FACTA UNIVERSITATIS (NIŠ)
Ser. Math. Inform. Vol. 37, No 1 (2022), 1–16
https://doi.org/10.22190/FUMI200819002A
Original Scientific Paper

λ-CONSTACYCLIC CODES OVER FINITE KRASNER HYPERFIELDS

Madeleine Al-Tahan[1] and Bijan Davvaz[2]

[1] **Madeleine Al-Tahan, Faculty of Science, Department of Mathematics and Physics**
Lebanese International University, Bekaa, Lebanon
[2] **Department of Mathematics**
Yazd Yniversity, Yazd, Iran

Abstract. The class of constacyclic codes plays an important role in the theory or error-correcting codes. They are considered as a remarkable generalization of cyclic codes. In this paper, we study constacyclic codes over finite Krasner hyperfields in which we characterize them by their generating polynomial. Moreover, we study the dual of these codes by finding their parity check polynomial.
Key words: Krasner hyperring, hyperfield, hyperring of polynomials, linear code, λ-constacyclic code.

1. Introduction

Coding theory was first established on a firm basis in 1948 in Claude Shannon's publication [23]. Since then, many researchers have worked on this topic from both theoretical and application perspectives. The study of linear codes has been of great importance and different classes of them were introduced such as cyclic codes, negacyclic codes and constacyclic codes. However, the latter constitutes a remarkable generalization of cyclic and negacyclic codes. Constacyclic codes form an important class of linear codes. They have practical applications and preferred roles in engineering as they can encode with shift registers. For more details about coding theory, the reader may refer to [14, 16]. Algebraic hyperstructures represent a natural

Received August 19, 2020, accepted: November 21, 2021
Communicated by Bojan Bašić
Corresponding Author: Bijan Davvaz, Department of Mathematics, Yazd Yniversity, Yazd, Iran | E-mail: davvaz@yazd.ac.ir
2010 *Mathematics Subject Classification.* Primary 20N20; Secondary 16Y99, 94B05

generalization of classical algebraic structures and they were introduced by Marty [17] in 1934 at the eighth Congress of Scandinavian Mathematicians. Where he generalized the notion of a group to that of a hypergroup. A hypergroup is a non-empty set equipped with an associative hyperoperation and reproductive hyperoperation. In a group, the composition of two elements is an element whereas in a hypergroup, the composition of two elements is a non-empty set. Since then, many different kinds of hyperstructures (hyperring, hypermodule, hypervector space, ...) were widely studied from the theoretical point of view and for their applications to many subjects of pure and applied mathematics (see [1, 2, 3, 4, 6, 7, 8, 10, 12, 20, 26, 27]). There exists different kinds of hyperrings. A special case of this type is the hyperring introduced by Krasner [15]. Also, Krasner introduced a new class of hyperrings and hyperfields: the quotient hyperrings and hyperfields. For more details about Krasner hyperrings we refer to [10, 15, 18, 21, 22]. Linear codes were assigned a certain algebraic structure where different researchers studied them over finite fields (see [13, 14]). Later, a connection between code theory and hyperstructure theory was established by Tallini in [24]. Davvaz et al. in [11] used the latter connection to study a certain classes of linear codes (cyclic and quasicyclic) over finite hyperrings.

Our paper is concerned about a special class of linear codes over finite hyperfields and it is organized as follows: after an Introduction, in Section 2, present some basic definitions about hyperstructures. In Section 3, we use the definition of the hyperring of polynomials from [11] to introduce some new definitions such as divisors of a polynomial in a hyperring and investigate their properties. In Section 4, we define contacyclic codes over finite hyperfields and we characterize them by their generating polynomial and parity check polynomial. Moreover, we present a construction technique of constacyclic codes over finite hyperfields.

2. Basic definitions

In this section, we present some definitions related to hyperstructures that are used throughout the paper (see [5, 8, 10, 11]).

Let H be a non-empty set. Then, a mapping $\circ : H \times H \to \mathcal{P}^*(H)$ is called a *binary hyperoperation* on H, where $\mathcal{P}^*(H)$ is the family of all non-empty subsets of H. The couple $(H, \circ)$ is called a *hypergroupoid*. In this definition, if A and B are two non-empty subsets of H and $x \in H$, then we define $A \circ B = \bigcup_{a \in A, b \in B} a \circ b$, $x \circ A = \{x\} \circ A$ and $A \circ x = A \circ \{x\}$. A hypergroupoid $(H, \circ)$ is called: a *semihypergroup* if for every $x, y, z \in H$, we have $x \circ (y \circ z) = (x \circ y) \circ z$; a *quasihypergroup* if for every $x \in H$, $x \circ H = H = H \circ x$ (this condition is called the reproduction axiom); a *hypergroup* if it is a semihypergroup and a quasihypergroup. A *Krasner hyperring* is an algebraic structure $(R, +, \cdot)$ which satisfies the following axiom: (1) $(R, +)$ is a commutative hypergroup; (2) there exists $0 \in R$ such that $0 + x = \{x\}$ for all $x \in R$; (3) for every $x \in R$ there exists unique $x' \in R$ such that $0 \in x + x'$; (x' is denoted by $-x$); (4) $z \in x + y$ implies that $y \in -x + z$ and $x \in z - y$; (5) $(R, \cdot)$ is a semigroup having zero as a bilaterally absorbing element, i.e., $x \cdot 0 = 0 \cdot x = 0$; (6) the multiplication "$\cdot$" is distributive with respect to the hyperoperation "$+$". Note that every ring is a Krasner hyperring. Different examples of Krasner hyperrings

were constructed. We refer to [8]. Let $(R, +, \cdot)$ be a Krasner hyperring and A be a non-empty subset of R. Then A is said to be a *subhyperring* of R if $(A, +, \cdot)$ is itself a hyperring. A subhyperring A of a Krasner hyperring $(R, +, \cdot)$ is a *hyperideal* of R if $r \cdot a \in A$ $(a \cdot r \in A)$ for all $a \in A, r \in R$. A commutative Krasner hyperring $(R, +, \cdot)$ with identity element "1" is a *Krasner hyperfield* if $(R \setminus \{0\}, \cdot)$ is a group. An *additive-multiplicative hyperring* is an algebraic structure $(R, +, \cdot)$ which satisfies the following axiom: (1) $(R, +)$ is a commutative hypergroup; (2) exists $0 \in R$ such that $0 + x = \{x\}$ for all $x \in R$; (3) for every $x \in R$ there exists unique $x' \in R$ such that $0 \in x + x'$, (x' is denoted by $-x$); (4) $z \in x + y$ implies that $y \in -x + z$ and $x \in z - y$; (5) $(R, \cdot)$ is a semihypergroup having zero as a bilaterally absorbing element, i.e., $x \cdot 0 = 0 \cdot x = 0$; (6) the multiplication "$\cdot$" is distributive with respect to the hyperoperation "+"; (7) for all $x, y \in R$, we have $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$. An additive-multiplicative hyperring $(R, +, \cdot)$ is called commutative if $(R, \cdot)$ is a commutative semihypergroup. Tallini in [25] introduced the notion of hypervector spaces and studied basic properties of them. Later R. Ameri et al. in [5] studied the properties of dimension of hypervector spaces and introduced the notions of linearly independent (respectively linearly dependent), generator and basis of a hypervector space. Let F be a Krasner hyperfield. A commutative hypergroup $(V, +)$ together with a map $\cdot : F \times V \to V$, is called a *hypervector space* over F if for all $a, b \in F$ and $x, y \in V$, the following conditions holds: (1) $a \cdot (x + y) = a \cdot x + a \cdot y$; (2) $(a + b) \cdot x = a \cdot x + b \cdot x$; (3) $a \cdot (b \cdot x) = (ab) \cdot x$; (4) $a \cdot (-x) = (-a) \cdot x = -(a \cdot x)$; (5) $x = 1 \cdot x$. For example, if F is a Krasner hyperfield and n is any positive integer, then F^n is a hypervector space over F. Let F be a Krasner hyperfield and $(V, +)$ be a hypervector space over F. A non-empty subset $A \subseteq V$ is called *subhypervector space* of V if for all $x, y \in A$ and $a \in F$: (1) $x - y \subseteq A$; (2) $a \cdot x \subseteq A$. A subset $S = \{v_1, v_2, \cdots, v_n\}$ of a hypervector space V over a Krasner hyperfield F is called *linearly independent* if $c_1, c_2, \cdots, c_n \in F$ and $0 \in c_1 \cdot v_1 + c_2 \cdot v_2 + \cdots + c_n \cdot v_n$ then $c_1 = c_2 = \cdots = c_n = 0$. A subset S of V is called *linearly dependent* if it is not linearly independent. A subset $S = \{v_1, v_2, \cdots, v_n\}$ of a hypervector space V over a Krasner hyperfield F is said to *span* V if for every vector $v \in V$, there exists $c_1, c_2, \cdots, c_n \in F$ such that $v \in c_1 \cdot v_1 + c_2 \cdot v_2 + \cdots + c_n \cdot v_n$. A *basis* for a hypervector space V is a linearly independent subset of V such that it spans V. We say that V is finite dimensional if it has a finite basis.

3. Hyperring of polynomials over Krasner hyperfields

In this section, we present the results of Davvaz et al. in [9, 11] about polynomial hyperrings and present more results related to them by introducing new definitions.

Let $(R, +, \cdot)$ be a commutative additive multiplicative hyperring and $a, b \in R$. Then a is a *divisor* of b, denoted as $a|b$ if there exists $x \in R$ such that $b \in a \cdot x$. If $a \in R$ and $B \subseteq R$, then by $a|B$ we mean that $a|b$ for all $b \in B$.

Lemma 3.1. *Let $(R, +, \cdot)$ be a commutative additive multiplicative hyperring and $a, b, c \in R$. If $a|b$ and $b|c$, then $a|c$.*

Proof. Since $a|b, b|c$, it follows that there exists $x, y \in R$ such that $b \in ax$ and

$c \in by$. The latter implies that $c \in (ax)y = a(xy)$. Thus, there exists $r \in xy$ such that $c \in ar$. Therefore, $a|c$. $\square$

Lemma 3.2. *Let $(R, +, \cdot)$ be a commutative additive multiplicative hyperring and $a, b, c \in R$. If $a|b$ and $a|c$ then $a|(bs + ct)$ for all $s, t \in R$.*

Proof. Since $a|b, a|c$, it follows that there exists $x, y \in R$ such that $b \in ax$ and $c \in ay$. The latter implies that $bs \subseteq axs$ and $ct \subseteq ayt$. We get now that $bs + ct \subseteq axs + ayt = a(xs + yt)$. Thus, for every $r \in bs + ct$ there exists $k \in (xs + yt)$ such that $r \in ak$. Therefore, $a|(bs + ct)$. $\square$

In [11], Davvaz et al. defined two hyperoperations on $R[x]$, the set of all polynomials over R, as follows: for $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i \in R[x]$,

$$f(x) \oplus g(x) = \Big\{ \sum_{i=0}^{M} c_i x^i : c_i \in a_i + b_i, M = max\{m, n\} \Big\},$$
$$f(x) \odot g(x) = \Big\{ \sum_{k=0}^{m+n} c_k x^k : c_k \in \sum_{i+j=k} a_i b_j \Big\}.$$

Let $(R, +, \cdot)$ be a Krasner hyperring with unit element 1, where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and x be an indeterminate. Then $(R[x], \oplus, \odot)$ is an additive multiplicative hyperring [11]. It is easy to see that if F is a Krasner hyperfield with the property $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ for all $a, b \in F$ then $F[x]$ is a commutative additive-mutiplicative hyperring.

Theorem 3.1. [11] *Let F be a Krasner hyperfield and $f(x), g(x) \in F[x]$. If $h(x) \in f(x) \odot g(x)$ then $deg(h(x)) = deg(f(x)) + deg(g(x))$.*

Corollary 3.1. *Let F be a Krasner hyperfield and $f_i(x) \in F[x]$ for $i = 1, 2, \cdots k$. If $h(x) \in f_1(x) \odot \cdots \odot f_k(x)$ then $deg(h(x)) = deg(f_1(x)) + \cdots + deg(f_k(x))$.*

Proof. The proof follows from Theorem 3.1 and by induction on i. $\square$

Theorem 3.2. [11] *(Division Algorithm) Let $(F, +, \cdot)$ be a Krasner hyperfield with unit element 1 where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$. If $a(x), b(x) \in F[x]$ and $b(x) \neq 0$ then there exists a pair of polynomials $q(x), r(x) \in F[x]$ such that*

$$a(x) \in q(x) \odot b(x) \oplus r(x), deg(r(x)) < deg(b(x)).$$

For simplicity, instead of $f(x) \oplus g(x), f(x) \odot g(x)$ we write $f(x) + g(x), f(x)g(x)$ respectively. Let F be a Krasner hyperfield with unit element 1 where for all $a, b \in F$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x), d(x) \in F[x]$. Then $d(x) = \gcd(f(x), g(x))$ if the following axioms are satisfied: (1) $d(x)|f(x)$ and $d(x)|g(x)$; (2) if there exists $e(x) \in F[x]$ such that $e(x)|f(x)$ and $e(x)|g(x)$ then $e(x)|d(x)$; (3) $d(x)$ is monic. If no such element exists, we say that $\gcd(f(x), g(x))$ does not exist. If $\gcd(f(x), g(x)) = 1$ then we say that $f(x)$ and $g(x)$ are coprime.

Proposition 3.1. *Let F be a Krasner hyperfield with unit element 1 where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x) \in F[x]$ such that $f(x)|g(x)$ and $g(x)|f(x)$. Then there exists $k \in F \setminus \{0\}$ such that $f(x) = kg(x)$. Moreover, if $f(x)$ and $g(x)$ are both monic then $f(x) = g(x)$.*

Proof. Since $f(x)|g(x)$ and $g(x)|f(x)$, it follows that there exists $d(x), e(x) \in F[x]$ such that $g(x) \in f(x)d(x)$ and $f(x) \in g(x)e(x)$. The latter implies that $g(x) \in g(x)e(x)d(x)$. Corollary 3.1 implies that $deg(g(x)) = deg(g(x)) + deg(d(x)) + deg(e(x))$. Thus, $d(x), e(x) \in F$, i.e., there exists $a, k \in F$ such that $g(x) \in \{af(x)\}$ and $f(x) \in \{kg(x)\}$. Therefore, $f(x) = kg(x)$. If $f(x), g(x)$ are monic, then $k = 1$. □

Proposition 3.2. *Let F be a Krasner hyperfield with unit element 1 where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x), d(x) \in F[x]$. If $\gcd(f(x), g(x))$ exists then it is unique.*

Proof. Let $d(x), e(x)$ be two monic polynomials in $F[x]$ such that $d(x) = \gcd(f(x), g(x))$ and $e(x) = \gcd(f(x), g(x))$. Then $d(x)|e(x)$ and $e(x)|d(x)$. Proposition 3.1 implies that $d(x) = e(x)$. □

Proposition 3.3. *Let F be a Krasner hyperfield with unit element 1, where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x), q(x), r(x) \in F[x]$ and $k \in F \setminus \{0\}$. Then the following holds: (1) $\gcd(f(x), g(x)) = \gcd(g(x), f(x))$; (2) $\gcd(f(x), \gcd(g(x), h(x))) = \gcd(\gcd(f(x), g(x)), h(x))$; (3) $\gcd(kf(x), g(x)) = \gcd(f(x), g(x))$; (4) if $f(x)|g(x)$ and $f(x)$ has leading coefficient $a_n \in F \setminus \{0\}$ then $\gcd(f(x), g(x)) = a_n^{-1} f(x)$; (5) if $f(x) \in q(x)g(x) + r(x)$ and $g(x) \neq 0$ then $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$.*

Proof. The proofs of (1) and (2) are straightforward.

(3) Let $d(x) = \gcd(kf(x), g(x))$ and $e(x) = \gcd(f(x), g(x))$ be two monic polynomials in $F[x]$. Since $d(x)|kf(x)$, it follows that there exists $p(x) \in F[x]$ such that $kf(x) \in d(x)p(x)$. We get that $f(x) = k^{-1}kf(x) \in k^{-1}d(x)p(x) = d(x)(k^{-1}p(x))$. The latter implies that $d(x)|f(x)$. Having $d(x)|g(x)$ implies that $d(x)|e(x)$. In a similar manner, we get that $e(x)|d(x)$. Proposition 3.1 completes the proof.

(4) Let $d(x) = \gcd(f(x), g(x))$. Having $a_n^{-1}f(x)|f(x)$ and $a_n^{-1}f(x)|g(x)$ implies that $a_n^{-1}f(x)|d(x)$. On the other hand, $d(x)|f(x)$ implies that $d(x)|a_n^{-1}f(x)$. Therefore, by means of Proposition 3.1, $d(x) = a_n^{-1}f(x)$.

(5) Let $d(x) = \gcd(f(x), g(x))$ and $e(x) = \gcd(g(x), r(x))$ be two monic polynomials in $F[x]$. Since $f(x) \in q(x)g(x) + r(x)$ and $R[x]$ is a commutative additive-multiplicative hyperring, it follows that $r(x) \in f(x) - q(x)g(x)$. Having $d(x)|f(x)$, $d(x)|g(x)$ implies, by Proposition 3.2, that $d(x)|r(x)$. Thus, $d(x)|e(x)$. On the other hand, from $e(x)|g(x)$ and $e(x)|r(x)$ we conclude that $e(x)|(q(x)g(x) + r(x))$. Thus, $e(x)|f(x)$. We obtain now that $e(x)|d(x)$. Proposition 3.1 completes the proof. □

Theorem 3.3. *Let F be a Krasner hyperfield with unit element 1 where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x) \in F[x]$. If $\gcd(f(x), g(x))$ exists then it is an element in M where $M = \bigcup\{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\}$.*

Proof. Let $M = \bigcup\{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\} \neq \emptyset$ as $f(x) = 1f(x) + 0g(x) \in M$. Let $e(x)$ be a monic polynomial in M with minimum degree ≥ 0. By division algorithm, there exists $q(x), r(x) \in F[x]$ such that $f(x) \in q(x)e(x) + r(x)$ with $deg(r(x)) < deg(e(x))$. We get that $r(x) \in f(x) - q(x)e(x)$. Since $e(x)$ is a linear combination of $f(x)$ and $g(x)$, it follows that $r(x) \in f(x) - q(x)e(x) \subseteq M$. Having $e(x)$ with minimum degree in M implies that $r(x) = 0$ and consequently, $e(x)|f(x)$. In a similar manner, we get $e(x)|g(x)$. Thus, $e(x)|\gcd(f(x), g(x)) = d(x)$. Since $d(x)|f(x), d(x)|g(x)$, it follows that $d(x)|(s(x)f(x) + t(x)g(x))$ for all $s(x), t(x) \in F[x]$. Thus, $d(x)|e(x)$. Proposition 3.1 asserts that $d(x) = e(x)$. □

Let F be a Krasner hyperfield with unit element 1 where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x), m(x) \in F[x]$. Then $m(x) = lcm(f(x), g(x))$ if the following axioms are satisfied: (1) $f(x)|m(x)$ and $g(x)|m(x)$; (2) if there exists $n(x) \in F[x]$ such that $f(x)|n(x)$ and $g(x)|n(x)$ then $m(x)|n(x)$; (3) $m(x)$ is monic.

Proposition 3.4. *Let F be a Krasner hyperfield with unit element 1 where for all $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ and $f(x), g(x), d(x) \in F[x]$. If $lcm(f(x), g(x))$ exists then it is unique.*

Proof. The proof is similar to that of Proposition 3.2. □

Example 3.1. Let $F_2 = \{0, 1\}$ and define $(F_2, +)$ and $(F_2, \cdot)$ by Table 3.1 and Table 3.2 respectively. It is easy to see that $(F_2, +, \cdot)$ is a Krasner hyperfield. Moreover, it is easy

Table 3.1: Cayley's table of $(F_2, +)$

$+$	0	1
0	0	1
1	1	F_2

Table 3.2: Cayley's table of $(F_2, \cdot)$

$\cdot$	0	1
0	0	0
1	0	1

to see that x and $x + 1$ are coprime and that $\gcd(x^2 + 1, x^2 + x + 1) = x + 1$.

4. Construction of λ-constacyclic codes over finite Krasner hyperfields and their dual

In [13], H.Q. Dinh studied constacyclic codes over finite fields. In this section, we study constacyclic codes and their dual over finite hyperfields. We recall the following definitions from [14].

Let $Q = \{a_1, \cdots, a_r\}$ be a set of r elements. An *r-ary code* C of length n is a non empty subset of Q^n. And every element in C is called a *codeword*. Let $A \subseteq Q$ and C be a code of length n (a non empty subset of Q^n). The *subcode* $C|_A$ of C is defined as: $C|_A = \{c_0c_1 \cdots c_n : c_0, c_1, \cdots, c_n \in A\}$. Inspired by the definitions of linear codes and constacyclic codes over finite fields, we define linear codes and constacyclic codes over finite Krasner hyperfields.

Let F be a Krasner hyperfield and $C \subseteq F^n$ be a code with length n. Then C is a *linear code* if C is a subhypervector space of F^n. Let F be a Krasner hyperfield, $\lambda \in F \setminus \{0\}$ and $C \subseteq F^n$ be a linear code over F. Then C is a *λ-constacyclic code* if for every codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, the λ-constacyclic shift $T_\lambda(c) = (\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. According to the above definition, having C a λ-constacyclic code is equivalent to having $T_\lambda(C) = C$ i.e., C is invariant under the λ-constacyclic shifts. If $\lambda = 1$ then C is a cyclic code over F and if $\lambda = -1$ then C is a negacyclic code over F.
Throughout this section, F is a Krasner hyperfield with unit element 1, where for all $a, b \in F$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

Proposition 4.1. *Let F be a Krasner hyperfield, K a subhyperfield of F and $C \subseteq F^n$ be a code of length n. If $\lambda \in K$ and C is a λ-constacyclic code then $C|_K \subseteq K^n$ is λ-constacyclic code.*

Proof. First, we show that $C|_K$ is linear. Suppose that $a = (a_0, a_1, \cdots, a_{n-1}), b = (b_0, b_1, \cdots, b_{n-1}) \in C|_K$ and $k \in K$. We have that $a-b = (a_0-b_0, a_1-b_1, \cdots, a_{n-1}-b_{n-1})$ and $ka = (ka_0, ka_1, \cdots, ka_{n-1})$. Linearity of C implies that $a-b, ka \in C$ and having K a subhyperfield of F implies that $a_i-b_i, ka_i \in K$ for all $i = 0, 1, \cdots, n-1$. Thus, $a-b, ka \in C|_K$. In order to prove that $C|_K$ is invariant under λ-contacyclic shifts, we have

$$T_\lambda(a) = (\lambda a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C.$$

Having $\lambda a_{n-1}, a_0, a_1, \cdots, a_{n-2} \in K$ implies that $T_\lambda(a) \in C|_K$. □

Theorem 4.1. *Let F be a Krasner hyperfield and $C_i \subseteq F^n$ be a λ-constacyclic code of length n for all $i = 1, \cdots, k$. Then the following holds: (1) $C_1 + C_2 = \{a + b : a \in C_1, b \in C_2\}$ is a λ-constacyclic code; (2) $C_1 \cap C_2$ is a λ-constacyclic code; (3) $C_1 + \cdots + C_k$ is a λ-constacyclic code; (4) $C_1 \cap \cdots \cap C_k$ is a λ-constacyclic code.*

Proof. Davvaz et al. in [11] proved that $C_1 + C_2$ and $C_1 \cap C_2$ are linear.

(1) Let $x \in C_1 + C_2$. Then there exists $a = (a_0, a_1, \cdots, a_{n-1}) \in C_1$ and $b = (b_0, b_1, \cdots, b_{n-1}) \in C_2$ such that $x = (x_0, \cdots, x_{n-1}) \in a + b$. Since C_1, C_2 are λ-constacyclic codes, it follows that $T_\lambda(a) = (\lambda a_{n-1}, a_0, \cdots, a_{n-2}) \in C_1$ and $T_\lambda(b) = (\lambda b_{n-1}, b_0, \cdots, b_{n-2}) \in C_2$. We have that $T_\lambda(x) = (\lambda x_{n-1}, x_0, \cdots, x_{n-2}) \in (\lambda(a_{n-1} + b_{n-1}), a_0 + b_0, \cdots, a_{n-2} + b_{n-2}) = T_\lambda(a) + T_\lambda(b)$. Thus, $T_\lambda(x) \in C_1 + C_2$.

(2) Let $x = (x_0, \cdots, x_{n-1}) \in C_1 \cap C_2$. Then $x \in C_1$ and $x \in C_2$. Having C_1, C_2 λ-constacyclic codes implies that $T_\lambda(x) \in C_1 \cap C_2$.

(3) The proof follows from 1. and using induction on i.

(4) The proof follows from 2. and using induction on i. □

The dual of a linear code over an algebraic structure consists of all words that are orthogonal to every codeword and it was first defined by J.H. Van Lint [16]. We present a similar definition to the dual that is applicable to hyperstructures and was presented in [11]. Let F be a Krasner hyperfield and $C \subseteq F^n$ be a linear code. The *dual* $C^\perp$ of C is defined as follows:

$$C^\perp = \Big\{ y \in F^n : 0 \in \langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \text{ for all } x \in C \Big\}.$$

Moreover, C is called *self-orthogonal* if $C \subseteq C^\perp$ and is called *self dual* if $C = C^\perp$.

Proposition 4.2. *Let F be a Krasner hyperfield and $C \subseteq F^n$ be a code of length n. If $\lambda \in F \setminus \{0\}$ and C is a λ-constacyclic code then $C^\perp$ is a λ^{-1}-constacyclic code.*

Proof. Davvaz et al. in [11] proved that $C^\perp$ is linear. Let $x = (x_0, \cdots, x_{n-1}) \in C^\perp \subseteq F^n$. For all $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, we have that $\lambda^{-1} T_\lambda^{n-1}(c) = (c_1, c_2, \ldots, c_{n-1}, \lambda^{-1} c_0) \in C$. We get that

$$0 \in \langle x, \lambda^{-1} T_\lambda^{n-1}(c) \rangle = c_1 x_0 + c_2 x_1 + \cdots + c_{n-1} x_{n-1} + \lambda^{-1} c_0 x_1 = \langle T_{\lambda^{-1}}(x), c \rangle.$$

Thus, $T_{\lambda^{-1}}(x) \in C^\perp$. □

Corollary 4.1. *Let F be a Krasner hyperfield and $C \subseteq F^n$ be a code of length n. If $\lambda \in F \setminus \{0\}$ with $\lambda^2 = 1$ and C is a λ-constacyclic code then $C^\perp$ is λ-constacyclic code.*

Proof. Since $\lambda^2 = 1$, it follows that $\lambda = \lambda^{-1}$. Proposition 4.2 completes the proof. □

Corollary 4.2. *Let F be a Krasner hyperfield and $C \subseteq F^n$ be a code of length n. If C is a cyclic or negacyclic code then $C^\perp$ is cyclic or negacyclic code respectively.*

Proof. The proof is straightforward by using Corollary 4.1. □

Theorem 4.2. Theorem 3.7, [11] *Let F be a Krasner hyperfield and $f(x) \in F[x]$ be a polynomial of degree $n > 0$. Then $R = F[x]/\langle f(x) \rangle = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_0, \cdots, a_{n-1} \in F\}$ is a complete system of representative of the residue classes mod $f(x)$ in $F[x]$. Moreover, R is called the residue class hyperring.*

Corollary 4.3. *Let F be a Krasner hyperfield and $\lambda \in F$. Then $R = F[x]/\langle x^n - \lambda \rangle = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_0, \cdots, a_{n-1} \in F\}$ is a complete system of representative of the residue classes mod $(x^n - \lambda)$ in $F[x]$. Moreover, R is called the residue class hyperring.*

Let F be a finite Krasner hyperfield. The polynomial $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ of degree at most $n-1$ may be regarded as the codeword $a = a_0a_1 \cdots a_{n-1}$ of length n in F^n. In fact, we define a correspondence between F^n and the residue class hyperring $F[x]/\langle x^n - \lambda\rangle$. i.e., we have the function:

$$F^n \to F[x]/\langle x^n - \lambda\rangle$$

$$a_0a_1 \cdots a_{n-1} \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$

Then for every element $a = (a_0, a_1, \cdots, a_{n-1}) \in F^n$, there is a corresponding element $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]/\langle x^n - \lambda\rangle$ and vice-versa. In this setting, the multiplication by x to an element $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]/\langle x^n - \lambda\rangle$ results in $xa(x) = xa_0 + a_1x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n = \lambda a_{n-1} + xa_0 + a_1x^2 + \cdots + a_{n-2}x^{n-1} \in F[x]/\langle x^n - \lambda\rangle$. The latter is equivalent to applying T_λ to the corresponding element of F^n.

Let C denote the image of C under the above map and $R = F[x]/\langle x^n - \lambda\rangle$.

Theorem 4.3. *A linear code C in F is λ-constacyclic if and only if C is a hyperideal of $F[x]/\langle x^n - \lambda\rangle$.*

Proof. If C is a hyperideal of R and $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ is any codeword then $xa(x) = \lambda a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2} \in C$ and hence $T_\lambda(a) \in C$.

Conversely, if C is λ-constacyclic then from $a(x) \in C$ we have $T_\lambda(a) = xa(x) = \lambda a_{n-1} + xa_0 + a_1x^2 + \cdots + a_{n-2}x^{n-1} \in C$. Thus, $T^i_\lambda(a) = x^ia(x) \in C$. Since C is linear, it follows that $b(x)a(x) \subseteq C$ for all $b(x) \in F[x]$. Therefore, C is hyperideal of R. □

Theorem 4.4. *If C is a hyperideal of R then there exists a unique monic polynomial $g(x) \in R$ of minimum degree in $C = \langle g(x)\rangle$.*

Proof. The proof is similar to that of Theorem 4.8 in [11]. □

Proposition 4.3. *Let $C = \langle g(x)\rangle$ be a hyperideal of R. Then $g(x)|(x^n - \lambda)$.*

Proof. By Division algorithm, there exists $q(x), r(x) \in F[x]$ such that $x^n - \lambda \in g(x)q(x) + r(x)$ and $deg(r(x)) < deg(g(x))$. We get that $0 \in g(x)q(x) + r(x)$ in R. Since R is commutative additive-multiplicative hyperring, it follows that $r(x) \in -q(x)g(x) + 0 = -q(x)g(x) \subseteq C$. Minimality of $g(x)$ in C implies that $r(x) = 0$. Therefore, $g(x)|(x^n - \lambda)$. □

Corollary 4.4. *Let $C_1 = \langle g_1(x)\rangle, C_2 = \langle g_2(x)\rangle$ be hyperideals of R. Then $C_1 \subseteq C_2$ if and only if $g_2(x)|g_1(x)$.*

Proof. Suppose that $C_1 = \langle g_1(x)\rangle \subseteq C_2 = \langle g_2(x)\rangle$. Then $g_1(x) \in \langle g_2(x)\rangle$, i.e., there exists $q(x) \in R$ such that $g_1(x) \in q(x)g_2(x)$. Thus, $g_2(x)|g_1(x)$.

Conversely, if $g_2(x)|g_1(x)$ then there exists $q(x) \in R$ such that $g_1(x) \in q(x)g_2(x)$. The latter implies that $g_1 \in \langle g_2(x)\rangle$. Since $\langle g_2(x)\rangle$ is a hyperideal of R, it follows that $\langle g_1(x)\rangle \subseteq \langle g_2(x)\rangle$. □

Corollary 4.5. *Let C be a λ-constacyclic code. Then there exists a unique polynomial $g(x) \in R$ such that $C = \langle g(x) \rangle$ and $g(x)|(x^n - \lambda)$. $g(x)$ is called the generating polynomial of C.*

Proof. The proof follows from Proposition 4.3, Theorem 4.3, and Theorem 4.4. □

Theorem 4.5. *Let $C = \langle g(x) \rangle$ be a λ-constacyclic code of length n. Then dimension of C is equal to $n - deg(g(x))$.*

Proof. Let $k = deg(g(x))$, $m = n - k$ and $c(x) \in C = \langle g(x) \rangle$. Then $c(x) = 0$ or $deg(c(x)) < n$. Since $c(x) \in C = \langle g(x) \rangle$, it follows that there exists $f(x) \in F[x]$ such that $c(x) \in f(x)g(x)$. Theorem 3.1 implies that $f(x) = 0$ or $deg(f(x)) < m$. Thus, we can write C as $C = \{t(x) \in f(x)g(x) : f(x) = 0 \text{ or } deg(f(x)) < m\}$.

Let $S = \{g(x), xg(x), \cdots, x^{m-1}g(x)\} \subseteq C$ and $a_0, \cdots a_{m-1} \in F$ such that $0 \in a_0 g(x) + \cdots a_{m-1}x^{m-1}g(x) = (a_0 + \cdots + a_{m-1}x^{m-1})g(x)$ in R. Then $0 \in f(x)g(x)$ where $f(x) = a_0 + \cdots + a_{m-1}x^{m-1} = 0$. The latter implies that $f(x) = a_0 + \cdots + a_{m-1}x^{m-1} = 0$ as $deg(f(x)) \leq m - 1 < m$. We get that $a_0 = \cdots = a_{m-1} = 0$ and hence, S is linearly independent.

Let $c(x) \in C$. Then there exists $f(x) \in F[x]$, $f(x) = 0$ or $deg(f(x)) < m$ such that $c(x) \in f(x)g(x)$. The latter implies that there exist $a_0, \cdots a_{m-1} \in F$ such that $c(x) \in (a_0 + \cdots + a_{m-1}x^{m-1})g(x) = a_0 g(x) + \cdots a_{m-1}x^{m-1}g(x)$. Thus, S spans C. Therefore, S is a basis for C and dimension of C is equal to the cardinality of S which is m. □

Theorem 4.6. *Let F be a Krasner hyperfield and $C_i \subseteq F^n$ be a λ-constacyclic code of length n with generating polynomial $g_i(x)$ for all $i = 1, \cdots, k$. Then the following holds: (1) If $\gcd(g_1(x), g_2(x))$ exists then $C_1 + C_2 = \langle \gcd(g_1(x), g_2(x)) \rangle$; (2) If $lcm(g_1(x), g_2(x))$ exists then $C_1 \cap C_2 = \langle lcm(g_1(x), g_2(x)) \rangle$; (3) If $\gcd(g_1(x), \cdots, g_k(x))$ exists then $C_1 + \cdots + C_k = \langle \gcd(g_1(x), \cdots, g_k(x)) \rangle$; (4) If $lcm(g_1(x), \cdots, g_k(x))$ exists then $C_1 \cap \cdots \cap C_k = \langle lcm(g_1(x), \cdots, g_k(x)) \rangle$.*

Proof. Theorem 4.1 asserts that $C_1 + C_2$ and $C_1 \cap C_2$ are λ-constacyclic codes.

(1) Corollary 4.5 asserts that there exists a monic polynomial $h(x) \in R$ such that $C_1 + C_2 = \langle h(x) \rangle$. Let $d(x) = \gcd(g_1(x), g_2(x))$. Having $g_1(x) = g_1(x) + 0 \in \langle h(x) \rangle, g_2(x) = 0 + g_2(x) \in \langle h(x) \rangle$ implies that $h(x)|g_1(x), h(x)|g_2(x)$. We get that $h(x)|d(x)$. Thus, $\langle d(x) \rangle \subseteq \langle h(x) \rangle$. On the other hand, $d(x)|g_1(x), d(x)|g_2(x)$ implies that $\langle g_1(x) \rangle \subseteq \langle d(x) \rangle$ and $\langle g_2(x) \rangle \subseteq \langle d(x) \rangle$. Thus, $\langle h(x) \rangle = C_1 + C_2 \subseteq \langle d(x) \rangle$.

(2) Corollary 4.5 asserts that there exists a monic polynomial $s(x) \in R$ such that $C_1 \cap C_2 = \langle s(x) \rangle$. Let $m(x) = lcm(g_1(x), g_2(x))$. Having $s(x) \in \langle g_1(x) \rangle$ and $s(x) \in \langle g_2(x) \rangle$ implies that $g_1(x)|s(x), g_2(x)|s(x)$. We get now that $m(x)|s(x)$. Thus, $\langle s(x) \rangle \subseteq \langle m(x) \rangle$. On the other hand, $g_1(x)|m(x)$ and $g_2(x)|m(x)$. Thus, $\langle m(x) \rangle \subseteq \langle g_1(x) \rangle$ and $\langle m(x) \rangle \subseteq \langle g_2(x) \rangle$. The latter implies that $\langle m(x) \rangle \subseteq C_1 \cap C_2 = \langle h(x) \rangle$.

(3) The proof follows from 1. and by using induction on i.

(4) The proof follows from 2. and by using induction on i. □

Corollary 4.6. *Let F be a Krasner hyperfield and $C_i = \langle g_i(x)\rangle \subseteq F^n$ be a λ-constacyclic code of length n for $i = 1, 2$. If $g_1(x)$ and $g_2(x)$ are coprime then $C_1 + C_2 = F^n$.*

Proof. Using Theorem 4.6, $C_1 + C_2 = \langle \gcd(g_1(x), g_2(x))\rangle = \langle 1\rangle = F^n$. □

Proposition 4.4. *Let $g(x) \in R$ with degree $k < n$ and $C = \langle g(x)\rangle$ be a λ-constacyclic code of length n. Then there exists a monic polynomial $h(x) = b_0 + b_1x + \cdots + b_{n-k}x^{n-k}$ with degree $n-k$ such that $x^n - \lambda \in g(x)h(x)$ and $b_0 \neq 0$.*

Proof. Since $g(x)|(x^n - \lambda)$ (by Corollary 4.5), it follows that there exist $h(x) \in F[x]$ such that $x^n - \lambda \in g(x)h(x)$. Theorem 3.1 asserts that $n = deg(g(x)) + deg(h(x))$. Since $x^n - \lambda$ and $g(x)$ are both monic, it follows that $h(x)$ is monic.
Let $f(x) = a_0 + a_1x + \cdots + a_kx^k$. Having $x^n - \lambda \in g(x)h(x)$ implies that $-\lambda = a_0b_0$. Thus, $b_0 \neq 0$. □

Let $C = \langle g(x)\rangle$ be a hyperideal of R. We define $Ann(C) = \{f(x) \in R : 0 \in f(x)g(x)\}$.

Proposition 4.5. *Let $C = \langle g(x)\rangle$ be a hyperideal of R. Then $Ann(C)$ is a hyperideal of R.*

Proof. Suppose that $f_1(x), f_2(x) \in Ann(C)$ and $f_3(x) \in R$. Having $0 \in f_1(x)g(x)$ and $0 \in f_2(x)g(x)$ implies that $0 \in f_1(x)g(x) - f_2(x)g(x) = (f_1(x) - f_2(x))g(x)$. Thus, $f_1(x) - f_2(x) \subseteq Ann(C)$. Moreover, having $0 \in f_1(x)g(x)$ implies that $0 = f_3(x)0 \in f_3(x)f_1(x)g(x)$. Thus, $f_3(x)f_1(x) \subseteq Ann(C)$. Therefore, $Ann(C)$ is a hyperideal of R. □

Proposition 4.6. *Let $C = \langle g(x)\rangle$ be a hyperideal of R. Then $Ann(C) = \langle h(x)\rangle$, where $h(x)$ is the unique monic polynomial such that $x^n - \lambda \in h(x)g(x)$. $h(x)$ is the parity check polynomial for C.*

Proof. Suppose that $deg(g(x)) = k < n$ and $h_1(x), h_2(x) \in F[x]$ such that $x^n - \lambda \in h_1(x)g(x)$ and $x^n - \lambda \in h_2(x)g(x)$. Then $h_1(x), h_2(x)$ are monic polynomials and $deg(h_1(x)) = deg(h_2(x)) = n-k$. It is easy to see that $h_1(x), h_2(x) \in Ann(C)$. Since $Ann(C)$ is a hyperideal of R (by Proposition 4.5), it follows that $h_1(x) - h_2(x) \subseteq Ann(C)$. Having $h_1(x), h_2(x)$ monic polynomials of degree $n-k$ and $0 \in (1-1)$ implies that there exists $h_3(x) \in h_1(x) - h_2(x)$ with $deg(h_3(x)) < n-k$. We get now that $h_3(x) \in Ann(C)$. Thus, $0 \in h_3(x)g(x)$ in R. The latter implies that $x^n - \lambda \in h_3(x)g(x)$ in $F[x]$ which is impossible as $deg(h_3(x)) + deg(g(x)) < n$. Therefore, there is unique monic polynomial, say $h(x)$ such that $x^n - \lambda \in h(x)g(x)$.

Since $Ann(C)$ is a hyperideal of R and $h(x) \in Ann(C)$, it follows that $\langle h(x)\rangle \subseteq Ann(C)$. Let $f(x) \in Ann(C)$. By Division algorithm, there exists $q(x), r(x) \in F[x]$ such that $f(x) \in q(x)h(x) + r(x)$ with $deg(r(x)) < deg(h(x))$. The latter implies that $r(x) \in f(x) - q(x)h(x) \subseteq Ann(C)$. We get now that $0 \in r(x)g(x)$. It is easy to see that $deg(r(x)) = n - k = deg(h(x))$ or $r(x) = 0$. Since $deg(r(x)) < deg(h(x))$, it follows that $r(x) = 0$. Therefore, $Ann(C) = \langle h(x)\rangle$. □

Proposition 4.7. *Let $\lambda \in F \setminus \{0\}$ and $a(x) = \sum_{i=0}^{n-1} a_i x^i, b(x) = \sum_{i=0}^{n-1} b_i x^i \in F[x]$. Then $0 \in a(x)b(x) \subseteq R$ if and only if $(a_0, a_1, \cdots, a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, \cdots, b_1, b_0)$ and all its λ^{-1}-constacyclic shifts.*

Proof. Let $T_{\lambda^{-1}}$ denote the λ^{-1}-constacyclic shifts for codewords of length n and let L be the smallest positive integer such that $\lambda^L = 1$. For $1 \leq j \leq n, 0 \leq l \leq L-1$,

$$\begin{aligned} T_{\lambda^{-1}}^{j+ln}(b_{n-1}, b_{n-2}, \cdots, b_0) &= \lambda^{-l} T_{\lambda^{-1}}^{j}(b_{n-1}, b_{n-2}, \cdots, b_0) \\ &= \lambda^{-l}(\lambda^{-1}b_{j-1}, \cdots, \lambda^{-1}b_0, b_{n-1}, \cdots, b_j). \end{aligned}$$

Therefore, $T_{\lambda^{-1}}^{i}(b_{n-1}, b_{n-2}, \cdots, b_0)$, $i = 0, 1, \cdots, n$ are all λ^{-1}-constacyclic shifts of $(b_{n-1}, b_{n-2}, \cdots, b_0)$. Let $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in a(x)b(x) \subseteq R$. Then, for $k = 0, 1, \cdots, n-1, 0 \leq i, j \leq n-1$,

$$\begin{aligned} c_k \in & \sum_{i+j=k} a_i b_j + \sum_{i+j=n+k} \lambda a_i b_j \\ & = \langle (a_0, \cdots, a_k, a_{k+1}, \cdots, a_{n-1}), (b_k, b_{k-1}, \cdots, b_0, \lambda b_{n-1}, \cdots, \lambda b_{k-1}) \rangle. \end{aligned}$$

Having

$$\begin{aligned} (b_k, b_{k-1}, \cdots, b_0, \lambda b_{n-1}, \cdots, \lambda b_{k-1}) &= (\lambda^{-1}b_k, \lambda^{-1}b_{k-1}, \cdots, \lambda^{-1}b_0, b_{n-1}, \cdots, b_{k-1})\lambda \\ &= T_{\lambda^{-1}}^{k+1}(b_{n-1}, \cdots, b_0) \end{aligned}$$

implies that

$$c_k \in \langle (a_0, a_1, \cdots, a_{n-1}), \lambda T_{\lambda^{-1}}^{k+1}(b_{n-1}, \cdots, b_0) \rangle.$$

$c(x) = 0$ if and only if $c_k = 0$ for all $k = 0, 1, \cdots, n-1$. The latter is equivalent to $(a_0, a_1, \cdots, a_{n-1})$ is orthogonal to $T_{\lambda^{-1}}^{k+1}(b_{n-1}, b_{n-2}, \cdots, b_1, b_0)$. □

Let $p(x) = a_0 + a_1 x + \cdots + a_k x^k \in F[x]$ with $a_k \neq 0$. Define the *reciprocal polynomial* $p^\star(x) = x^k p(x^{-1}) = a_0 x^k + a_1 x^{k-1} + \cdots + a_{k-1}x + a_k$.

Proposition 4.8. *Let $p(x) = a_0 + a_1 x + \cdots + a_k x^k, q(x) = b_0 + b_1 x + \cdots + b_m x^m \in F[x]$. then the following are true: (1) $(p(x)q(x))^\star = p^\star(x)q^\star(x)$; (2) $deg(p^\star(x)) = deg(p(x))$ if and only if $a_0 \neq 0$; (3) For every $p(x) \in F[x]$, there exists $q(x) \in F[x]$ such that $p(x) = q^\star(x)$.*

Proof. The proof is straightforward. □

Let $C = \langle g(x) \rangle$ and $Ann(C) = \langle h(x) \rangle$. Then $Ann^\star(C) = \{f^\star(x) : 0 \in f(x)g(x)\} = \{(a(x)h(x))^\star = a^\star(x)h^\star(x) : a(x) \in F[x]\} = \langle h^\star(x) \rangle$.

Proposition 4.9. *If $\lambda = \pm 1$ and C is a λ-contacyclic code of length n over F. Then $C^\perp = Ann^\star(C)$.*

Proof. Corollary 4.1 implies that C and $C^\perp$ are both λ-constacyclic codes. Theorem 4.3 implies that C and $C^\perp$ are both hyperideals of R. The assertion now follows from Proposition 4.7. □

Proposition 4.10. *Let $C = \langle g(x)\rangle$ be a λ-constacyclic code of length n and $\lambda = \pm 1$. Then dimension of $C^{\perp}$ is equal to $deg(g(x))$.*

Proof. Since $C^{\perp} = \langle h^{\star}(x)\rangle$ is a λ-constacyclic code of length n (by Proposition 4.9), it follows by Theorem 4.5 that the dimension of $C^{\perp}$ is $n - deg(h^{\star}(x)) = n - deg(h(x)) = deg(g(x))$. □

Corollary 4.7. *Let $C = \langle g(x)\rangle$ be a λ-constacyclic code of length n and $\lambda = \pm 1$. Then (dimension of $C^{\perp}$)+ (dimension of C)= n.*

Proof. The proof results from Theorem 4.5 and Proposition 4.10. □

Corollary 4.8. *If $\lambda = \pm 1$ and C is a λ-contacyclic code of length n over F. Then C is self-orthogonal if and only if $h^{\star}(x)|g(x)$.*

Proof. Having C a self-orthogonal λ-contacyclic code is equivalent to $C = \langle g(x)\rangle \subseteq C^{\perp} = \langle h^{\star}(x)\rangle$ by Proposition 4.9. The latter is equivalent to $h^{\star}(x)|g(x)$ by Proposition 4.4. □

Corollary 4.9. *Let $\lambda = \pm 1$, $h(x) = a_0 + a_1x + \cdots + a_{n-k}x^{n-k}$ and C is a λ-contacyclic code of length n over F. Then C is self-dual if and only if $h^{\star}(x) = a_0g(x)$. Moreover, if C is self-dual then n is even positive integer.*

Proof. Having C a self-dual λ-contacyclic code is equivalent to $C = \langle g(x)\rangle = C^{\perp} = \langle h^{\star}(x)\rangle$ by Proposition 4.9. The latter is equivalent to $h^{\star}(x)|g(x), g(x)|h^{\star}(x)$ by Proposition 4.4. Since $g(x)$ is monic, it follows that the latter is equivalent to having $h^{\star}(x) = a_0g(x)$.
Since $h^{\star}(x) = a_0g(x)$ and $a_0 \neq 0$, it follows that $n - k = deg(h(x)) = deg(h^{\star}(x)) = deg(a_0g(x)) = k$. Thus, n is even. □

For a commutative additive-multiplicative hyperring A with identity 1, a linear code C of length n over A is an A-subhypermodule of A^n, the checking of linearity is equivalent to the checking of the following two conditions: (1) $x, y \in C$ implies $x + y \subseteq C$; (2) $k \in A$ and $x \in C$ implies $kx \subseteq C$. Next, we generalize constacyclic codes over finite Krasner hyperfields by introducing quasi-λ-constacyclic over finite Krasner hyperfields.

Let T_{λ} be the λ-constacyclic shift operator. A linear code C of length n over F is said to be a quasi-λ-constacyclic (λ-QC) code if there exists a positive integer l such that $T_{\lambda}^{l}(C) = C$. The smallest positive integer l satisfying $T_{\lambda}^{l}(C) = C$ is called the index of C. For $l = 1$, C is simply the λ-constacyclic code over F.

Let C be a λ-QC code of index l and length n over a Krasner hyperfield F, where $n = lm$ for some positive integer m (m is called the *coindex* of the code C). Let $R = F[x]/\langle x^m - \lambda\rangle$ denote the residue class hyperring and

$$c = (c_{0,0}, c_{0,1}, \cdots, c_{0,l-1}, c_{1,0}, c_{1,1}, \cdots, c_{1,l-1}, \cdots, c_{m-1,0}, c_{m-1,1}, \cdots, c_{m-1,l-1})$$

denotes a codeword in C. We define a map $\phi : F^{lm} \to R^l$ by $\phi(c) = (c_0(x), c_1(x) \cdots, c_{l-1}(x)) \in R^l$, where for $j = 0, \cdots, l-1$,

$$c_j(x) = \sum_{i=0}^{m-1} c_{i,j}x^i \in R.$$

Let $\phi(C)$ denotes the image of C under ϕ. The following proposition holds.

Proposition 4.11. *The map ϕ induces a one-to-one correspondence between λ-QC code of index l and length lm over F and linear codes of length l over R.*

Proof. Since C is a linear code over F, it follows that $\phi(C)$ is closed under scalar multiplication by the elements of F. Having $x^m = \lambda \in R$ implies that for all $j = 0, 1, \cdots, l-1$,

$$xc_j(x) = \sum_{i=0}^{m-1} c_{i,j}x^{i+1} = \lambda c_{m-1,j} + \sum_{i=1}^{m-1} c_{i-1,j}x^i.$$

The word $(xc_0(x), xc_1(x) \cdots, xc_{l-1}(x)) \in R^l$ corresponds to the word $d \in R^{lm}$ given by:

$$\begin{aligned} d = \quad & (\lambda c_{m-1,0}, \lambda c_{m-1,1}, \cdots, \lambda c_{m-1,l-1}, c_{0,0}, \cdots, c_{0,l-1}, c_{1,0}, \cdots, c_{1,l-1}, \cdots, \\ & c_{m-2,0}, \cdots, c_{m-2,l-1}). \end{aligned}$$

$d = T_\lambda^l(c) \in C$ as C is λ-QC code of index l. Therefore, $\phi(C)$ is closed under multiplication by x, and hence $\phi(C)$ is a subhypermodule of R^l. By reversing the above argument, one sees immediately that every linear code over R of length l comes from a λ-QC of index l and length lm over F. □

5. Conclusion

In this paper, we dealt with constacyclic codes, an important class of linear codes. We studied them over finite hyperfields, characterized their dual, and found their generating polynomial and parity check polynomial. Moreover, we generalized the notion of constacyclic codes to quasi constacyclic codes.

For future work, it will be interesting to characterize the generating matrix and parity check matrix for constacyclic codes over finite hyperfields.

REFERENCES

1. M. Al- Tahan and B. Davvaz: *On the existence of hyperrings associated to arithmetic functions*, Journal of number theory, **174** (2017), 136-149.
2. M. Al- Tahan and B. Davvaz: *Algebraic hyperstructures associated to biological inheritance*, Mathematical Biosciences, **285** (2017), 112-118.

3. M. Al- Tahan and B. Davvaz: *Chemical hyperstructures for Astatine, Tellurium and for Bismuth*, Bulletin of Computational Applied Mathematics, **7**(1) (2019), 9-25.
4. M. Al-Tahan, B. Davvaz, F. Smarandache, and O. Anis: *On some NeutroHyperstructures*, Symmetry, **13**(4) (2021), 535.
5. R. Ameri and O.R. Dehghan: *On dimension of hypervector spaces*, European Journal of Pure and Applied Mathematics, **1**(2) (2008), 32-50.
6. P. Corsini: *Prolegomena of Hypergroup Theory*, Aviani Editore, 1993, 216 pp.
7. P. Corsini and V. Leoreanu: *Applications of Hyperstructures Theory*, Advances in Mathematics, Kluwer Academic Publisher, 2003.
8. B. Davvaz: *Polygroup Theory and Related Systems*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2013. viii+200 pp.
9. B. Davvaz and A. Koushky: *On hyperrings of polynomials*, Italian J. Pure Appl. Math., **15** (2004), 205-214.
10. B. Davvaz and V. Leoreanu-Fotea: *Hyperring Theory and Applications*, International Academic Press, USA, 2007.
11. B. Davvaz and T. Musavi: *Codes over hyperring*, Matematicki Vesnik, **68** (2016), 26-38.
12. B. Davvaz, S. Subiono, and M. Al-Tahan: *Calculus of meet plus hyperalgebra (Tropical semihyperrings)*, Communication in Algebra, **48**(5) (2020), 2143-2159.
13. H.Q. Dinh: *Repeated-root constacyclic codes of length* $2p^s$, Finite fields and their applications, **18** (2012), 133-143.
14. W.C. Huffman and V. Pless: *Fundamentals of Error Correcting Codes*, Cambrige, 2003.
15. M. Krasner: *A class of hyperrings and hyperfields*, Internat. J. Math. Math. Sci., **2** (1983), 307-312.
16. J.H. Van Lint: *Introduction to Coding Theory*, Springer, New York, 1982.
17. F. Marty: *Sur une generalization de la notion de group*. In: 8*th* Congress Math. Scandenaves, Stockholm, Sweden, 14–18 August 1934, pp. 45-49.
18. C.G. Massouros: *Method of constructions of hyperfields*, Internat. J. Math. and Math. Sci., **8**(4) (1985), 725-728.
19. H.K. Mirdar and S.M. Anvariyeh: *A hypervaluation of a hyperfield onto a totally ordered canonical hypergroup*, Studia Sci. Math. Hungar., **52**(1) (2015), 87-101.
20. S. Mirvakili, S.M. Anvariyeh, and B. Davvaz: *Transitivity of* γ*-relation on hyperfields*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.), **51**(99) (2008), 233-243.
21. S. Mirvakili and B. Davvaz: *Relations on Krasner* (m, n)*-hyperrings*, European Journal of Combinatorics, **31** (2010), 790-802.
22. A. Nakassis: *Expository and survey article of recent results in hyperring and hyperfield theory*, Internat. J. Math. Math. Sci., **11** (1988), 209-220.
23. C.E. Shannon: *A mathematical theory of communication*, Bell System Tech. J., **27** (1948), 379-423, 623-656.
24. G. Tallini: *On Steiner hypergroups and linear codes*, Convegno Ipergruppi. Altre Strutture multivoche e loro applicazioni. Udine, 1985, 87-91.
25. M.S. Tallini: *Hypervector spaces*. In: Proceedings of the Fourth International Congress on Algebraic Hyperstructures and Applications, Xanthi, Greece, 1990, pp. 167-174.

26. T. Vougiouklis: *Hyperstructures and Their Representations*, Aviani editor. Hadronic Press, Palm Harbor, USA, 1994.

27. T. Vougiouklis: *The fundamental relation in hyperrings. The general hyperfield.* In: Proc. Fourth Int. Congress on Algebraic Hyperstructures and Applications (AHA 1990), World Scientific, 1991, pp. 203-211.