Journal of Pure and Applied Mathematics: Advances and Applications
Volume 26, Number 1, 2023, Pages 25-48
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/jpamaa_7100122270

THE $m\Theta$ PROTOCOL $F5$ AND HAMMING $m\Theta$ CODES

PEMHA BINYAM GABRIEL CEDRIC

Department of Mathematics and Computer Sciences
Faculty of Sciences
University of Douala
P. O. Box 24157, Douala
Cameroon
e-mail: gpemha@yahoo.fr

Abstract

$\mathbb{F}_{p\mathbb{Z}}$ is the prime modal Θ-valent field with p^2 elements as presented by Ayissi Eteme in [5] in order to define on $\mathbb{F}_{p\mathbb{Z}}$ a notion of Hamming code which respects its structure of $m\Theta$ set. We show a relation between $m\Theta$ protocol $F5$ and Hamming $m\Theta$ code. By using this relation, we give a method to construct good $m\Theta$ steganographic protocols.

2020 Mathematics Subject Classification: 94A60, 03B45.
Keywords and phrases: $m\Theta$ set, Hamming $m\Theta$ codes, steganography, $m\Theta$ protocol $F5$.
Received December 28, 2022

1. Introduction

Steganography [4, 6] is the art and science of invisible communications. It is used, sometimes together with cryptography to protect information from unwanted third parties. The design of a steganographic system has two facets: firstly, the choice of accurate covers and the search for strategies to modify them in an imperceptible way; secondly, the design of efficient algorithms for embedding and extracting the information. Recall that error-correcting codes are commonly used for detecting and correcting errors in data transmission. It was first suggested by Crandall [9] and later implicitly used by Westfeld in the design of $F5$ [10].

An $m\Theta$ approach of the notion of code [11] has allowed to bring out the new classes of codes: $m\Theta$ codes. The $m\Theta$ codes [2, 12, 13] present an enrichment from the logical view-point compared with the classical codes. Indeed, with the $m\Theta$ codes, we can mathematically express that an information is lightly, partially or greatly damaged.

Let E be a finite $m\Theta$ set, then a non-empty subset $\mathcal{C}$ of E is called an $m\Theta$ code. Often E is the $m\Theta$ set of n-tuples from a finite alphabet A with p^2 elements. The elements of E are called $m\Theta$ words and the elements of $\mathcal{C}$ are called $m\Theta$ codewords. When A is a $m\Theta$ field, E is an n-dimensional vector space over A. In this case, $\mathcal{C}$ is called a linear $m\Theta$ code if $\mathcal{C}$ is a linear subspace of E. When $A = \mathbb{F}_{p\mathbb{Z}}$, the finite $m\Theta$ field of p^2 elements and E will be denoted $V(n, p\mathbb{Z})$.

Section 2 recalls firstly the essential notions of $m\Theta$ set, secondly the linear $m\Theta$ codes and lastly the Hamming $m\Theta$-distance of $(\mathcal{C}, F^n_{\alpha|\mathcal{C}})$. Section 3 presents the Hamming codes on $V(n, 2\mathbb{Z})$. Section 4 is devoted to the $m\Theta$ steganographic protocol $F5$ and Hamming $m\Theta$ codes.

2. Preliminaries

2.1. The modal Θ-valent set structure and the algebra of $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$

$m\Theta$ sets are considered to be non-classical sets which are compatible with a non-classical logic called the chrysippian $m\Theta$ logic.

Definition 1 ([14]). Let E be a non-empty set, I be a chain whose first and last elements are 0 and 1, respectively, $(F_\alpha)_{\alpha \in I_*}$, where $I_* = I \setminus \{0\}$ be a family of applications form E to E.

A $m\Theta$ set is the pair $(E, (F_\alpha)_{\alpha \in I_*})$ simply denoted by (E, F_α) satisfying the following four axioms:

- $\underset{\alpha}{\cap} F_\alpha(E) = \underset{\alpha \in I_*}{\cap} \{F_\alpha(x) : x \in E\} \neq \emptyset$;
- $\forall \alpha, \beta \in I_*$, if $\alpha \neq \beta$, then $F_\alpha \neq F_\beta$;
- $\forall \alpha, \beta \in I_*$, $F_\alpha \circ F_\beta = F_\beta$;
- $\forall x, y \in E$, if $\forall \alpha \in I_*$, $F_\alpha(x) = F_\alpha(y)$, then $x = y$.

Theorem 1 ([7]) (The theorem of $m\Theta$ determination). *Let* (E, F_α) *be a* $m\Theta$ *set.*

$$\forall x, y \in E, x =_\Theta y \text{ if and only if } \forall \alpha \in I_*, F_\alpha(x) = F_\alpha(y).$$

Proof. [7].

Definition 2 ([11]). Let $C(E, F_\alpha) = \underset{\alpha \in I_*}{\cap} F_\alpha(E)$. We call $C(E, F_\alpha)$ the set of $m\Theta$ invariant elements of the $m\Theta$ set (E, F_α).

Proposition 1 ([7]). *Let* (E, F_α) *be an* $m\Theta$ *set. The following properties are equivalent*:

(1) $x \in \bigcap_{\alpha \in I_*} F_\alpha(E)$;

(2) $\forall \alpha \in I_*,\ F_\alpha(x) = x$;

(3) $\forall \alpha, \beta \in I_*,\ F_\alpha(x) = F_\beta(x)$;

(4) $\exists \mu \in I_*,\ x = F_\mu(x)$.

Proof. [7].

Definition 3 ([1]). Let (E, F_α) and (E', F'_α) be two $m\Theta$ sets. Let X be a non-empty set. We shall call

(1) (E', F'_α) is a modal Θ-valent subset of (E, F_α) if the structure of $m\Theta$ set (E', F'_α) is the restriction to E' of the structure of the $m\Theta$ set (E, F_α), this means:

- $E' \subseteq E$;
- $\forall \alpha : \alpha \in I_*,\ F'_\alpha = F_{\alpha|_{E'}}$.

(2) X is a modal Θ-valent subset of (E, F_α) if:

- $X \subseteq E$;
- $(X, F_{\alpha|_X})$ is an $m\Theta s$ which is a modal Θ-valent subset of (E, F_α).

In all what follows we shall write $F_\alpha x$ for $F_\alpha(x)$, $F_\alpha E$ for $F_\alpha(E)$, etc.

Let $p \in \mathbb{N}$, a prime number. Let us recall that if $a \in \mathbb{F}_{p\mathbb{Z}}$.

$$\mathbb{F}_{p\mathbb{Z}} = \mathbb{F}_p \cup \{x_{pZ} : \neg(x \equiv 0 (\text{mod } p))\};\quad \mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}.$$

We define the $m\Theta$ support of a denoted $s(a)$ as follows:

$$s(a) = \begin{cases} a & \text{if } a \in \mathbb{F}_p; \\ x & \text{if } a = x_{p\mathbb{Z}} \text{ with } \rceil(x \equiv 0 (\text{mod } p)). \end{cases}$$

Thus $s(a) \in \mathbb{F}_p$.

Definition 4 ([14]). Let $\perp$ be a binary operation on $\mathbb{F}_p$. So, $\forall a, b \in \mathbb{F}_p$, $a \perp b \in \mathbb{F}_p$. Let $x, y \in \mathbb{F}_{p\mathbb{Z}}$. We define a binary operation $\perp^*$ on $\mathbb{F}_{p\mathbb{Z}}$ as follows:

$$x \perp^* y = \begin{cases} s(x) \perp s(y) & \text{if } \begin{cases} x, y \in \mathbb{F}_p \\ (s(x) \perp s(y)) \equiv 0 \,(\text{mod } p) \quad \text{otherwise} \end{cases} \\ (s(x) \perp s(y))_{p\mathbb{Z}} & \text{otherwise.} \end{cases}$$

$\perp^*$ as defined above on $\mathbb{F}_{p\mathbb{Z}}$ will be called an $m\Theta$ law on $\mathbb{F}_{p\mathbb{Z}}$ for $x, y \in \mathbb{F}_{p\mathbb{Z}}$.

Thus we can define $x + y \in \mathbb{F}_{p\mathbb{Z}}$ and $x \times y \in \mathbb{F}_{p\mathbb{Z}}$ for every $x, y \in \mathbb{F}_{p\mathbb{Z}}$, where $+$ and $\times$ are $m\Theta$ addition and $m\Theta$ multiplication, respectively.

Theorem 2 ([1]). $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha, +, \times)$ *is an* $m\Theta$ *ring of unity* 1 *and of* $m\Theta$ *unity* $\frac{1}{p\mathbb{Z}}$.

Proof. [1].

Remark 1. Since p is prime, $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$ is an $m\Theta$ field.

Definition 5 ([5]). x is a divisor of zero in $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$ if it exists $y \in \mathbb{F}_{p\mathbb{Z}}$ such that $x \times y = 0$.

Example 1 ([5]). $p = 2$, we have $\mathbb{F}_{2\mathbb{Z}} = \{0, 1, 1_{2\mathbb{Z}}, 3_{2\mathbb{Z}}\}$.

The table of $m\Theta$ determination and tables laws of $\mathbb{F}_{2\mathbb{Z}}$:

$\mathbb{F}_{2\mathbb{Z}}$	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
F_1	0	1	1	0
F_2	0	1	0	1

$+^{\Theta}$	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
1	1	0	0	0
$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	0	0	0
$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	0	0	0

$\times^{\Theta}$	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	0	0	0	0
1	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$1_{2\mathbb{Z}}$	0	$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$3_{2\mathbb{Z}}$	0	$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$

Observation:

$\mathbb{F}_{2\mathbb{Z}}$ has no divisor of zero, is a $m\Theta$ ring from four elements, that's a $m\Theta$ field of four elements.

2.2. Linear $m\Theta$ codes

Let (A, F_α) be a finite $m\Theta$ set. For every $n \in \mathbb{N}^*$, we shall denote in what follows the $m\Theta$ set product of (A, F_α) by (A^n, F_α^n), where F_α^n is the product on A^n of F_α. By definition, we have:

$$F_\alpha^n : A^n \longrightarrow A^n; \quad (a_1, \cdots, a_n) \mapsto F_\alpha^n(a_1, \cdots, a_n)$$

$$= (F_\alpha(a_1), \cdots, F_\alpha(a_n)).$$

Let k and n be two natural integers such that $k \neq 0$, $n \neq 0$, and $k \leq n$.

Definition 6 ([13]). Let us set $\mathcal{C} = f(E)$ the image of f. As f is injective, f is an $m\Theta$ bijection from E to $\mathcal{C}$. $(\mathcal{C}, F^n_{\alpha|\mathcal{C}})$ is considered as the $m\Theta$ set of all possible $m\Theta$ messages.

(1) An $m\Theta$ code of length n and of alphabet (A, F_α), the $m\Theta$ set $(\mathcal{C}, F^n_{\alpha|\mathcal{C}})$.

(2) Elements of $\mathcal{C}$, $m\Theta$ messages or $m\Theta$ words of the $m\Theta$ code $(\mathcal{C}, F^n_\alpha|_\mathcal{C})$.

(3) Elements of $\mathcal{C}$, $(\mathcal{C}, F^n_\alpha|_\mathcal{C}) = \cap_{\alpha \in I_*} F^n_\alpha|_\mathcal{C}(\mathcal{C})$, messages or words of the $m\Theta$ code $(\mathcal{C}, F^n_\alpha|_\mathcal{C})$.

Proposition 2 ([11]). $(\mathcal{C}, F^n_\alpha|_\mathcal{C})$ *is an* $m\Theta$ *part of* (A^n, F^n_α).

Proof. [11].

Proposition 3 ([11]). *Let* $(\mathcal{C}, F^n_\alpha|_\mathcal{C})$ *be a* $m\Theta$ *code of length* n *on* (A, F_α). *The set* $\mathcal{C}(\mathcal{C}, F^n_\alpha|_\mathcal{C}) = \cap_{\alpha \in I_*} F^n_\alpha|_\mathcal{C}(\mathcal{C})$ *is a classical code of length* n *on* $\cap_{\alpha \in I_*} F_\alpha(A) = \mathcal{C}(A, F_\alpha)$.

Proof. [11].

Definition 7 ([12]). Let $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ be the $m\Theta$ field with four elements $\forall \alpha \in I_*$, we call:

(1) Hamming α-weight of an element $x = (x_1, \cdots, x_n)$ of $(V(n, 2\mathbb{Z}), F^n_\alpha)$ the number of non zero coordinates of $F^n_\alpha(x)$. We denote it by $\omega_{H_\alpha}(x) = \omega(F^n_\alpha(x))$.

$$\omega_{H_\alpha}(x) = \omega(F^n_\alpha(x)) = \mathrm{Card}\{i | F_\alpha(x_i) \neq 0;\ i = 1, \cdots, n\}.$$

(2) Hamming $m\Theta$-weight of an element $x = (x_1, \cdots, x_n)$ of $(V(n, 2\mathbb{Z}), F_\alpha^n)$ the number denoted $\omega_{H_\Theta}(x)$ and defined as follows:

$$\omega_{H_\Theta}(x) = \begin{cases} \omega(x) & x \in \mathbb{F}_2^n; \\ \sum_{\alpha \in I_*} \omega_{H_\alpha}(x) = \sum_{\alpha \in I_*} \omega(F_\alpha^n(x)) & \text{otherwise.} \end{cases}$$

The alphabet used is the $m\Theta$ field $(\mathbb{F}_{p\mathbb{Z}} = (\frac{\mathbb{Z}_{p\mathbb{Z}}}{p\mathbb{Z}_{p\mathbb{Z}}}, F_\alpha))$.

Proposition 4 ([5]). *We set $E = V(k, p\mathbb{Z})$ and $\mathcal{C} = f(E)$. Let (E, F_α^k) be the $m\Theta$ set of $m\Theta$ message and f a $m\Theta$ linear encoder of (E, F_α^k) in $(V(n, p\mathbb{Z}), F_\alpha^n)$. Then, the $m\Theta$ code $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$ is an $m\Theta$ vector subspace of $(V(n, p\mathbb{Z}), F_\alpha^n)$ over $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$.*

Proof. [5].

Definition 8 ([13]). An $m\Theta$ linear code of $m\Theta$ dimension k and of length n on $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$ is an $m\Theta$ vector subspace of $m\Theta$ dimension k of $(V(n, p\mathbb{Z}), F_\alpha^n)$.

Proposition 5 ([5]). *Let $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ be a linear $m\Theta$ code of $m\Theta$ dimension k and of length n.*

Then $\mathcal{C}(\mathcal{C}, F_{\alpha|\mathcal{C}}^n) = \cap_{\alpha \in I_*} F_\alpha^n(\mathcal{C})$ is a linear code of dimension k and of length n.

Proof ([5]). As $\mathcal{C}(V(k, p\mathbb{Z}), F_\alpha^k)$. is a $\mathbb{F}_p$-vector space of dimension k, then $C(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ is a linear code of dimension k and of length n.

2.3. The Hamming $m\Theta$-distance of $(\mathcal{C}, F^n_{\alpha|\mathcal{C}})$

Let $(\mathcal{C}, F^n_{\alpha|\mathcal{C}})$ be an $m\Theta$ or a pseudo $m\Theta$ code of length n on (A, F_α). Our purpose is to define for $(\mathcal{C}, F^n_{\alpha|\mathcal{C}})$ a notion of distance which is compatible with its structure of $m\Theta$ code.

$\forall \alpha \in I_*$, we define d_{H_α} on $A^n \times A^n$ as follows:

$$d_{H_\alpha}(x, y) = d_H(F^n_\alpha x, F^n_\alpha y)$$

$$= \text{card}\{i : F_\alpha x_i \neq F_\alpha y_i;\ i = 1, \cdots, n\},$$

where $x = (x_1, \cdots, x_n)$; $y = (y_1, \cdots, y_n)$ and d_H is the Hamming distance on $(\mathcal{C}(A, F_\alpha))^n$.

Proposition 6. If *(A, F_α) is an $m\Theta$ set and $(\mathcal{C}, F_\alpha)$ is an $m\Theta$ code on (A, F_α), then $\forall x, y \in A^n$, we define d_{H_Θ} on $A^n \times A^n$ as follows*:

$$d_{H_\Theta}(x, y) = \begin{cases} d_H(x, y), & \text{if } x \text{ and } y \in (\mathcal{C}(A, F_\alpha))^n; \\ \sum_{\alpha \in I_*} d_{H_\alpha}(x, y) = \sum_{\alpha \in I_*} d_H(F_\alpha x, F_\alpha y) & \text{otherwise.} \end{cases}$$

$F^n_\alpha x = (F_\alpha x_1, \cdots, F_\alpha x_n)$; $F^n_\alpha y = (F_\alpha y_1, \cdots, F_\alpha y_n)$. Then d_{H_Θ} is an $m\Theta$ distance on (A^n, F^n_α).

Proof. [11].

Definition 9. d_{H_Θ} will be called the Hamming $m\Theta$ distance on (A^n, F^n_α).

Remark 2. $d_{H_\Theta | C(A^n, F^n_\alpha)}$ is the Hamming distance on $(\mathcal{C}(A, F_\alpha))^n$.

Definition 10. Let $(\mathcal{C}, F_\alpha)$ be an $m\Theta$ code; d_{H_Θ} is the $m\Theta$ Hamming distance. We define δ^Θ as follows:

$$\delta^\Theta = \min\{d_{H_\Theta}(x, y) : x, y \in \mathcal{C}; x \neq y\}.$$

We shall call δ^Θ the minimal $m\Theta$ distance of the $m\Theta$ code $(\mathcal{C}, F_\alpha)$.

3. The Hamming $m\Theta$ Codes

3.1. Generating and parity check matrices

Let $(\mathcal{C}, F_\alpha)$ denote a linear $m\Theta$ code in $V(n, p\mathbb{Z})$. Let G be a matrix whose rows generate $(\mathcal{C}, F_\alpha)$. The matrix G is called a generating matrix of $(\mathcal{C}, F_\alpha)$. The dual $m\Theta$ code of $(\mathcal{C}, F_\alpha)$, denoted $\mathcal{C}^\perp$, is defined to be the set

$$\mathcal{C}^\perp = \{x \in V(n, p\mathbb{Z}); \quad \forall\alpha \in I_*, \left\langle F_\alpha x, F_\alpha c\right\rangle = 0, \forall c \in (\mathcal{C}, F_\alpha)\},$$

where $\langle u, v\rangle := u_1v_1 + u_2v_2 + \cdots + u_nv_n$. Note that $\mathcal{C}^\perp$ is clearly also a linear $m\Theta$ code, and thus has a generating matrix H. By the definition of $\mathcal{C}^\perp$, it can be seen that

$$\mathcal{C} = \{c \in V(n, p\mathbb{Z}) / \forall\alpha \in I_*, F_\alpha(c)H^t = 0\}.$$

The matrix H is called a parity check matrix for $(\mathcal{C}, F_\alpha)$. If an $m\Theta$ word w is received, then it can be verified that w is an $m\Theta$ codeword simply by checking that $wH^t = 0$, i.e., $\forall\alpha \in I_*, F_\alpha(w)H^t = 0$.

3.2. Hamming codes on $V(n, 2\mathbb{Z})$

In this paragraph, we introduce the Hamming $m\Theta$ code which is a linear $m\Theta$ code in $V(n, 2\mathbb{Z})$ for some $n \geq 2$.

Let $\mathbb{F}_{2\mathbb{Z}}$ denote the $m\Theta$ field of four elements and let H be the matrix whose columns are all the non-zero $m\Theta$ vectors of length k over $\mathbb{F}_{2\mathbb{Z}}$, for some $k \in \mathbb{N}$. Note that there will be $2^k - 1$ of these. We define the Hamming $m\Theta$ code as follows:

Definition 11. Fix $k \geq 2$ and let $n = 2^k - 1$. Let H denote the $k \times n$ matrix defined above. The Hamming $m\Theta$ code $Ham_{2\mathbb{Z}}(n)$ is the linear $m\Theta$ subspace of $V(n, 2\mathbb{Z})$ consisting of the set of all α-vectors, $\alpha \in I_*$, orthogonal to all the rows of H. That is,

$$Ham_{2\mathbb{Z}}(n) = \{v \in V(n, 2\mathbb{Z}) / \forall\alpha \in I_*,\ F_\alpha(v) \times H^t = 0\}.$$

Proposition 7. *The Hamming* $m\Theta$ *code* $Ham_{2\mathbb{Z}}(n)$ *with* $k \times (2^k - 1)$ *parity check matrix is a* $(2^k - 1, 2^k - k - 1, 3)$-*code.*

Proof 9. That the length of the $m\Theta$ vectors in $Ham_{2\mathbb{Z}}(n)$ is $2^k - 1$ is clear. The $m\Theta$ code $Ham_{2\mathbb{Z}}(n)$ is defined to be the $m\Theta$ subspace of $V(n, 2\mathbb{Z})$ orthogonal to the rowspace of H, which has dimension k, and so the dimension of $Ham_{2\mathbb{Z}}(n)$ will be $2^k - k - 1$ by the rank-nullity theorem. By definition, no two columns of H are dependent, there exist three columns in H which are linearly dependent. This implies that the $m\Theta$ code generated will have minimum $m\Theta$ distance 3. To see this, recall that for a linear $m\Theta$ code, the minimum $m\Theta$ distance is equivalent to the minimum weight of an $m\Theta$ codeword. Suppose columns i, j, and k of H are linearly dependent. Then some linear combination of those three columns with non-zero coefficients will equal zero, and since the vectors are taken over $\mathbb{F}_{2\mathbb{Z}}$, the coefficients must be 1. So the α-vector with $1'$s in the i, j, and k position is in $Ham_{2\mathbb{Z}}(n)$, and so the minimum $m\Theta$ weight of the code is at most 3. It cannot be less than 3, or else some linear combination of two columns of H would be zero, which we have ruled out. Thus H will be the parity check matrix for a $(2^k - 1, 2^k - k - 1, 3)$-code.

4. The $m\Theta$ Steganographic Protocol $F5$ and Hamming $m\Theta$ Codes

4.1. The $m\Theta$ protocol $F5$

$F5$ is a steganographic system developed by Westfeld in 2001 [10]. The $m\Theta$ protocol $F5$ over the $m\Theta$ field $\mathbb{F}_{2\mathbb{Z}}$ permits to hide $m\Theta$ messages of length k (secret $m\Theta$ words) in cover $m\Theta$ words of length $n = 2^k - 1$ by partially or totally changing more than one of them ($m\Theta$ protocol of type $(2^k - 1, k, 1)$). Let $< F_\alpha^k m >_2$ be the binary expression of m with k bits (so can consider that $< m >_2$ is in $V(k, 2\mathbb{N})$).

Conversely, for $z \in V(k, 2\mathbb{N})$, $\forall \alpha \in I_*$, let $< F_\alpha^k z >_{10}$ be the integer which has $F_\alpha^k z$ as binary expression, then $1 \leq < F_\alpha^k(z) >_{10} \leq 2^k - 1$. Finally, let e_i be the i-th vector of the canonical basis of $V(2^k - 1, 2)$; $e_0 = 0_{V(2^k - 1, 2)}$.

Proposition 8. *The* $m\Theta$ *maps* $\gamma_{2\mathbb{Z}}$, $e_{2\mathbb{Z}}$, *and* $r_{2\mathbb{Z}}$ *as follows define*:

(i) $\gamma_{2\mathbb{Z}} : V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z}) \to (\mathbb{N}_{2\mathbb{Z}}, F'_\alpha)$

$$(x, m) \mapsto (< F_\alpha^k(m) + \sum_{i=1}^{2^k - 1} F_\alpha(x_i) < i >_2 >_{10})_{\alpha \in I_*},$$

(ii) $e_{2\mathbb{Z}} : V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z}) \to V(2^k - 1, 2\mathbb{Z})$

$$(x, m) \mapsto (F_\alpha^{2^k - 1}(u) + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x, m))})_{\alpha \in I_*},$$

(iii) $r_{2\mathbb{Z}} : V(2^k - 1, 2\mathbb{Z}) \to V(k, 2\mathbb{Z})$

$$x \mapsto (\sum_{i=1}^{2^k - 1} F_\alpha(x_i) < i >_2)_{\alpha \in I_*}$$

are well defined and $m\Theta$.

Proof. (i) • Let $(x, m), (x', m') \in V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z})$ let us suppose that $(x, m) = (x', m')(x = x'$ and $m = m')$ and let us show that $\gamma_{2\mathbb{Z}}(x, m) = \gamma_{2\mathbb{Z}}(x', m')$.

$$(x, m) = (x', m') \Rightarrow \forall \alpha \in I_* \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^k m = F_\alpha^k m' \end{cases}$$

$\forall \alpha \in I_*$;

$$F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 = F_\alpha^k t + \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2$$

$$\Rightarrow < F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10} = < F_\alpha^k m' + \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2 >_{10}$$

$$\Rightarrow (< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*}$$

$$= (< F_\alpha^k m' + \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2 >_{10})_{\alpha \in I_*}$$

$$\Rightarrow \gamma_{2\mathbb{Z}}(x, m) = \gamma_{2\mathbb{Z}}(x', t).$$

Therefore the map $\gamma_{2\mathbb{Z}}$ is well defined.

• Let us verify $\gamma_{2\mathbb{Z}}$ is $m\Theta$ map.

Let $(x, m), (x', m') \in V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z})$

$\forall \alpha \in I_*$,

$$\gamma_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k)(x, m) = \gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k m)$$

$$= (< F_\alpha^k(F_\alpha^k m) + \sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1}x)_i) < i >_2 >_{10})_{\alpha \in I_*}$$

$$= (< F_\alpha^k m + \sum_{i=1}^{2^k-1} (F_\alpha^{2^k-1}x)_i) < i >_2 >_{10})_{\alpha \in I_*}$$

$$= (< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*};$$

$$F'_\alpha \circ \gamma_{2\mathbb{Z}}(x, m) = F'_\alpha(< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*}$$

$$= (< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*}.$$

Therefore $\gamma_{2\mathbb{Z}}$ is an $m\Theta$ map.

(ii) • $(x, m), (x', m') \in V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z})$ such that $(x, m) = (x', m')(x = x'$ and $m = m')$, let's show that $e_{2\mathbb{Z}}(x, m) = e_{2\mathbb{Z}}(x', m')$.

$$(x, m) = (x', m') \Rightarrow \forall \alpha \in I_*, \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^k m = F_\alpha^k m' \end{cases}$$

$$\forall \alpha \in I_*, \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^k m = F_\alpha^k m' \end{cases} \Rightarrow \forall \alpha \in I_*, \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ \gamma_{2\mathbb{Z}}(x, m) = \gamma_{2\mathbb{Z}}(x', m') \end{cases}$$

$$\Rightarrow \forall \alpha \in I_*, \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F'_\alpha \gamma_{2\mathbb{Z}}(x, m) = F'_\alpha \gamma_{2\mathbb{Z}}(x', m') \end{cases}$$

$$\Rightarrow \forall\alpha \in I_*, \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ e_{F'_\alpha\gamma_{2\mathbb{Z}}(x,\, m)} = e_{F'_\alpha\gamma_{2\mathbb{Z}}(x',\, m')} \end{cases}$$

$$\Rightarrow \forall_\alpha^{I_*};\ F_\alpha^{2^k-1}x + e_{F'_\alpha\gamma_{2\mathbb{Z}}(x,\, m)} = F_\alpha^{2^k-1}x' + e_{F'_\alpha\gamma_{2\mathbb{Z}}(x',\, m')}$$

$$\Rightarrow (F_\alpha^{2^k-1}x + e_{F'_\alpha\gamma_{2\mathbb{Z}}(x,\, m)} = F_\alpha^{2^k-1}x' + e_{F'_\alpha\gamma_{2\mathbb{Z}}(x',\, m')})_{\alpha\in I_*}$$

$$\Rightarrow e_{2\mathbb{Z}}(x,\, m) = e_{2\mathbb{Z}}(x',\, m').$$

Therefore $e_{2\mathbb{Z}}$ is well defined.

• Let us verify $e_{2\mathbb{Z}}$ is an $m\Theta$ map.

Let $(x,\, m) \in V(2^k - 1,\, 2\mathbb{Z}) \times V(k,\, 2\mathbb{Z})$.

$$e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k)(x,\, m) = e_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m)$$

$$= (F_\alpha^{2^k-1}(F_\alpha^{2^k-1}x) + e_{F'_\alpha\gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m)})_{\alpha\in I_*}$$

$$= (F_\alpha^{2^k-1}x + e_{F'_\alpha\gamma_{2\mathbb{Z}}(x,\, m)})_{\alpha\in I_*} \quad (\gamma_{2\mathbb{Z}} \text{ is } m\Theta \text{ map}).$$

$$F'_\alpha \circ e_{2\mathbb{Z}}(x,\, m) = F'_\alpha(F_\alpha^{2^k-1}x + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x,\, m))})_{\alpha\in I_*}$$

$$= (F_\alpha^{2^k-1}x + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x,\, m))})_{\alpha\in I_*}.$$

Therefore,

$$e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k) = F'_\alpha \circ e_{2\mathbb{Z}}.$$

(iii) • Let us show that $r_{2\mathbb{Z}}$ is well defined.

Let us suppose that $x = x'$ $(F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x')$ and let us show that $r_{2\mathbb{Z}}x = r_{2\mathbb{Z}}x'$.

Let $\alpha \in I_*$;

$$F_\alpha^{2^k-1}(x) = F_\alpha^{2^k-1}(x') \Rightarrow F_\alpha x_i = F_\alpha x'_i$$

$$\Rightarrow F_\alpha x_i < i >_2 = F_\alpha y_i < i >_2$$

$$\Rightarrow \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 = \sum_{i=1}^{2^k-1} F_\alpha x'_i < i >_2$$

$$\Rightarrow (\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha \in I_*} = (\sum_{i=1}^{2^k-1} F_\alpha x'_i < i >_2)_{\alpha \in I_*}$$

$$\Rightarrow r_{2\mathbb{Z}}(x) = r_{2\mathbb{Z}}(x').$$

Therefore $r_{2\mathbb{Z}}$ is an $m\Theta$ map.

- Let us show that $r_{2\mathbb{Z}}$ is $m\Theta$ map.

Let $x \in V(2^k - 1, 2\mathbb{Z})$, let $\alpha \in I_*$.

$$r_{2\mathbb{Z}} \circ F_\alpha^{2^k-1}(x) = r_{2\mathbb{Z}}(F_\alpha^{2^k-1} x)$$

$$= (\sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1} x)_i) < i >_2)_{\alpha \in I_*}$$

$$= (\sum_{i=1}^{2^k-1} F_\alpha(F_\alpha x_i) < i >_2)_{\alpha \in I_*}$$

$$= (\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha \in I_*};$$

$$F'_\alpha \circ r_{2\mathbb{Z}}(x, m) = F'_\alpha((\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha \in I_*})$$

$$= (\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha \in I_*}.$$

Therefore $r_{2\mathbb{Z}}$ is an $m\Theta$ map.

Proposition 9. $(e_{2\mathbb{Z}}, r_{2\mathbb{Z}})$ *before define in the proposition* 0.8 *is an* $m\Theta$ *steganographic protocols.*

Proof. Let's show that $(e_{2\mathbb{Z}}, r_{2\mathbb{Z}})$ is an $m\Theta$ steganographic protocol. In other words, $r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, m)) = m$, for any $m \in \mathbb{F}_{2\mathbb{Z}}^k$ and for any $x \in V(2^k - 1, 2\mathbb{Z})$.

So, $\forall \alpha \in I_*$, $F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, m))) = F_\alpha^k(m)$.

(1)

$$\begin{aligned} F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, m))) &= r_{2\mathbb{Z}}(F_\alpha^{2^k-1} \circ e_{2\mathbb{Z}}(x, m)) \ (r_{2\mathbb{Z}} \text{ is } m\Theta \text{ map}) \\ &= r_{2\mathbb{Z}}(e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k))(x, m) \ (e_{2\mathbb{Z}} \text{ is } m\Theta \text{ map}) \\ &= r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k m)) \\ &= r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x, m))}), \end{aligned}$$

we put

$$\begin{aligned} j = F'_\alpha(\gamma_{2\mathbb{Z}}(x, m)) &= \gamma_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1}, F_\alpha^k)(x, m) \\ &= \gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x, F_\alpha^k m) \\ &= < F_\alpha^k(F_\alpha^k m) + \sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1}x)_i) < i >_2 >_{10} \\ &= < F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha(F_\alpha x_i) < i >_2 >_{10} \\ &= < F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha(x_i) < i >_2 >_{10}, \end{aligned}$$

then $< j >_2 = F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha(x) < i >_2$ $(*)$.

(2)

$$r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_j) = r_{2\mathbb{Z}}(F_\alpha x_1, F_\alpha x_2, \cdots, F_\alpha x_j + 1, \cdots, F_\alpha x_n)$$

$$= \sum_{i=1,\, i\neq j}^{2^k-1} \{F_\alpha(F_\alpha x_i) < i >_2 + (F_\alpha x_j + 1) < j >_2\}$$

$$= \sum_{i=1,\, i\neq j}^{2^k-1} \{F_\alpha(x_i) < i >_2 + (F_\alpha x_j + 1) < j >_2\}$$

changing $< j >_2$ by expression given in $(*)$ we obtain: $r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_j) = F_\alpha^k m$; so

$$\forall \alpha \in I_*,\ F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, m))) = F_\alpha^k(x, m).$$

Therefore, $r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x, m)) = (x, m)$. Thus $m\Theta$ protocol $F5$ is an $m\Theta$ steganographic protocol.

Remark 3. (1) Insert an $m\Theta$ message s by the $m\Theta$ steganographic protocol $F5$ in an $m\Theta$ covering u consists to change the $m\Theta$ coordinate number $\gamma_{2\mathbb{Z}}(u, s)$.

(2) $m\Theta$ extraction consists to add all products of each α-component, $\forall \alpha \in I_*$, to the value of the $F_{2\mathbb{Z}}$ expression of the index. In other words,

$$r_{2\mathbb{Z}}(u) = \sum_{i=1}^{2^k-1} F_\alpha u_i < i >_2.$$

Example 2. The covering radius of $[2^k - 1, 2^k - k - 1]_{2\mathbb{Z}}$. Hamming codes is one for all integers $k \geq 1$, which can be used to construct a stego-code and embed k bits of $m\Theta$ messages into $2^k - 1$ pixels by partially or totally changing at most one of them. Taking $[7, 4]_{2\mathbb{Z}}$ Hamming code as an example. How to embed $m = 01_{2\mathbb{Z}}1_{2\mathbb{Z}}$ into $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$ by the $m\Theta$ steganographic protocol $F5$.

$$F_1^3 m = 011,\ F_2^3 m = 000,\ F_1^7 x = 1100001,\ F_2^7 x = 0000100.$$

So, how to calculate $e_{2\mathbb{Z}}(01_{2\mathbb{Z}}1_{2\mathbb{Z}},\ 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}})$.

$$\begin{aligned}\gamma_{2\mathbb{Z}}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}},\ 01_{2\mathbb{Z}}1_{2\mathbb{Z}}) &= (< F_1^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) \\ &+ \sum_{i=1}^{7} F_1 x_i < i >_2>_{10},\ < F_2^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) \\ &+ \sum_{i=1}^{7} F_2 x_i < i >_2>_{10}) < F_1^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) \\ &+ \sum_{i=1}^{7} F_1 x_i < i >_2>_{10} = < 011 + 1(001) + 1(010) + 1(111) >_{10} \\ &= 7,\end{aligned}$$

and

$$\begin{aligned}< F_2^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_2 x_i < i >_2>_{10} &= < 000 + 1(101) >_{10} \\ &= 5.\end{aligned}$$

$$\gamma_{2\mathbb{Z}}(x,\ m) = (7;\ 5) = (F_1'(\gamma_{2\mathbb{Z}}(x,\ m));\ F_2'(\gamma_{2\mathbb{Z}}(x,\ m))).$$

$$e_{2\mathbb{Z}}(x,\ m) = (F_1^7 x + e_{F_1'(\gamma_{2\mathbb{Z}}(x,\ m))};\ F_2^7 x + e_{F_2'(\gamma_{2\mathbb{Z}}(x,\ m))}).$$

$$F_1^7 x + e_{F_1'(\gamma_{2\mathbb{Z}}(x,\ m))} = 1100001 + e_7 = 1100001 + 0000001 = 1100000.$$

$$F_2^7 x + e_{F_2'(\gamma_{2\mathbb{Z}}(x,\ m))} = 0000100 + e_5 = 0000100 + 0000100 = 0000000.$$

$$\begin{aligned}e_{2\mathbb{Z}}(x,\ m) &= (1100000,\ 0000000) \\ &= 1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000 \\ &= v.\end{aligned}$$

How to extract the $m\Theta$ message hidden m in the $m\Theta$ message $y = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000$?

In other words, how to calculate $r_{2\mathbb{Z}}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000)$? By applying the second point of the previous remark, we get that

$$r_{2\mathbb{Z}}(y) = (\sum_{i=1}^{7} F_1 y_i < i >_2, \sum_{i=1}^{7} F_2 y_i < i >_2)$$

$$\begin{aligned} r_{2\mathbb{Z}}(y) &= (1(001) + 1(010); 1(000)) \\ &= (011; 000) \\ &= 01_{2\mathbb{Z}}1_{2\mathbb{Z}} \\ &= m. \end{aligned}$$

4.2. The $F5$ $m\Theta$ algorithm

To increase embedding efficiency, the $F5$ algorithm introduces for the first time the concept of matrix embedding technique for embedding in the context of using Hamming codes.

More formally, the desired purpose of the matrix $m\Theta$ embedding technique is to communicate an $m\Theta$ message $m \in V(n-k, p\mathbb{Z})$ through the cover $m\Theta$ vector $x \in V(n, p\mathbb{Z})$, modifying it as little as possible.

The principle is to change the cover $m\Theta$ vector x to stego $m\Theta$ vector y, such that:

$$H(F_\alpha y)_{\alpha \in I_*} = (F_\alpha m)_{\alpha \in I_*},$$

with $H \in \mathcal{M}_{n-k,n}$ the parity check matrix of Hamming $m\Theta$ code. The $m\Theta$ transformation of the cover $m\Theta$ vector x into y is then carried out by seeking the $m\Theta$ vector of modification $e \in V(n, p\mathbb{Z})$:

$$(F_\alpha y)_{\alpha \in I_*} = (F_\alpha (x + e))_{\alpha \in I_*};$$

$$\begin{aligned} H(F_\alpha (x+e))_{\alpha \in I_*} = (F_\alpha m)_{\alpha \in I_*} \Leftrightarrow H(F_\alpha e)_{\alpha \in I_*} \\ = (F_\alpha m)_{\alpha \in I_*} - H(F_\alpha x)_{\alpha \in I_*}. \end{aligned}$$

Example 3. Taking [7, 4] Hamming $m\Theta$ code, we explain how to embed 3 $m\Theta$ bits of $\mathbb{F}_{2\mathbb{Z}}$ into 7 pixels. Let $m = 01_{2\mathbb{Z}}1_{2\mathbb{Z}}$ be the $m\Theta$ message that we want to insert in the cover $m\Theta$ vector $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$. The parity check matrix is therefore in the following form:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

The purpose is to find the α-vector $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$ such that $H(x + e) = m$.

Otherwise,

$$\begin{cases} F_1(m) = 011, \quad F_2(m) = 000, \\ F_1(x) = 1100001, \quad F_2(x) = 0000101. \end{cases}$$

So,

$$F_1(m) - H \times F_1(x) = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Thus, the modification α-vector is $F_1(e) = (0, 0, 0, 0, 0, 0, 1)$.

$$F_2(m) - H \times F_2(x) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

Thus, $F_2(e) = (0, 1, 0, 0, 0, 0, 0)$.

$$e = (F_1(e),\ F_2(e)) = (0,\ 3_{2\mathbb{Z}},\ 0,\ 0,\ 0,\ 0,\ 1_{2\mathbb{Z}}).$$

The cover $m\Theta$ vector x is then transformed into

$$y = x + e = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}} + 03_{2\mathbb{Z}}00001_{2\mathbb{Z}}$$

$$= 1_{2\mathbb{Z}}0003_{2\mathbb{Z}}00.$$

We have the cover $m\Theta$ vector $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$ and the stego $m\Theta$ vector $y = 1_{2\mathbb{Z}}0003_{2\mathbb{Z}}00$. When embedding m into x, it appears that 2 pixels of x have been partially damaged, namely the second and the last component of x. Indeed,

$$\begin{cases} 1_{2\mathbb{Z}} = (F_\alpha 1_{2\mathbb{Z}})_{\alpha \in I_*} = (F_1 1_{2\mathbb{Z}},\ F_2 1_{2\mathbb{Z}}) = (1, 0), \\ 0 = (F_\alpha 0)_{\alpha \in I_*} = (F_1 0,\ F_2 0) = (0, 0). \end{cases}$$

The passage from $1_{2\mathbb{Z}}$ to 0 shows that the pixels has been partially damaged.

5. Conclusion

This note shows that the Hamming $m\Theta$ code is an $\mathbb{F}_{2\mathbb{Z}}$-vector subspace of $V(n, 2\mathbb{Z})$ of dimension n. We have seen that there exists a close relation between the $m\Theta$ protocols $F5$ and the Hamming $m\Theta$ code. The embedding of an $m\Theta$ message of k bits into the cover $m\Theta$ vector of n pixels changes at the level of the α-modalities because it partially or totally damages at most one pixel of the cover $m\Theta$ vector.

References

[1] F. Ayissi Eteme, *chrm*Θ Introducing Pure and Applied Mathematics, Lambert Academic Publishing Saarbruken, Germany, 2015.

[2] J. A. Tsimi and Rose C. Youdom, The modal Θ-valent extensions of BCH codes, Journal of Information and Optimization Sciences 42(8) (2021), 1723-1764.

DOI: https://doi.org/10.1080/02522667.2021.1914364

[3] J. A. Tsimi and Pemha B. G. Cedric, A $m\Theta$ spectrum of Reed-Muller codes, Journal of Discrete Mathematical Sciences and Cryptography 25(6) (2022), 1791-1807.

DOI: https://doi.org/10.1080/09720529.2020.1814489

[4] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, Information hiding: A survey, Proceedings of the IEEE 87(7) (1999), 1062-1078.

DOI: https://doi.org/10.1109/5.771065

[5] F. A. Eteme and J. A. Tsimi, A $m\Theta$ approach of the algebraic theory of linear codes, Journal of Discrete Mathematical Sciences and Cryptography 14(6) (2011), 559-581.

DOI: https://doi.org/10.1080/09720529.2011.10698356

[6] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz and S. Pogreb, Applications for data hiding, IBM Systems Journal 39(3-4) (2000), 547-568.

DOI: https://doi.org/10.1147/sj.393.0547

[7] F. Ayissi Eteme, Logique et Algèbre de Structure Mathématiques Modales Θ-valentes Chrysippiennes, Edition Hermann, Paris, 2009.

[8] F. Ayissi Eteme, Complétion chrysippienne d'une algèbre de Lukasiewicz Θ-valent, CRAS Paris, 299, Série 1(3) (1984), pp. 69-72.

[9] R. Crandall, Some Notes on Steganography, 1998.

[10] A. Westfeld, F5–A Steganographic Algorithm: High Capacity Despite Better Steganalysis, in: Lecture Notes in Computer Science, Volume 2137, Springer, New York, 2001, pp. 289-302.

DOI: https://doi.org/10.1007/3-540-45496-9_21

[11] F. A. Eteme and J. A. Tsimi, A modal Θ-valent approach of the notion of code, Journal of Discrete Mathematical Sciences and Cryptography 14(5) (2011), 445-473.

DOI: https://doi.org/10.1080/09720529.2011.10698348

[12] J. A. Tsimi and Pemha B. G. Cedric, On a decoding algorithm of $m\Theta$ Reed-Muller codes, Journal of Discrete Mathematical Sciences and Cryptography, 2021.

DOI: https://doi.org/10.1080/09720529.2021.1920189

[13] J. A. Tsimi and Pemha B. G. Cedric, On the generalized modal Θ-valent Reed-Muller codes, Journal of Information and Optimization Sciences 42(8) (2021), 1885-1906.

DOI: https://doi.org/10.1080/02522667.2021.1961977

[14] F. Ayissi Eteme, Anneau chrysippien Θ-valent, CRAS, Paris 298, Série 1 (1984), pp.1-4.

■