Palestine Journal of Mathematics

Vol. 12(2)(2023) , 395–407

Reversible cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$

Nadeem ur Rehman, Mohd Azmi and Ghulam Mohammad

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 94B05; Secondary 95B15.

Keywords and phrases: Cyclic codes, Codes over rings, Hamming distance, Generator Polynomial.

Abstract In this article, we inspect the structure of reversible cyclic codes over the ring $\mathbb{S} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$, where $u^k = 0$. We determine a unique set of generators for cyclic codes over $\mathbb{S}$. We classify reversible cyclic codes with respect to their generators. We also give the condition for the dual of reversible cyclic codes of odd length over $\mathbb{S}$ to be reversible. Further, we have provided some examples of reversible cyclic codes in support of our work.

1 Introduction

Linear codes over finite rings draw much attention in the field of algebraic coding theory in the early 1970s. Following the achievement of the Gray maps, the research on the finite rings was motivated. A remarkable paper by Hammons et al. [1] has shown that some good non-linear binary codes can be viewed as an image of linear codes over $\mathbb{Z}_4$ under the Gray map. Since then, many families of codes have been studied over numerous finite rings like $\mathbb{Z}_4$, $\mathbb{F}_2 + v\mathbb{F}_2, v^2 = v$; $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0$; $\mathbb{Z}_{p^r} + u\mathbb{Z}_{p^r} + \cdots + u^{k-1}\mathbb{Z}_{p^r}, u^k = 0$ where p is a prime. In addition, cyclic codes are linear block codes in which the cyclic shift of each codeword is again the codeword. This is often known to be a central family of linear codes due to their rich algebraic properties. Such codes have been explored over numerous finite rings, and several new codes and different outcomes have been obtained in [2, 4, 5].

The characteristic properties of reversible cyclic codes were first described in 1964 by James L. Massey [6]. In 2007, the construction of reversible cyclic codes over $\mathbb{Z}_4$ was given by Siap and Abualrub [3]. In 2015, reversible cyclic codes were analyzed by Srinivasulu B and Bhaintwal [8] over $\mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$ and their consequences for DNA codes.

We examine reversible cyclic codes of arbitrary length n over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+\cdots+u^{k-1}\mathbb{F}_2$, $u^k = 0$. In DNA computing, building data storage and retrieval schemes, reversible cyclic codes have wide applications. The structure of DNA is used as a model for constructing good error-correcting codes, and conversely, error-correcting codes that show similar properties to DNA structure are also used to understand DNA itself.

First of all, in this article, we provide a few preliminary details in Section 2, while the structure of cyclic codes of arbitrary length n over the ring $\mathbb{S}$ is discussed in Section 3. The Section 4 has some important results over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ on reversible cyclic codes. We explore the dual reversible cyclic codes in Section 5. We discuss the minimum Hamming distance of reversible cyclic code in Section 6. Finally, we provide some examples in support of our conclusions in Section 7.

2 Preliminaries

In the remaining sections, we suppose that $\mathbb{S} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$, where $u^k = 0$. Also, we notice that this ring $\mathbb{S}$ is a commutative chain ring having 2^k elements with maximal ideal $u\mathbb{S}$. Also, u is nilpotent with nilpotent index k. Moreover $\mathbb{S}/u\mathbb{S} \cong \mathbb{F}_2$ is the residue field and $|u^i\mathbb{S}| = 2|(u^{i+1}\mathbb{S})| = 2^{k-i}$, $i = 0, 1, 2, \cdots, k-1$.

Here $\mathbb{S}_1 = \mathbb{F}_2 = \{0, 1\}$, $\mathbb{S}_2 = \mathbb{F}_2 + u\mathbb{F}_2$, $\mathbb{S}_3 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, . . . , etc.

A linear code $\mathscr{A}$ of length n over the ring $\mathbb{S} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ is an $\mathbb{S}$-submodule of $\mathbb{S}^n$. A linear code $\mathscr{A}$ is said to be a cyclic code if it is closed with respect to the cyclic shift, i.e., $(e_{n-1}, e_0, \ldots, e_{n-2}) \in \mathscr{A}$ whenever $(e_0, e_1, \ldots, e_{n-2}, e_{n-1}) \in$

$\mathscr{A}$. Also, cyclic code over $\mathbb{S}$ can be viewed as an ideal in $\mathbb{S}_n = \mathbb{S}[\vartheta]/\langle\vartheta^n - 1\rangle$ identifying $(e_0, e_1, e_2, \ldots, e_{n-2}, e_{n-1})$ by $e_0 + e_1\vartheta + e_2\vartheta^2 + \ldots + e_{n-2}\vartheta^{n-2} + e_{n-1}\vartheta^{n-1}$.

The Hamming weight of any codeword is the number of non-zero coordinates in it, and the Hamming distance between any two codewords is the number of the components in which these two codewords differ. Also, for a linear code $\mathscr{A}$, the minimum Hamming distance is equal to the minimum Hamming weight of $\mathscr{A}$, i.e., $d(\mathscr{A}) = w_H(\mathscr{A})$. For each polynomial $f(\vartheta) = f_0 + f_1\vartheta + \ldots + f_{n-1}\vartheta^{n-1} \in \mathbb{S}[\vartheta]/\langle\vartheta^n - 1\rangle$ with $f_{n-1} \neq 0$, the reciprocal of $f(\vartheta)$ is defined to be the poynomial $f^*(\vartheta) = \vartheta^{n-1}f(1/\vartheta) = f_{n-1} + f_{n-2}\vartheta + \ldots + f_0\vartheta^{n-1}$. We also note that $\deg f^*(\vartheta) \leq \deg f(\vartheta)$, and if $f_0 \neq 0$, then $\deg f^*(\vartheta) = \deg f(\vartheta)$. We say that $f(\vartheta)$ is self reciprocal if and only if $f^*(\vartheta) = f(\vartheta)$. Also for any two polynomials $f(\vartheta)$, $g(\vartheta)$ satisfying $f(\vartheta) \mid g(\vartheta)$ implies $f^*(\vartheta) \mid g^*(\vartheta)$.

3 Construction of cyclic codes over $\mathbb{S}$

The structure of cyclic codes over $\mathbb{S}_i$ depends on cyclic codes over $\mathbb{S}_{i-1}$ for $i = 2, 3, \ldots k$ and the structure of cyclic codes over $\mathbb{S}_2$ depends on cyclic codes over $\mathbb{S}_1 = \mathbb{F}_2$.

Now, let $\mathscr{A}_1$ be a cyclic code in $\mathbb{S}_{k,n} = \mathbb{S}_k[\vartheta]/\langle\vartheta^n - 1\rangle$.
Define $\psi_1 : \mathbb{S}_k \to \mathbb{S}_{k-1}$ by $\psi_1(a) = a$. ψ_1 is a ring homomorphism that can be extended to a homomorphism $\eta_1 : \mathscr{A}_1 \to \mathbb{S}_{k-1,n} = \mathbb{S}_{k-1}[\vartheta]/\langle\vartheta^n - 1\rangle$ defined by

$$\eta_1(c_0 + c_1\vartheta + c_2\vartheta^2 + \cdots + c_{n-2}\vartheta^{n-2} + c_{n-1}\vartheta^{n-1}) = \psi_1(c_0) + \psi_1(c_1)\vartheta + \ldots + \psi_1(c_{n-1})\vartheta^{n-1}.$$

Let $T_1 = \{r(\vartheta) : u^{k-1}r(\vartheta) \in \ker\eta_1\}$. Then T_1 is an ideal in $\mathbb{S}_{1,n} = \mathbb{S}_1[\vartheta]/\langle\vartheta^n - 1\rangle = \mathbb{F}_2[\vartheta]/\langle\vartheta^n - 1\rangle$ and hence a cyclic code in $\mathbb{F}_2[\vartheta]/\langle\vartheta^n - 1\rangle$. It is clear that T_1 is an ideal in $\mathbb{F}_2[\vartheta]/\langle\vartheta^n - 1\rangle$ and hence a cyclic code in $\mathbb{F}_2[\vartheta]/\langle\vartheta^n - 1\rangle$. So $T_1 = \langle\alpha_{k-1}(\vartheta)\rangle$ and $\ker\eta_1 = \langle u^{k-1}\alpha_{k-1}(\vartheta)\rangle$ with $\alpha_{k-1}(\vartheta) \mid \langle\vartheta^n - 1\rangle$.

Let $\mathscr{A}_2$ be a cyclic code in $\mathbb{S}_{k-1,n} = \mathbb{S}_{k-1}[\vartheta]/\langle\vartheta^n - 1\rangle$.
Define $\psi_1 : \mathbb{S}_{k-1} \to \mathbb{S}_{k-2}$ by $\psi_2(a) = a$. ψ_2 is a ring homomorphism that can be extended to a homomorphism $\eta_2 : \mathscr{A}_2 \to \mathbb{S}_{k-2}[\vartheta]/\langle\vartheta^n - 1\rangle$ defined by

$$\eta_2(c_0 + c_1\vartheta + c_2\vartheta^2 + \cdots + c_{n-2}\vartheta^{n-2} + c_{n-1}\vartheta^{n-1}) = \psi_2(c_0) + \psi_2(c_1)\vartheta + \ldots + \psi_2(c_{n-1})\vartheta^{n-1}.$$

Let $T_2 = \{r(\vartheta) : u^{k-2}r(\vartheta) \in \ker\eta_2\}$ be an ideal in $\mathbb{S}_{1,n} = \mathbb{F}_2[\vartheta]/\langle\vartheta^n - 1\rangle$ and hence a cyclic code in $\mathbb{F}_2[\vartheta]/\langle\vartheta^n - 1\rangle$. So $T_2 = \langle\alpha_{k-2}(\vartheta)\rangle$ and hence $\ker\eta_2 = \langle u^{k-2}\alpha_{k-2}(\vartheta)\rangle$ with $\alpha_{k-2}(\vartheta) \mid \langle\vartheta^n - 1\rangle$.

Let $\mathscr{A}_3$ be a cyclic code in $\mathbb{S}_{k-2,n} = \mathbb{S}_{k-2}[\vartheta]/\langle\vartheta^n - 1\rangle$.
Define $\psi_3 : \mathbb{S}_{k-2} \to \mathbb{S}_{k-3}$ by $\psi_3(a) = a$. ψ_3 is a ring homomorphism that can be extended to a homomorphism $\eta_3 : \mathscr{A}_3 \to \mathbb{S}_{k-3}[\vartheta]/\langle\vartheta^n - 1\rangle$. Continue in the same way as above until we define $\psi_k : \mathbb{S}_2 \to \mathbb{S}_1 = \mathbb{F}_2$ by $\psi_k(a) = a^2$. ψ_k is a ring homomorphism because $(a+b)^2 = a^2 + b^2$ in $\mathbb{S}_2$ and in $\mathbb{F}_2$.
Extend ψ_k to a homomorphism $\eta_k : \mathscr{A}_k \to \mathbb{F}_2(\vartheta)/\langle\vartheta^n - 1\rangle$ defined by

$$\eta_k(c_0 + c_1\vartheta + c_2\vartheta^2 + \cdots + c_{n-2}\vartheta^{n-2} + c_{n-1}\vartheta^{n-1}) = \psi_k(c_0) + \psi_k(c_1)\vartheta + \ldots + \psi_k(c_{n-1})\vartheta^{n-1}.$$

$$= c_0^2 + c_1^2\vartheta + \ldots + c_{n-1}^2\vartheta^{n-1}$$

where $\mathscr{A}_k$ is a cyclic code in $\mathbb{S}_{2,n} = \mathbb{S}_2[\vartheta]/\langle\vartheta^n - 1\rangle$, $\mathbb{S}_2 = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and $\ker\eta_k = \langle u\alpha_1(\vartheta)\rangle$ with $\alpha_1(\vartheta) \mid (\vartheta^n - 1)$.

The image of η_k is also an ideal and hence a binary cyclic code generated by g(ϑ) with $g(\vartheta) \mid (\vartheta^n - 1)$. So, $\mathscr{A}_k = \langle g(\vartheta) + up(\vartheta), u\alpha_1(\vartheta)\rangle$ for some binary polynomial $p(\vartheta)$. Note that $\alpha_1 \mid \left(p\frac{\vartheta^n - 1}{g}\right)$ because $\eta_k\left(\frac{\vartheta^n - 1}{g}[g + up]\right) = \eta_k\left(up\frac{\vartheta^n - 1}{g}\right) = 0$ implies $\left(up\frac{\vartheta^n - 1}{g}\right) \in \ker\eta_k = \langle u\alpha_1(\vartheta)\rangle$. Also $ug \in \ker\eta_k$. Therefore, $\alpha_1(\vartheta) \mid g(\vartheta)$.

We have begun with the theorem due to M. Al-ashker and M. Hamoudeh [11], which classifies all the cyclic codes in $\mathbb{S}_n$.

Theorem 3.1. *[11, Theorem 3.6] Let $\mathscr{A}_1$ be a cyclic code in $\mathbb{S}_{k,n} = \mathbb{S}_k[\vartheta]/\langle \vartheta^n - 1\rangle$, $\mathbb{S}_k = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^{k-1}\mathbb{F}_2$ with $u^k = 0$.*

(1) *If n is odd, then $\mathbb{S}_{k,n}$ is a principal ideal ring and*

$$\mathscr{A}_1 = \langle g, u\alpha_1, u^2\alpha_2, \ldots, u^{k-1}\alpha_{k-1}\rangle = \langle g + u\alpha_1 + u^2\alpha_2 + \ldots + u^{k-1}\alpha_{k-1}\rangle,$$

where $g(\vartheta), \alpha_1(\vartheta), \alpha_2(\vartheta), \ldots, \alpha_{k-1}(\vartheta)$ are binary polynomials with $\alpha_{k-1}(\vartheta) \mid \alpha_{k-2}(\vartheta) \mid \ldots \mid \alpha_2(\vartheta) \mid \alpha_1(\vartheta) \mid g(\vartheta) \mid (\vartheta^n - 1)$.

(2) *If n is not odd, then*

(a) *$\mathscr{A}_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}\rangle$ where $g(\vartheta)$, $p_i(\vartheta)$ are binary polynomials for $i = 1, 2, \ldots, k-1$ with $g(\vartheta) \mid (\vartheta^n - 1)$, $(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}) \mid (\vartheta^n - 1)$ in $\mathbb{S}_k$ and $\deg p_i < \deg p_{i-1}$ for all $2 \le i \le k-1$. OR,*

(b) *$\mathscr{A}_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, u^{k-1}\alpha_{k-1}\rangle$ where $\alpha_{k-1}(\vartheta) \mid g(\vartheta) \mid (\vartheta^n - 1)$, $(g + up) \mid (\vartheta^n - 1)$ in $\mathbb{S}_2$, and $g(\vartheta) \mid p_1(\vartheta)\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)$ and $\alpha_{k-1}(\vartheta) \mid p_1(\vartheta)\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)$, and $\alpha_{k-1}(\vartheta) \mid p_2(\vartheta)\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)$, … and $\alpha_{k-1}(\vartheta) \mid p_{k-1}(\vartheta)\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)\cdots\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)$ ($k-1$ times) and $\deg p_{k-1} < \deg \alpha_{k-1}$. OR,*

(c) *$\mathscr{A}_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, u\alpha_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2\alpha_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}\alpha_{k-2} + u^{k-1}t_1, u^{k-1}\alpha_{k-1}\rangle$ with $\alpha_{k-1}(\vartheta) \mid \alpha_{k-2}(\vartheta) \mid \ldots \alpha_2(\vartheta) \mid \alpha_1(\vartheta) \mid g(\vartheta) \mid (\vartheta^n - 1)$, $\alpha_1(\vartheta) \mid p_1(\vartheta)\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)$ and $\alpha_{k-2}(\vartheta) \mid p_1\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right), \ldots, \alpha_{k-1}(\vartheta) \mid t_1\left(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\right), \ldots,$ $, \alpha_{k-1}(\vartheta) \mid p_{k-1}\left(\frac{\vartheta^n - 1}{g(\vartheta)}\right)\cdots\left(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\right)$.*

Moreover, $\deg p_{k-1} < \deg \alpha_{k-1}, \ldots$, $\deg t_1 < \deg \alpha_{k-1}, \ldots$ and $\deg p_1 < \deg \alpha_{k-2}$.

4 Reversible cyclic code over $\mathbb{S}$

This section is devoted to the study of reversible codes for even and odd lengths and finding the necessary and sufficient condition for a cyclic code $\mathscr{A}$ over $\mathbb{S}$ to be reversible. For any codeword $e = (e_0, e_1, \ldots, e_{n-2}, e_{n-1}) \in \mathscr{A}$, the reverse of the codeword is denoted by e^r and defined as $e^r = (e_{n-1}, e_{n-2}, \ldots, e_0)$.

Definition 4.1. A linear code $\mathscr{A}$ of length n over a ring R is said to be reversible if $\vartheta^r \in \mathscr{A}$, for all $\vartheta \in \mathscr{A}$.

In [6], Massey characterized cyclic codes to be reversible over the finite fields as follows:

Theorem 4.2. *[6, Theorem 1] The cyclic code over $GF(q)$ generated by the monic polynomial $g(\vartheta)$ is reversible if and only if $g(\vartheta)$ is self-reciprocal.*

We mention some results of Mostafanasab and Yousefian Darani [9], which are necessary to prove our results.

Lemma 4.3. *[9, Propsition 2.5] Let $\mathscr{A}$ be a cyclic code of length n over a commutative ring T and $f(\vartheta) \in T[\vartheta]/\langle \vartheta^n - 1\rangle$. Then $f(\vartheta)^r \in \mathscr{A}$ if and only if $f^*(\vartheta) \in \mathscr{A}$.*

Lemma 4.4. *[9, Corollary 2.6] Let $\mathscr{A}$ be a cyclic code. Then $\mathscr{A}$ is reversible if and only if $f^*(\vartheta) \in \mathscr{A}$, for all $f(\vartheta) \in \mathscr{A}$.*

Lemma 4.5. *[9, Lemma 2.7] Let $f_i(\vartheta), g_i(\vartheta) \in \mathbb{F}_2[\vartheta]$ for $i = 1, 2, 3, \ldots, k-1$. If*

$$f_1(\vartheta) + uf_2(\vartheta) + u^2 f_3(\vartheta) + \ldots + u^{k-1} f_k(\vartheta) = g_1(\vartheta) + ug_2(\vartheta) + u^2 g_3(\vartheta) + \ldots + u^{k-1} g_k(\vartheta).$$

Then $f_i(\vartheta) = g_i(\vartheta)$, for $i = 1, 2, 3, \ldots, k-1$.

Lemma 4.6. *[9, Lemma 2.11] Let $f_i(\vartheta) \in \mathbb{F}_2[\vartheta]$ for $i = 1, 2, 3, \ldots, k-1$. Suppose that* $\deg(f_1(\vartheta)) = i_1$, $\deg(f_2(\vartheta)) = i_2, \ldots, \deg(f_{k-1}(\vartheta)) = i_{k-1}$ *where $i_1 > max\{i_1, i_2, \ldots i_{k-1}\}$. Then*

$$(f_1(\vartheta) + uf_2(\vartheta) + u^2 f_3(\vartheta) + \ldots + u^{k-1} f_k(w))^* = f_1^*(\vartheta) + u\vartheta^{i_1 - i_2} f_2^*(\vartheta) + u^2 \vartheta^{i_1 - i_3} f_3^*(\vartheta) + \ldots + u^{k-1} \vartheta^{i_1 - i_{k-1}} f_k^*.$$

Lemma 4.7. *Let $\mathscr{A}$ be a reversible cyclic code of length n over the ring $\mathbb{S}$ and $\eta_k : \mathscr{A} \to \mathbb{F}_2[\vartheta]/\langle \vartheta^n - 1 \rangle$ as defined in the Section 3, be a ring homomorphism. Then $\eta_k(\mathscr{A})$ is reversible.*

Proof. Let $\eta_k(c) \in \eta_k(\mathscr{A})$, where $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathscr{A}$. Hence $\eta_k(c) = (c_0^2, c_1^2, \cdots, c_{n-1}^2) \in \eta_k(\mathscr{A})$. Now as $\mathscr{A}$ is a reversible cyclic code, we have $c^r = (c_{n-1}, c_{n-2}, \cdots, c_0) \in \mathscr{A}$. Now, consider

$$\begin{aligned} \eta_k(c)^r &= (c_0^2, c_1^2, \cdots, c_{n-1}^2)^r \\ &= (c_{n-1}^2, c_{n-2}^2, \cdots, c_0^2) \\ &= \eta_k(c_{n-1}, c_{n-2}, \cdots, c_0) \in \eta_k(\mathscr{A}). \end{aligned}$$

so $\eta_k(\mathscr{A})$ is reversible. □

Lemma 4.8. *Let $\mathscr{A}$ be a reversible cyclic code over $\mathbb{S}$. Then $\langle g(\vartheta) \rangle, \langle \alpha_1(\vartheta) \rangle, \langle \alpha_2(\vartheta) \rangle, \ldots, \langle \alpha_{k-1}(\vartheta) \rangle$ are also reversible cyclic codes over $\mathbb{F}_2$.*

Proof. From the construction of generators of cyclic codes over $\mathbb{S}$, we have $\eta(\mathscr{A}) = \langle g(\vartheta) \rangle$ and by Lemma 4.7, $\eta(\mathscr{A})$ is reversible code over $\mathbb{F}_2$. Therefore, $\langle g(\vartheta) \rangle$ is reversible cyclic code over $\mathbb{F}_2$.
As $\ker \eta_1 = \{u^{k-1} r(\vartheta) \mid r(\vartheta)$ is a polynomial in $\mathscr{A}$ with coefficients in $\mathbb{F}_2\}$ and $J_1 = \{r(\vartheta) \mid u^{k-1} r(\vartheta) \in \ker \eta_1\} = \langle \alpha_{k-1}(\vartheta) \rangle$, it is sufficient to show that J_1 is reversible. Let $\mathbb{S}(\vartheta) = r_0 + r_1\vartheta + \cdots + r_{n-1}\vartheta^{n-1} \in J_1$ be arbitrary. Then $\mathbb{S}(\vartheta) \in \mathbb{F}_2[\vartheta]$ is a polynomial in $\mathscr{A}$. Since $\mathscr{A}$ is reversible cyclic code in $\mathbb{S}$, $\mathbb{S}^*(\vartheta)$ is also in $\mathscr{A}$. Also $u^{k-1} r^*(\vartheta) \in \ker \eta_1$, $\mathbb{S}^*(\vartheta) \in J_1$. Hence, $\langle \alpha_{k-1}(\vartheta) \rangle$ is a reversible cyclic code.
In the similar way, $\ker \eta_2 = \{u^{k-2} t(\vartheta) \mid t(\vartheta)$ is a polynomial in $\mathscr{A}$ with coefficients in $\mathbb{F}_2\}$ and $J_2 = \{t(\vartheta) \mid u^{k-2} t(\vartheta) \in \ker \eta_2\} = \langle \alpha_{k-2}(\vartheta) \rangle$, it is sufficient to show that J_2 is reversible. Let $t(\vartheta) = t_0 + t_1\vartheta + \cdots + t_{n-1}\vartheta^{n-1} \in J_2$ be arbitrary. Then $t(\vartheta) \in \mathbb{F}_2[\vartheta]$ is a polynomial in $\mathscr{A}$. Since $\mathscr{A}$ is reversible cyclic code in $\mathbb{S}$, $t^*(\vartheta)$ is also in $\mathscr{A}$. Thus, $u^{k-2} t^*(\vartheta) \in \ker \eta_2$, $t^*(\vartheta) \in J_2$. Hence, $\langle \alpha_{k-2}(\vartheta) \rangle$ is also a reversible cyclic code.

Continuing in the same way we get $\ker \eta_k = \{ue(\vartheta) \mid e(\vartheta)$ is a polynomial in $\mathscr{A}$ with coefficients in $\mathbb{F}_2\}$ and $J_k = \{e(\vartheta) \mid ue(\vartheta) \in \ker \eta_k\} = \langle \alpha_1(\vartheta) \rangle$, it is sufficient to show that J_k is reversible. Let $e(\vartheta) = e_0 + e_1\vartheta + \cdots + e_{n-1}\vartheta^{n-1} \in J_k$ be arbitrary. Then $e(\vartheta) \in \mathbb{F}_2[\vartheta]$ is a polynomial in $\mathscr{A}$. Since $\mathscr{A}$ is reversible cyclic code in $\mathbb{S}$, $e^*(\vartheta)$ is also in $\mathscr{A}$. Thus, $ue^*(\vartheta) \in \ker \eta_k$, $e^*(\vartheta) \in J_k$. Hence, $\langle \alpha_1(\vartheta) \rangle$ is also a reversible cyclic code. □

Theorem 4.9. *Let $\mathscr{A} = \langle g(\vartheta), u\alpha_1(\vartheta), u^2\alpha_2(\vartheta), \ldots, u^{k-1}\alpha_{k-1}(\vartheta) \rangle = \langle g(\vartheta) + u\alpha_1(\vartheta) + u^2\alpha_2(\vartheta) + \cdots + u^{k-1}\alpha_{k-1}(\vartheta) \rangle$ be a linear cyclic code of odd length n over $\mathbb{S}$, where $g(\vartheta), \alpha_1(\vartheta), \alpha_2(\vartheta), \cdots, \alpha_{k-1}(\vartheta)$ are binary polynomials with $\alpha_{k-1}(\vartheta) \mid \alpha_{k-2}(\vartheta) \mid \ldots \mid \alpha_2(\vartheta) \mid \alpha_1(\vartheta) \mid g(\vartheta) \mid (\vartheta^n - 1)$. Then $\mathscr{A}$ is reversible if and only if $g(\vartheta), \alpha_1(\vartheta), \alpha_2(\vartheta), \ldots, \alpha_{k-1}(\vartheta)$ are self reciprocal.*

Proof. Let $\mathscr{A}$ be a reversible cyclic code over $\mathbb{S}$. Then by Lemma 4.8 , $g(\vartheta)$, $\alpha_1(\vartheta)$,$\alpha_2(\vartheta)$, $, \ldots, \alpha_{k-2}(\vartheta), \alpha_{k-1}(\vartheta)$ are self reciprocal.

For the sufficient part, we assume that $g(\vartheta)$, $\alpha_1(\vartheta)$, $\alpha_2(\vartheta), \ldots \alpha_{k-2}(\vartheta), \alpha_{k-1}(\vartheta)$ are binary self-reciprocal polynomials. Let $c(\vartheta) \in \mathscr{A}$ i.e., $c(\vartheta) = g(\vartheta)n_1(\vartheta) + u\alpha_1(\vartheta)n_2(\vartheta) + u^2\alpha_2(\vartheta)n_3(\vartheta) + \ldots + u^{k-2}\alpha_{k-2}(\vartheta)n_{k-1}(\vartheta) + u^{k-1}\alpha_{k-1}(\vartheta)n_k(\vartheta)$ for some polynomials $n_1(\vartheta)$, $n_2(\vartheta)$, $n_3(\vartheta), \ldots, n_k(\vartheta)$ over $\mathbb{S}$. Now, $\mathscr{A}$ is reversible if and only if $c^*(\vartheta) \in \mathscr{A}$.
For this consider

$$\begin{aligned} c^*(\vartheta) &= (g(\vartheta)n_1(\vartheta) + u\alpha_1(\vartheta)n_2(\vartheta) + u^2\alpha_2(\vartheta)n_3(\vartheta) + \ldots \\ &\quad + \ldots + u^{k-2}\alpha_{k-2}(\vartheta)n_{k-1}(\vartheta) + u^{k-1}\alpha_{k-1}(\vartheta)n_k(\vartheta))^* \\ &= (g^*(\vartheta)n_1^*(\vartheta) + u\vartheta^{i_1}\alpha_1^*(\vartheta)n_2^*(\vartheta) + u^2\vartheta^{i_2}\alpha_2^*(\vartheta)n_3^*(\vartheta) + \ldots \\ &\quad + \ldots + u^{k-1}\vartheta^{i_{k-1}}\alpha_{k-1}^*(\vartheta)n_k^*(\vartheta)) \\ &= (g(\vartheta)n_1^*(\vartheta) + u\alpha_1(\vartheta)\vartheta^{i_1}n_2^*(\vartheta) + u^2\alpha_2(\vartheta)\vartheta^{i_2}n_3^*(\vartheta) + \ldots \\ &\quad + \ldots + u^{k-1}\alpha_{k-1}(\vartheta)\vartheta^{i_{k-1}}n_k^*(\vartheta)) \end{aligned}$$

where $n_1^*(\vartheta), n_2^*(\vartheta), n_3^*(\vartheta), \ldots, n_k^*(\vartheta)$ are polyanomials over $\mathbb{S}$. This implies

$$c^*(\vartheta) \in \langle g(\vartheta), u\alpha_1(\vartheta), u^2\alpha_2(\vartheta), \ldots, u^{k-2}\alpha_{k-2}(\vartheta), u^{k-1}\alpha_{k-1}(\vartheta)\rangle.$$

Thus, $\mathscr{A}$ is a reversible cyclic code over $\mathbb{S}$. □

Theorem 4.10. *Let $\mathscr{A} = \langle g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta)\rangle$ where $\mathscr{A}$ is a cyclic code of length n over $\mathbb{S}$ such that n is even with $deg(g(\vartheta)) = i_1$, $deg(p_1(\vartheta)) = i_2$, $deg(p_2(\vartheta)) = i_3, \ldots, deg(p_{k-1}(\vartheta)) = i_k$, where $i_1 > max\{i_2, i_3, i_3, \ldots, i_{k-1}\}$. Then $\mathscr{A}$ is reversible cyclic code if and only if*

(1) *$g(\vartheta)$ is self reciprocal.*

(2) *$\vartheta^{i_1-i_k}p_{k-1}^*(\vartheta) = p_{k-1}(\vartheta) + t_1(\vartheta)p_{k-2}(\vartheta) + t_2(\vartheta)p_{k-3}(\vartheta) + \ldots + t_{k-2}(\vartheta)p_1(\vartheta) + t_{k-1}(\vartheta)g(\vartheta)$ where $t_i = \{0, 1\}$ for $1 \le i \le k-1$.*

Proof. Suppose that $\mathscr{A}$ is reversible . Consider $\mathscr{A}$ as an $\mathbb{S}[\vartheta]$ module. Then, by Lemma 4.6, it follows that

$$\begin{aligned} &(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta))^* \\ &\quad = g^*(\vartheta) + u\vartheta^{i_1-i_2}p_1^*(\vartheta) + u^2\vartheta^{i_1-i_3}p_2^*(\vartheta) + \ldots + u^{k-2}\vartheta^{i_1-i_{k-1}}p_{k-2}^*(\vartheta) \\ &\quad\quad + u^{k-1}\vartheta^{i_1-i_k}p_{k-1}^*(\vartheta) \\ &\quad = t(\vartheta)(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta)) \in \mathscr{A}. \end{aligned}$$

For some polynomial $t(\vartheta) \in \mathbb{S}[\vartheta]$. Let $t(\vartheta) = t_0(\vartheta) + ut_1(\vartheta) + u^2t_2(\vartheta) + \ldots + u^{k-1}t_{k-1}(\vartheta)$, where $t_i(\vartheta) \in \mathbb{F}_2[\vartheta]$. Then

$$\begin{aligned} &(g^*(\vartheta) + u\vartheta^{i_1-i_2}p_1^*(\vartheta) + u^2\vartheta^{i_1-i_3}p_2^*(\vartheta) + \ldots + u^{k-1}\vartheta^{i_1-i_k}p_{k-1}^*(\vartheta)) \\ &\quad = t_0(\vartheta)g(\vartheta) + u(t_1(\vartheta)g(\vartheta) + t_0(\vartheta)p_1(\vartheta)) + u^2(t_0(\vartheta)p_2(\vartheta) + t_1(\vartheta)p_1(\vartheta) + \\ &\quad\quad + t_2(\vartheta)g(\vartheta)) + \ldots + u^{k-1}(t_0(\vartheta)p_{k-1}(\vartheta) + t_1(\vartheta)p_{k-2}(\vartheta) + t_2(\vartheta)p_{k-3}(\vartheta) + \ldots \\ &\quad\quad + \ldots + t_{k-2}(\vartheta)p_1(\vartheta) + t_{k-1}(\vartheta)g(\vartheta)). \end{aligned}$$

Application of Lemma 4.5 implies that

$$\begin{aligned} g^*(\vartheta) &= t_0(\vartheta)g(\vartheta), \\ \vartheta^{i_1-i_2}p_1^*(\vartheta) &= t_0(\vartheta)p_1(\vartheta) + t_1(\vartheta)g(\vartheta) \\ \vartheta^{i_1-i_3}p_2^*(\vartheta) &= t_0(\vartheta)p_2(\vartheta) + t_1(\vartheta)p_1(\vartheta) + t_2(\vartheta)g(\vartheta) \\ \vartheta^{i_1-i_4}p_3^*(\vartheta) &= t_0(\vartheta)p_3(\vartheta) + t_1(\vartheta)p_2(\vartheta) + t_2(\vartheta)p_1(\vartheta) + t_3(\vartheta)g(\vartheta) \\ &\vdots \\ \vartheta^{i_1-i_k}p_{k-1}^*(\vartheta) &= t_0(\vartheta)p_{k-1}(\vartheta) + t_1(\vartheta)p_{k-2}(\vartheta) + t_2(\vartheta)p_{k-3}(\vartheta) + \ldots \\ &\quad + \ldots + t_{k-2}(\vartheta)p_1(\vartheta) + t_{k-1}(\vartheta)g(\vartheta). \end{aligned}$$

Now as $g^*(\vartheta) = t_0(\vartheta)g(\vartheta)$ and deg $g^*(\vartheta) \leq$ deg $g(\vartheta)$; we have that $t_0(\vartheta) = 1$ and so $g(\vartheta)$ is self reciprocal. Therefore

$$\begin{aligned} \vartheta^{i_1-i_2}p_1^*(\vartheta) &= p_1(\vartheta) + t_1(\vartheta)g(\vartheta) \\ \vartheta^{i_1-i_3}p_2^*(\vartheta) &= p_2(\vartheta) + t_1(\vartheta)p_1(\vartheta) + t_2(\vartheta)g(\vartheta) \\ \vartheta^{i_1-i_4}p_3^*(\vartheta) &= p_3(\vartheta) + t_1(\vartheta)p_2(\vartheta) + t_2(\vartheta)p_1(\vartheta) + t_3(\vartheta)g(\vartheta) \\ &\vdots \\ \vartheta^{i_1-i_k}p_{k-1}^*(\vartheta) &= p_{k-1}(\vartheta) + t_1(\vartheta)p_{k-2}(\vartheta) + t_2(\vartheta)p_{k-3}(\vartheta) + \ldots \\ &\quad + \ldots + t_{k-2}(\vartheta)p_1(\vartheta) + t_{k-1}(\vartheta)g(\vartheta). \end{aligned}$$

From here, comparing the degrees on both sides of this first equality gives us $t_1(\vartheta) = 0$ or 1. Similarly in, $\vartheta^{i_1-i_3}p_2^*(\vartheta) = p_2(\vartheta)+t_1(\vartheta)p_1(\vartheta)+t_2(\vartheta)g(\vartheta)$, comparing the degrees on both sides we get $t_2(\vartheta) = 0$ or 1 provided $t_1(\vartheta) = 0$ or 1 as we already mentioned.
Continuing in a similar manner, after comparing the degrees of the polynomials in each equation, we deduce that the only possibility for each $t_i{}'$s for $1 \leq i \leq k-1$ is either 0 or 1.
Therefore we can conclude that $\mathscr{A}$ is a reversible cyclic code when $g(\vartheta)$ is self reciprocal and $\vartheta^{i_1-i_k}p_{k-1}^*(\vartheta) = p_{k-1}(\vartheta) + t_1(\vartheta)p_{k-2}(\vartheta) + t_2(\vartheta)p_{k-3}(\vartheta) + \ldots + t_{k-2}(\vartheta)p_1(\vartheta) + t_{k-1}(\vartheta)g(\vartheta)$ where $t_i = \{0, 1\}$ for $1 \leq i \leq k-1$.

Conversely suppose that (1) holds and we are taking a particular case of (2) where each $t_i = 1$, then

$$\begin{aligned} &(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta))^* \\ &\quad = g^*(\vartheta) + u\vartheta^{i_1-i_2}p_1^*(\vartheta) + u^2\vartheta^{i_1-i_3}p_2^*(\vartheta) + \ldots \\ &\qquad + \ldots + u^{k-2}\vartheta^{i_1-i_{k-1}}p_{k-2}^*(\vartheta) + u^{k-1}\vartheta^{i_1-i_k}p_{k-1}^*(\vartheta) \\ &\quad = g(\vartheta) + u(p_1(\vartheta) + g(\vartheta)) + u^2(p_2(\vartheta) + p_1(\vartheta) + g(\vartheta)) + \ldots \\ &\qquad + \ldots + u^{k-1}(p_{k-1}(\vartheta) + p_{k-2}(\vartheta) + \ldots + g(\vartheta)) \\ &\quad = (g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}) \\ &\qquad + u(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}) \\ &\qquad + u^2(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}) + \ldots \\ &\qquad + \ldots + u^{k-1}(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}) \in \mathscr{A}. \end{aligned}$$

Thus $\mathscr{A}$ is a reversible cyclic code over $\mathbb{S}$. □

Theorem 4.11. *Let* $\mathscr{A} = \langle g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta), u^{k-1}\alpha_{k-1}(\vartheta)\rangle$ *be a cyclic code of even length* n *over* $\mathbb{S}$ *with* $deg(g(\vartheta)) = i_1$, $deg(p_1(\vartheta)) = i_2$, $deg(p_2(\vartheta)) = i_3, \ldots, deg(p_{k-1}(\vartheta)) = i_k$, *where* $i_1 > max\{i_2, i_3, i_4, \ldots, i_{k-1}\}$. *Also* $\alpha_{k-1}(\vartheta) \mid g(\vartheta) \mid (\vartheta^n - 1)$. *Then* $\mathscr{A}$ *is reversible cyclic code iff*

(1) *$g(\vartheta)$ and $\alpha_{k-1}(\vartheta)$ are self reciprocal.*

(2) $\alpha_{k-1}(\vartheta) \mid \vartheta^{i_1-i_k}p^*_{k-1}(\vartheta) + p_{k-1}(\vartheta) + l_1(\vartheta)p_{k-2}(\vartheta) + l_2(\vartheta)p_{k-3}(\vartheta) + \ldots + l_{k-2}(\vartheta)p_1(\vartheta)$.

Proof. Assume that $\mathscr{A}$ is reversible. Notice that there are two polynomials $l(\vartheta)$, $q(\vartheta) \in \mathbb{S}[\vartheta]$ such that

$$\begin{aligned}
&(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta))^* \\
&= g^*(\vartheta) + u\vartheta^{i_1-i_2}p_1^*(\vartheta) + u^2\vartheta^{i_1-i_3}p_2^*(\vartheta) + \ldots \\
&\quad + \ldots + u^{k-2}\vartheta^{i_1-i_{k-1}}p^*_{k-2}(\vartheta) + u^{k-1}\vartheta^{i_1-i_k}p^*_{k-1}(\vartheta) \\
&= g(\vartheta) + u\vartheta^{i_1-i_2}p_1^*(\vartheta) + u^2\vartheta^{i_1-i_3}p_2^*(\vartheta) + \ldots \\
&\quad + \ldots + u^{k-2}\vartheta^{i_1-i_{k-1}}p^*_{k-2}(\vartheta) + u^{k-1}\vartheta^{i_1-i_k}p^*_{k-1}(\vartheta) \\
&= l(\vartheta)(g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta)) \\
&\quad + u^{k-1}q(\vartheta)\alpha_{k-1}(\vartheta) \in \mathscr{A}.
\end{aligned}$$

Let $l(\vartheta) = l_0(\vartheta) + ul_1(\vartheta) + u^2l_2(\vartheta) + \ldots + u^{k-1}l_{k-1}(\vartheta)$, where $l_i(\vartheta)$'s are polynomials in $\mathbb{F}_2[\vartheta]$. Also we can assume that $q(\vartheta) \in \mathbb{F}_2[\vartheta]$. Thus,

$$\begin{aligned}
&(g^*(\vartheta) + u\vartheta^{i_1-i_2}p_1^*(\vartheta) + u^2\vartheta^{i_1-i_3}p_2^*(\vartheta) + \ldots + u^{k-2}\vartheta^{i_1-i_{k-1}}p^*_{k-2}(\vartheta) + u^{k-1}\vartheta^{i_1-i_k}p^*_{k-1}(\vartheta)) \\
&= l_0(\vartheta)g(\vartheta) + u(l_0(\vartheta)p_1(\vartheta) + l_1(\vartheta)g(\vartheta)) + u^2(l_0(\vartheta)p_2(\vartheta) + l_1(\vartheta)p_1(\vartheta) + l_2(\vartheta)g(\vartheta)) \\
&\quad + \ldots + u^{k-1}(l_0(\vartheta)p_{k-1}(\vartheta) + l_1(\vartheta)p_{k-2}(\vartheta) + \ldots + l_{k-1}(\vartheta)g(\vartheta) + q(\vartheta)\alpha_{k-1}(\vartheta)).
\end{aligned}$$

Similar to the proof of 4.10, we deduce that $g(\vartheta)$ is self-reciprocal. Also $l_0(\vartheta) = 1$ and rest $l_i's = 0$ or 1, for $1 \le i \le k-1$. Here, we are interested in that case only when $l_{k-2}(\vartheta) = 0$ or 1, then

$$\begin{aligned}
\vartheta^{i_1-i_2}p_1^*(\vartheta) &= p_1(\vartheta) + l_1(\vartheta)g(\vartheta) \\
\vartheta^{i_1-i_3}p_2^*(\vartheta) &= p_2(\vartheta) + l_1(\vartheta)p_1(\vartheta) + l_2(\vartheta)g(\vartheta) \\
\vartheta^{i_1-i_4}p_3^*(\vartheta) &= p_3(\vartheta) + l_1(\vartheta)p_2(\vartheta) + l_2(\vartheta)p_1(\vartheta) + l_3(\vartheta)g(\vartheta) \\
&\vdots \\
\vartheta^{i_1-i_k}p^*_{k-1}(\vartheta) &= p_{k-1}(\vartheta) + l_1(\vartheta)p_{k-2}(\vartheta) + l_2(\vartheta)p_{k-3}(\vartheta) + \ldots \\
&\quad \ldots + l_{k-2}(\vartheta)p_1(\vartheta) + l_{k-1}(\vartheta)g(\vartheta) + q(\vartheta)\alpha_{k-1}(\vartheta).
\end{aligned}$$

Since, $\alpha_{k-1}(\vartheta) \mid g(\vartheta) \mid \langle \vartheta^n - 1\rangle$.

So, $\alpha_{k-1}(\vartheta) \mid \vartheta^{i_1-i_k}p^*_{k-1}(\vartheta) + p_{k-1}(\vartheta) + l_1(\vartheta)p_{k-2}(\vartheta) + l_2(\vartheta)p_{k-3}(\vartheta) + \ldots + l_{k-2}(\vartheta)p_1(\vartheta)$. Moreover, $u^{k-1}\alpha^*_{k-1}(\vartheta) \in \mathscr{A}$. Then, there exist polynomials $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_{k-2}, \lambda_{k-1} \in \mathbb{S}[\vartheta]$ and $\delta \in \mathbb{F}_2[\vartheta]$ such that

$$\begin{aligned}
u^{k-1}\alpha^*_{k-1}(\vartheta) &= l_0(\vartheta)g(\vartheta) + u(l_0(\vartheta)p_1(\vartheta) + l_1(\vartheta)g(\vartheta)) \\
&\quad + u^2(l_0(\vartheta)p_2(\vartheta) + l_1(\vartheta)p_1(\vartheta) + l_2(\vartheta)g(\vartheta)) \\
&\quad + \ldots + u^{k-1}(\lambda_0(\vartheta)p_{k-1}(\vartheta) + \lambda_1(\vartheta)p_{k-2}(\vartheta) + \ldots \\
&\quad + \ldots + \lambda_{k-1}(\vartheta)g(\vartheta) + \delta(\vartheta)\alpha_{k-1}(\vartheta)).
\end{aligned}$$

Therefore $\lambda_0=\lambda_1=\lambda_2=\lambda_3=\ldots=\lambda_{k-2} = 0$ and $\alpha^*_{k-1}(\vartheta) = \lambda_{k-1}(\vartheta)g(\vartheta) + \delta(\vartheta)\alpha_{k-1}(\vartheta)$. Since $\alpha_{k-1}(\vartheta) \mid g(\vartheta)$, we have $\alpha_{k-1}(\vartheta) \mid \alpha^*_{k-1}(\vartheta)$ and so $\alpha^*_{k-1}(\vartheta) = \alpha_{k-1}(\vartheta)$, i.e., $\alpha_{k-1}(\vartheta)$ is self-reciprocal.

Conversely suppose that $g(\vartheta)$ and $\alpha_{k-1}(\vartheta)$ are self reciprocal and condition (2) also holds. Then

$$\begin{aligned}
&(g(\vartheta) + up_1(\vartheta) + u^2 p_2(\vartheta) + \ldots + u^{k-1} p_{k-1}(\vartheta))^* \\
&\quad = g^*(\vartheta) + u\vartheta^{i_1-i_2} p_1^*(\vartheta) + u^2 \vartheta^{i_1-i_3} p_2^*(\vartheta) + \ldots \\
&\qquad + \ldots + u^{k-2} \vartheta^{i_1-i_{k-1}} p_{k-2}^*(\vartheta) + u^{k-1} \vartheta^{i_1-i_k} p_{k-1}^*(\vartheta). \\
&\quad = g(\vartheta) + u(p_1(\vartheta) + l_1(\vartheta) g(\vartheta)) + u^2(p_2(\vartheta) + l_1(\vartheta) p_1(\vartheta) + l_2(\vartheta) g(\vartheta)) + \ldots \\
&\qquad + u^{k-1}(p_{k-1}(\vartheta) + l_1(\vartheta) p_{k-2}(\vartheta) + l_2(\vartheta) p_{k-3}(\vartheta) + \ldots \\
&\qquad + \ldots + l_{k-1}(\vartheta) g(\vartheta) + \lambda(\vartheta)\alpha_2(\vartheta)). \\
&\quad = (g(\vartheta) + up_1(\vartheta) + u^2 p_2(\vartheta) + \ldots + u^{k-1} p_{k-1}(\vartheta)) \\
&\qquad + u(l_1(\vartheta)(g(\vartheta) + up_1(\vartheta) + u^2 p_2(\vartheta) + \ldots + u^{k-1} p_{k-1}(\vartheta))) \\
&\qquad + u^2(l_2(\vartheta)(g(\vartheta) + up_1(\vartheta) + u^2 p_2(\vartheta) + \ldots + u^{k-1} p_{k-1}(\vartheta))) + \ldots \\
&\qquad + \ldots + u^{k-1}(l_{k-1}(\vartheta)(g(\vartheta) + up_1(\vartheta) + u^2 p_2(\vartheta) + \ldots + u^{k-1} p_{k-1}(\vartheta))) \\
&\qquad + \lambda(\vartheta) u^{k-1}(\alpha_{k-1}(\vartheta)) \in \mathscr{A}.
\end{aligned}$$

Since each $l_i \in \{0,1\}$ for $1 \leq i \leq k-1$, in all the cases whichever the value $l_i's$ take $(g(\vartheta) + up_1(\vartheta) + u^2 p_2(\vartheta) + \ldots + u^{k-1} p_{k-1}(\vartheta))^* \in \mathscr{A}$. Therefore $\mathscr{A}$ is a reversible cyclic code. □

5 Dual of reversible cyclic code over $\mathbb{S}$

Let $\mathscr{A}$ be a cyclic $[n,k]$-code with parity check polynomial $b(\vartheta) = b_0 + b_1\vartheta + \cdots + b_k\vartheta^k$ and $\bar{b}(\vartheta) = b^*(\vartheta)$. Then for the characterization of $\mathscr{A}^\perp$ of cyclic code $\mathscr{A}$, we have the following result.

Theorem 5.1. *Let $\mathscr{A}^\perp$ be a dual code of a cyclic code $\mathscr{A}$ over $GF(q)$. Then $\mathscr{A}^\perp =< \bar{b}(\vartheta) >$ is reversible iff $b(\vartheta) \in \mathscr{A}^\perp$.*

Proof. Let $\bar{b}(\vartheta) = (b_k, b_{k-1}, \cdots, b_0) \in \mathscr{A}^\perp$. Then $(\bar{b}(\vartheta))^r = (b_0, b_1, \cdots, b_{k-1}, b_k) = b(\vartheta) \in \mathscr{A}^\perp$.
Conversely, suppose that $b(\vartheta) \in \mathscr{A}^\perp$, then $b(\vartheta) = (\bar{b}(\vartheta))^r$ which means $\bar{b}(\vartheta)^r = b(\vartheta) \in \mathscr{A}^\perp$. Hence $\mathscr{A}^\perp =< \bar{b}(\vartheta) >$ is reversible cyclic code. □

Definition 5.2. For any ideal J in $\mathbb{S}_n$; the annihilator $\mathbb{Q}(J)$ of J in $\mathbb{S}_n$ is defined as

$$\mathbb{Q}(J) = \{d(\vartheta) \mid f(\vartheta)d(\vartheta) = 0 \quad \forall f(\vartheta) \in J\}.$$

Also associated ideal of $\mathscr{A}^\perp$ of cyclic code $\mathscr{A}$ is

$$\mathbb{Q}(J)^* = \{c^*(\vartheta) \mid c(\vartheta) \in J\}.$$

Proposition 5.3. *Let $\mathscr{A}$ be a cyclic code of odd length n over $\mathbb{S}$. Then*

$$\mathbb{Q}(\mathscr{A}) = \Big\langle \frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}, \quad u\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}, \quad u^2\frac{\vartheta^n - 1}{\alpha_{k-3}(\vartheta)}, \ldots\ldots, u^{k-1}\frac{\vartheta^n - 1}{g(\vartheta)} \Big\rangle,$$

where $\mathbb{Q}(\mathscr{A})$ is the annihilator of $\mathscr{A}$.

Proof. It is given that $\mathscr{A}$ is a cyclic code of odd length over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^{k-1}\mathbb{F}_2$, we have

$$\begin{aligned}
\mathscr{A} &= \langle g(\vartheta), u\alpha_1(\vartheta), u^2\alpha_2(\vartheta), \ldots, u^{k-1}\alpha_{k-1}(\vartheta)\rangle \\
&= \langle g(\vartheta) + u\alpha_1(\vartheta) + u^2\alpha_2(\vartheta) + \ldots + u^{k-1}\alpha_{k-1}(\vartheta)\rangle
\end{aligned}$$

where $\alpha_{k-1}(\vartheta) \mid \alpha_{k-2}(\vartheta) \mid \dots \mid \alpha_2(\vartheta) \mid \alpha_1(\vartheta) \mid g(\vartheta) \mid (\vartheta^n - 1)$. Also, there exists $n_1(\vartheta), n_2(\vartheta), \dots, n_{k-1}(\vartheta), m_2(\vartheta), m_3(\vartheta), \dots, m_{k-1}(\vartheta), o_3(\vartheta), o_4(\vartheta), \dots, o_{k-1}(\vartheta), \dots, y_{k-2}(\vartheta), y_{k-1}(\vartheta)$ and $z_{k-1}(\vartheta)$ such that

$$\begin{aligned}
g(\vartheta) &= \alpha_1(\vartheta)n_1(\vartheta), \;\; g(\vartheta) = \alpha_2(\vartheta)n_2(\vartheta), \dots, g(\vartheta) = \alpha_{k-1}(\vartheta)n_{k-1}(\vartheta),\\
\alpha_1(\vartheta) &= \alpha_2(\vartheta)m_2(\vartheta), \;\; \alpha_1(\vartheta) = \alpha_3(\vartheta)m_3(\vartheta), \dots, \alpha_1(\vartheta) = \alpha_{k-1}(\vartheta)m_{k-1}(\vartheta),\\
\alpha_2(\vartheta) &= \alpha_3(\vartheta)o_3(\vartheta), \;\; \alpha_2(\vartheta) = \alpha_4(\vartheta)o_4(\vartheta), \dots, \alpha_2(\vartheta) = \alpha_{k-1}(\vartheta)o_{k-1}(\vartheta),\\
&\vdots\\
\alpha_{k-3}(\vartheta) &= \alpha_{k-2}(\vartheta)y_{k-2}(\vartheta), \;\; \alpha_{k-3}(\vartheta) = \alpha_{k-1}(\vartheta)y_{k-1}(\vartheta),\\
\alpha_{k-2}(\vartheta) &= \alpha_{k-1}(\vartheta)z_{k-1}(\vartheta).
\end{aligned}$$

Notice that

$$\begin{aligned}
&\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)(g(\vartheta) + u\alpha_1(\vartheta) + u^2\alpha_2(\vartheta) + \dots + u^{k-1}\alpha_{k-1}(\vartheta))\\
&= \Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)g(\vartheta) + u\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)\alpha_1(\vartheta) + u^2\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)\alpha_2(\vartheta) + \dots\\
&\quad + \dots + u^{k-1}\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)\alpha_{k-1}(\vartheta),\\
&= \Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)\alpha_{k-1}(\vartheta)n_{k-1}(\vartheta) + u\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)\alpha_{k-1}(\vartheta)m_{k-1}(\vartheta) + \dots\\
&\quad + \dots + u^{k-1}\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)\alpha_{k-1}(\vartheta),\\
&= 0.
\end{aligned}$$

Also, we notice that

$$\begin{aligned}
&u\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)(g(\vartheta) + u\alpha_1(\vartheta) + u^2\alpha_2(\vartheta) + \dots + u^{k-1}\alpha_{k-1}(\vartheta))\\
&= u\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)g(\vartheta) + u^2\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)\alpha_1(\vartheta) + u^3\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)\alpha_2(\vartheta) + \dots\\
&\quad + \dots + u^{k-1}\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)\alpha_{k-2}(\vartheta),\\
&= u\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)\alpha_{k-2}(\vartheta)n_{k-2}(\vartheta) + u^2\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)\alpha_{k-2}(\vartheta)m_{k-2}(\vartheta) + \dots\\
&\quad + \dots + u^{k-1}\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)\alpha_{k-2}(\vartheta),\\
&= 0.
\end{aligned}$$

Further

$$
\begin{aligned}
&u^2\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)(g(\vartheta)+u\alpha_1(\vartheta)+u^2\alpha_2(\vartheta)+\ldots+u^{k-1}\alpha_{k-1}(\vartheta))\\
&\quad = u^2\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)g(\vartheta)+u^3\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)\alpha_1(\vartheta)+u^4\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)\alpha_2(\vartheta)+\ldots\\
&\qquad +\ldots+u^{k-1}\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)\alpha_{k-3}(\vartheta),\\
&\quad = u^2\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)\alpha_{k-3}(\vartheta)n_{k-3}(\vartheta)+u^3\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)\alpha_{k-3}(\vartheta)m_{k-3}(\vartheta)+\ldots\\
&\qquad +\ldots+u^{k-1}\Big(\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)}\Big)\alpha_{k-3}(\vartheta),\\
&\quad = 0.
\end{aligned}
$$

So continuing in a similar manner, we get

$$
\begin{aligned}
&u^{k-1}\Big(\frac{\vartheta^n-1}{g(\vartheta)}\Big)(g(\vartheta)+u\alpha_1(\vartheta)+u^2\alpha_2(\vartheta)+\ldots+u^{k-1}\alpha_{k-1}(\vartheta))\\
&\quad = u^{k-1}\Big(\frac{\vartheta^n-1}{g(\vartheta)}\Big)g(\vartheta)\\
&\quad = 0.
\end{aligned}
$$

So,

$$
N=\Big\langle\frac{\vartheta^n-1}{\alpha_{k-1}(\vartheta)},\quad u\frac{\vartheta^n-1}{\alpha_{k-2}(\vartheta)},\quad u^2\frac{\vartheta^n-1}{\alpha_{k-3}(\vartheta)},\ldots\ldots,u^{k-1}\frac{\vartheta^n-1}{g(\vartheta)}\Big\rangle\subseteq\mathbb{Q}(\mathscr{A}).
$$

Now, to prove that $\mathbb{Q}(\mathscr{A})\subseteq N$. Suppose that

$$
\mathbb{Q}(\mathscr{A})=\big\langle h_0(\vartheta),uh_1(\vartheta),u^2h_2(\vartheta),\ldots,u^{k-1}h_{k-1}(\vartheta)\big\rangle.
$$

Then

$$
u^{k-1}h_{k-1}(\vartheta)(g(\vartheta)+u\alpha_1(\vartheta)+u^2\alpha_2(\vartheta+\ldots+u^{k-1}\alpha_{k-1}(\vartheta)))=0.
$$

From here, we conclude that there exists a polynomial $b_1(\vartheta)\in\mathbb{F}_2$ such that

$$
h_{k-1}(\vartheta)=\Big(\frac{\vartheta^n-1}{g(\vartheta)}\Big)b_1(\vartheta)\in N.
$$

Also

$$
\begin{aligned}
u^{k-2}h_{k-2}(\vartheta)(g(\vartheta)+u\alpha_1(\vartheta)+u^2\alpha_2(\vartheta)+\ldots+u^{k-1}\alpha_{k-1}(\vartheta))&=0\\
u^{k-2}h_{k-2}(\vartheta)g(\vartheta)+u^{k-1}h_{k-2}(\vartheta)\alpha_1(\vartheta)&=0.
\end{aligned}
$$

Since $h_{k-2}(\vartheta)g(\vartheta)=0$, $u^{k-1}h_{k-2}(\vartheta)\alpha_1(\vartheta)=0$ and so, there exists polynomial $b_2(\vartheta)\in\mathbb{F}_2$ such that

$$
h_{k-2}(\vartheta)=\Big(\frac{\vartheta^n-1}{\alpha_1(\vartheta)}\Big)b_2(\vartheta).
$$

Further, we notice that

$$
\begin{aligned}
u^{k-3}h_{k-3}(\vartheta)(g(\vartheta)+u\alpha_1(\vartheta)+u^2\alpha_2(\vartheta)+\ldots+u^{k-1}\alpha_{k-1}(\vartheta))&=0\\
u^{k-3}h_{k-3}(\vartheta)g(\vartheta)+u^{k-2}h_{k-3}(\vartheta)\alpha_1(\vartheta)+u^{k-1}h_{k-3}(\vartheta)\alpha_2(\vartheta)&=0.
\end{aligned}
$$

In above equation as $h_{k-3}(\vartheta)g(\vartheta)=0$ so there exists a polynomial $b_3(\vartheta)\in\mathbb{F}_2$ such that

$$
h_{k-3}(\vartheta)=\Big(\frac{\vartheta^n-1}{\alpha_2(\vartheta)}\Big)b_3(\vartheta).
$$

In a similar way, we reach the equation

$$h_0(\vartheta)(g(\vartheta) + u\alpha_1(\vartheta) + u^2\alpha_2(\vartheta) + \ldots + u^{k-1}\alpha_{k-1}(\vartheta)) = 0$$
$$h_0(\vartheta)g(\vartheta) + uh_0(\vartheta)\alpha_1(\vartheta) + u^2h_0(\vartheta)\alpha_2(\vartheta) + \ldots + u^{k-1}h_0(\vartheta)(\alpha_{k-1}(\vartheta)) = 0$$

which implies $h_0(\vartheta) = \Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)b_k(\vartheta)$ for some $b_k(\vartheta) \in \mathbb{F}_2$.
Hence,

$$\begin{aligned}\mathbb{Q}(\mathscr{A}) &= \big\langle h_0(\vartheta), uh_1(\vartheta), u^2h_2(\vartheta), \ldots, u^{k-1}h_{k-1}(\vartheta)\big\rangle \\ &\subseteq \Big\langle \frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}, \quad u\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}, \quad u^2\frac{\vartheta^n - 1}{\alpha_{k-3}(\vartheta)}, \ldots\ldots, u^{k-1}\frac{\vartheta^n - 1}{g(\vartheta)}\Big\rangle \in N.\end{aligned}$$

Therefore,

$$\mathbb{Q}(\mathscr{A}) = \Big\langle \frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}, \quad u\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}, \quad u^2\frac{\vartheta^n - 1}{\alpha_{k-3}(\vartheta)}, \ldots\ldots, u^{k-1}\frac{\vartheta^n - 1}{g(\vartheta)}\Big\rangle.$$

□

Theorem 5.4. *Let $\mathscr{A}$ be a cyclic code of odd length n over $\mathbb{S}$. Then*

$$\mathscr{A}^\perp = \Big\langle \Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)^*, u\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)^*, \ldots, u^{k-1}\Big(\frac{\vartheta^n - 1}{g(\vartheta)}\Big)^*\Big\rangle.$$

Theorem 5.5. *Let $\mathscr{A}$ be a reversible cyclic code of odd length n over $\mathbb{S}$ with $\alpha_{k-1}(\vartheta) \mid \alpha_{k-2}(\vartheta) \mid \ldots \mid \alpha_2(\vartheta) \mid \alpha_1(\vartheta) \mid g(\vartheta) | (\vartheta^n - 1)$ and*

$$\mathscr{A}^\perp = \Big\langle \Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)^*, u\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)^*, \ldots, u^{k-1}\Big(\frac{\vartheta^n - 1}{g(\vartheta)}\Big)^*\Big\rangle.$$

Then $\mathscr{A}^\perp$ is a reversible cyclic code over $\mathbb{S}$.

Proof. Let $\mathscr{A}$ be a reversible cyclic code of odd length n over $\mathbb{S}$. Then by Theorem 4.9 $g(\vartheta)$, $\alpha_1(\vartheta), \alpha_2(\vartheta), \ldots, \alpha_{k-1}(\vartheta)$ are self reciprocal. Suppose that $\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big) = v_1(\vartheta)$, $\Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big) = v_2(\vartheta)$, $\Big(\frac{\vartheta^n - 1}{\alpha_{k-3}(\vartheta)}\Big) = v_3(\vartheta), \ldots, \Big(\frac{\vartheta^n - 1}{\alpha_2(\vartheta)}\Big) = v_{k-2}(\vartheta)$, $\Big(\frac{\vartheta^n - 1}{\alpha_1(\vartheta)}\Big) = v_{k-1}(\vartheta)$ and $\Big(\frac{\vartheta^n - 1}{g(\vartheta)}\Big) = v_k(\vartheta)$.
Therefore,

$$\begin{aligned}\langle \vartheta^n - 1\rangle^* &= \alpha_{k-1}^*(\vartheta)v_1^*(\vartheta), \\ \langle \vartheta^n - 1\rangle^* &= \alpha_{k-2}^*(\vartheta)v_2^*(\vartheta), \\ \langle \vartheta^n - 1\rangle^* &= \alpha_{k-3}^*(\vartheta)v_3^*(\vartheta), \\ &\vdots \\ \langle \vartheta^n - 1\rangle^* &= \alpha_2^*(\vartheta)v_{k-2}^*(\vartheta), \\ \langle \vartheta^n - 1\rangle^* &= \alpha_1^*(\vartheta)v_{k-1}^*(\vartheta),\end{aligned}$$

and

$$\langle \vartheta^n - 1\rangle^* = g^*(\vartheta)v_k^*(\vartheta).$$

This implies

$$v_1^*(\vartheta) = \frac{\langle \vartheta^n - 1\rangle^*}{\alpha_{k-1}^*(\vartheta)} = \frac{-\langle \vartheta^n - 1\rangle}{\alpha_{k-1}(\vartheta)} = -v_1(\vartheta),$$
$$v_2^*(\vartheta) = \frac{\langle \vartheta^n - 1\rangle^*}{\alpha_{k-2}^*(\vartheta)} = \frac{-\langle \vartheta^n - 1\rangle}{\alpha_{k-2}(\vartheta)} = -v_2(\vartheta),$$
$$v_3^*(\vartheta) = \frac{\langle \vartheta^n - 1\rangle^*}{\alpha_{k-3}^*(\vartheta)} = \frac{-\langle \vartheta^n - 1\rangle}{\alpha_{k-3}(\vartheta)} = -v_3(\vartheta),$$
$$\vdots$$
$$v_{k-1}^*(\vartheta) = \frac{\langle \vartheta^n - 1\rangle^*}{\alpha_1^*(\vartheta)} = \frac{-\langle \vartheta^n - 1\rangle}{\alpha_1(\vartheta)} = -v_{k-1}(\vartheta)$$

and

$$v_k^*(\vartheta) = \frac{\langle \vartheta^n - 1\rangle^*}{g^*(\vartheta)} = \frac{-\langle \vartheta^n - 1\rangle}{g(\vartheta)} = -v_k(\vartheta).$$

Let $\bar{c}(\vartheta) \in \mathscr{A}^\perp$. Then

$$\begin{aligned}(\bar{c}(\vartheta))^* &= \Big(\Big(\frac{\vartheta^n - 1}{\alpha_{k-1}(\vartheta)}\Big)^* d_1(\vartheta) + \Big(\frac{\vartheta^n - 1}{\alpha_{k-2}(\vartheta)}\Big)^* d_2(\vartheta) + \ldots + \\ &\quad + \Big(\frac{\vartheta^n - 1}{\alpha_1(\vartheta)}\Big)^* d_{k-1}(\vartheta) + \Big(\frac{\vartheta^n - 1}{g(\vartheta)}\Big)^* d_k(\vartheta)\Big)^* \\ &= (-v_1(\vartheta)d_1(\vartheta) - v_2(\vartheta)d_2(\vartheta) - v_3(\vartheta)d_3(\vartheta) - \ldots - v_{k-1}(\vartheta)d_{k-1}(\vartheta) - v_k(\vartheta)d_k(\vartheta))^* \\ &= (-v_1^*(\vartheta)d_1^*(\vartheta) - \vartheta^{i_2}v_2^*(\vartheta)d_2^*(\vartheta) - \vartheta^{i_3}v_3^*(\vartheta)d_3^*(\vartheta) - \ldots - \vartheta^{i_k}v_k^*(\vartheta)d_k^*(\vartheta)) \\ &= (v_1^*(\vartheta)\gamma_1(\vartheta) + v_2^*(\vartheta)\gamma_2(\vartheta) + v_3^*(\vartheta)\gamma_3(\vartheta) + \ldots + v_k^*(\vartheta)\gamma_k(\vartheta)),\end{aligned}$$

where $\gamma_1(\vartheta) = -d_1^*(\vartheta)$, $\gamma_2(\vartheta) = -\vartheta^{i_2}d_2^*(\vartheta)$ and $\gamma_3(\vartheta) = -\vartheta^{i_3}d_3^*(\vartheta), \ldots, \gamma_k(\vartheta) = -\vartheta^{i_k}d_k^*(\vartheta)$ over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^{k-1}\mathbb{F}_2$. Thus $c(\vartheta) \in \mathscr{A}^\perp$. Thus, by Theorem 5.1, $\mathscr{A}^\perp$ is a reversible cyclic code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^{k-1}\mathbb{F}_2$. □

6 Minimum Hamming distance of a cyclic code over $\mathbb{S}$

In this section, we find the minimum Hamming distance of a cyclic code of length n over $\mathbb{S}$. Let $\mathscr{A} = \langle g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta) + \ldots + u^{k-1}p_{k-1}(\vartheta), u\alpha_1(\vartheta) + u^2q_1(\vartheta) + u^3q_2(\vartheta) + \ldots + u^{k-1}q_{k-2}(\vartheta), \ldots, u^{k-2}\alpha_{k-2}(\vartheta) + u^{k-1}t_1(\vartheta), u^{k-1}\alpha_{k-1}(\vartheta)\rangle$ be a cyclic code of length n over $\mathbb{S}$. Define $\mathscr{A}_{u^{k-1}} = \{n(\vartheta) \mid u^{k-1}n(\vartheta) \in \mathscr{A}\}$. Then $\mathscr{A}_{u^{k-1}}$ is a cyclic code of length n over $\mathbb{F}_2$. To find the minimum Hamming distance of the cyclic code, we use the following result.

Theorem 6.1. *[11, Theorem 4.4] If* $\mathscr{A} = \langle g(\vartheta)+up_1(\vartheta)+u^2p_2(\vartheta)+\ldots+u^{k-1}p_{k-1}(\vartheta), u\alpha_1(\vartheta)+u^2q_1(\vartheta)+u^3q_2(\vartheta)+\ldots+u^{k-1}q_{k-2}(\vartheta), \ldots, u^{k-2}\alpha_{k-2}(\vartheta)+u^{k-1}t_1(\vartheta), u^{k-1}\alpha_{k-1}(\vartheta)\rangle$ *is a cyclic code of length* n *over* $\mathbb{S}$ *with* $u^k = 0$*, then* $\mathscr{A}_{u^{k-1}} = \langle \alpha_{k-1}(\vartheta)\rangle$.

Proof. We know that $u^{k-1}\alpha_{k-1}(\vartheta) \in \mathscr{A}$, hence $\langle \alpha_{k-1}(\vartheta)\rangle \subseteq \mathscr{A}_{u^{k-1}}$. Now given an $b(\vartheta) \in \mathscr{A}_{u^{k-1}}$, then $u^{k-1}b(\vartheta) \in \mathscr{A}$ and hence there exist polynomials $c_1(\vartheta), c_2(\vartheta), \ldots, c_t(\vartheta) \in \mathbb{F}_2[\vartheta]$ such that $u^{k-1}b(\vartheta) = c_1(\vartheta)u^{k-1}g(\vartheta)+c_2(\vartheta)u^{k-1}\alpha_1(\vartheta)+c_3(\vartheta)u^{k-1}\alpha_2(\vartheta)+\ldots+c_t(\vartheta)u^{k-1}\alpha_{k-1}(\vartheta)$. Since $\alpha_{k-1}(\vartheta) \mid \alpha_{k-2}(\vartheta) \mid \ldots \mid \alpha_2(\vartheta) \mid \alpha(\vartheta) \mid g(\vartheta)$, we have $u^{k-1}b(\vartheta) = u^{k-1}m(\vartheta)\alpha_{k-1}(\vartheta)$ for some $m(\vartheta)$. So $\mathscr{A}_{u^{k-1}} \subseteq \langle \alpha_{k-1}(\vartheta)\rangle$ and hence $\mathscr{A}_{u^{k-1}} = \langle \alpha_{k-1}(\vartheta)\rangle$ □

Theorem 6.2. *[11, Theorem 4.4] Let* $\mathscr{A}$ *be a cyclic code of length* n *over* $\mathbb{S}$*. Then* $d_H(\mathscr{A}) = w_H(\mathscr{A}) = w_H(\mathscr{A}_{u^{k-1}}) = d_H(\mathscr{A}_{u^{k-1}})$*, where* $w_H(\mathscr{A})$ *is the minimum Hamming weight of cyclic code* $\mathscr{A}$*.*

Proof. For a given codeword $m(\vartheta) = m_0(\vartheta_0) + um_1(\vartheta) + u^2m_2(\vartheta) + \ldots + u^{k-1}m_{k-1}(\vartheta) \in \mathscr{A}$, where $m_0(\vartheta), m_1(\vartheta), m_2(\vartheta), \ldots, m_{k-1}(\vartheta) \in F_2[\vartheta]$. As $u^{k-1}m(\vartheta) = u^{k-1}m_0(\vartheta) \in \mathscr{A}$ and $w_H(u^{k-1}m(\vartheta)) \le w_H(m(\vartheta))$ and $u^{k-1}\mathscr{A}$ is a subcode of $\mathscr{A}$ with $w_H(u^{k-1}\mathscr{A}) \le w_H(\mathscr{A})$, it is sufficient to focus on the subcode $u^{k-1}\mathscr{A}$ in order to compute the Hamming weight of $\mathscr{A}$. Since $u^{k-1}\mathscr{A} = \langle u^{k-1}\alpha_{k-1}(\vartheta)\rangle$, thus $w_H(\mathscr{A}) = d_H(\mathscr{A}) = w_H(\mathscr{A}_{u^{k-1}}) = d_H(\mathscr{A}_{u^{k-1}})$. □

7 Examples

Example 7.1. For length $n = 15$ in $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, $\vartheta^{15} - 1 = (\vartheta + 1)(\vartheta^2 + \vartheta + 1)(\vartheta^4 + \vartheta + 1)(\vartheta^4 + \vartheta^3 + 1)(\vartheta^4 + \vartheta^3 + \vartheta^2 + \vartheta + 1)$ and let $\alpha_2(\vartheta) = 1$, $\alpha_1(\vartheta) = \vartheta^2 + \vartheta + 1$ and $g(\vartheta) = \vartheta^6 + \vartheta^4 + \vartheta^3 + \vartheta^2 + 1$. Here $\alpha_2(\vartheta) \mid \alpha_1(\vartheta) \mid g(\vartheta) \mid (\vartheta^{15} - 1)$, then by using Theorem 4.9, the code generated by $\langle g(\vartheta) + u\alpha_1(\vartheta) + u^2\alpha_2(\vartheta)\rangle$ is reversible cyclic code.

Example 7.2. Let $\vartheta^{32} - 1 = (\vartheta + 1)^{32} = g^{32}$ in $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Let $\mathscr{A} = \langle g(\vartheta) + up_1(\vartheta) + u^2p_2(\vartheta)\rangle$, where $g(\vartheta) = g^{30}$, $p_1(\vartheta) = \vartheta + \vartheta^5 + \vartheta^9 + \vartheta^{13} + \vartheta^{17} + \vartheta^{21} + \vartheta^{25} + \vartheta^{29}$ and $p_2(\vartheta) = \vartheta^2 + \vartheta^4 + \vartheta^{10} + \vartheta^{12} + \vartheta^{18} + \vartheta^{20} + \vartheta^{26} + \vartheta^{28}$. It is easy to check that $g(\vartheta) = \vartheta^{30} + \vartheta^{28} + \vartheta^{26} + \vartheta^{24} + \vartheta^{22} + \vartheta^{20} + \vartheta^{18} + \vartheta^{16} + \vartheta^{14} + \vartheta^{12} + \vartheta^{10} + \vartheta^8 + \vartheta^6 + \vartheta^4 + \vartheta^2 + 1$ is self-reciprocal. Also, $\vartheta^i p_1^*(\vartheta) = p_1(\vartheta)$ and $\vartheta^j p_2^*(\vartheta) = p_2(\vartheta)$, $i = d(g(\vartheta)) - d(p_1(\vartheta))$ & $j = d(g(\vartheta)) - d(p_2(\vartheta))$, where $d(g(\vartheta))$ denotes degree of $g(\vartheta)$. Therefore, by using Theorem 4.10, $\mathscr{A}$ is a reversible code.

References

[1] A. Hammons, P. 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**, 301-319 (1994).

[2] T. Abualrub and R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, *IEEE Trans. Inform. Theory* **49**(9), 2126-2133 (2003).

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

[4] T. Abualrub and I. Siap, On the construction of cyclic codes over the ring $\mathbb{Z}_2 + u\mathbb{Z}_2$, *Proc.* 9^{th} *WSEAS Internat. Conf. Appl. Math., Istanbul, Turkey*, 430-435 (2006).

[5] L. Ping and Z. Shixin, Cyclic codes of arbitrary lengths over the ring $\mathbb{F}_q + u\mathbb{F}_q$, *J. Univ. Sci. Technol. China* **38**(12), 1392-1396 (2008).

[6] J. L. Massey, Reversible codes, *Inf. Control* **7**(3), 369-380 (1964).

[7] K. Tzeng and C. Hartmann, On the minimum distance of certain reversible cyclic codes, *IEEE Trans. Inform. Theory*, **16**(5), 644-646 (1970).

[8] B. Srinivasulu and M. Bhaintwal, Reversible cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$ and their applications to DNA codes, *Proc.* 7^{th} *International Conference on Information Technology and Electrical Engineering*, 101-105 (2015).

[9] H. Mostafanasab, A. Yousefian Darani, On Cyclic DNA Codes Over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. *Commun. Math. Stat.* (2019).

[10] B. Yildiz, I. Siap, Cyclic codes over $\mathbb{F}_2[u]/ < u^4 - 1 >$ and applications to DNA codes, *Comput. Math. Appl.* **63**, 1169-1176 (2012)

[11] M. Al-ashker and M. Hamoudeh, Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + \ldots + u^{k-1}\mathbb{Z}_2$. *Turkish Journal of Mathematics*, **35**(4), 737-749 (1970).

[12] A. Dertli, Y. Cengellenmis and S. Eren, Quantum Codes over the Ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^m\mathbb{F}_2$, *International Journal of Algebra* **9**(3), 115-121, (2015).

[13] A. Dertli, Y. Cengellenmis and S. Eren, On quantum codes obtained from cyclic codes over A_2, *International Journal of quantum information* **13**(03), 1550031 (2015).

[14] W. Bosma, J. Cannon, *Handbook of magma functions*, Univ. of Sydney, Sydney, (1995).

Author information

Nadeem ur Rehman, Department of Mathematics, Aligarh Muslim University, Aligarh-202002, India.
E-mail: `nu.rehman.mm@amu.ac.in`

Mohd Azmi, Department of Mathematics, Aligarh Muslim University, Aligarh-202002, India.
E-mail: `waytoazmi40@gmail.com`

Ghulam Mohammad, Department of Mathematics, Aligarh Muslim University, Aligarh-202002, India.
E-mail: `mohdghulam202@gmail.com`

Received: 2022-06-08
Accepted: 2023-04-13