Conditional Recurrences and 2-Quasi-Cyclic Codes

Emre Güday[1] and Murat Sahin[2]

Bilecik Seyh Edebali University[1]
Ankara University[2]

8th Workshop on Design Theory, Hadamard Matrices and Applications (Hadamard 2025)
May 26-30, 2025

Outline

- **Purpose:** Construction of linear codes with desirable properties.
- **Method:**
  * Conditional linear recurrence relation
  * Some facts about the cyclic codes
- **Result:** 2-quasi-cyclic codes
  * 1-weight, and 2-weight codes,
  * Projective codes,
  * Almost Maximum Distance Seperable (AMDS) codes.

Isomorphism Between $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/\langle x^n - 1\rangle$

$\mathbb{F}_q^n$	$\cong$	$\mathbb{F}_q[x]/\langle x^n - 1\rangle =: \mathcal{R}$
$(c_0, c_1, \ldots, c_{n-1})$		$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$
$\mathbf{C} \subset \mathbb{F}_q^n$ code		$\mathbf{C} \subset \mathcal{R}$
$\mathbf{C} \leq \mathbb{F}_q^n$ linear code		$\mathbf{C} \leq \mathcal{R}$
Cyclic Codes		Ideals

Some Basic Definitions

- A linear code is called **quasi-cyclic** if there is some integer l such that every cyclic shift of a codeword by l places is again a codeword. A **cyclic code** is a quasi-cyclic code with $l = 1$.
- The number of nonzero components of $\mathbf{x} \in \mathbb{F}_q^n$ is called the **weight** of $\mathbf{x}$ and is denoted by $w(\mathbf{x})$.
- Let A_i denote the **number of codewords** (or frequency) with Hamming weight i in a code $\mathbf{C}$ of length n.
- The set $\{(0,1),\ (1,A_1),\ldots,(n,A_n)\}$ is called the **weight distribution** of the code $\mathbf{C}$.
- A code $\mathbf{C}$ is called t-**weight** if it has exactly t non-zero weights.

The Conditional Linear Recurrence Relation

Definition 1

Let $\mathbb{F}_q$ be a finite field, and let $a_{0,1}, a_{0,2}, a_{1,1}, a_{1,2}$ be elements of $\mathbb{F}_q$ such that $a_{0,2}a_{1,2} \neq 0$. **The conditional linear recurrence relation** *is defined for all $n \geq 2$ by:*

$$s_n = \begin{cases} a_{0,1}s_{n-1} + a_{0,2}s_{n-2}, & n \equiv 0 \ (mod\ 2), \\ a_{1,1}s_{n-1} + a_{1,2}s_{n-2}, & n \equiv 1 \ (mod\ 2). \end{cases} \tag{1}$$

A sequence $\{s_n\}_{n=0}^{\infty}$ that satisfy relation (1) is called **a conditional sequence**. *The pair (s_0, s_1) is referred as the* **initial values** *of the sequence.*

Lemma 1 (Panario et al., [5])

Let $\{s_n\}_{n=0}^{\infty}$ be a conditional sequence satisfying the relation (1). The sequence $\{s_n\}_{n=0}^{\infty}$ satisfies the linear recurrence relation,

$$s_{n+4} = (a_{0,1}a_{1,1} + a_{0,2} + a_{1,2})s_{n+2} - a_{0,2}a_{1,2}s_n. \tag{2}$$

The Main Problem

- It is known that the **linear recurrence relations** over any finite field generate the **cyclic codes** which is an important family of linear codes.

Problem 1

Construction of codes *which have* **good properties** *by using CLRR.*

Notation

- $\mathcal{S}$: The set of all conditional sequences satisfying the relation (1)
- $\mathcal{L}$: The set of all linear recurring sequences satisfying the relation (2)
- $A := a_{0,1}a_{1,1} + a_{0,2} + a_{1,2}$, $B := -a_{0,2}a_{1,2}$
- $f_{(2)}(x)$: The characteristic polynomial of $s_{n+2} = As_{n+1} + Bs_n$
- $\mathbf{C}^{(2)}$: 2-dimensional cyclic code corresponding to $f_{(2)}(x)$
- $f_{(4)}(x)$: The characteristic polynomial of $s_{n+4} = As_{n+2} + Bs_n$
- $\mathbf{C}^{(4)}$: 4-dimensional cyclic code corresponding to $f_{(4)}(x)$

A Link Between the Codes $\mathbf{C}^{(2)}$ and $\mathbf{C}^{(4)}$

Lemma 2 (Güday and Sahin, [3])

If $ord(f) = N$, then the code $\mathbf{C}^{(4)}$ is a $[2N, 4]$ code over $\mathbb{F}_q$.

Lemma 3 (Güday and Sahin, [3])

The code $\mathbf{C}^{(4)}$ is permutation equivalent to $\left(\mathbf{C}^{(2)}\right)^2$.

- We can construct a subcode of $\mathbf{C}^{(4)}$ using the conditional recurrences.
- This code is permutation equivalent to a subcode of the code $\left(\mathbf{C}^{(2)}\right)^2$.

Some Properties of the Conditional Sequences

Lemma 4

The set $\mathcal{S}$ is a 2-dimensional subspace of $\mathcal{L}$ over $\mathbb{F}_q$.

Result 1

Let $\{s_n\}_{n=0}^{\infty}$ be an arbitrary conditional sequence that satisfies relation (1). Then the sequence is periodic.

The Code Construction

Let $f(x) = f_{(2)}(x) = x^2 - Ax - B \in \mathbb{F}_q[x]$ be a polynomial, where $A = a_{0,1}a_{1,1} + a_{0,2} + a_{1,2}$, and $B = -a_{0,2}a_{1,2}$. The code $\mathbf{C}_f$, using the conditional recurrence relation (1), is defined by

$$\mathbf{C}_f = \left\{ (s_n)_{n=0}^{2N-1} : \ s_n = \sum_{j=1}^{2} a_{i,j} s_{n-j}, \ n \equiv i \ (mod\ 2), \ (s_0, s_1) \in \mathbb{F}_q^2 \right\}, \qquad (3)$$

where $N = ord(f)$.

- $\mathbf{C}_f$ is a $[2N, 2]$ code over $\mathbb{F}_q$.
- $\mathbf{C}_f$ is 2-quasi-cyclic code.

The Weight Distribution of $\mathbf{C}^{(4)}$

Theorem 1 (Güday and Sahin, [3])

Let the weight distribution of the code $\mathbf{C}^{(2)}$

a) *be* $\left\{(0,\ 1),\ (w_1 = N - \frac{N}{e},\ B_1),\ (w_2 = N,\ B_2)\right\}$.

i) *If* $e = 2$, *then* $\mathbf{C}^{(4)}$ *is a* 4*-weight code,*

ii) *If* $e > 2$, *then* $\mathbf{C}^{(4)}$ *is a* 5*-weight code.*

b) *be* $\left\{(0,\ 1),\ (w_1 = N - \frac{N}{p},\ B_1),\ (w_2 = N,\ B_2)\right\}$.

i) *If* $p = 2$, *then* $\mathbf{C}^{(4)}$ *is a* 4*-weight code,*

ii) *If* $p > 2$, *then* $\mathbf{C}^{(4)}$ *is a* 5*-weight code.*

The weight distribution of $\mathbf{C}^{(4)}$ *is given in Table 1.*

Table 1: The Weight Distribution of $\mathbf{C}^{(4)}$

For $e = 2$ (or $p = 2$)		For $e > 2$ (or $p > 2$)	
Weight	**Frequency**	**Weight**	**Frequency**
0	1	0	1
w_1	$2B_1$	w_1	$2B_1$
$2w_1$	$B_1^2 + 2B_2$	w_2	$2B_2$
$3w_1$	$2B_1B_2$	$2w_1$	B_1^2
$4w_1$	B_2^2	$w_1 + w_2$	$2B_1B_2$
		$2w_2$	B_2^2

The Weight Distribution of $\mathbf{C}^{(4)}$

Theorem 2 (Güday and Sahin, [3])

If $\mathbf{C}^{(2)}$ is a 1-weight code with nonzero weight $\{w_1 = N - \frac{N}{e}\}$, then the code $\mathbf{C}^{(2r)}$ is an r-weight code with nonzero weights $\{w_1, 2w_1, \ldots, rw_1\}$ and respective frequencies $\{r(q^2-1), \binom{r}{2}(q^2-1)^2, \ldots, (q^2-1)^r\}$.

Result 2

If $\mathbf{C}^{(2)}$ is a 1-weight code with nonzero weight $\{w_1 = N - \frac{N}{e}\}$, then $\mathbf{C}^{(4)}$ is a 2-weight code with nonzero weights $\{w_1, 2w_1\}$ and respective frequencies $\{2(q^2-1), (q^2-1)^2\}$.

Properties of the Conditional Sequences

Lemma 5

Let $a_{0,1}a_{1,1} \neq 0$. If $s_n = 0$ and $s_{n+1} \neq 0$, then $s_{n+2} \neq 0$ for all $n \in \mathbb{N}$.

Proof

Let $s_n = 0$ and $s_{n+1} \neq 0$ for some $n \in \mathbb{N}$. By the definition of relation (1),

$$\begin{aligned} s_{n+2} &= a_{i,1}s_{n+1} + a_{i,2}s_n \\ &= a_{i,1}s_{n+1} \end{aligned}$$

which is nonzero, since $a_{i,1} \neq 0$.

Properties of the Conditional Sequences

Lemma 6

Let $a_{0,1}a_{1,1} \neq 0$. The pairs (s_0, s_2) and (s_1, s_3) run the set $\mathbb{F}_q^2$ when (s_0, s_1) runs $\mathbb{F}_q^2$.

Proof

By definition, we can write $s_2 = a_{0,1}s_1 + a_{0,2}s_0$ and $s_3 = a_{1,1}s_2 + a_{1,2}s_1$. Since $a_{0,1}, a_{0,2}, a_{1,1}$, and $a_{1,2}$ are nonzero, the desired result is obtained.

On the Minimum Distance of the Code $\mathbf{C}_f$

Theorem 3

Let $d(\mathbf{C}^{(2)}) = w_1$. If $a_{0,1}a_{1,1} \neq 0$, then $d(\mathbf{C}_f) = 2w_1$, or $w_1 + w_2$.

Proof

Suppose that $\mathbf{C}^{(2)}$ is a two-weight code with nonzero weights $\{w_1, w_2\}$. By Lemma 3, all possible weights of the code $\mathbf{C}^{(4)}$ is of the form

i) $0 + w_1$
ii) $0 + w_2$
iii) $w_1 + w_1$
iv) $w_1 + w_2$
v) $w_2 + w_2$

By Lemma 5, parts (i) and (ii) can not be happened. Therefore, the minimum distance can be at least $2w_1$. On the other hand, since there exist codewords which has the weight w_1 that correspond the initial values $(0, s_1)$ with $s_1 \neq 0$ or $(s_0, 0)$ with $s_0 \neq 0$, part (v) also cannot occur. If $\mathbf{C}^{(2)}$ is a one-weight code, then $d(\mathbf{C}_f) = 2w_1$, clearly.

Projective, AMDS, and 1-Weight Code

Theorem 4

Let the polynomial $f(x) = x^2 - Ax - B = (x - \alpha)(x - \beta)$ *be irreducible over* $\mathbb{F}_q$, *where* $A = a_{0,1}a_{1,1} + a_{0,2} + a_{1,2}$, $B = -a_{0,2}a_{1,2}$. *Let* $e = q + 1$, *where* e *is the multiplicative order of element* $\frac{\beta}{\alpha}$ *in* $\mathbb{F}_{q^2}^*$. *Then the code* $\mathbf{C}_f$ *is a* 1*-weight code with nonzero weight* $\{2(N - \frac{N}{e})\}$. *Furthermore, the code* $\mathbf{C}_f$ *is AMDS and projective if* $e = N = q + 1$.

Proof

Since $f(x)$ *is irreducible over* $\mathbb{F}_q$ *and* $e = q + 1$, $\mathbf{C}^{(2)}$ *is a* 1*-weight code with weight* $w_1 = N - \frac{N}{e}$. *By Result 2,* $\mathbf{C}^{(4)}$ *has nonzero weights* $\{w_1, 2w_1\}$. *On the other hand, it is known from Lemma 5 that the code* $\mathbf{C}_f$ *does not have any codeword with weight* w_1. *Thus* $\mathbf{C}_f$ *is a* 1*-weight code with the nonzero weight* $\{2w_1\}$. *If* $e = N$, *then the code is projective by [6] and the parameters* $[n, k, d]$ *of the code* $\mathbf{C}_f$ *satisfy the bound* $d = n - k$ *which means that the code is AMDS.*

Two-Weight Code

In this case,

$$s_n = \begin{cases} a_{0,2}s_{n-2}, & n \equiv 0 \ (mod\ 2), \\ a_{1,2}s_{n-2}, & n \equiv 1 \ (mod\ 2). \end{cases} \tag{4}$$

$f_{(2)}(x) = (x - a_{0,2})(x - a_{1,2})$, $N = lcm\big(o(a_{0,2}), o(a_{1,2})\big)$.

Theorem 5

Suppose that $a_{0,1} = a_{1,1} = 0$ and $a_{0,2} \neq a_{1,2}$. Then the code $\mathbf{C}_f$ is a 2-weight code with nonzero weights $\{w_2, 2w_2\}$ and respective frequencies $\{2(q-1),\ (q-1)^2\}$. Furthermore, if $e = N$, then the code is projective.

Proof

Since $a_{0,2}, a_{1,2} \in \mathbb{F}_q^*$, $\mathbf{C}^{(2)}$ is 2-weight code. Suppose that $a_{0,2} \neq a_{1,2}$. If $e = N$, then the code is projective by [6].

REFERENCES

[1] Calderbank, R. and Kantor, W., M. The Geometry of Two-Weight Codes. *Bull. London Math. Soc.*, 18, pp.97-122 (1986)

[2] Delsarte, P. Weights of Linear Codes and Strongly Regular Normed Spaces. *Discrete Mathematics*, 3, pp.47-64 (1972)

[3] Güday, E., Sahin, M. Linear Recurring Sequences and Weight Distributions of Some Cyclic Codes. *Applicable Algebra in Engineering, Communication and Computing*, accepted for publication.

[4] Lidl, R. and Niederreiter, H. Finite Fields. Cambridge University Press, New York (1997)

[5] Panario, D., Sahin, M., and Wang, Q. A family of Fibonacci-like conditional sequences. *Integers* 13, (A78) (2013)

[6] Shi, M., Zhang, Z., and Solé, P. Two-Weight Codes and Second Order Recurrences. *Chinese Journal of Electronics*, Vol. 28, No.6, pp. 1127-1130 (2019)

Thank you!