Mehmet E. Koroglu · Ibrahim Ozbek · Irfan Siap

Optimal Codes from Fibonacci Polynomials and Secret Sharing Schemes

Received: date / Accepted: date

Abstract In this work, we study cyclic codes that have generators as Fibonacci polynomials over finite fields. We show that these cyclic codes in most cases produce families of maximum distance separable and optimal codes with interesting properties. We explore these relations and present some examples. Also, we present applications of these codes to secret sharing schemes.

Mathematics Subject Classification (2000) 94B05 · 94B15 · 11B39 · 11B50 · 94A62

1 Introduction

Error correcting codes are applied intensively in digital data transfer and storage. Due to this important nature, good error correcting codes which can be considered as codes with best possible parameters so called optimal codes and codes with rich algebraic structures are important for implementations. Cyclic codes serve such a purpose and studies on cyclic codes still cover an important part of the area. A linear code $C$ is a subspace of $V = \mathbb{F}_p^n$ where $\mathbb{F}_p$ denotes the finite field with $p$ elements. The elements of a linear code are called codewords. In order to detect hence correct errors, Hamming metric serves such a purpose. Given two elements in $V$ say $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$, the Hamming distance between $u$ and $v$ is the number of places that differ from each other i.e. $d(u, v) = |\{i : u_i \neq v_i\}|$. The smallest nonzero Hamming distance among the elements of $C$ is referred as the Hamming distance of the code $C$ and it is usually denoted by $d(C)$ or simply $d$. If $C$ is a linear code over $\mathbb{F}_p$ with dimension $k$ and minimum distance $d$, then $C$ is said to be an $[n, k, d]_p$-code. If an error detected while the received word is erroneous, then decoding this word to the closest codeword in $C$ is called the majority decoding method. It is also well known that a linear code with minimum distance $d = 2t + 1$ or $d = 2t + 2$ can correct up to $t$ errors. Given the length and the dimension, finding a linear code with best possible minimum distance is an important problem and it is an open problem except a few special cases. An inner product on $V$ of $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$, is defined as usual $\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i$ in $\mathbb{F}_p$. Then, we can associate a linear code $C^\perp$, called the dual code of $C$, to a code $C$ by $C^\perp = \{v \in V | \langle u, v \rangle = 0 \text{ for all } u \in C\}$. If $C$ is a linear code of length $n$ and dimension $k$, then it is well-known that $C^\perp$ is a linear code of length $n$.
and dimension \( n - k \). In literature, cyclic codes from sequences defined over some extension fields with special generators have been studied. Sequences over fields or rings in general have many applications such as Left Shift Registers (LSR), coding, cryptography, etc [17], [19]. This venue of the research is partially accomplished by considering some special sequences. In each case some special sequences are studied in order to understand the cyclic codes derived from them. Here, we study cyclic codes derived from Fibonacci sequences. In the literature there are studies where Fibonacci sequences and codes are related but to the best knowledge of the authors these studies are in different directions compared to the one presented in this paper. An example of such study is done by Lee et al. [11] where linear codes related to Fibonacci sequences are presented and burst error correction of such families are studied. There are further studies that are inspired by Fibonacci sequences and codes are related but to the best knowledge of the authors these studies are yet. However, the following theorem gives a restriction for possible values of \( l_p \).

**Theorem 1** [21] \( F_n \equiv a \mod p \) is divisible by \( l_p \).

**Theorem 2** [22] Let \( l_p \) denote the period of the Fibonacci sequence modulo \( p \). Then,

1. If \( p \) is prime and \( p \equiv 1 \mod 10 \), then \( l_p | p - 1 \).
2. If \( p \) is prime and \( p \equiv 3 \mod 10 \), then \( l_p | 2(p + 1) \).

**Lemma 1** [8] 5 is a quadratic residue modulo primes of the form \( 5t \pm 1 \) and a quadratic non-residue modulo primes of the form \( 5t \pm 2 \).

**Lemma 2** [22] If a prime \( p \) is of the form \( 5t \pm 1 \) then \( F_{p-1} \equiv 0 \) and \( F_p \equiv 1 \mod p \). If a prime \( p \) is of the form \( 5t \pm 2 \), then \( F_p \equiv -1 \) and \( F_{p+1} \equiv 0 \mod p \).

Let \( a \mod p \) denote the index of the subscript of the first nonzero term of the Fibonacci sequence which is divisible by \( p \). Let \( s \mod p \) be the least residue of \( F_{a(p)+1} \mod p \) and let \( \beta \mod p \) denote the order of \( s \mod p \) i.e. the smallest positive integer \( \beta \mod p \) such that \( s \mod p \equiv 1 \mod p \).

**Theorem 3** [18] \( l_p = a \mod p \beta \mod p \).

As a result of Theorem 3, \( \beta \mod p \) can be considered as the number of zeros in a single period of Fibonacci sequence computed in \( \mathbb{F}_p \).

**Theorem 4** [18] \( l_p = \gcd (2, \beta \mod p) \cdot \text{lcm} [a \mod p, \gamma \mod p] \), where \( \gamma (2) = 1 \) and \( \gamma (p) = 2 \) for \( p > 2 \).

**Corollary 1** [18]

1. \( l_p \) is even for \( p > 2 \).
2. \( \beta \mod p = 1, 2, \text{ or } 4 \).
Corollary 2 \[ \text{The nonempty subset } C \text{ of } \mathbb{F}_p \text{ is cyclic if and only if } \phi \text{ with } \| \phi \| = 1. \]
Since the minimum distance determines the error correction and detection capability of a code, it is an important parameter for codes, and also determining it is a very difficult problem. There are at least some bounds that help on estimating the minimum distance of a code. Now, we present definitions and theorems regarding some special bounds that are going to be referred in the sequel.

**Definition 5** [Singleton bound] If $C$ is a linear code with parameters $[n, k, d]$, then $k \leq n - d + 1$.

**Definition 6** [Singleton bound] A linear code with parameters $[n, k, d]$ such that $k + d = n + 1$ is called a maximum distance separable (MDS) code.

The code presented in Example 1 is MDS.

**Theorem 6** (Griesmer Bound) [13] Let $C$ be a $p$-ary code of parameters $[n, k, d]$, where $k \geq 1$. Then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil.$$

Here, if $\alpha$ is a real number, then $\lceil \alpha \rceil$ denotes the smallest integer larger or equal to (the ceil) $\alpha$.

**Example 2** Let $C$ be a cyclic linear code generated by the polynomial $g(x) = x^{14} + 6x^{13} + 2x^{12} + 4x^{11} + 5x^{10} + 6x^9 + 6x^8 + x^7 + 5x^3 + 3x^2 + 2x + 1$ over $\mathbb{F}_7[x]/(x^{16} - 1)$. The code $C$ has parameters $[16, 2, 14]_7$. Thus, we have $16 \geq \sum_{i=0}^{1} \left\lceil \frac{14}{7^i} \right\rceil = 14 + 2 = 16$. So, the given code meets the Griesmer bound.

2 Cyclic Codes Obtained from Fibonacci Polynomials

In this section we study cyclic codes that are generated by polynomials related to Fibonacci sequences.

**Definition 7** [13] Let $S = \{s_0, s_1, \ldots\}$ be an arbitrary sequence over $\mathbb{F}_p$. Assume that $s_{i+l} + c_{i-1}s_i - s_{i-l}$ for some elements $c_0, c_1, \ldots, c_{l-1} \in \mathbb{F}_p$ and for all $i = 0, 1, \ldots$. Then the polynomial $x^l + c_{l-1}x^{l-1} + \ldots + c_1x + c_0$ is called the characteristic polynomial of $S$. A characteristic polynomial of minimal degree is called the minimal polynomial of $S$.

For a periodic sequence $S = \{s_0, s_1, \ldots\}$ with a period $N$ we have $s_{i+N} - s_i = 0$, so $x^N - 1$ is a characteristic polynomial of $S$. If $N$ is a period of $S$, then the minimal polynomial of $S$ is

$$x^N - 1 = \gcd (x^N - 1, s_{N-1}x^{N-1} + \ldots + s_1x + s_0).$$

Let $F = \{F_0, F_1, \ldots, F_n, \ldots\}$ denote the Fibonacci sequence over $\mathbb{F}_p$ and suppose that the period of this sequence is equal to $l$. The polynomial $f(x) = \sum_{i=0}^{l-1} F_ix^i \in \mathbb{F}_p[x]$ is called Fibonacci polynomial of $F$ over $\mathbb{F}_p$.

**Theorem 7** Let $f(x) \in \mathbb{F}_p[x]$ be the Fibonacci polynomial with period $l = p - 1$ and $\beta (p) = 1$. Then,

1. $(f(x), x^{p-1} - 1) = \frac{x^{p-1} - 1}{x^l - 1} \in \mathbb{F}_p[x]$
2. The cyclic code $C = \langle f(x) \rangle$ generated by $f(x)$ with dimension 2, and the minimum distance $d = p - 2$.
3. $C = \langle f(x) \rangle$ is an MDS code of type $[p - 1, 2, p - 2]_p$.

**Proof** 1. By direct checking and applying the properties of Fibonacci sequence we see that $f(x)(x^2 + x - 1) = x^l - x \in \mathbb{F}_p[x]$. Since $x|f(x)$ but $x|x^{p-1} - 1$ we have $(f(x), x^{p-1} - 1) = \frac{x^{p-1} - 1}{x^l - 1}$. 


2. Let \( g(x) = (f(x), x^{p-1} - 1) \) be the cyclic code of length \( p - 1 \) generated by \( g(x) \) and dimension \( p - 1 - \deg(g(x)) = 2 \). This codes has exactly \( p^2 \) codewords. Since \( g(x) = f(x), \ w(f(x)) = w(g(x)) \). Since the number of zeros in a single period of given Fibonacci sequence is only one, then we have \( w(g(x)) = p - 2 \). Also, \( w(xg(x)) = p - 2 \) for which \( xg(x) \in C \). The codeword \( g(x) \) has the zero entry in its first coordinate and \( xg(x) \) has the zero entry in its second coordinate. Suppose that a codeword \( c(x) \in C \) has two entries with zeros. Then, \( g(x), xg(x), c(x) \) will give a linearly independent subset of vectors in \( C \) which is a contradiction to the dimension 2 of \( C \).

3. Follows from previous part and Definition 6

**Corollary 3** The codes given in Theorem 7 are RS codes.

**Theorem 8** Let \( f(x) \in \mathbb{F}_p[x] \) be the Fibonacci polynomial with period \( l = p - 1, \beta(p) = 1 \) and \( C = \langle f(x) \rangle \). Then, the dual code of \( C, C^\perp = \langle x^2 + x - 1 \rangle \) is an MDS code with parameters \([p - 1, p - 3, 3]_p\).

**Proof** Clearly the length of \( C^\perp \) is \( p - 1 \). Let us now determine the dimension and minimum distance of \( C^\perp \). Since \( C^\perp = \langle x^2 + x - 1 \rangle \), we have \( \dim(C^\perp) = p - 1 - 2 = p - 3 \). We know that \( C \) is MDS, so \( C^\perp \). By the Singleton bound we have \( p - 1 + 1 = p - 3 + d \). Thus \( d = 3 \).

**Corollary 4** Let \( f(x) \in \mathbb{F}_p[x] \) be the Fibonacci polynomial with period \( l = p - 1 \).

1. If \( \beta(p) = 2 \), then \( C = \langle f(x) \rangle \) is a cyclic code of type \([p - 1, 2, p - 3]_p\).
2. If \( \beta(p) = 4 \), then \( C = \langle f(x) \rangle \) is a cyclic code of type \([p - 1, 2, p - 5]_p\).

**Theorem 9** Let \( f(x) \in \mathbb{F}_p[x] \) be the Fibonacci polynomial with period \( l = 2p + 2 \) and \( \beta(p) = 2, 4 \). Then,

1. \((f(x), x^{p-1} - 1) = \frac{x^{p-1} - 1}{x^2 + x - 1} \in \mathbb{F}_p[x] \)
2. The cyclic code \( C = \langle f(x) \rangle \) generated by \( f(x) \) has dimension 2, and the minimum distance \( d = 2p + 2 - \beta(p) \).
3. \( C = \langle f(x) \rangle \) is a linear code of type \([2p + 2, 2, 2p + 2 - \beta(p)]_p\).

**Proof** Follows from Theorem 7.

**Corollary 5** Let \( f(x) \in \mathbb{F}_p[x] \) be the Fibonacci polynomial with period \( l = 2p + 2 \).

1. If \( \beta(p) = 2 \), then \( C = \langle f(x) \rangle \) is an optimal code of type \([2p + 2, 2, 2p]_p\).
2. If \( \beta(p) = 4 \), then \( C = \langle f(x) \rangle \) is a code of type \([2p + 2, 2, 2p - 2]_p\).

**Proof** 1. Since \( \beta(p) = 2 \), by the Theorem 9 \( C = \langle f(x) \rangle \) is a \([2p + 2, 2, 2p]_p\)-code. Recall that the Griesmer bound for a linear code \( C \) of type \([n, k, d]_p \) is \( n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil \). Thus we have \( 2p + 2 \geq \left\lceil \frac{2p}{p^0} \right\rceil + \left\lceil \frac{2p}{p^1} \right\rceil = 2p + 2 \). So, \( C = \langle f(x) \rangle \) is an optimal code.
2. Clearly, if \( \beta(p) = 4 \), then by the Theorem 9 \( C = \langle f(x) \rangle \) is a code of type \([2p + 2, 2, 2p - 2]_p\).

**Lemma 3** Let \( F_n \) be a Fibonacci sequences with period \( l \) over \( \mathbb{F}_p \). Then, there are \( \frac{l - \beta(p)}{\beta(p)} - 1 \) non-zero, non-multiple and different, two consecutive terms in a sequence.

**Proof** We know that there are \( l - \beta(p) \) nonzero terms in a sequence and if we obtain zero term in a sequence, then the length of subsequent terms until another zero term must be a multiple of the preceding part of the sequence. So there are \( \frac{l - \beta(p)}{\beta(p)} - 1 \) non-zero, non-multiple and different, two consecutive terms in a sequence.

**Theorem 10** The cyclic codes given in the Theorem 7 Corollary 4 and Theorem 9 are constant one or two weight codes.
Table 2 The weight distribution of the codes given in Theorem 7 for $\beta(p) = 1$

| Length | Weight $w$ | Multiplicity $A_w$ |
|--------|------------|---------------------|
| $l = p - 1$ | 0 | $1$ |
|         | $p - 2$ | $(p - 1)^2$ |
|         | $p - 1$ | $2(p - 1)$ |

Table 3 The weight distribution of the codes given in Corollary 4 and Theorem 9 for $\beta(p) = 2$

| Length | Weight $w$ | Multiplicity $A_w$ |
|--------|------------|---------------------|
| $l = p - 1$ | 0 | $1$ |
|         | $p - 3$ | $(p - 1)^2$ |
|         | $p - 1$ | $(p - 1)(p + 3)$ |
| $l = 2p + 2$ | 0 | $1$ |
|         | $2p$ | $p^2 - 1$ |

Proof Since the dimension of given codes are 2, the generator matrix is of the form

$$G = \begin{pmatrix} f(x) \\ x f(x) \end{pmatrix}.$$  

Thus we can generate in total $p^2$ codewords from the generator matrix $G$ where clearly one of them is all the zero vector. The number of nonzero coefficients of $f(x)$ is the same as with $x f(x)$ and the weight of these codewords are $l - \beta(p)$. So, from the rows of generator matrix $G$, we can obtain $2(p - 1)$ codewords of weight $l - \beta(p)$. Also, generalized Fibonacci sequences (for details see [9]) satisfies the following facts:

1. If we start with any two consecutive fibonacci numbers for $a$ and $b$, $\bar{G}(a,b,i)$ will be essentially the same as the fibonacci sequence but with its indices changed. The general rule is

$$\bar{G}(f(k), f(k + 1), i) = f(i + k)$$  \hfill (2)

2. Multiplying all the terms by $k$ gives the same sequence as the one with starting values $ka$ and $kb$

$$\bar{G}(ka, kb, i) = k\bar{G}(a, b, i).$$  \hfill (3)

The Equation (2) says that if we start with any two consecutive Fibonacci numbers, then we obtain codewords whose weight are the same with the codewords of the form $f(x)$. By Lemma 3 there are $\frac{l - \beta(p)}{\beta(p)} - 1$ non-zero, non-multiple and different, two consecutive terms in a Fibonacci sequence mod $p$. Also from the Equation (3), there are $p - 1$ multiple of each non-zero two consecutive terms. Then, we have \( \left(\frac{l - \beta(p)}{\beta(p)} - 1\right)(p - 1) \) codewords which has same weight with $f(x)$. Therefore, the total number of the codewords of weight $l - \beta(p)$ are $2(p - 1) + \left(\frac{l - \beta(p)}{\beta(p)} - 1\right)(p - 1)$. Since the minimum weight of the codes given in Theorem 7, Corollary 4 and Theorem 9 are $d = l - \beta(p)$, the other weights of the codewords must be $l$. Because every Fibonacci sequence mod $p$ has $\beta(p)$ parts and all these parts have the same weight. Thus, the number of codewords of weight $l$ are

$$p^2 - \left(1 + 2(p - 1) + \left(\frac{l - \beta(p)}{\beta(p)} - 1\right)(p - 1)\right).$$

Corollary 6 Let $A_w$ denote the number of codewords with Hamming weight $w$ in the codes given in the Theorem 7, Corollary 4 and Theorem 9. Then the weight distribution of these codes are given in Table 2, 3, 4.
Theorem 11

Let \( \beta(p) \) be the number of zeros of given extended Fibonacci sequence. Then, the cyclic code \( C = \langle t(x) \rangle \) generated by \( t(x) \) has dimension \( r \) and the minimum distance \( d = p^{r-1} - 1 - \beta(p) \). So, \( C = \langle t(x) \rangle \) is a linear code of type \([p^{r-1} - 1, r, p^{r-1} - 1 - \beta(p)]_p\).
Corollary 5, If we take Example 6, we have

For Example 5, from Theorem 7, the cyclic linear code \( C \) generated by \( f(x) \) is an MDS code of parameters \([10,2,9]_11\) and weight polynomial \( u^{10} + 100 u^9 + 20 u^8. \) Indeed, the Fibonacci polynomial of \( F \) is \( f(x) = x^5 + 2 x^3 + 4 x^2 + 5 x + 1 \) and the minimal polynomial of \( F \) is \( g(x) = \gcd(f(x), x^{10} - 1) = \frac{1}{x^5 + 2 x^3 + 5 x + 1}. \) The generator matrix of \( C \) is the following:

\[
G = \begin{bmatrix}
1 & 0 & 1 & 1 & 2 & 3 & 5 & 8 & 2 & 10 \\
0 & 1 & 1 & 2 & 3 & 5 & 8 & 2 & 10 & 1
\end{bmatrix}.
\]

Moreover, by the Theorem 8, the dual code of \( C, C^\perp \) is also an MDS code with parameters \([10,8,3]_11\) and generator matrix:

\[
H = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 10 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 10 & 9 & 9 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 8 & 8 & 8 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 6 & 6 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 3 & 3 & 3 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 9 & 9 & 9 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 11 & 11 & 11 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}.
\]

Example 5 For \( p = 19 \), we have

\[
F = \{0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1, \ldots\}
\]

and hence we have \( l_{19} = 18, a(19) = 18, \) and by the Theorem 8, \( 18 = 18 \beta (19), \) thus, \( \beta (19) = 1. \) From Theorem 7, the cyclic linear code \( C \), generated by \( f(x) \) is an MDS code with parameters \([18,2,17]_{19}\) and weight polynomial \( u^{18} + 324 u^{17} + 36 u^{18}. \) Indeed, the Fibonacci polynomial of \( F \) is \( f(x) = x^5 + 2 x^3 + 3 x^2 + 4 x + 1 \) and the minimal polynomial of \( F \) is \( g(x) = \gcd(f(x), x^{18} - 1) = \frac{1}{x^5 + 2 x^3 + 4 x + 1}. \) Furthermore, by the Theorem 8, the dual code of \( C, C^\perp \) is also an MDS code of type \([18,16,3]_{19}\).

Example 6 If we take \( p = 7 \), then \( F = \{0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, \ldots\} \) and hence we have \( l = 16, a(7) = 8, \) and by the Theorem 9, \( 16 = 8 \beta (7), \) so \( \beta (7) = 2. \) By the Theorem 2 and Corollary 5, \( C \) is an optimal code of type \([16,2,14]_7\) with weight polynomial \( u^{16} + 48 u^7 + 14. \) Actually, the Fibonacci polynomial of \( F \) is \( f(x) = x^5 + 2 x^3 + 3 x^2 + 4 x + 1 \) and the minimal polynomial of \( F \) is \( g(x) = \gcd(f(x), x^{16} - 1) = \frac{1}{x^5 + 2 x^3 + 4 x + 1}. \) This code attains the Griesmer bound and hence it is an optimal code.
3 Fibonacci Codes and Secret Sharing Schemes

3.1 Secret Sharing Schemes From Codes

Secret sharing system is a method of projecting a secret data to finitely many participants with the aim that a designed number of or designed participants can recover the data. In this system, a secret data $s$ is divided into shares and distributed to participants from the set $P = \{P_1, P_2, ..., P_{n-1}\}$ in such a way that only authorized subsets of $P$ can reconstruct the secret whereas unauthorized subsets cannot reconstruct the secret. There are several secret sharing system in literature [3], [4], [16], [20]. One of them is based on coding theory. In 1993, Massey has shown that every linear code can be used to construct the secret sharing scheme [15]. Let now us recall the system given by Massey. Let $C$ be an $[n, k, d]$ linear code over finite field $\mathbb{F}_p$ and $G = [g_0, g_1, ..., g_{n-1}]$ be a generator matrix of $C$ where $g_i$’s are the column vectors of $G$. In this system, column vectors of $G$ are nonzero. Dealer, who is a person building the system, randomly choose a vector from $\mathbb{F}_p^d$ to generate the codeword $uG = (v_0, v_1, ..., v_{n-1})$. The dealer picks the first coordinate of a codeword as a secret, i.e., $s = v_0 = ug_0$, and distributes $v_i$ to participants $P_i$ as a share for $1 \leq i \leq n - 1$. Since $s = v_0 = ug_0$, it is easily seen that set of shares $\{v_1, v_2, ..., v_{n-1}\}$ determines the secret $s$ if and only if $g_0$ is a linear combination of $g_1, g_2, ..., g_{n-1}$. To recover the secret $s$, firstly the linear equation $g_0 = \sum_{j=1}^{n} x_j g_{ij}$ is solved and $x_j$ is found, then the secret is computed by

$$v_0 = u g_0 = \sum_{j=1}^{n} x_j u g_{ij} = \sum_{j=1}^{n} x_j v_i.$$ 

**Definition 8** [15] Let $v$ be a vector of length $n$ over $\mathbb{F}_p$. The support of $v$ is defined as

$$\text{supp}(v) = \{0 \leq i \leq n - 1 : v_i \neq 0\}.$$ 

We say that a vector $v_2$ covers a vector $v_1$ if the support of vector $v_2$ contains that of $v_1$, i.e., $\text{supp}(v_1) \subseteq \text{supp}(v_2)$.

**Definition 9** [15] A nonzero vector $c$ is called minimal if it only covers its scalar multiples. If the first component of minimal vector $c$ is 1, then the vector $c$ is called minimal codeword.

**Definition 10** [12] The family of all authorized subsets of $P$ is called access structure of the scheme. Authorized subsets of $P$ are called minimal access sets if they can reconstruct the secret $s$ but any of its proper subsets cannot reconstruct the secret $s$.

Hence we have the following main lemma:

**Lemma 4** [15] Let $C$ be an $[n, k, d]$ linear code over finite field $\mathbb{F}_p$ and $C^\perp$ be the dual code of $C$. In the secret sharing scheme based on $C$, a set of shares $\{v_{i_1}, v_{i_2}, ..., v_{i_t}\}$ recovers the secret $s$ if and only if there is a codeword in $C^\perp$ such that

$$(1, 0, ..., 0, c_{i_1}, 0, ..., c_{i_t}, 0, ..., 0)$$

where $c_{i_j} \neq 0$ for at least one $j$, $1 \leq i_1 < ... < i_m \leq n - 1$ and $1 \leq m \leq n - 1$.

From Lemma 4 it is clear that there is a one to one correspondence between the set of minimal access sets and sets of minimal codewords. But, it is very hard to find the minimal codewords of linear codes in general.
3.2 Access Structures From Fibonacci Codes

In this section, we consider the secret sharing schemes obtained from Fibonacci codes whose minimal codewords can be characterized. Let us remind two lemmas in the literature which state the main results how to determine the access structure.

**Lemma 5** Let \( C \) be an \([n,k,d]\) code over \( \mathbb{F}_p \). Let \( w_{\min}, w_{\max} \) be a minimum and maximum nonzero weight of \( C \), respectively. If
\[
\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}
\]
then each nonzero codeword of \( C \) is a minimal vector.

**Lemma 6** Let \( C \) be an \([n,k,d]\) code over \( \mathbb{F}_p \) and let \( G = [g_0, g_1, \ldots, g_{n-1}] \) be its generator matrix. If each nonzero codeword of \( C \) is a minimal vector, then in the secret sharing scheme based on \( C^\perp \), there are altogether \( p^{k-1} \) minimal access sets. In addition, we have the followings:

1. If \( g_i \) is a multiple of \( g_0 \), \( 1 \leq i \leq n-1 \), then participant \( P_i \) must be in every minimal access set. Such a participant is called a dictatorial participant.
2. If \( g_i \) is not a multiple of \( g_0 \), \( 1 \leq i \leq n-1 \), then participant \( P_i \) must be in \( (p-1) p^{k-2} \) out of \( p^{k-1} \) minimal access sets.

**Theorem 12** From Corollary 6 and Table 3 in the secret sharing scheme based on the dual code of the code with parameters \([2p+2, 2, 2p]\) over \( \mathbb{F}_p \), there are \( p \) minimal access sets and \( P_{p+1} \) is a dictatorial participant. Furthermore, each of the other participant \( P_i \) is involved in \((p-1)\) minimal access sets.

**Proof** The codes of parameters \([2p+2, 2, 2p]\) are one weight codes and by Lemma 5 all codewords of such codes are minimal. Thus, from Lemma 6 there are \( p^{2-1} = p \) minimal access sets. Also, from the Fibonacci sequence \( \mod p \) and \( \beta(p) = 2 \), we have two multiple parts in a sequence. So, the \( g_{p+1} \) column is a multiple of \( g_0 \). This means that \( P_{p+1} \) is a dictatorial participant. The other remaining participants are involved in \((p-1) p^{2-2} = (p-1) \) minimal access sets.

**Example 7** The code \( C \) given in Example 6 has parameters \([16, 2, 14]\) with the following weight distribution:
\[
u^{16} + 48u^{2}v^{14}.
\]

In the secret sharing scheme based on the dual code of \( C \), the number of minimal access sets are \( 7 \), and the list of all these minimal access sets are as follows:
\[
\{2,3,4,5,6,7,8,10,11,12,13,14,15\}, \{1,2,3,4,5,6,8,9,10,11,12,13,14\},
\{1,2,3,4,5,7,8,9,10,11,12,13,15\}, \{1,2,4,5,6,7,8,9,10,12,13,14,15\},
\{1,2,3,5,6,7,8,9,10,11,13,14,15\}, \{1,2,3,4,6,7,8,9,10,11,12,14,15\},
\{1,3,4,5,6,7,8,9,11,12,13,14,15\}.
\]

where \( \{2,3,4,5,6,7,8,10,11,12,13,14,15\} \) denotes the access set
\[
\{P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}\}.
\]

In this example, \( P_8 \) is dictatorial participant and each participant is involved in exactly 6 minimal access sets.

**Theorem 13** From Corollary 6 and Table 2 in the secret sharing schemes based on the dual code of the code of parameters \([p-1, 2, p-2]\) over \( \mathbb{F}_p \), there are \( p-2 \) minimal access sets. Furthermore, each participant \( P_i \) is involved in \((p-3)\) minimal access sets.
Proof From Table 2 it is easily seen that the codewords of weight \( p - 2 \) whose first component 1 are minimal codewords. We have in total \( \binom{p}{2} = p \) codewords whose first component are 1. We should remove full weight codes whose first component are 1, to get minimality. There are 2 \((p - 1)\) codewords which have weight \( p - 1 \). So, there are \( \frac{2(p - 1)}{p - 1} = 2 \) codewords whose first component is 1. This gives us, the total number of the codewords of weight \( p - 2 \) whose first component is 1. Consequently, we have \( p - 2 \) minimal codewords. Therefore, there are \( p - 2 \) minimal access sets.

**Second part of proof:** If we fix \( i \), \( 1 \leq i \leq p - 2 \), participant \( P_i \) is involved in \( p - 2 \) minimal access sets. In this case we can choose remaining participants to recover the key in \((p - 3) \) ways. Hence this is a contradiction to \( p \) minimal access sets and \( P_i \) is minimal access sets.

We only state and skip the proofs of the following two lemmas since they can be proved similarly as in Theorem 12 and Theorem 13.

**Corollary 7** From Corollary 6 and Table 5 in the secret sharing scheme based on the dual code of the code of parameters \([p - 1, 2, p - 3]\) over \( \mathbb{F}_p \), there are \( \frac{p - 3}{2} \) minimal access sets and \( P_i \) is a dictatorial participant. Furthermore, each of the other participant \( P_i \) is involved in \( \left( \frac{p - 5}{4} \right) \) minimal access sets.

**Corollary 8** From Corollary 6 and Table 4 in the secret sharing schemes based on the dual code of the code of parameters \([p - 1, 2, p - 5]\) over \( \mathbb{F}_p \), there are \( \frac{p - 5}{2} \) minimal access sets and the set of \( \left\{ P_{p - 1}, P_{p - 1}, P_{3(p - 1)} \right\} \) are a dictatorial participants. Furthermore, each of the other participant \( P_i \) is involved in \( \left( \frac{p - 5}{2} \right) \) minimal access sets.

**Corollary 9** From Corollary 6 and Table 4 in the secret sharing schemes based on the dual code of the code of parameters \([2p + 2, 2, 2p - 2]\) over \( \mathbb{F}_p \), there are \( \frac{p - 1}{2} \) minimal access sets and \( \left\{ P_{p + 1}, P_{p + 1}, P_{3(p + 1)} \right\} \) are a dictatorial participant. Furthermore, each of the other participant \( P_i \) is involved in \( \left( \frac{p - 3}{2} \right) \) minimal access sets.

**Example 8** For \( \beta(p) = 1 \) and \( l = p - 1 \), we have a linear code of parameters \([10, 2, 9]_{11}\) given in Example 6 From Theorem 13 there are \( p - 2 = 9 \) minimal access sets and the list of all these minimal access sets are as follows:

\[
\{2, 3, 4, 5, 6, 7, 8, 9\}, \{1, 2, 3, 4, 5, 6, 7, 8\}, \{1, 2, 3, 4, 5, 6, 7, 9\}, \\
\{1, 2, 3, 5, 6, 7, 8, 9\}, \{1, 2, 4, 5, 6, 7, 8, 9\}, \{1, 2, 3, 4, 5, 6, 7, 9\}, \\
\{1, 2, 3, 4, 5, 6, 8, 9\}, \{1, 2, 3, 4, 5, 7, 8, 9\}, \{1, 3, 4, 5, 6, 7, 8, 9\}.
\]

In this example, each participant is involved in exactly \( p - 3 = 8 \) minimal access sets.

**Example 9** Let \( \beta(p) = 4 \) and \( p = 13 \). By the Theorem 4 we have linear code of parameters \([28, 2, 24]_{13}\). The weight polynomial of the given code is \( u^{28} + 84u^{24} + 84u^{28} \). From Corollary 9 there are \( \frac{p - 1}{2} = 6 \) minimal access sets and \( P_7, P_{14}, P_{21} \) are dictatorial participants. The list of all these minimal access sets are as follows:

\[
\{2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27\}, \\\n\{1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26\}, \\\n\{1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 27\}, \\\n\{1, 2, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27\}, \\\n\{1, 2, 3, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 26, 27\}, \\\n\{1, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 24, 25, 26, 27\}.
\]
4 Conclusion

In this paper, we studied cyclic codes with generator polynomials derived from Fibonacci sequences modulo a prime $p$. We showed that such cyclic codes enjoy very good properties as they give examples of MDS and optimal cyclic codes. Also, we are able to determine all parameters of such codes. Finally, we present applications to secret sharing schemes via Fibonacci codes.

Acknowledgements This research is partially supported by TUBITAK-ARDEB under the project with grant number 114F388

References

1. A. ASHIKHMIN, A. BAR, G. COHEN, L. HUGUET, Variations on minimal codewords in linear codes, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 96-105 (1995).
2. A. ASHIKHMIN, A. BAR, Minimal vectors in linear codes, IEEE T. Inform. Theory 44, 5, 2010–2017 (1998).
3. C. ASMUTH AND J. BLOOM, A modular approach to key safeguarding, IEEE T. Inform. Theory 30, 2, 208–210 (1983).
4. G. B. BLAKLEY, Safeguarding cryptographic keys, Proc. AFIPS 48, 313–317 (1979).
5. D. M. BURTON, Elementary Number Theory, Tata McGraw-Hill Education, 2006.
6. C. DING AND J. YUAN, Covering and secret sharing with linear codes, Dimacs. Ser. Discret. M., 11–25 (2003).
7. M. ESMAILI, M. ESMAILI, A Fibonacci-polynomial based coding method with error detection and correction, Computers and Mathematics with Applications 60, 10, 2738–2752 (2010).
8. M. HAZEWINKEL (EDITOR), Handbook of Algebra, Volume 1, Netherlands, 1995.
9. A.F. HORADAM, A generalized Fibonacci sequence, American Mathematical Monthly 68, 5, 455–459 (1961).
10. W. H. KAUTZ, Fibonacci codes for synchronization control, IEEE Transactions on Information Theory, 11, 2, 284–292 (1965).
11. G.Y. LEE, D.H. CHO, AND J.S. KIM, Burst-Error-Correcting Block Code Using Fibonacci Code, Journal of the Chungcheong Mathematical Society 22, 3, 367–374 (2009).
12. Z. LI, X. TING, L. HONG, Secret sharing schemes from binary linear codes, Information Sciences, 180, 4412–4419 (2010).
13. S. LING AND C. XING, Coding Theory; A First Course, United Kingdom, 2004.
14. F.J. MACWILLIAMS AND N.J.A. SLOANE, The Theory of Error-Correcting Codes, Vol. 16. Elsevier, 1977.
15. J. L. MASSEY, Minimal codewords and secret sharing, Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory 1993.
16. R.J. McELIECE AND D. V. SARWATE, On sharing secrets and Reed-Solomon codes, Commun. ACM 24, 9 (1981), 583–584 (1993).
17. K. NYBERG, Differentially uniform mappings for cryptography, Advances in Cryptology-EUROCRYPT 93, New York, 55–64.
18. D.W. ROBINSON, The Fibonacci matrix modulo m, Fibonacci Quart. 12, 29–36 (1963).
19. W. ST, C. DING, A simple stream cipher with proven properties, Cryptography and Communications, 4, 79–104 (2012).
20. A. SHAMIR, How to share a secret, Commun. ACM 22, 11, 612–613 (1979).
21. D. D. WALL, Fibonacci Series Modulo m, American Mathematical Monthly 67, 6, 525–532 (1960).
22. S. VAJDA, Fibonacci and Lucas Numbers, and the Golden Section, England, 1989.
