Cumhuriyet Sci. J., 46(2) (2025) 405-409
DOI: https://doi.org/10.17776/csj.1524109

Cumhuriyet Science Journal

| csj.cumhuriyet.edu.tr | Founded: 2002 ISSN: 2587-2680 e-ISSN: 2587-246X Publisher: Sivas Cumhuriyet University

Recursive Polynomial Sets and Their Some Algebraic Applications

Hacı Aktaş [1, a, *]

[1] *Department of Mathematics, Erciyes University, Kayseri, Türkiye.*
**Corresponding author*

Research Article

History
Received: 30/07/2024
Accepted: 12/03/2025

ABSTRACT

This paper primarily defines the framework for a new class of polynomial sets over a finite field GF (2), providing a recursive definition and delving into pertinent algebraic properties. We also studied some applications of the obtained polynomial classes on coding theory, such as obtaining new code classes. Our focus lies on polynomial sets with degrees equal to or less than n, for which we present a methodology for encoding and decoding utilizing an irreducible polynomial *p(x) = xm+xs+1, (m = 2n-1).* Furthermore, as an application of this method in coding theory, we created new code classes and studied some features of these codes.

Keywords: Polynomial sets, Polynomial codes, Generator matrix..

[a] *haciaktas@erciyes.edu.tr* *https://orcid.org/0009-0001-6977-5133*

Introduction

Polynomials appear in a wide range of scientific and mathematical fields. In more advanced mathematical settings, they are basic building blocks for formulating algebraic varieties and polynomial rings, which are essential concepts in algebra and algebraic geometry. Polynomial systems defined over finite fields hold particular significance owing to their wide-ranging applications in fields such as cryptography, coding theory, and various domains within information science and technology. Recursive polynomials have been studied in many fields for different purposes. For example, Cadilhac et al. [1] studied the expressive power of polynomial recursive sequences, a nonlinear extension of the well-known class of linear recursive sequences. Fu et al. [2] construct two classes of permutation polynomials over F_{q^2} with odd characteristic from rational Ŕedei functions. With the help of a computer, they find that the number of permutation polynomials of these types is quite big. Sidki et al.[3] gave three recursive algorithms for computing the orthogonal polynomials. Unlike the models mentioned above, we obtained polynomial sets using recurrence relations. We studied the algebraic structure of these polynomial sets and presented some examples of how these sets can be used in coding theory in our study.

In 1948, Claude Shannon's paper [4] gave rise to information theory and coding theory, which aim to improve communication regarding convenience, reliability, and efficiency. In recent studies on polynomial codes, Ding and Ling [5] constructed a new family of cyclic codes using q-polynomials. Abdullaev and Efanov [6] presented the revealed patterns of constructing polynomial codes with different detecting characteristics. Chiu [7] proposed an alternative expression of polar codes using polynomial representations. Wang, Hao, and Qiao [8] used a method to construct new q −ary linear codes and applied it to the construction of generalized $R-S$ codes over F_q in order to extend the length of the codes. Nalli and Haukkane [9] introduced $h(x)$ −Fibonacci polynomials that generalize both Catalan's Fibonacci polynomials and Byrd's Fibonacci polynomials, and also the k −Fibonacci numbers, and they provide properties for these $h(x)$ −Fibonacci polynomials. Prasad [10] defined $(h(x), g(y))$ − extension of Fibonacci p −numbers and golden $(p, h(x), g(y))$ −proportion. He also established a relation among Golden $(p, h(x), g(y))$ −proportion, Golden $(p, h(x))$ −proportion, and Golden p −proportion. Stakhov [11] considered a new approach to coding theory, which is based on the Q_p-matrices. Kaymak [12] introduced $h(x)$ −Fibonacci coding/decoding method for $h(x)$ −Fibonacci polynomials.

This article aims to define a new polynomial set and study its algebraic properties and then study some applications in coding theory using these polynomial sets. For this, we first define a set of polynomials. We then survey on algebraic properties of polynomials. Besides, we obtained code sets with the created polynomial classes. We studied some algebraic properties of these codes. We expressed tools such as the generator matrix, the parity check matrix, length, and weight. Finally, we conclude the study with suggestions for future research.

Preliminaries

This section provides some basic notions needed for the following sections. Let's give some well-known basic concepts in coding theory [13-16], as follows:

1. A linear $[n, k]$ code C of length n over $GF(q)$ is a k −dimensional vector subspace of $GF(q)^n$.

2. The number of non-zero coordinates in a code word, which is an element of C, is its (Hamming) weight. $wt(x)$ is the (Hamming) weight of a codeword x. A linear code C with a minimum weight is represented as follows: $w(C) := min\{wt(x): x \in C, x \neq 0\}$.

3. The (Hamming) distance between two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ is the number of places where they differ and is denoted by $d(x, y)$. A minimum distance of a linear code C is denoted by $d(C) = min\{d(x, y: x, y \in C\}$.

4. An alternative notation for a linear code C over $GF(q)$ is a $[n, k, d]$ linear code, where d is the minimum distance of C.

5. $x.y = \sum_{i=1}^{n} x_i y_i$ is the Euclidean inner product of the two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$.

6. $C^{\perp} = \{x \in GF(q)^n : x.y = 0, \forall y \in C\}$ is the definition of the dual code $C^{\perp}$ of C. C is referred to as self-orthogonal if $C \subset C^{\perp}$ and self-dual if $C = C^{\perp}$. Binary code is a linear code over $GF(2)$.

Definition 2.1. [13] A, $k \times n$ matrix whose rows form a basis of a linear $[n, k]$ −code is called a generator matrix of the code. $G = [I_k : A]$ is called the standard form generator matrix.

Definition 2.2. [13] A parity-check matrix H for an $[n, k]$ −code C is a generator matrix of $C^{\perp}$. If $G = [I_k : A]$ is the standard form generator matrix of an $[n, k]$ −code C, then a parity-check matrix for C is $H = [-A^T : I_{n-k}]$.

Polynomial Sets and Algebraic Properties

In this section, we will define a new polynomial set and study some of its algebraic properties. Firstly, we construct some polynomial sets. Throughout this paper,

$$GF(2)[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_i \in GF(2) = \{0,1\}\}$$

is the set of polynomials with coefficients in the field $GF(2)$ and indeterminate x.

Definition 3.1. $f_{rn} = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_i \in GF(2)\}$ is a polynomial set with degree equal to or less than n, and the recursive definition of these polynomials is as follows:

$$f_{0n} = \{0, x^n + x^{n-1} + \cdots + x + 1\}$$

$$f_{rn} = (x^n + f_{(r-1)(n-1)}) \cup f_{(r-1)(n-1)}$$

Example 3.2. A polynomial set f_{rn} is a set involving sets of polynomials.

$$f_{00} = \{0, 1\}$$

$$f_{01} = \{0, x + 1\}$$

$$f_{02} = \{0, x^2 + x + 1\}$$

$$f_{11} = (x + f_{00}) \cup f_{00} = \{0, 1, x, 1 + x\} = GF(2)^1[x]$$

$$f_{22} = (x^2 + f_{11}) \cup f_{11} = \{0, 1, x, 1 + x, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\} = GF(2)^2[x]$$

$$f_{nn} = (x^n + f_{(n-1)(n-1)}) \cup f_{(n-1)(n-1)} = GF(2)^n[x]$$

$$f_{12} = (x^2 + f_{01}) \cup f_{01} = \{0, 1 + x, x^2, x^2 + x + 1\}$$

$$f_{rn} = (x^n + f_{(r-1)(n-1)}) \cup f_{(r-1)(n-1)}$$

Here, f_{22} is a polynomial set with degree equal to or less than 2. Moreover, logical representations of the polynomial sets are provided in Table 1.

Table 1. Logical representations of the polynomial sets

	f_{00}	f_{01}	f_{02}	f_{11}	f_{12}	f_{22}
$\mathbf{0}$	1	1	1	1	1	1
$\mathbf{1}$	1	0	0	1	0	1
$\boldsymbol{x}$	0	0	0	1	0	1
$\mathbf{1+x}$	0	1	0	1	1	1
$\boldsymbol{x^2}$	0	0	0	0	1	1
$\mathbf{1+x^2}$	0	0	0	0	0	1
$\boldsymbol{x+x^2}$	0	0	0	0	0	1
$\mathbf{1+x+x^2}$	0	0	1	0	1	1

Proposition 3.3. $f_{rn} = (x^n + f_{(r-1)(n-1)}) \cup f_{(r-1)(n-1)}$ is a $r + 1$ dimensional vector space over field $GF(2)$ and has $2r + 1$ elements.

Proof. We use induction on r for the proof of the proposition. Since f_{1n} is a set

$$f_{1n} = (x^n + f_{0(n-1)}) \cup f_{0(n-1)}) = \{0, x^{n-1} + \cdots + x + 1, x^n, x^n + x^{n-1} + \cdots + x + 1\}$$

and $\{x^n, x^{n-1} + \cdots + x + 1\}$ is a bases for f_{1n}, it is a two dimensional vector space over $GF(2)$. Suppose that $f_{(r-1)(n-1)}$ is a vector space over $GF(2)$. Since $f_{rn} = (x^n + f_{(r-1)(n-1)}) \cup f_{(r-1)(n-1)}$ is a $r + 1$ dimensional and $(x^n + f_{(r-1)(n-1)}) \cap f_{(r-1)(n-1)} = \emptyset$, it is easy to show that $u + v \in f_{rn}$ for all $u, v \in f_{rn}$ and $ru \in f_{rn}$ for all $u \in f_{rn}, r \in GF(2)$. Thus f_{rn} is a vector space on $GF(2)$. The set $\{x^n, x^{n-1}, x^{n-2}, \dots, x^{n-(r-1)}, x^{n-r} + x^{n-(r+1)} + \cdots + x + 1\}$ is a base for f_{rn}. The number of elements of $f_{(r-1)(n-1)}$ is $2r$, so the number of elements of f_{rn} is $2r + 1$ and of dimension is r.

Example 3.4. Using Definition 3.1 and Example 3.2, we obtain $f_{3n} = \{0, x^{n-3} + x^{n-4} + \cdots + x + 1, x^{n-2}, x^{n-2} + x^{n-3} + \cdots + x + 1, x^{n-1}, x^{n-1} + x^{n-3} + \cdots + x + 1, x^{n-1} + x^{n-2}, x^{n-1} + x^{n-2} + \cdots + x + 1, x^n, x^n + x^{n-3} + \cdots + x + 1, x^n + x^{n-2}, x^n + x^{n-2} + \cdots + x + 1, x^n + x^{n-1}, x^n + x^{n-1} + x^{n-3} + \cdots + x + 1, x^n + x^{n-1} + x^{n-2}, x^n + x^{n-1} + \cdots + x + 1\}$. f_{3n} is a vector space over $GF(2)$.The set $\{x^n, x^{n-1}, x^{n-2}, x^{n-3} + x^{n-4} + \cdots + x + 1\}$ is a base for f_{3n}. Therefore, f_{3n} is a vector space of 4 dimensional and 24 elements.

Proposition 3.5. For $r + 1 \leq n$, f_{rn} is a subspace of $f_{(r+1)n}$.

Proof. From Proposition 3.3, we know that f_{rn} is a vector space. The set

$$\{x^n, x^{n-1}, x^{n-2}, \dots, x^{n-(r-1)}, x^{n-r} + x^{n-(r+1)} + \cdots + x + 1\}$$

is a base for the vector space f_{rn} and

$\{x^n, x^{n-1}, x^{n-2}, \dots, x^{n-(r-1)}, x^{n-r}, x^{n-(r+1)} + x^{n-(r+2)} + \cdots + x + 1\}$

is a base for vector space $f_{(r+1)n}$. The base of f_{rn} is a subset of the base of $f_{(r+1)n}$. Thus, f_{rn} subspace of $f_{(r+1)n}$

Polynomial Sets and Codes

In coding theory, a polynomial code is a type of linear code whose set of valid code words consists of polynomials divisible by a given fixed polynomial. In this section, we construct a new kind of polynomial code. We use polynomial sets f_{rn} for this.

Definition 4.1. Let f_{rn} be a polynomial set and $p(x)$ be a prime polynomial in $GF(2)[x]$ such that $p(x)$ has degree $m = 2n - 1$ and format $p(x) = xm + xs + 1$. Then, recursive definitions of these polynomials, such as;

$$F_{0n} = p(x) f_{0n}$$

$$F_{rn} = p(x) f_{rn}$$

F_{on} and F_{rn} are called generated polynomial sets (GPS) from f_{on} and f_{rn}, respectively. Corresponding to this definition, we formulate a polynomial set

$$F_{rn} = ((x^{n+m} + x^{n+s} + x^n) + f_{(r-1)(n-1)}) \cup f_{(r-1)(n-1)}.$$

GPS F_{rn} has polynomials of degree equal to or less than $n + m$.

Example 4.2. Let $f_{03} = \{0,\ x^3 + x^2 + x + 1\}$. Then, $p(x) = x^7 + x + 1$ is a prime polynomial of degree 23 – 1. Thus, $F_{03} = \{0, x^{10} + x^9 + x^8 + x^7 + x^4 + 1\}$. Moreover, let $f_{23} = \{0, x+1, x^2, x^2 + x + 1, x^3, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + x + 1\}$. Then, $F_{23} = p(x)\{0, x+1, x^2, x^2 + x + 1, x^3, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + x + 1\} = \{0, x^8 + x^7 + x^2 + 1, x^9 + x^3 + x^2, x^9 + x^8 + x^7 + x^3 + 1, x^{10} + x^4 + x^3, x^{10} + x^8 + x^7 + x^4 + x^3 + x^2 + 1, x^{10} + x^9 + x^4 + x^2, x^{10} + x^9 + x^8 + x^7 + x^4 + 1\}$.

Theorem 4.3. For $r \leq n, F_{rn}$ is a linear space of dimension $r + 1$ over $GF(2)$.

Proof. Let $p(x) = x^m + x^s + 1$ be an irreducible polynomial of degree $2n - 1$. Then $F_{0n} = p(x) f_{0n}$ is a linear space over $GF(2)$ and $\{p(x)(x^n + x^{n-1} + \cdots .+1)\}$ is a base of F_{0n}. The polynomial set $F_{rn} = p(x) f_{rn} = (x^{n+m} + x^{n+s} + x^n) + f_{(r-1)(n-1)}) \cup f_{(r-1)(n-1)}$ generated with the set $\{x^{2^n+n-1} + (x^s + 1)x^n, x^{2^n+n-2} + (x^s + 1)x^{n-1}, \ldots, x^{2^n+n-r} + (x^s + 1)x^{n-(r-1)}, x^{2^n+n-(r+1)} + p(x)(x^{n-(r+1)} + \cdots + 1)x^{n-r}(x^s + 1)\}$. It is obviously that the set $\{x^{2^n+n-1} + (x^s + 1)x^n, x^{2^n+n-2} + (x^s + 1)x^{n-1}, \ldots, x^{2^n+n-r} + (x^s + 1)x^{n-(r-1)}, x^{2^n+n-(r+1)} + p(x)(x^{n-(r+1)} + \cdots + 1)x^{n-r}(x^s + 1)\}$ is linear independent and it generate F_{rn}. Thus, for u(x), v(x) ∈ F_{rn}, u(x) + v(x)∈F_{rn}. In that case, F_{rn} is a linear space.

A string of length $n + 1$ can be represented by a polynomial, with the bits representing the coefficients of a polynomial over a field. The basic similarity between codes and polynomials is that codes are an ordered sequence of numbers strung together to mean a single expression. In the case of polynomials, the digits represent the coefficients of each term. The order instead represents the bit's position in the code. We could take the first bit to represent the highest power of x down to the last, meaning the constant term. Or we could consider the first bit to be the constant term and proceed up through the increasing powers of x.

Let $GF(2)^n[x]$ denote the set of all polynomials in $GF(2)[x]$ having a degree equal or less to n. The polynomial $q(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$ of degree at most n over $GF(2)$ may be regarded in general as the word $a_0 a_1 \ldots a_{n-1} a_n$ of length n + 1 in $GF(2)^n$. Of course, each word in $GF(2)^n$ corresponds to a polynomial in $GF(2)^n[x]$ so we define a one-to-one mapping between $GF(2)^n$ and $GF(2)^n[x]$. It is easy to check that this mapping is an isomorphism $GF^n(2) \cong GF^n(2)[x]$ as linear spaces. Now we define codes corresponding to polynomial set F_{rn}.

Definition 4.4. Let F_{rn} be a GPS and C_{rn} be a code set corresponding to the polynomial set F_{rn}. Then C_{rn} is the generated polynomial code (GPC).

Example 4.5. Let $F_{03} = \{0, x^{10} + x^9 + x^8 + x^7 + x^4 + 1\}$ and $F_{23} = p(x)\{0, x+1, x^2, x^2 + x + 1, x^3, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + x + 1\} = \{0, x^8 + x^7 + x^2 + 1, x^9 + x^3 + x^2, x^9 + x^8 + x^7 + x^3 + 1, x^{10} + x^4 + x^3, x^{10} + x^8 + x^7 + x^4 + x^3 + x^2 + 1, x^{10} + x^9 + x^4 + x^2, x^{10} + x^9 + x^8 + x^7 + x^4 + 1\}$ be GPS. Then, the codes GPC obtained from F_{03} and F_{23} are $C_{03} = \{00000000000, 11110010001\}$ and
$C_{23} = \{00000000000,\ 00110000101,\ 01000001100,\ 01110001001,\ 10000011000,\ 10110011101, 11000010100, 11110010001\}$ respectively.

Provide a recursive construction for the C_{rn} generator matrix, denoted by G_{rn}.

Definition 4.6. Let $p(x) = x^m + x^s + 1\ (m = 2n - 1)$ be an irreducible polynomial over $GF(2)[x]$. Then for 0 < r < n,

$$G_{rn} = \begin{pmatrix} x^{2^n+n-1} + (x^s + 1)x^n \\ x^{2^n+n-2} + (x^s + 1)x^{n-1} \\ x^{2^n+n-2} + (x^s + 1)x^{n-1} \\ \vdots \\ x^{2^n+n-r} + (x^s + 1)x^{n-(r-1)} \\ x^{2^n+n-(r+1)} + p(x)\left(x^{n-(r+1)} + \cdots + 1\right) \\ +(x^s + 1)x^{n-r} \end{pmatrix} \qquad (1)$$

is generator matrix of C_{rn}. From 1, we obtain for r = 0, $G_{0n} = (x^{2^n+n-1} + p(x)(x^{n-1} + \cdots + 1) + x^n(x^s + 1))$ and for r = n

$$G_{nn} = \begin{pmatrix} x^{2^n+n-1} + (x^s + 1)x^n \\ x^{2^n+n-2} + (x^s + 1)x^{n-1} \\ \vdots \\ x^{2^n-1} + x^s + 1 \end{pmatrix}$$

Example 4.7. The generator matrix for C_{02}, C_{22}, and C_{12}, are G_{02} = (110001), G_{22} =$\begin{pmatrix}1&0&0&1&1&1\\0&1&0&1&1&1\\0&0&1&0&1&1\end{pmatrix}$ and $G_{12}=\begin{pmatrix}1&0&1&1&0&0\\0&1&1&1&0&1\end{pmatrix}$.

If G_{rn} is form in 4.1, then G_{rn} is in standard form. If G_{rn} is not in standard form, then G_{rn} can be reduced to standard form with elementary operations of rows or columns.

Theorem 4.8. The binary C_{rn} code has a length of 2^n+n and a dimension of $r\ +\ 1$.
Proof. From the definition of F_{rn}, the largest degree polynomial in F_{rn} is 2^n-1+n. The length of the code words corresponding to this polynomial is 2^n+n. From the definition of generator matrix, G_{rn} has $r\ +\ 1$ rows and 2^n+n columns. Rows of G_{rn} are a base for code C_{rn}. So, the dimension of C_{rn} is $r\ +\ 1$.

Theorem 4.9. $C_{(r-1)n}$ is contained in C_{rn}.
Proof. For $r\ =\ 1$ and $r\ =\ 2$, the generator matrix are

$$G_{1n}=\begin{pmatrix}x^{2^n+n-1}+(x^s+1)x^n\\x^{2^n+n-2}+p(x)(x^{n-2}+\cdots+1)x^{n-1}(x^s+1)\end{pmatrix}$$

and

$$G_{2n}=\begin{pmatrix}x^{2^n+n-1}+(x^s+1)x^n\\x^{2^n+n-2}+(x^s+1)x^{n-1}\\x^{2^n+n-3}+(x^s+1)x^{n-2}\\x^{2^n+n-4}+p(x)(x^{n-3}+\cdots+1)x^{n-2}(x^s+1)\end{pmatrix}$$

Since G_{1n} is a submatrix of G_{2n}, we obviously have C_{1n} is contained in C_{2n}. In general, since $G_{(r-1)n}$ is a submatrix of G_{rn}, it follows that C_{rn} is a subcode of C_{2n}. In Table 2, we obtain some results for r and n.

Table 2. C_{rn} codes for r ∈ {1, 2, 3, 4, 5, 6} and n ∈ {2, 3, 4, 5, 6}

Code	2^n+n=Length	d= distance	$r+1=$ dimension	p(x)=irreducible polynomial
C_{12}	6	3	2	x^3+x+1
C_{22}	6	3	3	x^3+x+1
C_{13}	11	6	2	x^7+x+1
C_{23}	11	4	4	x^7+x+1
C_{33}	11	4	4	x^7+x+1
C_{14}	20	7	2	$x^{15}+x+1$
C_{24}	20	4	3	$x^{15}+x+1$
C_{34}	20	4	4	$x^{15}+x+1$
C_{44}	20	4	5	$x^{15}+x+1$
C_{15}	37	12	2	$x^{31}+x^3+1$
C_{25}	37	6	3	$x^{31}+x^3+1$
C_{35}	37	6	4	$x^{31}+x^3+1$
C_{45}	37	4	5	$x^{31}+x^3+1$
C_{55}	37	4	6	$x^{31}+x^3+1$
C_{16}	70	9	2	$x^{63}+x+1$
C_{26}	70	4	3	$x^{63}+x+1$
C_{36}	70	4	4	$x^{63}+x+1$
C_{46}	70	4	5	$x^{63}+x+1$
C_{56}	70	4	6	$x^{63}+x+1$
C_{66}	70	4	7	$x^{63}+x+1$

We construct a parity-check matrix using the generator matrix G_{rn} for code C_{rn}. The generator matrix given in (4.1) is in a standard form. From Definition 2.2 parity-check matrix is

$$H_{rn}=\begin{pmatrix}0\quad(x^s\ +\ 1)x^n\\0\quad(x^s\ +\ 1)x^{n-1}\\\vdots\quad\vdots\\0\quad(x^s\ +\ 1)x^{n-(r-1)}\\p(x)(x^{n-(r+1)}+\cdots+1)+x^{n-r}(x^s\ +\ 1)\\I_{2^n+n-(r+1)}\end{pmatrix}$$

If a parity-check matrix in standard form specifies a code H_{rn} =$\begin{pmatrix}B\\I_{2^n+n-(r+1)}\end{pmatrix}$ or H_{rn} =$(B:\quad I_{2^n+n-(r+1)})$, then a generator matrix for the code is G_{rn} = $[I_{r+1}:\quad -B^T]$. Many codes are most easily defined by specifying a party-heck matrix or a set of parity-check equations equivalently. If a code is given by a party-check matrix H_{rn}, which is not in standard form, then H_{rn} can be reduced to standard form, like for a generator matrix.

Example 4.10. Generator matrix in the standard form of the code C_{23} is

$$G_{23}=\begin{pmatrix}1&0&0&0&1&1&0&1&1&0&0&0\\0&1&0&0&0&1&1&0&1&1&0&0\\0&0&1&1&0&0&1&0&1&1&0&1\end{pmatrix}$$

We obtain a parity-check matrix of C_{23} from the generator matrix G_{23}. Thus,

$$H_{23}=\begin{pmatrix}0&1&1&0&1&1&0&0&0\\0&0&1&1&0&1&1&0&0\\1&0&0&1&0&1&1&0&1\\1&0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\end{pmatrix}$$

Moreover, H_{23} is a generator matrix of the dual code ${C_{23}}^{\perp}$.

Conclusion and Suggestions

In this paper, we defined a polynomial set f_{rn} with recursive formulae over $GF(2)$. f_{rn} has polynomials with degree equal to or less than n. We encode elements of f_{rn} using a $p(x)$ irreducible polynomial with the format $x^{2^n-1}+x^s+1$. We obtained a new polynomial set $F_{rn}=p(x)f_{rn}$. C_{rn} is a code corresponding to F_{rn}. We give coding and decoding algorithms for the code C_{rn}. This study focused on a polynomial set, polynomial code, a generator matrix, and a parity-check matrix of C_{rn}. To extend this study, one could study the same topic on finite fields $GF(q)$.

Conflict of interest

There are no conflicts of interest in this work.

Acknowledgments

We would like to thank the referees for their helpful comments and valuable suggestions.

References

[1] Cadilhac M., Mazowiecki F., Paperman C., Pilipczuk M., S´enizergues G., On Polynomial Recursive Sequences, Theory of Computing Systems, (68) (2024) 593–614.

[2] Fu S., Fenga X., Linc D., Wangd Q., A Recursive Construction of Permutation Polynomials over F_(q^2) with OddCharacteristic from R´edei Functions, Designs, Codes and Cryptography, 87 (2019) 1481–1498.

[3] Sidki S., Sadaka R., Benazzouz A., Computing recursive orthogonal polynomial with Schur complements, Journal of Computational and Applied Mathematics, 373 (2020) 112406.

[4] Shannon C., A Mathematical Theory of Communication, The Bell System Technical Journal, 27 (1948) 379–423, 623–656.

[5] Dinga C., Ling S., Aq-polynomial approach to cyclic codes, Finite Fields and Their Applications, 20 (2013) 1-14.

[6] R. Abdullaev, D. Efanov, Polynomial Codes Properties Application in Concurrent Error-Detection Systems of Combinational Logic Devices, IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia, 2021.

[7] Mao-Ching Chiu, Polynomial Representations of Polar Codes and Decoding under Overcomplete Representations, IEEE Communications Letters, 17 (12) (2013) 2340-2343.

[8] Wang X., Hao Y., Qiao D., Constructions of Polynomial Codes Based on Circular Permutation Over Finite Fields, IEEE, 8 (2020) 134219 - 134223.

[9] Nalli A. and Haukkanen P., On generalized Fibonacci and Lucas polynomials, Chaos Solitons And Fractals, 42 (2009) 3179-3186.

[10] Prasad B., Coding theory on (h(x), g(y))-extension of Fibonacci p-numbers polynomials, Universal Journal of Computational Mathematics, 2 (1) (2014) 6-10.

[11] Stakhov A. P., Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, Chaos Solitons and Fractals, 30 (1) (2006) 56-66.

[12] Kaymak O. O., Coding theory for h(x)-Fibonacci polynomials, J. BAUN Inst. Sci. Technol., 26 (1) (2024) 226-236

[13] Hill R., A First Course in Coding Theory. Oxford: Clarendon Press, (1986) 1-67.

[14] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes. New York: North-holland Publishing company, (1977) 1-37, 188-215.

[15] Ling S., Xing C., Coding Theory A First Course. Cambridge University Press, (2004) 39-57.

[16] Hoffman D. G., Leonard D. A., Lindner C. C., Phelps K. T., Rodger C. A., Wall J. R., Coding Theory, Marcel Dekker Inc., New York, (1991)29-117.Alam M. N., Bonyah E., Fayz-Al-Asad M., Reliable analysis for the Drinfeld-Sokolov-Wilson equation in mathematical physics, *Palest. J. Math.,* 11 (1) (2022) 397-407.