Finite Fields and Their Applications 110 (2026) 102732

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Trace duality and additive complementary pairs of additive cyclic codes over finite chain rings

Sanjit Bhowmick [a,1], Kuntal Deka [a], Alexandre Fotue Tabue [b,2], Edgar Martínez-Moro [c,*,3]

[a] *Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Assam, 781039, India*
[b] *Department of Mathematics, University of Bertoua, Bertoua, Cameroon*
[c] *Institute of Mathematics, University of Valladolid, Spain*

ARTICLE INFO

Article history:
Received 12 June 2025
Received in revised form 11 September 2025
Accepted 21 September 2025
Available online xxxx
Communicated by Gary L. Mullen

MSC:
94B05
15B05
12E10

Keywords:
Additive cyclic codes
Additive complementary pairs
Trace dual
Finite chain ring

ABSTRACT

This paper investigates the algebraic structure of complementary pairs of additive cyclic codes over a finite commutative chain ring of odd characteristic. We demonstrate that for every additive complementary pair of additive codes, both constituent codes are free modules. Moreover, we present a necessary and sufficient condition for a pair of additive codes over a finite commutative chain ring of odd characteristic to form an additive complementary pair. Finally, we show that, in the case of a complementary pair of additive cyclic codes over a finite chain ring of odd characteristic, one of the codes is permutation equivalent to the trace dual of the other.

* Corresponding author.
E-mail addresses: sanjitbhowmick@rnd.iitg.ac.in (S. Bhowmick), kuntaldeka@iitg.ac.in (K. Deka), alexfotue@gmail.com (A. Fotue Tabue), edgar.martinez@uva.es (E. Martínez-Moro).

[1] This author would like to thank the Indian Institute of Technology Guwahati for its hospitality and support.
[2] Supported by a "Research in Pairs" grant by CIMPA while his visit to the Institute of Mathematics, University of Valladolid, Spain.
[3] Partially supported by Grant PID2022-138906NB-C21 funded by MICIU/AEI/10.13039/501100011033 and by ERDF/EU.

https://doi.org/10.1016/j.ffa.2025.102732

1. Introduction

Given a finite field $\mathbb{F}_{q^m}$ (where q is a prime power) and a non-negative integer n, additive codes over $\mathbb{F}_{q^m}$ are subsets of $\mathbb{F}_{q^m}^n$ that are closed under addition but not necessarily under scalar multiplication by elements of $\mathbb{F}_{q^m}$. Delsarte first studied additive codes over a finite field in 1971 [10]. In particular, significant attention has been devoted to the class of additive codes that are closed under scalar multiplication by a subfield $\mathbb{F}_q \subset \mathbb{F}_{q^m}$, namely, $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^m}^n$. We will refer to them as $\mathbb{F}_{q^m}|\mathbb{F}_q$ linear codes and the main theory on such codes can be found in [13].

Now, if we consider a finite chain ring R, linear codes over R are simply R-submodules of R^n. For a given Galois extension $S|R$ of finite chain rings, we can also define $S|R$ additive codes in the same fashion as in the finite field case. If a code is closed under the cyclic shift, we refer to it as cyclic. There are a few works on cyclic additive codes over finite fields and finite chain rings; see, for example, [16,20,21] and the references therein.

In the context of quantum error-correcting codes, this class of codes has attracted interest, especially when the alphabet is a quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. For instance, Ashikhmin and Knill [1] constructed quantum codes using $\mathbb{F}_{q^2}|\mathbb{F}_q$ linear codes. Later, in [15], the authors revealed a deep connection between the existence of quantum error-correcting codes and $\mathbb{F}_{q^2}|\mathbb{F}_q$ linear codes endowed with a suitable inner product.

On the other hand, a pair of linear codes $\{\mathcal{C}, \mathcal{D}\}$ of length n over a finite field $\mathbb{F}_q$ is called a *linear complementary pair* (LCP) if $\mathcal{C} \cap \mathcal{D} = \{0\}$ and $\mathcal{C} + \mathcal{D} = \mathbb{F}_q^n$, that is, $\mathcal{C} \oplus \mathcal{D} = \mathbb{F}_q^n$. When $\mathcal{D} = \mathcal{C}^\perp$, the dual code of $\mathcal{C}$, the code $\mathcal{C}$ is referred to as a *linear complementary dual* (LCD) code. LCD codes were first introduced by Massey in 1992 [17], and the interest in both LCD and LCP codes has recently reemerged due to their applications in securing systems against side-channel and fault injection attacks [6,7]. In this context, the security parameter when one uses an LCP $\{\mathcal{C}, \mathcal{D}\}$ is defined as $\min\{\mathrm{d}(\mathcal{C}), \mathrm{d}(\mathcal{D}^\perp)\}$, where $\mathrm{d}(\mathcal{C})$ denotes the minimum Hamming distance of the code $\mathcal{C}$. In the LCD case, since $\mathcal{D}^\perp = \mathcal{C}$, the security parameter simplifies to $\mathrm{d}(\mathcal{C})$.

Carlet et al. [8] proved that if $\{\mathcal{C}, \mathcal{D}\}$ is an LCP where both $\mathcal{C}$ and $\mathcal{D}$ are cyclic codes over $\mathbb{F}_q$, then $\mathcal{C}$ is permutation equivalent to $\mathcal{D}^\perp$. They further showed that this result extends to 2D cyclic codes, provided the code length is relatively prime to the characteristic of $\mathbb{F}_q$ (i.e., the semi-simple case). Extending this result, Güneri et al. [12] showed that for abelian codes and the semisimple case, the equivalence $\mathcal{C} \simeq \mathcal{D}^\perp$ also holds. This result is more general and can be viewed in the context of group codes; thus, the same result has been proven for an LCP of group codes without requiring any assumption on the characteristic of the field (i.e., without the need for semi-simplicity), see [5]. Finally, this result also holds for LCP codes over finite chain rings [11]. Recently, a similar result was proven for an LCP of algebraic geometry codes in [3]. There are a few works on additive complementary dual codes; see, for example, [9] and the references therein.

In the present work, additive complementary pairs of additive cyclic codes over a finite commutative chain ring of odd characteristic are investigated. The main results in the

paper are the following. We establish that every additive complementary pair of codes forms a pair of free modules, and a necessary and sufficient condition is derived for the existence of such pairs over a finite commutative chain ring (see Theorems 5.5 and 5.9). Furthermore, in the case of cyclic additive codes over a finite commutative chain ring, we show that one code of the constituent codes is permutation equivalent to the trace dual of the other (see Theorem 6.4).

The paper outline is as follows. Section 2 provides some preliminaries on additive codes and the trace duality. In Section 3, we study the structure and polynomial definition of additive cyclic codes over a Galois extension $S|R$ of finite chain rings. Section 4 deals with the description of the trace dual of the additive codes defined in Section 3. Additive complementary pairs of codes (not necessarily cyclic ones) are studied in Section 5, while in Section 6, additive complementary pairs of cyclic codes are tackled, providing a generalization of the result in [8] for this type of codes.

2. Preliminaries

A chain ring is a ring whose ideal lattice forms a chain. In this paper, S and R will denote finite commutative chain rings. We will denote the maximal ideal of S as $\mathfrak{m}_S$ and its nilpotency index as e. We say that S is a ring extension of R, denoted $S|R$, if R is a subring of S, $\mathfrak{m}_R = \mathfrak{m}_S \cap \mathcal{R}$, and $1_R = 1_S$. The extension $S|R$ is a Galois extension of degree 2 if S is isomorphic to the quotient ring $R[x]/\langle f(x)\rangle$, where $f(x)$ is a basic irreducible polynomial of degree 2 over R. The Galois group $\mathtt{Aut}_R(S)$ of this extension consists of those ring automorphisms of S such that, when restricted to R, are the identity map of R. From now on, and throughout the entire paper, and the ring extension $S|R$ will be a Galois extension of degree 2 and, for technical reasons, R (thus also S) will be chain rings of odd characteristic.

We will denote by $R/\mathfrak{m} = \mathbb{F}_q$ and $S/\mathfrak{m} = \mathbb{F}_{q^2}$ the quotient of R (respectively S) by its maximal ideal. According to [18, Theorem XV.2], we have $\mathtt{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^2}) \simeq \mathtt{Aut}_R(S)$ and $\mathrm{rank}_R(S) = [\mathbb{F}_{q^2} : \mathbb{F}_q] = |\mathtt{Aut}_R(S)|$. Thus, the ring S can be regarded as a free R-module of rank 2.

For the chain ring S, the *Teichmüller set* $\mathcal{T} \subset S$ is the unique set of q^2 elements in S such that the image of $\mathcal{T}$ under the canonical projection $S \mapsto S/\mathfrak{m} = \mathbb{F}_{q^2}$ is the entire field, each element $t \in \mathcal{T}$ satisfies $t^{q^2} = t$, and $\mathcal{T}$ contains the multiplicative representatives of $\mathbb{F}_{q^2}$ in S. If $S|R$ is a Galois extension of finite chain rings of degree 2, then there exists an element $\xi \in S$ whose multiplicative order is $q^2 - 1$ [22, Theorem 14.27]. Then, given the following set is called the *Teichmüller set* of S

$$\mathcal{T}_S := \{0, 1, \xi, \xi^2, \ldots, \xi^{q^2-2}\}.$$

One can define $\zeta = \xi^{\frac{q^2-1}{q-1}}$, and hence $\zeta \in R$ has multiplicative order $q-1$. Thus, it is easy to check that the set $\mathcal{T}_R = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{q-2}\}$ is the *Teichmüller set* of R.

Let $\mathrm{Aut}_R(S)$ denote the group of all R-automorphisms of S. Since S is a Galois extension of R of degree 2, it follows, by an argument similar to that in [22, Corollary 14.33], that $\mathrm{Aut}_R(S)$ is a cyclic group of order 2.

In fact, the map $\phi : S \to S$ defined by

$$\phi(\alpha) = \alpha_0 + \alpha_1 \xi^q, \tag{1}$$

for $\alpha = \alpha_0 + \alpha_1 \xi$ with $(\alpha_0, \alpha_1) \in R^2$, is an automorphism of S that fixes R. Moreover, R is the largest subring of S fixed pointwise by ϕ. This automorphism ϕ is called the *Frobenius automorphism* of S over R, and it generates the cyclic group $\mathrm{Aut}_R(S)$.

Let $\mathrm{Tr} : S \to R$ the map given by $s \mapsto s + \phi(s)$, for all $s \in S$. Tr is called *the generalized trace* of S relative to R. It is well known that Tr is a surjective R-module homomorphism. The following lemma will be useful later.

Lemma 2.1. *The kernel of* Tr *is equal to* μR*, for some* $\mu \in S \setminus R$ *such that* $\mathrm{Tr}(\mu) = 0$*, i.e.,*

$$\mathrm{Ker}(\mathrm{Tr}) = \mu R = \{\mu r \mid r \in R\}. \tag{2}$$

Moreover, $\mu^2 \in R$ *and* $\mathrm{Tr}(\mu^2) = 2\mu^2$*.*

Proof. It is well known that Tr is a surjective R-module homomorphism. Therefore, by the first isomorphism theorem for modules, we have $S/\mathrm{Ker}(\mathrm{Tr}) \simeq R$. Consequently, $|\mathrm{Ker}(\mathrm{Tr})| = |R|$. Furthermore, we observe that for any $r \in R$, we have that $\mathrm{Tr}(r) = r + \phi(r) = 2r$, since ϕ is the Frobenius automorphism of S over R (and $\phi(r) = r$ for $r \in R$). Thus, $\mathrm{Tr}(r) \neq 0$ for all $r \in R \setminus \{0\}$ since the characteristic of R is an odd prime. Moreover, there exist $\mu \in S \setminus R$ such that $\mathrm{Tr}(\mu) = 0$. Let $x \in \mu R$, then $x = \mu r$, for some $r \in R$. It follows that $\mathrm{Tr}(x) = 0$, for all $x \in \mu R$; hence, $\mu R = \ker(\mathrm{Tr})$. Finally, $\mathrm{Tr}(\mu) = 0 \Leftrightarrow \mu = -\phi(\mu)$. Thus, $\phi(\mu^2) = (\phi(\mu))^2 = (-\mu)^2 = \mu^2$. It follows that $\mu^2 \in R$ and $\mathrm{Tr}(\mu^2) = 2\mu^2$. □

Furthermore, for an element $\mu \in S \setminus R$ such that $\mathrm{Tr}(\mu) = 0$, the set $\{1, \mu\}$ is a basis of S over R, as S is a free R-module. Note that μ is an invertible element in the ring S.

Definition 2.2. A linear code of length n over R is just an R-submodule of R^n. An $S|R$ additive code of length n is just an R-submodule of S^n.

Definition 2.3. For an $S|R$ additive code of length n, the trace dual of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \{\mathbf{a} \in S^n \mid \mathrm{Tr}(\mathbf{a} \cdot \mathbf{c}) = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}. \tag{3}$$

Note that $\mathcal{C} = \left(\mathcal{C}^{\perp_{\mathrm{Tr}}}\right)^{\perp_{\mathrm{Tr}}}$ and $|\mathcal{C}||\mathcal{C}^{\perp_{\mathrm{Tr}}}| = |S^n|$ (see [23]).

3. Structure of additive cyclic codes

Throughout the paper, we assume that the length of the codes n is a positive integer that is not divisible by the characteristic of the residue field $R/\mathfrak{m} = \mathbb{F}_q$. Thus, the polynomial $x^n - 1$ is square-free in $\mathbb{F}_q[x]$ and $x^n - 1$ admits a unique factorization into a product of pairwise coprime, basic irreducible polynomials in R (resp. S). We will denote the following polynomial quotient rings as

$$\mathcal{R}_n = R[x]/\langle x^n - 1\rangle, \qquad \mathcal{S}_n = S[x]/\langle x^n - 1\rangle. \tag{4}$$

Both rings $\mathcal{R}_n$ and $\mathcal{S}_n$ are principal, see [19]. If we set $\overline{x} = x + \langle x^n - 1\rangle$, the map

$$\begin{array}{rccc} \Psi: & S^n & \longrightarrow & \mathcal{S}_n \\ & (a_0, \ldots, a_{n-1}) & \mapsto & \sum_{j=0}^{n-1} a_j \overline{x}^j \end{array}$$

is an R-module isomorphism. Moreover, $\mathcal{R}_n$ is a free R-module of rank n, and $\mathcal{S}_n$ is a free R-module of rank $2n$.

Definition 3.1. An $S|R$ additive cyclic code of length n is an R-submodule $\mathcal{C}$ of S^n that satisfies

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \implies (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

It is easy to check that a (linear) cyclic code of length n over S can be seen as an R-submodule of $\mathcal{R}_n$, and an additive cyclic code of length n can be represented as an R-submodule of $\mathcal{S}_n$. We will follow this polynomial notation of (additive) cyclic codes in the rest of the paper. For more details on additive cyclic codes over chain rings, we refer to [16] and the references therein.

Lemma 3.2. *A nonempty subset $\mathcal{C}$ of S^n is an $S|R$ additive cyclic code of length n if and only if $\Psi(\mathcal{C})$ is an $\mathcal{R}_n$-submodule of $\mathcal{S}_n$.*

In the sequel, we identify any free $S|R$ additive code of length n with an $\mathcal{R}_n$-submodule of $\mathcal{S}_n$. The quotient ring $\mathcal{S}_n$ is a free $\mathcal{R}_n$-module of rank two. Therefore, any $\mathcal{R}_n$-submodule of $\mathcal{S}_n$ is generated by at most two elements of $\mathcal{S}_n$. From now on, recall also that $\mathrm{Ker}(\mathrm{Tr}) = \mu R$ (see 2.1).

Theorem 3.3. *Let $\mathcal{C}$ be a free $S|R$ additive cyclic code of length n. Then there exist unique monic divisors $f(x)$ and $g(x)$ of $x^n - 1$ in $R[x]$ and a polynomial $r(x)$ in $R[x]$ with $\deg(f(x)r(x)) < \deg(g(x))$ for which*

$$\mathcal{C} = \langle f(\overline{x})(1 + \mu r(\overline{x}))\rangle_{\mathcal{R}_n} \oplus \langle \mu g(\overline{x})\rangle_{\mathcal{R}_n}.$$

Moreover, $S_1 \cup S_2$ is an R-basis of $\mathcal{C}$, where

$$S_1 := \{\overline{x}^i f(\overline{x})(1+\mu r(\overline{x})) \mid 0 \le i < n - \deg(f(x))\};$$
$$S_2 := \{\overline{x}^j \mu g(\overline{x}) \ : \ 0 \le j < n - \deg(g(x))\}.$$

Proof. To prove the result, we first define a map

$$\begin{array}{rccc} \psi : & \mathcal{C} & \to & \mathcal{R}_n \\ & a(\overline{x}) + \mu b(\overline{x}) & \mapsto & a(\overline{x}). \end{array}$$

Note that ψ is an $\mathcal{R}_n$-module homomorphism. Therefore, $\psi(\mathcal{C})$ is an ideal of $\mathcal{R}_n$. Since $\mathcal{C}$ is free (as R-module), then there is a free submodule $\mathcal{C}_1$ of $\mathcal{C}$ such that the restriction of ψ to $\mathcal{C}_1$ is an R-module isomorphism. Thus $\psi(\mathcal{C})$ is a free cyclic code over R. Then there exists a unique divisor $f(x)$ of x^n-1 in $R[x]$ such that $\psi(\mathcal{C}) = \langle f(\overline{x})\rangle_{\mathcal{R}_n}$. Consequently, $\mathcal{C}_1$ is also cyclic. Thus, $\mathcal{C}_1 = \langle f(\overline{x}) + \mu r_0(\overline{x})\rangle_{\mathcal{R}_n}$ where $r_0(x) \in R[x]$. Besides, $\mathcal{C} = \mathcal{C}_1 \oplus \mathrm{Ker}(\psi)$ and $\mathrm{Ker}(\psi)$ is free as an R-module. Now,

$$\mathrm{Ker}(\psi) = \{a(\overline{x}) + \mu b(\overline{x}) \in \mathcal{C} \mid a(\overline{x}) = 0\}.$$

If we define the set $A = \{b(\overline{x}) \in \mathcal{R}_n \mid \mu b(\overline{x}) \in \mathrm{Ker}(\psi)\}$, then $\mathrm{Ker}(\psi) = \mu A$. We have A is an ideal of the principal ideal ring $\mathcal{R}_n$. Therefore, there exists a unique monic divisor $g(x)$ of $x^n - 1$ in $R[x]$ such that $A = \langle g(\overline{x})\rangle_{\mathcal{R}_n}$. Thus,

$$\mathcal{C} = \langle f(\overline{x}) + \mu r_0(\overline{x}), \mu g(\overline{x})\rangle_{\mathcal{R}_n}$$

for some polynomial $r_0(x)$ in $R[x]$. If $\deg(r_0(x)) \ge \deg(g(x))$. Then, by division algorithm, there exist $s(x)$ and $u(x)$ in $R[x]$ such that $r_0(x) = u(x)g(x) + s(x)$ with $\deg(s(x)) < \deg(g(x))$. Thus,

$$\mathcal{C} = \langle f(\overline{x}) + \mu r_0(\overline{x}), \mu g(\overline{x})\rangle_{\mathcal{R}_n} = \langle f(\overline{x}) + \mu s(\overline{x}), \mu g(\overline{x})\rangle_{\mathcal{R}_n}.$$

Hence, we may consider $\deg(r_0(x)) < \deg(g(x))$. Note that $h(\overline{x})(f(\overline{x}) + \mu r_0(\overline{x})) = \mu h(\overline{x}) r_0(\overline{x}) \in \mathcal{C}_1 \cap \mathrm{Ker}(\psi) = \{0\}$, where $f(x)h(x) = x^n - 1$. It follows that $x^n - 1$ divides $h(x)r_0(x)$. Thus, $f(x)$ divides $r_0(x)$, since $f(x)$ and $h(x)$ are coprime. Hence, we have that $r_0(x) = r(x)f(x)$ since $f(x)$ divides $r_0(x)$ and

$$\mathcal{C} = \langle f(\overline{x}) + \mu r_0(\overline{x})\rangle_{\mathcal{R}_n} \oplus \langle \mu g(\overline{x})\rangle_{\mathcal{R}_n} = \langle f(\overline{x})(1+\mu r(\overline{x}))\rangle_{\mathcal{R}_n} \oplus \langle \mu g(\overline{x})\rangle_{\mathcal{R}_n},$$

where $\deg(r(x)) < \deg(g(x)) - \deg(f(x))$. Moreover, the sets

$$\{\overline{x}^i f(\overline{x})(1+\mu r_0(\overline{x})) \mid 0 \le i < n - \deg(f)\}$$

and $\{\overline{x}^j \mu g(\overline{x}) \ : \ 0 \le j < n - \deg(g)\}$ are the R-bases of $\langle f(\overline{x}) + \mu r_0(\overline{x})\rangle_{\mathcal{R}_n}$ and $\langle \mu g(\overline{x})\rangle_{\mathcal{R}_n}$, respectively. Therefore, $S_1 \cup S_2$ is an R-basis of $\mathcal{C}$. $\square$

4. Trace duality

Recall that $\mathcal{S}_n$ is a free R-module of rank $2n$. The $\star$-inner and $\circledast$-inner product on $\mathcal{S}_n$, defined by

$$\left(\sum_{i=0}^{n-1} a_i\overline{x}^i\right) \star \left(\sum_{i=0}^{n-1} b_i\overline{x}^i\right) = \sum_{i=0}^{n-1} a_i b_i, \tag{5}$$

and

$$\left(\sum_{i=0}^{n-1} a_i\overline{x}^i\right) \circledast \left(\sum_{i=0}^{n-1} b_i\overline{x}^i\right) = \mathrm{Tr}\left(\sum_{i=0}^{n-1} a_i b_i\right), \tag{6}$$

are non-degenerate symmetric bilinear forms over S and R, respectively. The bilinear form on $\mathcal{S}_n$ with values in R given by $\circledast$ is called *the trace* over $\mathcal{S}_n$. Note that

$$\alpha\mathbf{u}(\overline{x}) \circledast \beta\mathbf{v}(\overline{x}) = \mathrm{Tr}(\alpha\beta)(\mathbf{u}(\overline{x}) \star \mathbf{v}(\overline{x})),$$

for all $(\mathbf{u}(\overline{x}), \mathbf{v}(\overline{x}))$ in $(\mathcal{R}_n)^2$ and $(\alpha, \beta) \in S^2$.

Remark 4.1. Let $a(\overline{x}), b(\overline{x}), a'(\overline{x}), b'(\overline{x}) \in \mathcal{R}_n$. Then

$$(a(\overline{x}) + \mu b(\overline{x})) \circledast (a'(\overline{x}) + \mu b'(\overline{x})) = 2(a(\overline{x}) \star a'(\overline{x}) + \mu^2(b(\overline{x}) \star b'(\overline{x}))).$$

Definition 4.1. Let $\mathcal{C}$ be an $S|R$ additive code of length n. The trace dual of $\mathcal{C}$, denoted $\mathcal{C}^{\perp_{\mathrm{Tr}}}$, is defined as

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} := \left\{\mathbf{u}(\overline{x}) \in \mathcal{S}_n \mid (\forall \mathbf{c}(\overline{x}) \in \mathcal{C})(\mathbf{u}(\overline{x}) \circledast \mathbf{c}(\overline{x}) = 0)\right\}. \tag{7}$$

Let $\mathcal{C}$ be an $S|R$ additive code of length n. If $\mathbf{u}(\overline{x}) \in \mathcal{C}^{\perp_{\mathrm{Tr}}}$, $\mathbf{c}(\overline{x}) \circledast \mathbf{u}(\overline{x}) = 0$ for all $\mathbf{c}(\overline{x}) \in \mathcal{C}$. Since $\mathbf{c}(\overline{x}) \in \mathcal{C}$, we know that $\overline{x}^{n-1}\mathbf{c}(\overline{x})$ is also a codeword. Thus,

$$0 = \overline{x}^{n-1}\mathbf{c}(\overline{x}) \circledast \mathbf{u}(\overline{x}) = \mathbf{c}(\overline{x}) \circledast \overline{x}\mathbf{u}(\overline{x})$$

for all $\mathbf{c}(\overline{x})$ from $\mathcal{C}$. Therefore $\overline{x}\mathbf{u}(\overline{x}) \in \mathcal{C}^{\perp_{\mathrm{Tr}}}$ and $\mathcal{C}^{\perp_{\mathrm{Tr}}}$ is also an $S|R$ additive code of length n. Henceforth, we obtain the following proposition.

Proposition 4.2. *Let $\mathcal{C}$ be an $S|R$ additive cyclic code of length n. Then $\mathcal{C}^{\perp_{\mathrm{Tr}}}$ is also an $S|R$ additive cyclic code of length n.*

The $\circledast$-inner product is an R-bilinear form. On the other hand, $\mathcal{C}$ and $\mathcal{C}^{\perp_{\mathrm{Tr}}}$ are $\mathcal{R}_n$-submodules of the $\mathcal{R}_n$-module. Thus, we have the following remark.

Lemma 4.2. *Let $f(x), f'(x), g(x)$ and $g'(x)$ be monic divisors of $x^n - 1$ over R and $(r(x), r'(x)) \in (R[x])^2$ with $\deg(f(x)r(x)) < \deg(g(x))$ and $\deg(f'(x)r'(x)) < \deg(g'(x))$ such that $\mathcal{C} = \langle f(\overline{x})(1 + \mu r(\overline{x})), \mu g(\overline{x})\rangle_{\mathcal{R}_n}$. Then*

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \langle f'(\overline{x})(1 + \mu r'(\overline{x})), \mu g'(\overline{x})\rangle_{\mathcal{R}_n}$$

if and only if for all $0 \le i, j < n$,

$$\overline{x}^i f(\overline{x}) \star \overline{x}^j f'(\overline{x}) = -\mu^2(\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x})); \tag{E1}$$

$$\overline{x}^i g(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x}) = 0; \tag{E2}$$

$$\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j g'(\overline{x}) = 0; \tag{E3}$$

$$\overline{x}^i g(\overline{x}) \star \overline{x}^j g'(\overline{x}) = 0. \tag{E4}$$

Moreover, $\deg(f(x)) + \deg(f'(x)) + \deg(g(x)) + \deg(g'(x)) = 2n$.

Proof. Set

$$A(\overline{x}) = f(\overline{x})\big(1+\mu r(\overline{x})\big), \quad B(\overline{x}) = \mu g(\overline{x}), \quad A'(\overline{x}) = f'(\overline{x})\big(1+\mu r'(\overline{x})\big), \quad B'(\overline{x}) = \mu g'(\overline{x}).$$

Every element of $\mathcal{C}$ (resp. $\mathcal{C}^{\perp_{\mathrm{Tr}}}$) is an $\mathcal{R}_n$-linear combination of shifts $\overline{x}^i A, \overline{x}^i B$ (resp. $\overline{x}^j A', \overline{x}^j B'$). Hence $\mathcal{C}^{\perp_{\mathrm{Tr}}} = \langle A', B'\rangle_{\mathcal{R}_n}$ if, and only if for all $0 \le i, j < n$ the four pairings

$$\overline{x}^i A \circledast \overline{x}^j A' = \overline{x}^i B \circledast \overline{x}^j A' = \overline{x}^i A \circledast \overline{x}^j B' = \overline{x}^i B \circledast \overline{x}^j B' = 0$$

vanish. Now, $\mathrm{Tr}(\mu) = 0$ and $\mathrm{Tr}(\mu^2) = 2\mu^2$, by bilinearity we have

$$\begin{aligned}
\overline{x}^i A \circledast \overline{x}^j A' &= 2\left(\overline{x}^i f(\overline{x}) \star \overline{x}^j f'(\overline{x}) + \mu^2\left(\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x})\right)\right);\\
\overline{x}^i B \circledast \overline{x}^j A' &= 2\mu^2\left(\overline{x}^i g(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x})\right);\\
\overline{x}^i A \circledast \overline{x}^j B' &= 2\mu^2\left(\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j g'(\overline{x})\right);\\
\overline{x}^i B \circledast \overline{x}^j B' &= 2\mu^2\left(\overline{x}^i g(\overline{x}) \star \overline{x}^j g'(\overline{x})\right).
\end{aligned}$$

Since μ^2 and 2 is invertible in R, we have

$$\begin{aligned}
\overline{x}^i f(\overline{x}) \star \overline{x}^j f'(\overline{x}) &= -\mu^2(\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x})),\\
\overline{x}^i g(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x}) &= 0,\\
\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j g'(\overline{x}) &= 0,\\
\overline{x}^i g(\overline{x}) \star \overline{x}^j g'(\overline{x}) &= 0,
\end{aligned}$$

which are precisely (E1)– (E4). This proves the equivalence.

Finally, the degree relation follows from the size/count identity for a code and its dual:

$$|\mathcal{C}| \cdot |\mathcal{C}^{\perp_{\mathrm{Tr}}}| = |\mathcal{R}_n|^2,$$

and the standard formula expressing the size of a cyclic code generated by polynomials of degrees $\deg(f), \deg(g)$ (and similarly for f', g'). Comparing exponents yields

$$\deg(f) + \deg(f') + \deg(g) + \deg(g') = 2n,$$

as required. □

Example 4.3. Let $R = \mathbb{Z}_9$ and define $S = R[\alpha]$, where $\alpha^2 = -1$. Consider the additive cyclic code $\mathcal{C} := \langle 1 + \alpha\overline{x} \rangle_{\mathcal{R}_n}$, where n is a positive integer coprime to 3. The trace dual of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \left\langle f'(\overline{x})\big(1 + \alpha r'(\overline{x})\big),\ \mu g'(\overline{x}) \right\rangle_{\mathcal{R}_n},$$

where $f'(x)$ and $g'(x)$ are monic divisors of $x^n - 1$ over R, and $r'(x) \in R[x]$ with $\deg(r'(x)) < \deg(g'(x)) - \deg(f'(x))$ (since $\mathrm{Tr}(\alpha) = 0$). We have $\mathrm{rk}_R(\mathcal{C}) = \mathrm{rk}_R(\mathcal{C}^{\perp_{\mathrm{Tr}}}) = n = \deg(f'(x)g'(x))$, and the following condition holds: For all $0 \le i, j < n$

$$\overline{x}^i \star \overline{x}^j f'(\overline{x}) = \overline{x}^{i+1} \star \overline{x}^j f'(\overline{x}) r'(\overline{x}), \text{ and } \overline{x}^i \star \overline{x}^j g'(\overline{x}) = 0. \tag{8}$$

From this, it follows that $g'(x) = x^n - 1$ and $f'(x) = 1$, so that $\deg(r'(x)) < n$. Then, equation (8) becomes: for all $0 \le i, j < n$, $\delta_{i,j} = \overline{x}^i \star \overline{x}^j = \overline{x}^{i+1} \star \overline{x}^j r'(\overline{x})$. This implies $r'(\overline{x}) = \overline{x}$, and therefore $\mathcal{C}$ is a trace self-dual additive cyclic code.

To determine the trace dual of an additive cyclic $R|S$ code of length n, we will define the following polynomial operator:

$$\begin{array}{rccc} {}^* : & S[x]\backslash\{0\} & \to & S[x]\backslash\{0\} \\ & a(x) & \mapsto & a^*(x) = x^{\deg(a(x))} a(x^{-1}). \end{array} \tag{9}$$

Note that if $a(0) \neq 0$ then $\deg(a) = \deg(a^*)$.

Lemma 4.4. *Let $a(x)$ and $b(x)$ be two polynomials over R of degree at most $n-1$. Then $x^n - 1$ divides $a(x)b(x)$ if and only if*

$$u(\overline{x})a(\overline{x}) \star v(\overline{x})b^*(\overline{x}) = 0$$

for any $(u(x), v(x)) \in (R[x])^2$.

Proof. Let us prove $x^n - 1$ divides $a(x)b(x)$ if and only if $u(\overline{x})a(\overline{x}) \star v(\overline{x})b^*(\overline{x}) = 0$, for any $(u(x), v(x)) \in (R[x])^2$.

$\Rightarrow$) Suppose $x^n - 1$ divides $a(x)b(x)$. Then in the quotient ring $\mathcal{R}_n$, we have $\mathbf{a}(\overline{x})\mathbf{b}(\overline{x}) = 0$. Multiplying on the left by any $u(\overline{x})$ and on the right by any $v(\overline{x})$, we get $u(\overline{x})a(\overline{x})b(\overline{x})v(\overline{x}) = 0$. That is,

$$u(x)a(x)b(x)v(x) = (x^n - 1)q(x),$$

for some $\mathbf{q}(x) \in R[x]$. Now consider

$$(u(\overline{x})a(\overline{x})) \star (v(\overline{x})b^*(\overline{x})) = [\text{constant term of}]\ u(x)a(x) \cdot (v(x)b^*(x^{-1})).$$

But since $b^*(x^{-1}) = x^{-\deg b}b(x)$, it follows that

$$u(x)a(x) \cdot v(x)b^*(x^{-1}) = x^{-\deg(b)}u(x)a(x)b(x)v(x) = x^{-\deg b}(x^n - 1)q(x).$$

Since $(x^n - 1)q(x)$ has no degree zero term, neither does $x^{-\deg b}(x^n - 1)q(x)$. Thus, the constant coefficient is zero: $(u(\overline{x})a(\overline{x})) \star (v(\overline{x})b^*(\overline{x})) = 0$.

$\Leftarrow$) Conversely, assume that for all $u(x), v(x) \in R[x]$,

$$(u(\overline{x})a(\overline{x})) \star (v(\overline{x})b^*(\overline{x})) = 0.$$

We argue by contradiction. Suppose that $a(\overline{x})b(\overline{x}) = 0$. Then $a(x)b(x)$ is nonzero in $\mathcal{R}_n$, which is a free R-module of rank n. The bilinear form

$$(f, g) \mapsto (f(\overline{x}) \star g(\overline{x}))$$

is non-degenerate on the free R-module $\mathcal{R}_n$. Hence, there exists some $w(x)$ such that $(w(\overline{x}) \star a(\overline{x})b(\overline{x})) \neq 0$. Define $u(x) = 1$ and $v(x) = w(x)a(x)x^{-\deg b}$, so that $v(x)b^*(x^{-1}) = w(x)a(x)b(x)$, and thus

$$(u(\overline{x})a(\overline{x})) \star (v(\overline{x})b^*(\overline{x})) = (a(\overline{x})) \star (w(\overline{x})a(\overline{x})b(\overline{x})) \neq 0.$$

This contradicts the hypothesis, so it must be that $a(\overline{x})b(\overline{x}) = 0$, i.e., $x^n - 1$ divides $a(x)b(x)$. $\square$

The following result characterizes the trace dual of an $S|R$ additive cyclic code of length n.

Theorem 4.5. *Let the polynomials $f(x), f'(x), g(x), g'(x) \in R[x]$ be monic divisors of $x^n - 1$. Suppose there exist monic polynomials $f_1(x), g_1(x), \ell(x) \in R[x]$ such that*

$$x^n - 1 = f(x)g_1(x)\ell(x) = f_1(x)g(x)\ell(x),$$

and there are monic polynomials $f_1'(x), g_1'(x), \ell'(x) \in R[x]$ *such that*

$$x^n - 1 = f'(x)g_1'(x)\ell'(x) = f_1'(x)g'(x)\ell'(x).$$

Let $r(x), r'(x) \in R[x]$ *be two polynomials such that* $\deg(f(x)r(x)) < \deg(g(x))$ *and* $\deg(f'(x)r'(x)) < \deg(g'(x))$ *and* $\mathcal{C} = \langle f(\overline{x})(1 + \mu r(\overline{x})), \mu g(\overline{x})\rangle_{\mathcal{R}_n}$. *Then*

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \langle f'(\overline{x})(1 + \mu r'(\overline{x})), \mu g'(\overline{x})\rangle_{\mathcal{R}_n}$$

if and only if in $R[x]$,

$$f_1^*(x)\ell^*(x) \mid f'(x)r'(x) \text{ and } g_1'(x)\ell'(x) \mid g^*(x)r'(x); \tag{R1}$$

$$g_1^*(x)\ell^*(x) \mid g'(x)r^*(x) \text{ and } f_1'(x)\ell'(x) \mid f^*(x)r^*(x); \tag{R2}$$

$$f_1^*(x)\ell^*(x) \mid g'(x) \text{ and } f_1'(x)\ell'(x) \mid g^*(x), \tag{R3}$$

and for all $0 \le i < n$,

$$\overline{x}^i f(\overline{x}) \star f'(\overline{x}) = -\mu^2 \left(\overline{x}^i f(\overline{x})r(\overline{x}) \star f'(\overline{x})r'(\overline{x})\right),$$

in $\mathcal{R}_n$. *Moreover,* $\ell^*(x) \mid f'(x)$.

Proof. Let $\mathcal{C} = \langle f(\overline{x})(1 + \mu r(\overline{x})), \mu g(\overline{x})\rangle_{\mathcal{R}_n}$ and its trace dual $\mathcal{C}^{\perp_{\mathrm{Tr}}} = \langle f'(\overline{x})(1 + \mu r'(\overline{x})), \mu g'(\overline{x})\rangle_{\mathcal{R}_n}$. By Lemma 4.2, this is equivalent to the following conditions holding for all the indexes $0 \le i, j < n$.

(E1) $\overline{x}^i f(\overline{x}) \star \overline{x}^j f'(\overline{x}) = -\mu^2 \left(\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x})\right)$

(E2) $\overline{x}^i g(\overline{x}) \star \overline{x}^j f'(\overline{x})r'(\overline{x}) = 0$

(E3) $\overline{x}^i f(\overline{x})r(\overline{x}) \star \overline{x}^j g'(\overline{x}) = 0$

(E4) $\overline{x}^i g(\overline{x}) \star \overline{x}^j g'(\overline{x}) = 0$

Using Lemma 4.4, conditions (E2)–(E4) can be translated into

- Condition (E2) is equivalent to

  $$x^n - 1 \mid g^*(x)f'(x)r'(x)$$

  Using the given factorizations $x^n - 1 = f(x)g_1(x)\ell(x) = f_1(x)g(x)\ell(x)$ and $x^n - 1 = f'(x)g_1'(x)\ell'(x) = f_1'(x)g'(x)\ell'(x)$, we obtain:

  $$f_1^*(x)\ell^*(x) \mid f'(x)r'(x) \text{ and } g_1'(x)\ell'(x) \mid g^*(x)r'(x)$$

  which is condition (R1).

- Condition (E3) is equivalent to $x^n - 1 \mid g'(x)f^*(x)r^*(x)$, which gives

$$g_1^*(x)\ell^*(x) \mid g'(x)r^*(x) \text{ and } f_1'(x)\ell'(x) \mid f^*(x)r^*(x)$$

  which is condition (R2).
- Condition (E4) is equivalent to $x^n - 1 \mid g^*(x)g'(x)$, which gives

$$f_1^*(x)\ell^*(x) \mid g'(x) \text{ and } f_1'(x)\ell'(x) \mid g^*(x)$$

  which is condition (R3).

Condition (E1) must hold for all $0 \le i < n$, thus

$$\overline{x}^i f(\overline{x}) \star f'(\overline{x}) = -\mu^2 \left(\overline{x}^i f(\overline{x})r(\overline{x}) \star f'(\overline{x})r'(\overline{x})\right)$$

This is a bilinear condition that ensures the consistency of the trace dual's structure and must be verified directly. From condition (E1) and (R1), we deduce that:

$$x^n - 1 \mid f^*(x)g_1^*(x)f'(x) \quad \Rightarrow \quad \ell^*(x) \mid f'(x)$$

This completes the set of necessary and sufficient conditions. Hence, the trace dual has the desired form if and only if conditions (R1)–(R3) hold, condition (E1) holds for all $0 \le i < n$, and $\ell^*(x) \mid f'(x)$. □

Example 4.6. Let $n = 8$, $p = 3$ and $S = \mathbb{Z}_9[\alpha]$ with $\alpha^2 = -1$ and $\mu = \alpha$. The factorization of $x^8 - 1$ into monic irreducible polynomial is given by

$$x^8 - 1 = (x+2)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2) \text{ in } \mathbb{F}_3[x],$$

and the factorization of $x^8 - 1$ into monic basic irreducible polynomial over $\mathbb{Z}_9$ is given by:

$$x^8 - 1 = (x+8)(x+1)(x^2+1)(x^2+4x+8)(x^2+5x+8).$$

Suppose $w(x) = x+8$, $f_1(x) = x+1$, $g_1(x) = (x^2+4x+8)(x^2+1)$, $\ell(x) = (x^2+5x+8)$, and $r(x) = x^2 + x + 3$. Let $\mathcal{C}$ be an $\mathbb{Z}_9[\alpha]|\mathbb{Z}_9$ additive cyclic code of length 8 defined by

$$\begin{aligned}\mathcal{C} &= \left\langle w(\overline{x})f_1(\overline{x})(1+\mu r(\overline{x})),\ \mu w(\overline{x})g_1(\overline{x})\right\rangle \\ &= \left\langle (\overline{x}+8)(\overline{x}+1)(1+2\alpha(\overline{x}^2+\overline{x}+3)),\ 2\alpha(\overline{x}+8)(\overline{x}^2+4\overline{x}+8)(\overline{x}^2+1)\right\rangle \\ &= \left\langle (\overline{x}^2+8)(1+2\alpha(\overline{x}^2+\overline{x}+3)),\ 2\alpha(\overline{x}^5+3\overline{x}^4+5\overline{x}^3+4\overline{x}^2+4\overline{x}+1)\right\rangle.\end{aligned}$$

The trace dual of $\mathcal{C}$ is given by $\mathcal{C}^{\perp_{\mathrm{Tr}}} = \langle f'(\overline{x})(1+\mu r'(\overline{x})), \mu g'(\overline{x})\rangle_{\mathcal{R}_n}$, where $x^8 - 1 = w'(x)f_1'(x)g_1'(x)\ell'(x) = f'(x)g_1'(x)\ell'(x) = f_1'(x)g'(x)\ell'(x)$. In this case, relations (R1), (R2) and (R3) translate into

- $(x+1)(x^2+4x+8) \mid f'(x)r'(x)$ and $g_1'(x)\ell'(x) \mid (x-1)(x^2+5x+8)(x^2+1)r'(x)$;
- $(x^2+5x+8)(x^2+1)(x^2+4x+8) \mid (3x^2+x+1)g'(x)$ *and* $f_1'(x)\ell'(x) \mid (x^2-1)(3x^3+x+1)$;
- $(x+1)(x^2+4x+8) \mid g'(x)$ and $f_1'(x)\ell'(x) \mid (x-1)(x^2+5x+8)(x^2+1)$.

Thus

$$\begin{aligned}(x+1)(x^2+4x+8) \mid f'(x)r'(x);\\ f_1'(x)\ell'(x) \mid (x-1)(x+1);\\ g_1'(x)\ell'(x) \mid (x-1)(x^2+5x+8)(x^2+1)r'(x);\\ \left(\frac{x^8-1}{w(x)}\right) \mid g'(x).\end{aligned}$$

In addition $(x^2+4x+8) \mid f'(x)$. Therefore $\deg(f'(x)) \geq 2$ and $g'(x) = \frac{x^8-1}{w(x)}$. But $\deg(f'(x)g'(x)) = 9$ and $0 \leq \deg(r'(x)) < \deg(g'(x)) - \deg(f'(x))$. Thus $f'(x) = x^2+4x+8$, $\ell'(x) = x-1$ and $0 \leq \deg(r'(x)) \leq 4$. Therefore $r'(x) = (x+1)(a_3x^3+a_2x^2+a_1x+a_0)$, where $(a_0,a_1,a_2,a_3) \in (\mathbb{Z}_9)^4$ and

$$\begin{aligned}\overline{x}^i(\overline{x}^2-1) \star (\overline{x}^2+4\overline{x}+8) =& \overline{x}^i(\overline{x}^4+\overline{x}^3+2\overline{x}^2+8\overline{x}+6)\\ &\star (\overline{x}^3+5\overline{x}^2+3\overline{x}+8)(a_3\overline{x}^3+a_2\overline{x}^2+a_1\overline{x}+a_0),\end{aligned}$$

for all $0 \leq i \leq 7$. Thus, we get $(a_0,a_1,a_2,a_3) = (6,4,3,5)$.

The following result states that for the trace dual code to be stated in terms of the reciprocal polynomials the remainder $r(x)$ should be 0.

Corollary 4.7. *Let $f(x), f'(x), g(x)$ and $g'(x)$ be monic divisors of x^n-1 in $R[x]$ and $(r(x), r'(x)) \in (R[x])^2$ with $\deg(f(x)r(x)) < \deg(g(x))$ and $\deg(f'(x)r'(x)) < \deg(g'(x))$ such that $\mathcal{C} = \langle f(\overline{x})(1+\mu r(\overline{x})), \mu g(\overline{x})\rangle_{\mathcal{R}_n}$ and*

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \langle f'(\overline{x})(1+\mu r'(\overline{x})), \mu g'(\overline{x})\rangle_{\mathcal{R}_n}$$

Then $f'(x) = \left(\frac{x^n-1}{f(x)}\right)^*$ and $g'(x) = \left(\frac{x^n-1}{g(x)}\right)^*$, if and only if $r(x) = r'(x) = 0$.

Proof. Let $f(x) = w(x)f_1(x)$ and $g(x) = w(x)g_1(x)$ where $f_1(x)$ and $g_1(x)$ are coprime with $x^n-1 = f(x)g_1(x)\ell(x) = f_1(x)g(x)\ell(x)$. Assume that $f'(x) = \left(\frac{x^n-1}{f(x)}\right)^* = g_1^*(x)\ell^*(x)$ and $g'(x) = \left(\frac{x^n-1}{g(x)}\right)^* = f_1^*(x)\ell^*(x)$. By Theorem 4.5, we have $f_1^*(x)\ell^*(x) | f^*(x)r^*(x)$ and $w^*(x)g_1^*(x) | g_1^*(x)\ell^*(x)r'(x)$. Thus $f_1^*(x)$ divides $r'(x)$ and $g_1(x)$ divides $r(x)$. Hence $r(x) = r'(x) = 0$, since $\deg(r(x)) < \deg(g_1(x)) - \deg(f_1(x))$ and $\deg(r'(x)) < \deg(g_1'(x)) - \deg(f_1'(x))$. The converse is a direct consequence of Lemma 4.4, and the fact that $\deg(f(x)) + \deg(f'(x)) + \deg(g(x)) + \deg(g'(x)) = 2n$. □

5. Additive complementary pairs of codes

In this section, we study additive complementary pairs of codes (ACPs) over finite commutative chain rings.

Definition 5.1. Let $\mathcal{C}$ and $\mathcal{D}$ be two $S|R$ additive codes. If $\mathcal{C}+_R\mathcal{D}=S^n$ and $\mathcal{C}\cap\mathcal{D}=\{\mathbf{0}\}$, then the pair $\{\mathcal{C},\mathcal{D}\}$ is called an ACP of codes.

Remark 5.1. As usual, we will denote the conditions in Definition 5.1 as $\mathcal{C}\oplus_R\mathcal{D}=S^n$. Note that for cyclic codes, we can use the identification of S^n with $\mathcal{S}_n$ and we can say that (taking into account now that the codes are ideals in $\mathcal{S}_n$) then they are an ACP if $\mathcal{C}\oplus_R\mathcal{D}=\mathcal{S}_n$.

Lemma 5.2. *[14, Theorem 2] Any projective module over a local ring is free module.*

Lemma 5.3. *Let $\mathcal{C}$ and $\mathcal{D}$ be two additive codes over $S|R$. If the pair $\{\mathcal{C},\mathcal{D}\}$ is an ACP of codes, then both $\mathcal{C}$ and $\mathcal{D}$ are free R-modules of S^n.*

Proof. Since the pair $\{\mathcal{C},\mathcal{D}\}$ forms an ACP of codes, then by Remark 5.1, we get $\mathcal{C}\oplus_R\mathcal{D}=S^n$ it follows that $C\oplus D$ is free R-module. This implies that $\mathcal{C}$ and $\mathcal{D}$ both are projective R-submodule of S^n. Since R and S are local rings, then by Lemma 5.2, $\mathcal{C}$ and $\mathcal{D}$ both are free R-submodule of S^n. □

Now, the result [2, Lemma 3.1] easily adapts to the case of additive codes.

Lemma 5.4. *Let $\mathcal{C}$ and $\mathcal{D}$ be two $S|R$ additive codes. Then we have the following theorem.*

1. $(\mathcal{C}+\mathcal{D})^{\perp_{\mathrm{Tr}}}=\mathcal{C}^{\perp_{\mathrm{Tr}}}\cap\mathcal{D}^{\perp_{\mathrm{Tr}}}$;
2. $\mathcal{C}^{\perp_{\mathrm{Tr}}}+\mathcal{D}^{\perp_{\mathrm{Tr}}}=(\mathcal{C}\cap\mathcal{D})^{\perp_{\mathrm{Tr}}}$.

Proof.

1. Let $\mathbf{x}\in(\mathcal{C}+\mathcal{D})^{\perp_{\mathrm{Tr}}}$. Then $\mathrm{Tr}(\mathbf{x},\mathbf{a})=0$ for all $\mathbf{a}\in\mathcal{C}+\mathcal{D}$, that is $\mathrm{Tr}(\mathbf{x},\mathbf{c}+\mathbf{d})=0$ for all $\mathbf{c}\in\mathcal{C},\mathbf{d}\in\mathcal{D}$. If $\mathbf{d}=0$ then $\mathrm{Tr}(\mathbf{x},\mathbf{c})=0$ for all $\mathbf{c}\in\mathcal{C}$, then $\mathbf{x}\in\mathcal{C}^{\perp_{\mathrm{Tr}}}$. Similarly, if $\mathbf{c}=0$ then $\mathrm{Tr}(\mathbf{x},\mathbf{d})=0$ for all $\mathbf{d}\in\mathcal{D}$, which implies $\mathbf{x}\in\mathcal{D}^{\perp_{\mathrm{Tr}}}$. Hence, $\mathbf{x}\in\mathcal{C}^{\perp_{\mathrm{Tr}}}\cap\mathcal{D}^{\perp_{\mathrm{Tr}}}$.
   On the other hand, let $\mathbf{y}\in\mathcal{C}^{\perp_{\mathrm{Tr}}}\cap\mathcal{D}^{\perp_{\mathrm{Tr}}}$. Then $\mathrm{Tr}(\mathbf{y},\mathbf{c})=0$ for all $\mathbf{c}\in\mathcal{C}$ and $\mathrm{Tr}(\mathbf{y},\mathbf{d})=0$ for all $\mathbf{d}\in\mathcal{D}$. That implies $\mathrm{Tr}(\mathbf{y},\mathbf{c}+\mathbf{d})=\mathrm{Tr}(\mathbf{y},\mathbf{c})+\mathrm{Tr}(\mathbf{y},\mathbf{d})=0$ for all $\mathbf{c}\in\mathcal{C},\ \mathbf{d}\in\mathcal{D}$. Hence, $\mathbf{y}\in(\mathcal{C}+\mathcal{D})^{\perp_{\mathrm{Tr}}}$.
2. As $\mathcal{C}^{\perp_{\mathrm{Tr}}}+\mathcal{D}^{\perp_{\mathrm{Tr}}}=\left((\mathcal{C}^{\perp_{\mathrm{Tr}}}+\mathcal{D}^{\perp_{\mathrm{Tr}}})^{\perp_{\mathrm{Tr}}}\right)^{\perp_{\mathrm{Tr}}}$, hence

$$\mathcal{C}^{\perp_{\mathrm{Tr}}}+\mathcal{D}^{\perp_{\mathrm{Tr}}}=(\mathcal{C}\cap\mathcal{D})^{\perp_{\mathrm{Tr}}}.\quad\square$$

Taking into account the previous lemma, we have

Theorem 5.5. *Let $\mathcal{C}$ and $\mathcal{D}$ be two additive codes over $S|R$. Then the following statements are equivalent.*

1. *the pair $(\mathcal{C}, \mathcal{D})$ is an ACP of codes;*
2. *the pair $(\mathcal{C}^{\perp_{\mathrm{Tr}}}, \mathcal{D}^{\perp_{\mathrm{Tr}}})$ is an ACP of codes.*

The following result was shown for the linear codes in [4]. Here, we state it for an additive code and will allow us to characterize the ACP of additive $S|R$-codes in terms of their ranks.

Lemma 5.6. *Let $\mathcal{C}$ and $\mathcal{D}$ be two free $S|R$ additive codes. Denote $\mathcal{C} +_R \mathcal{D} = \langle \mathcal{C} \cup \mathcal{D} \rangle_R$ that is the smallest R-submodule of S^n containing $\mathcal{C} \cup \mathcal{D}$. Then*

$$\mathrm{rank}_R(\mathcal{C} +_R \mathcal{D}) = \mathrm{rank}_R(C) + \mathrm{rank}_R(\mathcal{D}) - \mathrm{rank}_R(\mathcal{C} \cap \mathcal{D}).$$

Proof. To prove the result, consider the map

$$\begin{array}{rccc} \varphi: & \mathcal{C} \times \mathcal{D} & \mapsto & \mathcal{C} +_{\mathcal{R}} \mathcal{D} \\ & (x, y) & \mapsto & x + y. \end{array}$$

Obviously this map φ is an R-module homomorphism. Then by Remark 5.1, $\mathcal{C} +_R \mathcal{D}$ is also R-module. It is clear that the map φ is surjective. Therefore, according to the First Isomorphism Theorem, $\mathcal{C} \times \mathcal{D}/\mathrm{Ker}(\phi) \simeq \mathcal{C} +_R \mathcal{D}$ (as R-modules). Since $\mathcal{C} \cap \mathcal{D} \simeq \mathrm{Ker}(\phi)$ (as R-modules), it follows that $\frac{|\mathcal{C} \times \mathcal{D}|}{|\mathcal{C} \cap \mathcal{D}|} = |\mathcal{C} +_R \mathcal{D}|$. Thus, $\mathrm{rank}_R(\mathcal{C} +_R \mathcal{D}) = \mathrm{rank}_R(C) + \mathrm{rank}_R(\mathcal{D}) - \mathrm{rank}_R(\mathcal{C} \cap \mathcal{D})$. □

Since $\circledast$-inner product is non-degenerate, by Lemma 5.6, we have the following result.

Proposition 5.2. *Let $\mathcal{C}$ be a free $S|R$ additive code of length n. Then $\mathcal{C}^{\perp_{\mathrm{Tr}}}$ is free (as R-module),*

$$\left(\mathcal{C}^{\perp_{\mathrm{Tr}}}\right)^{\perp_{\mathrm{Tr}}} = \mathcal{C},$$

and $\mathrm{rank}_R(\mathcal{C}) + \mathrm{rank}_R(\mathcal{C}^{\perp_{\mathrm{Tr}}}) = 2n$.

Corollary 5.7. *Let $\mathcal{C}$ and $\mathcal{D}$ be two $S|R$ additive codes of length n. Then $\{\mathcal{C}, \mathcal{D}\}$ is an ACP of codes if and only if* $\mathrm{rank}_R(\mathcal{C} +_R \mathcal{D}) = \mathrm{rank}_R(\mathcal{C}) + \mathrm{rank}_R(\mathcal{D}) = 2n$.

Proof. By Lemma 5.3 $\mathcal{C}, \mathcal{D}$ are free R-modules since they form an ACP of codes. Thus, applying the Lemma 5.6, we easily deduce that $\{\mathcal{C}, \mathcal{D}\}$ is an ACP of codes if and only if $\mathrm{rank}_R(\mathcal{C} +_R \mathcal{D}) = \mathrm{rank}_R(\mathcal{C}) + \mathrm{rank}_R(\mathcal{D}) = 2n$. □

Let π the natural surjective ring homomorphism $\pi : S \to S/\mathfrak{m}_S = \mathbb{F}_{q^2}$ which naturally extends to a homomorphism from S^n to $\mathbb{F}_{q^2}^n$.

Lemma 5.8. *Let $\mathcal{C}$ and $\mathcal{D}$ be two $S|R$ additive codes. Then $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$ if and only if $\pi(C) \cap \pi(D) = \{\mathbf{0}\}$.*

Proof. Assume that $\pi(\mathcal{C}) \cap \pi(\mathcal{D}) = \{\mathbf{0}\}$. Let $\mathbf{v} \in \mathcal{C} \cap \mathcal{D}$. Then $\pi(\mathbf{v}) \in \pi(\mathcal{C}) \cap \pi(\mathcal{D})$ and, by hypothesis, $\pi(\mathbf{v}) = 0$. Therefore, $\mathbf{v} \in \mathfrak{m}_R(\mathcal{C} \cap \mathcal{D})$, which implies $\mathcal{C} \cap \mathcal{D} = \mathfrak{m}_R(\mathcal{C} \cap \mathcal{D})$. Since $\mathcal{C} \cap \mathcal{D}$ is a finitely generated right R-module, Nakayama's Lemma [18] implies that $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$.

Conversely, assume that $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$ and let $\mathbf{v} \in \pi(\mathcal{C}) \cap \pi(\mathcal{D})$. Then there exist $\mathbf{c} \in \mathcal{C}$ and $\mathbf{d} \in \mathcal{D}$ such that $\pi(\mathbf{c}) = \pi(\mathbf{d}) = \mathbf{v}$. Hence, $\pi(\mathbf{c} - \mathbf{d}) = 0$, which implies that $\mathbf{c} - \mathbf{d} \in \mathfrak{m}_R S^n$. Hence, there is a power γ^i of γ (the generator of $\mathfrak{m}_R$) with $1 \leq i < e$ such that $\gamma^i(\mathbf{c} - \mathbf{d}) = \mathbf{0}$, then $\gamma^i\mathbf{c} = \gamma^i\mathbf{d} \in C \cap D$. By assumption, $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$, so $\gamma^i\mathbf{c} = \gamma^i\mathbf{d} = \mathbf{0}$. Suppose $\mathbf{c} \notin \mathfrak{m}_R S^n$. Then $\gamma^i\mathbf{c} \neq \mathbf{0}$ which contradicts the previous statement. Thus, $\mathbf{c} \in \mathfrak{m}_R S^n$, implying $\pi(\mathbf{c}) = \mathbf{0}$, and hence $\mathbf{v} = \pi(\mathbf{c}) = \mathbf{0}$. This shows that $\pi(\mathcal{C}) \cap \pi(\mathcal{D}) = \{\mathbf{0}\}$. □

Theorem 5.9. *Let $\mathcal{C}$ and $\mathcal{D}$ be two $S|R$ additive codes of length n. The pair $\{\mathcal{C}, \mathcal{D}\}$ forms an ACP of codes if and only if the pair $\{\pi(\mathcal{C}), \pi(\mathcal{D})\}$ also forms an ACP of $\mathbb{F}_{q^2}|\mathbb{F}_q$-linear codes.*

Proof.

⇒) Since $\{\mathcal{C}, \mathcal{D}\}$ is an ACP, we have $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$, thus by Lemma 5.8, it follows that $\pi(C) \cap \pi(D) = \{\mathbf{0}\}$. Let $\mathbf{v} \in \mathbb{F}_{q^2}^n$. Since π is a subjective map, there exists $\mathbf{a} \in S^n$ such that $\pi(\mathbf{a}) = \mathbf{v}$. Since $\mathcal{C} +_R \mathcal{D} = S^n$, there are $\mathbf{c} \in \mathcal{C}$, $\mathbf{d} \in \mathcal{D}$ such that $\mathbf{a} = \mathbf{c} + \mathbf{d}$. Henceforth, $\mathbf{v} = \pi(\mathbf{a}) = \pi(\mathbf{c}) + \pi(\mathbf{d}) \in \pi(\mathcal{C}) + \pi(\mathcal{D})$. Therefore, $\pi(\mathcal{C}) +_{\mathbb{F}_q} \pi(\mathcal{D}) = \mathbb{F}_{q^2}^n$, and we conclude that $(\pi(C), \pi(D))$ is ACP.

⇐) Suppose now that $(\pi(C), \pi(D))$ is ACP of $\mathbb{F}_{q^2}|\mathbb{F}_q$-linear codes. Then $\pi(\mathcal{C}) \oplus_{\mathbb{F}_q} \pi(\mathcal{D}) = \mathbb{F}_q^n$, which implies $\pi(\mathcal{C}) \cap \pi(\mathcal{D}) = \{\mathbf{0}\}$. Thus, by Lemma 5.8, it follows that $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$.

Let $\{\pi(\mathbf{x}_1), \ldots, \pi(\mathbf{x}_k)\}$ be a basis of $\pi(\mathcal{C})$, and $\{\pi(\mathbf{x}_{k+1}), \ldots, \pi(\mathbf{x}_n)\}$ a basis of $\pi(\mathcal{D})$. Then, it is straightforward that $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ and $\{\mathbf{x}_{k+1}, \ldots, \mathbf{x}_n\}$ are minimal generating sets for $\mathcal{C}$ and $\mathcal{D}$, respectively. Since $\mathcal{C}$ and $\mathcal{D}$ are both free, we have $|\mathcal{C}||\mathcal{D}| = |S^n|$. Therefore, $\mathcal{C} +_R \mathcal{D} = S^n$, and the pair $\{\mathcal{C}, \mathcal{D}\}$ is an ACP of additive codes of length n. □

Let n be a positive integer. An $n \times n$ matrix A over $\mathcal{S}$ is said to be invertible over $\mathcal{S}$ if the matrix $\pi(\mathrm{A}) = (\pi(a_{ij}))$ is invertible over $\mathbb{F}_{q^2}$. For a free code C, consider a generator matrix G and parity-check matrix H of $\mathcal{C}$. Then, under the projection π, the matrices $\pi(\mathrm{G})$ and $\pi(\mathrm{H})$ serve as a generator matrix and a parity-check matrix of the projected code $\pi(\mathcal{C})$, respectively.

Proposition 5.3. *[2, Theorem 3.7] Let $\mathcal{C}$ and $\mathcal{D}$ be two free $S|R$ additive codes of length n with generator matrices G_1, G_2 and parity-check matrices H_1, H_2, respectively. Suppose that $|\mathcal{C}||\mathcal{D}| = |S^n|$. Then, the following statements are equivalent:*

a) *The pair $\{\pi(\mathcal{C}), \pi(\mathcal{D})\}$ forms ACP,*
b) *The matrix $\mathrm{Tr}\left(\pi(\mathrm{H}_2)\pi(\mathrm{G}_1)^\top\right)$ or $\mathrm{Tr}\left(\pi(\mathrm{H}_1)\pi(\mathrm{G}_2)^\top\right)$ is invertible over $\mathbb{F}_{q^2}$.*

Theorem 5.10. *Let $\mathcal{C}$ and $\mathcal{D}$ be two free additive codes of length n over $S|R$ with generator matrices G_1, G_2 and parity-check matrices H_1, H_2, respectively. Then the pair $\{\mathcal{C}, \mathcal{D}\}$ is ACP if and only if $\mathrm{Tr}\left(\mathrm{H}_2\mathrm{G}_1^\top\right)$ or $\mathrm{Tr}\left(\mathrm{H}_1\mathrm{G}_2^\top\right)$ is invertible.*

Proof. Suppose $\{\mathcal{C}, \mathcal{D}\}$ is ACP of free additive codes over $S|R$. Assume, for contradiction, that $\mathrm{Tr}\left(\mathrm{H}_2\mathrm{G}_1^\top\right)$ is not invertible. Then its image under the ring homomorphism π

$$\pi(\mathrm{Tr}\left(\mathrm{H}_2\mathrm{G}_1^\top\right)) = \mathrm{Tr}\left(\pi(\mathrm{H}_2)\pi(\mathrm{G}_1)^\top\right),$$

is also not invertible over $\mathbb{F}_{q^2}$.

By Proposition 5.3, this implies $\{\pi(\mathcal{C}), \pi(\mathcal{D})\}$ is not ACP. Then, by applying Theorem 5.9, (C, D) cannot be an ACP, contradicting our assumption. Hence, $\mathrm{Tr}\left(\mathrm{H}_2\mathrm{G}_1^\top\right)$ or $\mathrm{Tr}\left(\mathrm{H}_1\mathrm{G}_2^\top\right)$ must be invertible.

Conversely, assume $\mathrm{Tr}\left(\mathrm{H}_2\mathrm{G}_1^\top\right)$ or $\mathrm{Tr}\left(\mathrm{H}_1\mathrm{G}_2^\top\right)$ is invertible. Then the matrix $\mathrm{Tr}\big(\pi(\mathrm{H}_2)$ $\pi(\mathrm{G}_1)^\top\big)$ is invertible, implying $\{\pi(\mathcal{C}), \pi(\mathcal{D})\}$ is an ACP by Proposition 5.3. Therefore, by Theorem 5.9, $\{\mathcal{C}, \mathcal{D}\}$ is ACP. □

6. Additive complementary pairs of cyclic codes

In this Section, we study pairs $\{\mathcal{C}, \mathcal{D}\}$ that are ACP of additive $S|R$ cyclic codes. Note that by Lemma 5.3, both codes $\mathcal{C}$ and $\mathcal{D}$ are free $S|R$ additive codes with a representation as in Theorem 3.3.

Theorem 6.1. *Let $f_1(x), f_2(x), g_1(x)$ and $g_2(x)$ be monic divisors of $x^n - 1$ over R and $(r_1(x), r_2(x)) \in (R[x])^2$ with $\deg(f_1(x)r_1(x)) < \deg(g_1(x))$ and $\deg(f_2(x)r_2(x)) < \deg(g_2(x))$ such that*

$$\mathcal{C} = \langle f_1(\overline{x})(1 + \mu r_1(\overline{x})), \mu g_1(\overline{x})\rangle_{\mathcal{R}_n} \text{ and } \mathcal{D} = \langle f_2(\overline{x})(1 + \mu r_2(\overline{x})), \mu g_2(\overline{x})\rangle_{\mathcal{R}_n}$$

are two $S|R$ additive cyclic codes of length n. Then, the pair $(\mathcal{C}, \mathcal{D})$ is ACP if and only if $f_1(x)f_2(x) = g_1(x)g_2(x) = x^n - 1$.

Proof. Assume that $\{\mathcal{C}, \mathcal{D}\}$ is ACP. By Theorem 5.9 we know that $\{\pi(\mathcal{C}), \pi(\mathcal{D})\}$ is an ACP of $\mathbb{F}_q$-linear $\mathbb{F}_{q^2}$-codes. Then $\langle \pi(f_1(x))\rangle_{\mathbb{F}_q} + \langle \pi(f_2(x))\rangle_{\mathbb{F}_q} = \mathbb{F}_{q^2}^n$ and

$$\langle \mu\pi(g_1)(\overline{x})\rangle_{\mathbb{F}_q} \cap \langle \mu\pi(g_2)(\overline{x})\rangle_{\mathbb{F}_q} \subseteq \pi(\mathcal{C}) \cap \pi(\mathcal{D}) = \{0\}.$$

Thus $\gcd(\pi(f_1(x)), \pi(f_2(x))) = 1$, and $\operatorname{lcm}(\pi(g_1(x)), \pi(g_2(x))) = x^n - 1$. It follows that $\pi(f_1(x))\pi(f_2(x)) = \pi(g_1(x))\pi(g_2(x)) = x^n - 1$, since $f_1(x), f_2(x), g_1(x)$ and $g_2(x)$ are monic divisors of $x^n - 1$ and $\deg(f_1(x)f_2(x)) + \deg(g_1(x)g_2(x)) = 2n$. Hence, by Hensel lift, we have $f_1(x)f_2(x) = g_1(x)g_2(x) = x^n - 1$.

Conversely, suppose that $f_1(x)f_2(x) = g_1(x)g_2(x) = x^n - 1$. To prove the result, let us define a map

$$\begin{array}{rccc} \psi: & \mathcal{C} \cap \mathcal{D} & \to & \mathcal{R}_n \\ & a(\overline{x}) + \mu b(\overline{x}) & \mapsto & a(\overline{x}). \end{array}$$

Clearly, $\mathcal{C} \cap \mathcal{D}$ is $R|S$ additive cyclic code of length n. Obviously, $\mathtt{Im}(\psi) = \langle f_1(x)f_2(x)\rangle$ and $\mathrm{Ker}(\psi) = \langle g_1(x)g_2(x)\rangle$. By Theorem 3.3, we have

$$\mathcal{C} \cap \mathcal{D} = \langle f_1(\overline{x})f_2(\overline{x})(1 + \mu r(\overline{x})), \mu g_1(\overline{x})g_2(\overline{x})\rangle_{\mathcal{R}_n},$$

where $r(x) \in R[x]$. By hypothesis $f_1(\overline{x})f_2(\overline{x}) = g_1(\overline{x})g_2(\overline{x}) = \overline{x}^n - 1 = 0$. Thus, we obtain $\mathcal{C} \cap \mathcal{D} = \{\mathbf{0}\}$. Since $x^n - 1$ is square-free, we get $\langle f_1(\overline{x})\rangle + \langle f_2(\overline{x})\rangle = \mathcal{R}_n$ (f_1 and f_2 are coprime) and $\langle g_1(\overline{x})\rangle + \langle g_2(\overline{x})\rangle = \mathcal{R}_n$ ($g_1(x)$ and $g_2(x)$ are coprime polynomials) which results $\mathrm{rank}_R(\mathcal{C}) + \mathrm{rank}_R(\mathcal{D}) = 2n$. Therefore, applying Theorem 5.7, the result follows. □

Corollary 6.2. *Let $f_1(x), f_2(x), g_1(x)$ and $g_2(x)$ be monic divisors of $x^n - 1$ over R and $(r_1(x), r_2(x)) \in (R[x])^2$ with $\deg(f_1(x)r_1(x)) < \deg(g_1(x))$ and $\deg(f_2(x)r_2(x)) < \deg(g_2(x))$ such that*

$$\mathcal{C} = \langle f_1(\overline{x})(1 + \mu r_1(\overline{x})), \mu g_1(\overline{x})\rangle_{\mathcal{R}_n} \text{ and } \mathcal{D} = \langle f_2(\overline{x})(1 + \mu r_2(\overline{x})), \mu g_2(\overline{x})\rangle_{\mathcal{R}_n}.$$

If $\{\mathcal{C}, \mathcal{D}\}$ is ACP, then $r_1(x) = r_2(x) = 0$.

Proof. According to Theorem 6.1, it follows that $f_1f_2 = g_1g_2 = x^n - 1$. Consider this map

$$\begin{array}{rccc} \varphi: & \mathcal{S}_n & \to & \mathcal{R}_n \\ & a(\overline{x}) + \mu b(\overline{x}) & \mapsto & b(\overline{x}) \end{array}$$

that is an epimorphism of $\mathcal{R}_n$-modules. We have

$$\varphi(\mathcal{C}) = \langle f_1(\overline{x})r_1(\overline{x})), g_1(\overline{x})\rangle_{\mathcal{R}_n} \text{ and } \varphi(\mathcal{D}) = \langle f_2(\overline{x})r_2(\overline{x})), g_2(\overline{x})\rangle_{\mathcal{R}_n}.$$

Note that $\mathcal{R}_n$ is a principal ideal ring, thus there exist polynomials $d_1(x)$ and $d_2(x)$ monic divisors of $x^n - 1$ such that $\varphi(\mathcal{C}) = \langle d_1(\overline{x})\rangle_{\mathcal{R}_n}$ and $\varphi(\mathcal{D}) = \langle d_2(\overline{x})\rangle_{\mathcal{R}_n}$. Since $\mathcal{C} + \mathcal{D} = \mathcal{S}_n$ and φ is an epimorphism of $\mathcal{R}_n$-modules, it follows that $\varphi(\mathcal{C}) + \varphi(\mathcal{D}) = \mathcal{R}_n$. Thus $d_1(x)$ and $d_2(x)$ are coprime polynomials and $d_1(x)d_2(x)$ divides $x^n - 1$. According to Lemma 5.6, we have

$$\mathrm{rank}_R(\mathcal{R}_n) = \mathrm{rank}_R(\varphi(\mathcal{C})) + \mathrm{rank}_R(\varphi(\mathcal{D})) - \mathrm{rank}_R(\varphi(\mathcal{C}) \cap \varphi(\mathcal{D})).$$

Thus $\deg(d_1(x)) + \deg(d_2(x)) = n$. Hence $d_1(x)d_2(x) = x^n - 1$ and $d_1(x) = g_1(x)$ and $d_2(x) = g_2(x)$. Since $\deg(f_1(x)r_1(x)) < \deg(g_1(x))$ and $\deg(f_2(x)r_2(x)) < \deg(g_2(x))$, we have $f_1(x)r_2(x) = f_2(x)r_2(x) = 0$. It follows that $r_1(x) = r_2(x) = 0$, since $f_1(x)$ and $f_2(x)$. □

Corollary 6.3. *Let $f_1(x), f_2(x), g_1(x)$ and $g_2(x)$ be monic divisors of $x^n - 1$ over R such that $\mathcal{C} = \mathcal{C}_1 \oplus \mu\mathcal{C}_2$ and $\mathcal{D} = \mathcal{D}_1 \oplus \mu\mathcal{D}_2$, where $\mathcal{C}_1 = \langle f_1(\overline{x})\rangle, \mathcal{C}_2 = \langle g_1(\overline{x})\rangle, \mathcal{D}_1 = \langle f_2(\overline{x})\rangle$, and $\mathcal{D}_2 = \langle g_2(\overline{x})\rangle$. Let σ be the permutation of $\{0, 1, \cdots, n-1\}$ defined by $\sigma(i) = n-i-1$. Then the following assertions are equivalent.*

1. *The pair $\{\mathcal{C}, \mathcal{D}\}$ is ACP.*
2. *The pairs $\{\mathcal{C}_1, \mathcal{D}_1\}$ and $\{\mathcal{C}_2, \mathcal{D}_2\}$ are LCP of codes.*
3. *$\mathcal{C}_1^{\perp} = \sigma(\mathcal{D}_1)$ and $\mathcal{C}_2^{\perp} = \sigma(\mathcal{D}_2)$.*
4. *$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \sigma(\mathcal{D})$.*

Proof.

1) ⇒ 2): Assume $\{\mathcal{C}, \mathcal{D}\}$ is an ACP. By Theorem 6.1, we have $f_1(x)f_2(x) = g_1(x)g_2(x) = x^n - 1$. Since $\gcd(f_1(x), f_2(x)) = 1$ (and respectively $\gcd(g_1(x), g_2(x)) = 1$), the cyclic codes $\mathcal{C}_1 = \langle f_1(\bar{x})\rangle$, and $\mathcal{D}_1 = \langle f_2(\bar{x})\rangle$ satisfy

$$\mathcal{C}_1 \cap \mathcal{D}_1 = \langle \mathrm{lcm}(f_1, f_2)\rangle = \{0\}, \quad \mathcal{C}_1 + \mathcal{D}_1 = \langle \gcd(f_1, f_2)\rangle = R^n.$$

Thus $\{\mathcal{C}_1, \mathcal{D}_1\}$ is an LCP. Similarly $\{\mathcal{C}_2, \mathcal{D}_2\}$ is an LCP.

2) ⇒ 3): If $\{\mathcal{C}_i, \mathcal{D}_i\}$ is LCP, then $\mathcal{C}_i + \mathcal{D}_i = R^n$, and $\mathcal{C}_i \cap \mathcal{D}_i = \{\mathbf{0}\}$, and for cyclic codes this is equivalent to $f_i(x)\, g_i(x) = x^n - 1$. But by standard duality for cyclic codes, the Euclidean dual of $\langle f_i(\bar{x})\rangle$ is

$$\langle f_i(\bar{x})\rangle^{\perp} = \big\langle (x^n - 1)/f_i^*(\bar{x})\big\rangle,$$

and coefficient-reversal via $\sigma(i) = n-1-i$ satisfies $\langle f_i(\bar{x})\rangle^{\perp} = \sigma\big(\langle g_i(\bar{x})\rangle\big)$. Hence $\mathcal{C}_i^{\perp} = \sigma(\mathcal{D}_i)$, for $i = 1, 2$.

3) ⇒ 4): Assuming $\mathcal{C}_i^{\perp} = \sigma(\mathcal{D}_i)$ for $i = 1, 2$. Then

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \mathcal{C}_1^{\perp} \oplus \mu\, \mathcal{C}_2^{\perp} = \sigma(\mathcal{D}_1) \oplus \mu\, \sigma(\mathcal{D}_2) = \sigma(\mathcal{D}_1 \oplus \mu\, \mathcal{D}_2) = \sigma(\mathcal{D}).$$

4) ⇒ 1): According to Corollary 4.7, we have

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \left\langle \left(\frac{x^n - 1}{f_1(x)}\right)^*, \mu \left(\frac{x^n - 1}{g_1(x)}\right)^* \right\rangle_{\mathcal{R}_n}.$$

On the other hand, $\sigma(\mathcal{D}) = \langle f_2^*(x), \mu g_2^*(x)\rangle_{\mathcal{R}_n}$. Since $\mathcal{C}^{\perp_{\mathrm{Tr}}} = \sigma(\mathcal{D})$, by identification, it follows that $f_1(x)f_2(x) = g_1(x)g_2(x) = x^n - 1$. Hence, by Theorem 6.1, the pair $\{\mathcal{C}, \mathcal{D}\}$ is ACP. □

Finally, from the discussion above, we get a similar result to [8, Theorem 2.4] in the setting of additive $S|R$ cyclic codes.

Theorem 6.4. *Let the pair $\{\mathcal{C}, \mathcal{D}\}$ be an ACP of $S|R$ additive cyclic codes of length n and σ be the permutation of $\{0, 1, \ldots, n-1\}$ defined by $\sigma(i) = n - i - 1$. Then*

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \sigma(\mathcal{D}).$$

Proof. Let $\{\mathcal{C}, \mathcal{D}\}$ be an ACP of $S|R$ additive cyclic codes of length n. By Corollary 6.2, we have $r_1(x) = r_2(x) = 0$. Therefore, the codes can be written as:

$$\mathcal{C} = \langle f_1(\overline{x})\rangle \oplus \langle \mu g_1(\overline{x})\rangle = \mathcal{C}_1 \oplus \mu\mathcal{C}_2,$$
$$\mathcal{D} = \langle f_2(\overline{x})\rangle \oplus \langle \mu g_2(\overline{x})\rangle = \mathcal{D}_1 \oplus \mu\mathcal{D}_2,$$

where $\mathcal{C}_1 = \langle f_1(\overline{x})\rangle$, $\mathcal{C}_2 = \langle g_1(\overline{x})\rangle$, $\mathcal{D}_1 = \langle f_2(\overline{x})\rangle$, and $\mathcal{D}_2 = \langle g_2(\overline{x})\rangle$. Since $\{\mathcal{C}, \mathcal{D}\}$ is an ACP, then by Corollary 6.3. Thus, from the equivalence (1) ⇔ (4) we have

$$\mathcal{C}^{\perp_{\mathrm{Tr}}} = \sigma(\mathcal{D}). \quad \square$$

Data availability

No data was used for the research described in the article.

References

[1] Alexei Ashikhmin, Emanuel Knill, Nonbinary quantum stabilizer codes, IEEE Trans. Inf. Theory 47 (7) (2001) 3065–3072.
[2] Sanjit Bhowmick, Deepak K. Dalai, Additive complementary pairs of codes, Adv. Math. Commun. (2025).
[3] Sanjit Bhowmick, Deepak K. Dalai, Sihem Mesnager, On linear complementary pairs of algebraic geometry codes over finite fields, Discrete Math. 347 (12) (2024) 114193.
[4] Sanjit Bhowmick, Alexandre Fotue Tabue, Joydeb Pal, On the ℓ-DLIPs of codes over finite commutative rings, Discrete Math. 347 (4) (2024) 113853.
[5] Martino Borello, Javier de la Cruz, Wolfgang Willems, A note on linear complementary pairs of group codes, Discrete Math. 343 (8) (2020) 111905.
[6] Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, Houssem Maghrebi, Orthogonal direct sum masking, in: David Naccache, Damien Sauveron (Eds.), Information Security Theory and Practice. Securing the Internet of Things, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 40–56.
[7] Claude Carlet, Sylvain Guilley, Complementary dual codes for counter-measures to side-channel attacks, Adv. Math. Commun. 10 (1) (2016) 131–150.
[8] Claude Carlet, Cem Güneri, Ferruh Özbudak, Buket Özkaya, Patrick Solé, On linear complementary pairs of codes, IEEE Trans. Inf. Theory 64 (10) (2018) 6583–6589.

[9] Whan-Hyuk Choi, Cem Güneri, Jon-Lark Kim, Ferruh Özbudak, Theory of additive complementary dual codes, constructions and computations, Finite Fields Appl. 92 (2023) 102303.
[10] Philippe Delsarte, Majority logic decodable codes derived from finite inversive planes, Inf. Control 18 (1971) 319–325.
[11] Cem Güneri, Edgar Martínez-Moro, Selcen Sayıcı, Linear complementary pair of group codes over finite chain rings, Des. Codes Cryptogr. 88 (11) (2020) 2397–2405.
[12] Cem Güneri, Buket Özkaya, Selcen Sayıcı, On linear complementary pair of nD cyclic codes, IEEE Commun. Lett. 22 (12) (2018) 2404–2406.
[13] W. Cary Huffman, On the theory of $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes, Adv. Math. Commun. 7 (3) (2013) 349–378.
[14] Irving Kaplansky, Projective modules, Ann. Math. (2) 68 (1958) 372–377.
[15] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, Pradeep Kiran Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inf. Theory 52 (11) (2006) 4892–4914.
[16] Edgar Martinez-Moro, Kamil Otal, Ferruh Özbudak, Additive cyclic codes over finite commutative chain rings, Discrete Math. 341 (7) (2018) 1873–1884.
[17] James L. Massey, Linear codes with complementary duals 106/107 (1992) 337–342. A collection of contributions in honour of Jack van Lint.
[18] Bernard R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, vol. 28, Marcel Dekker, Inc., New York, 1974.
[19] Graham H. Norton, Ana Sălăgean, On the structure of linear and cyclic codes over finite chain rings, Appl. Algebra Eng. Commun. Comput. 10 (6) (2000) 489–506.
[20] Minjia Shi, Na Liu, Ferruh Özbudak, Patrick Solé, Additive cyclic complementary dual codes over $\mathbb{F}_4$, Finite Fields Appl. 83 (2022) 102087.
[21] Gyanendra K. Verma, Rajendra K. Sharma, Trace dual of additive cyclic codes over finite fields, Cryptogr. Commun. 16 (6) (2024) 1593–1608.
[22] Zhe-Xian Wan, Finite Fields and Galois Rings, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.
[23] Jay A. Wood, Duality for modules over finite rings and applications to coding theory, Am. J. Math. 121 (3) (1999) 555–575.