Discussiones Mathematicae
General Algebra and Applications 37 (2017) 147–160
doi:10.7151/dmgaa.1277

CODES OVER HYPERFIELDS

Surdive Atamewoue Tsafack

Department of Mathematics
University of Yaounde 1, Cameroon
e-mail: surdive@yahoo.fr

Selestin Ndjeya

Department of Mathematics
Higher Teacher Training College
University of Yaounde 1, Cameroon
e-mail: ndjeyas@yahoo.fr

Lutz Strüngmann

Faculty of Computer Sciences
Institute for Mathematical Biology
Mannheim University of Applied Sciences
68163 Mannheim, Germany
e-mail: l.struengmann@hs-mannheim.de

and

Celestin Lele

Department of Mathematics
University of Dschang, Cameroon
e-mail: celestinlele@yahoo.com

Abstract

In this paper, we define linear codes and cyclic codes over a finite Krasner hyperfield and we characterize these codes by their generator matrices and parity check matrices. We also demonstrate that codes over finite Krasner hyperfields are more interesting for code theory than codes over classical finite fields.

Keywords: hypervector space, hyperring, hyperfield, linear code.

2010 Mathematics Subject Classification: 20N20, 54B20, 94B05.

1. Introduction

In [10], Marty introduced the notion of an algebraic hyperstructure. Later, many authors have extended the works of Marty to hyperrings, hyperfields and in particular to the well known Krasner hyperfield [8]. In [3], Davvaz and Koushky used a Krasner hyperfield K to construct the hyperring of polynomials over K and they stated and proved some exciting properties of the hyperring of polynomials. In [1], Ameri and Dehghan treated the notion of hypervector space over a field, on which only the external composition is a hyperoperation; they stated and proved some interesting facts about the hypervector space. In [11], Sanjay Roy and Samanta introduced the notion of hypervector spaces over hyperfields, where both external and internal compositions are both hyperoperations.

Recently, Davvaz and Musavi [5] defined a hypervector space over a Krasner hyperfield and established some connections between the hypervector space and some interesting codes. They also defined linear codes and cyclic codes over hyperfields.

In this paper, we introduce the notion of distance and weight on a hypervector space over a finite Krasner hyperfield. We also define a generator and a parity check matrix of a hyperlinear code over a finite Krasner hyperfield and obtain some of their crucial properties. We also compute the number of code words of a linear code over such finite Krasner hyperfield and we show that in addition to the fact that the Singleton bound is respected, they have many more code words than the classical codes with the same parameters.

Our work is organized as follows: In section 2 we present some basic notions about algebraic hyperstructures and Krasner hyperfields that we will use in the sequel. We also investigate some properties of hypervector spaces of finite dimension and of polynomial hyperrings. In section 3 we develop the notion of linear codes and cyclic codes over a finite Krasner hyperfield and we characterize them by their generator matrix and their parity check matrix. We also define the distance for these codes.

Our main results on the importance of hyperfields in code theory are stated and proved, e.g. it is shown that the Singleton bound is respected.

2. Preliminaries

In this section, we recall the preliminary definitions and results that are required in the sequel (for references see [1, 2, 4, 8]). Let H be a non-empty set and $\mathcal{P}^*(H)$ be the set of all non-empty subsets of H. Then, a 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*. For any two non-empty subsets A and B of H and $x \in H$, we define $A \star B = \bigcup_{a\in A, b\in B} a \star b$, $A \star x = A \star \{x\}$ and $x \star B = \{x\} \star B$. A hypergroupoid $(H,\star)$ is called a *semihypergroup* if $(a\star b)\star c = a\star(b\star c)$, for all $a,b,c\in H$. A hypergroupoid $(H,\star)$ is called a *quasihypergroup* if for all $a\in H$, 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*.

Definition. A *canonical hypergroup* is an algebraic structure $(R,+)$, (where $+$ is a hyperoperation) such that the followings axioms holds:

(i) for any $x,y,z\in R$, $x+(y+z)=(x+y)+z$,

(ii) for any $x,y\in R$, $x+y=y+x$,

(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) for every $x,y,z\in R$, $z\in x+y$ implies $y\in -x+z$ and $x\in -y+z$.

Definition. A *Krasner hyperring* is an algebraic structure $(R,+,\cdot)$ where $+$ is a hyperoperation satisfying the following axioms:

(i) $(R,+)$ is a canonical hypergroup with 0 as additive identity,

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

(iii) the multiplication is distributive with respect to the hyperoperation "+".

A Krasner hyperring $(R,+,\cdot)$ is called *commutative* (with unit element) if $(R,\cdot)$ is a commutative semigroup (with unit). A commutative Krasner hyperring with unit is called a *Krasner hyperfield* if $(R\setminus\{0\},\cdot,1)$ is a group.

We now give an example of a finite hyperfield with two elements 0 and 1, that we name F_2 and which will be used it in the sequel.

Example 1. Let $F_2=\{0,1\}$ be the finite set with two elements. Then F_2 becomes a Krasner hyperfield with the following hyperoperation "+" and binary operation "$\cdot$"

$+$	0	1
0	$\{0\}$	$\{1\}$
1	$\{1\}$	$\{0,1\}$

and

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

A Krasner hyperring R is called a *hyperdomain* if R is a commutative hyperring with unit element and $a\cdot b=0$ 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 $r \cdot a \in A$ ($a \cdot r \in A$) 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 $A + B = \{x | \ x \in a + b$ for some $a \in A, b \in B\}$ and the product $A \cdot B$ is defined by $A \cdot B = \{x | x \in \sum_{i=1}^{n} a_i \cdot b_i$, with $a_i \in A, b_i \in B, n \in \mathbb{N}^*\}$. It is easy to see, that if A and B are hyperideals of R, then $A + B$ and $A \cdot B$ are also hyperideals of R.

Definition. An *additive-multiplicative hyperring* is an algebraic structure $(R,+,\cdot)$ (where $+$ and $\cdot$ are both hyperoperations) which satisfies the following axioms:

(i) $(R, +)$ is a canonical hypergroup with 0 as additive identity,

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

(iii) the hypermultiplication "$\cdot$" is distributive with respect to the hyperoperation "$+$",

(iv) 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 and 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.

We give an example of an additive-multiplicative hyperring.

Example 2. Let $F_4 = \{0, 1, 2, 3\}$ be a set with the hyperoperations as follows:

$+$	0	1	2	3
0	0	1	2	3
1	0	2	$\{1, 2\}$	F_4
2	1	$\{1, 2\}$	F_4	$\{2, 3\}$
3	2	F_4	$\{2, 3\}$	$\{1, 2, 3\}$

and

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	F_4	2
3	0	3	2	F_4

.

Then $(F_4, +, \cdot)$ is a commutative additive-multiplicative hyperring with multiplicative unit 1.

We close this section with the following definition

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

(i) for every $a, b \in A$ implies $a - b \subseteq A$,

(ii) for every $a \in A$, $r \in R$ implies $r \cdot a \subseteq A$ ($a \cdot r \subseteq A$).

2.1. Hypervector spaces over hyperfields

We will give some properties related to the hypervector space which will allow us to characterize linear codes over a Krasner hyperfield.

From now on, and for the rest of this paper, by F we mean a Krasner hyperfield.

Definition. Let F be a Krasner hyperfield. A commutative hypergroup $(V,+)$ together with a map $\cdot : F \times V \longrightarrow V$, is called a *hypervector space* over F if for all $a,b \in F$ and $x,y \in V$, the following conditions hold:

(i) $a \cdot (x+y) = a \cdot x + a \cdot y$ (right distributive law),

(ii) $(a+b) \cdot x = a \cdot x + b \cdot x$ (left distributive law),

(iii) $a \cdot (b \cdot x) = (ab) \cdot x$ (associative law),

(iv) $a \cdot (-x) = (-a) \cdot x = -(a \cdot x)$,

(v) $x = 1 \cdot x$.

Let us give an example next.

Example 3. If F is a Krasner hyperring, then for $n \in \mathbb{N}$, F^n is a hypervector space over F where the composition of elements is as follows:
$x + y = \{z \in F^n; z_i \in x_i + y_i, i = 1 \dots n\}$ and $a \cdot x = (a \cdot x_1, a \cdot x_2, \dots, a \cdot x_n)$ for any $x, y \in F^n$ and $a \in F$.

Definition. Let $(V,+,\cdot,1)$ be a hypervector space over F. A subset $A \subseteq V$ is called a *subhypervector space* of V if:

(i) $A \neq 0$,

(ii) for all $x,y \in A$, then $x - y \subseteq A$,

(iii) for all $a \in F$, for all $x \in A$, then $a \cdot x \in A$.

Definition. A subset S of a hypervector space V over F, is called *linearly independent* if for every $x_1, x_2, \dots, x_n$ in S and for every $a_1, a_2, \dots, a_n$ in F, such that $(n \in \mathbb{N} \setminus \{0,1\})$ $0 \in a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$ implies that $a_1 = a_2 = \cdots = a_n = 0$. A subset S of V is called *linearly dependent* if it is not linearly independent.

If S is a nonempty subset of V, the set $\langle S \rangle$ define by $\langle S \rangle = \bigcup \{\sum_{i=1}^{n} a_i \cdot x_i |\ x_i \in S, a_i \in F, n \in \mathbb{N} \setminus \{0,1\}\} \cup l(S)$ where $l(S) = \{a \cdot x |\ a \in F, x \in S\}$, is the smallest subhypervector space of V containing S.

Definition. Let V be a hypervector space over F. A vector $x \in V$ is said to be a *linear combination* of the vectors $x_1, x_2, \dots, x_n \in V$ if there exist $a_1, a_2, \dots, a_n \in F$ such that $x \in a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$.

Definition. Let V be a hypervector space over F and S be a subset of V. S is said to be a *basis* for V if,

(i) S is linearly independent,

(ii) every element of V can be expressed as a finite linear combination of elements from S.

As in the case of classical vector spaces, the dimension of a hypervector space is the number of elements in a basis. It is not hard to see that this number is independent of the chosen basis.

Example 4. Let $\mathbb{F}_2$ be the finite field with two elements. Let the set $B = \{101, 110\}$ be a basis of a vector subspace of $\mathbb{F}_2^3$ and for a subhypervector space of F_2^3. On the space $\mathbb{F}_2^3$, the subspace generated by B is the dimension 2 and it have 4 elements: $000, 101, 110, 011$. On the hypervector space F_2^3, the subhypervector space generated by B is the dimension 2 and it have 5 elements: $000, 101, 110, 011, 111$.

2.2. Polynomial hyperring

We recall the definition of a polynomial over the Krasner hyperfield F. Assume that for all $a, b \in F$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$. We denote by $F[x]$ the set of all polynomials in the variable x over F. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ be any two elements of $F[x]$. Let us define the set $\mathcal{P}^*(F)[x] = \{\sum_{k=0}^{n} A_k x^k$; where $A_k \in \mathcal{P}^*(F)$, $n \in \mathbb{N}\}$, the hypersum and hypermultiplication of $f(x)$ and $g(x)$ are defined as follows:

- $+ : F[x] \times F[x] \longrightarrow \mathcal{P}^*(F)[x]$
  $(f(x), g(x)) \longmapsto (f+g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_M + b_M)x^M$, where $M = \max\{n, m\}$.
- $\cdot : F[x] \times F[x] \longrightarrow \mathcal{P}^*(F)[x]$
  $(f(x), g(x)) \longmapsto (f \cdot g)(x) = \sum_{k=0}^{m+n} (\sum_{l+j=k} a_l \cdot b_j) x^k$, if $\deg(f) \geq 1$ and $\deg(g) \geq 1$.

If $\deg(f) < 1$ or $\deg(g) < 1$, then the hypermultiplication is reduced to $\cdot : F[x] \times F[x] \longrightarrow F[x]$

$$(f(x), g(x) \longmapsto (f \cdot g)(x) = \sum_{k=0}^{m+n} \left(\sum_{l+j=k} a_l \cdot b_j \right) x^k.$$

We recall the crucial result from [7]:

Theorem 5 [7]**.** *The algebraic structure $(F[x], +, \cdot)$ is an additive-multiplication hyperring.*

3. Linear codes and cyclic codes over finite hyperfields

In this section we shall study the concept of linear codes and cyclic codes over the finite Krasner hyperfield F_2 from Example 1. We first recall some basics from code theory. Let A be an alphabet. The *Hamming distance* $d_H(x, y)$ between two vectors $x, y \in A^n$ is defined to be the number of coordinates in which x differs from y. For a classical code $\mathcal{C} \subseteq A^n$ containing at least two words, the minimum distance of a code $\mathcal{C}$, denoted by $d(\mathcal{C})$, is $d(\mathcal{C}) = \min\{d_H(x, y) | x, y \in \mathcal{C}$ and $x \neq y\}$.

If A^n is a vector space, then $\mathcal{C} \subseteq A^n$ is a linear code if $\mathcal{C}$ is a sub-vector space. In this latter case, we compute for a code word $x \in \mathcal{C}$, $w_H(x)$ the number of nonzero coordinates in x also called *Hamming weight* of x. We denote by k =dim($\mathcal{C}$) the dimension of $\mathcal{C}$ and the code $\mathcal{C}$ is called an (n, k, d)-*code* which can be represented by his generator matrix (see [6] for more details).

For $n \in \mathbb{N} \setminus \{0, 1\}$ it is clear that, F_2^n is a hypervector space over F_2.

Definition. A *linear code* C of length n over F_2 is a subhypervector space over F_2 of the hypervector space F_2^n.

Here is an example:

Example 6.

(1) For $n = 3$, F_2^3 is a linear code of length 3 over F_2.

(2) $C = \{0000000, 1011111, 0111010, 1100101, 1101101, 1110111, 1001101, 0010010, 0101000, 1111111\}$ is a linear code of length 7 over F_2.

Definition. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two vectors in F_2^n ($n \geq 2$). The *inner product* of the vectors x and y in F_2^n is defined by $x \cdot y^t = \sum_{i=1}^{n} x_i \cdot y_i$ (where y^t mean the transpose of y).

Definition. Let C be a linear code of length n ($n \geq 2$) over F_2. The *dual* of C is defined by $C^{\perp} := \{y \in F_2^n | \ 0 \in x \cdot y^t, \ \forall x \in C\}$. The code C is *self-dual* if $C = C^{\perp}$.

Remark 7. In the previous Definition 3 if $n = 1$, then $C^{\perp} = \{y \in F_2 | \ 0 = x \cdot y^t, \forall x \in C\}$.

Here is an example of a dual code.

Example 8. Let $C = \{000, 101, 011, 110, 111\}$ be a linear code of length 3 over F_2. It's easy to check that the dual of C is defined by $C^{\perp} = \{000, 111\}$.

Definition. A cyclic code C of length n over F_2 is a linear code which is invariant by the shift map s, define by $s((a_0, \ldots, a_{n-1})) = (a_{n-1}, a_0, \ldots, a_{n-2})$, i.e., for all $(a_0, \ldots, a_{n-1}) \in C$, we have $s((a_0, \ldots, a_{n-1})) \in C$.

Example 9. $C = \{000, 101, 110, 011, 111\}$ is a cyclic code of length 3 over F_2. In fact $s(000) = 000$, $s(101) = 110$, $s(110) = 011$, $s(011) = 101$, $s(111) = 111$.

The polynomial $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ of degree at most $n-1$ over F_2 may be considered as the sequence $a = (a_0, a_1, a_2, \ldots, a_{n-1})$ of length n in F_2^n. In fact, there is a correspondence between F_2^n and the residue class hyperring $\frac{F_2[x]}{(x^n-1)}$ (see [6] for more details).

$$\begin{aligned} \phi : F_2^n &\longrightarrow \tfrac{F_2[x]}{(x^n-1)} \\ c = (c_0, c_1, c_2, \ldots, c_{n-1}) &\longmapsto c_0 + c_1x^1 + c_2x^2 + \cdots + c_{n-1}x^{n-1}. \end{aligned}$$

Using Theorem 3.7 in [5], the multiplication of x by any element of $\frac{F_2[x]}{(x^n-1)}$ is equivalent to applying the shift map s to the corresponding element of F_2^n, so we can use the polynomial to define a cyclic code (see Proposition 22).

Metric distance

We are now going to define a distance relation on linear codes over the finite hyperfield F_2, which will allow us to detect if there is an error in a received word.

Definition. Let $n \in \mathbb{N}^*$. The mapping

$$\begin{aligned} d_H : F_2^n \times F_2^n &\longrightarrow \mathbb{N} \\ (x, y) &\longmapsto d_H(x, y) = card\{i \in \mathbb{N} | x_i \neq y_i\} \end{aligned}$$

is a distance on F_2^n, called the *Hamming distance.*

Remark 10. If $x \in F_2^n$, then we write $x = (\{x_1\}, \ldots, \{x_n\})$ that now belongs to the cartesian product $(\mathcal{P}^*(F_2))^n$. Hence we can compute $w_H(x) = card\{i \in \mathbb{N}|\ 0 \notin x_i\} = d_H(0, x)$.

The following map denoted by w_H on the cartesian product $(\mathcal{P}^*(F_2))^n$:

$$\begin{aligned} w_H : (\mathcal{P}^*(F_2))^n &\longrightarrow \mathbb{N} \\ a = (a_1, \ldots, a_n) &\longmapsto card\{i \in \mathbb{N}|\ 0 \notin a_i\}. \end{aligned}$$

is the *Hamming weight* on the hypervector space F_2^n.

We can easily verify that for all $x, y \in F_2^n$, we have $d_H(x, y) = w_H(x - y)$ (as in the classical case). If C is a linear code over F_2, we call the integer number $d = \min\{w_H(x) | x \in C\}$ the *minimal distance* of the code C.

To obtain a linear code of length n over F_2 as a subhypervector space of F_2^n, it is sufficient to have a basis of the linear code. This basis can often be represented by a $k \times n$ matrix over F_2 (where k is the dimension of the code). Let $\mathcal{M}(F_2)$ be the set of all matrices over F_2 with.

Definition. Let C be a linear code over F_2. Any matrix from $\mathcal{M}(F_2)$ where the rows form a basis of the code C is called a *generator matrix* of $\mathcal{C}$.

Definition. Let $x = (x_1, \ldots, x_n)$ be a vector of F_2^n and $y = (y_1, y_2, \ldots, y_n)$ be an element of the cartesian product $(\mathcal{P}^*(F_2))^n$. We say that x *belongs* to y if $x_i \in y_i$ for any $i = 1 \ldots n$.

Remark 11. If G is a generator matrix of the linear code C of length n and dimension k, the product $a \cdot G$ (where $a \in F_2^k$) is the vector which belongs to $(\mathcal{P}^*(F_2))^n$ and is defined as:

$$(a_1, \ldots, a_k) \cdot \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} = \left(\sum_{i=1}^{k} a_i \cdot g_{i1}, \ldots, \sum_{i=1}^{k} a_i \cdot g_{in} \right).$$

Proposition 12. *Let $G \in \mathcal{M}_{k \times n}(F_2)$ be a generator matrix of the linear code C over F_2, then $C = \{c \in a \cdot G |\ a \in F_2^k\}$.*

Proof. Since C is a $[n, k]$-linear code over F_2, the rows of $G \in \mathcal{M}_{k \times n}(F_2)$ form a basis of C. Thus C consists of all linear combinations of the rows of G, therefore $C = \{c \in a \cdot G |\ a \in F_2^k\}$. ∎

Since the dual code $C^\perp$ of C over F_2 is also linear, $C^\perp$ has a generator matrix as well.

Definition. Given a linear $[n, k]$-code over F_2, we call a generator matrix for $C^\perp$ a *parity check matrix* for C.

Here and until the end of this paper, we will denoted by G the generator matrix and by H the parity check matrix of the linear code C over F_2.

Example 13. Let $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ be a generator matrix of the linear code C from Example 8. Then the parity check matrix of C is $H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

Theorem 14. *Let C be a linear code of length n ($n \geq 2$) and dimension k over F_2. Then $H \in \mathcal{M}_{(n-k) \times n}(F_2)$ and $0 \in G \cdot H^t$ (where H^t mean the transpose of H).*

Proof. Assume that $G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$ and $H = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$, where $g_i \in F_2^n$ and $h_j \in F_2^n$ (for $i = 1 \cdots k$ and $j = 1 \cdots n - k$).

Then $G \cdot H^t = \begin{pmatrix} g_1 \cdot h_1^t & g_1 \cdot h_2^t & \cdots & g_1 \cdot h_{n-k}^t \\ g_2 \cdot h_1^t & g_2 \cdot h_2^t & \cdots & g_2 \cdot h_{n-k}^t \\ \vdots & \vdots & \vdots & \vdots \\ g_k \cdot h_1^t & g_k \cdot h_2^t & \cdots & g_k \cdot h_{n-k}^t \end{pmatrix}$. Thus, by the definition of $C^{\perp}$, $0 \in G \cdot H^t$. ■

We now give some examples of hyperlinear codes over F_2.

Example 15. Let F_2^3 be a hypervector space over F_2 and C be a subhypervector space of F_2^3, with dimensional $k = 2$. Then C is a linear code of length $n = 3$ and dimension $k = 2$ over F_2.

(1) Let $G_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ be a generator matrix of the linear code $C = \{000, 010, 101, 111\}$ over F_2. G_1 is also a generator matrix of a linear code $C' = \{000, 010, 101, 111\}$ of length 3 and dimension 2 over the finite field $\mathbb{F}_2$. These two codes C and C' have the same parameters and $card(C) = card(C')$.

(2) Let $G_2 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ be another generator matrix of the linear code C over F_2. G_2 is also a generator matrix of a linear code C'' of length 3 and dimension 2 over the finite field $\mathbb{F}_2$. Here we have $C = \{000, 110, 101, 011, 111\}$, $C'' = \{000, 110, 101, 011\}$ and these two codes have the same parameters but $card(C) > card(C'')$.

(3) Let $G_{\min} = \begin{pmatrix} Id_k & Id_{n-k} \\ \cdot & 0 \end{pmatrix}$ where Id_k is the $k \times k$-identity matrix). $G_{\min}$ is a generator matrix of a linear code $C_{\min}$ of length n and dimension k over F_2 (with $n - k \leq k$). The linear code $C_{\min}$ over F_2 generated by $G_{\min}$ has the minimal number of code words, $card(C_{\min}) = 2^k$.

(4) Let $G_{\max} = \begin{pmatrix} Id_k & \mathbf{1}_{n-k} \end{pmatrix}$ (where Id_k is the identity matrix and $\mathbf{1}_{n-k}$ is the matrix such that every element is equal to 1). $G_{\max}$ is a generator matrix of a hyperlinear code $C_{\max}$ of length n and dimension $k > 2$ over F_2. The linear code $C_{\max}$ over F_2 generated by $G_{\max}$ has the maximal number of code words, $card(C_{\max}) = 2^{n-k} + \sum_{i=2}^{k-1} \begin{pmatrix} k \\ i \end{pmatrix} + k + 1$

Here we have this very important remark.

Remark 16. There exists a finite hyperfield such that for any other finite field of the same cardinality, the linear codes over the hyperfield are always better than the classical linear code over the finite field (i.e., they have more code words).

In classical coding theory, one of the most important problems mentioned in [9] is to find a code with a large number of words knowing the parameters (length, dimension and minimal distance). So the hyperstructure theory may help to increase the number of code words.

Theorem 17. *Let C be a linear code of length n and dimension k over F_2. If M is the cardinality of C, then*

$$2^k \leq M \leq \begin{cases} 2^{n-k} + k + 1, & \text{if } k \leq 2; \\ 2^{n-k} + \sum_{i=2}^{k-1} \begin{pmatrix} k \\ i \end{pmatrix} + k + 1, & \text{if } k > 2. \end{cases}$$

Proof. Since a generator matrix contains a basis of the hyperlinear code C as rows, it is sufficient to give a way how to construct a generator matrix for the code where the cardinality is maximal. If $k \leq 2$, this is trivial. If $k > 2$, then we choose a generator matrix such that:

- in the first k columns no 1 is repeated (this forces every code word to belong to only one linear combination),
- no sum of any set of elements in any column is equal to zero,
- all the elements of the $n - k$ last columns are equal to 1. (We need each combination to have a maximal number of code words.)

Therefore, the maximal number of code words is $2^{n-k} + \sum_{i=2}^{k-1} \begin{pmatrix} k \\ i \end{pmatrix} + k + 1$. ■

Corollary 18. *Let C be a linear code of length n and dimension k over F_2, and C' be a linear code of length n and dimension k over the field $\mathbb{F}_2$. Then $d \leq d' \leq n - k + 1$ where d is the minimal distance of C and d' is the minimal distance of C'.*

Remark 19. The previous Corollary 18 shows that a linear code over F_2 satisfies the Singleton bound.

Proposition 20. *Let C be a linear code of length n and dimension k over F_2, then $c \in C$ if and only if $0 \in c \cdot H^t$.*

Proof. $\Rightarrow$) Assume that $c \in C$, and let $H = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$ be the parity check matrix of the code C. Then $c \cdot H^t = (c \cdot h_1^t, c \cdot h_2^t, \ldots, c \cdot h_{n-k}^t)$, thus by definition of $C^\perp$, $0 \in c \cdot H^t$.

$\Leftarrow$) Assume that $0 \in c \cdot H^t$, then c belongs either to G, (the generator matrix of the code C) or to a linear combination of rows of G. Therefore $c \in C$. ■

Proposition 21. *Let C be a linear code of length n over F_2, then the double dual of C is equal to C, i.e., $(C^{\perp})^{\perp} = C$.*

Proof. Using Proposition 4.3 in [5], $(C^{\perp})^{\perp}$ is a linear code of length n over F_2, so it is sufficient to show that $C = (C^{\perp})^{\perp}$. By definition we have $(C^{\perp})^{\perp} = \{z \in F_2 |\ 0 \in y \cdot z^t;$ for all $y \in C^{\perp}\}$, so it is straightforward that $C \subseteq (C^{\perp})^{\perp}$. Now, let $z \in (C^{\perp})^{\perp}$. Let $H = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$ be the parity check matrix of the code C, then

$$\begin{aligned} z \cdot H^t &= \left(\sum_{i=1}^{n} z_i \cdot h_{1,i}, \ldots, \sum_{i=1}^{n} z_i \cdot h_{n-k,i} \right) \\ &= \left(\sum_{i=1}^{n} h_{1,i} \cdot z_i, \ldots, \sum_{i=1}^{n} h_{n-k,i} \cdot z_i \right) = \left(\sum_{i=1}^{n} h_{1,i} \cdot z^t, \ldots, \sum_{i=1}^{n} h_{n-k,i} \cdot z^t \right). \end{aligned}$$

Thus $0 \in z \cdot H^t$ by definition of $(C^{\perp})^{\perp}$, therefore $z \in C$. We conclude the proof by using Proposition 20. ∎

Since a cyclic code in F_2^n has only one generating polynomial [5], it is clear that this polynomial divides the polynomial $x^n - 1$.

Proposition 22. *If $g(x) = a_0 + a_1 x + \cdots + a_k x^k \in F_2[x]$ is the generating polynomial for a cyclic code C over F_2, then*

$$G = \begin{pmatrix} a_0 & \cdots & a_k & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_k & 0 & \cdots & 0 \\ 0 & 0 & a_0 & \cdots & a_k & \cdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & a_0 & \cdots & a_k \end{pmatrix}$$

is the generator matrix of the cyclic code C.

Proof. Let $g_1 = (a_0, \ldots, a_k, 0, \ldots, 0) \in F_2^n$, then G can also be write as

$$G = \begin{pmatrix} g_1 \\ s(g_1) = g_2 \\ s^2(g_1) = g_3 \\ \vdots \\ s^{k-1}(g_1) = g_k \end{pmatrix}$$

(where s is the shift function and $s^k = s \circ s \circ \cdots \circ s$, k-successive shifts).

Since the polynomial g generates C, we have $C = \langle g(x)\rangle$. Let $c \in C$, then $(c_i)_{i=1\cdots n} = c \in g(x)\cdot p(x)$ (where $b_0 + b_1x + \cdots + b_{n-1}x^{n-1} = p(x) \in \frac{F_2[x]}{(x^n-1)}$) implies that $c_i \in \sum_{l+j} a_l \cdot b_j$ if $i \leq k$ and $c_i = 0$ else if $(i > k)$.

Focusing on $g(x)$ and $p(x)$, the element c belongs to the sum $b_0 \cdot g(x) + b_1x \cdot g(x) + \cdots + b_{n-1} \cdot x^{n-1} \cdot g(x)$ because this sum can also be written as $e_1 \cdot g_1 + e_2 \cdot g_2 + \cdots + e_k \cdot g_k$ $(e = (e_1, \ldots, e_k) \in F_2^n)$, and C is a cyclic code generated by $g(x)$. ■

Proposition 23. *With the same notation as in Proposition* 22, *let* $h(x) \in \frac{F_2[x]}{(x^n-1)}$ *be a polynomial such that* $x^n - 1 \in h(x) \cdot g(x)$, *then*

(1) *The linear code C over F_2 can be represented by* $C = \{p(x) \in \frac{F_2[x]}{(x^n-1)} \mid 0 \in p(x) \cdot h(x)\}$.
(2) $h(x)$ *is the generating polynomial for the linear code* $C^{\perp}$.

Proof. Let C be a cyclic code of length n over F_2, generated by the polynomial $g(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k$ $(a_k = 1)$. Since $x^n - 1 \in h(x)\cdot g(x)$, then $deg(h(x)) = n-k$, the coefficient of the monomial of degree $n-k$ is 1 and if we assume that $h(x) = b_0 + b_1x + \cdots + b_{n-k-1}x^{n-k-1} + b_{n-k}x^{n-k} \in \frac{F_2[x]}{(x^n-1)}$ (with $b_{n-k} = 1$), we have $h(x)\cdot g(x) = \sum_{l=1}^{n}(\sum_{i+j=l} a_i \cdot b_j)x^l$, hence $0 \in \sum_{i+j=l} a_i \cdot b_j$.

Let $G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$ be the generator matrix of the code C, with a k-successive shift of $g_1 = (a_0, \ldots, a_k, 0, \ldots, 0) \in F_2^n$, let $H = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$ be $n-k$-successive shifts of $h_1 = (b_0, \ldots, b_{n-k}, 0, \ldots, 0) \in F_2^n$. Since $0 \in \sum_{i+j=l} a_i \cdot b_j$, then $0 \in G \cdot H^t$. Therefore by Theorem 14, H is the parity check matrix of the code C generated by $h(x)$. Therefore, $h(x)$ is the generating polynomial of the code $C^{\perp}$ and we deduce H. ■

4. CONCLUSION

In this work, we have defined concepts for linear codes and cyclic codes over the hyperfield F_2, such as the generator matrix, the parity check matrix and the Hamming distance. We have also characterized these linear codes and cyclic codes. We have that over a finite field and a finite Krasner hyperfield with the same cardinality, it is possible to have a code over a finite field and a code over a finite Krasner hyperfield with the same parameters (length, dimension, minimal distance) such that, the linear code over the hyperfield has more code words than the linear code over the field.

This hints at the fact that hyperstructure theory produces codes that have advantages over classical codes and thus we obtain a method that we might use in future work to solve some problems in classical coding theory.

Acknowledgement

The authors wish to thank the anonymous reviewers for their valuable suggestions.

References

[1] R. Ameri and O.R. Dehghan, *On dimension of hypervector spaces*, European J. Pure Appl. Math. **1** (2008) 32–50.

[2] P. Corsini and V. Leoreanu, Applications of Hyperstructure Theory (Kluwer Academical Publications, Dordrecht, 2003). doi:10.1007/978-1-4757-3714-1

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

[4] B. Davvaz and V. Leoreanu-Fotea, Hyperring Theory and applications (International Academic Press, USA, 2007).

[5] B. Davvaz and T. Musavi, *Codes over hyperrings*, Matematički Vesnik **68** (2016) 26–38.

[6] F. Galand, Construction de codes $\mathbb{Z}_{p^k}$-linéaires de bonne distance minimale et schémas de dissimulation fondés sur les codes de recouvrement (Ph.D Thesis, Université de Caen, 2004).

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

[8] M. Krasner, *A class of hyperrings and hyperfields*, Internat. J. Math. and Math. Sci. **6** (1983) 307–312. doi:10.1155/S0161171283000265

[9] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

[10] F. Marty, *Sur une generalization de la notion de groupe*, 8^{iem} Congres Math. Scandinaves, Stockholm (1934) 45–94.

[11] S. Roy and T.K. Samanta, *A note on hypervector spaces*, arXiv:1002.3816v3 [math.GM].

Received 8 September 2016
Revised 15 June 2017
Accepted 23 June 2017