EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 14, No. 3, 2021, 685-694
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Cyclic Codes from A Sequence over Finite Fields

Nopendri[1,3,*], Intan Muchtadi Alamsyah[1], Djoko Suprijanto[2], Aleams Barra[1]

[1] *Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Bandung, Indonesia*
[2] *Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Bandung, Indonesia*
[3] *Cybernetics Research Group, School of Industrial and System Engineering, Telkom University, Bandung, Indonesia*

Abstract. A cyclic code has been one of the most active research topics in coding theory due to its applications in many areas, such as data storage systems and communication, as they have efficient encoding and decoding algorithms. This paper explains the construction of a family of cyclic codes from sequences generated by a trace of a monomial over finite fields of odd characteristics. The parameter and some examples of the codes are presented in this paper.

2020 Mathematics Subject Classifications: 94B15, 94B65, 94A55

Key Words and Phrases: Cyclic codes, sequences, linear span, cyclotomic coset, minimal polynomials

1. Introduction

Let $GF(q)$ be finite fields with $q = p^m$ elements, where p is prime and $m \geq 1$. Consider $(GF(q))^n$ as a vector space over $GF(q)$. A q-ary $[n, k, d]$-*linear code* $\mathcal{C}$ is a k-dimensional subspace of $(GF(q))^n$ with the minimum nonzero weight d. A linear code $\mathcal{C}$ over the finite field $GF(q)$ is said to be *cyclic* if any $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. A word $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ in $\mathcal{C}$ can be represented as a polynomial $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ in ring $\mathcal{R}_n = GF(q)[x]/\langle x^n - 1\rangle$. So that $\mathcal{C} \subseteq (GF(q))^n$ can be identified by a subset of $\mathcal{R}_n$, in this case the cyclic code is an *ideal* of $\mathcal{R}_n$. Any ideal of $\mathcal{R}_n$ is principal, so that it is generated by a polynomial $g(x)$, where $g(x)$ is a divisor of $x^n - 1$. The polynomial g is called *generator* of the cyclic code $\mathcal{C}$. The dimension of cyclic code $\mathcal{C}$ can be determined from degree of generator polynomial g.

The error-correcting capability of cyclic codes may not be as good as some other linear codes in general. However, cyclic codes are widely used in many fields such as data storage

[*] Corresponding author.

DOI: https://doi.org/10.29020/nybg.ejpam.v14i3.3907

Email addresses: nopendri301@s.itb.ac.id (Nopendri), ntan@math.itb.ac.id (I.M.Alamsyah), djoko@math.itb.ac.id (D.Suprijanto),barra@math.itb.ac.id (A. Barra)

and communication systems because they have attractive algebraic properties and have efficient algorithms for encoding and decoding [2, 7, 11]. This code is also used to construct impressive structures such as quantum codes [18], frequency hopping sequences [5] and so on.

One of the main problems in coding theory research is finding the optimal code, which is the code that has the largest minimum distance d related to the ability to correct errors in the information transfer or meets some bounds from the best known linear code according to the tables [8].

The cyclic code can be constructed from a periodic sequence s [3, 6]. These sequences are generated from a function over a finite field. For simplicity, we call this cyclic code as $\mathcal{C}_s$. The results of Ding and Zhou's constructions in papers [3] and [6] are interesting, showing that the codes obtained are optimal.

Several open problems are presented in these papers [3, 6]. Some researchers have solved the problems, see [12, 14, 16, 17]. Finding the dimension and the generator polynomial of cyclic codes $\mathcal{C}_s$ from monomial $f(x) = x^{q^m-2} \in GF(q^m)[x]$ appear as an open problem in [3], and solved by [17] then. However, differing sequences provide some different results. In this paper, we discuss the construction of the cyclic code with the new sequence, and we say that "sequence $\check{s}$", from the monomial $f(x)$. This construction will generate a new cyclic code related to the code from the sequence s. We also add information about the minimum distance of the code.

This paper is organized as follows. Section 2 introduces some basic notation and results about q-cyclotomic cosets and sequences that will frequently be used to prove our main results in the following sections. The dimension and the generator polynomial of a class of cyclic codes defined by a sequence are determined in Section 3. The minimum distance of this cyclic code is also provided in that section. In Section 4, we conclude this paper.

2. Preliminaries

In this section, some basic notations and results on q-cyclotomic cosets modulo n and sequences used to prove the main result are introduced.

Definition 1. *Let $n = q^m-1$ and $Z_n = \{0, 1, 2, \dots, n-1\}$. For any integer $s, 0 \leq s \leq n-1$, the q-cyclotomic coset modulo n containing s is defined by*

$$C_s = \{s, qs, q^2 s, \dots, q^{l_s-1}s\} \subset \mathbb{Z}_n$$

where l_s is the least positive integer such that $q^{l_s} \equiv s(\mod n)$ and l_s is called the size of C_s.

Lemma 1. *[9] Let q be a power of a prime p and $n = q^m - 1$. For any $1 \leq s \leq n-1$ with $\gcd(s, n) = 1$ the length l_s of the q-cyclotomic coset C_s is equal to m.*

Definition 2. *Let $s^\infty = (s_t)_{t=0}^\infty$ be a sequence over $GF(q)$. A sequence s^∞ is called periodic with period N if there is positive integer N such that $s_t = s_{t+lN}$ for every $t, l \geq 0$.*

Definition 3. *The polynomial* $c(x) = a_k x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$ *over* $GF(q)$, *with* $a_k = 1$, *is called characteristic polynomial of* s^∞ *if*

$$a_k s_{n+k} + a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0 s_n = 0$$

for every $n = 0, 1, 2, \dots$. *Furthermore, the polynomial characteristic of the smallest degree of* s^∞ *is called minimal polynomial of* s^∞, *and denoted by* $\mathbb{M}_s(x)$.

The minimal polynomial $\mathbb{M}_s(x)$ of the sequence s^∞ is unique and divides $c(x)$. The degree of $\mathbb{M}_s(x)$ is called *linear span or linear complexity* of s^∞ and is denoted by $\mathbb{L}_s$.

For any sequence s^∞, we can determine the linear span and minimal polynomial of s^∞ from the following lemma [4, Theorem 5.3].

Lemma 2. *Let* $s^\infty = (s_t)_{t=0}^{\infty}$ *be a sequence with period* L *over* $GF(q)$. *Defined* $S^L(x) = \sum_{t=0}^{L-1} s_t x^t \in GF(q)[x]$. *Then the minimial polynomial* $\mathbb{M}_s(x)$ *of* s^∞ *is given by*

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

and the linear span $\mathbb{L}_s$ *is given by* $L - deg(\gcd(S^L(x), x^L - 1))$.

Another way is given in the following lemma [1], which is very important for proof of our main result.

Lemma 3. *Any sequence* s^∞ *over* $GF(q)$ *of period* $q^m - 1$ *has a unique powers-of-*α *representation of the form*

$$s_t = \sum_{i=0}^{q^m-2} c_i \alpha^{it}, \quad \textit{for all } t \geq 0,$$

where $c_i \in GF(q^m)$ *and* α *is a primitive element in* $GF(q^m)$. *Suppose that* $I = \{i | c_i \neq 0\}$, *then the minimal polynomial of* s^∞ *is*

$$\mathbb{M}_s(x) = \prod_{i \in I}(x - \alpha^i), \tag{1}$$

and the linear span of s^∞ *is* $\mathbb{L}_s = |I|$.

It should be noticed that in some references, the reciprocal of $\mathbb{M}_s(x)$ is the minimal polynomial of the sequence s^∞.

3. Cyclic codes from the monomial $f(x) = x^{q^m-2}$

In this section, we study a particular type of sequences $\check{s}^\infty$ defined by

$$\check{s}_t = \mathrm{Tr}_1^m(f(\alpha^t + 1) - f(\alpha^t)), \ t \geq 0, \tag{2}$$

where

$$f(x) = x^{q^m-2}, \tag{3}$$

is a function in $GF(q^m)[x]$, m is a positive integer, Tr_1^m is the trace function from $GF(q^m)$ to $GF(q)$ and α is a primitive element of $GF(q^m)^*$.

The objective of this part is to construct a class of cyclic code from this sequence with explicit monomial f. We call the cyclic code $\mathcal{C}_{\check{s}}$ with the generator polynomial from the minimal polynomial of the sequence $\check{s}^\infty = (\check{s}_t)_{t=0}^\infty$. Let $n = q^m - 1$ and $e = q^m - 2$. By Lemma 3 and (2), to get the parameters of the corresponding cyclic codes is to compute the powers-of-α representation of $\mathrm{Tr}_1^m(f(\alpha^t + 1) - f(\alpha^t))$ as follows:

$$\begin{aligned}
\check{s}_t &= \mathrm{Tr}_1^m(f(\alpha^t + 1) - f(\alpha^t)) \\
&= \mathrm{Tr}_1^m((\alpha^t + 1)^e - (\alpha^t)^e) \\
&= \mathrm{Tr}_1^m\left(\sum_{i=0}^{e} \binom{e}{i} \alpha^{it} - \alpha^{et}\right) \\
&= \sum_{i=0}^{q^m-2} \binom{e}{i} \sum_{j=0}^{m-1} \alpha^{q^j it} - \sum_{j=0}^{m-1} \alpha^{q^j et} \\
&= \sum_{\substack{i=0,\\ i \notin C_e}}^{q^m-2} \binom{e}{i} \sum_{j=0}^{m-1} \alpha^{q^j it} \qquad (4)\\
&= \sum_{\substack{i=0,\\ i \notin C_e}}^{q^m-2} \left(\sum_{j=0}^{m-1} \binom{e}{q^j i \mod n} \mod p\right) \alpha^{it} \\
&= \sum_{\substack{i=0,\\ i \notin C_e}}^{q^m-2} K_{e,q,m}(i) \alpha^{it},
\end{aligned}$$

where $K_{e,q,m}(i) = \sum_{j=0}^{m-1} \binom{e}{q^j i \mod n} \mod p$ and C_e is the q-cyclotomic coset containing e modulo n.

From (4), define

$$Supp(K_{e,q,m}) = \{i \in \mathbb{Z}_n : K_{e,q,m}(i) \neq 0, i \notin C_e\}. \tag{5}$$

Now, we need to count the $Supp(K_{e,q,m})$. To do this, we have to simplify (4). Note that the following lemma is well-known.

Lemma 4. *[15] Let $N > M > 0$, then*

$$\binom{N-1}{M} = \frac{N-M}{N}\binom{N}{M}.$$

Let $k_{ij} = q^j i \mod n$, from the Lemma 4 and note that the multiplicative inverse of $e+1$ is $p-1$ in modulo p, then

$$\begin{aligned} K_{e,q,m}(i) &\equiv \sum_{j=0}^{m-1} \binom{e}{k_{ij}} \\ &\equiv \sum_{j=0}^{m-1} \frac{e+1-k_{ij}}{e+1} \binom{e+1}{k_{ij}} \\ &\equiv \sum_{j=0}^{m-1} (1+k_{ij}) \binom{e+1}{k_{ij}} \mod p. \end{aligned} \tag{6}$$

The last part of (6) always has the same form for any j as the following lemma.

Lemma 5. *For any $i \in \mathbb{Z}_n$,*

$$\binom{e+1}{qi \mod n} = \binom{e+1}{i \mod n}.$$

Proof. Let $i = \sum_{j=0}^{m-1} i_j q^j$, then $qi \mod n = i_{m-1} + i_0 q + \cdots + i_{m-2} q^{m-1}$. Combaining the fact $e+1 = \sum_{j=0}^{m-1} (q-1) q^j$ and Lucas's theorem [13] we have

$$\begin{aligned} \binom{e+1}{qi \mod n} &\equiv \binom{q-1}{i_{m-2}} \cdots \binom{q-1}{i_0} \binom{q-1}{i_{m-1}} \\ &\equiv \binom{q-1}{i_{m-1}} \cdots \binom{q-1}{i_1} \binom{q-1}{i_0} \\ &\equiv \binom{e+1}{i} \mod p. \end{aligned}$$

This yields, for $k_{ij} = q^j i \mod n$, (where $j \in \mathbb{Z}_m$), $\binom{e+1}{k_{ij}} \equiv \binom{e+1}{i} \mod p$. Hence, the equation (6) equivalent to

$$\begin{aligned} K_{e,q,m}(i) &\equiv \binom{e+1}{i} \sum_{j=0}^{m-1} (1+k_{ij}) \\ &\equiv \binom{e+1}{i} \left(m + \sum_{j=0}^{m-1} k_{ij} \right) \mod p. \end{aligned}$$

The following lemma assures that the $\binom{e+1}{i}$ is not divided by p.

Lemma 6. *Let a be a positive integer and k be a nonnegative integer. For p prime then*

$$\binom{p^a-1}{k} \not\equiv 0 \mod p.$$

Proof.

$$\begin{aligned}\binom{p^a-1}{k} &\equiv \frac{(p^a-1)!}{k!(p^a-1-k)!}\\ &\equiv \frac{(p^a-1)(p^a-2)\cdots(p^a-k)}{k!}\\ &\equiv \frac{p^{ak}-\left(\sum\limits_{i=1}^{k} i\right)p^{(k-1)a}}{k!}\\ &+\frac{\left(\sum\limits_{i\neq j,i,j\in[k]} i.j\right)p^{(k-2)a}-\cdots+(-1)^k k!}{k!}\\ &\equiv (-1)^k \mod p.\end{aligned}$$

Let $s_q(i) = \sum\limits_{j=0}^{m-1} k_{ij}$, then (5) becomes

$$Supp(K_{e,q,m}) = \{i \in \mathbb{Z}_n : s_q(i) + m \not\equiv 0 \mod p\}\backslash\{i \in C_e\}. \tag{7}$$

Let $A = \{i \in \mathbb{Z}_n : s_q(i) + m \not\equiv 0 \mod p\}$ and $B = \{i \in C_e\}$. So, (7) becomes

$$Supp(K_{e,q,m}) = A\backslash B.$$

To get the cardinality of A we need to prove the following lemmas. Let $\lambda_1 = \frac{n}{q-1}$ and $\lambda_2 = q-1$, then $\lambda_1 = 1+q+q^2+\cdots+q^{m-1}$ and $\lambda_1\lambda_2 = n$.

Lemma 7. *Let $a \in \mathbb{Z}_n$ and $j \in \{0,1,2,\ldots,m-1\}$ such that $aq^j \geq n$ and $aq^j = \gamma n + \delta$, for some $\delta \in \mathbb{Z}_n$. Then*

$$aq^j \equiv aq^j - \gamma\lambda_2(1+q+q^2+\cdots+q^{m-1}) \mod n,$$

for some $\gamma \geq 0$.

Proof. Consider $\delta \in \mathbb{Z}_n$, that is $\delta = aq^j - \gamma n = aq^j - \gamma\lambda_1\lambda_2$, so that

$$\delta \equiv aq^j - \gamma\lambda_2(1+q+q^2+\cdots+q^{m-1}) \mod n,$$

for some $\gamma \geq 0$.

Lemma 8. *Let $b \in \mathbb{Z}_n, b \neq 0$. Then*

$$\begin{aligned} s_q(b) &= (bq^0 \mod n) + (bq^1 \mod n) + \cdots \\ &+ (bq^{m-1} \mod n) \\ &= (b-\gamma')(1+q+q^2+\cdots+q^{m-1}) \\ &= (b-\gamma')\frac{n}{q-1}, \end{aligned}$$

for some $\gamma' < b$.

Proof. Suppose $j_1, j_2, \cdots, j_t \in \{0, 1, 2, \cdots, m-1\}$ such that $bq^{j_i} \geq n$, for every $i = 1, 2, \cdots, t$. Then by Lemma 7, we have

$$bq^{j_i} \equiv bq^{j_i} - \gamma_i\lambda_2(1+q+\cdots+q^{m-1}) \mod n,$$

for some $\gamma_i \geq 0$ and for all $i = 1, 2, \cdots, t$. Hence

$$\begin{aligned} s_q(b) &= (bq^0 \mod n) + (bq^1 \mod n) + \cdots \\ &+ (bq^{m-1} \mod n) \\ &= b(q^0+q^1+q^2+\cdots+q^{m-1}) \\ &- (\lambda_2\sum_{i=0}^{t}\gamma_i(q^0+q^1+q^2+\cdots+q^{m-1})) \\ &= \left(b-\lambda_2\sum_{i=0}^{t}\gamma_i\right)(q^0+q^1+q^2+\cdots+q^{m-1}). \end{aligned}$$

Put $\gamma' = \lambda_2 \sum_{i=1}^{t} \gamma_i$.

Lemma 9. *If $(b-\gamma') \neq 0 \mod p$, then*

$$(b-\gamma')\lambda_1 = (b-\gamma')\frac{n}{q-1} \neq 0 \mod p.$$

Proof. Since $\lambda_1 | n = q^m - 1$, then $\gcd(\lambda_1, p) = 1$ so that $\lambda_1 \mod p$ is a unit in $\mathbb{Z}_p$. Consequently, if $(b-\gamma') \not\equiv 0 \mod p$, then $(b-\gamma')\lambda_1 \equiv (b-\gamma')\frac{n}{q-1} \not\equiv 0 \mod p$.

In order to determine $i \in \mathbb{Z}_n$ such that $s_q(i) \neq 0 \mod p$, it is equivalent to find i such that $i - \gamma' \not\equiv 0 \mod p$ (based on Lemma 8 and Lemma 9) and $i - \gamma' \not\equiv 0 \mod p$ if and only if $\gcd(i-\gamma', q^m) = 1$. Hence, from *Phi Euler function* we have

$$\#A = q^m(1-\frac{1}{p}). \tag{8}$$

The biggest element in $\mathbb{Z}_n$, that is $e = q^m - 2$, contained in A. It can be shown by the following lemma.

Lemma 10. *Let q be a prime power of p. Defined $s_q(i) = \sum_{j=0}^{m-1} k_{ij},$, where $k_{ij} = q^j i \mod n$ and $n = q^m - 1$. Then*

$$s_q(e) + m \not\equiv 0 \mod p,$$

where $e = q^m - 2$.

Proof.

$$\begin{aligned} s_q(e) + m &\equiv (e \mod n) + (qe \mod n) + \cdots \\ &+ (q^{m-1}e \mod n) + m \\ &\equiv (n-1) + (n-q) + \cdots + (n - q^{m-1}) + m \\ &\equiv mn + m - (1 + q + q^2 + \cdots + q^{m-1}) \\ &\equiv -1 \mod p. \end{aligned}$$

From Lemma 1 and $\gcd(e, n) = 1$ we have $|B| = |C_e| = m$. Thus, from (8), we have

$$\#Supp(K_{e,q,m}) = q^m(1 - \frac{1}{p}) - m. \tag{9}$$

The following theorem gives the minimal polynomial of the sequence $\check{s}^\infty$ in (2) with function (3).

Theorem 1. *Let $\check{s}^\infty$ be the sequence of (2), where $f(x) = x^{q^m-2}$, then the minimal polynomial of $\check{s}^\infty$ is given by*

$$\mathbb{M}_{\check{s}}(x) = \prod_{\substack{i \in \mathbb{Z}_n, \\ s_q(i)+m \not\equiv 0 \mod p, \\ i \notin C_e}} (x - \alpha^i), \tag{10}$$

and the linier span $\mathbb{L}_{\check{s}}$ of $\check{s}^\infty$ is

$$\mathbb{L}_{\check{s}} = q^m(1 - \frac{1}{p}) - m.$$

Proof. This theorem follows from Lemma 3, Lemma 10, Eq. (7) and Eq. (9).

The polynomial (10) in Theorem 1 can be used to construct a class of cyclic codes as the following.

Theorem 2. *The cyclic code $\mathcal{C}_{\check{s}}$ defined by sequence of Theorem 1 has parameters $[q^m - 1, \frac{q^m}{p} - 1 + m, d]$ where $d \geq \frac{q(p-1)}{p}$ and generator polynomial $\mathbb{M}_{\check{s}}(x)$ of (10).*

Proof. The dimension of $\mathcal{C}_{\check{s}}$ follows from Theorem 1. Therefore we consider the lower bound of minimum weight d. Note that the weight distribution of the cyclic code generated by $\mathbb{M}_{\check{s}}(x)$ is the same as that generated by the reciprocal polynomial of $\mathbb{M}_{\check{s}}(x)$.

Furthermore, the reciprocal polynomial of $\mathbb{M}_{\check{s}}(x)$ has zeros α^i where $i \in H = \{pj+1 : j = 1, 2, \ldots, \frac{q(p-1)}{p} - 1\}$. Thus, from the Hartmann-Tzeng bound [10, Theorem 1], we have $d \geq \frac{q(p-1)}{p}$.

Example 1. *Let $q = 3$, $m = 2$, and irreducible polynomial for $GF(3^2)$ is $x^2 + 2x + 2 = 0$. Then $\mathcal{C}_{\check{s}}$ is a $[8, 4, 2]$ cyclic code over $GF(3)$ with the generator polynomial $\mathbb{M}_{\check{s}}(x) = x^4 + 2$. It is known that for optimal linear codes of length 8 and dimension 4 over $GF(3)$, the minimal distance is $d = 4$.Its dual is a $[8, 4, 2]$ cyclic code.*

Example 2. *Let $q = 3, m = 3$, and α be a generator of $GF(3^3)^*$ with $\alpha^3 + 2\alpha + 1 = 0$. Then $\mathcal{C}_{\check{s}}$ is a $[26, 11, 6]$ cyclic code over $GF(3)$ with the generator polynomial $\mathbb{M}_{\check{s}}(x) = x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$. It is known that for optimal linear codes of length 26 and dimension 11 over $GF(3)$, the minimal distance satisfies $9 \leq d \leq 11$. Its dual is a [26, 15,4] cyclic code.*

Example 3. *Let $q = 3, m = 3$, and α be a generator of $GF(3^3)^*$ with $\alpha^3 + 2\alpha^2 + 1 = 0$. Then $\mathcal{C}_{\check{s}}$ is a $[26, 11, 6]$ cyclic code over $GF(3)$ with the generator polynomial $\mathbb{M}_{\check{s}}(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$. Its dual is a [26, 15,4] cyclic code.*

4. Conclusion

We have given the construction of a family of cyclic code from periodic sequence $\check{s}$ from a monomial $f(x) = x^{q^m-2}$ in $GF(q^m)$. The lower bound of the code is presented in Theorem 2. In general, the code $\mathcal{C}_{\check{s}}$ has parameter $[q^m - 1, \frac{q^m}{p} - 1 + m, d]$ with $d \geq \frac{q(p-1)}{p}$. Three examples are presented. Numerical examples show that for the same length and distance, the dual of cyclic codes presented in this paper has a lower dimension than in [3, 1983] and [17, page 27].

Acknowledgements

The authors are very grateful to the editors and the reviewers for their comments and suggestions to improve this paper's quality. The authors also thank Irwansyah for the valuable discussions. This work was supported by HIBAH RISET DASAR DIKTI 2019.

References

[1] M Antweiler and L Bömer. Complex sequences over $GF(p^m)$ with a two-level autocorrelation function and a large linear span. *IEEE Trans. Inform. Theory*, 38(1):120–130, 1992.

[2] R T Chien. Cyclic decoding procedures for bose-chaudhuri-hocquenghem codes. *IEEE Trans. Inform. Theory*, 10(4):357–363, 1964.

[3] C Ding. Cyclic codes from some monomials and trinomials. *SIAM Journal on Discrete Mathematics*, 27(4):1977–1994, 2013.

[4] C Ding, G Xiao, and W Shan. *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science*. Springer-Verlag Berlin Heidelberg, 1st edition, 1991.

[5] C Ding, Y Yang, and X Tang. Optimal sets of frequency hopping sequences from linear cyclic codes. *IEEE Trans. Inform. Theory*, 56(7):3605–3612, 2010.

[6] C Ding and Z Zhou. Binary cyclic codes from explicit polynomials over $GF(2^m)$. *Discrete Mathematics*, 321:76–89, 2014.

[7] G D Forney. On decoding BCH codes. *IEEE Trans. Inform. Theory*, 11(4):549–557, 1965.

[8] M Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007. Accessed on 2020-12-20.

[9] K C Gupta and S Maitra. Primitive polynomials over $GF(2)$ - A cryptologic approach. In *Information and Communications Security, Third International Conference, ICICS 2001, Xian, China, November 13-16, 2001*, pages 23–34, 2001.

[10] C R P Hartmann and K K Tzeng. Generalizations of the BCH bound. *Information and Control*, 20(5):489–498, 1972.

[11] W C Huffman and V Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2010.

[12] L Li, S Zhu, L Liu, and X Kai. Some q-ary cyclic codes from explicit monomials over $\mathbb{F}_q^m$. *Problems of Information Transmission*, 55(3):254–274, 2019.

[13] E Lucas. Théorie des fonctions numériques simplement périodiques. *Am. J. Math*, 1:229–231, 1878.

[14] Z Rajabi and K Khashyarmanesh. Some cyclic codes from some monomials. *Appl. Algebra Eng., Commun. Comput.*, 28(6):469–495, 2017.

[15] K H Rosen. *Discrete mathematics and its applications.* McGraw-Hill, 8th edition, 2019.

[16] A Syarifuddin and I Muchtadi-Alamsyah. Construction of cyclic codes over ternary field from periodic sequences. *Southeast Asian Bulletin of Mathematics*, 42(5):773–780, 2018.

[17] C Tang, Y Qi, and M Xu. A note on cyclic codes from APN functions. *Appl. Algebra Eng., Commun. Comput.*, 25(1):21–37, 2014.

[18] A Thangaraj and S W McLaughlin. Quantum codes from cyclic codes over GF(4^m). *IEEE Trans. Inform. Theory*, 47(3):1176–1178, 2001.