Binary cyclic codes from explicit polynomials over GF($2^m$)$^\star$

Cunsheng Ding$^a$, Zhengchun Zhou$^b,*$

$^a$ Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

$^b$ School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China

A R T I C L E   I N F O

Article history:
Received 14 August 2013
Received in revised form 18 December 2013
Accepted 23 December 2013

Keywords:
Polynomials
Permutation polynomials
Cyclic codes
Linear span
Sequences

A B S T R A C T

Cyclic codes are a subclass of linear codes and have applications in consumer electronics, data storage systems, and communication systems as they have very efficient encoding and decoding algorithms. In this paper, monomials and trinomials over finite fields with even characteristic are employed to construct a number of families of binary cyclic codes. Lower bounds on the minimum weight of some families of the cyclic codes are developed. The minimum weights of other families of the codes constructed in this paper are determined. The dimensions of the codes are flexible. Some of the codes presented in this paper are optimal or almost optimal in the sense that they meet some bounds on linear codes. Open problems regarding binary cyclic codes from monomials and trinomials are also presented.

© 2014 Published by Elsevier B.V.

1. Introduction

Let $q$ be a power of a prime $p$. A linear $[n, k, d]$ code over $GF(q)$ is a $k$-dimensional subspace of $GF(q)^n$ with minimum Hamming distance $d$. A linear $[n, k]$ code $C$ over the finite field $GF(q)$ is called cyclic if $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in GF(q)^n$ with $\sum_{i=0}^{n-1} c_i x^i \in GF(q)[x]/(x^n - 1)$, any code $C$ of length $n$ over $GF(q)$ corresponds to a subset of $GF(q)[x]/(x^n - 1)$. The linear code $C$ is cyclic if and only if the corresponding subset in $GF(q)[x]/(x^n - 1)$ is an ideal of the ring $GF(q)[x]/(x^n - 1)$. It is well known that every ideal of $GF(q)[x]/(x^n - 1)$ is principal. Let $C = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree. Then $g(x)$ is called the generator polynomial and $h(x) = (x^n - 1)/g(x)$ is referred to as the parity-check polynomial of $C$.

Cyclic codes have wide applications in storage and communication systems because they afford efficient encoding and decoding algorithms [5,12,27]. Cyclic codes have been studied for decades and a lot of progress has been made (see for example, [3,4,9–11,13,16,14,17,18,22,21,25,24,26,28,30]). The total number of cyclic codes over $GF(q)$ and their constructions are closely related to $q$-cyclotomic cosets modulo $n$, and thus many topics of number theory. One way of constructing cyclic codes over $GF(q)$ of length $n$ is to use the generator polynomial

$$\frac{x^n - 1}{\text{gcd}(S^n(x), x^n - 1)}$$

$^\star$ C. Ding’s research was supported by The Hong Kong Research Grants Council, Proj. No. 601013. Z. Zhou’s research was supported by the Natural Science Foundation of China under Grants 61201243 and 61373009, and the application fundamental research plan project of Sichuan Province under Grant 2013Y0167, and the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2013D10. Z. Zhou is also with National Mobile Communications Research Laboratory, Southeast University.

* Corresponding author.

E-mail addresses: cding@ust.hk (C. Ding), zzc@home.swjtu.edu.cn (Z. Zhou).

0012–365X/$–$ see front matter © 2014 Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.disc.2013.12.020
Lemma 2. Let \( s^\infty \) be a sequence over \( GF(q) \) of period \( q^m - 1 \) with the expansion in (3). Let the index set be \( I = \{i | c_i \neq 0\} \), then the minimal polynomial \( M_i(x) \) of \( s^\infty \) is \( M_i(x) = \prod_{i \in I}(1 - \alpha^i x) \), and the linear span of \( s^\infty \) is \( |I| \).

An alternative way to compute the linear span and minimal polynomial of \( M_i(x) \) is based on (3) and a result in [1].
Proof. According to Theorem 3 in [1], the reciprocal polynomial of $M_n(x)$ is given by $\prod_{i \in I} (x - \alpha^i)$. Thus we have $M_n(x) = x^{|I|} \prod_{i \in I} (1/x - \alpha^i) = \prod_{i \in I} (1 - \alpha^i x)$

which completes the proof. □

2.3. The 2-cyclotomic cosets modulo $2^m - 1$

Let $n = 2^m - 1$. The 2-cyclotomic coset containing $j$ modulo $n$ is defined by $C_j = \{ j, 2j, 2^2j, \ldots, 2^{\ell_j - 1} j \} \subset \mathbb{Z}_n$, where $\ell_j$ is the smallest positive integer such that $2^{\ell_j} j \equiv j \pmod{n}$. Clearly $\ell_j$ is also the size of $C_j$. It is known that $\ell_j$ divides $m$. The smallest integer in $C_j$ is called the coset leader of $C_j$. Let $\Gamma^*$ denote the set of all coset leaders and write $\Gamma^* = \Gamma \setminus \{0\}$. By definition, we have

$\bigcup_{j \in \Gamma} C_j = \mathbb{Z}_n := \{ 0, 1, 2, \ldots, n - 1 \}$

and

$C_i \cap C_j = \emptyset$ for any $i \neq j \in \Gamma$.

For any integer $j$ with $0 \leq j \leq 2^m - 1$, the 2-weight of $j$, denoted by $wt(j)$, is defined as the number of nonzero coefficients in its 2-adic expansion:

$j = j_0 + j_1 \cdot 2 + \cdots + j_{m-1} \cdot 2^{m-1}$, $j_i \in \{ 0, 1 \}$

The following lemmas will be useful in the sequel.

Lemma 3 ([29]). For any coset leader $j \in \Gamma^*$, $j$ is odd and $1 \leq j < 2^{n-1}$.

Lemma 4. For any $j \in \Gamma^*$ with $\ell_j = m$, the number of odd and even integers in the 2-cyclotomic coset $C_j$ are equal respectively to $wt(j)$ and $m - wt(j)$.

Proof. By Lemma 3, $j$ is odd. Then we can assume that $j = 1 + 2^{i_1} + 2^{i_2} + \cdots + 2^{i_{k-1}}$ where $k = wt(j)$ and $1 \leq i_1 < i_2 < \cdots < i_{k-1} \leq m - 1$. It is easy to check that the odd integers in $C_j$ are given by

$j, j2^{m-i_{k-1}} \mod n, j2^{m-i_{k-2}} \mod n, \ldots, j2^{m-i_1} \mod n$ (4)

which are pairwise distinct due to $\ell_j = m$. Thus the number of odd integers in the 2-cyclotomic coset $C_j$ is equal to $k$ and the number of even ones is equal to $m - k$. □

Lemma 5. All integers $1 \leq j \leq 2^m - 2$ with $wt(j) = m - 1$ are in the same 2-cyclotomic coset.

Proof. It is clear that the number of integers $1 \leq j \leq 2^m - 2$ with $wt(j) = m - 1$ is equal to $m$. Note that all the integers in the same coset have the same weight. The conclusion then follows from the facts that $wt(2^{m-1} - 1) = m - 1$ and $\ell_{2^{m-1}} = m$. □

Lemma 6. Let $h$ be an integer with $1 \leq h \leq \lceil \frac{m+1}{2} \rceil$ and $\Gamma_1 = \{ 1 \leq j \leq 2^h - 1 : j \text{ is odd} \}$. Then for any $j \in \Gamma_1$,

- $j$ is the coset leader of $C_j$;
- $\ell_j = m$ except that $\ell_{2^{m/2+1}} = m/2$ for even $m$.

Proof. We begin with the first assertion. For any $j \in \Gamma_1$, let $wt(j) = k$ and $j = 1 + 2^{i_1} + 2^{i_2} + \cdots + 2^{i_{k-1}}$, where $1 \leq i_1 < i_2 < \cdots < i_{k-1} \leq h - 1$. It follows from Lemma 3 that the coset leader must be odd. By Lemma 4, all the odd integers in the 2-cyclotomic coset containing $j$ are listed in (4) in which the least one is exactly $j$ due to $i_t \leq m/2$ for all $1 \leq t \leq k - 1$. This finishes the proof of the first assertion.

We now prove the second one. Note that for each $j \in \Gamma_1$, $\ell_j | m$ and $j$ is divisible by $(2^m - 1)/(2^j - 1)$. When $m$ is odd, if $\ell_j < m$, then $\ell_j \leq m/3$ and thus $(2^m - 1)/(2^j - 1) > 2^{m/3}$ which means that $j > 2^{m/3}$. This is impossible since $j < 2^{(m+1)/2}$. Thus $\ell_j = m$ for odd $m$. Similarly, when $m$ is even, if $\ell_j < m$, then $\ell_j \leq m/2$ and $(2^m - 1)/(2^j - 1) > 2^{m/2}$. It is easy to check that $j \in \Gamma_1$ is divisible by $(2^m - 1)/(2^j - 1)$ if and only if $j = 2^{m/2} + 1$ and $\ell_j = m/2$. □

2.4. PN and APN functions

A polynomial $f(x)$ over $\text{GF}(r)$ is called almost perfect nonlinear (APN) if

$$\max_{a \in \text{GF}(r)} \max_{b \in \text{GF}(r)} |\{x \in \text{GF}(r) : f(x + a) - f(x) = b\}| = 2,$$
and is referred to as perfect nonlinear or planar if
\[
\max_{a \in \text{GF}(r)^*} \max_{b \in \text{GF}(r)} |x \in \text{GF}(r) : f(x + a) - f(x) = b| = 1.
\]
In subsequent sections, we shall use the notions of PN and APN functions.

3. Codes defined by polynomials over finite fields $\text{GF}(r)$

3.1. A generic construction of cyclic codes with polynomials

Given any polynomial $f(x)$ over $\text{GF}(r)$, we define its associated sequence $s^\infty$ by
\[
s_i = \text{Tr}(f(\alpha^i + 1)) \quad (5)
\]
for all $i \geq 0$.

The objective of this paper is to consider the codes $C_s$ defined by some monomials and trinomials over $\text{GF}(2^m)$.

3.2. How to choose the polynomial $f(x)$

Regarding the generic construction of Section 3.1, the following two questions are natural.

• Is it possible to construct optimal cyclic codes meeting some bound on parameters of linear codes or cyclic codes with good parameters?
• If the answer to the question above is positive, how should we select the polynomial $f(x)$ over $\text{GF}(r)$?

It will be demonstrated in the sequel that the answer to the first question is indeed positive. However, it seems harder to answer the second question.

Any method of constructing an $[n, k]$ cyclic code over $\text{GF}(q)$ corresponds to the selection of a divisor $g(x)$ over $\text{GF}(q)$ of $x^n - 1$ of degree $n - k$, which is employed as the generator polynomial. The minimum weight $d$ and other parameters of this cyclic code are determined by the generator polynomial $g(x)$.

Suppose that an optimal $[n, k]$ cyclic code over $\text{GF}(q)$ exists. The question is how to determine a divisor $g(x)$ of $x^n - 1$ generating such a code. Note that $x^n - 1$ may have many divisors of small degrees. If the construction method is not well designed, optimal cyclic codes cannot be produced even if they exist.

The construction of Section 3.1 may produce cyclic codes with bad parameters. For example, let $(q, m) = (2, 6)$, let $\alpha$ be the generator of $\text{GF}(2^6)$ with $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$, and let $f(x) = x^\alpha$. When $e \in \{7, 14, 28, 35, 49, 56\}$, the binary code $C_s$ defined by the monomial $f(x)$ has parameters $[63, 45, 3]$. These codes are very bad as there are binary cyclic codes with parameters $[63, 45, 8]$ and $[63, 57, 3]$.

On the other hand, the construction of Section 3.1 may also produce optimal cyclic codes. For example, let $(q, m) = (2, 6)$ and $f(x) = x^{e}$. When
\[
e \in \{1, 2, 4, 5, 8, 10, 16, 17, 20, 32, 34, 40\},
\]
the binary code $C_s$ defined by the monomial $f(x)$ has parameters $[63, 57, 3]$ and is equivalent to the binary Hamming code with the same parameters. This cyclic code is optimal, as it attains the sphere packing bound.

Hence, a monomial may determine either good or bad cyclic codes within the framework of the construction of Section 3.1. Now the question is how to choose a monomial $f(x)$ over $\text{GF}(r)$ so that the cyclic code $C_s$ defined by $f(x)$ has good parameters.

In this paper, we employ monomials and trinomials $f(x)$ over $\text{GF}(r)$ that are either permutations on $\text{GF}(r)$ or such that $|f(\text{GF}(r)))|$ is very close to $r$. Most of the monomials and trinomials $f(x)$ employed in this paper are either almost perfect nonlinear or planar functions on $\text{GF}(r)$. These polynomials are considered here as their image size $|f(\text{GF}(r)))|$ is at least $r/2$ and they produce cyclic codes with good parameters.

Observe that it is unnecessary to require that $f(x)$ is highly nonlinear, in order to obtain cyclic codes $C_s$ with good parameters. Both linear and highly nonlinear polynomials $f(x)$ could give optimal cyclic codes $C_s$ when they are plugged into the generic construction of Section 3.1. In subsequent sections, some PN and APN monomials will be employed to obtain optimal cyclic codes $C_s$. When $m$ is even and $f(x) = x^{e}$, the code $C_s$ has parameters $[2^m - 1, 2^m - 1 - m, 3]$ and is optimal. Hence, linear permutations $f(x)$ may yield optimal cyclic codes $C_s$ when they are plugged into the construction method described above.

4. Binary cyclic codes from the permutation monomial $f(x) = x^{2^t+3}$

In this section we study the code $C_s$ defined by the permutation monomial $f(x) = x^{2^t+3}$ over $\text{GF}(2^{2t+1})$. Before doing this, we need to prove the following lemma.

Lemma 7. Let $m = 2t + 1 \geq 7$. Let $s^\infty$ be the sequence of (5), where $f(x) = x^{2^t+3}$. Then the linear span $L_s$ of $s^\infty$ is equal to $5m + 1$ and the minimal polynomial $M_s(x)$ of $s^\infty$ is given by
\[
M_s(x) = (x - 1)m_{2^t-1}(x)m_{2^t-3}(x)m_{2^t-2}(x)m_{2^t-1}(x)m_{2^t}(x)m_{2^t+1}(x).
\]

(6)
Proof. By definition, we have
\[ s_t = \text{Tr} \left( (\alpha^t + 1)^{2^{t+2} + 1} \right) \]
\[ = \text{Tr} \left( (\alpha^t)^{2^{t+3}} + (\alpha^t)^{2^{t+2}} + (\alpha^t)^{2^{t+1}} + (\alpha^t)^3 + 1 \right) \]
\[ = \sum_{j=0}^{m-1} (\alpha^t)^{(2^{t+3})j^2} + \sum_{j=0}^{m-1} (\alpha^t)^{(2^{t+2})j^2} + \sum_{j=0}^{m-1} (\alpha^t)^{(2^{t+1})j^2} + \sum_{j=0}^{m-1} (\alpha^t)^{3j^2} + \sum_{j=0}^{m-1} (\alpha^t)^{j^2} + 1. \quad (7) \]

By Lemma 6, the following 2-cyclotomic cosets are pairwise disjoint and have size \( m \):
\[ C_1, C_3, C_{2^t+1}, C_{2^t-1+1}. \quad (8) \]

It is clear that the 2-cyclotomic coset \( C_{2^t+3} \) is disjoint from all the cosets in (8). We now prove that \( C_{2^t+3} \) has size \( m \). It is sufficient to show that \( \gcd \) := \( \gcd(2^{t+1} - 1, 2^t + 3) = 1 \). The conclusion is true for all \( 1 \leq t \leq 4 \). So we consider only the case for \( t \geq 5 \).

Note that \( 2^{2^t+1} - 1 = (2^{t+1} - 6)(2^t + 3) + 17 \). We have \( \gcd = \gcd(2^t + 3, 17) \). Since \( 2^t + 3 = 2^t - 4(2^4 + 1) - (2^4 - 3) \), we obtain that \( \gcd = \gcd(2^t - 4, 17) \). Let \( t_1 = \lfloor t/4 \rfloor \). Using the Euclidean division recursively and the fact \( 2^4 \equiv -1 (\text{mod} \ 17) \), one gets
\[ \gcd = \begin{cases} 
\gcd((-1)^{t_1} - 1, 3, 17) = 1 & \text{if } t \equiv 0 \text{ (mod } 4) \\
\gcd((-1)^{t_1} - 2^1, 3, 17) = 1 & \text{if } t \equiv 1 \text{ (mod } 4) \\
\gcd((-1)^{t_1} - 2^2, 3, 17) = 1 & \text{if } t \equiv 2 \text{ (mod } 4) \\
\gcd((-1)^{t_1} - 2^3, 3, 17) = 1 & \text{if } t \equiv 3 \text{ (mod } 4) 
\end{cases} \]

Therefore, \( \ell_{2^t+3} = |C_{2^t+3}| = \ell_{2^t-1+3} = m \).

The desired conclusions on the linear span and the minimal polynomial \( M_s(x) \) then follow from Lemma 2, (7) and the results on the five cyclotomic cosets and their sizes. \( \square \)

The following theorem provides information on the code \( C_s \).

Theorem 8. Let \( m \geq 7 \) be odd. The binary code \( C_s \), defined by the sequence of Lemma 7 has parameters \([2^m - 1, 2^m - 2 - 5m, d]\) and generator polynomial \( M_s(x) \) of (6), where \( d \geq 8 \).

Proof. The dimension of \( C_s \) follows from Lemma 7 and the definition of the code \( C_s \). We need to prove the conclusion on the minimum distance of \( C_s \). To this end, let \( D_s \) denote the cyclic code with generator polynomial \( m_{s^{-1}}(x) = m_{s^{-1}}(\alpha x^r) \) of (6), and let \( D_s \) be the even-weight subcode of \( D_s \). Then \( D_s \) is a triple-error-correcting code for any \( j \) with \( \gcd(j, m) = 1 \) [19]. This means that the minimum distance of \( D_s \) is equal to 7 and that of \( D_s \) is 8. Take \( j = t \), then \( D_s \) has generator polynomial \( m_{s^{-1}}(x) = m_{s^{-1}}(x) \) and \( C_s \) is a subcode of \( D_s \). The conclusion then follows from the fact that \( x - 1 \) is a factor of \( M_s(x) \). \( \square \)

Example 1. Let \( m = 5 \) and \( \alpha \) be a generator of \( GF(2^m)^* \) with \( \alpha^2 + \alpha^2 + 1 = 0 \). Then the generator polynomial of the code \( C_s \) is \( M_s(x) = x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^6 + x^3 + 1 \), and \( C_s \) is a [31, 15, 8] binary cyclic code. Its dual is a [31, 16, 7] cyclic code. Both codes are optimal according to the Database.

Example 2. Let \( m = 7 \) and \( \alpha \) be a generator of \( GF(2^m)^* \) with \( \alpha^2 + \alpha + 1 = 0 \). Then the generator polynomial of the code \( C_s \) is \( M_s(x) = x^{36} + x^{34} + x^{33} + x^{32} + x^{29} + x^{28} + x^{27} + x^{26} + x^{23} + x^{24} + x^{21} + x^{12} + x^9 + x^8 + x^7 + x^5 + x^3 + x + 1 \) and \( C_s \) is a [127, 91, 8] binary cyclic code.

It can be seen from Example 2 that the bound on the minimal distance of \( C_s \) in Theorem 8 is tight in some cases.

5. Binary cyclic codes from the permutation monomial \( f(x) = x^{2^h-1} \)

Consider monomials over \( GF(2^m) \) of the form \( f(x) = x^{2^h-1} \), where \( h \) is a positive integer with \( 1 \leq h \leq \lceil \frac{m}{2} \rceil \).

In this section, we deal with the binary code \( C_s \) defined by the sequence \( s_{\infty} \) of (5), where \( f(x) = x^{2^h-1} \).

We need to do some preparations before presenting and proving the main results of this section. Let \( t \) be a positive integer. We define \( T = 2^t - 1 \). For any odd \( a \in \{1, 2, 3, \ldots, T\} \), define
\[ e_a^{(t)} = \begin{cases} 
1, & \text{if } a = 2^h - 1 \\
\log_2 \frac{T}{a}, & \text{if } 1 \leq a < 2^h - 1. 
\end{cases} \]

and
\[ k_a^{(t)} = e_a^{(t)} \mod 2. \quad (9) \]
Let
\[ B_a^{(t)} = \{ 2^i a : i = 0, 1, 2, \ldots, e_a^{(t)} - 1 \} . \]
Then it can be verified that
\[ \bigcup_{1 \leq 2j+1 \leq T} B_{2j+1}^{(t)} = \{ 1, 2, 3, \ldots, T \} \]
and
\[ B_a^{(t)} \cap B_b^{(t)} = \emptyset \]
for any pair of distinct odd numbers \( a \) and \( b \) in \( \{ 1, 2, 3, \ldots, T \} \).

The following lemma follows directly from the definitions of \( e_a^{(t)} \) and \( b_a^{(t)} \).

**Lemma 9.** Let \( a \) be an odd integer in \( \{ 0, 1, 2, \ldots, T \} \). Then
\[
\begin{align*}
B_a^{(t+1)} &= B_a^{(t)} \cup \{ a2^j \} \quad \text{if } 1 \leq a \leq 2^t - 1, \\
B_a^{(t+1)} &= \{ a \} \quad \text{if } 2^t + 1 \leq a \leq 2^{t+1} - 1, \\
e_a^{(t+1)} &= e_a^{(t)} + 1 \quad \text{if } 1 \leq a \leq 2^t - 1, \\
e_a^{(t+1)} &= 1 \quad \text{if } 2^t + 1 \leq a \leq 2^{t+1} - 1.
\end{align*}
\]

**Lemma 10.** Let \( N_t \) denote the total number of odd \( e_a^{(t)} \) when \( a \) ranges over all odd numbers in the set \( \{ 1, 2, \ldots, T \} \). Then \( N_1 = 1 \) and
\[ N_t = \frac{2^t + (-1)^{t-1}}{3} \]
for all \( t \geq 2 \).

**Proof.** It is easily checked that \( N_2 = 1, N_3 = 3 \) and \( N_4 = 5 \). It follows from Lemma 9 that
\[ N_t = 2^{t-2} + (2^{t-2} - N_{t-1}) \]
Hence
\[ N_t - 2^{t-2} = 2^{t-3} - (N_{t-1} - 2^{t-3}) = 3 \times 2^{t-4} + (N_{t-2} - 2^{t-4}) \]
With the recursive application of this formula, one obtains the desired expression for \( N_t \). \( \Box \)

**Lemma 11.** Let \( s^\infty \) be the sequence of (5), where \( f(x) = x^{2h-1}, 2 \leq h \leq \lceil \frac{m}{T} \rceil \). Then the linear span \( L_s \) of \( s^\infty \) is given by
\[
L_s = \begin{cases} 
\frac{m(2^h + (-1)^{h-1})}{3}, & \text{if } m \text{ is even} \\
\frac{m(2^h + (-1)^{h-1}) + 3}{3}, & \text{if } m \text{ is odd}.
\end{cases} \tag{10}
\]
We have thus
\[
M_s(x) = (x - 1)^{\sum_{2j+1}^m} \prod_{1 \leq 2j+1 \leq 2h-1 \atop x \in \{ 2j+1 \}} m_{x^{2j+1}}(x). \tag{11}
\]

**Proof.** We have
\[
\begin{align*}
\text{Tr}(f(x+1)) &= \text{Tr} \left( (x+1)^{\sum_{i=0}^{2h-1} x^i} \right) = \text{Tr} \left( \prod_{i=0}^{h-1} (x^i + 1) \right) = \text{Tr} \left( \sum_{i=0}^{2h-1} x^i \right) \\
&= \text{Tr}(1) + \text{Tr} \left( \sum_{i=1}^{2h-1} x^i \right) = \text{Tr}(1) + \text{Tr} \left( \sum_{1 \leq 2i+1 \leq 2h-1 \atop x \in \{ 2i+1 \}} \right) \tag{12}
\end{align*}
\]
where the last equality follows from Lemma 6.

By definition, the sequence of (5) is given by \( s_t = \text{Tr}(\alpha^i + 1) \) for all \( t \geq 0 \). The desired conclusions on the linear span and the minimal polynomial \( M_s(x) \) then follow from Lemmas 6 and 10 and Eq. (12). \( \Box \)

The following theorem provides information on the code \( C_s \).
Theorem 12. Let \( h \geq 2 \). The binary code \( C_{s} \) defined by the binary sequence of Lemma 11 has parameters \([2^{m} - 1, 2^{m} - 1 - \mathbb{L}_{s}, d]\) and generator polynomial \( M_{s}(x) \) of (11), where \( \mathbb{L}_{s} \) is given in (10) and

\[
\begin{cases}
  d \geq 2^{h-2} + 2 & \text{if } m \text{ is odd and } h > 2 \\
  2^{h-2} + 1 & \text{if } m \text{ is even and } h > 2,
\end{cases}
\]

Proof. The dimension of \( C_{s} \) follows from Lemma 11 and the definition of the code \( C_{s} \). We now derive lower bounds on the minimum weight \( d \) of the code. It is well known that the codes generated by \( M_{s}(x) \) and its reciprocal have the same weight distribution. It follows from Lemmas 9 and 11 that the reciprocal of \( M_{s}(x) \) has zeros \( \alpha^{2j+1} \) for all \( j \) in \([2^{h-2}, 2^{h-2} + 1, \ldots, 2^{h-1} - 1]\). By the Hartmann–Tzeng bound, we have \( d \geq 2^{h-2} + 1 \). If \( m \) is odd, \( C_{s} \) is an even-weight code. In this case, \( d \geq 2^{h-2} + 2 \). \( \Box \)

Example 3. Let \((m, h) = (7, 2)\) and \( \alpha \) be a generator of \( GF(2^{m}) \) with \( \alpha^{7} + \alpha + 1 = 0 \). Then the generator polynomial of the code \( C_{s} \) is \( M_{s}(x) = x^{8} + x^{6} + x^{5} + x^{4} + x^{3} + x^{2} + x + 1 \), and \( C_{s} \) is a \([127, 119, 4]\) binary cyclic code which is optimal according to the Database.

Example 4. Let \((m, h) = (7, 3)\) and \( \alpha \) be a generator of \( GF(2^{m}) \) with \( \alpha^{7} + \alpha + 1 = 0 \). Then the generator polynomial of the code \( C_{s} \) is \( M_{s}(x) = x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{8} + x^{7} + x^{6} + x^{5} + x^{4} + 1 \) and \( C_{s} \) is a \([127, 105, d] \) binary cyclic code, where \( 4 \leq d \leq 8 \).

Remark 13. The code \( C_{s} \) of Theorem 12 may be bad when \( \gcd(h, m) \neq 1 \). In this case the monomial \( f(x) = x^{2^{h}-1} \) is not a permutation of \( GF(2^{m}) \). For example, when \((m, h) = (6, 3)\), \( C_{s} \) is a \([63, 45, 3]\) binary cyclic code, while the best known linear code in the Database has parameters \([63, 45, 8]\). Hence, we are interested in this code only when \( \gcd(h, m) = 1 \), which guarantees that \( f(x) = x^{2^{h}-1} \) is a permutation of \( GF(2^{m}) \).

6. Binary cyclic codes from the permutation monomial \( f(x) = x^{e}, \, e = 2^{(m-1)/2} + 2^{(m-1)/4} - 1 \) and \( m \equiv 1 \pmod{4} \)

Let \( f(x) = x^{e} \), where \( e = 2^{(m-1)/2} + 2^{(m-1)/4} - 1 \) and \( m \equiv 1 \pmod{4} \). It can be proved that \( f(x) \) is a permutation of \( GF(r) \).

Define \( h = (m-1)/4 \). We have then

\[
\text{Tr}(f(x + 1)) = \text{Tr}\left( (x^{2^{h}} + 1)(x + 1)^{2^{h-1}} \right) = \text{Tr}\left( (x^{2^{h}} + 1) \prod_{i=0}^{h-1} (x^{2} + 1) \right)
\]

\[
= \text{Tr}\left( (x^{2^{h}} + 1) \sum_{i=0}^{2^{h}-1} x^{i} \right) = 1 + \text{Tr}\left( \sum_{i=0}^{2^{h}-1} x^{i+2^{2h}} + \sum_{i=1}^{2^{h}-1} x^{i} \right)
\]

(13)

The sequence \( s_{t} \) of (5) defined by the monomial \( f(x) = x^{e} \) is then given by

\[
s_{t} = 1 + \text{Tr}\left( \sum_{i=0}^{2^{h-1}} (\alpha^{f})^{i+2^{2h}} + \sum_{i=1}^{2^{h-1}} (\alpha^{f})^{i} \right)
\]

(14)

for all \( t \geq 0 \), where \( \alpha \) is a generator of \( GF(2^{m})^{*} \). In this section, we deal with the code \( C_{s} \) defined by the sequence \( s_{t} \) of (14).

To this end, we need to prove a number of auxiliary results on 2-cyclotomic cosets.

We define the following two sets for convenience:

\( A = \{0, 1, 2, \ldots, 2^{h} - 1\}, \quad B = 2^{2h} + A = \{i + 2^{2h} : i \in A\} \).

Lemma 14. For any \( j \in B \), we have \( \ell_{j} = |C_{j}| = m \).

Proof. Let \( j = 1 + 2^{2n} \), where \( i \in A \). For any \( u \) with \( 1 \leq u \leq m - 1 \), define

\[
\Delta_{1}(j, u) = j(2^{u} - 1) = (i + 2^{2h})(2^{u} - 1), \quad \Delta_{2}(j, u) = j(2^{m-u} - 1) = (i + 2^{2h})(2^{m-u} - 1).
\]

If \( \ell_{j} < m \), there would be an integer \( 1 \leq u \leq m - 1 \) such that \( \Delta_{1}(j, u) \equiv 0 \pmod{n} \) for all \( t \in \{1, 2\} \).

Note that \( 1 \leq u \leq m - 1 \). We have that \( \Delta_{1}(j, u) \neq 0 \) and \( \Delta_{2}(j, u) \neq 0 \). When \( u \leq m - 2h - 1 \), we have

\[
2^{h} \leq \Delta_{1}(j, u) \leq (2^{2h} + 2^{h} - 1)(2^{m-2h-1} - 1) < n.
\]

In this case, \( \Delta_{1}(j, u) \not\equiv 0 \pmod{n} \).

When \( u \geq m - 2h \), we have \( m - u \leq 2h \) and

\[
2^{h} \leq \Delta_{2}(j, u) \leq (2^{2h} + 2^{h} - 1)(2^{2h} - 1) < n.
\]

In this case, \( \Delta_{2}(j, u) \not\equiv 0 \pmod{n} \).

Combining the conclusions of the two cases above completes the proof. \( \Box \)

Lemma 15. For any pair of distinct \( i \) and \( j \) in \( B \), \( C_{i} \cap C_{j} = \emptyset \), i.e., they cannot be in the same 2-cyclotomic coset modulo \( n \).
Lemma 17. Let $i = i_1 + 2^{2h}$ and $j = j_1 + 2^{2h}$, where $i_1 \in A$ and $j_1 \in A$. Define

$$
\Delta_1(i, j, u) = j2^u - j - (i_1 + 2^{2h})2^u - (j_1 + 2^{2h}),
$$

$$
\Delta_2(i, j, u) = j2^{m-u} - i - (j_1 + 2^{2h})2^{m-u} - (i_1 + 2^{2h}).
$$

If $C_i = C_j$, there would be an integer $1 \leq u \leq m - 1$ such that $\Delta_t(i, j, u) \equiv 0 \pmod{n}$ for all $t \in \{1, 2\}$.

We first prove that $\Delta_1(i, j, u) \not\equiv 0$. When $u = 0$, $\Delta_1(i, j, u) = i_1 - j_1 \not\equiv 0$. When $1 \leq u \leq m - 1$, we have

$$
\Delta_1(i, j, u) \geq 2i_1 + 2^{2h+1} - 2^{2h} - j_1 > 0.
$$

Since $1 \leq u \leq m - 1$, one can similarly prove that $\Delta_2(i, j, u) > 0$.

When $u \leq m - 2h - 1$, we have

$$
-n < -2^{2h} \leq \Delta_1(i, j, u) \leq (2^{2h} + 2^h - 1)(2^{m-2h-1} - 1) < n.
$$

In this case, $\Delta_1(i, j, u) \not\equiv 0 \pmod{n}$.

When $u \geq m - 2h$, we have $m - u \leq 2h$ and

$$
0 < \Delta_2(i, j, u) \leq (2^{2h} + 2^h - 1)2^{2h} - 1 < n.
$$

In this case, $\Delta_2(i, j, u) \not\equiv 0 \pmod{n}$.

Combining the conclusions of the two cases above completes the proof. \qed

Lemma 16. For any $i + 2^{2h} \in B$ and odd $j \in A$,

$$
C_{i+2^{2h}} \cap C_j = \begin{cases} C_j & \text{if } (i, j) = (0, 1) \\ \emptyset & \text{otherwise.} \end{cases}
$$

Proof. Define

$$
\Delta_1(i, j, u) = j2^u - (i + 2^{2h}), \quad \Delta_2(i, j, u) = (i + 2^{2h})2^{m-u} - j.
$$

Suppose $C_{i+2^{2h}} = C_j$, thus, there would be an integer $0 \leq u \leq m - 1$ such that $\Delta_t(i, j, u) \equiv 0 \pmod{n}$ for all $t \in \{1, 2\}$.

If $u = 2h$, then

$$
0 \equiv \Delta_1(i, j, u) \equiv 2^{2h+1}(j2^{2h} - (i + 2^{2h})) \pmod{n}
$$

$$
\equiv j2^m - i2^{2h+1} - 2^m \pmod{n}
$$

$$
\equiv j - 1 - i2^{2h+1} \pmod{n}
$$

$$
\equiv j - 1 - i2^{2h+1}.
$$

Whence, the only solution of $\Delta_1(i, j, 2h) \equiv 0 \pmod{n}$ is $(i, j) = (0, 1)$.

We now consider the case that $0 \leq u < 2h$. We claim that $\Delta_1(i, j, u) \not\equiv 0$. Suppose on the contrary that $\Delta_1(i, j, u) = 0$. We would then have $j2^u - i - 2^{2h} = 0$. Because $u < 2h$ and $j$ is odd, there is an odd $i_1$ such that $i = 2^hi_1$. It then follows from $i < 2^h$ that $u < h$. We obtain then

$$
j = i_1 + 2^{2h-u} > i_1 + 2^h > 2^h - 1.
$$

This is contrary to the assumption that $j \in A$. This proves that $\Delta_1(i, j, u) \not\equiv 0$.

Finally, we deal with the case that $2h + 1 \leq u < 4h = m - 1$. We prove that $\Delta_2(i, j, u) \not\equiv 0 \pmod{n}$ in this case. Since $j$ is odd, $\Delta_2(i, j, u) \not\equiv 0$. We have also

$$
\Delta_2(i, j, u) = i2^{m-u} + 2^{m+2h-u} - j \leq (2^{h+1} - 1)2^{m-u} + 2^{m-1} - j \leq 2^{m-(h-1)} + 2^{m-1} - j < n.
$$

Clearly, $\Delta_2(i, j, u) > -j > -n$. Hence in this case we have $\Delta_2(i, j, u) \not\equiv 0 \pmod{n}$.

The proof of the lemma follows from the above conclusions. \qed

Lemma 17. Let $m \geq 9$ be odd. Let $s^\infty$ be the sequence of $(14)$. Then the linear span $\mathbb{L}_s$ of $s^\infty$ is given by

$$
\mathbb{L}_s = \begin{cases} m \left( \frac{(2^{m+7/4}) + (-1)^{(m-5)/4}}{4} + 3, \quad \text{if } m \equiv 1 \pmod{8} \\ m \left( \frac{(2^{m+7/4}) + 3}{4} + (-1)^{(m-5)/4} - 6 + 3 \right), \quad \text{if } m \equiv 5 \pmod{8}. \end{cases}
$$

We have also

$$
\mathbb{M}_s(x) = (x - 1) \prod_{i=0}^{\frac{m+1}{4}-1} m_{x - \frac{m+1}{2} - 1}^{\frac{m+1}{4}-1} (x) \prod_{1 \leq j \leq i \leq \frac{m}{4} - 1} m_{x - j - 1}^{i \frac{m}{4} - 1}(x).
$$
if $m \equiv 1 \pmod{8}$; and

$$M_s(x) = (x - 1) \prod_{i=1}^{\frac{m-1}{2}} m_{a-2i}^{m-1} (x) \prod_{i=1}^{\frac{m+1}{2}} m_{a-2i-1}^{m-1} (x)$$

if $m \equiv 5 \pmod{8}$, where $\kappa^{(h)}_{2^i+1}$ was defined in Section 5.

**Proof.** By Lemma 15, the monomials in the function

$$\text{Tr} \left( \sum_{i=0}^{2^h-1} x^{i+2^{2h}} \right)$$

will not cancel each other. Lemmas 10 and 11 say that after cancellation, we have

$$\text{Tr} \left( \sum_{i=0}^{2^h-1} x^i \right) = \text{Tr} \left( \sum_{i=1}^{2^h} x^{2i+1} \right).$$

By Lemma 16, the monomials in the function of (17) will not cancel the monomials in the function in the right-hand side of (18) if $m \equiv 1 \pmod{8}$, and only the term $x^{2^{2h}}$ in the function of (17) cancels the monomial $x$ in the function in the right-hand side of (18) if $m \equiv 5 \pmod{8}$.

The desired conclusions on the linear span and the minimal polynomial $M_s(x)$ then follow from Lemmas 2, 14, and Eq. (13). □

The following theorem provides information on the code $C_s$.

**Theorem 18.** Let $m \geq 9$ be odd. The binary code $C_s$ defined by the sequence of (14) has parameters $[2^m - 1, 2^m - 1 - L_s, d]$ and generator polynomial $M_s(x)$, where $L_s$ and $M_s(x)$ are given in Lemma 17 and the minimum weight $d$ fulfills the following bounds:

$$d \geq \begin{cases} \frac{2^{(m-1)/4} + 2}{2^{(m-1)/4}} & \text{if } m \equiv 1 \pmod{8} \\ \frac{2^{(m-1)/4}}{2^{(m-1)/4}} & \text{if } m \equiv 5 \pmod{8} \end{cases}.$$

**Proof.** The dimension and the generator polynomial of $C_s$ follow from Lemma 17 and the definition of the code $C_s$. We now derive the lower bounds on the minimum weight $d$. It is well known that the codes generated by $M_s(x)$ and its reciprocal have the same weight distribution. The reciprocal of $M_s(x)$ has the zeros $\alpha^{i+2^{2h}}$ for all $i$ in $\{0, 1, 2, \ldots, 2^h - 1\}$ if $m \equiv 1 \pmod{8}$, and for all $i$ in $\{1, 2, \ldots, 2^h - 1\}$ if $m \equiv 5 \pmod{8}$. Note that $C_s$ is an even-weight code. Then the desired bounds on $d$ follow from the BCH bound. □

**Example 5.** Let $m = 5$ and $\alpha$ be a generator of GF$(2^m)^*$ with $\alpha^5 + \alpha^2 + 1 = 0$. Then the generator polynomial of the code $C_s$ is $M_s(x) = x^6 + x^3 + x^2 + 1$, and $C_s$ is a [31, 25, 4] binary cyclic code which is optimal according to the Database.

**Example 6.** Let $m = 9$ and $\alpha$ be a generator of GF$(2^m)^*$ with $\alpha^9 + \alpha^3 + 1 = 0$. Then the generator polynomial of the code $C_s$ is $M_s(x) = x^{46} + x^{45} + x^{41} + x^{40} + x^{39} + x^{36} + x^{35} + x^{33} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{12} + x^{11} + x^7 + x^6 + x^2 + x + 1$ and $C_s$ is a [511, 465, $d$] binary cyclic code, where $d \geq 6$. The actual minimum weight may be larger than 6.

7. **Binary cyclic codes from the monomials $f(x) = x^{2^{2h}-2^h+1}$, where $\gcd(m, h) = 1$**

Define $f(x) = x^e$, where $e = 2^{2h} - 2^h + 1$ and $\gcd(m, h) = 1$. In this section, we have the following additional restrictions on $h$:

$$1 \leq h \leq \begin{cases} \frac{m-1}{4} & \text{if } m \equiv 1 \pmod{4}, \\ \frac{m-4}{4} & \text{if } m \equiv 3 \pmod{4}, \\ \frac{m-4}{4} & \text{if } m \equiv 0 \pmod{4}, \\ \frac{m-2}{4} & \text{if } m \equiv 2 \pmod{4}. \end{cases}$$

(20)
Note that
\[
\text{Tr}(f(x + 1)) = \text{Tr} \left( (x + 1)(x + 1)^{\sum_{i=0}^{h-1} x^{bi}} \right) = \text{Tr} \left( (x + 1) \prod_{i=0}^{h-1} (x^{bi} + 1) \right) = \text{Tr} \left( \sum_{i=0}^{h-1} x^{2bi+1} \right) = \text{Tr} \left( \sum_{i=0}^{h-1} x^{i+2m-h} + \sum_{i=1}^{2b-1} x^i \right) + 1. \tag{21}
\]

The sequence \(s^\infty\) of (5) defined by \(f(x)\) is then
\[
s_t = \text{Tr} \left( \sum_{i=0}^{2b-1} (\alpha^i)^{i+2m-h} + \sum_{i=1}^{2b-1} (\alpha^i)^i \right) + 1 \tag{22}
\]
for all \(t \geq 0\), where \(\alpha\) is a generator of GF\((2^m)\).^c

In this section, we deal with the code \(C_s\) defined by the sequence \(s^\infty\) of (23). It is noticed that the final expression of the function of (21) is of the same format as that of the function of (13). The proofs of the lemmas and theorems in this section are very similar to those of Section 5. Hence, we present only the main results without providing proofs.

We define the following two sets for convenience:

\[ A = \{0, 1, 2, \ldots, 2^h - 1\}, \quad B = 2^m - h + A = \{i + 2^m - h : i \in A\}. \]

**Lemma 19.** Let \(h\) satisfy the conditions of (20). For any \(j \in B\), the size \(\ell_j = |C_j| = m\).

**Proof.** The proof of Lemma 14 is easily modified into a proof for this lemma. The detail is omitted. \(\square\)

**Lemma 20.** Let \(h\) satisfy the conditions of (20). For any pair of distinct \(i\) and \(j\) in \(B\), \(C_i \cap C_j = \emptyset\), i.e., they cannot be in the same 2-cyclotomic coset modulo \(n\).

**Proof.** The proof of Lemma 15 is easily modified into a proof for this lemma. The detail is omitted. \(\square\)

**Lemma 21.** Let \(h\) satisfy the conditions of (20). For any \(i + 2^m - h \in B\) and odd \(j \in A\),

\[ C_{i+2^m-h} \cap C_j = \begin{cases} C_j & \text{if } (i, j) = (0, 1) \\ \emptyset & \text{otherwise}. \end{cases} \tag{24} \]

**Proof.** The proof of Lemma 16 is easily modified into a proof for this lemma. The detail is omitted here. \(\square\)

**Lemma 22.** Let \(h\) satisfy the conditions of (20). Let \(s^\infty\) be the sequence of (23). Then the linear span \(\mathbb{L}_s\) of \(s^\infty\) is given by

\[
\mathbb{L}_s = \begin{cases} m (2^{h+2} + (-1)^{h-1}) + 3 & \text{if } h \text{ is even} \\ \frac{3}{m (2^{h+2} + (-1)^{h-1} - 6) + 3} & \text{if } h \text{ is odd.} \end{cases} \tag{25} \]

We have also

\[
\begin{align*}
M_s(x) &= (x - 1) \prod_{i=0}^{2b-1} m_{\alpha^i-h-2^m-h} (x) \prod_{1 \leq j_1 < j_2 \leq 2b-1, k_{j_1+1}^h \neq k_{j_2+1}^h} m_{\alpha^{j_2-h-1}} (x) \\

text{if } h \text{ is even; and} \\
M_s(x) &= (x - 1) \prod_{i=1}^{2b-1} m_{\alpha^i-h-2^m-h} (x) \prod_{3 \leq j_1 < j_2 \leq 2b-1, k_{j_1+1}^b \neq k_{j_2+1}^b} m_{\alpha^{j_2-h-1}} (x) \\

text{if } h \text{ is odd, where } k_j^h \text{ was defined in Section 5.}
\end{align*}
\]
Lemma 24 \[ \text{Lemma 25. Let } m \in \mathbb{Z} \text{ be the sequence of } \alpha \text{ and do this, we first introduce some notations and lemmas which will be used in the sequel. Let } \rho \text{ define the following bounds:} \]

\[
d \geq \begin{cases} 
2^h + 2 & \text{if } h \text{ is even} \\
2^h & \text{if } h \text{ is odd.}
\end{cases}
\] (26)

Proof. The proof of Lemma 17 is easily modified into a proof for this lemma. The detail is omitted. \(\square\)

Theorem 23. Let \( h \) satisfy the conditions of (20). The binary code \( C_s \) defined by the sequence of (23) has parameters \([2^m - 1, 2^m - 1 - L_s, d] \) and generator polynomial \( M_s(x) \), where \( L_s \) and \( M_s(x) \) are given in Lemma 22 and the minimum weight \( d \) has the following bounds:

\[
d \geq \begin{cases} 
2^h + 2 & \text{if } h \text{ is even} \\
2^h & \text{if } h \text{ is odd.}
\end{cases}
\] (26)

Proof. The proof of Theorem 18 is easily modified into a proof for this lemma with the help of the lemmas presented in this section. The detail is omitted here. \(\square\)

Example 7. Let \((m, h) = (5, 2)\) and \( \alpha \) be a generator of \( GF(2^m)^* \) with \( \alpha^5 + \alpha^2 + 1 = 0 \). Then the generator polynomial of the code \( C_s \) is \( M_s(x) = x^{16} + x^{14} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1 \) and \( C_s \) is a \([31, 15, 8]\) binary cyclic code. Its dual is a \([31, 16, 7]\) cyclic code. Both codes are optimal according to the Database. In this example, the condition of (20) is not satisfied. So the conclusions on the code of this example do not agree with the conclusions of Theorem 23.

Example 8. Let \((m, h) = (7, 2)\) and \( \alpha \) be a generator of \( GF(2^m)^* \) with \( \alpha^7 + \alpha + 1 = 0 \). Then the generator polynomial of the code \( C_s \) is \( M_s(x) = x^{36} + x^{34} + x^{27} + x^{21} + x^{20} + x^{18} + x^{13} + x^{12} + x^8 + x^7 + x^6 + x^5 + x^2 + 1 \) and \( C_s \) is a \([127, 91, 8]\) binary cyclic code.

In this section, we obtained interesting results on the code \( C_s \) under the conditions of (20). When \( h \) is outside the range, it may be hard to determine the dimension of the code \( C_s \), let alone its minimum distance. Hence, it would be interesting to solve the following open problem.

Open Problem 1. Determine the dimension and the minimum weight of the code \( C_s \) of this section when \( h \) satisfies

\[
\begin{cases} 
\frac{m-1}{2} \geq h > \frac{m-1}{4} \text{ if } m \equiv 1 \pmod{4}, \\
\frac{m-3}{2} \geq h > \frac{m-3}{4} \text{ if } m \equiv 3 \pmod{4}, \\
\frac{m-4}{2} \geq h > \frac{m-4}{4} \text{ if } m \equiv 0 \pmod{4}, \\
\frac{m-2}{2} \geq h > \frac{m-2}{4} \text{ if } m \equiv 2 \pmod{4}.
\end{cases}
\] (27)

8. Binary cyclic codes from a trinomial over GF(2^m)

In this section, we study the code \( C_s \) from the trinomial \( x + x^r + x^{2h-1} \) where \( wt(r) = m - 1 \) and \( 0 \leq h \leq \lceil \frac{m}{2} \rceil \). Before doing this, we first introduce some notations and lemmas which will be used in the sequel. Let \( \rho_i \) denote the number of even integers in the 2-cyclotomic coset \( C_i \). For each \( i \in I' \), define

\[
v_i = \frac{m \rho_i}{\ell_i} \pmod{2}
\] (28)

where \( \ell_i = |C_i| \).

Lemma 24 ([29]). With the same notations as before,

\[
\text{Tr}((1 + \alpha^s)^{2^m-2}) = \sum_{j \in I'} v_j \left( \sum_{i \in C_j} (\alpha^s)^i \right).
\] (29)

Furthermore, the total number of nonzero coefficients of \( \alpha^s \) in (29) is equal to \( 2^{m-1} \).

Lemma 25. Let \( m \geq 4, r \) be an integer with \( 1 \leq r \leq 2^m - 2 \) and \( wt(r) = m - 1 \), and \( h \) an integer with \( 0 \leq h \leq \lceil \frac{m}{2} \rceil \). Let \( s^\infty \) be the sequence of (5), where \( f(x) = x + x^r + x^{2h-1} \). Then the linear span of \( s^\infty \) is given by

\[
\mathbb{L}_s = \begin{cases} 
2^{m-1} + m, & \text{if } m \text{ is odd and } h = 0 \\
2^{m-1} - m, & \text{if } m \text{ is even and } h = 0 \\
2^{m-1}, & \text{if } h \neq 0
\end{cases}
\] (30)

C. Ding, Z. Zhou / Discrete Mathematics 321 (2014) 76–89
and the minimal polynomial of $s^\infty$ is given by

$$
M_2(x) = \begin{cases} 
    m_{u-1}(x) \prod_{j \in \Gamma \setminus \{1\}, \eta_1 = 1} m_{u-j}(x), & \text{if } m \text{ is odd and } h = 0 \\
    \prod_{j \in \Gamma \setminus \{1\}, \eta_1 = 1} m_{u-j}(x), & \text{if } m \text{ is even and } h = 0 \\
    \prod_{j \in \Gamma, \eta_1 = 1} m_{u-j}(x), & \text{if } h \neq 0
\end{cases}
$$

(31)

where $m_{u-j}(x)$ is the minimal polynomial of $\alpha^{-j}$ over $\mathbb{GF}(2)$, $u_1 = (v_1 + \kappa_1^{(h)} + 1) \mod 2$, $u_{2j+1} = (v_{2j+1} + \kappa_{2j+1}^{(h)}) \mod 2$ for $3 \leq 2j + 1 \leq 2^h - 1$, and $u_j = v_j$ for $j \in \Gamma \setminus \{2i + 1 : 1 \leq 2i + 1 \leq 2^h - 1\}$. Herein, $\kappa_{2j+1}^{(h)}$ is given by (9).

**Proof.** Note that $wt(r) = wt(2^m - 2) = m - 1$. It then follows from Lemma 5 and the properties of the trace function that $\text{Tr}(x') = \text{Tr}(x^{2^{m - 2}})$ for all $x \in \mathbb{GF}(2^m)$.

We first deal with the case of $h = 0$ where $f(x) = 1 + x + x'$. According to Lemma 24, one has

$$
\text{Tr}(1 + \alpha^i) = \text{Tr}(1) + \text{Tr}(1 + \alpha^i) + \text{Tr}((1 + \alpha^i)^{2^{m-2} - 2})
$$

$$
= \sum_{i \in \mathbb{C}_1} (\alpha^i)^1 + \sum_{j \in \Gamma} v_j \left( \sum_{i \in \mathbb{C}_j} (\alpha^i)^j \right)
$$

(32)

$$
= \sum_{i \in \mathbb{C}_1} (1 + v_1)(\alpha^i)^1 + \sum_{j \in \Gamma \setminus \{1\}} v_j \left( \sum_{i \in \mathbb{C}_j} (\alpha^i)^j \right)
$$

where $1 + v_1$ is performed modulo 2. By the definition of $v_1$, $v_1 = (m - 1) \mod 2$. The desired conclusion on the linear span and minimal polynomial of $s^\infty$ for the case $h = 0$ then follows from Eq. (32) and Lemma 2.

Now we assume that $h \neq 0$. From the proof of Lemma 11, we know that

$$
\text{Tr} \left( \sum_{i=1}^{2^h-1} x^i \right) = \sum_{1 \leq j \leq 2^h-1} \text{Tr}(x^{2^j+1}).
$$

It then follows from Lemma 24 that

$$
\text{Tr}(1 + \alpha^i) = \text{Tr}(1 + \alpha^i) + \text{Tr}((1 + \alpha^i)^{2^{m-2} - 2}) + \text{Tr}((1 + \alpha^i)^{2^{h-1}})
$$

$$
= \sum_{i \in \mathbb{C}_1} (\alpha^i)^1 + \sum_{j \in \Gamma} v_j \left( \sum_{i \in \mathbb{C}_j} (\alpha^i)^j \right) + \sum_{j \in \Gamma \setminus \{1\}} \kappa_j^{(h)} \left( \sum_{i \in \mathbb{C}_j} (\alpha^i)^j \right)
$$

(33)

where $\Gamma_1 = \{2i + 1 : 1 \leq 2i + 1 \leq 2^h - 1\}$, $u_1 = (v_1 + \kappa_1^{(h)} + 1) \mod 2$, $u_j = (v_j + \kappa_j^{(h)}) \mod 2$ for $j \in \Gamma \setminus \{1\}$ and $u_j = v_j$ for $j \in \Gamma_1$. The minimal polynomial in (31) then follows from Eq. (33).

Finally, we show that the linear span of $s^\infty$ is equal to $2^{m-1}$ when $h \neq 0$, i.e., the total number of nonzero coefficient of $\alpha^a$ in (33) is equal to $2^{m-1}$. According to Lemmas 6 and 24, it is sufficient to prove that the number of $j \in \Gamma_1$ such that $u_j \neq 0$ is equal to the number of $j \in \Gamma_1$ such that $u_j \neq 0$. By the definition of $v_j$ and Lemma 4, we have $u_1 = (m - 1) \mod 2$, $v_3 = (m - 2) \mod 2$. According to the definition of $\kappa_j^{(h)}$ in (9), we have $\kappa_1^{(h)} = h \mod 2$ and $\kappa_j^{(h)} = (h - 1) \mod 2$. Thus, $u_1 = (m + h) \mod 2$ and $u_3 = (m + h - 1) \mod 2$. Independently of the parity of $m$, there are exactly one nonzero $u_i$ and $v_i$ for $i \in \{1, 3\}$. Note that, for any integer $a$ with $2 \leq a \leq h - 1$, the number of odd integers $j$ satisfying $2^a < j < 2^{a+1}$ is equal to $2^{a-1}$. It is clear that when $2j + 1$ ranges over the odd integers between $2^a$ and $2^{a+1}$, the number of $2j + 1$ such that $wt(2j + 1) = \text{even}$ is equal to $2^{a-2}$. It then follows from Lemma 4 that

$$
||\{2^a < 2j + 1 < 2^{a+1} : v_{2j+1} = 1\}|| = ||\{2^a < 2j + 1 < 2^{a+1} : v_{2j+1} = 0\}|| = 2^{a-2}.
$$

On the other hand, when $2j + 1$ runs over the odd integers from $2^a$ to $2^{a+1}$, $\kappa_{2j+1}^{(h)}$ has the same value for these $j$'s due to the definition of $\kappa_{2j+1}^{(h)}$ in (9). If $\kappa_j^{(h)} = 0$, $u_j = v_j$, and otherwise $u_j = v_j + 1$. Thus we have

$$
||\{2^a < 2j + 1 < 2^{a+1} : u_{2j+1} = 1\}|| = ||\{2^a < 2j + 1 < 2^{a+1} : u_{2j+1} = 0\}|| = 2^{a-2}.
$$
It then follows that
\[ |\{j \in \Gamma_1 : u_j = 1\}| = |\{j \in \Gamma_1 : v_j = 1\}|. \]

By Lemma 6, |C_j| = m for each j ∈ Π_1. The conclusion then follows from the analysis above. □

**Theorem 26.** The code C_s defined by the sequence of Lemma 25 has parameters [n, n − L_s, d] and generator polynomial M_s(x) of (31), where L_s is given by (30) and
\[ d \geq \begin{cases} 
8, & \text{if } m \text{ is odd and } h = 0 \\
3, & \text{if } m \text{ is even and } h = 0.
\end{cases} \]

**Proof.** The dimension of C_s follows from Lemma 25 and the definition of this code. We only need to prove the conclusion on the minimal distance d of C_s. It is known that codes generated by any polynomial g(x) and its reciprocal have the same weight distribution. When m is odd and h = 0, since v_3 = v_5 = 1, the reciprocal of M_s(x) has zeros α^t for t ∈ {0, 1, 2, 3, 4, 5, 6}. It then follows from the BCH bound that d ≥ 8. When m is odd and h = 0, note that v_7 = v_13 = 1, the reciprocal of M_s(x) has zeros α^t for t ∈ {13, 14}. By the BCH bound, d ≥ 3. □

**Open Problem 2.** Develop a tight lower bound on the minimal distance of the code C_s in Theorem 26 for the case h > 0.

When r = 2^m − 2 and h = 1, f(x) becomes the monomial x^{2^m−2} which is the inverse APN function. It was pointed in [7] that the code C_s from the inverse APN function may have poor minimal distance when m is even. However, when we choose some other h, the corresponding codes may have excellent minimal distance. This is demonstrated by some of the examples below.

**Example 9.** Let m = 4, r = 2^m − 2, h = 1, and α be the generator of GF(2^m) with α^4 + α + 1 = 0. Then the generator polynomial of C_s is M_s(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 and C_s is a [15, 7, 3] binary cyclic code. It is not optimal.

**Example 10.** Let m = 4, r = 2^m − 2, h = 0, and α be the generator of GF(2^m) with α^4 + α + 1 = 0. Then the generator polynomial of C_s is M_s(x) = x^4 + x + 1 and C_s is a [15, 11, 3] optimal binary cyclic code. The optimal binary linear code with the same parameters in the Database is not cyclic.

**Example 11.** Let m = 4, r = 2^m − 2, h = 2, and α be the generator of GF(2^m) with α^4 + α + 1 = 0. Then the generator polynomial of C_s is M_s(x) = x^8 + x^7 + x^5 + x^4 + x^3 + 1 and C_s is a [15, 7, 5] optimal binary cyclic code. The optimal binary linear code with the same parameters in the Database is not cyclic.

**Example 12.** Let m = 5, r = 2^m − 2, h = 0, and α be the generator of GF(2^m) with α^5 + α^2 + 1 = 0. Then the generator polynomial of C_s is M_s(x) = x^7 + x^6 + x^5 + x^4 + x^3 + 1 and C_s is a [31, 10, 12] optimal binary cyclic code.

**Example 13.** Let m = 5, r = 2^m − 2, h = 1, and α be the generator of GF(2^m) with α^5 + α^2 + 1 = 0. Then the generator polynomial of C_s is M_s(x) = x^{16} + x^{14} + x^{13} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1 and C_s is a [31, 15, 8] optimal binary cyclic code. The optimal binary linear code with the same parameters in the Database is not cyclic.

9. Open problems regarding binary cyclic codes from monomials

In the previous sections, we investigated binary cyclic codes defined by some monomials. It would be good if the following open problems could be solved.

**Open Problem 3.** Determine the dimension and the minimum weight of the code C_s defined by the monomials x^e, where e = 2^{(m−1)/2} + 2^{(m−1)/4} − 1 and m ≡ 3 (mod 4).

**Open Problem 4.** Determine the dimension and the minimum weight of the code C_s defined by the monomials x^e, where e = 2^k + 2^3i + 2^0i + 2^l − 1 and m = 5i.

10. Concluding remarks and summary

In this paper, we constructed a number of families of binary cyclic codes with monomials and trinomials of special types. The dimension of some of the codes is flexible. We determined the minimum weight for some families of cyclic codes, and developed tight lower bounds for other families of cyclic codes. The main results of this paper showed that the approach of constructing cyclic codes with polynomials is promising.

The binary sequences defined by some of the monomials and trinomials have large linear span. These sequences have also reasonable autocorrelation property. They could be employed in certain stream ciphers as keystreams. So the contribution of this paper in cryptography is the computation of the linear spans of these sequences.
It is known that long BCH codes are bad [20]. However, it was indicated in [2,23] that there may be good cyclic codes. The cyclic codes presented in this paper proved that some families of cyclic codes are in fact very good.

Four open problems regarding binary cyclic codes were proposed in this paper. The reader is cordially invited to attack them.

Acknowledgments

The authors are very grateful to the reviewers and the editor, Prof. Marco Buratti, for their comments and suggestions that improved the presentation and quality of this paper.

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 (1) (1992) 120–130.
[2] E.R. Berlekamp, J. Justesen, Some long cyclic binary codes are not so bad, IEEE Trans. Inform. Theory 20 (3) (1974) 351–356.
[3] A.R. Calderbank, W. Li, B. Poonen, A 2-adic approach to the analysis of cyclic codes, IEEE Trans. Inform. Theory 43 (1997) 977–986.
[4] C. Carlet, C. Ding, J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, IEEE Trans. Inform. Theory 51 (6) (2005) 2089–2102.
[5] K.T. Chen, Cyclic decoding procedure for the Bose–Chaudhuri–Hocquenghem codes, IEEE Trans. Inform. Theory 10 (1964) 357–363.
[6] C. Ding, Cyclic codes from the two-prime sequences, IEEE Trans. Inform. Theory 58 (2012) 357–363.
[7] C. Ding, Cyclic codes from some monomials and trinomials, SIAM J. Discrete Math. 27 (2013) 1977–1994.
[8] C. Ding, C. Xiao, W. Shan, The Stability Theory of Stream Ciphers, in: Lecture Notes in Computer Science, vol. 561, Springer-Verlag, Heidelberg, 1991.
[9] H.Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl. 14 (1) (2008) 22–40.
[10] S.T. Dougherty, S. Ling, Cyclic codes over $Z_4$ of even length, Des. Codes Cryptogr. 39 (2) (2006) 127–153.
[11] T. Feng, On cyclic codes of length $2^r$ — 1 with two zeros whose dual codes have three weights, Des. Codes Cryptogr. 62 (3) (2012) 253–258.
[12] G.D. Forney, On decoding BCH codes, IEEE Trans. Inform. Theory 11 (4) (1995) 549–557.
[13] C. Güneri, F. Özbudak, Weil–Serre type bounds for cyclic codes, IEEE Trans. Inform. Theory 54 (12) (2008) 5381–5395.
[14] B. Heijne, J. Top, On the minimal distance of binary self-dual cyclic codes, IEEE Trans. Inform. Theory 55 (11) (2009) 4860–4863.
[15] T. Helleseth, P.V. Kumar, Sequences with low correlation, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 1765–1854.
[16] Q. Huang, Q. Diao, S. Lin, K. Abdel-Ghaffar, Cyclic and quasi-cyclic LDPC codes on constrained parity-check matrices and their trapping sets, IEEE Trans. Inform. Theory 58 (5) (2012) 2648–2671.
[17] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[18] Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory 57 (4) (2011) 2243–2251.
[19] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes, Inf. Control 18 (1971) 369–394.
[20] S. Lin, E.J. Weldon, Long BCH codes are bad, Inf. Control 11 (1967) 445–451.
[21] J.H. van Lint, R.M. Wilson, On the minimum distance of cyclic codes, IEEE Trans. Inform. Theory 32 (1) (1986) 23–40.
[22] J. Luo, K. Feng, Cyclic codes and sequences from generalized Coulter–Matthews function, IEEE Trans. Inform. Theory 54 (12) (2008) 5345–5353.
[23] C. Martínez-Pérez, W. Willems, Is the class of cyclic codes asymptotically good? IEEE Trans. Inform. Theory 52 (2) (2006) 696–700.
[24] M.J. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, IEEE Trans. Inform. Theory 53 (2) (2007) 843–847.
[25] O. Moreno, P.V. Kumar, Minimum distance bounds for cyclic codes and Deligne’s theorem, IEEE Trans. Inform. Theory 39 (5) (1993) 1524–1534.
[26] J. Park, J. Moon, Error-pattern-correcting cyclic codes tailored to a prescribed set of error cluster patterns, IEEE Trans. Inform. Theory 55 (4) (2009) 1747–1765.
[27] E. Prange, Some cyclic error-correcting codes with simple decoding algorithms, Air Force Cambridge Research Center-TN-58-156, Cambridge, Mass, April 1958.
[28] A. Rao, N. Pinnawala, A family of two-weight irreducible cyclic codes, IEEE Trans. Inform. Theory 56 (6) (2010) 2568–2570.
[29] W. Si, C. Ding, A simple stream cipher with proven properties, Cryptogr. Commun. 4 (2) (2012) 79–104.
[30] X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao, The weight distribution of a class of $p$-ary cyclic codes, Finite Fields Appl. 16 (1) (2010) 56–73.

Further reading

[1] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory Ser. A 113 (2006) 1526–1535.
[2] C.R.P. Hartmann, K.K. Tzeng, Generalizations of the BCH bound, Inf. Control 20 (1972) 489–498.