МАТЕМАТИЧКИ ВЕСНИК
68, 1 (2016), 26–38
March 2016

оригинални научни рад
research paper

# CODES OVER HYPERRINGS

**B. Davvaz and T. Musavi**

**Abstract.** Hyperrings are essentially rings, with approximately modified axioms in which addition or multiplication is a hyperoperation. In this paper, we focus on an important subclass of codes with additional structure called linear codes. Indeed, we introduce the notion of linear codes on finite hyperrings and we present a construction technique of cyclic codes over finite hyperrings. Since polynomial hyperrings are one of the main tools in our study, we analyze them too.

## 1. Introduction

Codes over rings have been discussed in a series of papers originating with Blake [1,2], who presented generalized notions of Hamming codes, Reed-Solomon codes, and BCH codes over arbitrary integer residue rings. In the past decade, a substantial research has been done on linear codes over finite rings. Many authors used to focus their research on codes over integer residue rings. Nowadays quite a few papers are concerned with linear codes over other classes of rings. Linear codes over finite rings with identity have recently raised a great interest for their new role in algebraic coding theory and for their successful application in combined coding and modulation. In [12], Greferath investigated cyclic linear codes over arbitrary (not necessarily commutative) finite rings. Some aspects of codes over finite rings (fields) has been earlier given in [13,14,17,23].

Algebraic hyperstructures were introduced by Marty in [18]. A hypergroup is an algebraic structure similar to a group, but the composition of two elements is a non-empty set. Mittas introduced in [22] the notion of canonical hypergroups. Several books have been written on this topic, see [3,4,6,26]. Hyperrings are essentially rings, with approximately modified axioms in which addition or multiplication is a hyperoperation. This concept has been studied by a variety of authors. A well known type of a hyperring is called the Krasner hyperring [16]. This concept has been studied by a variety of authors. Some principal notions of hyperring theory can be found in [5,7,10,19–21,24]. Davvaz and Koushky constructed in [8] the

*2010 Mathematics Subject Classification*: 20N20, 16Y99, 94B05
*Keywords and phrases*: hyperring; hyperring of polynomials; hyperideal; linear code; cyclic code.

hyperring of polynomials over a hyperring and they stated and proved some properties of the hyperring of polynomials. Then, Jančić-Rašović in [15] considered the construction of the hyperring of polynomials over a commutative hyperring $R$, for which $(R,+)$ is not necessarily a regular hypergroup. A recent book on hyperring theory is published by Davvaz and Leoreanu-Fotea [9]. They studied and analyzed several kinds of hyperrings.

Tallini established connections between code theory and hyperstructure theory [25]. Corsini and Leoreanu in Chapter 8 of [4] studied this connection too.

This paper is organized as follows. In Section 2, we present some basic facts about algebraic hyperstructures and hyperrings. In Section 3, we investigate some properties of polynomial hyperrings. In Section 4, we focus on an important subclass of codes with additional structure called linear codes. Indeed, we develop the notion of linear codes on hyperrings instead of rings (or fields). Also, we present a construction technique of cyclic codes over finite hyperrings.

## 2. Preliminaries

Let $H$ be a non-empty set and $\mathcal{P}^*(H)$ be the set of all non-empty subsets of $H$. Then, the map $\star : H \times H \longrightarrow \mathcal{P}^*(H)$, where $(x,y) \mapsto x \star y \subseteq H$ is called a *hyperoperation* and the couple $(H,\star)$ is called a *hypergroupoid* or *hyperstructure*. For any two non-empty subsets $A$ and $B$ of $H$ and $x \in H$, we define

$$A \star B = \bigcup_{a\in A, b\in B} a \star b, \quad A \star x = A \star \{x\} \text{ and } x \star B = \{x\} \star B.$$

A hypergroupoid $(H,\star)$ is called a *semihypergroup* if for all $a,b,c$ of $H$ we have $(a \star b) \star c = a \star (b \star c)$. A hypergroupoid $(H,\star)$ is called a *quasihypergroup* if for all $a$ of $H$ we have $a \star H = H \star a = H$. A hypergroupoid $(H,\star)$ which is both a semihypergroup and a quasihypergroup is called a *hypergroup*.

A *Krasner hyperring* is an algebraic structure $(R,+,\cdot)$ which satisfies the following axioms:

(1) $(R,+)$ is a canonical hypergroup, i.e.,
   (i) for every $x,y,z \in R$, $x+(y+z) = (x+y)+z$,
   (ii) for every $x,y \in R$, $x+y = y+x$,
   (iii) there exists $0 \in R$ such that $0+x = x$ for every $x \in R$,
   (iv) for every $x \in R$ there exists a unique element $x' \in R$ such that $0 \in x+x'$; (We shall write $-x$ for $x'$ and we call it the opposite of $x$.)
   (v) $z \in x+y$ implies $y \in -x+z$ and $x \in z-y$;

(2) $(R,\cdot)$ is a semigroup having zero as a bilaterally absorbing element, i.e., $x \cdot 0 = 0 \cdot x = 0$.

(3) The multiplication is distributive with respect to the hyperoperation $+$.

In the above definition, for simplicity of notation we write sometimes $xy$ instead of $x \cdot y$ and in (iii), $0+x = \{x\}$ instead of $0+x = x$.

Example 1. [9] Let $R = \{0,1,2\}$ be a set with the hyperoperation $+$ and the binary operation $\cdot$ defined as follows:

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | $R$ |
| 1 | 1 | 1 | $R$ |
| 2 | 2 | $R$ | 2 |

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 1 | 2 |

Then, $(R, +, \cdot)$ is a Krasner hyperring.

A Krasner hyperring $(R, +, \cdot)$ is called commutative (with unit element) if $(R, \cdot)$ is a commutative semigroup (with unit). A commutative Krasner hyperring is called a *Krasner hyperfield* if $(R - \{0\}, \cdot)$ is a group. A Krasner hyperring $R$ is called a *hyperdomain* if $R$ is a commutative hyperring with unit element and $ab = 0$ implies that $a = 0$ or $b = 0$ for all $a, b \in R$. Let $(R, +, \cdot)$ be a 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. The subhyperring $A$ of $R$ is *normal* in $R$ if and only if $x + A - x \subseteq A$ for all $x \in R$. A subhyperring $A$ of a hyperring $R$ is a *left* (*right*) *hyperideal* of $R$ if $ra \in A$ ($ar \in A$) for all $r \in R$, $a \in A$. Also, $A$ is called a *hyperideal* if $A$ is both a left and a right hyperideal. Let $A$ and $B$ be non-empty subsets of a hyperring $R$. The *sum* $A + B$ is defined by

$$A + B = \{x \mid x \in a + b \text{ for some } a \in A, b \in B\}.$$

The *product* $AB$ is defined by

$$AB = \{x \mid x \in \sum_{i=1}^{n} a_i b_i, a_i \in A, b_i \in B, n \in \mathbb{Z}^+\}.$$

If $A$ and $B$ are hyperideals of $R$, then $A + B$ and $AB$ are also hyperideals of $R$.

Let $A = \{a_1, a_2, \dots, a_r\}$ be a set of $r$ elements. An $r$-ary code $C$ of length $n$ is a non-empty subset of $n$-tuples with entries in $A$, i.e., $C \subset A^n$. The elements of the code $C$ are called codewords, and $C$ is called an *$r$-ary block code*. The size $r$ of the code alphabet is called the *radix of the code*. We denote the number of the codewords in a code $C$ by $|C|$. If $C \subset A^n$ contains $M$ codewords, then we say that $C$ has length $n$ and size $M$ and we denote it by $(n, M)$-code. The (*Hamming distance*) $d(x, y)$ between two vectors $x, y \in A^n$ is defined to be the number of coordinates in which $x$ and $y$ differ. $w_t(x)$ of a vector $x \in A^n$ is the number of non-zero coordinates in $x$. For a code $C$ containing at least two words, the minimum distance of a code $C$, denoted by $d(C)$, is

$$d(C) = \min\{d(x; y) : x, y \in C; x \neq y\}.$$

## 3. Polynomial hyperrings

An *additive-multiplicative hyperring* is an algebraic structure $(R, +, \cdot)$ which satisfies the following axioms:

(1) $(R, +)$ is a canonical hypergroup, i.e.,
(i) for every $x, y, z \in R$, $x + (y + z) = (x + y) + z$,

(ii) for every $x, y \in R$, $\ x + y = y + x$,
(iii) there exists $0 \in R$ such that $0 + x = x$ for every $x \in R$, where 0 is called additive identity,
(iv) for every $x \in R$ there exists a unique element $x' \in R$ such that $0 \in x + x'$ (We shall write $-x$ for $x'$ and we call it the opposite of $x$),
(v) $z \in x + y$ implies $y \in -x + z$ and $x \in z - y$.

(2) $(R, \cdot)$ is a semihypergroup having zero as a bilaterally absorbing element, i.e., $x \cdot 0 = 0 \cdot x = 0$.

(3) The hypermultiplication $\cdot$ is distributive with respect to the hyperoperation $+$.

(4) 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. Also, $R$ is called a hyperring with multiplicative identity if there exists $e \in R$ such that $x \cdot e = x = e \cdot x$ for every $x \in R$. We fix the notation 1 for the multiplicative identity.

EXAMPLE 2. Let $R = \{0,\ a,\ b,\ c\}$ be a set with two hyperoperations defined as follows:

| $+$ | $0$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $0$ | $0$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $\{0, a\}$ | $c$ | $\{b, c\}$ |
| $b$ | $b$ | $c$ | $\{0, b\}$ | $\{a, c\}$ |
| $c$ | $c$ | $\{b, c\}$ | $\{a, c\}$ | $R$ |

| $\cdot$ | $0$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $a$ | $0$ | $\{0, a\}$ | $0$ | $\{0, a\}$ |
| $b$ | $0$ | $0$ | $\{0, b\}$ | $\{0, b\}$ |
| $c$ | $0$ | $\{0, a\}$ | $\{0, b\}$ | $R$ |

Then, $(R, +, \cdot)$ is an additive-multiplicative hyperring.

A non-empty subset $A$ of an additive-multiplicative hyperring $R$ is a *left* (*right*) *hyperideal* if

(1) $a, b \in A$ implies $a - b \subseteq A$,

(2) $a \in A, r \in R$ imply $ra \subseteq A$ ($ar \subseteq A$).

Let $X$ be a subset of an additive-multiplicative hyperring $R$. Let $\{A_i \mid i \in J\}$ be the family of all hyperideals in $R$ which contain $X$. Then, $\bigcap_{i \in J} A_i$ is called the *hyperideal generated by* $X$. This hyperideal is denoted by $\langle X \rangle$. If $X = \{x_1, x_2, \ldots, x_n\}$, then the hyperideal $\langle X \rangle$ is denoted $\langle x_1, x_2, \ldots, x_n \rangle$.

LEMMA 3.1. *Let $R$ be an additive-multiplicative hyperring, $a \in R$ and $X \subset R$. Then*

*(1) The principal hyperideal $\langle a \rangle$ is equal to the set*

$$\Big\{t \mid t \in ra+as+na+k(a-a)+\sum_{i=1}^{m} r_i a s_i, r, s, r_i, s_i \in R, m \in \mathbb{Z}^+ and \ \ n, k \in \mathbb{Z}\Big\}.$$

*(2) If $R$ has a unit element, then*

$$\langle a \rangle = \Big\{t \mid t \in k(a-a) + \sum_{i=1}^{m} r_i a s_i, r_i, s_i \in R, m, k \in \mathbb{Z}^+\Big\}.$$

*(3) If $a$ is in the center of $R$, then*

$$\langle a \rangle = \Big\{t \mid t \in ra + na + k(a-a), r \in R, n \in \mathbb{Z}^+\Big\},$$

*where the center of $R$ is the set $\{x \in R \mid xy = yx \ for \ all \ y \in R\}$.*

*(4) $Ra = \{ra \mid r \in R\}$ is a left hyperideal in $R$ and $aR = \{r \mid r \in R\}$ is a right hyperideal in $R$. If $R$ has a unit element, then $a \in aR \cap Ra$.*

*(5) If $R$ has a unit element and $a$ is in the center of $R$, then $Ra = \langle a \rangle = aR$.*

*(6) If $R$ has a unit element and $X$ is included in the center of $R$, then*

$$\langle X \rangle = \Big\{t \mid t \in \sum_{i=1}^{m} r_i x_i, r_i \in R, x_i \in X, m \in \mathbb{Z}^+\Big\}.$$

Let $(R, +, \cdot)$ be a Krasner hyperring with unit element 1, where for every $a, b \in R$, $a(-b) = (-a)b = -(ab)$ and $x$ be an indeterminate. Assume that $i$ is a non-negative integer. Then, the expressions of the form $a_i x^i$ with $a_i \in R$ are called *monomials of degree $i$* in the indeterminate $x$ with coefficients in $R$. A formal sum

$$a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n \tag{1}$$

of a finite number of monomials $a_0 x^0, a_1 x^1, a_2 x^2, \ldots, a_n x^n$ with coefficients in $R$, where $n$ is any nonnegative integer, is called a polynomial. In polynomial (1), $a_i x^i$ is called its $i$-th degree term and $a_i$ is called the coefficient of term. When $a_i = 1$ we write $1x^i = x^i$. When $a_i = 0$, we usually omit the term $a_i x^i$ in the expression (1). In particular terms $0x^{n+1}, 0x^{n+2}, \ldots$ can be regarded as omitted in (1). In what follows, we define $x^0 = 1$ and $x^1 = x$. Often the simple notations $f(x), g(x), h(x), \ldots$ are used for polynomials.

Let $f(x)$ and $g(x)$ be two polynomials over $R$. If all their coefficients of terms of the same degree are equal, we say that $f(x), g(x)$ are equal or, in other words, that $f(x), g(x)$ are the same polynomials, written as $f(x) = g(x)$. In particular $a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n$ and $a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n + 0x^{n+1} 0x^{n+2} + \cdots + 0x^{n+m}$ are equal polynomials. Later on we will frequently use the summation sign $\sum$ to simplify to notation of the polynomial $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n$ as $f(x) = \sum_{i=0}^{n} a_i x^i$. If $a_n \neq 0$, $f(x)$ is called a polynomial of degree $n$, denoted by

$\deg f(x) = n$, and $a_n$ is called its leading coefficient. If $a_n = 1$, $f(x)$ is called a monic polynomial. When all the coefficients of $f(x)$ are 0, $f(x)$ is called the zero polynomial, denoted by 0 and we define $\deg 0 = -\infty$.

We denote by $R[x]$ the set of all polynomials in $x$ over $R$. Let $f(x)$ and $g(x)$ be any two elements of $R[x]$ and $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i$. Let $M = \max\{n, m\}$. Set

$$a_{n+1} = a_{n+2} = \cdots = a_M = 0, \text{ if } n < M$$
$$b_{m+1} = b_{m+2} = \cdots = b_M = 0, \text{ if } m < M.$$

Then, $f(x)$ and $g(x)$ can be written as $f(x) = \sum_{i=0}^{M} a_i x^i, g(x) = \sum_{i=0}^{M} b_i x^i$ . The hypersum and hypermultiplication of $f(x)$ and $g(x)$ are defined as follows:

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

THEOREM 3.2. *$(R[x], \oplus, \odot)$ is an additive-multiplication hyperring.*

*Proof.* The proof is similar to the polynomial hyperring construction in [8] and [15]. ■

$R[x]$ is called the *hyperring of polynomials* in an indeterminate $x$ over the Krasner hyperring $R$ or the hyperring of polynomials of $x$ over $R$. The zero element 0 of $R$ is the zero element of $R[x]$ and the identity 1 of $R$ is the identity of $R[x]$. Moreover, we have

THEOREM 3.3. *Let $(F, +, \cdot)$ be a Krasner hyperfield and $f(x), g(x) \in F[x]$.*

*(i) If $h(x) \in f(x) \odot g(x)$, then $\deg h(x) = \deg f(x) + \deg g(x)$,*

*(2) If $t(x) \in f(x) \oplus g(x)$, then $\deg t(x) \leq \max\{\deg\ f(x), \deg\ g(x)\}$.*

*Proof.* If one or both of $f(x)$ and $g(x)$ is 0, then $f(x) \odot g(x) = 0$ and both sides of (i) are $-\infty$. Suppose that both $f(x)$ and $g(x)$ are not 0. Assume that $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ and that $\deg f(x) = n$ and $\deg g(x) = m$. Then, $a_n \neq 0$ and $b_m \neq 0$. By the definition of hypermultiplication of polynomials, the coefficient of $x^{n+m}$ in every elements of $f(x) \odot g(x)$ is $a_n b_m \neq 0$ and all of the coefficients of terms of $\deg > n + m$ are 0. Therefore, for $h(x) \in f(x) \odot g(x)$, $\deg(h(x)) = m + n = \deg\ f(x) + \deg\ g(x)$.

The proof of (ii) is obvious. ■

THEOREM 3.4. (Division algorithm) *Let $F$ be a Krasner hyperfield with unit element 1, where for every $a, b \in R$, $a(-b) = (-a)b = -(ab)$ and $(F[x], \oplus, \odot)$ is the polynomials hyperring of $F$. If $a(x)$ and $b(x) \in F[x]$ and $b(x) \neq 0$, then there exists a pair of polynomials $q(x)$ and $r(x)$ such that*

$$a(x) \in q(x) \odot b(x) \oplus r(x), \quad \deg r(x) < \deg b(x). \tag{2}$$

*Proof.* We apply induction in the degree of $a(x)$. When $\deg a(x) < \deg b(x)$, let $q(x) = 0$ and $r(x) = a(x)$. Then,

$$a(x) \in 0 \odot b(x) \oplus r(x) = 0 \oplus a(x) = \{a(x)\}, \quad \deg a(x) = \deg r(x) < \deg b(x),$$

so we have relation (2). When $\deg a(x) \geq \deg b(x)$, let $\deg a(x) = n, \deg b(x) = m$ and

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$
$$b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$

where $a_n \neq 0$ and $b_m \neq 0$. Then, $n \geq m$. Now we consider $a(x) \ominus a_n b_m^{-1} x^{n-m} \odot b(x)$ (where $b_m^{-1}$ is the multiplicative inverse of $b_m$ in Krasner hyperfield $F$). Thus, by Theorem 3.3, $a_n b_m^{-1} x^{n-m} \odot b(x)$ is a polynomial of degree $n$ and with leading coefficient $a_n b_m^{-1} b_m = a_n$. Hence, $a_n b_m^{-1} x^{n-m} \odot b(x) = d_0 + d_1x + d_2x^2 + \cdots + d_nx^n$ (where $d_n = a_n$) and

$$a(x) \ominus a_n b_m^{-1} x^{n-m} \odot b(x) = \Big\{ \sum_{k=0}^{n} c_k x^k | c_k \in a_k - d_k \Big\}. \tag{3}$$

Thus, for every polynomial $\sum_{k=0}^{n} c_k x^k \in a(x) \ominus a_n b_m^{-1} x^{n-m} \odot b(x)$ the coefficient of $n$-th monomial, i.e., $c_n$, is an element of $a_n - a_n$. On the other hand, we have $0 \in a_n - a_n$. So, by choosing $c_n = 0$, it follows that there exists a polynomial

$$a_1(x) \in a(x) \ominus a_n b_m^{-1} x^{n-m} \odot b(x) \tag{4}$$

such that $\deg a_1(x) < n$. By the induction hypothesis, there exists a pair of polynomials $q_1(x)$ and $r_1(x)$ such that

$$a_1(x) \in q_1(x) \odot b(x) \oplus r_1(x), \ \deg r_1(x) < \deg b(x). \tag{5}$$

Hence, by (4) and (5), we obtain

$$a(x) \in a_1(x) \oplus a_n b_m^{-1} x^{n-m} \odot b(x) \subseteq q_1(x) \odot b(x) \oplus r_1(x) \oplus a_n b_m^{-1} x^{n-m} \odot b(x),$$

where $\deg r_1(x) < \deg b(x)$. By using the definition, we obtain

$$a(x) \in (q_1(x) \oplus a_n b_m^{-1} x^{n-m}) \odot b(x) \oplus r_1(x), \ \deg r_1(x) < \deg b(x),$$

Now, let $q(x) = q_1(x) \oplus a_n b_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$. Then, (2) follows. ■

Let $(R, \oplus, \odot)$ be any additive-multiplicative hyperring and $m$ be a fixed element of $R$. For any two elements $a, b \in R$, we define

$$a \equiv b \pmod{m} \Longleftrightarrow \exists r \in R \ \text{ s.t. : } \ a \in m \odot r \oplus b.$$

Lemma 3.5. *The above relation is an equivalence relation on $R$.*

*Proof.* (1) For every $a \in R$ with considered $r = 0$ we have $a \in m \odot 0 \oplus a = 0 \oplus a = \{a\}$, hence $a \equiv a \pmod{m}$.

(2 For every $a, b \in R$ if $a \equiv b \pmod{m}$, there exists $r \in R$ such that $a \in m \odot r \oplus b$. By using the definition, we get $b \in -(m \odot r) \oplus a$. So, $b \in m \odot (-r) \oplus a$, which implies that $b \equiv a \pmod{m}$.

(3) For every $a, b, c \in R$ if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, $\exists r, r' \in R$ such that $a \in m \odot r \oplus b$, $b \in m \odot r' \oplus c$, then it follows $a \in m \odot r \oplus m \odot r' \oplus c$. Thus, $a \in m \odot (r \oplus r') \oplus c$. So, there exists $t \in r \oplus r'$ such that $a \in m \odot t \oplus c$. Hence, $a \equiv c \pmod{m}$. ■

Each equivalence class is called a *residue class modulo* $m$ in $R$. The residue class modulo $m$ containing $a \in R$ will be denoted by $\overline{a}$. Denote the set of residue classes modulo $m$ in $R$ by $R/(m)$. Clearly, when $m = 0$, $R/(m) = R$. Let $a \in R$, then $\overline{a} \in R/(m)$. Clearly, $b \in \overline{a}$ if and only if $b \equiv a \pmod{m}$, i.e., $b \in m \odot r \oplus a$ for some $r \in R$. Let $\overline{a}$, $\overline{b}$ be two residue classes modulo $m$. Define hypersum and hypermultiplication of $\overline{a}$, $\overline{b}$ by

$$\overline{a} \boxplus \overline{b} = \{\overline{t} \mid t \in a \oplus b\},$$
$$\overline{a} \boxdot \overline{b} = \{\overline{s} \mid s \in a \odot b\}.$$

THEOREM 3.6. *$R/(m)$ is an additive-multiplicative huperring with respect the above hyperoperations.*

*Proof.* It is straightforward. ■

We observe that polynomial hyperring $(R[x], \oplus, \odot)$ created of Krasner hyperring $(R, +, \cdot)$, is an additive-multiplicative hyperring. Thus, for any polynomial $f(x)$, where $\deg f(x) = n > 0$, we can consider residue class hyperring $R[x]/(f(x))$.

THEOREM 3.7. *Let $F$ be a Krasner hyperfield and $f(x)$ be a polynomial of degree $n > 0$ of additive-multiplicative hyperring $F[x]$. Then the set of elements*

$$S = \{a_0 + a_1 x + a_2 + \cdots + a_{n-1}x^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}.$$

*is a complete system of representative of the residue classes* $\mod f(x)$ *in* $F[x]$.

*Proof.* Suppose that $g(x) \in F[x]$. By the division algorithm, there exist polynomials $q(x)$ and $r(x) \in F[x]$ such that

$$g(x) \in f(x) \odot r(x) \oplus q(x) \ , \ \deg\ r(x) < \deg\ f(x).$$

Since $\deg\ r(x) < \deg\ f(x) = n$, $r(x) \in S$, $g(x) \equiv r(x) \pmod{f(x)}$ and $\overline{g(x)} = \overline{r(x)}$. This proves that any polynomial in $F[x]$ lies in the residue class modulo $f(x)$ contaning a polynomial in $S$. Let

$$g_1(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1},$$
$$g_2(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1}x^{n-1},$$

be two elements of $S$. If $\overline{g_1(x)} = \overline{g_2(x)}$, then $g_1(x) \equiv g_2(x) \pmod{f(x)}$, so there is $r(x) \in F[x]$ such that $g_1(x) \in f(x) \odot r(x) \oplus g_2(x)$ and hence $g_1(x) \ominus g_2(x) \subseteq f(x) \odot r(x) \oplus g_2(x) \ominus g_2(x)$. But by Theorem 3.3, for every $c(x) \in g_1(x) \ominus g_2(x)$, $\deg c(x) \leq n - 1$ and for every $t(x) \in f(x) \odot r(x) \oplus g_2(x) \ominus g_2(x)$, $\deg t(x) = n + \deg\ r(x)$, i.e., $\deg t(x) \geq n$. Therefore, $S$ is a complete system of representatives of the residue classes modulo $f(x)$ in $F[x]$. ■

## 4. Construction of codes over a finite hyperring

Let the code alphabet be a finite Krasner hyperring $(R, +, \cdot)$ and $|R| = r$.

Let $R$ be a Krasner hyperring. A commutative hypergroup $A$ together with the map $\cdot : R \times A \to A$ (scalar multiplication) is called a *(left) hypermodul* over $R$, if for every $r, s \in R$ and $a, b \in A$,

(1) $r(a + b) = ra + rb$,

(2) $(r + s)a = ra + sa$,

(3) $r(sa) = (rs)a$.

For example, if $R$ is a Krasner hyperring, then $R^n$ is a hypermodul over $R$.

Definition 4.1. An $r$-ary linear code $C$ of length $n$ over $R$ is an $R$-subhypermodule of $R^n$. Namely, for every $c_1, c_2 \in C$ and $a_1, a_2 \in R$ we have $a_1c_1 + a_2c_2 \subseteq C$.

Example 3. Let $(R, +, \cdot)$ be a finite Krasner hyperring and $I$ be a hyperideal of $R$. Then, $I^n \subseteq R^n$ and $I^n$ is a linear code of length $n$ over $R$, i.e., $I^n$ is an $R$-subhypermodule of $R^n$. For every $c_1 = (c_{10}, c_{11}, \ldots, c_{1,n-1})$, $c_2 = (c_{20}, c_{21}, \ldots, c_{2,n-1}) \in C$ and $a_1, a_2 \in R$ we have

$$\begin{aligned} a_1c_1 + a_2c_2 &= a_1(c_{10}, c_{11}, \ldots, c_{1,n-1}) + a_2(c_{20}, c_{21}, \ldots, c_{2,n-1}) \\ &= (a_1c_{10}, a_1c_{11}, \ldots, a_1c_{1,n-1}) + (a_2c_{20}, a_2c_{21}, \ldots, a_2c_{2,n-1}) \\ &= (a_1c_{10} + a_2c_{20}, a_1c_{11} + a_2c_{21}, \ldots, a_1c_{1,n-1} + a_2c_{2,n-1}). \end{aligned}$$

Since $I$ is a hyperideal of $R$, we have, for $0 \leq j \leq n-1$, that $a_1c_{1j} + a_2c_{2j} \subseteq I$. Consequently, $a_1c_1 + a_2c_2 = (a_1c_{10} + a_2c_{20}, a_1c_{11} + a_2c_{21}, \ldots, a_1c_{1,n-1} + a_2c_{2,n-1}) \subseteq I^n$.

Definition 4.2. The *inner product* of vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $R^n$ is

$$x \cdot y^\top = \sum_{i=1}^{n} x_i y_i.$$

$C^\perp$, the *dual of linear code* $C$ is defined by

$$C^\perp = \{y \in R^n \mid 0 \in x.y^\top, \ \forall x \in C\}.$$

Proposition 4.3. *The dual of a linear code $C$ of length $n$ over $R$ is linear.*

*Proof.* Suppose that $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ are two elements of $C^\perp$ and $a, b \in R$. Then, for every $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ we have

$$\begin{aligned} 0 \in c.x^\top &= c_0x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1}, \\ 0 \in c.y^\top &= c_0y_0 + c_1y_1 + \cdots + c_{n-1}y_{n-1}. \end{aligned}$$

It is sufficient to show that $0 \in c \cdot (ax + by)^\top = c \cdot ax^\top + c \cdot by^\top$. We have

$$\begin{aligned}
&c \cdot (ax + by)^\top \\
&= \{(c_0, c_1, \ldots, c_{n-1}) \cdot (t_0, t_1, \ldots, t_{n-1})^\top \mid t_i \in ax_i + by_i, \quad 0 \leq i \leq n-1\} \\
&= \{c_0t_0 + c_1t_1 + \cdots + c_{n-1}t_{n-1} \mid t_i \in ax_i + by_i, \quad 0 \leq i \leq n-1\} \\
&\subseteq c_0(ax_0 + by_0) + c_1(ax_1 + by_1) + \cdots + c_{n-1}(ax_{n-1} + by_{n-1}) \\
&= c_0ax_0 + c_0by_0 + c_1ax_1 + c_1by_1 + \cdots + c_{n-1}ax_{n-1} + c_{n-1}by_{n-1} \\
&= a(c_0x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1}) + b(c_0y_0 + c_1y_1 + \cdots + c_{n-1}y_{n-1}) \\
&= a(c \cdot x^\top) + b(c \cdot y^\top).
\end{aligned}$$

Now, by (4), we get that $0 \in a(c \cdot x^\top) + b(c \cdot y^\top)$. Hence, $0 \in c \cdot (ax + by)^\top$. This implies that $ax + by \subseteq C^\top$. Therefore, $C^\top$ is a linear code. ∎

Definition 4.4. Let $c$ be a vector of length $n$ over $R$. The *cyclic shift* $T(c)$ is the vector of length $n$:

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

Definition 4.5. A code $C$ of length $n$ over a finite Krasner hyperfield $F$ (finite Krasner hyperring $R$) is said to be *cyclic* if $T(c) \in C$ whenever $c \in C$, i.e., $T(C) = C$.

Theorem 4.6. *If $C_1$ and $C_2$ are cyclic codes of length $n$ over a finite Krasner hyperfield $F$ (finite Krasner hyperring $R$), then*

*(1)* $C_1 + C_2 = \{c_1 + c_2 \mid c_1 \in C_1, c_2 \in C_2\}$ *is cyclic.*

*(2)* $C_1 \cap C_2$ *is cyclic.*

*Proof.* (1) First, we prove that $C_1 + C_2$ is linear. Let $t, s \in C$ and $a, b \in R$. Then, there exist $c_1, d_1 \in C_1$ and $c_2, d_2 \in C_2$ such that $t \in c_1 + c_2$ and $s \in d_1 + d_2$. Thus, $at \in a(c_1 + c_2)$ and $bs \in b(d_1 + d_2)$. This implies that $at \in ac_1 + ac_2$ and $bs \in bd_1 + bd_2$. Since $C_1, C_2$ are linear, $ac_1, bd_1 \in C_1$ and $ac_2, bd_2 \in C_2$. Hence,

$$at \in C_1 + C_2 \text{ and } bs \in C_1 + C_2.$$

Thus, $at + bs \subseteq C_1 + C_2$ and so $C_1 + C_2$ is linear. Now, we prove that the $C_1 + C_2$ is cyclic. Assume that

$$t = (t_0, t_1, \ldots, t_{n-1}) \in C_1 + C_2 = \{a \mid a \in c + d, c \in C_1, d \in C_2\}.$$

Then, there exist $c = (c_0, c_1, \ldots, c_{n-1}) \in C_1$ and $d = (d_0, d_1, \ldots, d_{n-1}) \in C_2$ such that $t \in c + d$. It is sufficient to show that $(t_{n-1}, t_0, \ldots, t_{n-2}) \in C_1 + C_2$. Since $C_1$ and $C_2$ are cyclic, $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C_1$ and $(d_{n-1}, d_0, \ldots, d_{n-2}) \in C_2$. Therefore, $(c_{n-1}, c_0, \ldots, c_{n-2}) + (d_{n-1}, d_0, \ldots, d_{n-2}) \subseteq C_1 + C_2$, i.e.,

$$\{(s_{n-1}, s_0, \ldots, s_{n-2}) \mid s_i \in c_i + d_i, \quad 0 \leq i \leq n-1\} \subseteq C_1 + C_2,$$

such as $(t_{n-1}, t_0, \ldots, t_{n-2}) \in C_1 + C_2$. Thus, $C_1 + C_2$ is cyclic.

(2) First, we prove that $C_1 \cap C_2$ is linear. If $x, y \in C_1 \cap C_2$ and $a, b \in R$, then $x \in C_1, C_2$ and $y \in C_1, C_2$. Since $C_1, C_2$ are linear, $ax + by \subseteq C_1$ and $ax + by \subseteq C_2$. Therefore, $ax + by \subseteq C_1 \cap C_2$ and this means that $C_1 \cap C_2$ is linear. Finally, we prove that the $C_1 \cap C_2$ is cyclic. Assume that $t = (t_0, t_1, \ldots, t_{n-1}) \in C_1 \cap C_2$. It is enough to show that $(t_{n-1}, t_0, \ldots, t_{n-2}) \in C_1 \cap C_2$. Since $C_1, C_2$ are cyclic, hence $(t_{n-1}, t_0, \ldots, t_{n-2}) \in C_1, C_2$. Consequently, $(t_{n-1}, t_0, \ldots, t_{n-2}) \in C_1 \cap C_2$. ■

Let $F$ be a finite Krasner hyperfield. The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ of degree at most $n-1$ over $F$ may be regarded as the word $a = a_0a_1a_2 \ldots a_{n-1}$ of length $n$ in $F^n$ . In fact, we define a correspondence between $F^n$ and residue class hyperring $F[x]/(x^n - 1)$, i.e., we have the function

$$F^n \longrightarrow F[x]/(x^n - 1)$$
$$c_0c_1 \ldots c_{n-1} \mapsto c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

Then, for every element $c = (c_0, c_1, \ldots, c_{n-1})$ of $F^n$, there is a corresponding element $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ and vice-versa. Under this correspondence, $T(c)$ for some $c = (c_0, c_1, \ldots, c_{n-1}) \in F^n$ corresponds to the element $c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-2} \in F[x]/(x^n - 1)$. In this setting, multiplication by $x$ to any element of $F[x]/(x^n - 1)$ is equivalent to applying $T$ to the corresponding element of $F^n$. Let $C$ denote the image of $C$ under the above map.

THEOREM 4.7. *A linear code $C$ in $F$ is cyclic if and only if $C$ is a hyperideal in $F[x]/(x^n - 1)$.*

*Proof.* If $C$ is a hyperideal in $F[x]/(x^n-1)$ and $c(x) = c_0+c_1x+\cdots+c_{n-1}c^{n-1}$ is any codeword, then $x \odot c(x)$ is also a codeword, i.e. $c_{n-1}+c_0x+\cdots+c_{n-2}x^{n-2} \in C$ and hence $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

Conversely, if $C$ is cyclic, then from $c(x) \in C$ we have $x \odot c(x) \in C$. Therefore, $x^i \odot c(x) \in C$, and since $C$ is linear, then $a(x)c(x) \in C$ for each polynomial $a(x)$. Thus, $C$ is a hyperideal. ■

THEOREM 4.8. *If $C$ is a hyperideal in $F[x]/(x^n - 1)$, then there is a unique monic polynomial $g(x)$ of minimum degree in $C = \langle g(x) \rangle$, and it is called the generating polynomial for code $C$.*

*Proof.* Suppose that $C$ contains two distinct monic polynomials $g_1 = a_0+a_1x+\cdots+x^r$ and $g_2 = b_0+b_1x+\cdots+x^r$ of minimum degree $r$. Since $C$ is a hyperideal, hence $g_1-g_2 \subseteq C$. Thus, $(a_0-b_0)+(a_1-b_1)x+\cdots+(1-1)x^r \subseteq C$. Since $0 \in 1-1$, hence $(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{r-1} - b_{r-1})x^{r-1} \subseteq C$. Hence, there exists a non-zero polynomial in $C$ of degree less than $r$, which is not possible. Therefore, there is a unique monic polynomial $g(x)$ of degree $r$ in $C$. Since $g(x) \in C$ and $C$ is a hyperideal, we have $\langle g(x) \rangle \subset C$. On the other hand, suppose that $p(x) \in C$. By the division algorithm, we obtain $p(x) \in q(x) \odot g(x) \oplus r(x)$, where $r(x) \neq 0$ and $\deg(r(x)) < r$. If $r(x) \neq 0$, then we obtain $r(x) \in p(x) \ominus q(x)g(x)$. Since $C$ is a hyperideal, $p(x) \in C$ and $\langle g(x) \rangle \subseteq C$ implies that $r(x) \in p(x) \ominus q(x)g(x) \subseteq C$. Thus, $r(x) \in C$ and this means that $C$ contains a polynomial of degree less than

$r$, which is a conflict. So, $r(x) = 0$, $p(x) \in q(x) \odot g(x) \subseteq < g(x) >$. Therefore, $C \subset \langle g(x) \rangle$. ■

For a commutative Krasner hyperring $A$ with identity, a linear code $C$ of length $n$ over $A$ is an $A$-subhypermodule of $A^n$. If $C$ is a subset 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) $\lambda \in A$ and $x \in C$ imply $\lambda x \in C$.

DEFINITION 4.9. Let $T$ be the standard cyclic shift operator. A linear code $C$ of length $n$ over $R$ is said to be a *quasi-cyclic* (QC) *code* if it is invariant under $T^l$ for some positive integer $l$, i.e., if $T^l(C) = C$. The smallest positive integer $l$ such that $T^l(C) = C$ is called the *index* of $C$. For $l = 1$, $C$ is simply a cyclic code over $A$. A $QC$ code of index $l$ is also called an $l - QC$ code.

Let $C$ be a quasi-cyclic code of length $n$ and index $l$ over hyperfield $F$, where $l$ is a divisor of $n$, i.e., for some positive integer $m$, $n = lm$. Let $R = F[x]/(x^m - 1)$ denote the residue class hyperring. Let

$$C = (c_{00}, c_{01}, \ldots, c_{0,l-1}, c_{10}, \ldots, c_{1,l-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,l-1})$$

denote a codeword in $C$. We define a map $\phi : R^{lm} \longrightarrow \mathcal{R}^l$ by $\phi(c) = (c_0(x), c_1(x), \ldots, c_{l-1}(x)) \in \mathcal{R}^l$, where

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

Let $\phi(C)$ denote the image of $C$ under $\phi$. The following proposition is true.

PROPOSITION 4.10. *The map $\phi$ induces a one-to-one correspondence between quasi-cyclic codes over $F$ of index $l$ and length $lm$ and linear codes over $R$ of length $l$ .*

*Proof.* Since $C$ is a linear code over $F$, $\phi(C)$ is closed under scalar multiplication by elements of $F$. Since $x^m = 1$ is in $R$,

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

where the subscript $i - 1$ is considered to be in $\{0, 1, \ldots, m-1\}$ by taking modulo $m$. The word

$$(xc_0(x), xc_1(x), \ldots, xc_{l-1}(x)) \in \mathcal{R}^l,$$

corresponds to the word

$$(c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,l-1}, c_{00}, c_{01}, \ldots, c_{0,l-1}, \ldots, c_{m-2,0}, \ldots, c_{m-2,l-1}) \in R^{lm},$$

which is in $C$ since $C$ is quasi-cyclic of index $l$. Therefore, $\phi(C)$ is closed under multiplication by $x$, and hence $\phi(C)$ is an $R$-submodule of $R^n$. By reversing the

above argument, one sees immediately that every linear code over $R$ of length $l$ comes from a quasi-cyclic code of index $l$ and length $lm$ over $F$. ■

REFERENCES


[**1**] I.F. Blake, *Codes over certain rings*, Information and Control, **20** (1972), 396–404.

[**2**] I.F. Blake, *Codes over integer residue rings*, Information & Control, **29** (1975), 295–300.

[**3**] P. Corsini, *Prolegomena of Hypergroup Theory*, Second edition, Aviani Editor, 1993.

[**4**] P. Corsini and V. Leoreanu, *Applications of Hyperstructure Theory*, Kluwer Academical Publications, Dordrecht, 2003.

[**5**] I. Cristea and S. Jančić-Rašović, *Composition hyperrings*, An. St. Univ. Ovidius Constanta, **21**(2) (2013), 81–94.

[**6**] B. Davvaz, *Polygroup Theory and Related Systems*, World Scientific, 2013.

[**7**] B. Davvaz, *Approximations in hyperrings*, J. Mult.-Valued Logic Soft Comput., **15** (5-6) (2009), 471–488.

[**8**] B. Davvaz and A. Koushky, *On hyperring of polynomials*, Ital. J. Pure Appl. Math., **15** (2004), 205–214.

[**9**] B. Davvaz and V. Leoreanv-Fotea, *Hyperring Theory and Applications*, International Academic Press, USA, 2007.

[**10**] B. Davvaz and T. Vougiouklis, *Commutative rings obtained from hyperrings ($H_v$-rings) with $\alpha^*$-relations*, Comm. Algebra, **35** (2007), 3307–3320.

[**11**] A.A. de Andrade and R. Palazzo Jr., *Linear codes over finite rings*, TEMA Tend. Mat. Apl. Comput., **6**(2) (2005), 207–217.

[**12**] M. Greferath, *Cyclic codes over finite rings*, Discrete Math., **177** (1997), 273–277.

[**13**] D. Hofman, *Coding Theory*, Markel Dekker, 1990.

[**14**] W.C. Huffman and V. Pless, *Fundementals of Error-Correcting Codes*, Cambridge, U.K.: Cambridge Univ. Press, 2003.

[**15**] S. Jančić-Rašović, *About the hyperring of polynomials*, Ital. J. Pure Appl. Math., **21** (2007), 223–234.

[**16**] M. Krasner, *A class of hyperrings and hyperfields*, Int. J. Math. Math. Sci. **2** (1983), 307–312.

[**17**] S. Ling, P. Sole, *On the algebraic structures of quasi-cyclic codes II: finite fields*, IEEE Trans. Inf. Theory **47** (2001), 2751–2760.

[**18**] F. Marty, *Sur une generalization de la notion de groupe*, $8^{iem}$ congres Math. Scandinaves, Stockholm, (1934), 45–49.

[**19**] S. Mirvakili and B. Davvaz, *Strongly transitive geometric spaces: Applications to hyperrings*, Rev. Un. Mat. Argentina, **53**(1) (2012), 43–53.

[**20**] S. Mirvakili, B. Davvaz, *Applications of the $\alpha^*$-relation to Krasner hyperrings*, J. Algebra, **362** (2012), 145–156.

[**21**] S. Mirvakili and B. Davvaz, *Relationship between rings and hyperrings by using the notion of fundamental relations*, Comm. Algebra, **41** (2013), 70–82.

[**22**] J. Mittas, *Hypergroupes canoniques*, Math. Balkanica, **2** (1972), 165–179.

[**23**] S. Roman, *Coding and Information Theory*, Springer-Verlag, 1992.

[**24**] S. Spartalis, *A class of hyperrings*, Riv. Mat. Pura Appl., **4** (1989), 55–64.

[**25**] G. Tallini, *On Steiner hyper groups and Linear codes*, Convegno Ipergruppi, Altre Strutture multivoche e loro applicazioni, Udine, 1985, 87–91.

[**26**] T. Vougiouklis, *Hyperstructures and Their Representations*, Hadronic Press, Florida, 1994.


(received 13.04.2015; in revised form 01.09.2015; available online 10.10.2015)

Department of Mathematics, Yazd University, Yazd, Iran

*E-mail*: davvaz@yazd.ac.ir, bdavvaz@yahoo.com