Electronic Journal of
Graph Theory and Applications

Linear codes and cyclic codes over finite rings and their generalizations: a survey

Djoko Suprijanto

Combinatorial Mathematics Research Group,
Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung,
Jalan Ganesa 10 Bandung, Indonesia

Center for Research Collaboration on Graph Theory and Combinatorics, Indonesia

djoko.suprijanto@itb.ac.id

To Edy Tri Baskoro on the occasion of his 57+1 birthday

Abstract

We survey a recent progress of cyclic codes over finite rings and their generalization to skew cyclic as well as skew cyclic codes with derivation over finite rings, focusing on structural properties of the codes. We also report recent developments on the construction methods of linear codes from graphs, in particular strongly regular as well as distance regular graphs.

Keywords: Finite rings, linear codes, cyclic codes, skew polynomial ring, skew cyclic codes, skew cyclic codes with derivation, strongly regular graphs, distance regular graphs
Mathematics Subject Classification: 94B05, 94B15, 05C50, 05C90
DOI: 10.5614/ejgta.2023.11.2.11

1. Introduction

The appearance of noise in communication channels is unavoidable thing in our life. The theory of error-correcting codes emerges as a response to this problem. It is the landmark paper of Shannon [53] on the mathematical theory of communication, which showed the existence of good codes, that marked the beginning of Information Theory and Coding Theory. Unfortunately, the proof given by Shannon is not constructive in the sense that he merely stated the existence of good

Received: 17 August 2022, Revised: 13 September 2023, Accepted: 25 September 2023.

codes, but the construction method to obtain the codes is not given. Constructing good codes over certain alphabets remains one of the main problems in coding theory.

The study of codes has grown into an important subject that intersect various scientific disciplines, including information theory, electrical engineering, computer sciences, and also mathematics for the purpose of designing efficient and reliable methods of data transmission.

Codes over finite rings were introduced by Ian F. Blake in 1970's [8, 9], although long before him, Assmus and Mattson [4] first mention rings as possible alphabets for linear codes. Blake [8] showed a way to construct codes over $\mathbb{Z}_m$ from cyclic codes over $\mathbb{F}_p$, where p is a prime factor of m. He [9] then further observed the structure of codes over $\mathbb{Z}_{p^r}$. Spiegel [57, 58] generalized Blake's results to codes over $\mathbb{Z}_m$, where m is an arbitrary positive integer. Study of codes over finite rings attracted great interest in algebraic coding theory through the work of Hammons, Kumar, Calderbank, Sloane, and Solé [33], where they show how several well-known families of nonlinear binary codes were intimately related to linear codes over $\mathbb{Z}_4$. Since Hammons et al. [33] many people have been considering codes over various finite rings.

In the meantime, the study of cyclic codes over finite fields began earlier with two 1957 and 1958 AFCRL reports by E. Prange [49, 50]. Cyclic codes are an extremely important class of codes from two perspectives: theoretically, cyclic codes are rich mathematical theory, and practically, cyclic codes can be implemented easily in decoding schemes.

Surprisingly, study of linear codes constructed from graphs has begun only several years after Prange [49, 50] introduced the notion of cyclic codes. It was Kasami [41] in 1961 who introduced graph-theoretic codes. Four years later, Hakimi and Frank [32] established a class of optimum cutset codes, namely optimum codes constructed from the so-called a cut-set matrix of a connected undirected graph. Later, Borrow and Franaszczuk [10] showed that the codes constructed by Hakimi and Frank [32] contains an infinite subclass of binary cyclic codes, namely binary Bose-Chaudhuri-Hocquenghem (BCH) codes. The paper of Borrow and Franaszczuk [10] seem to be the first one that considered cyclic codes constructed from graphs.

The purpose of this paper is to provide a short survey on the study of cyclic codes over finite rings and their generalization to the so-called skew cyclic codes as well as skew cyclic codes with derivation over finite rings, from my personal viewpoint. In addition, we also give some progress on linear codes from graphs, in particular from strongly regular and distance regular graphs. While for the cyclic codes we emphasize on the structural properties, for the study of linear codes from graphs we emphasize on the varieties of construction methods of linear codes from graphs. This paper is a slightly expanded version of my talk at the International Conference on Graph Theory and Information Security V 2022 (ICGTIS V 2022) in Bandung, West Java, Indonesia, on May 22-25, 2022, and hosted by Institut Teknologi Bandung, conducted in celebrating Prof. Edy Tri Baskoro's 58th birthday.

The rest of the paper is organized as follows. In Section 2 we consider cyclic codes over the ring B_k, including some history on the development of cyclic codes over finite rings and the characterization of cyclic and quasi cyclic codes over the ring B_k. The characterizations of skew cyclic codes over the ring A_k and B_k are given in Section 3. We also provide algorithms to construct skew cyclic codes over the ring A_k and B_k. Section 4 describes the skew cyclic codes with derivation over certain finite non-chain rings. Some recent progress on construction methods of linear codes over finite fields and finite rings, in particular self-dual codes constructed from graphs, are also reported in Section 5. This survey is ended by some remarks. We follow [34, 45] for undefined terms in coding theory.

2. Cyclic codes over the ring B_k

2.1. Historical remarks

Cyclic codes over finite rings seem to be extensively explored for the first time in the work of Calderbank and Sloane [17], although we can found some early works on it (see, for example, the work of Shankar [52], where he used the Chinese Remainder Theorem to investigate a class of cyclic codes, called BCH codes, over the ring $\mathbb{Z}_m$). In their paper [17], Calderbank and Sloane derived some basic properties regarding the structure of cyclic codes of length n over the ring $\mathbb{Z}_{p^r}$, where p is prime not divisible by n, and r is a positive integer. Unfortunately, as it is stated explicitly by the authors, almost all the main theoretical results in [17] are easily verified by the methods of representation theory or commutative algebra, and the proofs are not given there. Later, Kanwar and López-Permouth [40], reproved some results of Calderbank and Sloane [17] by another, and more elementary approach. Norton and Sălăngean-Mandache [46] extended the structure theorems obtained by [17] and [40] to cyclic codes over finite chain rings. In 2004, Dinh and López-Permouth [24] derived structural properties of cyclic as well as negacyclic codes over finite chain rings in a more general setting. Their approach [24] is different with the one used in [46]. Moreover, the results of [24] are also more detailed compare with [46].

Later, Abualrub and Siap [1] derived structural properties of cyclic codes over the non-chain rings $\mathbb{Z}_2 + u\mathbb{Z}_2$, with $u^2 = 0$, and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, with $u^3 = 0$ (which further investigated by Bandi and Bhaintwal [5] for the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 0$). Recently, in 2014, Cengellenmis, Dertli, and Dougherty [20] investigated linear codes over an infinite family of ring A_k defined as

$$A_k := \mathbb{F}_2[v_1, \ldots, v_k]/\langle v_i^2 - v_i,\ v_iv_j - v_jv_i\rangle_{i,j=1}^k,$$

including structures of cyclic codes over the ring A_k. Four years later, together with Irwansyah, the author [37] investigated linear codes over the infinite family of ring B_k which is a generalization of the ring considered by Cengellenmis, Dertli, and Dougherty above. We generalized the ring A_k into B_k by changing the binary finite field $\mathbb{F}_2$ in the ring A_k by an arbitrary finite field $\mathbb{F}_{p^r}$, with p is a prime number and r is a positive integer.

In the next part, we mention the structural properties of the cyclic codes over B_k. We begin with the basic facts regarding the ring B_k.

2.2. The ring B_k

Let v_i, for $1 \leq i \leq k$, be an indeterminate and $\mathbb{F}_q$ be a finite field of order q. The ring B_k is the ring of the form

$$B_k := \mathbb{F}_{p^r}[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i,\ v_iv_j - v_jv_i\rangle_{i,j=1}^k,$$

for some prime p and a positive integer r. It is a finite non-chain ring as there exist more than one maximal ideals. For example, if $k = 1$, then $B_1 = \mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$, where $v^2 = v$. We also define $B_0 := \mathbb{F}_{p^r}$. The ring B_k forms a commutative algebra over the field $\mathbb{F}_{p^r}$.

For any given positive integer k, let $[k] := \{1, 2, \ldots, k\}$. The ring B_k can be viewed as an $\mathbb{F}_{p^r}$-vector space with dimension 2^k whose basis consists of elements of the form $\prod_{i\in H} w_i$, where $H \in 2^{[k]}$ and $w_i \in \{v_i, 1 - v_i\}$ for $1 \leq i \leq k$ ([36, Lemma 1]). Also, the ring B_k has characteristic p and cardinality $(p^r)^{2^k}$ ([36, Lemma 2]). Moreover, the ring B_k is isomorphic via the Chinese Remainder Theorem to $\mathbb{F}_{p^r}^{2^k}$ ([37, Theorem 4]).

Every element a in B_k can be written as

$$a = \sum_{S\in 2^{[k]}} \alpha_S v_S,$$

for some $\alpha_S \in \mathbb{F}_{p^r}$, where $v_S := \prod_{i\in S} v_i$, and $v_\emptyset := 1$.

2.3. *Cyclic codes over B_k*

Let R be a finite commutative ring. A nonempty set C is called a *code* of length n over R if $C \subseteq R^n$. If C is a submodule of R^n, we call C is a *linear code.* Let $f(x) \in R[x]$. The following correspondence will help us to convert the combinatorial structure of cyclic codes into an algebraic one:

$$\pi : R^n \ni (c_0, c_1, \ldots, c_{n-1}) \longmapsto c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in R[x]/\langle f(x)\rangle.$$

Definition 1. *A linear code $C \subseteq R^n$ is called* polycyclic *over R if $\pi(C)$ is an ideal in $R[x]/\langle f(x)\rangle$.*

(1) *If $f(x) = x^n - 1$, then C is called a* cyclic codes.

(2) *If $f(x) = x^n + 1$, then C is called a* negacyclic code.

(3) *If $f(x) = x^n + \lambda$, λ a unit in R, then C is called a* constacyclic code.

Define a *λ-constacyclic shift operator* T_λ on R^n as follows:

$$T_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

Then, the definition above is equivalent to (all codes below are linear):

$(1)'$ C is a *cyclic code* if $T_1(C) = T(C) = C$.

$(2)'$ C is a *negacyclic code* if $T_{-1}(C) = C$.

$(3)'$ C is a *λ-constacyclic code* if $T_\lambda(C) = C$.

C is called a *quasi-cyclic of index l* if $T^l(C) = C$, for some positive integer l.

Recall the Gray map φ defined on B_k :

$$\begin{array}{rccl} \varphi : & B_k & \longrightarrow & \mathbb{F}_{p^r}^{2^k}, \\ & a = \sum_{i=1}^{2^k} \alpha_{S_i} v_{S_i} & \longmapsto & (\sum_{S\subseteq S_1} \alpha_S, \sum_{S\subseteq S_2} \alpha_S, \ldots, \sum_{S\subseteq S_{2^k}} \alpha_S). \end{array}$$

The map φ is bijective. Furthermore, this map can be extended into n tuples of B_k naturally:

$$\begin{array}{rccl} \overline{\varphi} : & B_k^n & \longrightarrow & \mathbb{F}_{p^r}^{n2^k}, \\ & (a_1, a_2, \ldots, a_n) & \longmapsto & (\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)). \end{array}$$

We obtain a characterization of cyclic as well as quasi-cyclic codes over B_k. First, the theorem below characterize quasi-cyclic codes over B_k.

Theorem 2.1 ([37, Theorem 32])**.** *A code C with length n is* quasi-cyclic *of index l over B_k if and only if $C = \overline{\varphi}^{-1}(C_1, C_2, \ldots, C_{2^k})$ and each code C_i with length n is quasi-cyclic of length l over $\mathbb{F}_{p^r}$, for $1 \leq i \leq 2^k$.*

Since cyclic codes are just the quasi-cyclic codes of index $l = 1$, by Theorem 2.1, we have the following consequence which is a characterization of cyclic codes over B_k.

Theorem 2.2 ([37, Theorem 33])**.** *A code C is a* cyclic code *of length n over B_k if and only if $C = \overline{\varphi}^{-1}(C_1, C_2, \ldots, C_{2^k})$ and C_i is a cyclic code of length n over $\mathbb{F}_{p^r}$, for all $1 \leq i \leq 2^k$.*

In terms of polynomial generators, we have the following properties.

Corollary 2.1 ([37, Corollary 34])**.** *Let $C = \overline{\varphi}^{-1}(C_1, C_2, \ldots, C_{2^k})$ be a quasi-cyclic code over B_k, where $C_1, C_2, \ldots, C_{2^k}$ are quasi-cyclic codes over $\mathbb{F}_{p^r}$. If $C_i = \langle g_{1_i}(x), \ldots, g_{m_i}(x)\rangle$, for all $i = 1, \ldots, 2^k$, then*

$$C = \big\langle v_{S_1} g_{1_1}(x), \ldots, v_{S_{2^k}} g_{1_1}(x), \ldots, v_{S_1} g_{m_1}(x), \ldots, v_{S_{2^k}} g_{m_1}(x), \\ \ldots, v_{S_1} g_{m_s}(x), \ldots, v_{S_{2^k}} g_{m_s}(x)\big\rangle .$$

Again, the following corollary follows from Corollary 2.1.

Corollary 2.2 ([37, Corollary 35])**.** *Let $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$ be a cyclic code over B_k, where $C_1, \ldots, C_{2^k}$ are cyclic codes over $\mathbb{F}_{p^r}$. If $C_i = \langle g_i(x)\rangle$, for all $i = 1, \ldots, 2^k$, then*

$$C = \big\langle v_{S_1} g_1(x), \ldots, v_{S_{2^k}} g_1(x), \ldots, v_{S_1} g_{2^k}(x), \ldots, v_{S_{2^k}} g_{2^k}(x)\big\rangle .$$

3. Skew cyclic codes over the rings A_k and B_k

Now, we consider skew cyclic codes as a ”one-step” generalization of the notion of cyclic codes. We begin with some basic facts regarding the so-called skew-polynomial rings.

Let θ be an automorphism of $\mathbb{F}_{p^r}$. Consider the set

$$\mathbb{F}_{p^r}[x;\theta] := \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \,:\, a_i \in \mathbb{F}_{p^r}\}$$

of formal polynomials where coefficients are written on the left of the variable x.

$\mathbb{F}_{p^r}[x;\theta]$ forms a ring under the usual addition of polynomials and the multiplication is defined by the basic rule

$$xa := \theta(a)x.$$

The multiplication is extended to all elements in $\mathbb{F}_{p^r}[x;\theta]$ by associativity and distributivity. $\mathbb{F}_{p^r}[x;\theta]$ is called a *skew polynomial ring* over $\mathbb{F}_{p^r}$, and each element in $\mathbb{F}_{p^r}[x;\theta]$ is called a *skew polynomial*. This family of polynomial ring has been introduced at almost a century ago by Ore [43]. It is easy to check that $\mathbb{F}_{p^r}[x;\theta]$ is *non-commutative* unless θ is identity automorphism of $\mathbb{F}_{p^r}$.

Given an automorphism θ of $\mathbb{F}_{p^r}$ and a unit $\lambda \in \mathbb{F}_{p^r}$, a code C is said to be a *skew θ-λ-constacyclic* of length n if it is closed under the *θ-λ-constacyclic shift* $T_{\theta,\lambda} : \mathbb{F}_{p^r} \longrightarrow \mathbb{F}_{p^r}$ defined by

$$T_{\theta,\lambda}(v_0, v_1, \ldots, v_{n-1}) = (\theta(\lambda v_{n-1}), \theta(v_0), \ldots, \theta(v_{n-2})).$$

In particular, when $\lambda = 1$ or $\lambda = -1$, such codes are called *skew cyclic* and *skew negacyclic codes*, respectively.

The concept of *skew-cyclic codes* which is also called *θ-cyclic codes* over finite fields was introduced by Boucher, Geiselmann, and Ulmer in 2007 [11]. It is well known that each cyclic code corresponds to a divisor of $x^n - 1$. Similarly, each skew-cyclic code corresponds to a right divisor of $x^n - 1$. Since skew-polynomials do not necessarily have unique irreducible factorizations, a polynomial $x^n - 1$ may have a considerable number of right divisors. It leads to many skew cyclic codes, which imply a better opportunity to obtain codes with good parameters. It is a motivation of [11] to introduced the notion of skew cyclic codes. In 2008 and 2009, Boucher, Solé, and Ulmer [12] as well as Boucher and Ulmer [13, 14] further investigated skew cyclic codes over finite rings. Recently, together with his colleagues, the author investigated skew-cyclic codes over the ring A_k and B_k, in [35] and [36], respectively.

3.1. Skew cyclic codes over the ring A_k

3.1.1. Basic facts on codes over A_k

Since A_k is a special case of B_k, then any element of A_k can be described by exactly the same way with the element of B_k. For $A, B \subseteq [k]$ we have that $v_A v_B = v_{A\cup B}$ which gives that

$$\sum_{B\in 2^{[k]}} \alpha_B v_B \cdot \sum_{C\in 2^{[k]}} \beta_C v_C = \sum_{D\in 2^{[k]}} \left(\sum_{B\cup C = D} \alpha_B \beta_C \right) v_D.$$

It is shown in [20] that the only unit in the ring A_k is 1. It is also shown that the ideal $\langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{v_i, 1 + v_i\}$, is a maximal ideal of cardinality $2^{2^k - 1}$. Note that this gives 2^k maximal ideals. Hence, except for the case when $k = 0$, namely the finite field of order 2, the ring is not a local ring.

The ring A_k is a principal ideal ring. In particular, let $I = \langle \alpha_1, \alpha_2, \ldots, \alpha_s \rangle$ be an ideal in A_k, then I is a principal ideal generated by the element which is the sum of all non-empty products of the α_i, that is

$$I = \left\langle \sum_{\substack{A\subseteq [s],\\ A\neq\emptyset}} \prod_{i\in A} \alpha_i \right\rangle.$$

We shall define a set of automorphisms in the ring A_k based on the set S. Define the map Θ_i by

$$\Theta_i(v_j) := \begin{cases} v_i + 1, & i = j, \\ v_j, & i \neq j. \end{cases}$$

For $S \subseteq [k]$, the automorphism Θ_S is defined by:

$$\Theta_S := \prod_{i\in S} \Theta_i.$$

Note that Θ_S is an involution on the ring A_k. We shall use this involution to define Θ_S-cyclic codes.

Gray maps were defined on all commutative rings of order 4 (see [25] for a description of these four Gray maps). For the ring $A_1 = \mathbb{F}_2 + v\mathbb{F}_2$, we have the Gray map $\phi_1 : A_1 \to \mathbb{F}_2^2$ defined by $\phi(a + bv_1) = (a, a + b)$. For A_1 this is realized as

$$\begin{aligned} 0 &\longmapsto 00 \\ 1 &\longmapsto 11 \\ v &\longmapsto 01 \\ 1+v &\longmapsto 10. \end{aligned}$$

We extend this map inductively as follows. Every element in the ring A_k can be written as $\alpha + \beta v_k$, where $\alpha, \beta \in A_{k-1}$. Then for $k \geq 2$, define $\phi_k : A_k \to A_{k-1}^2$ by

$$\phi_k(\alpha + \beta v_k) = (\alpha, \alpha + \beta).$$

Then define a Gray map $\Phi_k : A_k \to \mathbb{F}_2^{2^k}$ by $\Phi_1(\gamma) = \phi_1(\gamma)$, $\Phi_2(\gamma) = \phi_1(\phi_2(\gamma))$ and

$$\Phi_k(\gamma) = \phi_1(\phi_2(\ldots(\phi_{k-2}(\phi_{k-1}(\phi_k(\gamma))\ldots).$$

It follows immediately that $\Phi_k(1) = \mathbf{1}$, the all-one vector. We note that the Gray map Φ_k is a bijection and is a linear map.

We can also define another map which will be used later for constructing generators for Θ_S-cyclic codes. Let $p, k \in \mathbb{N}$, where $p < k$. Let $\Omega_p = \{p+1, p+2, \ldots, k\}$ and $s = 2^{k-p}$. We have that $|2^{(\Omega_p)}| = s$. We can define a Gray map as follows:

$$\Psi_{k,p} : A_k \to A_p^s.$$

Denote the coordinates of A_p^s by the lexicographic ordering of the subsets of Ω_p and denote them by $B_1, B_2 \ldots, B_s$. Note that $B_1 = \emptyset$ and $B_s = \Omega_p$. An element of A_k can be written as $\sum_{B \subseteq \Omega_p} \alpha_B w_B$, where $\alpha_B \in A_p$ and $w_B = \prod_{i \in B} v_i$. Then we have

$$\Psi_{k,p}\left(\sum_{B \subseteq \Omega_p} \alpha_B w_B\right) = \left(\sum_{D \subseteq B_1} \alpha_D, \sum_{D \subseteq B_2} \alpha_D, \ldots, \sum_{D \subseteq B_s} \alpha_D\right).$$

For $p = 0$, $\Psi_{k,0}$ is the same map as Ψ_k [20]. In that paper, it is shown that Ψ_k and Φ_k are conjugate, in the sense that their images are permutation equivalent.

Notice that the representation of an element in A_k can be changed by replacing any v_i with $1 + v_i$. In that way, we can let u_i be either v_i or $v_i + 1$ for each i. Then we have an alternative definition of $\Psi_{k,p}$ as

$$\overline{\Psi}_{k,p}\left(\sum_{B \subseteq \Omega_p} \alpha_B y_B\right) = \left(\sum_{D \subseteq B_1} \alpha_D, \sum_{D \subseteq B_2} \alpha_D, \ldots, \sum_{D \subseteq B_s} \alpha_D\right)$$

where $y_B = \prod_{i\in B} u_i$. Any result for $\Psi_{k,p}$ can be replaced for $\overline{\Psi}_{k,p}$.

Let T be the matrix that performs the cyclic shift on a vector. That is $T(v_1, v_2, \ldots, v_n) = (v_n, v_1, \ldots, v_{n-1})$. Let $\sigma_{i,k}$ be the permutation on $\{1, 2, \ldots, 2^k\}$ defined by

$$(\sigma_{i,k})_{\{p2^i+1,\ldots,(p+1)2^i\}} = T^{2^{i-1}}(p2^i + 1, \ldots, (p+1)2^i),$$

for all $0 \le p \le 2^{k-i} - 1$. Let $\Sigma_{i,k}$ be the permutation on elements of $\mathbb{F}_2^{2^k}$ induced by $\sigma_{i,k}$. That is, for $\mathbf{x} = (x_1, x_2, \ldots, x_{2^k}) \in \mathbb{F}_2^{2^k}$,

$$\Sigma_{i,k}(\mathbf{x}) = \left(x_{\sigma_{i,k}(1)}, x_{\sigma_{i,k}(2)}, \ldots, x_{\sigma_{i,k}(2^k)}\right). \tag{1}$$

In other word, $\Sigma_{i,k}$ is a permutation induced by $\sigma_{i,k}$. We have the following.

Lemma 3.1 ([35, Lemma 2.6]). *Let $k \ge 1$ and $1 \le i \le k$. For $x \in A_k$ we have*

$$\Sigma_{i,k}(\Phi_k(x)) = \Phi_k(\Theta_i(x)).$$

We can extend the definition of Σ to subsets of $[k]$. For all $A \subseteq [k]$ we define the permutation $\Sigma_{A,k}$ by

$$\Sigma_{A,k} = \prod_{i\in A} \Sigma_{i,k}.$$

It is clear that for all $x \in A_k$ we have

$$\Sigma_{A,k}(\Phi_k(x)) = \Phi_k(\Theta_A(x)). \tag{2}$$

3.1.2. Characterization of skew cyclic codes over A_k

Let $S \subseteq [k]$ and let $\Sigma_S = \tau_S \circ T^{2^k}$ be the permutation on elements of $\mathbb{F}_2^{n2^k}$ where T is the cyclic shift modulo $n2^k$ and τ_S is the permutation on elements of $\mathbb{F}_2^{n2^k}$ defined for all

$$\mathbf{x} = (x_1^1, \ldots, x_{2^k}^1, x_1^2, \ldots, x_{2^k}^2, \ldots, x_1^n, \ldots, x_{2^k}^n) \in \mathbb{F}_2^{n2^k},$$

by

$$\begin{aligned}\tau_S(\mathbf{x}) &= \tau_S((x_1^1, \ldots, x_{2^k}^1, x_1^2, \ldots, x_{2^k}^2, \ldots, x_1^n, \ldots, x_{2^k}^n)) \\ &= (\Sigma_{S,k}(x^1), \Sigma_{S,k}(x^2), \ldots, \Sigma_{S,k}(x^n))\end{aligned}$$

where $x^j = (x_1^j, \ldots, x_{2^k}^j)$. Since T^{2^k} and τ_S commute, Σ_S can be written as $T^{2^k} \circ \tau_S$ as well. Let σ_S denote permutation on $\{1, 2, \ldots, n2^k\}$, the indices of elements in $\mathbb{F}_2^{n2^k}$, that induce the permutation Σ_S above. Then we have the following necessary and sufficient conditions for the code C to be a skew cyclic over A_k.

Lemma 3.2 ([35, Lemma 4.1]). *Let C be a code in A_k^n. The code $\Phi_k(C)$ is fixed by the permutation Σ_S if and only if C is a Θ_S-cyclic code.*

We have the first characterization of the code C to be a Θ_S-cyclic over A_k, given in term of the Gray map Φ_k as follows.

Theorem 3.1 ([35, Theorem 4.3])**.** *Let C be a code in A_k^n.*

1. *If n is odd then C is a skew-cyclic code if and only if $\Phi_k(C)$ is equivalent to an additive $2^{k-1}-$quasi-cyclic code C' in $\mathbb{F}_2^{n2^k}$.*
2. *If n is even then C is a skew-cyclic code if and only if $\Phi_k(C)$ is equivalent to an additive 2^k-quasi-cyclic code C' in $\mathbb{F}_2^{n2^k}$.*

We also have the second characterization of Θ_S-cyclic codes using the map $\Psi_{k,p}$ as follows.

Theorem 3.2 ([35, Theorem 4.4])**.** *An A_k-linear code C is Θ_S-cyclic of length n if and only if $C = \Psi_{k,p}^{-1}(C_1,\dots,C_s)$, where $C_1,\dots,C_s$ are quasi-cyclic codes of index 2 which satisfy*

$$T_{\Theta_{S'}}(C_i) \subseteq C_{\mu(i)} \tag{3}$$

for some $S' \subseteq S$ and permutation μ.

Next, we illustrate some constructions of skew cyclic codes over A_k.

First, the ring A_k is isomorphic to $\mathbb{F}_2^{2^k}$ via the Chinese Remainder Theorem ([20, Theorem 2.5]). Let $CRT : \mathbb{F}_2^{2^k} \to A_k$ be this canonical map. Let $CRT(C_1,....,C_{2^k})$ be the code over A_k formed by taking the map from $C_1 \times C_2 \times \cdots \times C_{2^k}$ where each C_i is a binary code.

Define the following map $\Gamma : \mathbb{F}_2^{n2^k} \longmapsto \mathbb{F}_2^n \times \mathbb{F}_2^n \times \cdots \times \mathbb{F}_2^n$ by

$$\Gamma(x_1^1,\dots,x_1^{2^k},x_2^1,\dots,x_1^{2^k},x_3^1,\dots,x_n^1,\dots,x_n^{2^k}) = ((x_1^1,\dots,x_n^1),(x_1^2,\dots,x_n^2),\dots,(x_1^{2^k},\dots,x_n^{2^k})).$$

For all codes C over A_k with $C = CRT(C_1,\dots,C_{2^k})$ we have that

$$\Gamma \circ \Phi_k(C) = (C_1, C_2, \dots, C_{2^k}).$$

Lemma 3.3 ([35, Proposition 5.1])**.** *Let n be an even integer and let $C_1, C_2, \dots, C_{2^k}$ be binary cyclic codes in $\mathbb{F}_2^n$. Then for all $A \subseteq [k]$ there exists a Θ_A-cyclic code C in A_k^n.*

We define the map

$$\Gamma_1 : \mathbb{F}_2^{n2^{k-1}} \longmapsto \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \times \cdots \times \mathbb{F}_2^{2n}, \tag{4}$$

with

$$\Gamma_1(x_1^1,\dots,x_1^{2^{k-1}},x_2^1,\dots,x_2^{2^{k-1}},\dots,x_{2n}^1,\dots,x_{2n}^{2^{k-1}}) = ((x_1^1,\dots,x_{2n}^1),(x_1^2,\dots,x_{2n}^2),\dots,(x_1^{2^{k-1}},\dots,x_{2n}^{2^{k-1}})).$$

Lemma 3.4 ([35, Proposition 5.2])**.** *Let n be an odd integer and let $C_1, C_2, \dots, C_{2^{k-1}}$ be binary cyclic codes in $\mathbb{F}_2^{2n}$. Then for all $S \subseteq [k]$ there exists a Θ_S-cyclic code C in A_k^n.*

We know describe an algorithm for constructing Θ_S-cyclic codes.

1. Construction of Θ_A-cyclic codes in A_k of even length.

   (a) We consider $C_1,\dots,C_{2^k}$ binary cyclic codes in $\mathbb{F}_2^n$

(b) We apply Γ^{-1} and we obtain C' a 2^k- quasi-cyclic code in $\mathbb{F}_2^{n2^k}$.

(c) We apply $\Phi_k^{-1} \circ \sigma_{S_2}^{-1}$ to C'. We obtain a Θ_S-cyclic code C in A_k.

2. Construction of Θ_S-cyclic codes in A_k of odd length.
   (a) We consider $C_1, \ldots, C_{2^{k-1}}$ binary cyclic codes in $\mathbb{F}_2^{2n}$
   (b) We apply Γ_1^{-1} and we obtain C' a $2^{k-1}-$quasi-cyclic code in $\mathbb{F}_2^{n2^k}$.
   (c) We apply $\Phi_k^{-1} \circ \sigma_{S_1}^{-1}$ to C'. We obtain a Θ_S-cyclic code C in A_k^n.
3. Construction of Θ_S-cyclic codes over A_k from codes over A_p, where $p < k$.
   (a) Given $C_1, \ldots, C_s$ quasi-cyclic codes of index 2 in A_p which satisfy Equation (3) in Theorem 3.2, for some $S' \subseteq S$.
   (b) Appling $\Psi_{k,p}$ to $(C_1, \ldots, C_s)$, we obtain a Θ_S-cyclic code over A_k.

In terms of skew-polynomial rings, the third construction of a Θ_S-cyclic code above will be as follows.

Lemma 3.5 ([35, Proposition 5.3]). *Let $C = \Psi_{k,p}^{-1}(C_1, \ldots, C_s)$ be Θ_S-cyclic codes over A_k, where $C_1, \ldots, C_s$ are codes over A_p, for some $p < k$. If $C_i = \langle g_{1_i}(x), \ldots, g_{m_i}(x)\rangle$, for all $i = 1, \ldots, s$, then*

$$C = \langle g_{1_1}(x), \ldots, g_{m_1}(x), \ldots, g_{1_s}(x), \ldots, g_{m_s}(x)\rangle.$$

Now, let us turn to the skew cyclic codes over B_k.

3.2. *Skew cyclic codes over the ring B_k*

As it is clear from the definition, the ring B_k is a generalization of the ring A_k. We also have further facts regarding the Gray map on B_k, and also the automorphism on B_k. We knew that every element in B_k can be written as every element in A_k, and also the map Φ_k on A_k also define a Gray map on B_k. Moreover, the automorphism Θ_S as defined on A_k also holds as an automorphism on B_k.

Now, let S_1, S_2 be two elements of $2^{[k]}$ with the same cardinality. Let λ_{S_1,S_2} be a one-on-one correspondence between S_1 and S_2 and $\lambda_{S_1,S_2}(i) = i$ for all $i \notin S_1$. For any $\alpha \in \mathbb{F}_{p^r}$, we define the map $\Lambda_{S_1,S_2,t}$ as follows.

$$\Lambda_{S_1,S_2,t}(\alpha v_i) = \alpha^{p^t} v_{\lambda_{S_1,S_2}(i)},$$

for every $i \in S_1$, where $0 \leq t \leq r$. It is easy to check that $\Lambda_{S_1,S_2,t}$ defines an automorphism on B_k.

Using two classes of automorphisms Θ_S and $\Lambda_{S_1,S_2,t}$, we can describe all automorphisms in the ring B_k as given in the lemma below.

Lemma 3.6 ([36, Lemma 9]). *If θ is an automorphism in the ring B_k, then there exist S, S_1, S_2, three subsets of $[k]$, some integer t, where $|S_1| = |S_2|$ and $0 \leq t \leq r$, such that*

$$\theta = \Theta_S \circ \Lambda_{S_1,S_2,t}.$$

Let T be the matrix that performs the cyclic shift on a vector. Let $\sigma_{i,k}$ be the permutation of $\{1, 2, \dots, 2^k\}$ defined by

$$(\sigma_{i,k})_{\{j2^i+1,\dots,(j+1)2^i\}} = T^{2^{i-1}}(j2^i + 1, \dots, (j+1)2^i)$$

for all $0 \leq j \leq 2^{k-i} - 1$. Let $\Sigma_{i,k}$ be the permutation on elements of $\mathbb{F}_{p^r}^{2^k}$ induced by $\sigma_{i,k}$. That is, for $\mathbf{x} = (x_1, x_2, \dots, x_{2^k}) \in \mathbb{F}_{p^r}^{2^k}$,

$$\Sigma_{i,k}(\mathbf{x}) = \left(x_{\sigma_{i,k}(1)}, x_{\sigma_{i,k}(2)}, \dots, x_{\sigma_{i,k}(2^k)}\right). \tag{5}$$

Related to the Gray map, Lemma 3.1 above also holds for the ring B_k, as mentioned below.

Lemma 3.7 ([36, Lemma 10]). *Let $k \geq 1$ and $1 \leq i \leq k$. For $x \in B_k$ we have*

$$\Sigma_{i,k}(\Phi_k(x)) = \Phi_k(\Theta_i(x))$$

3.3. *Characterization of skew cyclic codes over B_k*

Let $S, S_1, S_2 \subseteq \{1, 2, \dots, k\}$, where $|S_1| = |S_2|$ and let $\Xi_{S,S_1,S_2} = \xi_{S,S_1,S_2,t} \circ T^{2^k}$ be a bijective map on elements of $\mathbb{F}_{p^r}^{n2^k}$ where T is the cyclic shift modulo $n2^k$ and $\xi_{S,S_1,S_2,t}$ defined for all elements

$$\mathbf{x} = (x_1^1, \dots, x_{2^k}^1, x_1^2, \dots, x_{2^k}^2, \dots, x_1^n, \dots, x_{2^k}^n) \in \mathbb{F}_2^{n2^k},$$

by

$$\begin{aligned}\xi_{S,S_1,S_2,t}(\mathbf{x}) &= \xi_{S,S_1,S_2,t}((x_1^1, \dots, x_{2^k}^1, x_1^2, \dots, x_{2^k}^2 \dots, x_1^n, \dots, x_{2^k}^n)) \\ &= ((\Sigma_{S,k} \circ \Gamma_{S_1,S_2,t})(\mathbf{x}^1), (\Sigma_{S,k} \circ \Gamma_{S_1,S_2,t})(\mathbf{x}^2), \dots, (\Sigma_{S,k} \circ \Gamma_{S_1,S_2,t})(\mathbf{x}^n))\end{aligned}$$

where $\mathbf{x}^j = (x_1^j, \dots, x_{2^k}^j)$, for $1 \leq j \leq n$. Since T^{2^k} and $\xi_{S,S_1,S_2,t}$ commute, $\Xi_{S,S_1,S_2,t}$ can be written as $T^{2^k} \circ \xi_{S,S_1,S_2,t}$ as well. Now we are ready to provide the first characterization of θ-cyclic codes over B_k.

Theorem 3.3 ([36, Lemma 15]). *Let C be a code in B_k^n and $\theta = \Theta_S \circ \Lambda_{S_1,S_2,t}$ be an automorphism in B_k, for some $S, S_1, S_2 \subseteq [k]$ and an integer t, where $0 \leq t \leq r$. Then, the code $\Phi_k(C)$ is fixed by the bijection $\Xi_{S,S_1,S_2,t}$ if and only if C is a θ-cyclic code.*

Let $\tilde{\lambda}_{S_1,S_2}$ be a permutation on $\{1, 2, \dots, 2^k\}$ induced by $\Theta_S \circ \Lambda_{S_1,S_2,t}$, and $\mathrm{Ord}(\tilde{\lambda}_{S_1,S_2})$ be the order of $\tilde{\lambda}_{S_1,S_2}$. The following theorem also gives a second characterization for θ-cyclic codes over the ring B_k.

Theorem 3.4 ([36, Theorem 17]). *A linear code C over B_k is θ-cyclic of length n if and only if there exist quasi-$\tilde{\theta}$-cyclic codes $C_1, C_2, \dots, C_{2^k}$ of length n over $\mathbb{F}_{p^r}$ with index $\mathrm{Ord}(\tilde{\lambda}_{S_1,S_2})$, such that*

$$C = \overline{\varphi}_k^{-1}(C_1, C_2, \dots, C_{2^k})$$

where $\tilde{\theta} = \phi^{t\,\mathrm{Ord}(\tilde{\lambda}_{S_1,S_2})}$, for some t as in the Lemma, with ϕ is the Frobenius automorphism in $\mathbb{F}_{p^r}$, and $T_{\tilde{\theta}}(C_i) \subseteq C_j$, where $j \in S \cup S_2$, for all $i = 1, 2, \dots, 2^k$.

Theorem above gives us an algorithm to construct skew-cyclic codes over the ring B_k as follows.

Algorithm 3.5. Given n, the ring B_k, and an automorphism θ.

(1) Decompose θ into $\theta = \Theta_S \circ \Lambda_{S_1,S_2,t}$.

(2) Determine $\mathrm{Ord}(\tilde{\lambda}_{S_1,S_2})$ and $\tilde{\theta} = \theta|_{\mathbb{F}_{p^r}} = \phi^t$, where ϕ is the Frobenius automorphism in $\mathbb{F}_{p^r}$.

(3) Choose quasi-$\tilde{\theta}$-cyclic codes over $\mathbb{F}_{p^r}$, say $C_1, \ldots, C_{2^k}$, such that

$$T_{\tilde{\theta}}^{t_1}(C_i) \subseteq C_j,$$

where $j \in S \cup S_2$, for all $i = 1, 2, \ldots, 2^k$.

(4) Calculate $C = \overline{\varphi}_k^{-1}(C_1, \ldots, C_{2^k})$.

(5) C is a θ-cyclic code over the ring B_k.

4. Skew cyclic codes with derivation over non-chain rings

Seven years later, after introducing the notion skew cyclic codes over finite fields, Boucher and Ulmer [15] further generalized the concept of cyclic codes over finite fields to the skew cyclic codes with derivation over finite fields. These codes may be regarded as a ”two-step” generalization of cyclic codes, namely by considering non identity automorphism and non zero derivation.

Let $\mathbf{R}$ be a finite ring and $\Theta : \mathbf{R} \longrightarrow \mathbf{R}$ be an automorphism of $\mathbf{R}$. Then a map $\Delta_\Theta : \mathbf{R} \longrightarrow \mathbf{R}$ is called a *derivation* on $\mathbf{R}$ if the following two conditions are satisfied:

(i) $\Delta_\Theta(x + y) = \Delta_\Theta(x) + \Delta_\Theta(y)$, and

(ii) $\Delta_\Theta(xy) = \Delta_\Theta(x)y + \Theta(x)\Delta_\Theta(y)$.

Let $\mathbf{R}$ be a ring with automorphism Θ and derivation Δ_Θ. The skew-polynomial ring $\mathbf{R}[x; \Theta, \Delta_\Theta]$ is the set of all polynomials over $\mathbf{R}$ with ordinary addition of polynomials and multiplication defined by

$$xa := \Theta(a)x + \Delta_\Theta(a),$$

for any $a \in \mathbf{R}$. This multiplication is extended to all polynomials in $\mathbf{R}[x; \Theta, \Delta_\Theta]$ in the usual manner. This kind of ring was introduced by Ore [43] in 1933, where $\mathbf{R}$ is equal to the finite field $\mathbb{F}_q$.

A code $C \subseteq \mathbf{R}^n$ is called a Δ_Θ-linear code of length n over $\mathbf{R}$ if C is a left $\mathbf{R}[x; \Theta, \Delta_\Theta]$-submodule of $\mathbf{R}[x; \Theta, \Delta_\Theta]/\langle f(x) \rangle$ for a polynomial $f(x) \in \mathbf{R}[x; \Theta, \Delta_\Theta]$ of degree n. If $f(x)$ is a central element then C is called a central Δ_Θ-linear code.

A code $C \subseteq \mathbf{R}^n$ is called a Δ_Θ-*cyclic code* of length n over $\mathbf{R}$ if C is a Δ_Θ-linear code and for all $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ we have

$$T_{\Delta_\Theta}(\mathbf{c}) := (\Theta(c_{n-1}) + \Delta_\Theta(c_0), \Theta(c_0) + \Delta_\Theta(c_1), \ldots, \Theta(c_{n-2}) + \Delta_\Theta(c_{n-1})) \in C.$$

Here, T_{Δ_Θ} is called a *shifting operator of* Δ_Θ*-cyclic.*

The notion of skew cyclic codes with derivation (or Δ_Θ-cyclic codes) over finite fields was introduced by Boucher and Ulmer [15] in 2014. Sharma and Baintwal [54] generalized the notion of Δ_Θ-cyclic codes over a finite ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 1$. Ma, Gao, Li and Fu [44] further generalized the observation of Sharma and Baitwall above, by considering $\mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 1$. Recently, Patel and Prakash [47] investigated Δ_Θ-cyclic codes over $\frac{\mathbb{F}_q[u,v]}{\langle u^2-u, v^2-v\rangle} = B_2$. Very recently, together with Tang, the author investigated Δ_Θ-cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$, with $v^2 = v$.

Let $R_1 := \mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 1$ and $R_3 := \mathbb{Z}_4 + v\mathbb{Z}_4$, with $v^2 = v$, denote the finite rings considered by Sharma and Bainthwal [54] and also Suprijanto and Tang [60], respectively. The following automorphisms θ and their related derivations Δ_θ have been defined by several authors:

- $\theta_1(a + ub) = a + (u + 2)b$ and $\Delta_{\theta_1}(a + ub) = 2b + 2ub$ (Ma, Gao, Li, and Fu [44]; Sharma and Bainthwal [54]).
- $\theta_2(a + ub + vc + uvd) = a^{p^t} + ub^{p^t} + vc^{p^t} + uvp^{p^t}$ and $\Delta_{\theta_2}(a + ub + vc + uvd) = (1 + u + v + uv)(\theta_2(a + ub + vc + uvd) - (a + ub + vc + uvd))$ (Patel and Prakash [47]).
- $\theta_3(a + bv) = a + b - bv$ and $\Delta_{\theta_3}(a + bv) = (1 + 2v)\ (\theta_3(a + bv) - (a + bv))$ (Suprijanto and Tang [60]).

By using the above notations, we have some properties regarding automorphisms and their related derivations.

Lemma 4.1. *The following statements hold:*

(1) For $i = 1$ *or* $i = 3$*, we have* $\Delta_{\theta_i}\theta_i + \theta_i\Delta_{\theta_i} \equiv 0$ *([54], [60]).*

(1′) $\Delta_{\theta_2}\theta_2 = \theta_2\Delta_{\theta_2}$ *([47]).*

(2) For $i = 1$ *or* $i = 3$*, we have* $\Delta_{\theta_i}\Delta_{\theta_i} \equiv 0$ *([54], [60]).*

(3) Let $i = 1$ *or* $i = 3$*. For all* $x \in R$*, we have* $\Delta_{\theta_i}(x) = 0 \iff \theta_i(x) = x$ *([54], [60]).*

Sharma and Bainthwal [54] also Suprijanto and Tang [60] proved the following property for the rings they considered. This property is important to do a multiplicative operation in the rings.

Lemma 4.2 ([54], [60])**.** *Let* R_1 *and* R_3 *denote the finite rings as defined above. For all* $a \in R_1$ *or* $a \in R_3$*, we have* $x^2a = ax^2$*.*

The similar property was also proved by Patel and Prakash [47], for the finite field of order 4.

Lemma 4.3 ([47])**.** *For all* $a \in \mathbb{F}_4$*, we have* $x^2a = \theta_2^2(a)x^2$*.*

As a corollary, the following property hold.

Corollary 4.1 ([54], [60])**.** *Let* $i = 1$ *or* $i = 3$*. For all* $a \in R_i,\ n \in \mathbb{Z}^+$*, we have*

$$x^n a = \begin{cases} (\theta_i(a)x + \Delta_{\theta_i}(a))x^{n-1}, & n \text{ is odd}, \\ ax^n, & n \text{ is even}. \end{cases}$$

Corollary 4.2 ([47]). *For all $a \in \mathbb{F}_4,\ n \in \mathbb{Z}^+$, we have*

$$x^n a = \begin{cases} (\theta_2(a)x + \Delta_{\theta_2}(a))x^{n-1}, & n \textit{ is odd},\\ \theta_2(a)x^n, & n \textit{ is even}. \end{cases}$$

Since the rings R_1, R_3, and B_2 are all not left/ right Euclidean rings, then the division algorithm does not hold. But a kind of modified division algorithm still holds, which means that we can still apply the division algorithm on some particular elements of the rings.

Lemma 4.4 (Right-division algorithm). *Let R be R_1, R_3, or B_2. Let $f(x), g(x) \in R[x;\theta,\Delta_\theta]$ such that the leading coefficient of $g(x)$ is a unit. Then there exist $q(x), r(x) \in R[x;\theta,\Delta_\theta]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

4.1. Structural properties of skew cyclic codes with derivation

Let R denote the ring R_1, R_3, or B_2. Let θ be an automorphism θ_1, θ_2, or θ_3 defined above and let $Delta_\theta$ be their related derivations. For our purpose, to convert the algebraic structures of Δ_θ-cyclic codes into combinatorial structures and vice versa, we consider the following correspondence:

$$\begin{array}{ccc} R[x;\theta,\Delta_\theta]/\langle f(x)\rangle & \longrightarrow & R^n,\\ c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} & \longmapsto & (c_0, c_1, \ldots, c_{n-1}). \end{array}$$

Let R_{n,Δ_θ} denote the ring $R[x;\theta,\Delta_\theta]/\langle x^n - 1\rangle$.

Lemma 4.5 ([47], [54], [60]). *If $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in R_{n,\Delta_\theta}$ is identified by a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in R^n$, then $xc(x)$ is identified by $T_{\Delta_\theta}(\mathbf{c}) \in R^n$.*

Lemma 4.6 ([47], [54], [60]). *A code $C \subseteq R^n$ is Δ_θ-cyclic code if and only if C is a $R[x;\theta,\Delta_\theta]$-submodule of R_{n,Δ_θ}.*

Corollary 4.3 ([47], [54], [60]). *If $C \subseteq R^n$ is a Δ_θ-cyclic code of even length n, then C is an ideal of R_{n,Δ_θ}.*

Lemma 4.7 ([47], [54], [60]). *Let $C \subseteq R^n$ be a Δ_θ-cyclic code. Then the following two statements hold.*

(1) If n is odd, then C is a cyclic code of length n over R.

(2) If n is even, then C is a quasi-cyclic code of length n and index 2 over R.

Remark 4.1. Patel and Prakash [47] proved that the Lemma 4.7 holds only for $R = \mathbb{F}_4$.

Lemma 4.8. *If $C \subseteq R^n$ is a Δ_θ-cyclic code and $g(x)$ is a nonzero polynomial in C of smallest degree with leading coefficient is a unit in R, then the following three statements hold.*

(1) $C = \langle g(x)\rangle$.

(2) $g(x)$ is a right divisor of $x^n - 1$.

(3) $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$ is a basis of C, with $k = \deg(g(x))$.

Remark 4.2. Patel and Prakash [47] proved only the properties (1) and (2) in Lemma 4.8.

5. Linear codes from graphs

Around twenty years ago, Tonchev [68] wrote a short survey on linear codes over a binary field $\mathbb{F}_2$ constructed from adjacency matrices of undirected graphs. Among the main and important result mentioned in [68] is a theorem below.

Theorem 5.1 ([68])**.** *Let $G = (V, E)$ be an undirected graph on n vertices having an adjacency matrix A. Then the class of binary linear codes of length $2n$ and dimension n defined by generator matrices of the form (I, A) contains codes with minimum Hamming distance*

$$d \geq 0.22n.$$

From the proof of the above theorem, it becomes clear that the theorem shows the existence of optimal binary linear codes constructed from graphs, namely from the class of all graphs with n vertices, we may obtain linear codes that for large n meet the Gilbert–Varshamov bound. Unfortunately, the proof does not provide a constructive way to find such codes. However, we may obtain many good linear codes from certain class of graphs, such as strongly regular and distance regular graphs.

5.1. Linear codes from strongly regular graphs

A graph $G = (V, E)$ is called strongly regular of parameters (n, k, λ, μ) if G is a graph on $|V| = n$ vertices which is regular of degree k and satisfies the following properties:

(1) any two adjacent vertices have exactly λ common neighbors, and

(2) any two non-adjacent vertices have exactly μ common neighbors.

Tonchev [66, 68] showed that linear codes constructed from strongly regular graphs have an efficient decoding algorithm, called majority logic decoding (see [45, 67] for a detail description about majority logic decoding). In particular, he [66] succeed to construct optimal and nearly optimal linear codes over $\mathbb{F}_2$ of length 50 and 100 from Hoffman-Singleton and Higman-Sims graphs, two famous strongly regular graphs having parameters $(50, 7, 0, 1)$ and $(100, 22, 0, 6)$, respectively. We note that Hoffman-Singleton and Higman-Sims graph is a unique strongly regular graph on 50 and 100 vertices, respectively, with the above mentioned parameters (see [16] p. 285 and 303). Using the Hoffman-Singleton graph, Tonchev [66] obtained binary linear codes with parameters (1) $[50, 21, 12]$, (2) $[50; 29; 8]$, (3) $[50, 22, 7]$, and (4) $[50, 28, 8]$, while from Higman-Sims graphs he [66] obtained binary linear codes with parameters (5) $[100, 22, 22]$, (6) $[100, 78, 6]$, (7) $[100, 22, 32]$, and (8) $[100, 78, 8]$. Tonchev [66] also showed that the code (8) is optimal, while the codes (1), (2), (4), and (7) have the highest known minimum distance for a known code of the given length and dimension. The codes (2), (4), (6), and (8) admit majority logic decoding.

Afterwards, Haemers, Peeters, and van Rijckevorsel [31] looked at linear codes over $\mathbb{F}_2$ generated by A and $I + A$, where A is an adjacency matrix of a strongly regular graph. They considered linear codes constructed from strongly regular graphs on vertices up to 45. This includes some famous strongly regular graphs like Triangular graphs, Lattice graphs, Paley graphs, and also the graphs related to a symplectic form over $\mathbb{F}_2$. They did a more structural approach by deriving the relation between the binary codes obtained from strongly regular graphs with regular two-graphs and also Seidel switching (see Section 5 in [31] for detail accounts).

The construction of linear codes from graphs, in particular from strongly regular graphs, further investigated by many people. In 2007, Dougherty, Kim, and Solé [26] introduced a very general construction method of self-dual codes over finite commutative rings from strongly regular graphs as well as doubly regular tournaments. As it is well-known, association schemes of class-2 consist of either strongly regular graphs (SRG) or doubly regular tournaments (DRT). A strongly regular graph is equivalent to a symmetric association scheme of class-2. Namely, if for all $i \in [0,2]_{\mathbb{Z}}$, we have $A_i^T = A_i$. In this case, A_1 is the adjacency matrix of a strongly regular graph. If the association scheme is not symmetric, then we have $A_2 = A_1^T$, and here A_1 is the adjacency matrix of a doubly regular tournament. (See [6] or [7] the definition of and undefined terms related to association schemes).

The general constructions given by [26] can be described as follows. Let R be a finite commutative ring, and let $r, s, t \in R$. Define a matrix

$$Q_R(r,s,t) := (rI + sA + t\overline{A}),$$

where A is the adjacency matrix of a strongly regular graph or a doubly regular tournament.

The **pure** construction is

$$\mathcal{P}_R(r,s,t) = (I \mid Q_R(r,s,t)).$$

The **bordered** construction is

$$\mathcal{B}_R(r,s,t) = \left(\begin{array}{c|c|c|c} 1 & 0 \cdots 0 & \alpha & \beta \cdots \beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_R(r,s,t) \\ 0 & & \gamma & \end{array}\right),$$

where α, β, and γ are scalars which is determined according to specific cases (namely, depending on the specific ring R).

Let $P_R(r,s,t)$ be the row span over R of $\mathcal{P}_R(r,s,t)$ and let $B_R(r,s,t)$ be the row span over R of $\mathcal{B}_R(r,s,t)$. The code $P_R(r,s,t)$ is a code over R of length $2v$ and the code $B_R(r,s,t)$ is a code over R of length $2v+2$, where v is a cardinality of vertex set of the strongly regular graph or the doubly regular tournament. Two main results in [26] are given below.

Theorem 5.2. *Let G be a strongly regular graph or doubly regular tournament with parameters (v,k,λ,μ). The code $P_R(r,s,t)$ formed from an SRG is Euclidean self-dual over R if and only if*

$$\begin{aligned} (r^2 + s^2k - t^2 - t^2k + t^2v) &= -1, \\ (2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k) &= 0, \\ (2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k) &= 0. \end{aligned}$$

The code $P_R(r,s,t)$ formed from a DRT is Euclidean self-dual over R if and only if

$$\begin{aligned} (r^2 + (s^2 + t2)k) &= -1, \\ (rt + sr + (s^2+t^2)(k-1-\lambda) + st\lambda + st\mu) &= 0, \\ (rt + sr + (s^2+t^2)(k-\mu) + st\mu + st\lambda) &= 0. \end{aligned}$$

Furthermore, the self-dual code is Type II over $\mathbb{Z}_{2m}$ if and only if $1 + r^2 + s^2k + t^2(v - k - 1) \equiv 0 \pmod{4m}$.

Theorem 5.3. *The code $B_R(r, s, t)$ formed from an SRG is Euclidean self-dual over R if and only if*

$$\begin{aligned}
(r^2 + s^2k - t^2 - t^2k + t^2v) &= -(1 + \gamma^2),\\
(2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k) &= -\gamma^2,\\
(2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k) &= -\gamma^2,\\
1 + \alpha^2 + v\beta^2 &= 0,\\
\alpha\gamma + \beta(r + sk + t(v - k - 1)) &= 0.
\end{aligned}$$

The code $B_R(r, s, t)$ formed from a DRT is Euclidean self-dual over R if and only if

$$\begin{aligned}
(r^2 + (s^2 + t^2)k) &= -(1 + \gamma^2),\\
(rt + sr + (s^2 + t^2)(k - 1 - \lambda) + st\lambda + st\mu) &= -\gamma^2,\\
(rt + sr + (s^2 + t^2)(k - \mu) + st\mu + st\lambda) &= -\gamma^2,\\
1 + \alpha^2 + v\beta^2 &= 0,\\
\alpha\gamma + \beta(r + sk + t(v - k - 1)) &= 0.
\end{aligned}$$

Furthermore, this self-dual code is Type II over $\mathbb{Z}_{2m}$ if and only if $1+\gamma^2+r^2+s^2k+t^2(v-k-1) \equiv 0 \pmod{4m}$ *and* $1 + \alpha^2 + v\beta^2 \equiv 0 \pmod{4m}$.

The work of Dougherty, Kim, and Solé [26] generalized several known constructions such as ternary symmetric codes by Pless [48], binary double circulant codes by Karlin [45, p. 507], quaternary double circulant codes by Calderbank and Sloane [18], and also quadratic double circulant codes by Gaborit [30]. Their work [26] provided a new breakthrough in study of constructing codes from graphs.

As concrete examples, they [26] obtained many new self-dual codes over certain finite rings having good properties and parameters. Moreover, by using pure and bordered constructions above, the author together with Nugraha [59] constructed many extremal or nearly-extremal linear codes over finite fields of various lengths.

Very recently, Fellah, Guenda, Özbudak, and Seneviratne [27] constructed self-dual codes over certain finite fields from Paley-type bipartite graphs as well as their complements. They [27] obtained many optimal or nearly optimal self-dual codes.

5.2. *Linear codes from directed strongly regular graphs*

Beside (undirected) strongly regular graphs, recently directed strongly regular graphs have also attracted coding theorists in connection with construction of linear codes. It is well-known that doubly regular tournaments are equivalent to skew Hadamard matrices [51]. It is also known that doubly regular tournaments are special case of directed strongly regular graphs [2]. Since doubly regular tournaments lead to many good codes [42], it is very natural to consider codes constructed from the adjacency matrices of directed strongly regular graphs. This facts have motivated Alahmadi, Alkenani, Kim, Shi, and Solé [2] to consider linear codes from directed strongly regular graphs.

Let A be a v by v $(0,1)$-matrix having zero diagonal. Thus A is the adjacency matrix of a directed simple graph without loops on v vertices. This graph is a directed strongly regular graph (DSRG) of parameters (v,k,t,λ,μ) if it satisfies the following pair of relations:

(1) $AJ = JA = kJ$,

(2) $A^2 = tI + \lambda A + \mu(J - I - A)$,

where I and J denote the identity and all-one matrices, respectively, of order v. This concept was defined by Duval in 1998 [16].

Although, so far, the codes constructed from directed strongly regular graphs are not optimal, but they [2] believed that there are many interesting combinatorial aspects of directed strongly regular graphs in the same way that linear codes are relevant to combinatorial aspects of designs. There are huge study of the later objects, but it is beyond the scope of this paper. (See the book of Assmus and Key [3] for the record of early development and see Ding and Tang's book [23] for recent developments on it).

5.3. Linear codes from distance regular graphs

Very recently, there is a new development on linear codes constructed from graphs. Crnković, Rukavina, and Švob proposed a construction method of linear codes, in particular self-orthogonal codes over a finite field $\mathbb{F}_q$ as well as a finite ring $\mathbb{Z}_m$ from equitable partitions of symmetric association schemes. Their construction methods then be applied to distance regular graphs to obtain self-orthogonal codes, which some of them are optimal. We describe here their methods a bit detail.

Let $\{C_0, C_1, \ldots, C_{t-1}\}$ be a partition of X. The characteristic matrix H is the $n \times t$ matrix whose j-th column is the characteristic vector of C_j, where $j = 0, 1, \ldots, t-1$. A partition $\Pi = \{C_0, C_1, \ldots, C_{t-1}\}$ of the n vertices of a graph G is *equitable* (or regular) if for every pair of (not necessarily distinct) indices $i, j \in \{0, 1, \ldots, t-1\}$ there is a nonnegative integer b_{ij} such that each vertex $v \in C_i$ has exactly b_{ij} neighbors in C_j, regardless of the choice of v. The $t \times t$ quotient matrix $B = (b_{ij})$ is well-defined if and only if the partition Π is equitable. An equitable (or regular) partition of an association scheme (X, R) is a partition of X which is equitable with respect to each of the graphs Γ_i, $i \in \{1, 2, \ldots, d\}$ corresponding to the association scheme $(X, \mathcal{R})$ with d classes.

The main theorems in [21] below give a construction method of self-orthogonal codes over a finite field $\mathbb{F}_q$ and a finite ring $\mathbb{Z}_m$, respectively.

Theorem 5.4. *Let Π be an equitable partition of a d-class association scheme $(X, \mathcal{R})$ with n cells of the same length $\frac{|X|}{n}$ and let p be a prime number. If there exists $i \in [1, d]_{\mathbb{Z}}$ such that for all $k \in [0, d]_{\mathbb{Z}}$ the prime p divides p_{ii}^k, then the rows of the matrix M_i span a self-orthogonal code of length n over the field $\mathbb{F}_q$, where $q = p^m$ is a prime power.*

Theorem 5.5. *Let Π be an equitable partition of a d-class association scheme $(X, \mathcal{R})$ with n cells of the same length $\frac{|X|}{n}$ and let p be a prime number. If there exists $i \in [1, d]_{\mathbb{Z}}$ such that for all*

$k \in [0,d]_{\mathbb{Z}}$ the prime m divides p_{ii}^{k}, then the rows of the matrix M_i span a self-orthogonal code of length n over the ring $\mathbb{Z}_m$.

In the above two theorems,

$$M_i := (H^T H)^{-1} H^T A_i H,$$

with A_i is an adjacency matrix corresponding to a relation R_i in the association schemes.

By using the above construction method, they [21] constructed self-orthogonal codes over finite fields from several classes of distance regular graphs: Hadamard graph on 48 vertices, $d = 4$; Doubled Gewirtz graph, $d = 5$; Incidence graph of $GH(3,3)$, $d = 6$; Doubled odd graph $D(O_4)$, $d = 7$; Foster graph, $d = 8$; (here d is a diameter of the distance regular graphs).

6. Final remarks

We have reported some progress of study on cyclic codes over finite rings as well as their ”one-step” and ”two-step” generalization. We also mentioned an overview on the study of linear codes constructed from graphs, with emphasize on (directed or undirected) strongly regular graphs and also distance regular graphs. However, there are many more interesting aspects of cyclic codes as well as linear codes from graphs to consider, but the constraints of space and time have not permitted it. We list some of them.

(1) **Negacyclic and constacyclic codes over finite rings.**
Negacyclic and constacyclic codes (see again Subsection 2.3 for the definitions) are also generalizations of cyclic codes in another direction. There are many results regarding negacyclic as well as constacyclic codes over finite rings, but we did not mention here. We can see, for examples, [69] for an early work, and [24] for a significant progress on negacyclic codes over finite rings. See also [63] for an early work on constacyclic codes over finite rings. For skew constacyclic codes over finite rings, the readers can also look at [39], which seem to be the first paper investigated this aspect. On the other hand, the paper by Ma, Gao, Li, and Li [44] seem to be the first one that consider skew constacyclic codes with derivation over certain finite ring. It is very interesting to consider the similar aspects, namely skew constacyclic codes as well as skew constacyclic codes with derivation over other finite rings.

(2) **Applications of cyclic codes over finite rings to the construction of quantum codes.**
One of successful application in the investigation of cyclic codes over finite rings is its application to construct good quantum codes. We can find many articles on it. In a recent article, together with Tang, the author provides many examples of quantum codes constructed from cyclic codes over a finite non-chain ring, namely a ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q + v^4\mathbb{F}_q$, where $q = p^r$, for a positive integer r, with $4 \mid (p-1)$, and $v^5 = v$ (see [61]). Very recently, together with Irwansyah, the author [62] has derived some structural properties of constacyclic codes over the ring B_k (See also [38], where we derived several structural properties of linear codes over very general family of finite rings, where B_k is a special case of it). We are now doing on the construction of good quantum codes from these constacyclic codes.

(3) **Codes from incidence matrices of graphs**
What we have considered so far in Section 5 is constructing linear codes by using the adjacency matrices of graphs. There are also many observations on constructing linear codes from the incidence matrices of graphs. This approach has been doing by Jennifer D. Key and her school of thoughts (see, for examples, [22], [28] and [29]), but we did not include here.

(4) **Graph from linear and cyclic codes.**
Regarding the interplay between codes and graphs, what we have discussed is how to construct good linear codes from graphs. However, there is also a "reverse" study: constructing graphs from codes and deriving their properties. This kind of study has recently been done, for examples, by Cardinali, Giuzzi, and Kwiatkowski [19], Shi and Solé [55], Shi, Helleseth, and Solé [56], and recently by the author as a joint work with Tang [65]. The development on this project also missed in this review.

As a final statement, we have to highlight that beside its theoretical and foundational aspects (see, for example, [70]), among the motivation in studying linear codes over finite rings is to construct linear codes with good parameters via the Gray map, that can not be obtained by direct constructions. However, very recently, together with Tang, the author [60, 64] succeeded to construct many linear codes over the ring $\mathbb{Z}_4$ having new parameters by direct construction methods. It is very interesting to construct cyclic codes with good parameters over the ring $\mathbb{Z}_{2^k}$ as well as $\mathbb{Z}_{2k}$, for certain positive integer k, by direct construction methods.

Acknowledgment

This research is supported by the Institut Teknologi Bandung (ITB) and the Ministry of Education, Culture, Research and Technology (*Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi (Kemdikbudristek)*), Republic of Indonesia.

References

[1] T. Abualrub and I. Siap, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.* **42**(3) (2007), 273-287.

[2] A. Alahmadi, A. Alkenani, J.-L. Kim, M. Shi, and Patrick Solé, Directed strongly regular graphs and their codes, *Bull. Korean Math. Soc.* **54**(2) (2017), 497-505.

[3] E. F. Assmus and J. E. Key, *Designs and their Codes*, Cambridge, 1994.

[4] E. F. Assmus Jr. and H. F. Mattson, Error-correcting codes: An axiomatic approach, *Inf. Control* **6** (1963), 315-330.

[5] R.K. Bandi and M. Bhaintwal, A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, *Discrete Math. Algorithms Appl.* **8**(1) (2016), 1650017 (17 pages).

[6] E. Bannai, Et. Bannai, T. Ito, and R. Tanaka, *Algebraic combinatorics,* Walter de Gruyter, Berlin/ Boston, 2021.

[7] E. Bannai and T. Ito, *Algebraic combinatorics I: Association schemes,* Benjamin/ Cummings, Menlo Park, California, 1984.

[8] I.F. Blake, Codes over certain rings, *Inf. Control* **20** 1972, 396-404.

[9] I.F. Blake, Codes over integer residu rings, *Inf. Control* **29** 1975, 295-300.

[10] L.S. Borrow and B.M. Franaszczuk, On cyclic codes generated by graphs, *Inf. Control* **22** (1973), 296-301.

[11] D. Boucher, W. Geiselmann, and F. Ulmer, Skew cyclic codes, *Appl. Algebra Engrg. Comm. Comput.* **18**(4) (2007), 379-389.

[12] D. Boucher, Solé, and Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.* **2**(3) (2008), 273-292.

[13] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.* **44**(3-4) (2009), 1644-1656.

[14] D. Boucher and F. Ulmer, Coding as modules over skew polynomial rings, in Proceedings of the 12th IMA Conference on Cryptography and Coding, *Lecture Notes in Comput. Sci.* **5921** (2009), 38-55.

[15] D. Boucher and F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, *Des. Codes Cryptogr.* **70**(3) (2014), 405-431.

[16] A.E. Brouwer and H. van Maldeghem, *Strongly regular graphs,* Encyclopedia Math. Appl. 182, Cambridge University Press, 2022.

[17] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Des. Codes Cryptogr.* **6** (1995), 21-35.

[18] A. R. Calderbank and N. J. A. Sloane, Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices, *J. Algebraic Combin.* **6**(2) (1997), 119-131.

[19] I. Cardinali, L. Giuzzi, and M. Kwiatkowski, On the Grassmann graph of linear codes, *Finite Fields Appl.* **75** (2021), 101895.

[20] Y. Cengellenmis, A. Dertli, and S.T. Dougherty, Codes over an infinite family of rings with a Gray map, *Des. Codes Cryptogr.*, **72**(3) (2014), 559-580.

[21] D. Crnković, S Rukavina, and A. Švob, Self-orthogonal codes from equitable partitions of association schemes, *J. Algebraic Combin.* **55**(1) (2022), 157-171.

[22] P. Dankelmann, J. D. Key, and B. G. Rodrigues, Codes from incidence matrices of graphs, *Des. Codes Cryptogr.* **68** (2013), 373-393.

[23] C. Ding and C. Tang, *Designs from linear codes* (2nd Ed.), World Scientific, 2021.

[24] H.Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Inform. Theory* **50**(8) (2004), 1728-1744.

[25] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solé. Type IV self-dual codes over rings, *IEEE Trans. Inform. Theory* **45**(7) (1999), 2345-2360.

[26] S.T. Dougherty, J.-L. Kim, and P. Solé, Doubly circulant codes from two class association schemes, *Adv. Math. Commun.* **1**(1) 2007, 45-64.

[27] N. Fellah, K. Guenda, F. Özbudak, and P. Seneviratne, Construction of self dual codes from graphs, *Appl. Algebra Engrg. Comm. Comput.* (to appear) (https://doi.org/10.1007/s00200-022-00567-2).

[28] W. Fish, J.D. Key, and E. Mwambene, Codes from incidence matrices and line graphs of Hamming graphs, *Discr. Math.* **310**(13-14) (2010), 1884-1897.

[29] W. Fish, J.D. Key, and E. Mwambene, Codes from the incidence matrices of graphs on 3-sets, *Discr. Math.* **311**(16) (2011), 1823-1840.

[30] P. Gaborit, Quadratic double circulant codes over fields, *J. Combin. Theory Ser. A* **97**(1) (2002), 85-107.

[31] W. H. Haemers, R. Peeters, and J.M. van Rijckevorsel, Binary codes of strongly regular graphs, *Des, Codes Cryptogr.* **17**(1-3) (1999), 187-209.

[32] S.L. Hakimi and H. Frank, Cut-set matrices and linear codes, *IEEE Trans. Inform. Theory* IT-11 (1965), 457-458.

[33] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and Related Codes, *IEEE Trans. Inform. Theory* **40** 1994, 301-319.

[34] W.C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes,* Cambridge University Press, 2003.

[35] Irwansyah, A. Barra, S.T. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, P. Sole, D. Suprijanto, and O. Yemen, Θ_S-cyclic codes over A_k, *Int. J. Comput. Math. Comput. Syst. Theory* **1**(1) (2016), 14-31.

[36] Irwansyah, A. Barra, A. Muchlis, I. Muchtadi-Alamsyah, and D. Suprijanto, Skew cyclic codes over B_k, *J. Appl. Math. Comput.* **57**(1-2) (2018), 69-84.

[37] Irwansyah and D. Suprijanto, Structure of linear codes over the ring B_k, *J. Appl. Math. Comput.* **58**(1-2) (2018), 755-775.

[38] Irwansyah and D. Suprijanto, Linear codes over a general infinite family of rings and MacWilliams-type relations, *Discrete Math. Lett.* **11** (2023), 53-60.

[39] S. Jitman, S. Ling, and P. Udomkavanich, Skew constacyclic codes over finite chain rings, *Ad. Math. Commun.* **6**(1) (2021), 39-63.

[40] P. Kanwar and S. R. López-Permouth, Cyclic codes over the integers modulo p^m, *Finite Fields Appl.* **3**(4) (1997), 119-131.

[41] T. Kasami, Topological approach to construction of group codes, *J. Inst. Elec. Commun. Eng. Jap.* **44** (1961), 1316-1321.

[42] J.-L. Kim and P. Solé, Skew Hadamard designs and their codes, *Des. Codes Cryptogr.* **49**(1-3) (2008), 135-145.

[43] O. Ore, Theory of non-commutative polynomials, *Annals. Math.* **34** (1933), 480-508.

[44] F. Ma, J. Gao, J. Li, and F.-W. Li, (σ, δ)-Skew quasi-cyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, *Cryptogr. Commun.* **13**(2) (2021), 307-320.

[45] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[46] G. Norton and A. Sălăgean-Mandache, On the structure of linear cyclic codes over finite chain rings, *Appl. Algebra Eng. Commun. Comput.* **10**(6) (2000), 489–506.

[47] S. Patel and O. Prakash, (θ, δ_θ)-Cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2 - u, v^2 - vuv - vu\rangle$, *Des. Codes Cryptogr.* **90**(11) (2022), 2763-2781.

[48] V. Pless, On a new family of symmetry codes and related new 5-designs, *Bull. AMS*, **75** (1969), 1339-1342.

[49] E. Prange, Cyclic error-correcting codes in two symbols, *AFCRC-TN-57-I03, Air Force Cambridge Research Center,* Cambridge, Mass., Sept. 1957.

[50] E. Prange, Some cyclic error-correcting codes with simple decoding algorithms, *AFCRC-TN-58-156, Air Force Cambridge Research Center,* Bedford, Mass., April 1958.

[51] K.B. Reid and E. Brown, Doubly regular tournaments are equivalent to skew Hadamard matrices,*J. Combin. Theory Ser. A* **12**(3) (1972), 332-338.

[52] P. Shankar, On BCH codes over arbitrary integer rings, *IEEE Trans. Inform. Theory* **25**(4) (1979), 480-483.

[53] C.E. Shannon, A mathematical theory of communication, *Bell System Tech. J.* **27**(3) (1948), 379-423, and **27**(4) (1948), 623-656.

[54] A. Sharma and M. Bhaintwal, A class of skew cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with derivation, *Adv. Math. Commun.* **12**(4) (2018), 723-739.

[55] M. Shi and P. Solé, Three-weight codes, triple sum sets, and strongly walk regular graphs, *Des. Codes Cryptogr.* **87**(10) (2019), 2395-2404.

[56] M. Shi, T. Helleseth, and P. Solé, Strongly regular graphs from reducible cyclic codes, *J. Algebraic Combin.* **55**(1) (2022), 173-184.

[57] E. Spiegel, Code over $\mathbb{Z}_m$, *Inf. Control* **35** (1977), 48-51.

[58] E. Spiegel, Codes over $\mathbb{Z}_m$, revisited, *Inf. Control* **37** (1978), 100-104.

[59] D. Suprijanto and T. Nugraha, A note on linear codes from Johnson graphs, *JP Journal of Algebra Number Theory App.* **38**(5) (2016), 473-488.

[60] D. Suprijanto and H.C. Tang, Skew cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with derivation, *submitted* (2023).

[61] D. Suprijanto and H.C. Tang, Quantum codes constructed from cyclic codes over a finite non-chain ring, *IAENG Int. J. Comput. Sci.* **49**(3) (2022), 695-700.

[62] D. Suprijanto and Irwansyah, Constacyclic codes over the ring B_k and quantum codes, (tentative title, a work in preparation).

[63] H. Tapia-Recilias and G. Vega, Some constacyclic codes over $\mathbb{Z}_{2^k}$ and binary quasi-cyclic codes, *Discrete Appl. Math.* **128**(1 SPEC) (2003), 305-316.

[64] H.C. Tang and D. Suprijanto, New optimal linear codes over $\mathbb{Z}_4$, *Bull. Aust. Math. Soc.* **107**(1) (2023), 158-169.

[65] H.C. Tang and D. Suprijanto, A general family of Plotkin-optimal two-weight codes over $\mathbb{Z}_4$, *Des, Codes Cryptogr.* **91**(5) (2023), 1737-1750.

[66] V.D. Tonchev, Binary codes derived from the Hoffman–Singleton and Higman–Sims graphs, *IEEE Trans. Inform. Theory* **43**(3) (1997), 1021-1025.

[67] V.D. Tonchev, Codes and Designs, in: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, Chapter 15, Elsevier, Amsterdam, 1998, pp. 1229-1267.

[68] V.D. Tonchev, Error-correcting codes from graphs, *Discr. Math.* **257**(2-3) (2002), 549-557.

[69] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **45**(7) (1999), 2527-2532.

[70] J. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* **121** (1999), 555-575.