IMHOTEP

AFRICAN JOURNAL OF PURE AND APPLIED MATHEMATICS

Imhotep Mathematical Proceedings
Volume 4, Numéro 1, (2017),
pp. 1 - 8.

Some Applications of Hyperstructures in Coding Theory

S. Atamewoue Tsafack
Department of Mathematics, Faculty of Sciences, University of Yaoundé I, Cameroon. P.O. Box 812 Yaounde, Cameroon.
surdive@yahoo.fr

Selestin Ndjeya
Department of Mathematics, Higher Teacher Training College, University of Yaoundé I, Cameroon. P.O. Box 47 Yaounde.
ndjeyas@yahoo.fr

Celestin Lele
Department of Mathematics and Computer Science, University of Dschang, Cameroon, B.P. 67 Dschang, Cameroon.
celestinlele@yahoo.com

Abstract

The notion of hyperrings (hyperfields) is a generalization of the notion of rings (fields) where the additive composition " $+$ " and/or the multiplicative composition " $\cdot$ " are changed to a hyperoperation. Similarly, there is the notion of hypervector space and hypermodule where internal and/or external compositions on the classical form have been generalized. 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.

Proceedings of the 6^{th} annual workshop on CRyptography, Algebra and Geometry (CRAG-6), 15- 17 June 2016, University of Bamenda, Bamenda, Cameroon.

http://imhotep-journal.org/index.php/imhotep/
Imhotep Mathematical Proceedings

IMHOTEP - Math. Proc. **4** (2017), 1–8
1608-9324/010001-0, DOI 13.1007/s00009-003-0000

IMHOTEP Mathematical Proceedings

Some Applications of Hyperstructures in Coding Theory

S. Atamewoue Tsafack, Selestin Ndjeya and Celestin Lele

Abstract. The notion of hyperrings (hyperfields) is a generalization of the notion of rings (fields) where the additive composition " + " and/or the multiplicative composition " $\cdot$ " are changed to a hyperoperation. Similarly, there is the notion of hypervector space and hypermodule where internal and/or external compositions on the classical form have been generalized. 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.

Mathematics Subject Classification (2010). 20N20 (primary), 54B20, 94B05 (secondary).

Keywords. Hypervector space, Hyperring, Hyperfield, Linear code.

I. Introduction

In [9], 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 [6]. In [10], 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 discussed 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 [8], Sanjay Roy and Samanta, introduced the notion of hypervector spaces over hyperfields, on which external and internal compositions are both hyperoperations.
Recently, Davvaz and Musavi [3] defined a hypervector space over a Krasner hyperfield and they 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 crucial properties of them. 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.

Communication presentée au 6ème atelier annuel sur la CRyptographie, Algèbre et Géométrie (CRAG-6), 15 - 17 Juin 2016, Université de Bamenda, Bamenda, Cameroun / Paper presented at the 6th annual workshop on CRyptography, Algebra and Geometry (CRAG-6), 15- 17 June 2016, University of Bamenda, Bamenda, Cameroon.

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.

II. Preliminaries

In this section, we recall the preliminary definitions and results that are required in the sequel (for references see [1, 2, 6]).
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 for all elements 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 $a \in H$ 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 II.1. *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) $z \in x + y$ implies $y \in -x + z$ and $x \in -y + z$.

Definition II.2. *A Krasner hyperring is an algebraic structure $(R, +, \cdot)$ (where only $+$ is a hyperoperation) which satisfies the followings 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 classical 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 II.3. *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 "·"*

+	*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 $A + B = \{x|\ x \in a+b \text{ for some } a \in A, b \in B\}$ 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 II.4. *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 "·" 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 close this section with the following definition

Definition II.5. *A non-empty subset* A *of an additive-multiplicative hyperring* R *is a left (right) hyperideal if,*
(i) $a, b \in A$ *implies* $a - b \subseteq A$,
(ii) $a \in A$, $r \in R$ *implies* $r \cdot a \subseteq A$ $(a \cdot r \subseteq A)$.

II.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 II.6. *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.

Example II.7. *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 are as follows:*

$x + y = \{z \in F^n; z_i \in x_i + y_i, i = 1...n\}$ *and* $a \cdot x = (a \cdot x_1, a \cdot x_2, ..., a \cdot x_n)$ *for any* $x, y \in F^n$ *and* $a \in F$.

Definition II.8. *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 II.9. *A subset* S *of a hypervector space over* F*,* V *is called linearly independent if for every vectors* $x_1, x_2, ..., x_n$ *in* S *and for every coefficients* $a_1, a_2, ..., a_n$ *in* F*,* $(n \in \mathbb{N} \setminus \{0, 1\})$ $0 \in a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$ *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 II.10. *Let* V *be a hypervector space over* F*. A vector* $x \in V$ *is said to be a linear combination of the vectors* $x_1, x_2, ..., x_n \in V$ *if there exist* $a_1, a_2, ..., a_n \in F$ *such that* $x \in a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$.

Definition II.11. *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.

II.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 $M = max\{n, m\}$.

- $\cdot : F[x] \times F[x] \longrightarrow \mathcal{P}^*(F)[x]$
  $(f(x), g(x)) \longmapsto (f \cdot g)(x) = \sum_{k=0}^{m+n} (\sum_{l+j=k} a_l \cdot b_j)x^k, if deg(f) \geq 1 \text{ and } deg(g) \geq 1$

If $deg(f) < 1$ or $deg(g) < 1$, then the hypermultiplication is reduced to $\cdot : F[x] \times F[x] \longrightarrow F[x]$ $(f(x), g(x) \longmapsto (f \cdot g)(x) = \sum_{k=0}^{m+n} (\sum_{l+j=k} a_l \cdot b_j) x^k$.

We recall the crucial result from [7]:

Theorem II.12. [7] *The algebraic structure* $(F[x], +, \cdot)$ *is an additive-multiplication hyperring.*

III. 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 II.3. 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 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 [4] 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 III.1. *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 III.2. . • *For $n = 3$, F_2^3 is a linear code of length 3 over F_2.*
• $C = \{0000000, 1011111, 0111010, 1100101, 1101101, 1110111, 1001101, 0010010, 0101000, 1111111\}$ *is a linear code of length 7 over F_2.*

Definition III.3. *Let $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ 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 III.4. *Let C be a linear code of length n $(n \geq 2)$ over F_2. The dual of C is defined by $C^\perp = \{y \in F_2^n |\ 0 \in x \cdot y^t, \forall x \in C\}$ and denoted by $C^\perp$.*
The code C is self-dual if $C = C^\perp$.

Remark III.5. *In the previous Definition* III.4 *if $n = 1$, then $C^\perp = \{y \in F_2 |\ 0 = x \cdot y^t, \forall x \in C\}$.*

Definition III.6. *A cyclic code C of length n over F_2 is a linear code which is invariant by the shift map s, define by $s((a_0, ..., a_{n-1})) = (a_{n-1}, a_0, ..., a_{n-2})$. i.e. for all $(a_0, ..., a_{n-1}) \in C$, we have $s((a_0, ..., a_{n-1})) \in C$.*

Example III.7. $C = \{000, 101, 110, 011, 111\}$ *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 $a = (a_0, a_1, a_2, ..., a_{n-1})$ 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 [3] for more details).

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

Using Theorem 3.7 in [3], 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.

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 III.8. *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.

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

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

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.

Remark III.9. *If $x \in F_2^n$, then we write $x = (\{x_1\},...,\{x_n\})$ that now belongs to the cartesian product $(\mathcal{P}^*(F_2))^n$. Hence we can compute $w_H(x) = card\{i \in \mathbb{N} | \ 0 \notin x_i\} = d_H(0,x)$.*

To obtain the 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 $(l \times n)$-matrices over F_2 with $l \leq n$.

Definition III.10. *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 III.11. *Let $x = (x_1,...,x_n)$ be a vector of F_2^n and $y = (y_1,y_2,...,y_n)$ 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 $i = 1...n$.*

Remark III.12. *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:*

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

Proposition III.13. *Let $G \in \mathcal{M}_{k \times n}(F_2)$ be a generator matrix of the linear code C over F_2, then $C = \{c \in a \cdot G | \ a \in F_2^k\}$.*

Definition III.14. *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.

Theorem III.15. *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).*

Remark III.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 in the sense that they have more code words.*

In classical coding theory, one of the most important problems mentioned in [5] *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 III.17. *Let C be a linear code of length n and dimension k over F_2. If M is the cardinality of C, then* $2^k \leq M \leq \begin{cases} 2^{n-k} + k + 1, & \text{if } k \leq 2; \\ 2^{n-k} + \sum_{i=2}^{k-1} \begin{pmatrix} k \\ i \end{pmatrix} + k + 1, & \text{if } k > 2. \end{cases}$

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

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

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

Since a cyclic code in F_2^n has only one generating polynomial [3], it is clear that this polynomial divides the polynomial $x^n - 1$.

Proposition III.22. *If $g(x) = a_0 + a_1x + \cdots + a_kx^k \in F_2[x]$, 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.*

Proposition III.23. *With the same notation as in Proposition* III.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 $C^{\perp}$.

IV. Conclusion

In this work, we have defined many 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 noticed 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.
So the hyperstructure theory produces codes that have advantages over classical codes and thus we obtain a method that we might use in future works to solve some problems in classical coding theory.

References

[1] R. Ameri and O.R. Dehghan, On Dimension of Hypervector Spaces, *European Journal of Pure and Applied Mathematics* **1**, $n^0 2$, 32-50 (2008).

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

[3] B. Davvaz and T. Musavi, Codes Over Hyperrings, *Matematički Vesnik* **68** $n^0 1$, 26-38 (2016).

[4] 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).

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

[6] M. Krasner, A Class of Hyperrings and Hyperfields *Internat. J. Math. and Math. Sci.* **6** $n^0 2$, 307-312 (1983).

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

[8] S. Roy and T.K. Samanta, *A Note on Hypervector Spaces*, Discussiones Mathematicae - General Algebra and Applications, **3** (1) (2011), 75 – 99.

[9] F. Marty, Sur une generalization de la notion de groupe, 8^{iem} *congress Math. Scandinaves, Stockholm*, 4549 (1934).

[10] B. Davvaz and A. Koushky, On Hyperring of Polynomials, *Ital. J. Pure Appl. Math.*, $n^0 15$, 205214 (2004).

S. Atamewoue Tsafack
e-mail: `surdive@yahoo.fr`
Department of Mathematics, Faculty of Sciences, University of Yaoundé I, Cameroon. P.O. Box 812 Yaounde, Cameroon.

Selestin Ndjeya
e-mail: `ndjeyas@yahoo.fr`
Department of Mathematics, Higher Teacher Training College, University of Yaoundé I, Cameroon. P.O. Box 47 Yaounde, Cameroon.

Celestin Lele
e-mail: `celestinlele@yahoo.com`
Department of Mathematics and Computer Science, University of Dschang, Cameroon, B.P. 67 Dschang.