$\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes

Lingyu Diao and Jian Gao*

School of Mathematics and Statistics,
Shandong University of Technology,
Zibo, 255000, China
Email: dlylotus@163.com
Email: dezhougaojian@163.com
*Corresponding author

Abstract: Additive cyclic codes of length (α, β) over $\mathbb{Z}_p\mathbb{Z}_p[u]$ can be viewed as $\mathbb{Z}_p[u][x]$-submodules of $\mathbb{Z}_p[x]/(x^\alpha - 1) \times \mathbb{Z}_p[u][x]/(x^\beta - 1)$, where $\mathbb{Z}_p[u] = \mathbb{Z}_p + u\mathbb{Z}_p$, $u^2 = 0$. In this paper, we determine the generator polynomials and the minimal generating sets of this family of codes as $\mathbb{Z}_p[u]$-submodules of $\mathbb{Z}_p[x]/(x^\alpha - 1) \times \mathbb{Z}_p[u][x]/(x^\beta - 1)$. Further, we also determine the generator polynomials of the dual codes of $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes. Moreover, some binary quantum codes are constructed by additive cyclic codes over $\mathbb{Z}_2\mathbb{Z}_2[u]$.

Keywords: additive cyclic codes; minimal generating sets; binary quantum codes.

Reference to this paper should be made as follows: Diao, L. and Gao, J. (2018) '$\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes', *Int. J. Information and Coding Theory*, Vol. 5, No. 1, pp.1–17.

Biographical notes: Lingyu Diao received her BE from Shandong University of Technology in 2016. She is now a Master candidate of School of Mathematics and Statistics at Shandong University of Technology. Her research interests include coding theory and information theory.

Jian Gao received his PhD from Chern Institute of Mathematics at Nankai University in 2015. He is now teaching in School of Mathematics and Statistics at Shandong University of Technology. His research interests include coding theory and cryptography.

1 Introduction

Codes over finite rings have been studied since the early 1970s. Hammons et al. (1994) showed that some certain good nonlinear binary codes can be constructed from cyclic codes over $\mathbb{Z}_4$ via the Gray map. Recently, many coding scholars have done a lot of works on codes over finite rings. Delsarte and Levenshtein (1998) defined additive codes as the subgroups of the underlying commutative group. In the year 2009, Borges et al. (2009) proposed the concept of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The generator matrices and the duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are also studied (Borges et al., 2009). Afterward, the additive code has been applied in the engineering field, which has aroused the interest of encoding scholars, and some good results have emerged (Abualrub et al., 2014b; Aydogdu et al., 2015; Aydogdu and Siap, 20). $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes are first studied by Abualrub et al. (2014a). Borges et al. have studied the structural properties of dual codes of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes (Borges et al., 2016). As an interesting generalisation, Srinivasulu and Maheshanand (2016) studied the additive cyclic codes and their dual codes over $\mathbb{Z}_2\mathbb{Z}_2[u]$.

In the year 1995, Shor has found the first quantum error-correcting code (Shor, 1995). Later, a method to construct quantum error-correcting codes from classical error-correcting codes was introduced by Calderbank et al. (1998). Recently, the construction of quantum error-correcting codes by using classical error-correcting codes over the finite field $\mathbb{F}_q$ has developed rapidly. In the year 2009, Qian has given a method to construct quantum error-correcting codes by using cyclic codes over the finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ (Qian et al., 2009).

The paper is organised as follows. In Section 2, we give some preliminaries. In Section 3, we introduce some definitions and give some structural properties of additive cyclic codes over $\mathbb{Z}_p\mathbb{Z}_p[u]$. Moreover, we determine the minimal generating sets of additive cyclic codes over $\mathbb{Z}_p\mathbb{Z}_p[u]$. In Section 4, we determine the relationship of generators between the additive cyclic code and its dual code. In Section 5, we give a necessary and sufficient condition for the additive cyclic code that contains its dual code over $\mathbb{Z}_2\mathbb{Z}_2[u]$. Finally, some binary quantum codes are obtained from additive cyclic codes over $\mathbb{Z}_2\mathbb{Z}_2[u]$.

2 Preliminaries

Let $\mathbb{Z}_p$ be the ring of integers modulo p. Let $\mathbb{Z}_p[u] = \mathbb{Z}_p + u\mathbb{Z}_p = \{a + ub \mid a, b \in \mathbb{Z}_p\}$, where $u^2 = 0$. $\mathbb{Z}_p[u]$ is a commutative ring, and $\mathbb{Z}_p$ is a proper subring of $\mathbb{Z}_p[u]$. Let $\mathbb{Z}_p\mathbb{Z}_p[u] = \mathbb{Z}_p \times \mathbb{Z}_p[u] = \{(v|v')|v \in \mathbb{Z}_p \text{ and } v' \in \mathbb{Z}_p[u]\}$. $\mathbb{Z}_p\mathbb{Z}_p[u]$ is a commutative group with respect to componentwise addition. We denote the space of n-tuples over these rings as $\mathbb{Z}_p^n$ and $\mathbb{Z}_p[u]^n$. If that any non-empty subset $\mathcal{C}$ of $\mathbb{Z}_p^n$ is a vector space then we say that it is a linear code. A code over $\mathbb{Z}_p[u]$ is a non-empty subset $\mathscr{C}$ of $\mathbb{Z}_p[u]^n$ and a submodule of $\mathbb{Z}_p[u]^n$ is called a linear code over $\mathbb{Z}_p[u]$.

For a vector $\mathbb{v} \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$, we write $\mathbb{v} = (v|v')$ where $v = (v_0, \dots, v_{\alpha-1}) \in \mathbb{Z}_p^\alpha$ and $v' = (v'_0, \dots, v'_{\beta-1}) \in \mathbb{Z}_p[u]^\beta$.

Definition 1: A non-empty subset $\mathscr{C}$ of $\mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ is called a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code if $\mathscr{C}$ is an additive subgroup of $\mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$.

Let $\mathscr{C}$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code. Since $\mathscr{C}$ is an additive subgroup of $\mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$, it is also isomorphic to a commutative structure like $\mathbb{Z}_p^{k_0} \times \mathbb{Z}_p^{2k_1} \times \mathbb{Z}_p^{k_2}$. Therefore, $\mathscr{C}$ is of type $p^{k_0+2k_1+k_2}$ as a group, it has $|\mathscr{C}| = p^{k_0+2k_1+k_2}$ codewords. Considering all these parameters, we will say that $\mathscr{C}$ is of type $(\alpha, \beta; k_0, k_1, k_2)$.

Let X (respectively Y) be the set of $\mathbb{Z}_p$ (respectively $\mathbb{Z}_p[u]$) coordinate positions. Then $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set X corresponds to the first α coordinates and Y corresponds to the last β coordinates. Call $\mathscr{C}_X$ (respectively $\mathscr{C}_Y$) the punctured code of $\mathscr{C}$ by deleting the coordinates outside X (respectively Y). A $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code $\mathscr{C}$ is said to be separable if $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$.

We define a Grey map as $\Phi : \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta \to \mathbb{Z}_p^{\alpha+2\beta}$ such that $\Phi(\mathbb{u}) = \Phi(u|u') = (u, \phi(u'))$, where ϕ is the usual Grey map defined by

$$\begin{aligned} &\phi : \mathbb{Z}_p[u] \to \mathbb{Z}_p^2 \\ &\quad a + ub \mapsto (b, a+b). \end{aligned}$$

Definition 2: Let $\mathbb{v} = (v|v') \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$, where $v = (v_0, \dots, v_{\alpha-1}) \in \mathbb{Z}_p^\alpha$ and $v' = (v'_0, \dots, v'_{\beta-1}) \in \mathbb{Z}_p[u]^\beta$. Then the Lee weight of $\mathbb{v}$ is defined as

$$w_L(\mathbb{v}) = w_H(\Phi(\mathbb{v})),$$

where w_H denotes the Hamming weight.

Definition 3: Let $\mathbb{v}, \mathbb{w} \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$. Then the Lee distance of $\mathbb{v}$ and $\mathbb{w}$ is defined as

$$d_L(\mathbb{v}, \mathbb{w}) = w_L(\mathbb{v} - \mathbb{w}).$$

An inner product for two elements $\mathbb{v}, \mathbb{w} \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ is defined as Aydogdu et al. (2015) $\mathbb{v} \cdot \mathbb{w} = u(\sum_{i=0}^{\alpha-1} v_i w_i) + \sum_{j=0}^{\beta-1} v'_j w'_j \in \mathbb{Z}_p[u]$.

Let $\mathscr{C}$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code. The additive dual code of $\mathscr{C}$, denoted by $\mathscr{C}^\perp$, is then defined in a standard way as $\mathscr{C}^\perp = \{\mathbb{w} \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta \mid \mathbb{v} \cdot \mathbb{w} = 0, \text{ for all } \mathbb{v} \in \mathscr{C}\}$. If $\mathscr{C}$ is separable then $\mathscr{C}^\perp = (\mathscr{C}_X)^\perp \times (\mathscr{C}_Y)^\perp$.

Proposition 1: *Let $\mathscr{C}$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code of type $(\alpha, \beta; k_0, k_1, k_2)$. Then*

$$\begin{aligned} &\text{(i) } |\mathscr{C}| = p^{k_0} p^{2k_1} p^{k_2}, && |\mathscr{C}^\perp| = p^{\alpha-k_0} p^{2(\beta-k_1-k_2)} p^{k_2}, \\ &\text{(ii) } |\mathscr{C}_X| = p^{k_0+k_{1,1}}, && |(\mathscr{C}_X)^\perp| = p^{\alpha-k_0-k_{1,1}}, \\ &\text{(iii) } |\mathscr{C}_Y| = p^{2k_1} p^{k_2+k_{0,2}}, && |(\mathscr{C}_Y)^\perp| = p^{2(\beta-k_1-k_2-k_{0,2})} p^{k_2+k_{0,2}}, \end{aligned}$$

where $k_0 = k_{0,1} + k_{0,2}$ and $k_1 = k_{1,1} + k_{1,2}$.

Proof: The proof is similar to that of Proposition 4.8 appeared in Srinivasulu and Maheshanand (2016). □

3 $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes

Let $\mathbb{v} = (v|v') \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ and let i be an integer. Then we denote by

$$\mathbb{v}^{(i)} = (v^{(i)}|v'^{(i)}) = (v_{0+i}, v_{1+i}, \dots, v_{\alpha-1+i}|v'_{0+i}, v'_{1+i}, \dots, v'_{\beta-1+i})$$

the ith cyclic shift of $\mathbb{v}$, where the subscripts are read modulo α and β, respectively.

Definition 4: Let $\mathscr{C} \subseteq \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code. The code $\mathscr{C}$ is called a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code if for any codeword $\mathbb{v} \in \mathscr{C}$ we have $\mathbb{v}^{(1)} \in \mathscr{C}$.

Let $R_{\alpha,\beta} = \mathbb{Z}_p[x]/(x^\alpha - 1) \times \mathbb{Z}_p[u][x]/(x^\beta - 1)$, where $\beta \geq 0$ and $\gcd(\beta, p) = 1$. We consider the mapping $\delta : \mathbb{Z}_p[u] \to \mathbb{Z}_p$ defined by $\delta(a + ub) = a$. Clearly, δ is well defined and is a ring homomorphism. Let $\lambda(x) = c_0 + c_1 x + \cdots + c_t x^t \in \mathbb{Z}_p[u][x]$, define the operation $\star : \mathbb{Z}_p[u][x] \times R_{\alpha,\beta} \to R_{\alpha,\beta}$ as $\lambda(x) \star (p(x)|q(x)) = (\delta(\lambda(x))p(x)|\lambda(x)q(x))$ where $\delta(\lambda(x)) = \delta(c_0) + \delta(c_1)x + \cdots + \delta(c_t)x^t$. From Srinivasulu and Maheshanand (2016), we know that $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes are identified as $\mathbb{Z}_p[u][x]$-submodules of $R_{\alpha,\beta}$.

Theorem 1 (Abualrub et al., 2014a)**:** *Let $\mathscr{C}$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha, \beta; k_0, k_1, k_2)$. Then it is of the form*

$$\mathscr{C} = \langle (b(x)|0), (l(x)|f(x)h(x) + uf(x)) \rangle,$$

where $f(x)h(x)g(x) = x^\beta - 1$ in $\mathbb{Z}_p[u][x]$, $b(x), l(x) \in \mathbb{Z}_p[x]/(x^\alpha - 1)$ with $b(x)|(x^\alpha - 1)$, $\deg(l(x)) < \deg(b(x))$ and $b(x)|\frac{x^\beta - 1}{f(x)} l(x) \pmod{p}$.

Note that if $\mathscr{C}$ is a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code with $\mathscr{C} = \langle (b(x)|0), (l(x)|f(x)h(x) + uf(x)) \rangle$, then the canonical projections $\mathscr{C}_X$ and $\mathscr{C}_Y$ are a cyclic code over $\mathbb{Z}_p$ and a cyclic code over $\mathbb{Z}_p[u]$ generated by $\gcd(b(x), l(x))$ and $f(x)h(x) + uf(x)$, respectively (see MacMilliams and Sloane (1975) and Wan (1997)). Moreover, if $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$, then $l(x) = 0$.

Since $b(x)|\frac{x^\beta - 1}{f(x)} l(x) \pmod{p}$, we have the following result.

Corollary 1: *Let $\mathscr{C}$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha, \beta; k_0, k_1, k_2)$ with $\mathscr{C} = \langle (b(x)|0), (l(x)|f(x)h(x) + uf(x)) \rangle$. Then,*

$$b(x)|\frac{x^\beta - 1}{f(x)} \gcd(b(x), l(x)) \pmod{p},$$
$$b(x)|h(x)\gcd(b(x), l(x)g(x)) \pmod{p}.$$

In the following, a polynomial $f(x) \in \mathbb{Z}_p[x]$ or $\mathbb{Z}_p[u][x]$ will be denoted simply by f and the parameter β will be an integer satisfied $\gcd(\beta, p) = 1$.

Theorem 2: *Let $\mathscr{C} = \langle (b|0), (l|fh + uf) \rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha, \beta; k_0, k_1, k_2)$, where $fhg = x^\beta - 1$. Let*

$$S_1 = \bigcup_{i=0}^{\alpha - \deg(b) - 1} \{x^i \star (b|0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg(g) - 1} \{x^i \star (l|fh + uf)\},$$

$$S_3 = \bigcup_{i=0}^{\deg(h) - 1} \{x^i \star (lg|ufg)\}.$$

Then $S_1 \cup S_2 \cup S_3$ forms a minimal generating set for $\mathscr{C}$ as a $\mathbb{Z}_p[u]$-module.

Proof: The proof is similar to that of Theorem 3.10 appeared in Srinivasulu and Maheshanand (2016). □

Theorem 3: *Let $\mathscr{C} = \langle (b|0), (l|fh + uf)\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha, \beta; k_0, k_1, k_2)$, where $fhg = x^\beta - 1$. Then*

$$k_0 = \alpha - \deg(\gcd(b, lg)),$$

$$k_1 = \deg(g),$$

$$k_2 = \deg(fh) - \deg(f) - \deg(b) + \deg(\gcd(b, lg)).$$

Proof: The proof is similar to that of Theorem 4.9 appeared in Srinivasulu and Maheshanand (2016). □

Theorem 4: *Let $\mathscr{C} = \langle (b|0), (l|fh + uf)\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha, \beta; k_0, k_1, k_2)$, where $fhg = x^\beta - 1$, $k_0 = k_{0,1} + k_{0,2}$ and $k_1 = k_{1,1} + k_{1,2}$. Then $k_{1,1} = \deg(\gcd(b, lg)) - \deg(\gcd(b, l))$.*

Proof: The proof is similar to that of Theorem 4.10 appeared in Srinivasulu and Maheshanand (2016). □

4 Duality of $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes

Lemma 1: *If $\mathscr{C}$ is any $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code, then $\mathscr{C}^\perp$ is also cyclic.*

Proof: The proof is similar to that of Proposition 4.4 in Srinivasulu and Maheshanand (2016). □

Denote

$$\mathscr{C}^\perp = \langle (\bar{b}|0), (\bar{l}|\overline{fh} + u\bar{f})\rangle,$$

where $\overline{fhg} = x^\beta - 1$ in $\mathbb{Z}_p[u][x]$, $\bar{b}, \bar{l} \in \mathbb{Z}_p[x]/(x^\alpha - 1)$ with $\bar{b}|(x^\alpha - 1)$, $\deg(\bar{l}) < \deg(\bar{b})$ and $\bar{b}|\frac{x^\beta - 1}{\bar{f}}\bar{l} \pmod{p}$.

We denote $p^*(x)$ the reciprocal polynomial of a polynomial $p(x)$, i.e., $p^*(x) = x^{\deg(p(x))}p(x^{-1})$.

In the following, we denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$.

Proposition 2: *Let $n, m \in \mathbb{N}$. Then,*

$$x^{nm} - 1 = (x^n - 1)\theta_m(x^n).$$

Proof: Obvious that $y^m - 1 = (y - 1)\theta_m(y)$. Let $y = x^n$. Then the result is obtained immediately. □

In the following, let $m = \mathrm{lcm}[\alpha, \beta]$.

Definition 5: Let $\mathbb{v}(x) = (v(x)|v'(x)), \mathbb{w}(x) = (w(x)|w'(x)) \in R_{\alpha,\beta}$. We define the map

$$\circ : R_{\alpha,\beta} \times R_{\alpha,\beta} \to \mathbb{Z}_p[u][x]/(x^m - 1)$$

such that

$$\begin{aligned}\circ(\mathbb{v}(x), \mathbb{w}(x)) =& uv(x)\theta_{\frac{m}{\alpha}}(x^\alpha)x^{m-1-\deg(w(x))}w^*(x)\\ &+ v'(x)\theta_{\frac{m}{\beta}}(x^\beta)x^{m-1-\deg(w'(x))}w'^*(x) \mod (x^m - 1).\end{aligned}$$

From now on, we denote $\circ(\mathbb{v}(x), \mathbb{w}(x))$ by $\mathbb{v}(x) \circ \mathbb{w}(x)$. Note that $\mathbb{v}(x) \circ \mathbb{w}(x) \in \mathbb{Z}_p[u][x]/(x^m - 1)$.

Proposition 3: *Let* $\mathbb{v}, \mathbb{w} \in \mathbb{Z}_p^\alpha \times \mathbb{Z}_p[u]^\beta$ *be with associated polynomials* $\mathbb{v}(x) = (v(x)|v'(x))$ *and* $\mathbb{w}(x) = (w(x)|w'(x))$. *Then,* $\mathbb{v}$ *is orthogonal to* $\mathbb{w}$ *and all its shifts if and only if*

$$\mathbb{v}(x) \circ \mathbb{w}(x) = 0.$$

Proof: The proof is similar to that of Lemma 4.6 appeared in Srinivasulu and Maheshanand (2016). □

Lemma 2: *Let* $\mathbb{v}(x) = (v(x)|v'(x)), \mathbb{w}(x) = (w(x)|w'(x)) \in R_{\alpha,\beta}$ *such that* $\mathbb{v}(x) \circ \mathbb{w}(x) = 0$. *If* $v'(x) = 0$ *or* $w'(x) = 0$, *then* $v(x)w^*(x) \equiv 0 \pmod{x^\alpha - 1}$ *over* $\mathbb{Z}_p$. *If* $v(x) = 0$ *or* $w(x) = 0$, *then* $v'(x)w'^*(x) \equiv 0 \pmod{x^\beta - 1}$ *over* $\mathbb{Z}_p[u]$.

Proof: Let $v'(x) = 0$ or $w'(x) = 0$. Then

$$\begin{aligned}0 &= \mathbb{v}(x) \circ \mathbb{w}(x)\\ &= uv(x)\theta_{\frac{m}{\alpha}}(x^\alpha)x^{m-1-\deg(w(x))}w^*(x) + 0 \mod (x^m - 1).\end{aligned}$$

Therefore,

$$uv(x)\theta_{\frac{m}{\alpha}}(x^\alpha)x^{m-1-\deg(w(x))}w^*(x) = u\mu'(x)(x^m - 1),$$

for some $\mu'(x) \in \mathbb{Z}_p[u][x]$. This is equivalent to

$$v(x)\theta_{\frac{m}{\alpha}}(x^\alpha)x^{m-1-\deg(w(x))}w^*(x) = \mu'(x)(x^m - 1) \in \mathbb{Z}_p[x].$$

From Proposition 2, $x^m - 1 = (x^\alpha - 1)\theta_{\frac{m}{\alpha}}(x^\alpha)$. So,

$$v(x)x^m w^*(x) = \mu(x)(x^\alpha - 1),$$

$$v(x)w^*(x) \equiv 0 \pmod{x^\alpha - 1}.$$

A similar argument can be used to prove the other case. □

Lemma 3 (Srinivasulu and Maheshanand, 2016)**:** *If $\mathscr{C}$ is a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive code of type $(\alpha,\beta;k_0,k_1,k_2)$, then $\mathscr{C}^{\perp}$ is an additive code of type $(\alpha,\beta;\alpha-k_0,\beta-k_1-k_2,k_2)$.*

Proposition 4: *Let $\mathscr{C}=\langle(b|0),(l|fh+uf)\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha,\beta;k_0,k_1,k_2)$, where $fhg=x^{\beta}-1$, and with dual code $\mathscr{C}^{\perp}=\langle(\bar{b}|0),(\bar{l}|\overline{fh}+u\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h}=x^{\beta}-1$. Then*

$$\deg(\bar{b})=\alpha-\deg(\gcd(b,l)),$$
$$\deg(\overline{fh})=\beta-\deg(f)-\deg(b)+\deg(\gcd(b,lg)),$$
$$\deg(\bar{f})=\beta-\deg(fh)+\deg(\gcd(b,l))-\deg(\gcd(b,lg)).$$

Proof: From Proposition 1, Theorems 3, 4 and Lemma 3, it is easy to prove the results. □

Proposition 5: *Let $\mathscr{C}=\langle(b|0),(l|fh+uf)\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha,\beta;k_0,k_1,k_2)$, where $fhg=x^{\beta}-1$, and with dual code $\mathscr{C}^{\perp}=\langle(\bar{b}|0),(\bar{l}|\overline{fh}+u\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h}=x^{\beta}-1$. Then,*

$$\bar{b}=\frac{1-x^{\alpha}}{(\gcd(b,l))^{*}}\in\mathbb{Z}_p[x].$$

Proof: Since $(\bar{b}|0)\in\mathscr{C}^{\perp}$ and $(b|0),(l|fh+uf)\in\mathscr{C}$, then, from Proposition 3,

$$(b|0)\circ(\bar{b}|0)=0,$$

$$(l|fh+uf)\circ(\bar{b}|0)=0.$$

Hence, by Lemma 2,

$$b\bar{b}^{*}\equiv 0 \pmod{(x^{\alpha}-1)}$$

and

$$l\bar{b}^{*}\equiv 0 \pmod{(x^{\alpha}-1)}$$

over $\mathbb{Z}_p$. Obviously, we obtain that $\gcd(b,l)\bar{b}^{*}\equiv 0 \pmod{(x^{\alpha}-1)}$, which implies that there exists $\mu\in\mathbb{Z}_p[x]$ such that $\gcd(b,l)\bar{b}^{*}=\mu(x^{\alpha}-1)$. Furthermore, since $\gcd(b,l)|(x^{\alpha}-1)$ and $\bar{b}^{*}|(x^{\alpha}-1)$, from Proposition 4, $\deg(\bar{b})=\alpha-\deg(\gcd(b,l))$. So, we have that $\mu=1$. Therefore

$$\bar{b}^{*}=\frac{x^{\alpha}-1}{(\gcd(b,l))}\in\mathbb{Z}_p[x].$$

Then

$$\bar{b}=\frac{1-x^{\alpha}}{(\gcd(b,l))^{*}}\in\mathbb{Z}_p[x].$$

□

Proposition 6: *Let $\mathscr{C} = \langle (b|0), (l|fh+uf) \rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha, \beta; k_0, k_1, k_2)$, where $fhg = x^\beta - 1$, and with dual code $\mathscr{C}^\perp = \langle (\bar{b}|0), (\bar{l}|\overline{fh}+u\bar{f}) \rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then,*

$$\overline{fh} = \frac{(x^\beta - 1)\gcd(b, lg)^*}{f^* b^*} \in \mathbb{Z}_p[u][x].$$

Proof: Since $\gcd(h, g) = 1$, so we have $p_1 fh + p_2 fg = f$, for some $p_1, p_2 \in \mathbb{Z}_p[u][x]$. Since $(b \mid 0), (0 \mid ufh), (lg \mid ufg) \in \mathscr{C}$, so

$$(0|\frac{b}{\gcd(b, lg)}(up_1 fh + up_2 fg)) = (0|\frac{b}{\gcd(b, lg)}uf) \in \mathscr{C}.$$

And since $(\bar{l}|\overline{fh}+u\bar{f}) \in \mathscr{C}^\perp$, hence, from Proposition 3,

$$(\bar{l}|\overline{fh}+u\bar{f}) \circ (0|\frac{b}{\gcd(b, lg)}uf) = 0.$$

Then, by Lemma 2,

$$(\overline{fh}+u\bar{f})\left(\frac{b^* u f^*}{\gcd(b, lg)^*}\right) \equiv 0 \pmod{(x^\beta - 1)}.$$

This is equivalent to

$$(u\overline{fh})\left(\frac{b^* f^*}{\gcd(b, lg)^*}\right) = u\mu(x^\beta - 1), \tag{1}$$

for some $\mu \in \mathbb{Z}_p[u][x]$.

If (1) holds over $\mathbb{Z}_p[u]$, then it is equivalent to

$$(\overline{fh})\left(\frac{b^* f^*}{\gcd(b, lg)^*}\right) = \mu(x^\beta - 1) \in \mathbb{Z}_p[u][x].$$

We known that $\overline{fh}|x^\beta - 1$, from Corollary 1, we can get $\left(\frac{b^* f^*}{\gcd(b,lg)^*}\right)|(x^\beta - 1)$. By Proposition 4, $\deg(\overline{fh}) = \beta - \deg(f) - \deg(b) + \deg(\gcd(b, lg))$, thus

$$\beta = \deg(\overline{fh}\frac{b^* f^*}{\gcd(b, lg)^*}) = \deg(x^\beta - 1).$$

So, we obtain that $\mu = 1 \in \mathbb{Z}_p[u]$, and hence,

$$\overline{fh} = \frac{(x^\beta - 1)\gcd(b, lg)^*}{f^* b^*} \in \mathbb{Z}_p[u][x].$$

□

Proposition 7: *Let* $\mathscr{C} = \langle (b|0), (l|fh + uf)\rangle$ *be a* $\mathbb{Z}_p\mathbb{Z}_p[u]$*-additive cyclic code of type* $(\alpha, \beta; k_0, k_1, k_2)$*, where* $fhg = x^\beta - 1$*, and with dual code* $\mathscr{C}^\perp = \langle (\overline{b}|0), (\overline{l}|\overline{fh} + u\overline{f})\rangle$*, where* $\overline{f}\overline{g}\overline{h} = x^\beta - 1$*. Then,*

$$\overline{f} = \frac{(x^\beta - 1)\mathrm{gcd}(b, l)^*}{f^*h^*\mathrm{gcd}(b, lg)^*} \in \mathbb{Z}_p[u][x].$$

Proof: In $\mathbb{Z}_p[x]$, one can factorise the polynomials $b,\ l,\ lg$ in the following way

$$l = \mathrm{gcd}(b, l)\rho,$$

$$lg = \mathrm{gcd}(b, lg)\rho\tau_1,$$

$$b = \mathrm{gcd}(b, lg)\tau_2,$$

where $\mathrm{gcd}(\tau_1, \tau_2) = 1$. Therefore, there exist $t_1, t_2 \in \mathbb{Z}_p[x]$ such that $t_1\tau_1 + t_2\tau_2 = 1$. Then,

$$\mathrm{gcd}(b, lg)\rho(t_1\tau_1 + t_2\tau_2) = \mathrm{gcd}(b, lg)\rho$$

and

$$t_1 lg + \rho t_2 b = \frac{\mathrm{gcd}(b, lg)}{\mathrm{gcd}(b, l)} l.$$

Thus,

$$\frac{\mathrm{gcd}(b, lg)}{\mathrm{gcd}(b, l)} \star (l|fh + uf) - t_1 \star (lg|ufg) - \rho t_2 \star (b|0) =$$
$$(0|\frac{\mathrm{gcd}(b, lg)}{\mathrm{gcd}(b, l)}(fh + uf) - t_1 ufg) \in \mathscr{C}.$$

Since $\mathrm{gcd}(\overline{h}, \overline{g}) = 1$, then there exist $\overline{p_1}, \overline{p_2} \in \mathbb{Z}_p[u][x]$ such that $u\overline{p_1}\,\overline{fh} + u\overline{p_2}\,\overline{f}\overline{g} = u\overline{f}$. So, $(u\overline{p_1} + \overline{p_2 g}) \star (\overline{l}|\overline{fh} + u\overline{f}) = (\overline{p_2}\overline{l}\overline{g}|u\overline{f}) \in \mathscr{C}^\perp$. Then, from Proposition 3,

$$(\overline{p_2}\overline{l}\overline{g}|u\overline{f}) \circ (0|\frac{\mathrm{gcd}(b, lg)}{\mathrm{gcd}(b, l)}(fh + uf) - t_1 ufg) = 0.$$

By Lemma 2 and, arranging properly, we obtain that

$$u\overline{f}\left(\frac{\mathrm{gcd}(b, lg)^*}{\mathrm{gcd}(b, l)^*}\right) f^*h^* \equiv 0 \pmod{(x^\beta - 1)}.$$

This is equivalent to

$$u\overline{f}\left(\frac{\mathrm{gcd}(b, lg)^*}{\mathrm{gcd}(b, l)^*}\right) f^*h^* = u\mu(x^\beta - 1), \tag{2}$$

for some $\mu \in \mathbb{Z}_p[u][x]$.

If (2) holds over $\mathbb{Z}_p[u]$, then it is equivalent to

$$\overline{f}\left(\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}\right)f^*h^* = \mu(x^\beta - 1) \in \mathbb{Z}_p[u][x].$$

It is known that $\overline{f}|(x^\beta-1)$. From Corollary 1, we have that $\left(\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}\right)f^*h^*|(x^\beta-1)$. By Proposition 4, $\deg(\overline{f}) = \beta - \deg(fh) + \deg(\gcd(b,l)) - \deg(\gcd(b,lg))$. Thus

$$\beta = \deg(\overline{f}\left(\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}\right)f^*h^*) = \deg(x^\beta - 1).$$

Hence, we obtain that $\mu = 1$, and hence,

$$\overline{f} = \frac{(x^\beta-1)\gcd(b,l)^*}{f^*h^*\gcd(b,lg)^*} \in \mathbb{Z}_p[u][x].$$

□

Proposition 8: *Let $\mathscr{C} = \langle (b|0), (l|fh+uf)\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code of type $(\alpha,\beta;k_0,k_1,k_2)$, where $fhg = x^\beta - 1$, and with dual code $\mathscr{C}^\perp = \langle (\overline{b}|0), (\overline{l}|\overline{fh}+u\overline{f})\rangle$, where $\overline{f}\overline{g}\overline{h} = x^\beta - 1$. Let $\rho = \frac{l}{\gcd(b,l)}$. Then*

$$\overline{l} = \frac{x^\alpha - 1}{b^*}(\lambda_1+\lambda_2).$$

where

$$\begin{cases} \lambda_1 = -\dfrac{\gcd(b,lg)^*}{\gcd(b,l)^*}x^{m-\deg(f)+\deg(l)}(\rho^*)^{-1} \mod \left(\dfrac{b^*}{\gcd(b,lg)^*}\right), \\ \lambda_2 = -\dfrac{b^*}{\gcd(b,lg)^*}x^{m-\deg(fh)+\deg(l)}(\rho^*)^{-1} \mod \left(\dfrac{b^*}{\gcd(b,l)^*}\right). \end{cases}$$

Proof: Since $(b|0) \in \mathscr{C}$ and $(\overline{l}|\overline{fh}+u\overline{f}) \in \mathscr{C}^\perp$, then from Proposition 3, $(\overline{l}|\overline{fh}+u\overline{f}) \circ (b|0) = 0$. By Lemma 2, $\overline{l}b^* \equiv 0 \pmod{x^\alpha - 1}$ and, for some $\lambda \in \mathbb{Z}_p[x]$, we have that $\overline{l} = \frac{x^\alpha-1}{b^*}\lambda$. Next, we will calculate λ.

Since $\frac{\gcd(b,lg)}{\gcd(b,l)} \star (l|fh+uf) \in \mathscr{C}$ and $(\overline{l}|\overline{fh}+u\overline{f}) \in \mathscr{C}^\perp$, then from Proposition 3, $(\overline{l}|\overline{fh}+u\overline{f}) \circ \left(\frac{\gcd(b,lg)}{\gcd(b,l)}l|\frac{\gcd(b,lg)}{\gcd(b,l)}fh + u\frac{\gcd(b,lg)}{\gcd(b,l)}f\right) = 0$. Let $t = \deg\left(\frac{\gcd(b,lg)}{\gcd(b,l)}\right)$ and note that $(fh+uf)^* = f^*h^* + ux^{\deg(h)}f^*$. By Definition 5, we obtain that

$$\begin{aligned}0 =&(\bar{l}|\overline{fh}+u\overline{f})\circ\left(\frac{\gcd(b,lg)}{\gcd(b,l)}l|\frac{\gcd(b,lg)}{\gcd(b,l)}fh+u\frac{\gcd(b,lg)}{\gcd(b,l)}f\right)=\\ &u\bar{l}\theta_{\frac{m}{\alpha}}(x^{\alpha})x^{m-\deg(l)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}l^*\\ &+\overline{fh}\theta_{\frac{m}{\beta}}(x^{\beta})x^{m-\deg(fh)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}f^*h^*\\ &+u\overline{fh}\theta_{\frac{m}{\beta}}(x^{\beta})x^{m-\deg(f)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}f^*\\ &+u\overline{f}\theta_{\frac{m}{\beta}}(x^{\beta})x^{m-\deg(fh)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}f^*h^* \mod (x^m-1).\end{aligned} \tag{3}$$

By Proposition 2, we know that $\theta_{\frac{m}{\alpha}}(x^{\alpha})=\frac{x^m-1}{x^{\alpha}-1}$ and $\theta_{\frac{m}{\beta}}(x^{\beta})=\frac{x^m-1}{x^{\beta}-1}$. And $\bar{l}=\frac{x^{\alpha}-1}{b^*}\lambda$. Applying Propositions 6 and 7, we know that $\overline{fh}=\frac{(x^{\beta}-1)\gcd(b,lg)^*}{f^*b^*}$ and $\overline{f}=\frac{(x^{\beta}-1)\gcd(b,l)^*}{f^*h^*\gcd(b,lg)^*}$. In addend (3), we can replace all the above. Moreover, by Corollary 1, $\frac{b^*}{\gcd(b,lg)^*}|h^*$. Therefore

$$\begin{aligned}0 =&(\bar{l}|\overline{fh}+u\overline{f})\circ\left(\frac{\gcd(b,lg)}{\gcd(b,l)}l|\frac{\gcd(b,lg)}{\gcd(b,l)}fh+u\frac{\gcd(b,lg)}{\gcd(b,l)}f\right)=\\ &u\frac{x^m-1}{b^*}\lambda x^{m-\deg(l)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}l^*\\ &+u\frac{(x^m-1)\gcd(b,lg)^*}{b^*}x^{m-\deg(f)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*} \mod (x^m-1).\end{aligned} \tag{4}$$

Clearly, the addend (4) is equal to

$$\begin{aligned}&u\frac{(x^m-1)\gcd(b,lg)^*}{b^*}(\lambda x^{m-\deg(l)-1-t}\rho^*\\ &+x^{m-\deg(f)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*})\equiv 0 \pmod{(x^m-1)}.\end{aligned} \tag{5}$$

This is equivalent to

$$\begin{aligned}&\frac{(x^m-1)\gcd(b,lg)^*}{b^*}(\lambda x^{m-\deg(l)-1-t}\rho^*\\ &+x^{m-\deg(f)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*})\equiv 0 \pmod{(x^m-1)}\end{aligned}$$

over $\mathbb{Z}_p$. Therefore,

$$(\lambda x^{m-\deg(l)-1-t}\rho^*+x^{m-\deg(f)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*})\equiv 0 \pmod{(x^m-1)} \tag{6}$$

or

$$(\lambda x^{m-\deg(l)-1-t}\rho^*+x^{m-\deg(f)-1-t}\frac{\gcd(b,lg)^*}{\gcd(b,l)^*})\equiv 0 \pmod{\left(\frac{b^*}{\gcd(b,lg)^*}\right)}. \tag{7}$$

Since $\left(\frac{b^*}{\gcd(b,lg)^*}\right)|(x^m-1)$, then (6) implies (7). Since $\gcd(\rho, \frac{b}{\gcd(b,lg)})=1$, therefore ρ^* is invertible modulo $\left(\frac{b^*}{\gcd(b,lg)^*}\right)$. So,

$$\lambda = -\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}x^{m-\deg(f)+\deg(l)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,lg)^*}\right).$$

Let $\lambda_1 = -\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}x^{m-\deg(f)+\deg(l)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,lg)^*}\right)$. Then $\lambda=\lambda_1+\lambda_2$ with $\lambda_2 \equiv 0 \pmod{\left(\frac{b^*}{\gcd(b,lg)^*}\right)}$.

Since $(l|fh+uf) \in \mathscr{C}$ and $(\bar{l}|\overline{fh}+u\overline{f}) \in \mathscr{C}^\perp$, then, by Proposition 3 and Definition 5,

$$\begin{aligned}0 =&(\bar{l}|\overline{fh}+u\overline{f}) \circ (l|fh+uf) = \\ &u\bar{l}\theta_{\frac{m}{\alpha}}(x^\alpha)x^{m-\deg(l)-1}l^* \\ &+\overline{fh}\theta_{\frac{m}{\beta}}(x^\beta)x^{m-\deg(fh)-1}f^*h^* \\ &+u\overline{fh}\theta_{\frac{m}{\beta}}(x^\beta)x^{m-\deg(f)-1}f^* \\ &+u\overline{f}\theta_{\frac{m}{\beta}}(x^\beta)x^{m-\deg(\mathrm{fh})-1}f^*h^* \mod (x^m-1).\end{aligned} \tag{8}$$

By Proposition 2, we know that $\theta_{\frac{m}{\alpha}}(x^\alpha)=\frac{x^m-1}{x^\alpha-1}$ and $\theta_{\frac{m}{\beta}}(x^\beta)=\frac{x^m-1}{x^\beta-1}$. Then $\bar{l}=\frac{x^\alpha-1}{b^*}\lambda$. Applying Propositions 6 and 7, we know that $\overline{fh}=\frac{(x^\beta-1)\gcd(b,lg)^*}{f^*b^*}$ and $\overline{f}=\frac{(x^\beta-1)\gcd(b,l)^*}{f^*h^*\gcd(b,lg)^*}$. In addend (8), we can replace all the above. Moreover, by Corollary 1, $\frac{b^*}{\gcd(b,lg)^*}|h^*$. Therefore, we get that

$$\begin{aligned}0 =&(\bar{l}|\overline{fh}+u\overline{f}) \circ (l|fh+uf) = \\ &u\frac{x^m-1}{b^*}(\lambda_1+\lambda_2)x^{m-\deg(l)-1}l^* \\ &+u\frac{(x^m-1)\gcd(b,lg)^*}{b^*}x^{m-\deg(f)-1} \\ &+u\frac{(x^m-1)\gcd(b,l)^*}{\gcd(b,lg)^*}x^{m-\deg(fh)-1} \mod (x^m-1).\end{aligned} \tag{9}$$

Clearly, the addend (9) is equal to

$$\begin{aligned}&u\frac{x^m-1}{b^*}(\lambda_1+\lambda_2)x^{m-\deg(l)-1}l^* \\ &+u\frac{(x^m-1)\gcd(b,lg)^*}{b^*}x^{m-\deg(f)-1} \\ &+u\frac{(x^m-1)\gcd(b,l)^*}{\gcd(b,lg)^*}x^{m-\deg(fh)-1} \equiv 0 \pmod{(x^m-1)}.\end{aligned}$$

Since $\lambda_1 = -\frac{\gcd(b,lg)^*}{\gcd(b,l)^*}x^{m-\deg(f)+\deg(l)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,lg)^*}\right)$, so

$$\begin{aligned}&u\frac{x^m-1}{b^*}\lambda_1 x^{m-\deg(l)-1}l^* \\ &+u\frac{(x^m-1)\gcd(b,lg)^*}{b^*}x^{m-\deg(f)-1} \equiv 0 \pmod{(x^m-1)}.\end{aligned}$$

Thus,

$$\begin{aligned}&u\frac{x^m-1}{b^*}\lambda_2 x^{m-\deg(l)-1}l^*\\&\quad+u\frac{(x^m-1)\mathrm{gcd}(b,l)^*}{\mathrm{gcd}(b,lg)^*}x^{m-\deg(fh)-1}\equiv 0 \pmod{(x^m-1)}.\end{aligned}$$

Substituting $\frac{l^*}{\mathrm{gcd}(b,l)^*}=\rho^*$, we obtain that

$$\begin{aligned}&u\frac{(x^m-1)\mathrm{gcd}(b,l)^*}{b^*}(\lambda_2 x^{m-\deg(l)-1}\rho^*\\&\quad+\frac{b^*}{\mathrm{gcd}(b,lg)^*}x^{m-\deg(fh)-1})\equiv 0 \pmod{(x^m-1)}.\end{aligned}$$

Arguing similar to the calculation of λ in equation (5), we obtain that

$$\lambda_2=-\frac{b^*}{\mathrm{gcd}(b,lg)^*}x^{m-\deg(fh)+\deg(l)}(\rho^*)^{-1} \bmod \left(\frac{b^*}{\mathrm{gcd}(b,l)^*}\right).$$

□

Theorem 5: *Let* $\mathscr{C}=\langle(b|0),(l|fh+uf)\rangle$ *be a* $\mathbb{Z}_p\mathbb{Z}_p[u]$*-additive cyclic code of type* $(\alpha,\beta;k_0,k_1,k_2)$, *where* $fhg=x^\beta-1$, *and with dual code* $\mathscr{C}^\perp=\langle(\bar{b}|0),(\bar{l}|\overline{fh}+u\bar{f})\rangle$, *where* $\bar{f}\bar{g}\bar{h}=x^\beta-1$. *Let* $\rho=\frac{l}{\mathrm{gcd}(b,l)}$. *Then*

1) $\bar{b}=\frac{1-x^\alpha}{(\mathrm{gcd}(b,l))^*}\in\mathbb{Z}_p[x]$;
2) $\overline{fh}=\frac{(x^\beta-1)\mathrm{gcd}(b,lg)^*}{f^*b^*}\in\mathbb{Z}_p[u][x]$;
3) $\bar{f}=\frac{(x^\beta-1)\mathrm{gcd}(b,l)^*}{f^*h^*\mathrm{gcd}(b,lg)^*}\in\mathbb{Z}_p[u][x]$;
4)

$$\bar{l}=\frac{x^\alpha-1}{b^*}(\lambda_1+\lambda_2),$$

where

$$\begin{cases}\lambda_1=-\dfrac{\mathrm{gcd}(b,lg)^*}{\mathrm{gcd}(b,l)^*}x^{m-\deg(f)+\deg(l)}(\rho^*)^{-1} \bmod \left(\dfrac{b^*}{\mathrm{gcd}(b,lg)^*}\right),\\ \lambda_2=-\dfrac{b^*}{\mathrm{gcd}(b,lg)^*}x^{m-\deg(fh)+\deg(l)}(\rho^*)^{-1} \bmod \left(\dfrac{b^*}{\mathrm{gcd}(b,l)^*}\right).\end{cases}$$

Example 1: Let $p=3,\alpha=4,\beta=4$, $b(x)=x^3+2x^2+x+2, l(x)=x^2+1, f(x)=x+1, h(x)=x+2, g(x)=x^2+1$. According to the results above, we have that $\mathscr{C}=\langle(b|0),(l|fh+uf)\rangle$ is a $\mathbb{Z}_3\mathbb{Z}_3[u]$-additive cyclic code of type $(4,4;2,2,0)$. By Theorem 2, $S_1\cup S_2\cup S_3$ forms a minimal generating set for $\mathscr{C}$ as an $\mathbb{Z}_3[u]$-module, where $S_1=\{(b|0)\}, S_2=\{(l|fh+uf), x\star(l|fh+uf)\}, S_3=\{(lg|ufg)\}$. Then, the generator matrix of $\mathscr{C}$ is

$$G=\begin{pmatrix}2\,1\,2\,1 & 0 & 0 & 0\,0\\ 1\,0\,1\,0 & 2+u & u & 1\,0\\ 0\,1\,0\,1 & 0 & 2+u & u\,1\\ 2\,0\,2\,0 & u & u & u\,u\end{pmatrix}.$$

Applying the formulas of Theorem 5, we have that $\bar{b} = 2x^2 + 1$ and $\overline{fh} = 2x^2 + 2, \bar{f} = 2x^2 + 2, \bar{l} = x + 1$. Therefore, $\mathscr{C}^\perp = \langle(\bar{b}|0), (\bar{l}|\overline{fh} + u\bar{f})\rangle$, is of type $(4, 4; 2, 2, 0)$. By Theorem 2, $S_1 \cup S_2 \cup S_3$ forms a minimal generating set for $\mathscr{C}^\perp$ as an $\mathbb{Z}_3[u]$-module, where $S_1 = \{(\bar{b}|0), x \star (\bar{b}|0)\}, S_2 = \{(\bar{l}|\overline{fh} + u\bar{f}), x \star (\bar{l}|\overline{fh} + u\bar{f})\}, S_3 = \emptyset$. Then, the generator matrix of $\mathscr{C}^\perp$ is

$$H = \begin{pmatrix} 1\,0\,2\,0 & 0 & 0 & 0 & 0 \\ 0\,1\,0\,2 & 0 & 0 & 0 & 0 \\ 1\,1\,0\,0 & 2+2u & 0 & 2+2u & 0 \\ 0\,1\,1\,0 & 0 & 2+2u & 0 & 2+2u \end{pmatrix}.$$

5 Quantum codes from $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive cyclic codes

Proposition 9: *Let $\mathscr{C}$ be a code of length $\alpha + \beta$ over $\mathbb{Z}_2\mathbb{Z}_2[u]$. If $\mathscr{C}$ is self-orthogonal, so is $\Phi(\mathscr{C})$.*

Proof: Let $\mathbb{v} = (v_0, v_1, \ldots, v_{\alpha-1}|v'_0, v'_1, \ldots, v'_{\beta-1}), \mathbb{w} = (w_0, w_1, \ldots, w_{\alpha-1}|w'_0, w'_1, \ldots, w'_{\beta-1}) \in \mathscr{C}$, where $v'_j = a_j + ub_j, w'_j = c_j + ud_j, j = 0, \cdots \beta - 1$. Then

$$\begin{aligned} \mathbb{v} \cdot \mathbb{w} &= u(\sum_{i=0}^{\alpha-1} v_i w_i) + \sum_{j=0}^{\beta-1} v'_j w'_j \\ &= u(\sum_{i=0}^{\alpha-1} v_i w_i) + \sum_{j=0}^{\beta-1} [a_j c_j + u(a_j d_j + b_j c_j)]. \end{aligned}$$

If $\mathscr{C}$ is self-orthogonal, then $\sum_{i=0}^{\alpha-1} v_i w_i + \sum_{j=0}^{\beta-1}(a_j d_j + b_j c_j) = 0$ and $\sum_{j=0}^{\beta-1} a_j c_j = 0$. Thus, in $\mathbb{Z}_2$, we have

$$\Phi(\mathbb{v}) \cdot \Phi(\mathbb{w}) = \sum_{i=0}^{\alpha-1} v_i w_i + \sum_{j=0}^{\beta-1}(b_j d_j + a_j d_j + a_j c_j + b_j c_j + b_j d_j) = 0.$$

Therefore, $\Phi(\mathscr{C})$ is self-orthogonal. □

Note that if $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive cyclic code with $\mathscr{C} = \langle(b(x)|0), (l(x)|f(x)h(x) + uf(x))\rangle$, then the canonical projections $\mathscr{C}_X$ and $\mathscr{C}_Y$ are a cyclic code over $\mathbb{Z}_2$ and a cyclic code over $\mathbb{Z}_2[u]$ generated by $\gcd(b(x), l(x))$ and $f(x)h(x) + uf(x)$, respectively. If $\mathscr{C}$ is separable, then $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$ and $l(x) = 0$.

Lemma 3 (Calderbank et al., 1998)**:** *Let $\mathscr{C}_X = \langle b(x)\rangle$ is a binary linear cyclic code of length α over $\mathbb{Z}_2$. Then $\mathscr{C}_X$ contains its dual code if and only if*

$$x^\alpha - 1 \equiv 0 \pmod{b(x)b^*(x)}.$$

Lemma 4 (Qian et al., 2009)**:** *Let* $\mathscr{C}_Y = \langle f(x)h(x) + uf(x)\rangle$ *be a cyclic code of length* β *over* $\mathbb{Z}_2[u]$*, where* $f(x)h(x)g(x) = x^\beta - 1$*. Then* $\mathscr{C}_Y$ *contains its dual code if and only if*

$$\begin{aligned}
&x^\beta - 1 \equiv 0 \pmod{(uf(x)g(x))(f(x)g(x))^*},\\
&x^\beta - 1 \equiv 0 \pmod{(f(x)h(x))u(f(x)h(x))^*},\\
&x^\beta - 1 \equiv 0 \pmod{(f(x)h(x))(f(x)g(x))^*},\\
&x^\beta - 1 \equiv 0 \pmod{(uf(x)g(x))u(f(x)h(x))^*}.
\end{aligned}$$

Theorem 6: *Let* $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$ *be a separable cyclic code of length* $\alpha + \beta$ *over* $\mathbb{Z}_2\mathbb{Z}_2[u]$*. Then* $\mathscr{C}^\perp \subseteq \mathscr{C}$ *if and only if* $(\mathscr{C}_X)^\perp \subseteq \mathscr{C}_X$ *and* $(\mathscr{C}_Y)^\perp \subseteq \mathscr{C}_Y$*.*

Proof: If $\mathscr{C}^\perp \subseteq \mathscr{C}$, let $\mathbb{v} = (v|v') \in \mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$, where $v \in \mathscr{C}_X,\ v' \in \mathscr{C}_Y$. Let $\mathbb{w} = (w|w') \in \mathscr{C}^\perp = (\mathscr{C}_X)^\perp \times (\mathscr{C}_Y)^\perp$ such that $\mathbb{v} \cdot \mathbb{w} = u(vw) + v'w' = 0$. Then $vw = 0, v'w' = 0$, it implies that $w \in (\mathscr{C}_X)^\perp, w' \in (\mathscr{C}_Y)^\perp$. Since $\mathbb{w} = (w|w') \in \mathscr{C}$, where $w \in \mathscr{C}_X,\ w' \in \mathscr{C}_Y$, it follows that $(\mathscr{C}_X)^\perp \subseteq \mathscr{C}_X$ and $(\mathscr{C}_Y)^\perp \subseteq \mathscr{C}_Y$.

Conversely, if $(\mathscr{C}_X)^\perp \subseteq \mathscr{C}_X$ and $(\mathscr{C}_Y)^\perp \subseteq \mathscr{C}_Y$. Let $\mathbb{v} = (v|v') \in \mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$, where $v \in \mathscr{C}_X,\ v' \in \mathscr{C}_Y$. Let $\mathbb{w} = (w|w') \in \mathscr{C}^\perp = (\mathscr{C}_X)^\perp \times (\mathscr{C}_Y)^\perp$ such that $\mathbb{v} \cdot \mathbb{w} = u(vw) + v'w' = 0$. Then $vw = 0, v'w' = 0$, which implies that $w \in (\mathscr{C}_X)^\perp, w' \in (\mathscr{C}_Y)^\perp$. So, $w \in \mathscr{C}_X,\ w' \in \mathscr{C}_Y$. Hence, $\mathbb{w} = (w|w') \in \mathscr{C}$, so, $\mathscr{C}^\perp \subseteq \mathscr{C}$. □

Corollary 2: *Let* $\mathscr{C} = \mathscr{C}_X \times \mathscr{C}_Y$ *be a separable cyclic code of length* $\alpha + \beta$ *over* $\mathbb{Z}_2\mathbb{Z}_2[u]$*, where* $\mathscr{C}_X = \langle b(x)\rangle$ *and* $\mathscr{C}_Y = \langle f(x)h(x) + uf(x)\rangle$*. Then* $\mathscr{C}^\perp \subseteq \mathscr{C}$ *if and only if the following two conditions are satisfied*

(i) $x^\alpha - 1 \equiv 0 \pmod{b(x)b^*(x)}$.

(ii) $x^\beta - 1 \equiv 0 \pmod{(uf(x)g(x))(f(x)g(x))^*}$, $x^\beta - 1 \equiv 0 \pmod{(f(x)h(x))u(f(x)h(x))^*}$, $x^\beta - 1 \equiv 0 \pmod{(f(x)h(x))(f(x)g(x))^*}$ *and* $x^\beta - 1 \equiv 0 \pmod{(uf(x)g(x))u(f(x)h(x))^*}$.

Theorem 7 (Calderbank et al., 1998)**:** *Let* C *and* C' *be binary* $[n, k, d]$ *and* $[n, k_1, d_1]$ *codes, respectively. If* $C^\perp \subset C'$*, then an* $[[n, k + k_1 - n, \min\{d, d_1\}]]$ *quantum code can be constructed. Especially, if* $C^\perp \subseteq C$*, then there exists an* $[[n, 2k - n, d]]$ *quantum code.*

Using Proposition 9, Corollary 2, and Theorem 7, we can construct quantum codes as follows.

Theorem 8: *Let* $\mathscr{C} = ((b(x)|0), (0|f(x)h(x) + uf(x)))$ *be a* $[\alpha + \beta, 2^{k_0}4^{k_1}2^{k_2}, d_L]$ *separable additive cyclic code of length* $\alpha + \beta$ *over* $\mathbb{Z}_2\mathbb{Z}_2[u]$*, where* d_L *is the minimum Lee distance of* $\mathscr{C}$ *and* $f(x)h(x)g(x) = x^\beta - 1$*. If* $\mathscr{C}^\perp \subseteq \mathscr{C}$*, then there exists a quantum code with parameters* $[[\alpha + 2\beta, 2k_0 + 4k_1 + 2k_2 - \alpha - 2\beta, d_L]]$*.*

Example 2: Let $\alpha = 14, \beta = 7$. $x^{14} - 1 = (x+1)^2(x^3 + x + 1)^2(x^3 + x^2 + 1)^2$ in $\mathbb{Z}_2[x]$ and $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$ in $\mathbb{Z}_2[u][x]$. Let $b(x) = x + 1, f(x) = x + 1, h(x) = x^3 + x^2 + 1, g(x) = x^3 + x + 1,$ and $\mathscr{C} = \langle (b(x)|0), (0|f(x)h(x) + uf(x))\rangle$. Then, $\mathscr{C}$ is a $[21, 2^{13}4^32^3, 2]$ additive cyclic code. Observe that it satisfies the two conditions in Corollary 2. Thus, we have $\mathscr{C}^\perp \subseteq \mathscr{C}$. Then, there exists a quantum code with parameters $[[28, 16, 2]]$.

Example 3: Let $\alpha = 31, \beta = 23$. $x^{31} - 1 = (x+1)(x^5+x^2+1)(x^5+x^3+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)$ in $\mathbb{Z}_2[x]$ and $x^{23} - 1 = (x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$ in $\mathbb{Z}_2[u][x]$. Let $b(x) = x^{10}+x^8+x^6+x^5+x^4+x+1, f(x) = x+1, h(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1, g(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$, and $\mathscr{C} = \langle (b(x)|0), (0|f(x)h(x)+uf(x)) \rangle$. Then, $\mathscr{C}$ is a $[54, 2^{21}4^{11}2^{11}, 5]$ additive cyclic code. Observe that it satisfies the two conditions in Corollary 2. Thus, we have $\mathscr{C}^{\perp} \subseteq \mathscr{C}$. Then, there exists a quantum code with parameters $[[77, 31, 5]]$.

Example 4: Let $\alpha = 93, \beta = 23$. $x^{93} - 1 = (x+1)(x^2+x+1)(x^5+x^2+1)(x^5+x^3+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)(x^{10}+x^5+x^4+x^2+1)(x^{10}+x^8+x^3+x+1)(x^{10}+x^8+x^6+x^5+1)(x^{10}+x^9+x^7+x^2+1)(x^{10}+x^9+x^7+x^5+x^2+x+1)(x^{10}+x^9+x^8+x^5+x^3+x+1)$ in $\mathbb{Z}_2[x]$ and $x^{23} - 1 = (x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$ in $\mathbb{Z}_2[u][x]$. Let $b(x) = x^{15}+x^{14}+x^{11}+x^7+x^5+x^3+x^2+x+1, f(x) = x+1, h(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1, g(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$, and $\mathscr{C} = \langle (b(x)|0), (0|f(x)h(x)+uf(x)) \rangle$. Then, $\mathscr{C}$ is a $[116, 2^{78}4^{11}2^{11}, 5]$ additive cyclic code. Observe that it satisfies the two conditions in Corollary 2. Thus, we have $\mathscr{C}^{\perp} \subseteq \mathscr{C}$. Then, there exists a quantum code with parameters $[[139, 83, 5]]$.

Some more quantum codes with larger length obtained from additive cyclic codes over the ring $\mathbb{Z}_2\mathbb{Z}_2[u]$ are listed in Table 1.

Table 1 Quantum codes $[[N, K, D]]$

α	β	$[\alpha+\beta, 2^{k_0}4^{k_1}2^{k_2}, d_L]$	$[[N, K, D]]$
91	21	$[112, 2^{76}4^{15}2^5, 4]$	$[[133, 89, 4]]$
93	23	$[116, 2^{78}4^{11}2^{11}, 5]$	$[[139, 83, 5]]$
105	21	$[126, 2^{90}4^{15}2^5, 4]$	$[[147, 103, 4]]$
117	15	$[132, 2^{93}4^8 2^5, 6]$	$[[147, 81, 6]]$
126	7	$[133, 2^{113}4^3 2^3, 4]$	$[[140, 104, 4]]$
126	21	$[147, 2^{113}4^{15}2^5, 4]$	$[[168, 128, 4]]$
127	23	$[150, 2^{113}4^{11}2^{11}, 5]$	$[[173, 119, 5]]$
133	15	$[148, 2^{112}4^8 2^5, 6]$	$[[163, 103, 6]]$
154	7	$[161, 2^{138}4^3 2^3, 4]$	$[[168, 126, 4]]$
154	21	$[175, 2^{138}4^{15}2^5, 4]$	$[[196, 150, 4]]$

6 Conclusion

In this paper, we consider the additive cyclic codes over $\mathbb{Z}_p\mathbb{Z}_p[u]$. We determine the generator polynomials of this family of codes, and give their minimal generating sets. Further, we also discuss the relationship of generators between the $\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic code and its dual. Examples are given to show that some quantum codes can be constructed. We believe that some more good quantum codes can be obtained from this class of codes, and it will be an interesting and challenge work in future.

Acknowledgement

The authors would like to thank the anonymous referees and the editor for their careful reading of the paper and valuable comments.

This research is supported by the National Natural Science Foundation of China (Grant Nos. 11701336, 11626144 and 11671235).

References

Abualrub, T., Siap, I. and Aydin, N. (2014a) '$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes', *IEEE Trans. Inform. Theory*, Vol. 60, pp.1508–1514.

Abualrub, T., Siap, I. and Aydogdu, I. (2014b) '$\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-linear cyclic codes', *Proceedings of the International MultiConference of Engineers and Computer Scientists, II*, HongKong, pp.312–613.

Aydogdu, I., Abualrub, T. and Siap, I. (2015) 'On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes', *Int. J. Comput. Math.*, Vol. 92, pp.1806–1814.

Aydogdu, I. and Siap, I. (2015) 'On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes', *Linear Multilinear Algebra*, Vol. 63, pp.2089–2102.

Borges, J., Fernández-Córdoba, C., Pujol, J. and Rifà, J. (2009) '$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: geneartor matrices and duality', *Des. Codes Cryptogr.*, Vol. 54, pp.167–179.

Borges, J., Fernández-Córdoba, C. and Ten-Valls, R. (2016) '$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes', *IEEE Trans. Inform. Theory*, Vol. 62, pp.6348–6354.

Calderbank, A.R., Rains, E.M., Shor, P.M. and Sloane, N.J.A. (1998) 'Quantum error correction via codes over GF(4)', *IEEE Trans. Inform. Theory*, Vol. 44, pp.1369–1387.

Delsarte, P. and Levenshtein, V.I. (1998) 'Association schemes and coding theory', *IEEE Trans. Inform. Theory*, Vol. 44, pp.2477–2504.

Hammons, A., Kumar, P., Calderbank, A., Sloane, N.J.A. and Solé, P. (1994) 'The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes', *IEEE Trans. Inform. Theory*, Vol. 40, pp.301–319.

MacMilliams, F.J. and Sloane, N.J.A. (1975) *The Theory of Error-Correcting Codes*, Pte. Ltd: North-Holland Publishing Company, Amsterdam, New York, Oxford.

Qian, J., Ma, W. and Guo, W. (2009) 'Quantum codes from cyclic codes over finite ring', *International Journal of Quantum Information*, Vol. 7, pp.1277–1283.

Shor, P.W. (1995) 'Scheme for reducing decoherence in quantum computer memory', *Phys. Rev. A*, Vol. 52, p.2493.

Srinivasulu, B. and Maheshanand, B. (2016) '$\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-additive cyclic codes and their duals', *Discrete Math. Algorithm. Appl.*, Vol. 8, pp.1793–8317.

Wan, Z-X. (1997) *Quaternary Codes*, Pte. Ltd: World Scientific Publishing Company, Singapore.