Chapter

Non Classical Structures and Linear Codes

Surdive Atamewoue Tsafack

Abstract

This chapter present some new perspectives in the field of coding theory. In fact notions of fuzzy sets and hyperstructures which are consider here as non classical structures are use in the construction of linear codes as it is doing for fields and rings. We study the properties of these classes of codes using well known notions like the orthogonal of a code, generating matrix, parity check matrix and polynomials. In some cases particularly for linear codes construct on a Krasner hyperfield we compare them with those construct on finite field called here classical structures, and we obtain that linear codes construct on a Krasner hyperfield have more codes words with the same parameters.

Keywords: Linear codes, Fuzzy set, Krasner hyperstructures, Fuzzy logic, Algebraic hyperstructures

1. Introduction

In mathematics, non classical structures as fuzzy sets and algebraic hyperstructures approach better many well known real life situation, and represent natural extension of classical algebraic structures.

Regarding fuzzy sets theory (fuzzy logic), this was introduced in the middle of 1960 by Lotfi Zadeh [1]. This concept is considered today as one of the most important of the second half of twentieth century, this in view of its applications in technological sciences and the impressive quantities of paper and book related to it.

As for algebraic hyperstructures, they were introduced by a french mathematician F. Marty [2] in 1934. Since then, more than a thousand papers and several book have been written on this topic. A well known type of algebraic hyperstructures is due to Krasner [3], who used as a technical tool in a study of his on the approximation of valued fields. In the literature they are called Krasner hyperrings and Krasner hyperfields.

Transmission on coding theory always suppose to encode its information and decode the received information, this is what the classical coding theory introduced in 1948 by C. Shannon [4] deals with. It should ne noted that the handling information are certains. So how can we do if the informations are uncertain? Thus as a new perspective for the algebraic coding, we present below a connection between fuzzy sets, Krasner hyperstructures and linear codes, and we find out how they can bring more in classical coding theory.

2. Fuzzy linear codes over $\mathbb{Z}_{p^k}$

2.1 Preliminaries

The theory of fuzzy code as we present here were introduce by Shum and Chen De Gang [5], although they have authors such as Hall Diall and Von Kaenel [6, 7] who also worked on it. In this section, we shall formulate the preliminary definitions and results that are required for a good understanding of the sequel (we can see it in [8–10]).

Definition 2.1. Let X be a non-empty set, let I and J be two fuzzy subsets in X, then:

- $(I \cap J)(x) = min\{I(x), J(x)\}$, $(I \cup J)(x) = max\{I(x), J(x)\}$,
- $I = J$ if and only if $I(x) = J(x)$, $I \subseteq J$ if and only if $I(x) \leq J(x)$,
- $(I + J)(x) = max\{I(y) \wedge J(z) | x = y + z\}$, $(IJ)(x) = max\{I(y) \wedge J(z) | x = yz\}$.

These for all $x, y, z \in X$.

Let denoted by M the $\mathbb{Z}_{p^k}$-module $\mathbb{Z}_{p^k}^n$, where p is a prime integer and $n, k \in \mathbb{N} \backslash \{0\}$.

The following definitions on the fuzzy linear space derive from [11, 12].

Definition 2.2. We called a fuzzy submodule of M, a fuzzy subset $\mathcal{F}\sqcap$ of a $\mathbb{Z}_{p^k}$-module M such that for all $x, y \in M$ and $r \in \mathbb{Z}_{p^k}$, we have:

- $\mathcal{F}(x + y) \geq min\{\mathcal{F}\sqcap(x), \mathcal{F}\sqcap(y)\}$.
- $\mathcal{F}(rx) \geq \mathcal{F}\sqcap(x)$.

Definition 2.3. Let $\mathcal{F}\sqcap$ be a fuzzy subset of a nonempty set M. For $t \in [0, 1]$, we called the the upper t-level cut and lower t-level cut of $\mathcal{F}\sqcap$, the sets $\mathcal{F}\sqcap_t = \{x \in M | \mathcal{F}\sqcap(x) \geq t\}$ and $\overline{\mathcal{F}\sqcap_t} = \{x \in M | \mathcal{F}\sqcap(x) \leq t\}$ respectively.

Proposition 2.4. *$\mathcal{F}\sqcap$ is a fuzzy submodule of an $\mathbb{Z}_{p^k}$-module M if and only if for all $\alpha, \beta \in \mathbb{Z}_{p^k}$; $x, y \in M$, we have $\mathcal{F}\sqcap(\alpha x + \beta y) \geq min\{\mathcal{F}\sqcap(x), \mathcal{F}\sqcap(y)\}$.*

The following difinition recalled the notion on fuzzy ideal of a ring.

Definition 2.5. *We called a fuzzy ideal of $\mathbb{Z}_{p^k}$, a fuzzy subset I of a ring $\mathbb{Z}_{p^k}$ such that for each $x, y \in \mathbb{Z}_{p^k}$;*

- $I(x - y) \geq min\{I(x), I(y)\}$.
- $I(xy) \geq max\{I(x), I(y)\}$.

Definition 2.6. Let G be a group and R a ring. We denote by **RG** the set of all formal linear combinations of the form $\alpha = \sum_{g \in G} a_g g$ (where $a_g \in R$ and $a_g = 0$ almost everywhere, that is only a finite number of coefficients are different from zero in each of these sums).

Definition 2.7. Let **RG** a ring group which is the group algebra of $<x>$ on the ring $\mathbb{Z}_{p^k}$ (where x is an invertible element of $\mathbb{Z}_{p^k}$). A fuzzy subset I of **RG** is called a fuzzy ideal of **RG**, if for all $\alpha, \beta \in$ **RG**,

- $I(\alpha\beta) \geq max\{I(\alpha), I(\beta)\}$.

- $I(\alpha - \beta) \geq min\,\{I(\alpha), I(\beta)\}$.

When we use the transfer principle in [13], we easily get the next Proposition.

Proposition 2.8. *A is a fuzzy ideal of RG if and only if for all* $t \in [0,1]$, *if* $A_t \neq \emptyset$, *then* A_t *is an ideal of RG.*

The following is very important, the give the meaning of the linear code over the ring $\mathbb{Z}_{p^k}$.

Definition 2.9. A submodule of $\mathbb{Z}_{p^k}^n$, is called a linear code of length n over $\mathbb{Z}_{p^k}$. (with n a positive integer).

Contrary to the vector spaces, the module do not admit in general a basis. However it possesses a generating family and therefore a generating matrix, but the decomposition of the elements on this family is not necessarily unique.

Definition 2.10. We called generating matrix of a linear code over $\mathbb{Z}_{p^k}$ all matrix of $\mathcal{M}\left(\mathbb{Z}_{p^k}\right)$, where the lines are the minimal generating family of code.

The equivalence of two codes is define by the following definition.

Definition 2.11. Let C_{p^k} and C'_{p^k} two linear codes over $\mathbb{Z}_{p^k}$ of generating matrix G and G' respectively. The codes C_{p^k} and C'_{p^k} are equivalences if there exists a permutation matrix P, such that $G' = GP$.

To define a dual of a code which is helpful when we fine some properties of the codes, we need to know the inner product.

Definition 2.12. Let C_{p^k} be a linear code of length n over $\mathbb{Z}_{p^k}$, the dual of the code C_{p^k} that we note $C_{p^k}^{\perp}$ is the submodule of $\mathbb{Z}_{p^k}^n$ define by; $C_{p^k}^{\perp} = \{a|$ for all $b \in C_{p^k}, a.b = 0\}$. where "$\cdot$" is the natural inner product on the submodule $\mathbb{Z}_{p^k}^n$.

In a linear code C_{p^k} of length n over $\mathbb{Z}_{p^k}$, if for all $(a_0, \cdots, a_{n-1}) \in C_{p^k}$, then $s((a_0, \cdots, a_{n-1})) \in C_{p^k}$ (where s is the shift map), then the code is said to cyclic.

2.2 On fuzzy linear codes over $\mathbb{Z}_{p^k}$

Now we bring fuzzy logic in linear codes and introduce the notion of fuzzy linear code over the ring $\mathbb{Z}_{p^k}$.

Definition 2.13. Let $M = \mathbb{Z}_{p^k}^n$ be a $\mathbb{Z}_{p^k}$-module. The fuzzy submodule $\mathcal{F}\sqcap$ of M is called fuzzy linear code of length n over $\mathbb{Z}_{p^k}$.

Using the transfer principle of Kondo [13], we have what is follow.

Proposition 2.14. *Let A be a fuzzy set on* $\mathbb{Z}_{p^k}^n$.

A is a fuzzy linear code of length n over $\mathbb{Z}_{p^k}$ if and only if for any $t \in [0,1]$, if $A_t \neq \emptyset$, then A_t is a linear code of length n over $\mathbb{Z}_{p^k}$.

Corollary 2.15. *Let A be a fuzzy set on* $\mathbb{Z}_{p^k}^n$.

A is a fuzzy linear code of length n over $\mathbb{Z}_{p^k}$ if and only if the characteristic function of any upper t-level cut $A_t \neq \emptyset$ for $t \in [0,1]$ is a fuzzy linear code of length n over $\mathbb{Z}_{p^k}$.

Example 2.16. *Consider a fuzzy subset* $\mathcal{F}\sqcap$ *on* $\mathbb{Z}_4$ *as follows:*

$$\mathcal{F}\sqcap : \mathbb{Z}_4 \to [0,1], x \mapsto \begin{cases} 1 & if \;\; x = 0; \\ \frac{1}{3} & if \;\; x = 1; \\ \frac{1}{3} & if \;\; x = 2; \\ \frac{1}{3} & if \;\; x = 3. \end{cases}.$$

Then $\mathcal{F}\sqcap$ is a fuzzy submodule on $\mathbb{Z}_4$-module $\mathbb{Z}_4$, hence $\mathcal{F}\sqcap$ is a fuzzy linear code over $\mathbb{Z}_4$.

Remark 2.17. Let $\mathcal{F}\sqcap$ be a fuzzy linear code of length n over $\mathbb{Z}_{p^k}$, since $\mathbb{Z}_{p^k}^n$ is a finite set, then $Im(\mathcal{F}\sqcap) = \left\{\mathcal{F}\sqcap(x)|x \in \mathbb{Z}_{p^k}^n\right\}$ is finite. Let $Im(\mathcal{F}\sqcap)$ is set as: $t_1 > t_2 > \cdots > t_m$ (where $t_i \in [0,1]$) that is $Im(\mathcal{F}\sqcap)$ have m elements.

Since $\mathcal{F}\sqcap_{t_i}$ is a linear code over $\mathbb{Z}_{p^k}$, let G_{t_i} his generator matrix, $\mathcal{F}\sqcap$ can be determined by m matrixes G_{t_1}, G_{t_2}, $\cdots$, G_{t_m} as in the below Theorem 2.31.

There are some know notions of the orthogonality in fuzzy space, but no one of them does not hold here because these definitions does not meet the transfer principle in the sense of the orthogonality for the t-level cut sets. So we have to introduce an new notion of orthogonality on fuzzy submodules.

Definition 2.18. Let $\mathcal{F}\sqcap_1$ and Fu_2 be two fuzzy submodules on module $\mathbb{Z}_{p^k}^n$ over the ring $\mathbb{Z}_{p^k}$. We said that $\mathcal{F}\sqcap_1$ and $\mathcal{F}\sqcap_2$ are orthogonal if $Im(\mathcal{F}\sqcap_2) = \{1-\alpha|\ \alpha \in Im(\mathcal{F}\sqcap_1)\}$ and for all $t \in [0,1]$, $(\mathcal{F}\sqcap_2)_{1-t} = \left((\mathcal{F}\sqcap_1)_t\right)^{\perp} = \{y \in \mathbb{Z}_{p^k}^n| <x,y> \ = 0,\ \text{for all}\ x \in (\mathcal{F}\sqcap_1)_t\}$. Where $<,>$ is the standard inner product on $\mathbb{Z}_{p^k}^n$.

Noted that $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_2$ means $\mathcal{F}\sqcap_1$ and $\mathcal{F}\sqcap_2$ are orthogonal. We what is follow as an example.

Example 2.19. *Consider the two fuzzy submodules $\mathcal{F}\sqcap_1$ and $\mathcal{F}\sqcap_2$ on $\mathbb{Z}_4$ defined as follows:*

$$\mathcal{F}\sqcap_1 : \mathbb{Z}_4 \to [0,1], x \mapsto \begin{cases} \frac{1}{2} & \textit{if}\ \ x = 0; \\ \frac{1}{4} & \textit{if}\ \ x = 1; \\ \frac{1}{3} & \textit{if}\ \ x = 2; \\ \frac{1}{4} & \textit{if}\ \ x = 3. \end{cases} \quad \textit{and}\ \mathcal{F}\sqcap_2 : \mathbb{Z}_4 \to [0,1],$$

$$x \mapsto \begin{cases} \frac{3}{4} & \textit{if}\ \ x = 0; \\ \frac{1}{2} & \textit{if}\ \ x = 1; \\ \frac{2}{3} & \textit{if}\ \ x = 2; \\ \frac{1}{2} & \textit{if}\ \ x = 3. \end{cases}.$$

We easily observe that:
$(\mathcal{F}\sqcap_1)_{\frac{1}{2}} = \{0\}$ and $(\mathcal{F}\sqcap_2)_{\frac{1}{2}} = \mathbb{Z}_4$,
$(\mathcal{F}\sqcap_1)_{\frac{1}{4}} = \mathbb{Z}_4$ and $(\mathcal{F}\sqcap_1)_{\frac{3}{4}} = \{0\}$,
$(\mathcal{F}\sqcap_1)_{\frac{1}{3}} = \{0,2\}$ and $(\mathcal{F}\sqcap_1)_{\frac{2}{3}} = \{0,2\}$.
Thus $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_2$.

Remark 2.20. Let $\mathcal{F}\sqcap_1$ be a fuzzy submodule on module $\mathbb{Z}_{p^k}^n$ such that $\forall x \in \mathbb{Z}_{p^k}^n$, $\mathcal{F}\sqcap_1(x) = \gamma$ (with $\gamma \in [0,1]$), then it does not exists a fuzzy set $\mathcal{F}\sqcap$ on $\mathbb{Z}_{p^k}^n$ such that $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap$.

The previous Remark 2.20 show that the orthogonal of some fuzzy submodule in our sense does not always exists, so it is important to see under which condition the orthogonal of fuzzy submodule exists. The following theorem show the existence of the orthogonal of some fuzzy submodule.

Theorem 2.21. *Let $\mathcal{F}\sqcap_1$ be a fuzzy submodule on a finite module $\mathbb{Z}_{p^k}^n$. If $Im(\mathcal{F}\sqcap_1)$ have more that one element and for all $\varsigma \in Im(\mathcal{F}\sqcap_1)$ there exist $\epsilon \in Im(\mathcal{F}\sqcap_1)$ such that $A_\varsigma = (A_\epsilon)^\perp$, then there always exists a fuzzy submodule $\mathcal{F}\sqcap_2$ on $\mathbb{Z}_{p^k}^n$ such that $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_2$.*

Proof. Let $\mathcal{F}\sqcap_1$ be a fuzzy submodule on $\mathbb{Z}_{p^k}^n$. Assume that $|Im(\mathcal{F}\sqcap_1)| = m > 1$ and for any $\varsigma \in Im(A)$ there exist $\epsilon \in Im(\mathcal{F}\sqcap_1)$ such that $(\mathcal{F}\sqcap_1)_\varsigma = \left((\mathcal{F}\sqcap_1)_\epsilon\right)^\perp$.

Assume that $Im(\mathcal{F}\sqcap_1) = \{t_1 > t_2 > \cdots > t_m\}$. Let the sets $M_i = \left\{x \in \mathbb{Z}_{p^k}^n | \mathcal{F}\sqcap_1(x) = t_i\right\}$, $i = 1, \cdots, m$. These sets form a partition of $\mathbb{Z}_{p^k}^n$.

Let us define a fuzzy set $\mathcal{F}\sqcap$ as follow:

$\mathcal{F}\sqcap : \mathbb{Z}_{p^k}^n \to [0, 1], x \mapsto 1 - t_{m-i+1}$, if $x \in M_i$.

Since $Im(\mathcal{F}\sqcap_1) = \{t_1 > t_2 > \cdots > t_m\}$, we have $(\mathcal{F}\sqcap_1)_{t_1} \subseteq (\mathcal{F}1)_{t_2} \subseteq \cdots \subseteq (\mathcal{F}\sqcap_1)_{t_m}$. As for any $\varsigma \in Im(\mathcal{F}\sqcap_1)$ there exist $\epsilon \in Im(A)$ such that $A_\varsigma = (A_\epsilon)^\perp$, then $A_{t_i} = \left(A_{t_{m-i+1}}\right)^\perp$.

Thus $\mathcal{F}\sqcap_{1-t_{m-i+1}} = \left\{x \in \mathbb{Z}_{p^k}^n | \mathcal{F}\sqcap(x) \geq 1 - t_{m-i+1}\right\} = M_i \cup M_{i-1} \cup \cdots \cup M_1 = (\mathcal{F}\sqcap_1)_{t_i} = \left((\mathcal{F}\sqcap_1)_{t_{m-i+1}}\right)^\perp$.

Then by taken $\mathcal{F}\sqcap_2 = \mathcal{F}\sqcap$ we obtain the need fuzzy submodule. □

When the orthogonality exist, there is unique. We have the following theorem to show it.

Theorem 2.22. *Let $\mathcal{F}\sqcap_1$, $\mathcal{F}\sqcap_2$ and $\mathcal{F}\sqcap_3$ be three fuzzy submodules on module $\mathbb{Z}_{p^k}^n$, such that $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_2$ and $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_3$, then $\mathcal{F}\sqcap_2 = \mathcal{F}\sqcap_3$.*

Proof. Consider that $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_2$ and $\mathcal{F}\sqcap_1 \perp \mathcal{F}\sqcap_1 3$.

Let $t \in [0, 1]$, and $b \in (\mathcal{F}\sqcap_2)_{1-t}$, then $< a, b > = 0$, for all $a \in (\mathcal{F}\sqcap_1)_t$. Thus $b \in (\mathcal{F}\sqcap_3)_{1-t}$ and $(\mathcal{F}\sqcap_2)_{1-t} \subseteq (\mathcal{F}\sqcap_3)_{1-t}$. Therefore $(\mathcal{F}\sqcap_3)_t \subseteq (\mathcal{F}\sqcap_3)_t$.

In the same way, we show that $(\mathcal{F}\sqcap_2)_t \subseteq (\mathcal{F}\sqcap_3)_t$. Therefore $\mathcal{F}\sqcap_2 = \mathcal{F}\sqcap_3$. □

Corollary 2.23. *The orthogonal of a fuzzy set on $\mathbb{Z}_{p^k}^n$ is a fuzzy submodule on $\mathbb{Z}_{p^k}^n$.*

The orthogonality is an indempotent operator, in fact if $\mathcal{F}\sqcap$ be a fuzzy submodule on $\mathbb{Z}_{p^k}^n$ then $(\mathcal{F}\sqcap^\perp)^\perp = \mathcal{F}\sqcap_1$.

The notion of equivalence on fuzzy linear code can be define as follow.

Definition 2.24. Let $\mathcal{F}\sqcap_1$ and $\mathcal{F}\sqcap_2$ be two fuzzy linear codes over $\mathbb{Z}_{p^k}$. $\mathcal{F}\sqcap_1$ and $\mathcal{F}\sqcap_2$ are said to be equivalent if for all $t \in [0, 1]$, the linear codes $(\mathcal{F}\sqcap_1)_t$ and $(\mathcal{F}\sqcap_2)_t$ are equivalent.

Example 2.25. *Let C_{G_1} and C_{G_2} be two equivalent linear codes of length n over $\mathbb{Z}_{p^k}$.*

We define the equivalent fuzzy linear codes as follow:

$$\mathcal{F}\sqcap_1 : \mathbb{Z}_{p^k}^n \to [0, 1], x \mapsto \begin{cases} 1 & \textit{if } x \in C_{G_1}; \\ 0 & \textit{otherwise}. \end{cases} \text{ and.}$$

$$\mathcal{F}\sqcap_2 : \mathbb{Z}_{p^k}^n \to [0, 1], x \mapsto \begin{cases} 1 & \textit{if } x \in C_{G_2}; \\ 0 & \textit{otherwise}. \end{cases}.$$

Thus the 1 and 0 -level cut of the both fuzzy linear codes give $(\mathcal{F}\sqcap_1)_1 = C_{G_1}$ and $(\mathcal{F}\sqcap_2)_1 = C_{G_2}$,

$(\mathcal{F}\sqcap_1)_0 = \mathbb{Z}_{p^k}^n$ and $(\mathcal{F}\sqcap_2)_0 = \mathbb{Z}_{p^k}^n$.

Remark 2.26. Two equivalent fuzzy linear codes over $\mathbb{Z}_{p^k}$ have the same image.

2.3 Fuzzy linear codes in a practical way

As we have said in the introduction, how fuzzy linear code can deal with uncertain information in a practical way? This subsection allow us to use directly fuzzyness in the information theory.

Let us draw the communication channel as follows:

$$\begin{tikzcd} F^k \arrow[r, "Encoding"] & F^n \arrow[r, "Channel"] & \mathbb{R}^n \arrow[r, "Decoding"] & F^k \end{tikzcd}$$

Assume that $R^k = \mathbb{Z}_2^2$ and $R^n = \mathbb{Z}_2^3$, that means that $k = 2$ and $n = 3$. Let $\mathcal{C} \subseteq R^3$ be a linear code over R, in the classical case, when we send a codeword $a = (101) \in \mathcal{C}$ through a communication channel, the signal receive can be read as $a' = (0.98, 0.03, 0.49)$ and modulate to $a'' = (100)$. Thus to know if a'' belong to the code $\mathcal{C}$, we use syndrome calculation [14]. Since the modulation have gave a wrong word, we can consider that a' have more information than a'', in the sense that we can estimate a level to which a word 0 is modulate to 1, and a word 1 is modulate to 0. Therefore it is possible to use the idea of fuzzy logic to recover the transmit codeword.

Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_2^3$. To each $a \in \mathcal{C}$, we find $t \in [0, 1]$ such that t estimate the degree of which the element of $\mathbb{R}^3$, obtain from a through the transmission channel belong to the code $\mathcal{C}$. Thus in $\mathbb{Z}_2^3$ the information that we handle are certain, whereas in $\mathbb{R}^3$ there are uncertain. When we associate to all elements of $\mathbb{Z}_2^3$ the degree of which its correspond element obtain through the transmission channel belong to $\mathbb{Z}_2^3$, then we obtain a fuzzy code. If the fuzzy code are fuzzy linear code, then we can recover the code $\mathcal{C}$ just by using the upper t-level cut. Thus we deal directly with the uncertain information to obtain the code $\mathcal{C}$.

The following example illustrate this reconstruction of the code by using uncertain information in the case of fuzzy linear code.

Example 2.27. *Let* $\mathbb{Z}_2^3 = \{000, 001, 010, 100, 110, 101, 011, 111\}$ *and* $C = \{000, 001, 110, 111\}$ *be a linear code over* $\mathbb{Z}_2$.

Assume that after the transmission we obtain respectively $\{000; 0.01, 01; 1.01, 10; 1.001, 1, 0.999\}$. Let $\mathcal{F}\sqcap : \mathbb{Z}_2^3 \to [0, 1]$ such that

$$x \mapsto \begin{cases} \{1\} & \text{if } x = 000; \\ \{0.99\} & \text{if } x = 001; \\ \{0.9\} & \text{if } x = 010; \\ \{0.9\} & \text{if } x = 100; \\ \{0.99\} & \text{if } x = 110; \\ \{0.9\} & \text{if } x = 101; \\ \{0.9\} & \text{if } x = 011; \\ \{0.99\} & \text{if } x = 111. \end{cases}.$$

Then by finding a $t \in [0, 1]$ such that $\mathcal{F}\sqcap_t = \{x \in \mathbb{Z}_2^3 | \mathcal{F}\sqcap(x) \geq t\} = C$, we obtain $t > 0.9$. Thus, for $t = 0.99$, we are sure that the receive codeword is in $\mathcal{C}$.

It should be better to investigate in deep this approach.

2.4 Fuzzy cyclic code over $\mathbb{Z}_{p^k}$

Let the module $\mathbb{Z}_{p^k}^n$, in this subsection we will consider the case where the integers n and p are coprime.

Definition 2.28. A fuzzy module $\mathcal{F}\sqcap$ on the module $\mathbb{Z}_{p^k}^n$ is called a fuzzy cyclic code of length n over $\mathbb{Z}_{p^k}$ if for all $(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{Z}_{p^k}^n$, then $\mathcal{F}\sqcap((a_{n-1}, a_0, \cdots, a_{n-2})) \geq \mathcal{F}\sqcap((a_0, a_1, \cdots, a_{n-1}))$.

The following proposition give a caracterization of the fuzzy cyclic codes.

Proposition 2.29. *[15] A fuzzy submodule* $\mathcal{F}\sqcap$ *on on* $\mathbb{Z}_{p^k}^n$ *is a fuzzy cyclic code if and only if for all.*

$(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{Z}_{p^k}^n$, we have $\mathcal{F}\sqcap((a_0, a_1, \cdots, a_{n-1})) = \mathcal{F}\sqcap((a_{n-1}, a_0, \cdots, a_{n-2})) = \cdots =$

$$\mathcal{F}\sqcap((a_1, a_2, \cdots, a_{n-1}, a_0)).$$

Proposition 2.30. *$\mathcal{F}\sqcap$ is a fuzzy cyclic code of length n over $\mathbb{Z}_{p^k}$ if and only if for all $t \in [0,1]$, if $(\mathcal{F}\sqcap)_t \neq \emptyset$, then $(\mathcal{F}\sqcap)_t$ is a ideal of the factor ring $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$.*

Proof. Assume that $\mathcal{F}\sqcap$ is a fuzzy cyclic code over $\mathbb{Z}_{p^k}$ and $t \in [0,1]$ such that $(\mathcal{F}\sqcap)_t \neq \emptyset$. Then $(\mathcal{F}\sqcap)_t$ is a cyclic code over $\mathbb{Z}_{p^k}$.

Let $\psi : \mathbb{Z}_{p^k}^n \to \frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}, \underline{c} = (c_0, \cdots, c_{n-1}) \mapsto \psi(\underline{c}) = \sum_{i=0}^{n-1} c_i X^i$.

It is prove by easy way that ψ is a isomorphism of $\mathbb{Z}_{p^k}$-module, which send a cyclic codes over $\mathbb{Z}_{p^k}$ onto the ideals of the factor ring $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$. Therefore, $\forall t \in [0,1]$, $\mathcal{F}\sqcap_t$ is a ideal of $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$.

Conversely, assume that, $\forall t \in [0,1]$ such that $\mathcal{F}\sqcap_t \neq \emptyset$, $\mathcal{F}\sqcap_t$ is a ideal of factor ring $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$. Since $\mathcal{F}\sqcap_t$ is a ideal of factor ring $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$, then $\mathcal{F}\sqcap_t$ is a submodule of $\mathbb{Z}_{p^k}$-module $\mathbb{Z}_{p^k}^n$. Hence $\mathcal{F}\sqcap_t \neq \emptyset$, is a linear code over $\mathbb{Z}_{p^k}$, then $\mathcal{F}\sqcap$ is a fuzzy linear code. Due to ψ, $\forall t \in [0,1]$, $\mathcal{F}\sqcap_t$ is a cyclic code over $\mathbb{Z}_{p^k}$, then $\mathcal{F}\sqcap$ is a fuzzy cyclic code over $\mathbb{Z}_{p^k}$. □

Since $\mathbb{Z}_{p^k}$ is a finite ring, then $Im(\mathcal{F}\sqcap) = \left\{\mathcal{F}\sqcap(x) \in [0,1] | x \in \mathbb{Z}_{p^k}^n\right\}$ is also finite. Assume that $Im(\mathcal{F}\sqcap) = \{t_1 > t_2 > \cdots > t_m\}$, then $\mathcal{F}\sqcap_{t_1} \subseteq \mathcal{F}\sqcap_{t_2} \subseteq \cdots \subseteq \mathcal{F}\sqcap_{t_{m-1}} \subseteq A_{t_m} = \mathbb{Z}_{p^k}^n$.

Let $g_i^{(k)}(X) \in \mathbb{Z}_{p^k}[X]$ the generator polynomial of $\mathcal{F}\sqcap_{t_i}$, note that $g_i^{(k)}(X)$ is the Hensel lifting of order k of some polynomial $g_i(X) \in \mathbb{Z}_p[X]$ which divide $X^n - 1$, the cyclic code $<g_i^{(k)}(X)> \subset \frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$ is called the **lifted code** of the cyclic code $<g_i(X)> \subset \frac{\mathbb{Z}_p[X]}{(X^n-1)}$ [8].

Since $\mathcal{F}\sqcap_{t_1} \subseteq \mathcal{F}\sqcap_{t_2} \subseteq \cdots \subseteq \mathcal{F}\sqcap_{t_{m-1}} \subseteq \mathcal{F}\sqcap_{t_m} = \mathbb{Z}_{p^k}^n$, then $g_{i+1}^{(k)}(X) | g_i^{(k)}(X), i = 1, \cdots, m-1$. So we define the polynomial $h_i^{(k)}(X) = (X^n - 1)/g_i^{(k)}(X)$ which is called the check polynomial of the cyclic code $\mathcal{F}\sqcap_{t_i} = <g_i^{(k)}(X)>, i = 1, \cdots, m$.

Theorem 2.31. *Let $\mathcal{G} = \left\{g_1^{(k)}(X), g_2^{(k)}(X), \cdots, g_m^{(k)}(X)\right\}$ be a set of polynomial in $\mathbb{Z}_{p^k}[X]$, such that $g_i(X)$ divide $X^n - 1$, $i = 1, \cdots, m$. If $g_{i+1}^{(k)}(X) | g_i^{(k)}(X)$ for $i = 1, 2, \cdots, m-1$ and $<g_m^{(k)}(X)> = \mathbb{Z}_{p^k}^n$, then the set $\mathcal{G}$ can determined a fuzzy cyclic code $\mathcal{F}\sqcap$ and $\left\{ <g_i^{(k)}(X)> | i = 1, \cdots, m\right\}$ is the family of upper level cut cyclic subcodes of $\mathcal{F}\sqcap$.*

The proof is leave for the reader but he can check it in [15].

3. Fuzzy $\mathbb{Z}_{p^k}$-linear code

In the previous section, we study define and fuzzy linear codes over the ring $\mathbb{Z}_{p^k}$ in the previous section. Now define the notion on **fuzzy Gray map**, we are going to use it in the construction of the fuzzy $\mathbb{Z}_{p^k}$-linear codes which is different from the fuzzy linear codes over the ring $\mathbb{Z}_{p^k}$.

3.1 Fuzzy Gray map

When we order and enumerate a binary sequences of a fixed length we obtain the code of Gray in it original form. For the length two which interest us directly we have the following Gray code:

$$0 \mapsto 00$$

$$1 \mapsto 01$$

$$2 \mapsto 11$$

$$3 \mapsto 10.$$

Let $\phi : \mathbb{Z}_{2^2} \to \mathbb{Z}_2^2$ the Gray map.

Using the extension principle [16], we will define the fuzzy Gray map between two fuzzy spaces by what is follow.

Definition 3.1. Consider the Gray map $\phi : \mathbb{Z}_{2^2} \to \mathbb{Z}_2^2$. Let $\mathcal{F}(\mathbb{Z}_{2^2})$, $\mathcal{F}\left(\mathbb{Z}_2^2\right)$ the set of all the fuzzy subset on $\mathbb{Z}_{2^2}$ and $\mathbb{Z}_2^2$ respectively. The fuzzy Gray map is the map $\hat{\phi} : \mathcal{F}(\mathbb{Z}_{2^2}) \to \mathcal{F}\left(\mathbb{Z}_2^2\right)$, such that for all $\mathcal{F}\sqcap \in \mathcal{F}(\mathbb{Z}_{2^2})$, $\hat{\phi}(\mathcal{F}\sqcap)(y) = sup\{A(x) | y = \phi(x)\}$.

The next Theorem is straightforward.

Theorem 3.2. *The fuzzy Gray map $\hat{\psi}$ is a bijection.*

Proof: It is due to the fact that ψ is one to one function. □

As in crisp case, we have the following Proposition which is very important.

Proposition 3.3. *If $\mathcal{F}\sqcap$ is a fuzzy linear code over $\mathbb{Z}_{2^2}$ and ϕ the Gray map, then $\hat{\phi}(\mathcal{F}\sqcap)$ is no always a fuzzy linear code over the field $\mathbb{Z}_2$.*

The Gray map give a way to construct the nonlinear codes as binary image of the linear codes, we have for example the case of Kerdock, Preparata, and Goethals codes which have very good properties and also useful (We refer reader for it on [17, 18]). Moreover if $\mathcal{C}$ is a linear code of length n over $\mathbb{Z}_4$, then $C = \psi(\mathcal{C})$ is a nonlinear code of length $2n$ over $\mathbb{Z}_2$ in generally [18]. In that way we construct a fuzzy Kerdock code in the following example.

Example 3.4. *Let* $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & 0 & 1 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 3 & 2 \end{pmatrix}$ *be a generating matrix for a linear code $\mathcal{C}$ of length 8 over $\mathbb{Z}_4$. Then his image under the Gray map ϕ give a Kerdock code C.*

Let $\mathcal{F}\sqcap : \mathbb{Z}_4^8 \to [0, 1], x \mapsto \begin{cases} 1, & if \ \ x \in \mathcal{C}; \\ 0, & otherwise. \end{cases}$ Thus $\mathcal{F}\sqcap$ is a fuzzy linear code over $\mathbb{Z}_4$.

Since ϕ is a bijection, we construct $\hat{\phi}(\mathcal{F}\sqcap) : \mathbb{Z}_2^{16} \to [0, 1], y \mapsto \begin{cases} 1, & y \in \ \mathcal{E}; \\ 0, & otherwise. \end{cases}$,

where $\mathcal{E} = \{y \in \mathbb{Z}_2^{16} | y = \phi(x) \text{ and } x \in C\}$.

Noted that as $\mathcal{E}$ is not a linear code over $\mathbb{Z}_2$, then $\hat{\phi}(Fu)$ is a fuzzy $\mathbb{Z}_2$-linear code but not a fuzzy linear code over $\mathbb{Z}_2$.

$\hat{\phi}(\mathcal{F}\sqcap)$ is a fuzzy Kerdock code of length 16.

By the Example, we remark that a fuzzy $\mathbb{Z}_4$-linear code is not in generally a fuzzy linear code over $\mathbb{Z}_2$.

If we define the fuzzy binary relation R_ϕ on $\mathbb{Z}_{2^2} \times \mathbb{Z}_2^2$ by $R_\phi(x, y) = \begin{cases} 1, & \text{if } y = \psi(x); \\ 0, & \text{otherwise.} \end{cases}$ It is easy to see [19] that $\hat{\phi}(\mathcal{F}\sqcap)(y) = sup\{\mathcal{F}\sqcap(x) | y = \phi(x)\}$ can be represented by $\hat{\phi}(\mathcal{F}\sqcap)(y) = sup\{\, min\,\{\mathcal{F}\sqcap(x), R_\phi(x, y)\} | x \in \mathbb{Z}_2^2\}$.

We now define fuzzy generalized gray map. First we consider the generalized Gray map as in [8] $\Phi : \mathbb{Z}_{p^k} \to \mathbb{Z}_p^{p^{k-1}}$.

Definition 3.5. The map $\hat{\Phi} : \mathcal{F}\left(\mathbb{Z}_{p^k}\right) \to \mathcal{F}\left(\mathbb{Z}_p^{p^{k-1}}\right)$, such that for any $\mathcal{F}\sqcap \in \mathcal{F}\left(\mathbb{Z}_{p^k}\right)$,

$$\hat{\Phi}(\mathcal{F}\sqcap)(y) = \begin{cases} sup\{\mathcal{F}\sqcap(x) | y = \Phi(x)\}, & \text{if a such x exists;} \\ 0, & \text{otherwise.} \end{cases}$$

Is called a fuzzy generalized gray map.

Remark 3.6.

1. The Definition 3.5 can be simply write $\hat{\Phi}(A)(y) = \begin{cases} \mathcal{F}\sqcap(x), & \text{if } y = \Phi(x); \\ 0, & \text{otherwise.} \end{cases}$

   This because $\Phi : \mathbb{Z}_{p^k} \to \mathbb{Z}_p^{p^{k-1}}$ cannot give more than one image for one element.

2. Let $\mathcal{F}\sqcap_1 \in \mathcal{F}\left(\mathbb{Z}_p^{p^{k-1}}\right)$ such that $\mathcal{F}\sqcap_1(y) = t \neq 0$ for any $y \in \mathbb{Z}_p^{p^{k-1}}$. There does not exist a fuzzy subset $\mathcal{F}\sqcap \in \mathcal{F}\left(\mathbb{Z}_{p^k}\right)$ such that $\hat{\Phi}(\mathcal{F}\sqcap) = \mathcal{F}\sqcap_1$.

Thus $\hat{\Phi}$ is not a bijection map.

3.2 Fuzzy $\mathbb{Z}_{p^k}$-linear code

In the following, we will note $\hat{\Phi}$ the map on $\mathcal{F}\left(\mathbb{Z}_{p^k}^n\right)$ onto $\mathcal{F}\left(\mathbb{Z}_p^{n.p^{k-1}}\right)$ which spreads the fuzzy generalized Gray map.

Let define fuzzy $\mathbb{Z}_{p^k}$-linear code.

Definition 3.7. A fuzzy code *Fu* over $\mathbb{Z}_p$ is a fuzzy $\mathbb{Z}_{p^k}$-linear code if it is an image under the fuzzy generalized Gray map of a fuzzy linear code over the ring $\mathbb{Z}_{p^k}$.

For a fuzzy $\mathbb{Z}_{p^k}$-linear code, if it is the image under the generalized Gray map of a cyclic code over the ring $\mathbb{Z}_{p^k}$. Then the fuzzy code *Fu* is called a fuzzy $\mathbb{Z}_{p^k}$-cyclic code.

Remark 3.8. A fuzzy $\mathbb{Z}_{p^k}$-linear code is a fuzzy code over the fields $\mathbb{Z}_p$.

Example 3.9.

$$\text{Let } \mathcal{F}\sqcap : \mathbb{Z}_2^6 \to [0, 1], w = (a, b, c, d, e, f) \mapsto \begin{cases} 1, & \textit{if } e = f = 0; \\ 0, & \textit{otherwise}. \end{cases}$$

$\mathcal{F}\sqcap$ is a fuzzy linear code of length 6 over $\mathbb{Z}_2$.

$$\text{Let } \mathcal{F}\sqcap' : \mathbb{Z}_4^3 \to [0, 1], v = (x, y, z) \mapsto \begin{cases} 1, & \textit{if } z = 0; \\ 0, & \textit{otherwise}. \end{cases}$$

$\mathcal{F}\sqcap'$ is a fuzzy linear code of length 3 over $\mathbb{Z}_4$.

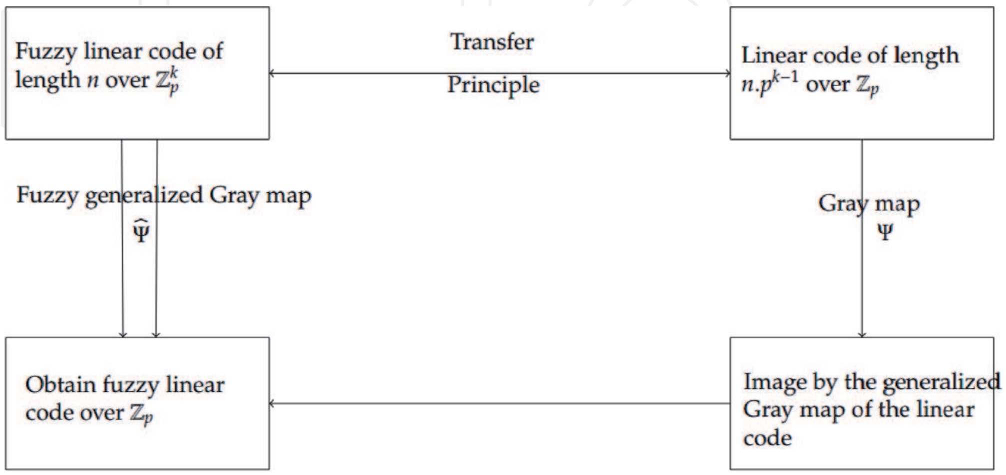
Since $\mathcal{F}\sqcap = \hat{\phi}(\mathcal{F}\sqcap')$. Then $\mathcal{F}\sqcap'$ is a fuzzy $\mathbb{Z}_4$-linear code.

Using crisp case technic we prove he following Proposition.

Proposition 3.10. *Let Fu be a fuzzy $\mathbb{Z}_{p^k}$-linear code, then Fu is no always a fuzzy linear code over the field $\mathbb{Z}_p$.*

Proof. The need here is to construct an counter-example, which is done in the Example 3.9. □

The following diagram give a construct the fuzzy $\mathbb{Z}_{p^k}$-linear code. This holds because the fuzzy generalized Gray map image of fuzzy linear code can be a fuzzy linear code over the field $\mathbb{Z}_p$:


Fuzzy linear code of length n over $\mathbb{Z}_p^k$
Transfer
Principle
Linear code of length $n.p^{k-1}$ over $\mathbb{Z}_p$
Fuzzy generalized Gray map
$\widehat{\Psi}$
Gray map
Ψ
Obtain fuzzy linear code over $\mathbb{Z}_p$
Image by the generalized Gray map of the linear code

We construct some codes using the both methods.

Example 3.11.

1. *Let $\mathcal{F}\sqcap : \mathbb{Z}_{p^k}^n \to [0,1]$ be a linear code such that $\mathcal{F}\sqcap$ have three upper t-level cut $\mathcal{F}\sqcap_{t_3} \subseteq \mathcal{F}\sqcap_{t_2} \subseteq \mathcal{F}\sqcap_{t_1}$. Let $\mathcal{F}\sqcap'_{t_3} = \Phi(\mathcal{F}\sqcap_{t_3})$, $\mathcal{F}\sqcap'_{t_2} = \Phi(\mathcal{F}\sqcap_{t_2})$ and $\mathcal{F}\sqcap'_{t_1} = \Phi(\mathcal{F}\sqcap_{t_1})$, we have $\mathcal{F}\sqcap'_{t_3} = \Phi(\mathcal{F}\sqcap_{t_3}) \subseteq \mathcal{F}\sqcap'_{t_2} = \Phi(\mathcal{F}\sqcap t_2) \subseteq \mathcal{F}\sqcap'_{t_1} = \Phi(\mathcal{F}\sqcap_{t_1})$. We construct $\mathcal{F}\sqcap' = \hat{\Phi}(\mathcal{F}\sqcap)$ as follow:*

$$\mathcal{F}\sqcap' : \mathbb{Z}_p^{n.p^{k-1}} \to [0,1], y \mapsto \begin{cases} t_3, & \textit{if } \; y \in \; \mathcal{F}\sqcap'_{t_3}; \\ t_2, & \textit{if } \; y \in \; \mathcal{F}\sqcap'_{t_2}; \\ t_1, & \textit{if } \; y \in \; \mathcal{F}\sqcap'_{t_1}; \\ 0, & \textit{otherwise}. \end{cases}$$

2. Let $\mathcal{F}\sqcap : \mathbb{Z}_4 \to [0,1], x \mapsto \begin{cases} \dfrac{1}{2} & \textit{if } \; x = 0; \\ \dfrac{1}{3} & \textit{if } \; x = 2; \\ \dfrac{1}{4} & \textit{if } \; x = 1, 3. \end{cases}$

be a fuzzy linear code over $\mathbb{Z}_4$. Then $\mathcal{F}\sqcap\frac{1}{2} = \{0\}$, $\mathcal{F}\sqcap\frac{1}{3} = \{0, 2\}$ and $\mathcal{F}\sqcap\frac{1}{4} = \mathbb{Z}_4$. We construct $\mathcal{F}\sqcap'\frac{1}{2} = \{00\}$, $\mathcal{F}\sqcap'\frac{1}{3} = \{00, 11\}$ and $\mathcal{F}\sqcap'\frac{1}{4} = \mathbb{Z}_2^2$, the Gray map image of $\mathcal{F}\sqcap_{\frac{1}{2}}$, $\mathcal{F}\sqcap\frac{1}{3}$ and $\mathcal{F}\sqcap\frac{1}{4}$ respectively, we define

$$\mathcal{F}\sqcap' \quad : \mathbb{Z}_2^2 \to [0,1], y \mapsto \begin{cases} \dfrac{1}{2} & \textit{if } \; x \in \; \mathcal{F}\sqcap\frac{1}{2}, \; y = \phi(x) \; ; \\ \dfrac{1}{3} & \textit{if } \; x \in \; \mathcal{F}\sqcap\frac{1}{3} \setminus \; \mathcal{F}\sqcap\frac{1}{2}, \; y = \phi(x); \\ \dfrac{1}{4} & \textit{if } \; x \in \; \mathcal{F}\sqcap\frac{1}{4} \setminus \; \mathcal{F}\sqcap\frac{1}{3}, \; y = \phi(x). \end{cases}$$

We obtain the same code $\mathcal{F}\sqcap'$ and $\hat{\phi}(\mathcal{F}\sqcap)$.

Proposition 3.12. *[15] If for all $t \in [0, 1]$, $\mathcal{F}\sqcap_t' = \Phi(\mathcal{F}\sqcap_t)$ (when $\mathcal{F}\sqcap_t \neq \varnothing$) is a linear code over $\mathbb{Z}_p$, then this two constructions of the fuzzy $\mathbb{Z}_p$-linear code above are give the same fuzzy code.*

Proof. This follows directly from the definition of the fuzzy generalized Gray map and the fact that the image under the generalized Gray map of a linear code is not a linear code in general. □

4. Linear codes over Krasner hyperfields

4.1 Preliminaries

This section recall notions and results that are required in the sequel. All of this can also be check on [3, 20–22].

Let $\mathcal{H}$ be a non-empty set and $\mathcal{P}^*(\mathcal{H})$ be the set of all non-empty subsets of $\mathcal{H}$. Then, a map $\circledast : \mathcal{H} \times \mathcal{H} \to \mathcal{P}^*(\mathcal{H})$, where $(h_1, h_2) \mapsto h_1 \circledast h_2 \subseteq \mathcal{H}$ is called a hyperoperation and the couple $(\mathcal{H}, \ , \circledast, \ )$ is called a hypergroupoid.

For all non-empty subsets A and B of $\mathcal{H}$ and $h \in \mathcal{H}$, we define $A \circledast B = \bigcup_{a \in A, b \in B} a \circledast b$, $A \circledast h = A \circledast \{h\}$ and $h \circledast B = \{h\} \circledast B$.

Definition 4.1. A canonical hypergroup $(\mathcal{R}, \oplus)$ is an algebraic structure in which the following axioms hold:

1. For any $x, y, z \in \mathcal{R}$, $x \oplus (y \oplus z) = (x \oplus y) \oplus z$,

2. For any $x, y \in \mathcal{R}$, $x \oplus y = y \oplus x$,

3. There exists an additive identity $0 \in R$ such that $0 \oplus x = \{x\}$ for every $x \in \mathcal{R}$.

4. For every $x \in \mathcal{R}$ there exists a unique element x' (an opposite of x with respect to hyperoperation "$\oplus$") in $\mathcal{R}$ such that $0 \in x \oplus x'$,

5. For any $x, y, z \in \mathcal{R}$, $z \in x \oplus y$ implies $y \in x' \oplus z$ and $x \in z \oplus y'$.

Remark 4.2. Note that, in the classical group $(R, +)$, the concept of opposite of $x \in R$ is the same as inverse.

A canonical hypergroup with a multiplicative operation which satisfies the following conditions is called a Krasner hyperring.

Definition 4.3. An algebraic hyperstructure $(\mathcal{R}, \oplus, \cdot)$, where "$\cdot$" is usual multiplication on $\mathcal{R}$, is called a Krasner hyperring when the following axioms hold:

1. $(\mathcal{R}, \oplus)$ is a canonical hypergroup with 0 as additive identity,

2. $(\mathcal{R}, \cdot)$ is a semigroup having 0 as a bilaterally absorbing element,

3. The multiplication "$\cdot$" is both left and right distributive over the hyperoperation "$\oplus$".

A Krasner hyperring is called commutative (with unit element) if $(\mathcal{R}, \cdot)$ is a commutative semigroup (with unit element) and such is denoted $(R, \oplus, \cdot, 0, 1)$.

Definition 4.4. Let $(R, \oplus, \cdot, 0, 1)$ be a commutative Krasner hyperring with unit such that $(R \backslash \{0\}, \cdot, 1)$ is a group. Then, $(R, \oplus, \cdot, 0, 1)$ is called a Krasner hyperfield.

This Example is from Krasner.

Example 4.5. *[?] Consider a field* $(F, +, \cdot)$ *and a subgroup* G *of* $(F\backslash\{0\}, \cdot)$. *Take* $H = F/G = \{aG|\ a \in F\}$ *with the hyperoperation and the multiplication given by:*

$$\begin{cases} aG \oplus bG = \{\bar{c} = cG|\ \bar{c} \in aG + bG\} \\ aG \cdot bG = abG \end{cases}$$

Then $(H, \oplus, \cdot)$ is a Krasner hyperfield.

We now give an example of a finite hyperfield with two elements 0 and 1, that we name $\mathcal{F}_2$ and which will be used it in the sequel.

Example 4.6. *Let* $\mathcal{F}_2 = \{0, 1\}$ *be the finite set with two elements. Then* $\mathcal{F}_2$ *becomes a Krasner hyperfield with the following hyperoperation "*$\oplus$*" and binary operation "*$\cdot$*".*

$\oplus$	0	1
0	$\{0\}$	$\{1\}$
1	$\{1\}$	$\{0,1\}$

and

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

Let $(\mathcal{R}, \oplus, \cdot)$ be a hyperring, A and B be a non-empty subset of $\mathcal{R}$. Then, A is said to be a subhyperring of $\mathcal{R}$ if $(A, \oplus, \cdot)$ is itself a hyperring. A subhyperring A of a hyperring $\mathcal{R}$ is a left (right) hyperideal of $\mathcal{R}$ if $r \cdot a \in A$ $(a \cdot r \in A)$ for all $r \in \mathcal{R}$, $a \in A$. Also, A is called a hyperideal if A is both a left and a right hyperideal. We define $A \oplus B$ by $A \oplus B = \{x|\ x \in a \oplus b$ 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 $a_i \in A, b_i \in B, n \in \mathbb{N}^*\}$. If A and B are hyperideals of $\mathcal{R}$, then $A \oplus B$ and $A \cdot B$ are also hyperideals of $\mathcal{R}$.

Definition 4.7. An algebraic structure $(\mathcal{R}, \oplus, \cdot)$ (where $\oplus$ and $\cdot$ are both hyperoperations) is called additive-multiplicative hyperring if the satisfies the following axioms:

1. $(\mathcal{R}, \oplus)$ is a canonical hypergroup with 0 as additive identity,
2. $(\mathcal{R}, \cdot)$ is a semihypergroup having 0 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 $x, y \in \mathcal{R}$, we have $x \cdot (y') = (x') \cdot y = (x \cdot y)'$.

An additive-multiplicative hyperring $(\mathcal{R}, \oplus, \cdot)$ is said to be commutative if $(\mathcal{R}, \cdot)$ is a commutative semihypergroup. and $(\mathcal{R}, \oplus, \cdot)$ is called a hyperring with multiplicative identity if there exists $e \in \mathcal{R}$ such that $x \cdot e = x = e \cdot x$ for every $x \in \mathcal{R}$.

We close this section with the following definition of the ideal in a additive-multiplicative hyperring.

Definition 4.8 A non-empty subset A of an additive-multiplicative hyperring $\mathcal{R}$ is a left (right) hyperideal if,

1. for all $a, b \in A$, then $a \oplus b' \subseteq A$,

2. for all $a \in A$, $r \in \mathcal{R}$, then $r \cdot a \subseteq A$ $(a \cdot r \subseteq A)$.

4.2 Hypervector spaces over hyperfields

We give some properties related to the hypervector space as it is done by Sanjay Roy and Samanta [23] and all these will allow us to characterize linear codes over a Krasner hyperfield.

From now on, and for the rest of this section, by $\mathcal{F}$ we mean a Krasner hyperfield.

Definition 4.9. [23] Let $\mathcal{F}$ be a Krasner hyperfield. A commutative hypergroup $(\mathcal{V}, \oplus_{\mathcal{V}})$ together with a map $\cdot : \mathcal{F} \times \mathcal{V}\int \to \mathcal{V}\int$, is called a hypervector space over $\mathcal{F}$ if for any $a, b \in \mathcal{F}$ and $x, y \in \mathcal{V}\int$, the following conditions hold:

1. $a \cdot \left(x \oplus_{\mathcal{V}\int} y \right) = a \cdot x \oplus_{\mathcal{V}\int} a \cdot y$ (right distributive law),

2. $\left(a \oplus_{\mathcal{V}\int} b \right) \cdot x = a \cdot x \oplus_{\mathcal{V}\int} b \cdot x$ (left distributive law),

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

4. $a \cdot (x') = (a') \cdot x = (a \cdot x)'$,

5. $x = 1 \cdot x$.

Let us give that trivial example of a hypervector space.

Example 4.10. *Let $n \in \mathbb{N}$, $\mathcal{F}^n$ is a hypervector space over $\mathcal{F}$ where the composition of elements are as follows:*

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

Definition 4.11. [23] Let $(\mathcal{V}\int, \oplus, \cdot, 1)$ be a hypervector space over $\mathcal{F}$. A subset $A \subseteq \mathcal{V}\int$ is called a subhypervector space of $\mathcal{V}\int$ if:

1. $A \neq 0$,

2. for all $x, y \in A$, then $x \oplus y' \subseteq A$,

3. for all $a \in \mathcal{F}$, for all $x \in A$, then $a \cdot x \in A$.

Definition 4.12. [23] Let $\mathcal{S}$ be a subset of a hypervector space $\mathcal{V}\int$ over $\mathcal{F}$. $\mathcal{S}$ is said to be linearly independent if for every $x_1, x_2, \dots, x_n$ in $\mathcal{S}$ and for every $a_1, a_2, \dots, a_n$ in $\mathcal{F}$, $(n \in \mathbb{N} \backslash \{0, 1\})$ such that $0 \in a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$ implies that $a_1 = a_2 = \cdots = a_n = 0$.

If $\mathcal{S}$ is not linearly independent, then we said that $\mathcal{S}$ is linearly dependent.

If $\mathcal{S}$ is a nonempty subset of $\mathcal{V}\int$, then the smallest subhypervector space of $\mathcal{V}$ containing $\mathcal{S}$ is the set define by

$\langle \mathcal{S} \rangle = \cup \left\{ \sum_{i=1}^{n} a_i \cdot x_i | \, x_i \in \mathcal{S}, a_i \in \mathcal{F}, n \in \mathbb{N} \backslash \{0, 1\} \right\} \cup l(\mathcal{S})$, (where $l(\mathcal{S}) = \{ a \cdot x | \, a \in \mathcal{F}, x \in \mathcal{S} \}$).

Definition 4.13. [23] Let $\mathcal{V}\int$ be a hypervector space over $\mathcal{F}$. A vector $x \in \mathcal{V}\int$ is said to be a linear combination of the vectors $x_1, x_2, \dots, x_n \in \mathcal{V}\int$ if there exist $a_1, a_2, \dots, a_n \in \mathcal{F}$ such that $x \in a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$ in the hypervector spaces, the notion of basis exists and he have the following definition.

Definition 4.14. *[23] Let $\mathcal{V}\int$ be a hypervector space over $\mathcal{F}$ and $\mathcal{B}$ be a subset of $\mathcal{V}\int$. The set $\mathcal{B}$ is said to be a basis for $\mathcal{V}\int$ if,*

1. $\mathcal{S}$ is linearly independent,

2. every element of $\mathcal{V}\int$ can be expressed as a finite linear combination of elements from $\mathcal{S}$.

4.3 Polynomial hyperring

We assume that $\mathcal{F}$ is such that for all $a, b \in \mathcal{F}$, $a \cdot (b') = (a') \cdot b = (a \cdot b)'$.

Let denote by $\mathcal{F}[x]$ the set of all polynomials in the variable x over $\mathcal{F}$. Let the polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ in $\mathcal{F}[x]$.

Let us define the set $\mathcal{P}^*(\mathcal{F})[x] = \{\sum_{k=0}^{n} A_k x^k;\ \text{where } A_k \in \mathcal{P}^*(\mathcal{F}), n \in \mathbb{N}\}$, the hypersum and hypermultiplication of $f(x)$ and $g(x)$ are defined as follows:

$$\overline{\oplus} : \mathcal{F}[x] \times \mathcal{F}[x] \to \mathcal{P}^*(\mathcal{F})[x] \tag{1}$$

$$(f(x), g(x)) \mapsto (f \overline{\oplus} g)(x) = (a_0 \oplus b_0) + (a_1 \oplus b_1)x + \cdots + (a_M \oplus b_M)x^M, \tag{2}$$

$$\textit{where } M = \textit{max}\,\{n, m\}. \tag{3}$$

$$\overline{\cdot} : F[x] \times F[x] \to \mathcal{P}^*(F)[x] \tag{4}$$

$$(f(x), g(x)) \mapsto (f \overline{\cdot} g)(x) = \sum_{k=0}^{m+n} \left(\sum_{l+j=k} a_l \cdot b_j \right) x^k, \textit{if } deg(f) \geq 1 \textit{ and } deg(g) \geq 1 \tag{5}$$

The following remark is from Jančic-Rašović [24].

Remark 4.15. The algebraic hyperstructure $(\mathcal{F}[x], \overline{\oplus}, \overline{\cdot})$ is an additive-multiplication hyperring.

4.4 Linear codes and cyclic codes over finite hyperfields

In this section we shall define and discuss about the concept of linear and cyclic codes over the finite Krasner hyperfield $\mathcal{F}_2$ from the **Example 4.6**. Let us recall some basics from code theory. Let $\mathcal{C}$ be a linear code, the Hamming distance $d_H(x, y)$ between two vectors $x, y \in \mathcal{C}$ is defined to be the number of coordinates in which x differs from y. The minimum distance of a code $\mathcal{C}$, denoted by $d(\mathcal{C})$, is $d(\mathcal{C}) = \min\{d_H(x, y) |\, x, y \in \mathcal{C} \text{ and } x \neq y\}$. In this case we can also compute for a code word $x \in \mathcal{C}$, the integer $w_H(x)$ which is the number of nonzero coordinates in x also called Hamming weight of x.

We denoted 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 [25].

Let us define linear code over $\mathcal{F}_2$.

Definition 4.16. A subhypervector space of the hypervector space $\mathcal{F}_2^n$ is called a linear code $\mathcal{C}$ of length n over $\mathcal{F}_2$.

The concept of dual code is a very useful in the coding theory. Let us define it on the Krasner hyperfield $\mathcal{F}_2$.

Definition 4.17. Let $\mathcal{C}$ be a linear code of length n $(n \geq 2)$ over $\mathcal{F}_2$. The dual of $\mathcal{C}$ is also a linear code defined by $\mathcal{C}^{\perp} := \{y \in \mathcal{F}_2^n \mid 0 \in x \cdot y^t, \forall x \in \mathcal{C}\}$.

The code $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$.

Here is an basic example of a linear code and his dual.

Example 4.18. *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* $C^{\perp} = \{000, 111\}$.

As in the classical case, the notion of cyclic code on hyperstructures still works with polynomials. So i that way 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 $\mathcal{F}_2$ 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 $\mathcal{F}_2^n$ and the residue class hyperring $\frac{\mathcal{F}_2[x]}{(x^n-1)}$ [25].

$$\xi : \mathcal{F}_2^n \rightarrow \frac{\mathcal{F}_2[x]}{(x^n - 1)}$$

$$c = (c_0, c_1, c_2, \ldots, c_{n-1}) \mapsto c_0 + c_1x^1 + c_2x^2 + \cdots + c_{n-1}x^{n-1}.$$

Using Theorem 3.7 in [26], the multiplication of x by any element of $\frac{\mathcal{F}_2[x]}{(x^n-1)}$ is equivalent to applying the shift map s of the Definition?? to the corresponding element of $\mathcal{F}_2^n$, so we use the polynomial to define cyclic code.

We are now going to define a distance relation on linear codes over the finite hyperfield $\mathcal{F}_2$, which will allow us to detect if there is an error in a received word.

Proposition 4.19. *The mapping define by*

$$\lceil_{\mathcal{H}} : \mathcal{F}_2^n \times \mathcal{F}_2^n \rightarrow \mathbb{N}$$

$$(x, y) \mapsto \lceil_{\mathcal{H}}(x, y) = card\{i \in \mathbb{N} \mid x_i \neq y_i\}$$

is a distance on $\mathcal{F}_2^n$, called the Hamming distance.

Proof. The proof is similar to the classical case. □

The following remark will be helpful to define Hamming weight.

Remark 4.20. For an $x \in \mathcal{F}_2^n$, we write $x = (\{x_1\}, \ldots, \{x_n\})$ such that x belongs now to the cartesian product $(\mathcal{P}^*(\mathcal{F}_2))^n$. Hence we can compute $w_H(x) = card\{i \in \mathbb{N} \mid 0 \notin x_i\} = d_H(0, x)$.

The following map denoted by w_H on the cartesian product $(\mathcal{P}^*(\mathcal{F}_2))^n$:

$$w_H : (\mathcal{P}^*(\mathcal{F}_2))^n \rightarrow \mathbb{N}$$

$$a = (a_1, \ldots, a_n) \mapsto card\{i \in \mathbb{N} \mid 0 \notin a_i\}.$$

is the Hamming weight on $\mathcal{F}_2^n$. So for all $x, y \in \mathcal{F}_2^n$, we have $\lceil_{\mathcal{H}}(x, y) = w_H(x \oplus y')$.

If $\mathcal{C}$ is a linear code over $\mathcal{F}_2$, the integer number $\lceil = \min\{w_H(x) | x \in \mathcal{C}\}$ is called the minimal distance of the code $\mathcal{C}$.

To characterized a linear code of length n over $\mathcal{F}_2$ as a subhypervector space of $\mathcal{F}_2^n$, it is sufficient to have a basis of that linear code. This basis can often be represented by a $k \times n$-matrix over $\mathcal{F}_2$ (where k is the dimension of the code).

We denoted by $\mathcal{M}(\mathcal{F}_2)$ be the set of all matrices over $\mathcal{F}_2$.

Definition 4.21. Let $\mathcal{C}$ be a linear code over $\mathcal{F}_2$. We called a generator matrix of $\mathcal{C}$ any matrix from $\mathcal{M}(\mathcal{F}_2)$ where the rows form a basis of the code $\mathcal{C}$.

Proposition 4.22. *Let* $\mathcal{B}_{\rfloor} \in \mathcal{M}_{k \times n}(\mathcal{F}_2)$ *be a generating matrix of the linear code* $\mathcal{C}$ *over* $\mathcal{F}_2$, *then* $\mathcal{C} = \{c \in a \cdot \mathcal{B}_{\rfloor} \mid a \in \mathcal{F}_2^k\}$.

Proof. Let $\mathcal{C}$ be a $[n, k]$-linear code over $\mathcal{F}_2$ and $\mathcal{B}_\rfloor$ a generating matrix of $\mathcal{C}$. Then the rows of $\mathcal{B}_\rfloor \in \mathcal{M}_{k\times n}(\mathcal{F}_2)$ form a basis of $\mathcal{C}$. So $\mathcal{C}$ consists of all linear combinations of the rows of $\mathcal{B}_\rfloor$, therefore $\mathcal{C} = \left\{c \in a \cdot \mathcal{B}_\rfloor \mid a \in \mathcal{F}_2^k\right\}$. □.

It is know that the dual code $\mathcal{C}^\perp$ of the linear code $\mathcal{C}$ over $\mathcal{F}_2$ is also linear, so $\mathcal{C}^\perp$ has a generating matrix called a parity check matrix.

Here and until the end of this paper, we will denoted by $\mathcal{B}_\rfloor$ the generating matrix and by $\mathcal{H}_\rfloor$ the parity check matrix of the linear code $\mathcal{C}$ over $\mathcal{F}_2$.

Example 4.23. *Let* $\mathcal{B}_\rfloor = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ *be a generating matrix of the linear code C from Example 4.18. Then the parity check matrix of* $\mathcal{C}$ *is* $\mathcal{H}_\rfloor = (1\ 1\ 1)$.

Theorem 4.24. *Let* $\mathcal{C}$ *be a linear code of length n* $(n \geq 2)$ *and dimension k over* $\mathcal{F}_2$. *Then* $\mathcal{H}_\rfloor \in \mathcal{M}_{(n-k)\times n}(\mathcal{F}_2)$ *and* $0 \in \mathcal{B}_\rfloor \cdot \mathcal{H}_\rfloor{}^t$. *(It should be noted that* $\mathcal{H}_\rfloor{}^t$ *means the transpose of* $\mathcal{H}_\rfloor$*).*

Proof. Let the generating matrix and the parity check matrix be denoted respectively by $\mathcal{B}_\rfloor = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$ and $\mathcal{H}_\rfloor = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$, where $g_i \in \mathcal{F}_2^n$ and $h_j \in \mathcal{F}_2^n$ (for $i = 1\cdots k$ and $j = 1\cdots n-k$).

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

We now give some examples of linear codes over $\mathcal{F}_2$ and we make some comparison between the linear codes over the finite field with two elements $\mathbb{F}_2$ and the linear code over the Krasner hyperfield $\mathcal{F}_2$.

Example 4.25. *Let* $\mathcal{F}_2^3$ *be a hypervector space over* $\mathcal{F}_2$ *and C be a subhypervector space of* $\mathcal{F}_2^3$, *with dimensional* $k = 2$. *Then C is a linear code of length* $n = 3$ *and dimension* $k = 2$ *over* $\mathcal{F}_2$.

1. *Let* $\mathcal{B}_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ *be a generating matrix of the linear code* $\mathcal{C}_1 = \{000, 010, 101, 111\}$ *over* $\mathcal{F}_2$. $\mathcal{B}_1$ *is also a generating matrix of a linear code* $\mathcal{C}_2 = \{000, 010, 101, 111\}$ *of length 3 and dimension 2 over the finite field* $\mathbb{F}_2$. *These two codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *have the same parameters and* $card(\mathcal{C}_1) = card(\mathcal{C}_2)$.

2. *Let* $\mathcal{B}_2 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ *be another generating matrix of the linear code C over* $\mathcal{F}_2$. $\mathcal{B}_2$ *is also a generating matrix of a linear code* $\mathcal{C}_2'$ *of length 3 and dimension 2 over the finite field* $\mathbb{F}_2$.

   Here we have that $\mathcal{C}_1 = \{000, 110, 101, 011, 111\}$, $\mathcal{C}_2' = \{000, 110, 101, 011\}$, so these two codes have the same parameters but $card(\mathcal{C}_1) > card\left(\mathcal{C}_2'\right)$.

3. *Let* $\mathcal{B}_{min} = \begin{pmatrix} Id_k & Id_{n-k} \\ \cdot & 0 \end{pmatrix}$ *(where* Id_k *is the* $k \times k$*-identity matrix).*

$\mathcal{B}_{min}$ is a generating matrix of a linear code $\mathcal{C}_{min}$ of length n and dimension k over $\mathcal{F}_2$ (with $n-k \leq k$). The linear code $\mathcal{C}_{min}$ over $\mathcal{F}_2$ generated by $\mathcal{B}_{min}$ has the minimal number of code words, $card(\mathcal{C}_{min}) = 2^k$.

4. Let $\mathcal{B}_{max} = \begin{pmatrix} Id_k & 1_{n-k} \end{pmatrix}$ (where Id_k is the identity matrix and 1_{n-k} is the matrix such that every element is equal to 1).

$\mathcal{B}_{max}$ is a generating matrix of a hyperlinear code $\mathcal{C}_{max}$ of length n and dimension $k>2$ over $\mathcal{F}_2$. The linear code $\mathcal{C}_{max}$ over $\mathcal{F}_2$ generated by $\mathcal{G}_{max}$ has the maximal number of code words, $card(\mathcal{C}_{max}) = 2^{n-k} + \sum_{i=2}^{k-1} \binom{k}{i} + k + 1$.

This remark is deduce from the previous example.

Remark 4.26. 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 by MacWilliams and Sloane in their book *The Theory of Error-Correcting Codes* [27] 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. That is the subject of the next theorem.

Theorem 4.27. *Let $\mathcal{C}$ be a linear code of length n and dimension k over $\mathcal{F}_2$. If M is the cardinality of $\mathcal{C}$, then* $2^k \leq M \leq \begin{cases} 2^{n-k} + k + 1, & \text{if } k \leq 2; \\ 2^{n-k} + \sum\limits_{i=2}^{k-1} \binom{k}{i} + k + 1, & \text{if } k > 2. \end{cases}$.

Proof. Since a generating matrix contains a basis of the linear code $\mathcal{C}$ 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:

1. in the first k columns no 1 is repeated. (this forces that every code word belongs to only one linear combination).

2. not any sum of elements in one column is equal to zero.

3. all the elements of the $n-k$ last columns are equal to 1. (because we need every combination has the maximal number of code words)

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

We deduce from the Theorem 4.27 what is follow, which mean that a linear code over the hyperfield F_2 satisfies the Singleton bound.

Corollary 4.28. *Let $\mathcal{C}$ be a linear code of length n and dimension k over $\mathcal{F}_2$, and $\mathcal{C}'$ be a linear code of length n and dimension k over the finite field $\mathbb{F}_2$. Then $d \leq d' \leq n-k+1$ (where d is the minimal distance of $\mathcal{C}$ and d' is the minimal distance of $\mathcal{C}'$).*

The following next propositions give some characterization of the linear codes over $\mathcal{F}_2$ using their generating matrix and their parity check matrix.

Proposition 4.29. *Let $\mathcal{C}$ be a linear code of length n and dimension k over $\mathcal{F}_2$, then $c \in \mathcal{C}$ if and only if $0 \in c \cdot \mathcal{H}_{\lrcorner}{}^t$.*

Proof. ⇒): Let $c \in \mathcal{C}$ and $\mathcal{H}_\lrcorner = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$ be the parity check matrix of the code $\mathcal{C}$. Then $c \cdot \mathcal{H}_\lrcorner{}^t = \left(c \cdot h_1^t, c \cdot h_2^t, \cdots, c \cdot h_{n-k}^t\right)$, thus by definition of $\mathcal{C}^\perp$, $0 \in c \cdot \mathcal{H}_\lrcorner{}^t$.

⇐) Assume that $0 \in c \cdot \mathcal{H}_\lrcorner{}^t$, then c belongs either to $\mathcal{B}_\lrcorner$, or to a linear combination of rows of $\mathcal{B}_\lrcorner$. Therefore $c \in \mathcal{C}$. □

Proposition 4.30. *Let $\mathcal{C}$ be a linear code of length n over $\mathcal{F}_2$, then the double dual of $\mathcal{C}$ is equals to $\mathcal{C}$, that is $\left(\mathcal{C}^\perp\right)^\perp = \mathcal{C}$.*

Proof. Using Proposition 4.3 in [26], $\left(\mathcal{C}^\perp\right)^\perp$ is a linear code of length n over $\mathcal{F}_2$, so it is sufficient to show that $\mathcal{C} = \left(\mathcal{C}^\perp\right)^\perp$. By definition we have $\left(\mathcal{C}^\perp\right)^\perp = \{a \in \mathcal{F}_2 |\ 0 \in y \cdot a^t;$ for all $y \in \mathcal{C}^\perp\}$, so it is straightforward that $\mathcal{C} \subseteq \left(\mathcal{C}^\perp\right)^\perp$. Now, let $a \in \left(\mathcal{C}^\perp\right)^\perp$. Let $\mathcal{H}_\lrcorner = \begin{pmatrix} h_1 \\ \vdots \\ h_{n-k} \end{pmatrix}$ be the parity check matrix of the code $\mathcal{C}$, then

$$a \cdot \mathcal{H}_\lrcorner{}^t = \left(\sum_{i=1}^{n} a_i \cdot h_{1,i}, \cdots, \sum_{i=1}^{n} a_i \cdot h_{n-k,i}\right)$$

$$= \left(\sum_{i=1}^{n} h_{1,i} \cdot a_i, \cdots, \sum_{i=1}^{n} h_{n-k,i} \cdot a_i\right) = \left(\sum_{i=1}^{n} h_{1,i} \cdot a^t, \cdots, \sum_{i=1}^{n} h_{n-k,i} \cdot a^t\right).$$

Thus $0 \in a \cdot \mathcal{H}_\lrcorner{}^t$ by definition of $\left(\mathcal{C}^\perp\right)^\perp$, therefore $a \in \mathcal{C}$. We conclude the proof by using Proposition 4.29. □

It is known from [26] that cyclic code in $\mathcal{F}_2^n$ has only one generating polynomial, so it is clear that this polynomial divides the polynomial $x^n - 1$.

Proposition 4.31. *If $g(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathcal{F}_2[x]$, is the generating polynomial for a cyclic code $\mathcal{C}$ over $\mathcal{F}_2$, then $\mathcal{B}_\lrcorner = \begin{pmatrix} a_0 & \cdots & a_k & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_k & 0 & \cdots & 0 \\ 0 & 0 & a_0 & & a_k & \cdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & a_0 & \cdots & a_k \end{pmatrix}$ is the generator matrix of the cyclic code $\mathcal{C}$.*

Proof. Let $g_1 = (a_0, \ldots, a_k, 0, \ldots, 0) \in \mathcal{F}_2^n$, then $\mathcal{B}_\lrcorner$ can also be write as $\mathcal{B}_\lrcorner = \begin{pmatrix} g_1 \\ s(g_1) = g_2 \\ s^2(g_1) = g_3 \\ \vdots \\ s^{k-1}(g_1) = g_k \end{pmatrix}$ (where s is the shift function and $s^k = s \circ s \circ \cdots \circ s$, k-successive shifts).

Since the polynomial g generates $\mathcal{C}$, we have $\mathcal{C} = \ <g(x)>$. Let $c \in \mathcal{C}$, then $(c_i)_{i=1\cdots n} = c \in g(x) \cdot p(x)$ (where $b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} = p(x) \in \frac{\mathcal{F}_2[x]}{(x^n - 1)}$) implies that $c_i \in \sum_{l+j} a_l \cdot b_j$ if $i \le k$ and $c_i = 0$ else if $(i > k)$.

Focus on $g(x)$ and $p(x)$, the element c belongs to the sum $b_0 \cdot g(x) + b_1 x \cdot g(x) + \cdots + b_{n-1} \cdot x^{n-1} \cdot g(x)$ because this sum can also be written as $e_1 \cdot g_1 + e_2 \cdot g_2 + \cdots + e_k \cdot g_k$ $(e = (e_1, \ldots, e_k) \in \mathcal{F}_2^n)$, and $\mathcal{C}$ is a cyclic code generated by $g(x)$. □

The following Proposition use same notations as in Proposition 4.31.

Proposition 4.32. *[28] Let* $h(x) \in \frac{\mathcal{F}_2[x]}{(x^n-1)}$ *be a polynomial such that* $x^n - 1 \in h(x) \cdot g(x)$*, then*

1. *The linear code* $\mathcal{C}$ *over* $\mathcal{F}_2$ *can be represented as* $\mathcal{C} = \left\{p(x) \in \frac{\mathcal{F}_2[x]}{(x^n-1)} | \ 0 \in p(x) \cdot h(x)\right\}$.

2. $h(x)$ *is the generating polynomial for the linear code* $\mathcal{C}^{\perp}$.

To illustrate what is doing for cyclic codes and polynomials, we have this example.

Example 4.33. *Let* $\mathcal{C}$ *be a linear code over* $\mathcal{F}_2$ *generate by the polynomial* $g(x) = 1 + x^2 \in \frac{\mathcal{F}_2[x]}{(x^3-1)}$. *Then the generator matrix of the code* $\mathcal{C}$ *is given by* $\mathcal{B}_\lrcorner = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

Since $x^3 - 1 \in (1 + x^2)\dot{\odot}\}(1 + x + x^2)$, then the polynomial $h(x) = 1 + x + x^2$ is the parity check polynomial of the code $\mathcal{C}$, and the parity check matrix is given by $\mathcal{H}_\lrcorner = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

Thus $\mathcal{C} = \left\{p(x) \in \frac{F_2[x]}{(x^3-1)} | \ x^3 - 1 \in p(x)\dot{\odot}\}(1 + x + x^2)\right\} = \{0, 1 + x^2, 1 + x, 1 + x + x^2, x + x^2\}$.

5. Conclusions

This Chapter divides in three sections **Fuzzy linear codes over** $\mathbb{Z}_{p^k}$, **Fuzzy** $\mathbb{Z}_{p^k}$**-linear codes** and **Linear codes over Krasner hyperfields** just introduce some new perspectives in the field of coding theory. In the first and second section, we define and give some related properties of these on codes. We show in some example that fuzzy linear code can deal with uncertain information directly. The third section, which joint the previous sections in the sense that fuzzy fields/rings and Krasner hyperfields are non classical structures which approxim very well many real life situation, study linear codes over Krasner hyperfields as linear codes over finite fields. Many of their properties are given and the important thing that arise here is that with almost the same parameters linear codes construct on Krasner hyperfields have much code words than one construct on fields.

Author details

Surdive Atamewoue Tsafack
University of Yaounde I, Yaounde, Cameroon

*Address all correspondence to: surdive@yahoo.fr

References

[1] L.A. Zadeh, Fuzzy sets, *Information and Control* **8** 338-353 (1965).

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

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

[4] C.E. Shannon, Communication in presence of noise, *IEEE*, **37**, 10-21 (1949).

[5] K. P. Shum, Chen De Gang, Some note on the theory of fuzzy code, *Electronic BUSEFAL-81, Polytech.univ-savoie, France* 132-136 (2000).

[6] L. O. Hall and G. Diall, On fuzzy code for asymmetric and unidirectional errors, *Fuzzy sets and systems* **36**, 365-373 (1990).

[7] P.A. Von Kaenel, Fuzzy codes and distance properties, *Fuzzy sets and systems* **8**, 199-204 (1982).

[8] 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).

[9] M. Maschinchi and M.M. Zahedi, On L-fuzzy primary submodules, *Fuzzy Sets and Systems* **49**, 231-236 (1992).

[10] C.V. Negoita and D.A. Ralescu, Applications of Fuzzy Sets and System Analysis, (*Birkhous, Basel*) (1975).

[11] R. Biswas, Fuzzy fields and fuzzy linear space redefined, *Fuzzy Sets and Systems* **33**, 257-259 (1989).

[12] *S. Nanda*, Fuzzy fields and fuzzy linear space, *Fuzzy Sets and Systems* **19**, 89-94 (1986).

[13] M. Kondo, Wieslaw A. Dubek, On transfer principle in fuzzy Theory, *Mathware and soft computing* **12**, 41-55 (2005).

[14] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, *IEEE Transactions on Informations Theory* **44**, 1543-1547 (1998).

[15] S. Atamewoue Tsafack , S. Ndjeya , L. Strüngmann and C. Lele, Fuzzy Linear Codes, *Fuzzy Information and Engineering*, https://doi.org/10.1080/16168658.2019.1706959 (2020).

[16] L.A. Zadeh, The concept of a linguistic variable and its application to approximate reasoning I, II, III, *Information Sciences* **8-9**, 199-257, 301-357, 43-80 (1975).

[17] A.M. Kerdock, A class of low-rate nonlinear codes, *Information and Control* **20** (1972).

[18] R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane et P. Solé, Kerdock, Preparata, Goethals and other codes are linear over $\mathbb{Z}_4$, *IEEE Transactions on Information Theory* **40**, 301-319 (1994).

[19] I. Perfilieva, Fuzzy function: Theoretical and practical point of view. *Atlantis Press* 480-486 (2011).

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

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

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

[23] Sanjay Roy and T.K. Samanta, A Note on Hypervector Spaces, *Discussiones MathematicaeGeneral Algebra and Applications* **31**, 75-99 (2011).

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

[25] 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).

[26] B. Davvaz and T. Musavi, Codes Over Hyperrings, *Matematički Vesnik* **68**, 26-38 (2016).

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

[28] S. Atamewoue Tsafack, S. Ndjeya, L. Strüngmann and C. Lele, Codes over Hyperfields, Discussioness Mathematicae Genenal Algerbra and Applcations **37**, 147-160 (2017).