L(x)=\sum_{i=0}^{h}\ell_i x^{q^i}$ with all coefficients ℓ_i in $\mathrm{GF}(q)$ and h being a nonnegative integer. Although q-polynomials can be defined in an extension field of $\mathrm{GF}(q)$, we consider only q-polynomials over $\mathrm{GF}(q)$ in this paper. In this section, we define q-polynomial codes over $\mathrm{GF}(q)$ with q-polynomials over $\mathrm{GF}(q)$, and establish theoretical foundations for these codes.

4.1. Description of q-polynomial codes

Let q be a prime power and let n be a positive integer. Define $r=q^n$. Let λ be an element of $\mathrm{GF}(r)^*$. Define

$$\mathcal{C}_\lambda=\left\{(c_0,c_1,\ldots,c_{n-1})\in \mathrm{GF}(q)^n\colon\ c(\lambda)=0 \text{ where } c(x)=\sum_{i=0}^{n-1}c_i x^{q^i}\right\}. \tag{8}$$

Clearly, $\mathcal{C}_\lambda$ is an $[n,k,d]$ cyclic linear code over GF(q), where k and d depend on q, n and λ. Since $\lambda \neq 0$, we have obviously that $d \geqslant 2$. The following two examples demonstrate that q-polynomial codes can be optimal linear codes.

Example 4.1. Let $(q,n) = (3,8)$, and let γ be a generator of GF$(r)^*$ with $\gamma^8 + 2\gamma^5 + \gamma^4 + 2\gamma^2 + 2\gamma + 2 = 0$. Define $\lambda = \gamma^2$. Then $\mathcal{C}_\lambda$ is an $[8,4,4]$ cyclic code over GF(3) with weight enumerator $1 + 20y^4 + 32y^5 + 8y^6 + 16y^7 + 4y^8$ and generator polynomial $x^4 + 2x^3 + 2x + 2$. This code is optimal, while the best code known in the Database with parameters $[8,4,4]$ is not known to be cyclic.

Example 4.2. Let $(q,n) = (3,8)$, and let γ be a generator of GF$(r)^*$ with $\gamma^8 + 2\gamma^5 + \gamma^4 + 2\gamma^2 + 2\gamma + 2 = 0$. Define $\lambda = \gamma^{10}$. Then $\mathcal{C}_\lambda$ is an $[8,2,6]$ cyclic code over GF(3) with weight enumerator $1 + 8y^6$ and generator polynomial $x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1$. This code is optimal, while the best code known in the Database with parameters $[8,2,6]$ is not known to be cyclic.

These two examples show that q-polynomial codes can be optimal linear codes in addition to that they are cyclic.

4.2. Parameters and properties of q-polynomial codes

By the Normal Basis Theorem, GF(r) has a *normal basis* $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ over GF(q), where $\alpha \in$ GF$(r)^*$. Such an α is called a *normal element* of GF(r) over GF(q). Then λ has a unique expression of the form

$$\lambda = \sum_{i=0}^{n-1} \lambda_i \alpha^{q^i}, \tag{9}$$

where all $\lambda_i \in$ GF(q).

Theorem 4.3. *Let λ be as in (9), and let $\lambda = \gamma^s$ for some $s \geqslant 0$, where γ is a generator of* GF$(r)^*$. *The dimension of the code $\mathcal{C}_\lambda$ is equal to $n - \mathrm{rank}(B_\lambda)$, where the matrix B_λ is defined by*

$$B_\lambda = \begin{bmatrix} \lambda_0 & \lambda_{n-1} & \lambda_{n-2} & \cdots & \lambda_2 & \lambda_1 \\ \lambda_1 & \lambda_0 & \lambda_{n-1} & \cdots & \lambda_3 & \lambda_2 \\ \lambda_2 & \lambda_1 & \lambda_0 & \cdots & \lambda_4 & \lambda_3 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ \lambda_{n-1} & \lambda_{n-2} & \lambda_{n-3} & \cdots & \lambda_1 & \lambda_0 \end{bmatrix}, \tag{10}$$

and these λ_i are defined in (9). The dimension of the code is also equal to $n - \mathbb{L}_\lambda$, where $\mathbb{L}_\lambda$ denotes the linear span of the sequence λ^∞.

Furthermore, the dimension of the code $\mathcal{C}_\lambda$ is no less than $n - \ell_s$, where ℓ_s denotes the size of the q-cyclotomic coset modulo $r-1$ containing s.

Proof. For any linearized polynomial

$$c(x) = \sum_{i=0}^{n-1} c_i x^{q^i} \in \mathrm{GF}(q)[x],$$

we have

$$c(\lambda) = \sum_{i=0}^{n-1} c_i \lambda^{q^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} c_j \lambda_{(i-j) \bmod n} \right) \alpha^{q^i}.$$

Hence $c(\lambda) = 0$ if and only if

$$\sum_{j=0}^{n-1} c_j \lambda_{(i-j) \bmod n} = 0, \quad i = 0, 1, 2, \dots, n-1. \tag{11}$$

This proves that B_λ is a parity-check matrix of the code $\mathcal{C}_\lambda$. Therefore, the dimension of the code $\mathcal{C}_\lambda$ is equal to $n - \mathrm{rank}(B_\lambda)$.

It then follows from Lemma 3.4 that the dimension of the code is also equal to $n - \mathbb{L}_\lambda$, where $\mathbb{L}_\lambda$ denotes the linear span of the sequence λ^∞. By the definition of ℓ_s, it is easily seen that $\mathrm{rank}(B_\lambda) \leqslant \ell_s$. The desired last conclusion follows from the first conclusion of this theorem. This completes the proof. □

Two polynomials

$$A(x) = a_0 x + a_1 x^q + a_2 x^{q^2} + \dots + a_{t-1} x^{q^{t-1}} \in \mathrm{GF}(q)[x]$$

and

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1} \in \mathrm{GF}(q)[x]$$

are called q-associates of each other. More precisely, $a(x)$ is the *conventional q-associate* of $A(x)$ and $A(x)$ is the *linearized q-associate* of $a(x)$.

We now describe the generator polynomial of the code $\mathcal{C}_\lambda$. To this end, we need the following lemma [12, p. 116, Theorem 3.62].

Lemma 4.4. *Let $A_1(x)$ and $A_2(x)$ be two q-polynomials over* GF(q) *with conventional q-associates $a_1(x)$ and $a_2(x)$. Then $A_1(x)$ divides $A_2(x)$ if and only if $a_1(x)$ divides $a_2(x)$.*

Theorem 4.5. *Let γ be a generator of* GF$(r)^*$, *and let $\lambda = \gamma^s$ for some positive integer s. Let ℓ_s denote the size of the q-cyclotomic coset modulo $r-1$ containing s. Let H_λ denote the subspace of* GF(r) *over* GF(q) *spanned by the set*

$$\{\lambda, \lambda^q, \lambda^{q^2}, \dots, \lambda^{q^{\ell_s - 1}}\}.$$

Define

$$G_\lambda(x) = \prod_{z \in H_\lambda} (x - z). \tag{12}$$

Then $G_\lambda(x)$ is a q-polynomial over GF(q) *and divides $x^{q^n} - x$.*

Let $g_\lambda(x)$ be the conventional q-associate of $G_\lambda(x)$. Then $g_\lambda(x)$ is the generator polynomial of the code $\mathcal{C}_\lambda$.

Proof. According to Theorem 3.52 in [12, p. 110], $G_\lambda(x)$ is a q-polynomial over GF(q^n). It is obvious that $G_\lambda(x)$ divides $x^{q^n} - x$. Now we prove that the coefficients of $G_\lambda(x)$ are in GF(q).

If $z = \sum_{i=0}^{\ell_s - 1} z_i \lambda^{q^i} \in H_\lambda$, where all $z_i \in \mathrm{GF}(q)$, then

$$z^{q^j} = \sum_{i=0}^{\ell_s - 1} z_{(i-j) \bmod \ell_s} \lambda^{q^i},$$

which is still an element of H_λ for all integers $j \geqslant 0$. Let z be any nonzero element in $H_\lambda \subset \mathrm{GF}(r)$. Then z can be expressed as γ^t for some integer t. Let ℓ_t denote the size of the cyclotomic coset modulo $r-1$ containing t. Then we have $z^{q^{\ell_t}} = z$. Define

$$P_z(x) = \prod_{i=0}^{\ell_t - 1} \left(x - z^{q^i}\right).$$

It is clear that $P_z(x)$ is a polynomial over $\mathrm{GF}(q)$, as the set $\{z, z^q, z^{q^2}, \ldots, z^{q^{\ell_t - 1}}\}$ is fixed by the Frobenius automorphism $y \mapsto y^q$. Note that $G_\lambda(x)$ is the product of a number of such polynomials $P_z(x)$ and the polynomial x. Hence the coefficients of $G_\lambda(x)$ must be in $\mathrm{GF}(q)$. This completes the proof of the first part of this theorem.

It follows from the conclusion of the first part of this theorem that $g_\lambda(x)$ is a polynomial over $\mathrm{GF}(q)$ and divides $x^n - 1$. Then by Lemma 4.4, any q-polynomial $V(x)$ is divisible by $G_\lambda(x)$ if and only if its conventional associate $v(x)$ is divisible by $g_\lambda(x)$.

Let $V(x)$ be any q-polynomial. If $G_\lambda(x)$ divides $V(x)$, then $V(\lambda) = G_\lambda(\lambda) = 0$. If $V(\lambda) = 0$, then $V(\lambda^{q^j}) = V(\lambda)^{q^j} = 0$ for all j and $V(y) = 0$ for all $y \in H_\lambda$. Hence any q-polynomial $V(x)$ satisfies $V(\lambda) = 0$ if and only if $V(x)$ is divisible by $G_\lambda(x)$. Combining this fact and the conclusions made above proves this theorem. □

The generator polynomial of the code $\mathcal{C}_\lambda$ is described in the following theorem when λ is given in the format of (9).

Theorem 4.6. *Let λ be given in the format of (9). Then the generator polynomial of the code $\mathcal{C}_\lambda$ is equal to $\epsilon^{-1} m_\lambda^*(x)$, where ϵ is the constant term of the minimal polynomial $m_\lambda(x)$ of the sequence λ^∞. In other words, the generator polynomial, denoted by $g_\lambda(x)$, of $\mathcal{C}_\lambda$ is given by*

$$g_\lambda(x) = \frac{x^n - 1}{\gcd(x^n - 1, \Lambda^n(x))}; \tag{13}$$

where $\Lambda^n(x) = \sum_{i=0}^{n-1} \lambda_i x^i$ and $m_\lambda^*(x)$ denotes the reciprocal of $m_\lambda^{(}x)$.

Proof. By (11), $c(x) = \sum_{i=0}^{n-1} c_i x^{q^i}$ is a codeword of $\mathcal{C}_\lambda$ if and only if

$$\sum_{j=0}^{n-1} c_j \lambda_{(i-j) \bmod n} = 0, \quad i = 0, 1, 2, \ldots, n-1,$$

which is equivalent to

$$\sum_{j=0}^{n-1} c_{(i-j) \bmod n} \lambda_j = 0, \quad i = 0, 1, 2, \ldots, n-1. \tag{14}$$

This set of equations holds if and only if the reciprocal of the minimal polynomial of the sequence λ^∞ divides $\sum_{i=0}^{n-1} c_i x^i$. The last conclusion of this theorem follows from Lemma 3.1. This completes the proof. □

Theorem 4.7. *Let* λ *be defined as in* (9)*, and let*

$$\bar{\lambda} = \sum_{i=0}^{n-1} \bar{\lambda}_i \alpha^{q^i},$$

where $\bar{\lambda}^\infty$ *is the dual sequence of* λ^∞ *defined in* (6)*. Then the dual of the code* $\mathcal{C}_\lambda$ *is equal to* $\mathcal{C}_{\bar{\lambda}}$*.*

Proof. By Theorem 4.6, the generator polynomials of $\mathcal{C}_\lambda$ and $\mathcal{C}_{\bar{\lambda}}$ are $a^{-1}m^*_\lambda(x)$ and $b^{-1}m^*_{\bar{\lambda}}(x)$, where a and b are the constant terms of $m_\lambda(x)$ and $m_{\bar{\lambda}}(x)$, respectively. It then follows from Theorem 3.5 that $\mathcal{C}_\lambda$ and $\mathcal{C}_{\bar{\lambda}}$ are duals of each other. □

Theorem 4.8. *Let* α *and* $\tilde{\alpha}$ *be two normal elements of* $\mathrm{GF}(r)$ *over* $\mathrm{GF}(q)$*. Define*

$$\lambda = \sum_{i=0}^{n-1} \lambda_i \alpha^{q^i} \quad \textit{and} \quad \tilde{\lambda} = \sum_{i=0}^{n-1} \lambda_i \tilde{\alpha}^{q^i},$$

where $\lambda_i \in \mathrm{GF}(q)$ *for all* i*. Then the two codes* $\mathcal{C}_\lambda$ *and* $\mathcal{C}_{\tilde{\lambda}}$ *are identical.*

Proof. The conclusion of this theorem follows from the proof of Theorem 4.6. □

The following theorem is easy to prove. We omit its proof.

Theorem 4.9. *Let* λ *and* $\tilde{\lambda}$ *be two elements of* $\mathrm{GF}(r)$*. Then* $\mathcal{C}_\lambda = \mathcal{C}_{\tilde{\lambda}}$ *if*

- $\tilde{\lambda} = \lambda^{q^i}$ *for some* i *with* $0 \leqslant i \leqslant n-1$*, or*
- $\tilde{\lambda} = b\lambda$ *for some* $b \in \mathrm{GF}(q)^*$*.*

4.3. *Every cyclic code over* GF(q) *is a* q*-polynomial code*

One basic question concerning the q-polynomial approach is whether every cyclic code of length n over $\mathrm{GF}(q)$ can be expressed as the code $\mathcal{C}_\beta$ of (8) for some $\beta \in \mathrm{GF}(q^n)$. The answer to this question is given in the following theorem.

Theorem 4.10. *Every cyclic code of length* n *over* $\mathrm{GF}(q)$ *can be expressed as the code* $\mathcal{C}_\beta$ *of* (8) *for some* $\beta \in \mathrm{GF}(q^n)$*, and is thus a* q*-polynomial code.*

Proof. Every cyclic code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$ must have a generator polynomial $g(x)$ over $\mathrm{GF}(q)$ that divides $x^n - 1$. The reciprocal $g^*(x)$ also divides $x^n - 1$. Let ϵ be the constant term of $g(x)$. Then $\epsilon \neq 0$. The monic polynomial $\epsilon^{-1} g^*(x)$ must be factorized into a product of the form

$$\epsilon^{-1} g^*(x) = g_1(x)^{e_1} g_2(x)^{e_2} \cdots g_t(x)^{e_t}$$

where t and e_i $(1 \leqslant i \leqslant t)$ are positive integers, and $g_i(x)$ $(1 \leqslant i \leqslant t)$ are pairwise distinct irreducible monic polynomials over $\mathrm{GF}(q)$.

Assume that the degree of the polynomial $g_i(x)^{e_i}$ is σ_i for each i. Denote by $\delta^{(i)}$ the sequence generated by the characteristic polynomial $g_i(x)^{e_i}$ and the initial seed

$$\left(\delta_0^{(i)}, \delta_1^{(i)}, \ldots, \delta_{\sigma_i-2}^{(i)}, \delta_{\sigma_i-1}^{(i)}\right) = (0, 0, \ldots, 0, 1).$$

Such a sequence is called an *impulse response* sequence [12, Section 4]. The sequences $\delta^{(i)}$ are eventually periodic (i.e., after deleting an initial segment, the sequences become periodic). Let $(\delta^{(i)})^\infty$ be a periodic sequence after deleting an initial segment of $\delta^{(i)}$. By Corollary 8.52 in [12, Section 4], the characteristic polynomial $g_i(x)^{e_i}$ is the minimal polynomial of the sequence $(\delta^{(i)})^\infty$. Let λ^∞ be the sum of the sequences $(\delta^{(1)})^\infty$, $(\delta^{(2)})^\infty$, $\ldots$, $(\delta^{(t)})^\infty$. Since all the polynomials $g_i(x)$ are pairwise distinct and irreducible over GF(q), it follows from Theorem 8.55 in [12] that the minimal polynomial of λ^∞ is equal to $\epsilon^{-1}g^*(x) = \prod_{i=1}^t g_i(x)^{e_i}$.

Let λ be defined as in (9), where these λ_i are the entries of the sequence λ^∞ just defined above. It follows from Theorem 4.6 that the code $\mathcal{C}_\lambda$ of (8) has generator polynomial $g(x)$, and is thus equal to the code $\mathcal{C}$. This completes the proof. □

The proof of this theorem is constructive and can be employed to find the code $\mathcal{C}_\lambda$ given a cyclic code $\mathcal{C}$. However, it may not be convenient to use it.

4.4. Fundamental questions on the q-polynomial approach to cyclic codes

In Section 4.3, it is proved that every cyclic code of length n over GF(q) is a q-polynomial code $\mathcal{C}_\lambda$ for some $\lambda \in \mathrm{GF}(r)$, where $r = q^n$. The following are fundamental questions regarding the q-polynomial approach to cyclic codes.

1. How to express a known class of cyclic codes as q-polynomial codes $\mathcal{C}_\lambda$ by choosing an element $\lambda \in \mathrm{GF}(r)$?
2. How to use the q-polynomial expression $\mathcal{C}_\lambda$ of a cyclic code over GF(q) to prove new properties for the code?
3. How to construct a new cyclic code $\mathcal{C}_\lambda$ with desirable parameters and good error-correcting capability by choosing a proper $\lambda \in \mathrm{GF}(r)$?

These problems are to be investigated and answered. There would be many ways to choose a $\lambda \in \mathrm{GF}(r)$ regarding the first and third questions. In this paper, we consider two methods. The first one is to choose $\lambda = \gamma^i$, where γ is a fixed generator of $\mathrm{GF}(r)^*$ and i is a properly chosen integer with $0 \leqslant i \leqslant r-2$. In this way, the problem of choosing a λ becomes that of choosing the integer i.

The second method for choosing a $\lambda \in \mathrm{GF}(r)$ is to fix a normal element α of GF(r) over GF(q), then choose a sequence $\lambda^\infty = (\lambda_i)_{i=0}^\infty$ of period n over GF(q), and finally define

$$\lambda = \sum_{i=0}^{n-1} \lambda_i \alpha^{q^i}.$$

In this way, the problem of choosing a λ becomes that of choosing the sequence λ^∞. By Theorem 4.8, the code $\mathcal{C}_\lambda$ depends only on the sequence λ^∞ and is independent of the choice of the normal element α.

Both methods have their advantages and disadvantages. In this paper, we consider both of them.

A key question regarding this paper is the following:

Key Question 4.11. *Is the q-polynomial approach to cyclic codes really useful*?

We will justify that this new approach to cyclic codes could be useful in Section 5 by constructing a family of almost optimal cyclic codes with this approach.

5. A family of almost optimal *q*-polynomial codes

As a justification of the usefulness of the q-polynomial approach to cyclic codes, we introduce a family of almost optimal cyclic codes defined with this approach in this section. To this end, we need the following lemma that follows directly from Lemma 3.3 with $N = q+1$.

Lemma 5.1. *Let $t \geqslant 2$ be even. Define $n = (q^t-1)/(q+1)$ and*

$$\lambda_i = \mathrm{Tr}_{q^t/q}\left(\eta^i\right)$$

for all $i \geqslant 0$, where $\eta = \zeta^{q+1}$ and ζ is a generator of $\mathrm{GF}(q^t)^*$. Then the sequence has period n.

When $t \geqslant 4$, the linear span of the sequence λ^∞ is equal to t and the minimal polynomial of the sequence λ^∞ is

$$P(x) = \prod_{j=0}^{t-1}\left(x - \eta^{q^j}\right), \tag{15}$$

where $\eta = \zeta^{q+1}$.

Theorem 5.2. *Let $t \geqslant 4$ be an even integer, and let $n = (q^t-1)/(q+1)$. Let λ^∞ be the sequence over $\mathrm{GF}(q)$ defined in Lemma 5.1, and let λ be defined as in (9). The set $\mathcal{C}_\lambda$ of (8) is a cyclic code over $\mathrm{GF}(q)$ with parameters $[n, n-t, d]$, where*

$$d = \begin{cases} 2 & \text{if } q > 2, \\ 5 & \text{if } q = 2 \text{ and } t = 4, \\ 3 & \text{if } q = 2 \text{ and } t > 4. \end{cases} \tag{16}$$

In addition, the polynomial $P(x)$ of (15) is the generator polynomial of the code $\mathcal{C}_\lambda$.

Proof. Let $C_0^{(q+1,q^t)} = \langle \zeta^{q+1} \rangle$, the subgroup of $\mathrm{GF}(q^t)^*$ generated by ζ^{q+1}, where ζ is a generator of $\mathrm{GF}(q^t)^*$. Since $(q+1)$ divides $(q^t-1)/(q-1)$, $\mathrm{GF}(q)^* \subset C_0^{(q+1,q^t)}$. Hence

$$\mathrm{GF}(q)^* \cap C_0^{(q+1,q^t)} = \mathrm{GF}(q)^*. \tag{17}$$

The matrix B_λ of (10) has rank t, as the linear span of the periodic sequences λ^∞ is t by Lemma 5.1. By Theorem 4.3, the dimension is $k = \frac{q^t-1}{q+1} - t$.

Since $\lambda \neq 0$, $d \geqslant 2$. The proof of Theorem 4.3 shows that the matrix B_λ of (10) is a parity-check matrix of the code $\mathcal{C}_\lambda$. Hence, $d = 2$ if and only if two different columns of the matrix B_λ are linearly dependent over $\mathrm{GF}(q)$. Note that B_λ is circulant. We have $d = 2$ if and only if there exist a $u \in \mathrm{GF}(q)^*$ and a $1 \leqslant h \leqslant n-1$ such that

$$\mathrm{Tr}_{q^t/q}\left(\eta^{i+h}\right) = u\,\mathrm{Tr}_{q^t/q}\left(\eta^i\right) = 0 \quad \text{for all } 0 \leqslant i \leqslant n-1,$$

which is equivalent to

$$\mathrm{Tr}_{q^t/q}\left(\eta^i\left(\eta^h - u\right)\right) = 0 \quad \text{for all } 0 \leqslant i \leqslant n-1. \tag{18}$$

When $q > 2$, it follows from (17) that there is a $u \in \mathrm{GF}(q)^* \setminus \{1\}$ such that $u = \eta^h$ for some $1 \leqslant h \leqslant n-1$. Hence, the minimum distance $d = 2$.

When $q=2$, then the only choice for u is $u=1$. In this case, there is no $1 \leqslant h \leqslant n-1$ with $\eta^h = 1$. Hence in this case $d \geqslant 3$. When $(q,t)=(2,4)$, it is easily checked that $\mathcal{C}_\lambda$ is a $[5,1,5]$ cyclic code. Now we assume that $q=2$ and $t>4$, and prove that $d=3$. Note that $d=3$ if and only if three different columns of the matrix B_λ are linearly dependent over GF(q). Note that B_λ is circulant. Then $d=3$ if and only if there exist two distinct integers $1 \leqslant h_1 \leqslant n-1$ and $1 \leqslant h_2 \leqslant n-1$ such that

$$\mathrm{Tr}_{q^t/q}\big(\eta^{i+h_2}\big) + \mathrm{Tr}_{q^t/q}\big(\eta^{i+h_1}\big) + \mathrm{Tr}_{q^t/q}\big(\eta^{i}\big) = 0 \quad \text{for all } 0 \leqslant i \leqslant n-1,$$

which is equivalent to

$$\mathrm{Tr}_{q^t/q}\big(\eta^i\big(\eta^{h_2}+\eta^{h_1}+1\big)\big) = 0 \quad \text{for all } 0 \leqslant i \leqslant n-1. \tag{19}$$

It is known that $|C_0^{(q+1,q^t)} \cap (C_0^{(q+1,q^t)}+1)| > 0$ [2,3]. Hence there exist two distinct integers $1 \leqslant h_1 \leqslant n-1$ and $1 \leqslant h_2 \leqslant n-1$ such that

$$\eta^{h_2}+\eta^{h_1}+1=0.$$

It follows that $d=3$ if $q=2$ and $t>4$.

The conclusion on the generator polynomial follows from Theorem 4.6 and Lemma 5.1. □

It follows from the Sphere Packing bound that the dimension of any binary linear code with length $n=(2^t-1)/3$ and minimum distance $d=3$ is at most $n-t+1$. Since the binary code $\mathcal{C}_\lambda$ of Theorem 5.2 has dimension $n-t$, it is an almost optimal linear code.

Example 5.3. Let $(q,t)=(2,6)$. Then $n=(q^t-1)/(q+1)=21$. Let γ be a generator of GF$(q^n)^*$ with $\gamma^{21}+\gamma^6+\gamma^5+\gamma^2+1=0$. Let the normal element α of GF(q^n) over GF(q) be

$$\begin{aligned}\alpha = {} & \gamma^{20}+\gamma^{19}+\gamma^{18}+\gamma^{17}+\gamma^{16}+\gamma^{13}+\gamma^{11} \\ & +\gamma^9+\gamma^8+\gamma^7+\gamma^6+\gamma^5+\gamma^4+\gamma^2+\gamma.\end{aligned}$$

Let ζ be a generator of GF$(q^t)^*$ with minimal polynomial $\zeta^6+\zeta^4+\zeta^3+\zeta+1=0$ over GF(q). The sequence

$$(\lambda_i)_{i=0}^{20} = (011010011001001010000)$$

has linear span 6. Hence

$$\lambda = \gamma^{20}+\gamma^{16}+\gamma^{15}+\gamma^{14}+\gamma^{13}+\gamma^7+\gamma^6+\gamma^5+\gamma^3+1.$$

Then $\mathcal{C}_\lambda$ is a $[21,15,3]$ cyclic code over GF(2) with generator polynomial $x^6+x^5+x^4+x^2+1$ and weight enumerator

$$\begin{aligned}& 1+28y^3+84y^4+273y^5+924y^6+1956y^7+2982y^8 \\ & +4340y^9+5796y^{10}+5796y^{11}+4340y^{12}+2982y^{13} \\ & +1956y^{14}+924y^{15}+273y^{16}+84y^{17}+28y^{18}+y^{21}.\end{aligned}$$

This is the best binary cyclic code with length 21 and dimension 15 according to our exhaustive experimental results, while the optimal linear code of length 21 and dimension 15 in the Database has minimum distance 4.

Example 5.4. Let $(q,t)=(2,8)$. Then $n=(q^t-1)/(q+1)=85$. Let γ be a generator of $\mathrm{GF}(q^n)^*$ with

$$\gamma^{85}+\gamma^{22}+\gamma^{20}+\gamma^{18}+\gamma^{16}+\gamma^{15}+\gamma^{14}+\gamma^{7}+\gamma^{6}+\gamma^{2}+1=0.$$

Then $\mathcal{C}_\lambda$ is an $[85,77,3]$ cyclic code over GF(2) with generator polynomial

$$1+x+x^2+x^4+x^5+x^7+x^8.$$

This is the best binary cyclic code with length 85 and dimension 77 according to our experimental results, while the optimal linear code of length 85 and dimension 77 in the Database has minimum distance 4.

6. Earlier related works

There has been some prior work on the use of q-polynomials for the construction of codes. In particular, using q-polynomial evaluations, Gabidulin [8] defined a type of codes, commonly called *Gabidulin codes*, with rank metric. These codes are defined over some extension field $\mathrm{GF}(q^N)$ of $\mathrm{GF}(q)$, and the q-polynomials employed take coefficients in $\mathrm{GF}(q^N)$.

A subclass of the Gabidulin codes consists of the so-called q-cyclic codes, which are defined as follows [8]. An $[n,k]$ code $\mathcal{C}$ over $\mathrm{GF}(q^N)$ is called q-cyclic if $(c_0,c_1,\ldots,c_{n-1})\in\mathcal{C}$ implies that $(c_{n-1}^q,c_0^q,c_1^q,\ldots,c_{n-2}^q)\in\mathcal{C}$. These codes are generalizations of cyclic codes: the case where $N=1$ corresponds precisely to cyclic codes over $\mathrm{GF}(q)$. However, even in this case, the Gabidulin codes are equipped with the rank metric while classical cyclic codes are normally associated with the Hamming metric. These two metrics are clearly different: when $N=1$, the rank distance between two codewords of length n is always bounded above by 1, which is not the case with the Hamming metric. Furthermore, [8] only considers q-cyclic codes in the case $n=N$. With this restriction, a q-cyclic code is a cyclic code over $\mathrm{GF}(q)$ if and only if $n=1$. In other words, a q-cyclic code is not a q-polynomial code studied above (due to Theorem 4.10) if the length $n>1$.

In a different direction, Boucher, Geiselmann and Ulmer introduced another generalization of cyclic codes, in the form of skew-cyclic codes or θ-cyclic codes [5,4]. Let θ be an automorphism of $\mathrm{GF}(q)$. A linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ is said to be θ-cyclic if $(c_0,c_1,\ldots,c_{n-1})\in\mathcal{C}$ implies that $(\theta(c_{n-1}),\theta(c_0),\ldots,\theta(c_{n-2}))\in\mathcal{C}$. The case where θ is the identity automorphism corresponds to cyclic codes.

Let λ be an element of $\mathrm{GF}(q^n)^*$. Define

$$\bar{\mathcal{C}}_\lambda=\left\{(c_0,c_1,\ldots,c_{n-1})\in\big(\mathrm{GF}(q^n)\big)^n\colon \sum_{i=0}^{n-1}c_i\lambda^{q^i}=0\right\}. \tag{20}$$

Then the q-polynomial code $\mathcal{C}_\lambda$ defined in (8) is a subfield subcode of the code $\bar{\mathcal{C}}_\lambda$ defined above, by restricting the coordinates to $\mathrm{GF}(q)$. It is easily seen that $\bar{\mathcal{C}}_\lambda$ is a θ-cyclic code, where θ is the Frobenius automorphism of $\mathrm{GF}(q^n)$. Hence every q-polynomial code is a subfield subcode of a skew-cyclic code over an extension field, so is every cyclic code over $\mathrm{GF}(q)$ (due to Theorem 4.10).

7. Summary and concluding remarks

The contributions of this paper are the following:

1. The introduction of the q-polynomial approach to cyclic codes over $\mathrm{GF}(q)$ and the establishment of the theoretical foundations of this approach in Section 4.
2. The construction of a class of q-polynomial codes in Section 5, which are almost optimal when $q=2$.

The discovery of the family of almost optimal cyclic codes of Section 5 demonstrates that the q-polynomial approach to cyclic codes could be promising. It would be an interesting problem to employ the q-polynomial approach to construct more new cyclic codes with desirable parameters and good error-correcting capability. The reader is cordially invited to join this adventure.

It would be worthwhile to note that we provided information on the generator polynomial of q-polynomial codes whenever this is possible. This should not give the reader the incorrect impression that it is unnecessary to develop the q-polynomial approach to cyclic codes.

Acknowledgments

The authors are very grateful to the reviewers for their detailed comments and suggestions that improved the quality and presentation of this paper, and also to Dr. Somphong Jitman and Dr. Qi Wang for helpful discussions.

Cunsheng Ding's research is supported by the Hong Kong Research Grants Council (grant No. 600812). San Ling's research is supported by the Singapore National Research Foundation Competitive Research Programme (grant No. NRF-CRP2-2007-03).

References

[1] M. Antweiler, L. Bomer, Complex sequences over GF(p^M) with a two-level autocorrelation function and a large linear span, IEEE Trans. Inform. Theory 38 (1992) 120–130.
[2] L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, Inf. Control 20 (1972) 158–175.
[3] L.D. Baumert, W.H. Mills, R.L. Ward, Uniform cyclotomy, J. Number Theory 14 (1982) 67–82.
[4] D. Boucher, F. Ulmer, Coding with skew polynomials rings, J. Symbolic Comput. 44 (2009) 1644–1656.
[5] D. Boucher, W. Geiselmann, F. Ulmer, Skew cyclic codes, Appl. Algebra Engrg. Comm. Comput. 18 (2007) 379–389.
[6] R.T. Chien, Cyclic decoding procedure for the Bose–Chaudhuri–Hocquenghem codes, IEEE Trans. Inform. Theory 10 (1964) 357–363.
[7] P. Delsarte, On subfield subcodes of modified Reed–Solomon codes, IEEE Trans. Inform. Theory 21 (1975) 575–576.
[8] E.M. Gabidulin, Theory of codes with maximum rank distance, Probl. Inf. Transm. 21 (1985) 1–12.
[9] G.L. Feng, K.K. Tzeng, Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations, IEEE Trans. Inform. Theory 37 (6) (1991) 1716–1723.
[10] G.D. Forney, On decoding BCH codes, IEEE Trans. Inform. Theory 11 (1965) 549–557.
[11] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[12] L. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[13] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Math. Library, vol. 16, North-Holland, Amsterdam, 1977.
[14] E. Prange, Some cyclic error-correcting codes with simple decoding algorithms, Air Force Cambridge Research Center-TN-58-156, Cambridge, MA, 1958.
[15] C. Rong, T. Helleseth, Use characteristic sets to decode cyclic codes up to actual minimum distance, in: London Math. Soc. Lecture Note Ser., vol. 233, 1996, pp. 297–312.
[16] T. Schaub, A linear complexity approach to cyclic codes, Dissertation ETH No. 8730 in Technical Sciences, Swiss Federal Inst. of Tech., Zurich, 1988.