UNIVERSITÉ DE YAOUNDÉ 1

ÉCOLE NORMALE SUPÉRIEURE DE YAOUNDÉ

Département de Mathématiques

Mémoire de DIPES 2

GRAPHES

ET
CODES LINÉAIRES

Soutenu et présenté par :

EBANDA EBANDA Junior Lebon

Matricule : **14y122**

Licence en Mathématiques

Sous la direction de :

Pr. MOUAHA Christophe

Maître de conférences

École Normale Supérieure, Université de Yaoundé 1

*Année Académique :***2018-2019**

♣ Dédicace ♣

Je dédie ce mémoire à :

ma mère Mme KUM Suzanne OWU épouse EBANDA.

♣ Remerciements ♣

Je remercie le Dieu tout puissant pour la protection et tous les autres bienfaits.

Je remercie également :

♡ Le professeur **MOUAHA Christophe** d'avoir accepté de diriger ce travail et de créer autour de moi un cadre de recherche serein par ses conseils, ses encouragements et son soutien permanent.

♡ Mes parents M.**EBANDA NKOU Hyacinth** et Mme.**KUM Suzanne OWU**, mes oncles et tantes pour le soutien moral et financier continu que j'ai reçu de leur part pendant ces cinq dernières années.

♡ La famille **MVONDO** pour son accueil, son soutien et sa gentillesse.

♡ Tous les enseignants du département de mathématiques pour nous avoir transmis leurs savoirs tout au long de cette formation.

♡ Mes camarades de promotion pour la solidarité, les bonnes relations et surtout l'esprit d'équipe que nous avons cultivé pendant toutes ces dernières années.

♣ Déclaration sur l'honneur ♣

Le présent document est une œuvre originale du candidat et n'a été soumis nulle part ailleurs en partie ou en totalité, pour une évaluation académique. Les contributions externes ont été dûment mentionnées et recensées en bibliographie.

Signature du candidat

EBANDA EBANDA Junior Lebon.

♣ Résumé ♣

Les codes linéaires construits dans le cadre de ce travail sont des codes binaires systématiques $(I_n|\overline{A})$ *où* $\overline{A}$ *est la matrice obtenue de la matrice d'adjacence d'un graphe à* n *sommets. Ils corrigent une seule erreur car leur distance minimale est égale à* 3*.*

Mots clés : Codes linéaires ; graphes bipartis ; matrice génératrice ; matrice d'adjacence ; distance minimale.

♣ Abstract ♣

The linear codes built here are systematic binary codes $(I_n|\overline{A}(G))$. $\overline{A}(G)$ *is the matrix obtained to the adjacency matrix of a biparti graph. These codes correct only one error because thier minimun ditance is* 3.

Keys words : Linear codes ; bipartis graphs ; generator matrix ;adjacency matrix ; minimun distance.

♣ Table des matières ♣

♣ Introduction ♣

La communication est le fait qu'un expéditeur envoie un message à un récepteur, elle a évolué avec l'avènement des TIC notamment avec l'apparition des ordinateurs et de l'internet. Malgré le fait que les TIC ont amélioré la qualité de la communication, elles ont aussi apporté des problèmes à l'instar des virus et des pirates informatiques qui sont à l'origine des erreurs de communication.

La théorie des graphes est une branche des mathématiques discrètes utilisée dans de nombreux domaines tels que le transport, l'architecture et permet de modéliser plusieurs situations de vie. Elle a tardivement reçu une attention soutenue de la part de la communauté mathématique. Les premiers développements majeurs de cette théorie datent du milieu du vingtième siècle avec l'apparition d'un des premiers ouvrages traitant de la théorie des graphes ``*Théorie der endlichen und unendlichen graphen* ´´écrit par König [10] . Depuis cette époque, la théorie des graphes s'est largement développée. Nous présenterons dans ce mémoire le lien qui existe entre cette théorie et la théorie des codes.

La théorie des codes est un domaine qui a pour but de transmettre, de stocker et de sécuriser les données numériques contre les ennemis. Ces opérations rencontrent des difficultés dûs à des raisons diverses à l'instar des poussières ou des rayures qui dégradent les données contenues sur un disque BLU-RAY et des perturbations électromagnétiques qui détériorent les données dans les communications satellitaires et téléphoniques. Pour résoudre ce problème, de nombreux mathématiciens à l'instar de Claude SHANNON, Richard HAMMING [3] ont mis sur pieds des dispositifs de correction (codes correcteurs d'erreurs). La correction d'erreurs est directement lié à la distance minimale car un code qui a une grande distance minimale corrige plusieurs erreurs. Nous allons présenter une approche de construction des codes linéaires à partir des graphes bipartis et regarder leurs distance minimale.

L'organisation de notre travail est la suivante :

– Le premier chapitre présente les structures algébriques : anneaux, corps, espaces vecto-

riels et matrices.

- Le deuxième chapitre se concentre sur les graphes plus précisément les graphes bipartis.
- Le chapitre trois concerne les codes linéaires sur les corps de Galois.
- Le dernier chapitre sera consacré à la construction des codes linéaires à partir des graphes bipartis.

⋆ ⋆ CHAPITRE UN ⋆ ⋆

PRÉLIMINAIRES

1.1 STRUCTURES ALGÉBRIQUES

Dans ce chapitre, nous rappelons quelques notions sur les anneaux, les corps, les espaces vectoriels et les matrices.

1.1.1 Anneaux et Corps

Anneaux

Définition 1.1.1. Un anneau est un triplet $(A, +, \cdot)$ où A est un ensemble non vide, $+$ et $\cdot$ sont des lois de composition interne dans A vérifiant les propriétés suivantes :

P_1) $(A, +)$ est un groupe commutatif (dont l'élément neutre est noté 0_A).

P_2) La loi $\cdot$ est associative et distributive par rapport à $+$, c'est-à-dire :

$\forall (a, b, c) \in A^3$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ et $a \cdot (b + c) = a \cdot b + a \cdot c$; $(b + c) \cdot a = b \cdot a + c \cdot a$.

Si la loi $\cdot$ admet un élément neutre noté 1_A l'anneau est dit unitaire.

Si la loi $\cdot$ est commutative l'anneau est commutatif ou abélien.

Dans la suite, sauf mention du contraire A est un anneau commutatif et unitaire.

Définition 1.1.2. Soit B un sous-ensemble non vide de A.

On dit que B est un sous-anneau si la restriction des lois de l'anneau A à B confère à B une structure d'anneau (c'est-à-dire $(B, +, \cdot)$ est un anneau).

Proposition 1.1.1. Soit B un sous-ensemble non vide de A, alors les propriétés suivantes sont équivalents :

1. B est un sous-anneau de A.
2. $\forall (x, y) \in B^2, x - y \in B$ et $xy \in B$.

Preuve . Voir[9]

Définition 1.1.3. Soient x et y dans A avec $x \neq 0_A$. On dit que x divise y s'il existe un élément z de A tel $y = zx$.

Définition 1.1.4. Un élément x de A est dit inversible dans A s'il est un diviseur de l'unité de l'anneau A. Autrement dit, un élément x de A est dit inversible dans A s'il existe un élément y de A tel que $xy = 1_A$. L' élément y est appelé l'inverse de x.

Proposition 1.1.2. Soit x un élément de A. Si x est inversible, alors son inverse est unique.

Preuve . Supposons que x_1 et x_2 sont des inverses de x ; alors $xx_1 = xx_2 = 1_A$, ce qui implique que

$$x_1xx_1 = x_1xx_2 = 1_A \text{ d'où } x_1 = x_2.$$

Définition 1.1.5. Soit x un élément non nul de A. On dit que x est un diviseur de zéro s'il existe un élément non nul y de A tel que $xy = 0$

Définition 1.1.6. L'anneau A est dit intègre lorsqu'il n'a pas de diviseurs de zéro.

$$\text{C'est-à-dire : } \forall x, y \in A,\ xy = 0 \Longrightarrow (x = 0 \text{ ou } y = 0).$$

Définition 1.1.7. Soit I un sous-groupe additif de A, on dit que I est un idéal si

$$\forall (a, i) \in A \times I,\ ai \in I \text{ et } ia \in I.$$

Définition 1.1.8. Soit $X \subseteq A$.
L'idéal engendré par X noté (X) est l'intersection de tous les idéaux contenant X.

Définition 1.1.9. A est dit principal si tout idéal de A est engendré par un élément de A.

Proposition 1.1.3. Soit A un anneau unitaire d'élément unité 1_A, alors l'application

$$\begin{array}{rccc} \psi : & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & n \cdot 1_A \end{array}$$

est un morphisme d'anneaux.

Preuve . En effet, pour $n, m \in \mathbb{Z}$,

$$\begin{aligned} \psi(n+m) &= (n+m)\cdot 1_A \\ &= n\cdot 1_A + m\cdot 1_A \\ &= \psi(n)+\psi(m) \end{aligned}$$

et

$$\begin{aligned} \psi(nm) &= (nm)1_A \\ &= (n\cdot 1_A)(m\cdot 1_A) \\ &= \psi(n)\psi(m) \end{aligned}$$

D'où le résultat.

Remarque 1.1.1. Si ψ est non injectif, alors $Ker\psi$ est un idéal propre de $\mathbb{Z}$. $\mathbb{Z}$ étant principal, $Ker\psi$ est de la forme $m\mathbb{Z}$ où m est un entier naturel non nul.

Définition 1.1.10.

1. Si $Ker\psi = 0$, on dit que A est de caractéristique nulle.
2. Si $Ker\psi = m\mathbb{Z}$, $(m \in \mathbb{N}^*)$ on dit que A est de caractéristique m.

Corps

Définition 1.1.11. Un corps est anneau unitaire dans lequel tout élément non nul est inversible.
Un corps commutatif est un anneau commutatif unitaire dans tout élément non nul est inversible.

Définition 1.1.12. Soit L une partie non vide de $\mathbb{K}$.
L est un sous-corps de $\mathbb{K}$ si la restriction des lois de $\mathbb{K}$ à L lui confère une structure de corps ; c'est-à-dire :

1. $\forall$ (a,b) $\in L^2$, a-b $\in L$.
2. $\forall$ (a,b) $\in L^2$, a.b $\in L$.
3. $\forall$ a $\in L$ $a \neq 0$, $a^{-1} \in L$.

Définition 1.1.13. Un corps fini est un corps qui a un nombre fini d'éléments fini.
On l'appelle aussi corps de Galois.

Proposition 1.1.4. Tout corps est un anneau intègre.

Preuve . Soient $\mathbb{K}$ un corps, $x, y \in \mathbb{K}$ tels que $x \neq 0$ et $xy = 0$.

Alors $y = 1_A \cdot y = (xx^{-1})y = x^{-1}(xy) = x^{-1}0 = 0$.

D'où $\mathbb{K}$ est intègre.

Théorème 1.1.1. (théorème de Wedderburn)

Tout corps fini est commutatif.

Proposition 1.1.5. La caractéristique d'un corps fini est un nombre premier.

Preuve . Soit $\mathbb{K}$ un corps fini de caractéristique m.

Comme le corps $\mathbb{K}$ a un nombre fini d'éléments, le morphisme ψ ne peut être injectif, donc son noyau est distinct de l'idéal nul. Ainsi, m est un entier naturel non nul. De plus m est distinct de 1 (car si $m = 1$, alors on a : $Ker\psi = \mathbb{Z}$ ce qui est absurde). Supposons que m n'est pas premier, alors il existe deux entiers p et q non nuls et tous distincts de 1 tels que $m = pq$. Puisque p et q sont non nuls et strictement inférieurs à m, $p1_{\mathbb{K}}$ et $q1_{\mathbb{K}}$ sont deux éléments non nuls de $\mathbb{K}$.

On a :

$$(p \cdot 1_{\mathbb{K}})(q \cdot 1_{\mathbb{K}}) = (p \cdot q)1_{\mathbb{K}} = m \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}.$$

Ce qui contredit le fait que le corps $\mathbb{K}$ soit intègre. D'où m est premier.

Proposition 1.1.6. Le cardinal d'un corps fini est une puissance de sa caractéristique.

Proposition 1.1.7. Soit $(\mathbb{K}, +, \cdot)$ un corps.

Alors $\mathbb{K}$ ne possède pas d'idéaux non triviaux.

Preuve . Soit I un idéal de K.

Si I$\neq \{0_K\}$ alors il existe $a \in I$ tel que a$\neq 0_K$.

Mais $a \in K \setminus \{0\}$ et donc a^{-1} existe dans K.

Ainsi $aa^{-1} = a^{-1}a = 1_K \in I$ car I est un idéal de K. Pour tout $x \in K$, on a :$x = 1_K.x \in I$ c'est-à-dire $K \subseteq I$ d'où $I = K$.

Proposition 1.1.8. Soit $p \in \mathbb{N}$ avec $p \geq 2$.

$$\mathbb{Z}/p\mathbb{Z} \text{ est un domaine d'intégrité} \Longleftrightarrow p \text{ premier.}$$

Preuve .

Supposons que $\mathbb{Z}/p\mathbb{Z}$ est un domaine d'intégrité et que p non premier. p non premier entraine qu'il existe $p_1, p_2 \in \mathbb{N},\ 1 < p_1 < p$ et $1 < p_2 < p$ tels que $p = p_1p_2$ alors $\overline{p} = \overline{0} = \overline{p_1p_2} = \overline{p_1}.\overline{p_2}$

où $\forall i \in \{1,2\}$, $\overline{p_i} = p_i + p\mathbb{Z}$. On a $\overline{p_1}, \overline{p_2} \in \mathbb{Z}/p\mathbb{Z}$ et $\overline{p_1}.\overline{p_2} = \overline{0}$ ce qui est absurde car $\mathbb{Z}/p\mathbb{Z}$ est sans diviseur de zéro d'où p est premier.

Réciproquement supposons que soit p premier.

Pour montrer que $\mathbb{Z}/p\mathbb{Z}$ est un domaine d'intégrité, il suffit de montrer que $\mathbb{Z}/p\mathbb{Z}$ est sans diviseurs de zéro. Soit $\overline{p}_1, \overline{p}_2 \in \mathbb{Z}/p\mathbb{Z}$ tel que :$\overline{p_1 p_2} = \overline{0}$

$$\begin{aligned} \overline{p_1 p_2} = \overline{0} &\implies p | p_1 p_2 \\ &\implies p | p_1 \ ou \ p | p_2 \\ &\implies \overline{p}_1 = \overline{0} \ ou \ \overline{p}_2 = \overline{0} \end{aligned}$$

D'où le résultat.

Proposition 1.1.9. Tout domaine d'intégrité fini est un corps.

Preuve . Soit K un domaine d'intégrité fini.

En supposant que K possède n éléments, posons $K = \{0, 1, k_3, k_4, k_5, \ldots, k_n\}$.

Soit $u \in K$, $u \neq 0$ alors $uK = \{0, u, uk_3, uk_4, \ldots, uk_n\}$.

$uk_i = uk_j$ si et seulement si $k_i = k_j$; donc tous les éléments de uK sont distincts.

Ainsi uK possède aussi n éléments et de plus, comme $uK \subseteq K$ alors $uK = K$.

$1_K \in K = uK$ par conséquent il existe $u' \in K$ tel que $1_K = uu' = u'u$ ainsi u est inversible, c'est-à-dire tout élément non nul de K est inversible d'où K est un corps.

Proposition 1.1.10. Soit $p \in \mathbb{N}$ avec $p \geq 2$

$$\mathbb{Z}/p\mathbb{Z} \text{ est corps} \iff p \text{ est premier.}$$

Preuve . Supposons que p soit un nombre entier premier.

$$\begin{aligned} ppremier &\implies \mathbb{Z}/p\mathbb{Z} \text{ est un domaine d'intégrité.} \\ &\implies \mathbb{Z}/p\mathbb{Z} \text{ est un corps car } \mathbb{Z}/p\mathbb{Z} \text{ est fini.} \end{aligned}$$

$\mathbb{Z}/p\mathbb{Z}$ est donc un domaine d'intégrité fini c'est-à-dire un corps.

Réciproquement supposons que $\mathbb{Z}/p\mathbb{Z}$ soit un corps.

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z}\text{corps} &\implies \mathbb{Z}/p\mathbb{Z} \text{ est un domaine d'intégrité} \\ &\implies \text{p est premier} \end{aligned}$$

1.1.2 Espaces vectoriels

Dans toute cette partie $\mathbb{K}$ désigne un corps commutatif.

Définition 1.1.14. On appelle $\mathbb{K}$-espace vectoriel tout ensemble E muni d'une loi notée $+$ et d'une loi externe $\cdot$

$$\begin{array}{ccccc} \cdot & K \times E & \longrightarrow & E \\ & (\lambda, x) & \longmapsto & \lambda \cdot x \end{array}$$ telles que :

1. $(E, +)$ est un groupe abélien
2. $\forall\, (\lambda, \mu) \in \mathbb{K}, \forall x \in E$
   $(\lambda + \mu)x = \lambda x + \mu x$
3. $\forall \lambda \in \mathbb{K}, \forall (x, y) \in E^2$
   $\lambda(x + y) = \lambda x + \lambda y$
4. $\forall (\lambda, \mu) \in \mathbb{K}^2, \forall x \in E, \lambda(\mu x) = (\lambda\mu)x$
5. $\forall x \in E, 1_{\mathbb{K}} x = x.$

Dans la suite $\mathbb{K}$-ev désignera $\mathbb{K}$-espace vectoriel.

Définition 1.1.15. Soient E un $\mathbb{K}$-ev, Fune partie non vide de E.

On dit que F est un sous-espace vectoriel de E si et seulement si :

1. $F \neq \emptyset$.
2. $\forall (x, y) \in F^2$ et $\forall \lambda \in \mathbb{K}, x + \lambda y \in F$.

Définition 1.1.16. Soient E un $\mathbb{K}$-ev, $n \in \mathbb{N}^*$ et $(e_1, \ldots, e_n) \in E^n$.

1. On dit que la famille finie $(e_1, \ldots, e_n)$ est liée si et seulement si
   $$\exists (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n - \{(0, \ldots, 0)\}, \textstyle\sum_{i=1}^n \lambda_i e_i = 0.$$
2. On dit que la famille finie $(e_1, \ldots, e_n)$ est libre si et seulement si elle n'est pas liée, c'est-à-dire
   $$\forall (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n,$$
   $$\textstyle\sum_{i=1}^n \lambda_i e_i = 0 \Longrightarrow (\forall i \in \{1, \ldots, n\},\ \lambda_i = 0).$$

Définition 1.1.17. (En dimension finie)

Une famille de vecteurs $\{e_1, \ldots, e_n\}$ d'un espace vectoriel E est dite génératrice si

$$\forall x \in E, \exists\, (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n \text{ tel que } x = \textstyle\sum_{i=1}^n \lambda_i e_i.$$

Définition 1.1.18. On dit qu'une famille $\mathcal{B}$ d'éléments d'un $\mathbb{K}$-ev est une base de E si $\mathcal{B}$ est une famille libre et génératrice de E.

Proposition 1.1.11. Une famille finie $\mathcal{B} = (e_1, \ldots, e_n)$ d'éléments d'un $\mathbb{K}$-ev E est une base si et seulement si

$$\forall x \in E \ \exists!(x_1, \ldots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^{n} x_i e_i.$$

Preuve .

Supposons que $\mathcal{B} = (e_1, \ldots, e_n)$ soit une base de E.soit $x \in E$

$$x \in E \implies \exists(x_1, \ldots, x_n) \in \mathbb{K}^n \setminus x = \sum_{i=1}^{n} x_i e_i$$

Supposons qu'il existe $(y_1, \ldots, y_n) \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^{n} y_i e_i$.

$$\begin{aligned} x = \sum_{i=1}^{n} y_i e_i &\implies \sum_{i=1}^{n} (x_i - y_i) e_i = 0 \\ &\implies \forall i \in \{1, \ldots, n\}, \ x_i - y_i = 0 \text{ car } \mathcal{B} \text{ une famille libre de } E \\ &\implies \forall i \in \{1, \ldots, n\}, \ x_i = y_i \end{aligned}$$

Ce qui prouve l'unicité.

Réciproquement supposons $\forall x \in E \ \exists!(x_1, \ldots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^{n} x_i e_i$.

Par hypothèse, $\mathcal{B} = (e_1, \ldots, e_n)$ est déjà une famille génératrice car tout élément de E s'écrit comme combinaison linéaire d'éléments de $\mathcal{B}$.

soit $(x_1, \ldots, x_n) \in \mathbb{K}^n$ tel que $\sum_{i=1}^{n} x_i e_i = 0$

$$\begin{aligned} \sum_{i=1}^{n} x_i e_i = 0 &\implies \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} 0 e_i \\ &\implies x_1 = x_2 = \cdots = x_n = 0 \text{ par unicité de la décomposition} \end{aligned}$$

D'où$\mathcal{B} = (e_1, \ldots, e_n)$ est une famille libre de E et par conséquent une base de E.

Proposition 1.1.12. Soient E un $\mathbb{K}$-ev de dimension finie $n \in \mathbb{N}^*$ et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E, l'application φ définie par

$$\begin{aligned} \varphi : \ E &\longrightarrow \mathbb{K}^n \\ x &\longmapsto (x_1, \ldots, x_n) \end{aligned}$$

est un isomorphisme d'espaces vectoriels.

Preuve . Soit $(x, y) \in E^2$ tel que $\varphi(x) = \varphi(y)$.

$$\begin{aligned} \varphi(x) = \varphi(y) &\implies (x_1, \ldots, x_n) = (y_1, \ldots, y_n) \\ &\implies \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} y_i e_i \\ &\implies x = y \end{aligned}$$

d'où φ est injective.

Soit $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$, posons $y = \sum_{i=1}^{n} \alpha_i e_i$, on a $y \in E$ et $\varphi(y) = (\alpha_1, \ldots, \alpha_n)$ d'où φ est surjective. Ce qui permet de conclure que φ est bijective.

Soient x et y dans E et $\lambda \in \mathbb{K}$,

$$\begin{aligned} \varphi(x + \lambda y) &= (x_1 + \lambda y_1, x_2 + \lambda y_2, \ldots, x_n + \lambda y_n) \\ &= (x_1, x_2, \ldots, x_n) + \lambda(y_1, y_2, \ldots, y_n) \\ &= \varphi(x) + \lambda\varphi(y) \end{aligned}$$

d'où φ est un isomorphisme de $\mathbb{K}$ espaces vectoriels .

Proposition 1.1.13. Si $\mathbb{K}$ est un corps fini et E un $\mathbb{K}$-ev de dimension finie n, on a

$$card(E) = (card\ \mathbb{K})^n$$

Preuve . D'après la proposition précédente E est isomorphe à $\mathbb{K}^n$ d'où $card(E) = (card\ \mathbb{K})^n$

1.2 CALCUL MATRICIEL

Soient $n, p \in \mathbb{N}^*$ et $\mathbb{K}$ un corps.

Définition 1.2.1.

1. On appelle matrice à n lignes , p colonnes et à éléments (ou coefficients ou termes) dans $\mathbb{K}$ toute application de $\{1, \ldots, n\} \times \{1, \ldots, p\}$ dans $\mathbb{K}$ définie par :

$$\begin{aligned} A : \ \{1, \ldots, n\} \times \{1, \ldots, p\} &\longrightarrow \mathbb{K} \\ (i, j) &\longmapsto a_{ij} \end{aligned}$$

On note cette application sous forme de tableau par

$$A = (a_{ij})_{1 \le i \le n, 1 \le j \le p} = (a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1p} \\ a_{21} & a_{22} & \ldots & a_{2p} \\ \vdots & \vdots & \ldots & \vdots \\ \vdots & \vdots & \ldots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{np} \end{pmatrix}$$

2. $M_{n,p}(\mathbb{K})$ désigne l'ensemble des matrices de taille $n \times p$ sur $\mathbb{K}$.
3. Une matrice est dite carrée lorsque $n = p$.

Définition 1.2.2.

1. Addition

   Soient $A = (a_{ij})_{ij}$ et $B = (b_{ij})_{ij}$ deux matrices de même taille $n \times p$. $A + B$ est la matrice de taille $n \times p$ définie par :

   $A + B = (a_{ij} + b_{ij})_{ij}$.

2. Multiplication par un scalaire.

   Soit $A = (a_{ij})_{ij}$ une matrice et $\lambda \in \mathbb{K}$ le produit de A par λ est la matrice définie par :

   $\lambda A = (\lambda a_{ij})_{ij}$.

3. Produit

   Soient A et B deux matrices de taille $n \times p$ et $p \times q$ respectivement. Le produit de A par B est la matrice définie par :

   $AB = (c_{ik})_{ik}$ avec $c_{ik} = \sum_{j=1}^{p} a_{ij} b_{jk}$

Définition 1.2.3.

Soit A une matrice

$$A = a_{ij})_{ij} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{pmatrix} \text{ de } M_{n,p}(\mathbb{K}),$$

on appelle transposée de A la matrice notée ${}^tA$ de $M_{p,n}(\mathbb{K})$ définie par :

$$\begin{aligned} {}^tA &= (a_{ij})_{ji} \\ &= \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ a_{1p} & a_{2p} & \dots & a_{np} \end{pmatrix} \end{aligned}$$

Proposition 1.2.1.

1. $\forall\, A \in M_{n,p}(\mathbb{K})$, ${}^t({}^tA) = A$.

2. $\forall \alpha \in \mathbb{K}, \forall (A,B) \in (M_{n,p}(\mathbb{K}))^2,\ {}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB$
3. $\forall A \in M_{n,p}(\mathbb{K}), \forall B \in M_{p,q}(\mathbb{K}),\ {}^t(AB) = {}^tB\, {}^tA$

Preuve .

1. Immédiat
2. En notant $A = (a_{ij})_{ij}$ et B=$(b_{ij})_{ij}$ on a $\alpha A + B = (\alpha a_{ij} + b_{ij})_{ij}$
   donc ${}^t(\alpha A + B) = (\alpha a_{ij} + b_{ij})_{ij}$ et

$$\begin{aligned} \alpha {}^tA + {}^tB &= \alpha (a_{ij})_{ij} + (b_{ij})_{ij} \\ &= (\alpha a_{ij} + b_{ij})_{ij} \end{aligned}$$

   d'où ${}^t(\alpha A + B) = \alpha\, {}^tA + {}^tB$
3. En posant A=$(a_{ij})_{ij}$, B=$(b_{jk})_{jk}$ on a ${}^tA = (\alpha_{ij})_{ji}$ et ${}^tB = (\beta_{ij})_{kj}$
   où $\alpha_{ji} = a_{ij}$ et $\beta_{kj} = b_{ik}$ et $AB = (c_{ik})_{ik}$,${}^tB{}^tA = (\gamma_{ki})_{ki}$ avec
   $c_{ik} = \sum_{j=1}^{p} a_{ij}b_{jk}$ et $\gamma_{ki} = \sum_{j=1}^{p} \beta_{kj}\alpha_{ji} = \sum_{j=1}^{p} b_{jk}a_{ij} = c_{ik}$ ainsi
   ${}^tB\, {}^tA = {}^t(AB)$

⋆ ⋆ CHAPITRE DEUX ⋆ ⋆

GRAPHES

2.1 Généralités

2.1.1 Définitions

Définition 2.1.1. [1] Soient V un ensemble (fini ou non) et E une partie de $V \times V$.

- On appelle graphe la donnée du couple (V, E) et on note $G = (V, E)$.
- Les éléments de V sont appelés les sommets ou nœuds de G .
- Les éléments de E sont appelés les arcs ou les arêtes de G.
- Le graphe est fini lorsque V est fini non vide.

Définition 2.1.2. Soient I un ensemble d'indices, $U = \{v_i | i \in I\}$ et $a = (v_i, v_j) \in E$ avec $i, j \in I$

- v_i est appelé origine de l'arc a, v_j est appelé destination de l'arc a.
- L'arc a est appelé boucle lorsque $v_i = v_j$.

Définition 2.1.3. Soient $G = (V, E)$ et $H = (F, D)$ deux graphes.

Le graphe $H = (F, D)$ est un sous-graphe de G si :

1. $F \subseteq V$
2. $D \subseteq E \cap (F \times F)$.

Définition 2.1.4. Dans le cas où G est un graphe fini :

- Le demi-degré sortant d'un sommet v noté $d^+(v)$ est le nombre d'éléments de $w^+(v)$.
- Le demi-degré entrant d'un sommet v noté $d^-(v)$ est le nombre d'éléments de $w^-(v)$.
- Le degré d'un sommet v noté $d(v)$ est défini par $d(v) = d^-(v) + d^+(v)$

Exemple 2.1.1. Considérons le graphe $G = (V, E)$ où $V = \{a, b, c, d\}$ et $E = \{(a, b), (a, c), (d, d), (b, d), (c, d), (b, a)\}$ alors :

1. $w^+(a)$=$\{(a,b),(a,c)\}$ et $d^+(a)=2$
2. $w^+(b)$=$\{(b,d),(b,a)\}$ et $d^+(b)=2$
3. $w^-(b)$=$\{(a,b)\}$ et $d^-(b)$=1. On obtient $d(b)=3$.
   le graphe $H=(F,D)$ avec $F=\{a,b,c\}$ et $D=\{(a,b),(a,c),(b,a)\}$ est un sous-graphe de G.

Lemme 2.1.1. Soit $G=(V,E)$ un graphe orienté et fini, alors les $w^+(v)$ $v\in N$ et les $w^-(v)$ $v\in M$ (où $N=\{v\in V/\exists x\in V,(v,x)\in E\}$ et M=$\{v\in V/\exists x\in V,(x,v)\in E\}$) forment chacun une partition de E.

Preuve.
1. Soit $v\in N$ alors il existe $x\in V$ tel que $(v,x)\in E$ d'où $w^+(v)\neq\emptyset$.
2. Soit $u,v\in N$ supposons que $w^+(v)\bigcap w^+(u)\neq\emptyset$. Soit alors $(x,y)\in w^+(v)\bigcap w^+(u)$ on a $(x,y)=(v,a)=(u,b)$ avec $a,b,y\in V$ c'est-à-dire $v=x=u$ et $a=y=b$ d'où $u=v$
3. Soit $v\in N$ on a $w^+(v)\subset E$ donc $\bigcup_{u\in N}w^+(u)\subseteq E$. Soit $(a,b)\in E$ alors $(a,b)\in w^+(a)$ et $a\in N$ d'où $E=\bigcup_{u\in N}w^+(u)$; De même on montre que $E=\bigcup_{v\in M}w^-(v)$.

Proposition 2.1.1. Si $G=(V,E)$ est un graphe orienté et fini alors :

1. $\sum_{v\in V}d^+(v)$=$\sum_{v\in V}d^-(v)$=$|E|$.
2. $\sum_{v\in V}d(v)=2|E|$.

Preuve.
1. D'après le lemme 2.1.1 on a $E=\bigcup_{v\in M}w^-(v)$=$\bigcup_{u\in N}w^+(u)$ d'où $\sum_{v\in V}d^-(v)=\sum_{v\in V}d^+(v)=|E|$.
2. Soit $v\in V$ on a d(v)=$d^+(v)+d^-(v)$ donc

$$\begin{aligned}\sum_{v\in V}d(v) &= \sum_{v\in V}d^+(v)+\sum_{v\in V}d^-(v)\\ &= |E|+|E|\\ &= 2|E|.\end{aligned}$$

Définition 2.1.5. Un multi-ensemble est un ensemble au sein duquel un même élément est répété plus d'une fois.

Définition 2.1.6. Un multi-graphe $G=(V,E)$ est un graphe pour lequel l'ensemble E des arcs est un multi-ensemble.

Exemple 2.1.2. Posons $V = \{v_1, v_2, v_3, v_4\}$ et $E = \{(v_1, v_2), (v_1, v_2), (v_2, v_4), (v_3, v_2)\}$ alors $G = (V, E)$ est un multi-graphe.

Dans ce type de graphe on peut trouver plusieurs arcs reliant deux sommets donnés.

Remarque 2.1.1. Un multi-graphe $G = (V, E)$ est fini si V et E sont finis.

Définition 2.1.7. Soit $p \geq 1$.Un p-graphe est un multi-graphe $G = (V, E)$ pour lequel tout arc de E est répété au plus p fois.

Définition 2.1.8. Un graphe $G = (V, E)$ est dit simple (ou strict) s'il ne s'agit pas d'un multi-graphe et E est irréflexif c'est -à-dire que quelque soit $v \in V$, (v, v) n'appartient pas à E.

Exemple 2.1.3. Soient $V = \{v_1, v_2, v_3\}$ et $E = \{(v_1, v_2), (v_2, v_3), (v_1, v_3)\}$ alors G=(V,E) est un graphe simple.

Définition 2.1.9. Soit $G = (V, E)$ un graphe (resp un multi-graphe). Si E est une relation symétrique, on dira que G est un graphe (resp un multi-graphe) non orienté ou non dirigé.

Définition 2.1.10. Soient $k \geq 1$ et $G = (V, E)$ un multi-graphe orienté (resp.non orienté). On dit que G est k régulier si pour tout $v \in V$, $d^+(v) = k$ (resp $deg(v) = k$).

Définition 2.1.11. Un graphe $G = (V, E)$ est complet si $E = V \times V \setminus \{(v, v), v \in V\}$;c'est-à-dire qu'on ne tient pas compte des boucles.

Remarque 2.1.2. Un graphe complet est non dirigé. K_n est le graphe simple non orienté complet à n sommets.

Définition 2.1.12. Un graphe $G = (V, E)$ est dit N-partis avec $N \geq 2$ si V peut- être partitionné en N sous-ensembles V_1,. . .,V_N tels que

$$E \subseteq \bigcup_{i \neq j} V_i \times V_j.$$

Lorsque $N = 2$ on parle de graphe biparti. Si $\mid V_1 \mid = m$ et $\mid V_2 \mid = n$ et $E = V_1 \times V_2$ on parle de graphe biparti complet et on note K_{mn}.

2.2 Graphes et algèbre linéaire

Dans cette partie nous établissons le lien entre la théorie des graphes et l'algèbre linéaire.

Définition 2.2.1. Soit $G = (V, E)$ un multi-graphe non orienté dont les sommets sont ordonnés par V=$\{v_1, \ldots, v_n\}$. La matrice d'adjacence de G est la matrice $A(G)$ dont l'élément a_{ij} est égal au nombre d'arêtes $\{v_i, v_j\}$ présentes dans E.

Exemple 2.2.1. Soient $V = \{0, 1, 2\}$ et $E = \{(0, 1), (0, 2), (1, 0), (2, 0), (2, 1), (1, 2)\}$, alors $G = (V, E)$ est un graphe non-orienté de matrice d'adjacence :

$$A(G) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Proposition 2.2.1. Soit $G = (V, E)$ un multi-graphe non orienté. La matrice d'adjacence $A(G)$ de G est une matrice symétrique.

Preuve . $A(G) = (a_{ij})$ où a_{ij} est le nombre d'arêtes $\{v_i, v_j\}$, comme le graphe est non-orienté , il y a autant d'arêtes $\{v_i, v_j\}$ que d'arêtes $\{v_j, v_i\}$ donc a_{ij} =a_{ji} pour tout $i, j \in \{1, \ldots, n\}$ ainsi ${}^tA(G)$=$A(G)$ d'où $A(G)$ est symétrique.

Définition 2.2.2. Deux graphes $G_i = (V_i; E_i)$ $i = 1, 2$ sont isomorphes s'il existe une bijection $\varphi : V_1 \longrightarrow V_2$ telle que :

$$(x, y) \in E_1 \Longleftrightarrow (\varphi(x), \varphi(y)) \in E_2$$

Définition 2.2.3. Une matrice de permutation est une matrice où chaque ligne et chaque colonne contiennent exactement un coefficient non-nul qui est égal à 1.

Proposition 2.2.2. Deux graphes G_1 et G_2 sont isomorphes s'il existe une matrice de permutation P telle que

$$A(G_1) = P^{-1}A(G_2)P$$

Preuve . Voir [10] page 70.

Définition 2.2.4. Matrice d'adjacence version graphe orienté.
Soit $G = (V, E)$ un multi-graphe orienté dont les sommets sont ordonnées par $V = \{v_1, \ldots, v_n\}$. La matrice d'adjacence de G est la matrice $A(G)$ dont l'élément $[A(G)]_{i,j}$ est égal au nombre d'arcs (v_i, v_j) présents dans E.

Exemple 2.2.2. Considérons le graphe $G = (V, E)$ où $V = \{v_1, v_2, v_3, v_4\}$ et $E = \{(v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_3), (v_4, v_1)\}$. La matrice d'adjacence de G est donnée par :

$$A(G) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Remarque 2.2.1. Pour les graphes orientés, la matrice adjacence n'est pas toujours symétrique.

2.3 Domaines d'applications des graphes

La théorie des graphes a de nombreuses applications à l'instar de :

1. L'informatique (Programmation).
2. La recherche opérationnelle (Tournés de distribution, ordonnancement de tâches, l'optimisation des plans de production industrielle).
3. La cartographie(Coloriage des cartes).
4. Théorie du codage.

⋆ ⋆ CHAPITRE TROIS ⋆ ⋆

CODES LINÉAIRES SUR LES CORPS DE GALOIS

3.1 Généralités sur les codes linéaires

3.1.1 Définitions et premières propriétés

Définition 3.1.1. Soient $\mathcal{A}$ un ensemble non vide de cardinal q et n un entier naturel non nul.

- On appelle code de longueur n sur $\mathcal{A}$ toute partie non vide C de $\mathcal{A}^n$.
- L'ensemble $\mathcal{A}$ est appelé alphabet du code.
- Tout élément $x = (x_1, \ldots, x_n)$ de C est appelé mot de code.

Proposition 3.1.1. L'application $d_H : \mathcal{A}^n \times \mathcal{A}^n \longrightarrow \mathbb{N}$ définie par :

$$\forall x, y \in \mathcal{A}^n, d_H(x, y) = Card\{i \in \{1, \ldots, n\}/x_i \neq y_i\}$$

est une distance sur $\mathcal{A}^n$

Preuve . Soient x, y et z dans $\mathcal{A}^n$

1. (Axiome de séparation)

$$\begin{aligned} d_H(x, y) = 0 &\iff Card\{i \in \{1, \ldots, n\}/x_i \neq y_i\} = 0 \\ &\iff \{i \in \{1, \ldots, n\}/x_i \neq y_i\} = \emptyset \\ &\iff \forall i \in \{1, \ldots, n\}, x_i = y_i \\ &\iff x = y \end{aligned}$$

2. (Axiome de symétrie)

$$\begin{aligned} d_H(x,y) &= Card\{i \in \{1,\dots,n\}/x_i \neq y_i\} \\ &= Card\{i \in \{1,\dots,n\}/y_i \neq x_i\} \\ &= d_H(y,x) \end{aligned}$$

3. (Inégalité triangulaire).

   Posons U=$\{i/x_i \neq z_i\}$, S=$\{i/x_i \neq z_i \wedge x_i = y_i\}$ et $T = \{i/x_i \neq z_i \wedge x_i \neq y_i\}$.

   $$\text{On a } S \bigcap T = U \text{ et } S \bigcap T = \emptyset.$$

   En effet supposons que $S \bigcap T \neq \emptyset$. Soit $i_0 \in \{1,\dots,n\}$ tel que $i_0 \in S \bigcap T$.

   $$i_0 \in S \bigcap T \Longrightarrow x_{i_0} \neq y_{i_0} \text{ et } x_{i_0} = y_{i_0}.$$

   ce qui est absurde d'où $S \bigcap T = \emptyset$.

   On a $T \subseteq U$ et $S \subseteq U$ donc $S \bigcup T \subseteq U$. Il reste à montrer que $U \subseteq S \bigcup T$.

   Soit $i \in \{1,\dots,n\}$ tel que $i \in U$.

   $$\begin{aligned} i \in U &\Longrightarrow x_i \neq z_i \\ &\Longrightarrow (x_i \neq z_i \wedge x_i = y_i) \; ou \; (x_i \neq z_i \wedge x_i \neq y_i) \\ &\Longrightarrow i \in S \bigcup T \end{aligned}$$

   ainsi, $U = S \bigcup T$.

   $d_H(x,z) = Card(U) = card(T) + Card(S)$, de plus

   $Card(T) \leq d_H(x,y)$ et $Card(S) \leq d_H(y,z)$

   d'où $d_H(x,z) \leq d_H(x,y) + d_H(y,z)$.

Définition 3.1.2. La distance d_H de la proposition 3.1.1 est appelé distance de Hamming sur $\mathcal{A}^n$.

Définition 3.1.3. Soient $\mathbb{F}_q$ le corps de Galois de cardinal q et n un entier naturel non nul. On appelle code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$ tout $\mathbb{F}_q$-sous -espace vectoriel de $\mathbb{F}_q^n$ de dimension k.

Dans la suite, C est un code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$.

Définition 3.1.4. Soit $x = (x_1,\dots,x_n)$ un mot de C.
On appelle poids de Hamming de x l'entier $\omega_H(x)$ défini comme suit :

$$\omega_H(x) = Card\{i \in \{1, \dots n\}/x_i \neq 0\}.$$

Proposition 3.1.2. Les mots d'un code linéaire binaire sont soit tous de poids pair ou soit en nombre égal de poids pair et impair.

Preuve . Voir [3] page 24.

Remarque 3.1.1. Pour tous mots x et y de C, on a l'égalité suivante :

$$d_H(x, y) = \omega_H(x - y) \text{ et } d_H(x, 0) = \omega_H(x).$$

Définition 3.1.5. Soit C un code, on appelle distance minimale de C l'entier d défini par :

$$d = min\{d_H(x, y) : x, y \in C, x \neq y\} = min\{\omega_H(x) : x \in C, x \neq 0\}$$

Notation 3.1.1. On écrit C$[n, k, d]_q$ pour dire que C est un code linéaire sur $\mathbb{F}_q$ de longueur n, de dimension k et de distance minimale d.

Proposition 3.1.3. Soit $C \subseteq \mathbb{F}_q^n$.
Si C est un $[n, k, d]$-code sur $\mathbb{F}_q$ alors $Card(C) = q^k$.

Preuve . Puisque C est un code linéaire sur $\mathbb{F}_q$, C est donc un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k ainsi d'après la proposition 1.1.13, $C \cong \mathbb{F}_q^k$ d'où $|C| = q^k$

Proposition 3.1.4. (Borne de Singleton) Soit $C \subseteq \mathbb{F}_q^n$.
Si C est un $[n, k, d]$-code sur $\mathbb{F}_q$ alors $d \leq n - k + 1$

Le théorème suivant donne une condition d'existence des codes linéaires.

Théorème 3.1.1 (Borne de VARSHAMOV-Gilbert)**.** Soit C un $[n, k, d]$-code linéaire sur $\mathbb{F}_q$.

$$\sum_{i=0}^{d-2}(q-1)^i \binom{n-1}{i} < q^{n-k} \Longrightarrow \text{(il existe } un[n, k, d] - code) \text{ sur } \mathbb{F}_q.$$

Définition 3.1.6. Soit C un $[n, k, d]$-code et soit P_i le nombre de mots de poids i.
Le n-uplet $(P_0, P_1, \dots, P_n)$ est appelé distribution des poids du code C .

Proposition 3.1.5. Soit C un $[n, k, d]_q$-code linéaire.
Si $(P_0, P_1, \dots, P_n)$ est la distribution de poids de C alors

1. $P_0 = 1$
2. $\forall i\ 1 \leq i \leq d - 1$, $P_i = 0$

3. $\forall i \geq d$, $P_d \geq 1$

Preuve . Voir [3] page 29

Définition 3.1.7. Soit C un $[n, k, d]$-code de distribution de poids $(P_1, P_2, \ldots, P_n)$, on appelle polynôme énumérateur de poids du code C le polynôme à deux inconnues défini comme suit :

$$W_C(x, y) = \sum_{i=1}^{n} P_i x^{n-i} y^i \text{ où } x, y \in C.$$

3.1.2 Matrice génératrice d'un code linéaire

Définition 3.1.8. Soient $C[n, k]_q$-code linéaire et $(e_1, e_2, \ldots, e_n)$ une $\mathbb{F}_q$- base de C.
On appelle matrice génératrice de C toute matrice dont les lignes sont formés des composantes des vecteurs de base de C par rapport à la base canonique de $\mathbb{F}_q^n$ sur $\mathbb{F}_q$.

Remarque 3.1.2. Toute matrice génératrice d'un $[n, k]_q$-code linéaire est de taille $k \times n$.

Proposition 3.1.6. Si G est une matrice génératrice d'un code C, alors toute autre matrice de C est de la forme $A \cdot G$ où A est une matrice carrée inversible d'ordre k à coefficients dans $\mathbb{F}_q$

Preuve . Soient G et $G^{'}$ deux matrices génératrices de C, alors les lignes $x_1, x_2, \ldots, x_k$ de G forment une base de C sur $\mathbb{F}_q$. De même, les lignes $y_1, y_2, \ldots, y_k$ de $G^{'}$ forment une base de C sur $\mathbb{F}_q$. Ainsi, pour tout $i \in [|1, k|]$, il existe $t_{i1}, t_{i2}, \ldots, t_{ik} \in \mathbb{F}_q$ tels que $y_i = \sum_{j=1}^{k} t_{ij} x_j$. Donc $G^{'} = AG$ où $A = (t_{ij})_{1 \leq i,j \leq k}$ est une matrice carrée d'ordre k à coefficients dans $\mathbb{F}_q$. De même il existe une matrice carrée $A^{'}$ d'ordre k à coefficients dans $\mathbb{F}_q$ telle que $G = A^{'}G^{'}$. Ainsi $G^{'} = AA^{'}G^{'}$ et $G = A^{'}AG$, ce qui implique $AA^{'} = A^{'}A = I_k$. D'où A est inversible.

Proposition et Définition 3.1.1. Soient C un $[n, k] - code$ sur $\mathbb{F}_q$ et G une matrice génératrice C alors :

1. L'application $\begin{array}{rccc} \varphi : & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & u & \longmapsto & uG \end{array}$
   est un morphisme injectif d'espaces vectoriels appelé **encodeur.**
2. $C = Im\varphi$ =$\{uG / u \in \mathbb{F}_q^k\}$.

Preuve . 1. Soient $u, v \in \mathbb{F}_q^n$ et $\lambda \in \mathbb{F}_q$ on a

$$\begin{aligned}
\varphi(u+\lambda v) &= (u+\lambda v)G \\
&= (u_1+\lambda v_1, \ldots, u_k+\lambda v_k)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix}. \\
&= (u_1+\lambda v_1)e_1 + (u_2+\lambda v_2)e_2 + \ldots + (u_k+\lambda e_k)v_k \\
&= u_1e_1 + \lambda v_1e_1 + u_2e_2 + \lambda v_2e_2 + \cdots + u_ke_k + \lambda e_kv_k \\
&= \sum_{i=1}^{k} u_ie_i + \sum_{i=1}^{k} \lambda v_ie_i \\
&= (u_1, \ldots, u_k)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix} + \lambda(v_1, \ldots, v_k)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix} \\
&= uG + \lambda vG \\
&= \varphi(u) + \lambda\varphi(v)
\end{aligned}$$

ainsi φ est un morphisme. Soient u, v dans $\mathbb{F}_q^k$ tels que $\varphi(u) = \varphi(v)$.

$$\begin{aligned}
\varphi(u) = \varphi(v) &\implies uG = vG \\
&\implies \sum_{i=1}^{k} u_ie_i = \sum_{i=1}^{k} v_ie_i \\
&\implies \sum_{i=1}^{k} (u_i - v_i)e_i = 0 \\
&\implies \forall 1 \leq i \leq k, (u_i - v_i) = 0 \text{ car } (e_i)_{1\leq i\leq k} \text{ est une base de C} \\
&\implies \forall 1 \leq i \leq k, u_i = v_i \\
&\implies u = v
\end{aligned}$$

d'où φ est injectif.

2. Soit $x \in \mathbb{F}_q^n$ tel que $x \in C$.

$$\begin{aligned} x \in C &\iff x = \sum_{i=1}^{k} \lambda_i e_i \text{ car } (e_i)_{1\leq i\leq k} \text{ est une base de C} \\ &\iff x = (\lambda_1, \ldots, \lambda_k) \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix} \\ &\iff x = (\lambda_1, \ldots, \lambda_k)G \end{aligned}$$

D'où $C = \{uG/u \in \mathbb{F}_q^k\}$.

3.1.3 Détection et correction d'erreurs

Lors de la transmission d'un message des erreurs peuvent se produire dus à de nombreuses raisons.La théorie du codage a donc pour rôle de détecter et de corriger les erreurs de transmission d'un message. Mais il se pose le problème de savoir à quelles conditions un code linéaire peut détecter et corriger une erreur. Les définitions suivantes nous donnent ces conditions.

Proposition et Définition 3.1.2. Soit $t \geq 1$. Nous dirons qu'un $[n, k, d]_q$-code détecte t erreurs si pour tout $x \in C$, les chaines $y \in \mathbb{F}_q^n$ vérifiant $x \neq y$ et $d(x, y) \leq t$ ne sont pas dans C.

Proposition et Définition 3.1.3. Soit $t \geq 1$. Nous dirons qu'un $[n, k, d]_q$-code corrige t erreurs si pour tout $y \in \mathbb{F}_q^n$ il existe au plus un $x \in C$ tel que $x \neq y$ et $d_H(x, y) \leq t$

Définition 3.1.9. On appelle capacité correctrice d'un code C$[n, k, d]_q$ le nombre $E(\frac{d-1}{2})$ c'est le nombre maximal d'erreurs que peut corriger un code.

Théorème 3.1.2. Soit C un $[n, k, d]$-code linéaire sur $\mathbb{F}_q$.

1. C détecte t erreurs si et seulement si $t < d$.
2. C corrige t erreurs si et seulement si $d \geq 2t + 1$.

Preuve .

1. Supposons que C détecte t erreurs montrons que $t < d = mind_H(x, y)$ $x, y \in C$ avec $x \neq y$.

   Si $t \geq d$ alors il existe $x_0, y_0 \in C$ tel que $d(x_0, y_0) \leq t$ mais comme C corrige t erreurs alors sans nuire la généralité on suppose que $y_0 \notin C$ ce qui est absurde car $y_0 \in C$, d'où

$t < d$.

Inversement supposons que $t < d$, soient $x \in C$ et $y \in \mathbb{F}_q^n$ tels que

$x \neq y$ et $d_H(x, y) \leq t$. Montrons que $y \notin C$, si $y \in C$ on a $d_H(x, y) < t < d = mind_H(x, y)\ x, y \in C$ avec $x \neq y$ ce qui contredit la minimalité de d, d'où $y \notin C$.

2. Soient $d \leq 2t$ et $x, z \in C$ où $x \neq y$ et où $d_H(x, y) \leq 2t$. On peut alors choisir un $y \in \mathbb{F}_q^n$ tel que $d_H(x, y) \leq t$ et $d_H(z, y) \leq t$. Nous avons donc deux mots du code dont la distance à y est inférieure ou égale à t, ceci implique que le code ne corrige pas t erreurs.

   Soit $y \in \mathbb{F}_q^n$, supposons que $d \geq 2t + 1$ et qu'il existe $x_1$et x_2 dans C tels que $x_1 \neq y$, $x_2 \neq y$, $d_H(x_1, y) \leq t$ et $d_H(x_2, y) \leq t$; on a $d_H(x_1, x_2) \leq 2t$ c'est-à-dire $d \leq 2t$ ce qui est absurde car $d \geq 2t + 1$ d'où il existe au plus un x dans C tel que $x \neq y$ et $d_H(x, y) \geq 2t + 1$.

3.2 Dual d'un code linéaire

Proposition 3.2.1. L'application (,) : $\mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ définie par

$$\forall x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n, (x, y) = (\sum_1^n x_i y_i) mod\ q$$

est un ``produit scalaire´´sur $\mathbb{F}_q^n$

Preuve . Immédiate

Remarque 3.2.1. (;) est un produit scalaire par abus de langage car (;) n'est pas défini positive.

Définition 3.2.1. On appelle code dual du code linéaire C le code $C^\perp$ défini par :

$$C^\perp = \{y \in \mathbb{F}_q^n / \forall x \in C, (x, y) = 0\}.$$

Autrement dit $C^\perp$ est l'orthogonal de C par rapport à (;) .

Définition 3.2.2. Toute matrice génératrice H du code dual de C est appelée matrice de contrôle de C .

Proposition 3.2.2. Si C est un $[n, k, d]$-code sur $\mathbb{F}_q$ alors $Card(C^\perp) = q^{n-k}$

Preuve . Puisque dim $C^\perp = n - k$ on remplace C par $C^\perp$ et k par $n - k$ dans la preuve de la proposition 3.2.3 pour avoir le résultat.

Théorème 3.2.1. Soient C un code linéaire sur $\mathbb{F}_q$, G une matrice génératrice de C et $\mathcal{B} = (v_i)_{1\leq i\leq k}$ une base de C.

1. $C^\perp = \{x \in \mathbb{F}_q^n | x\ {}^tG = 0\}$.
2. Si C est un $[n,k]$-code alors $C^\perp$ est un $[n, n-k]$-code.
3. $C^{\perp\perp} = C$

Preuve .

1. Soit $x \in C^\perp$ montrons que $x^tG = 0$.

$$\begin{aligned} x \in C^\perp &\implies \forall c \in C, < x, c >= 0 \\ &\implies \forall i \in \{1,\dots,k\}, < x, v_i >= 0 \\ &\implies \forall i \in \{1,\dots,k\}, x_1v_{i1} + \cdots + x_nv_{in} = 0 \end{aligned}$$

On a

$$\begin{aligned} x\ {}^tG &= (x_1,\dots,x_n)\begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ v_{k1} & v_{k2} & \dots & v_{kn} \end{pmatrix}^t \\ &= (x_1,\dots,x_n)\begin{pmatrix} v_{11} & v_{21} & \dots & v_{k1} \\ v_{12} & v_{22} & \dots & v_{k2} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ v_{1n} & v_{2n} & \dots & v_{kn} \end{pmatrix} \\ &= (< x, v_1 >, < x, v_2 >, \dots, < x, v_k >) \\ &= (0, 0, \dots, 0) \end{aligned}$$

d'où $C^\perp \subseteq \{x \in \mathbb{F}_q^n / a\ {}^tG = 0\}$.

Soit $x \in \{a \in \mathbb{F}_q^n / xG^t = 0\}$ montrons que $x \in C^\perp$.

On a a=$(a_1,\dots,a_n)$ et ${}^tG = \begin{pmatrix} v_{11} & v_{21} & \dots & v_{k1} \\ v_{12} & v_{22} & \dots & v_{k2} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ v_{1n} & v_{2n} & \dots & v_{kn} \end{pmatrix}$ donc,

$a^tG = (a_1v_{11} + a_2v_{12} + \ldots + a_nv_{1n} =< a, v_1 >, < a, v_2 >, \ldots, < a, v_k >)$.

$$x \in \{a \in \mathbb{F}_q^n / a^tG = 0\} \implies x\ {}^tG = 0$$
$$\implies < x, v_1 >=< x, v_2 >= \ldots =< x, v_k >= 0$$

Soit $y \in C$ alors y=$\sum_{i=1}^{k} \alpha_i v_i$ on a,

$$\begin{aligned} < x, y > &= < x, \sum_{i=1}^{k} \alpha_i v_i > \\ &= \sum_{i=1}^{k} < x, \alpha_i v_i > \\ &= \sum_{i=1}^{k} \alpha_i < x, v_i > \\ &= 0 \end{aligned}$$

d'où $x \in C^\perp$ et par conséquent $C^\perp = \{a \in \mathbb{F}_q^n / a\ {}^tG = 0\}$

2. Soit C un $[n, k]$-code linéaire sur $\mathbb{F}_q$. Puisque (;) est non-dégénéré, on a $dimC + dimC^\perp = n$ d'où

$$\begin{aligned} dimC^\perp &= n - dimC \\ &= n - k \end{aligned}$$

et par conséquent $C^\perp$ est un $[n, n-k]$-code linéaire sur $\mathbb{F}_q$

3. On sait que
$C^\perp = \{x \in \mathbb{F}_q^n / \forall a \in C < x, a >= 0\}$ et $C^{\perp\perp} = \{x \in \mathbb{F}_q^n) / \forall a \in C^\perp < x, a >= 0\}$.
Soient $y \in C$ et $a \in C^\perp$ on a $< y, a >= 0$ d'où $y \in C^{\perp\perp}$ ainsi $C \subseteq C^{\perp\perp}$, or d'après 2) dim $C^\perp = n - k$ donc dim $C^{\perp\perp} = n - (n - k) = k$, on a alors $C \subseteq C^{\perp\perp}$ et dim $C^{\perp\perp}$=dim C d'où $C^{\perp\perp} = C$.

Proposition 3.2.3. Soient C un $[n, k]_q$-code, H une matrice de contrôle et $x \in \mathbb{F}_q^n$.

$$x \in C \iff x^tH = 0$$

Preuve . Soit $x \in \mathbb{F}_q^n$

Supposons que $x \in C$,

$$x \in C \implies \forall\ a \in C^\perp, < x, a >= 0$$
$$\implies \forall i \in \{1 \ldots n-k\}, < x, e_i >= 0 \text{ car } (e_i)_{1 \le i \le n-k} \text{ est une base de } C^\perp.$$

On obtient le système suivant : $\begin{cases} x_1e_{11} + x_2e_{12} + \cdots + x_ne_{1n} &= 0 \\ x_1e_{21} + x_2e_{22} + \cdots + x_ne_{2n} &= 0 \\ x_1e_{31} + x_2e_{32} + \cdots + x_ne_{3n} &= 0 \\ \vdots & \vdots \\ x_1e_{n-k1} + x_2e_{n-k2} + \cdots + x_ne_{n-kn} &= 0 \end{cases}$

c'est-à-dire $H^tx = 0$ car $H = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{n-k} \end{pmatrix}$

ainsi ${}^t(H^tx) = 0$ d'où $x^tH = 0$.

Inversement supposons que $x^tH = 0$,

$x^tH = 0 \Longrightarrow x \in C^{\perp\perp} = C$ car H est une matrice génératrice de $C^{\perp}$.

Proposition 3.2.4. Soit $C \subseteq \mathbb{F}_q^n$.

si C un $[n, k, d]$-code sur $\mathbb{F}_q$ de matrice G et de matrice de contrôle H alors

$$G\ {}^tH = 0$$

Preuve . Soient C $[n, k]$-code et $x \in \mathbb{F}_q^n$ alors d'après la proposition 3.2.3 $x \in C \iff x\ {}^tH = 0$.

$$\begin{aligned} G\ {}^tH &= \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix} {}^tH \\ &= \begin{pmatrix} e_1\ {}^tH \\ e_2\ {}^tH \\ \vdots \\ e_k\ {}^tH \end{pmatrix} \\ &= 0 \end{aligned}$$

car $\forall i \in \{1, \ldots, k\}$, e_i est mot de C d'où le résultat.

Proposition 3.2.5. Soient C un $[n, k, d]$ -code et H une matrice de contrôle du code C.
La distance minimale d est le plus petit nombre de colonnes linéairement dépendantes de H.

Preuve . Soient $x = (x_1, x_2, \ldots, x_n) \in C$ tel que $\omega_H(x) = d$ et H_i la i-ème colonne de H.

$$\begin{aligned}
\omega_H(x) = d &\implies x_{d+1} = x_{d+2} = \cdots = x_n = 0 \\
&\implies x^t H = x_1^t H_1 + x_2^t H_2 + \cdots + x_d^t H_d \\
&\implies x_1^t H_1 + x_2^t H_2 + \cdots + x_d^t H_d = 0 \text{ (car } x^t H = 0) \\
&\implies x_1 H_1 + x_2 H_2 + \cdots + x_d H_d = 0 \text{ (car } {}^t({}^t H_i) = H_i) \\
&\implies H \text{ possede d colonnes linéaires dépendanttes.}
\end{aligned}$$

Supposons que H possède m colonnes linéairement dépendantes avec $m < d$, H possède m colonnes linéairement dépendantes signifie qu'il existe $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_q^*$ tel que
$\alpha_1 H_1 + \alpha_2 H_2 + \cdots + \alpha_d H_d = 0$.

$$\begin{aligned}
x_1 H_1 + x_2 H_2 + \cdots + x_d H_d = 0 &\implies {}^t(x_1 H_1 + x_2 H_2 + \cdots + x_d H_d) = 0 \\
&\implies x_1^t H_1 + x_2^t H_2 + \cdots + x_d^t H_d = 0 \\
&\implies (\alpha_1, \alpha_2, \ldots, \alpha_m, 0, \ldots, 0)^t H = 0 \\
&\implies \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m, 0, \ldots, 0) \in C.
\end{aligned}$$

Comme $\forall i \in \{1, 2, \ldots, m\}$, $\alpha_i \neq 0$, α est donc un mot de C de poids m avec $m < d$ ce qui est absurde d'où d est le plus petit nombre de colonnes linéairement dépendantes de H.

Proposition 3.2.6. Soient C un $[n, k]$-code linéaire sur $\mathbb{F}_q$ et H une matrice de contrôle C.
d est la distance minimale de C si et seulement si tout système de $d-1$ colonnes de H est linéairement indépendantes.

Preuve . Supposons que d soit la distance minimale de C, que $\mathcal{S} = (H_i)_{1 \leq i \leq d-1}$ soit un système de $d-1$ colonnes de H et que $x_1, x_2, \ldots, x_{d-1} \in \mathbb{F}_q$ tels que
$x_1 H_1 + x_2 H_2 + \cdots + x_{d-1} H_{d-1} = 0$.

$$\begin{aligned}
x_1 H_1 + x_2 H_2 + \cdots + x_{d-1} H_{d-1} = 0 &\implies x_1\, {}^t H_1 + x_2\, {}^t H_2 + \cdots + x_{d-1}\, {}^t H_{d-1} = 0 \\
&\implies (x_1, \ldots, x_{d-1}, 0, \ldots, 0)\, {}^t H = 0 \\
&\implies x = (x_1, \ldots, x_{d-1}, 0, \ldots, 0)) \in C
\end{aligned}$$

Supposons qu'il existe $i_0 \in \{1, \ldots, d-1\}$ tel que $x_{i_0} \neq 0$ alors $0 < \omega_H(x) < d$ ce qui contredit le fait que d est la distance minimale de C, ainsi $\forall i \in \{1, \ldots, d-1\}$, $x_i = 0$ d'où

$\mathcal{S} = (H_i)_{1\leq i\leq d-1}$ est un système linéairement indépendant.

Le théorème suivant nous permet d'avoir l'énumérateur de poids de $C^\perp$ connaissant l'énumérateur de poids de C.

Théorème 3.2.2. Soient C un $[n, k, d]$-code sur $\mathbb{F}_q$ et $C^\perp$ son dual, alors les polynômes énumérateurs de poids C et $C^\perp$ sont liés par le relation suivante

$$W_{C^\perp}(x, y) = \frac{1}{q^k} W_C(x + (q-1)y, x - y)$$

appelée identité de MacWilliams.

Preuve . Voir [3] page 22.

Ce théorème nous permet de montrer la non-existence d'un code linéaire.

Exemple 3.2.1. Soit $C = \{(0,0,0,0), (1,0,0,1), (0,1,0,1), (1,1,0,0)\}$, C est un code linéaire sur $\mathbb{F}_2$.
Déterminons les polynômes énumérateurs de poids de C et $C^\perp$.

$$\begin{aligned} W_C(x,y) &= \sum_{i=1}^{4} P_i x^{4-i} y^i \\ &= P_0x^4 + P_1x^3y + P_2x^2y^2 + P_3xy^3 + P_4y^4 \\ &= x^4 + 3x^2y^2 \end{aligned}$$

car $P_0 = 1$,$P_1 = P_3 = 0$ et $P_2 = 3$. Comme $P_2 = 3$ et $P_1 = 0$, C est un $[4, 2, 2]$-code.

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{2^2}[(x+y)^4 + 3(x+y)^2(x-y)^2] \\ &= \frac{1}{4}[x^4 + 4x^3y + 6x^2y^2 + 4x^1y^3 + y^4 + 3x^4 - 6x^2y^2 + 3y^4] \\ &= x^4 + x^3y^1 + x^1y^3 + y^4 \end{aligned}$$

$C^\perp$ est donc un $[4, 2, 1]$-code car $P_1 \neq 0$.

Exemple 3.2.2. Nous allons monter que sur $\mathbb{F}_2$ il n'existe pas un $[7, 2, 5]$-code.
La borne de Singleton nous donne $k \leq 7 - 5 + 1 = 3$; ainsi $k = 2$ est possible.
Maintenant en utilisant la proposition 3.1.2 nous obtenons seulement deux cas possibles pour la

distribution de poids d'un tel code, à savoir :$(1,0,0,0,0,1,1,1)$ et $(1,0,0,0,0,2,1,0)$, ce qui nous donne respectivement les polynômes de distribution de poids suivants :

$$W_C(x,y) = x^7 + x^2y^5 + xy^6 + y^7,$$
$$W_C(x,y) = x^7 + 2x^2y^5 + xy^6$$

En appliquant l'identité de MacWilliams afin d'obtenir le polynôme de distribution de poids du code dual il vient que :

$$W_{C^\perp}(x,y) = 2x^2y^5 + 3xy^6 + x^7 - 2x^6y + 13x^5y^2 + 15x^3y^4,$$
$$W_{C^\perp}(x,y) = x^7 - x^6y + 8x^5y^2 + 10x^4y^2 + 5x^4y^4 + 7x^2y^5 + 2xy^6.$$

Comme le dual d'un code linéaire est aussi un code linéaire, on obtient la non-existence de notre $[7,2,5]$-code car les coefficients de $W_{C^\perp}$ ne sont tous positifs.

3.3 Codes linéaires équivalents et systématiques.

Définition 3.3.1. Soit A une matrice carrée d'ordre n à coefficients dans $\mathbb{F}_q$. On dit que A est une matrice monomiale si A possède un seul élément non nul sur chaque ligne et chaque colonne.

Définition 3.3.2. Une transformation sur $\mathbb{F}_q^n$ est dite mononiale si la matrice associée à cette transformation dans la base canonique est monomiale.

Proposition 3.3.1. Soient T et G deux transformations monomiale alors :

1. T^{-1} est monomiale.
2. $T \circ G$ est monomiale .

Preuve . 1. Soit T une transformation mononiale et A_T sa matrice relativement à la base canonique de $\mathbb{F}_q^n$.

$A_T = (a_{ij})_{1\leq i,j\leq n}$ et les coefficients a_{ij} pour i_0 et j_0 fixés dans $\{1,2,3,\ldots,n\}$ vérifient : $a_{i_0j_0} \neq 0 \Longrightarrow \forall k,q \in \{1,2,3,\ldots,n\} \setminus \{i,j\}\ a_{i_0k} = a_{qj_0} = 0$.

On a det$A_T = \prod a_{ij}$ avec $a_{ij} \neq 0$ donc

$$\begin{aligned} A_T^{-1} &= \frac{1}{detA_T}\ {}^t(com(A_T)) \\ &= ((-1)^{i+j})\frac{1}{a_{ij}}) \end{aligned}$$

d'où T^{-1} est monomiale.

2. Soient T et G deux transformation mononiales de matrices respectives A_T et A_G dans la base canonique de $\mathbb{F}_q^n$.

   $A_{T\circ G} = A_T A_G$ est la matrice de $T \circ G$, on montre facilement que cette matrice est monomiale.

Exemple 3.3.1. Soient $\lambda_1, \ldots, \lambda_n$ des éléments non nuls de $\mathbb{F}_q$ et $\alpha \in \mathcal{S}_n$ alors l'application

$$\begin{array}{rccc} \alpha_{\lambda_1\ldots\lambda_n} : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (x_1, \ldots, x_n) & \longmapsto & (\lambda_1 x_{\alpha(1)}, \ldots, \lambda_n x_{\alpha(n)}) \end{array}$$

est une transformation monomiale .

En effet soient $X = (x_1, \ldots, x_n)$ et $Y = (y_1, \ldots, y_n)$ des éléments de $\mathbb{F}_q^n$ et $\lambda \in \mathbb{F}_q$ on a

$\alpha_{\lambda_1\ldots\lambda_n}(X + Y) = \alpha_{\lambda_1\ldots\lambda_n}(x_1 + y_1, \ldots, x_n + y_n)$ et

$\alpha_{\lambda_1\ldots\lambda_n}(X) + \alpha_{\lambda_1\ldots\lambda_n}(Y) = (\lambda_1(x_{\alpha(1)} + y_{\alpha(1)}), \ldots, (\lambda_n(x_{\alpha(n)} + y_\alpha(n))$.

$\forall\, i \in \{1, \ldots, n\}$, posons $z_i = x_i + y_i$. Comme $\alpha(i) \in \{1, \ldots, n\}$ car α est une permutation

$z_{\alpha(i)} = x_{\alpha(i)} + y_{\alpha(i)}$ on a $\lambda_i z_{\alpha(i)} = \lambda_i(x_{\alpha(i)} + y_{\alpha(i)})$ et

$$\begin{aligned} \alpha_{\lambda_1\ldots\lambda_n}(X + Y) &= \alpha_{\lambda_1\ldots\lambda_n}(x_1 + y_1, \ldots, x_n + y_n) \\ &= \alpha_{\lambda_1\ldots\lambda_n}(z_1, \ldots, z_n) \\ &= (\lambda_1 z_{\alpha(1)}, \ldots, \lambda_n z_{\alpha(n)}) \\ &= (\lambda_1(x_{\alpha(1)} + y_{\alpha(1)}), \ldots, \lambda_n(x_{\alpha(n)} + y_{\alpha(n)})) \\ &= \alpha_{\lambda_1\ldots\lambda_n}(X) + \delta_{\lambda_1\ldots\lambda_n}(Y) \end{aligned}$$

et

$$\begin{aligned} \alpha_{\lambda_1\ldots\lambda_n}(\lambda X) &= (\lambda\lambda_1 x_{\alpha(1)}, \ldots, \lambda\lambda_n x_{\alpha(n)}) \\ &= \lambda(\lambda_1 x_{\alpha(1)}, \ldots, \lambda_n x_{\alpha(n)}) \\ &= \lambda\delta_{\lambda_1\ldots\lambda_n}(X) \end{aligned}$$

d'où $\alpha_{\lambda_1\ldots\lambda_n}$ est linéaire.

La matrice de $\alpha_{\lambda_1\ldots\lambda_n}$ notée M_α est une matrice de taille $n \times n$ dont les entrées sont nulles sauf les $(\alpha(i), i)$ qui valent λ_i.

Remarque 3.3.1. On a $\alpha_{\lambda_1\ldots\lambda_n}(x) = xM_\alpha$ et $w_H(\alpha_{\lambda_1\ldots\lambda_n}(x)) = w_H(x)$ car $\mathbb{F}_q$ est un corps et de plus permuter les composantes d'un mot ne change pas son poids.

Proposition et Définition 3.3.1. Soient C_1 et C_2 deux codes linéaires sur $\mathbb{F}_q$.

C_1 et C_2 sont équivalents si seulement s'il existe une transformation monomiale T telle que

$$C_1 = T(C_2).$$

Preuve .

1. Soit C un code, $C = id(C) \Longleftrightarrow C \equiv C$ donc $\equiv$ est réflexive.
2. Soient C_1 et C_2 deux codes tels que $C_1 \equiv C_2$.

$$\begin{aligned} C_1 \equiv C_2 &\implies \exists\, une\ transformation\ monomiale\ T\ telle\ que\ C_1 = T(C_2) \\ &\implies T^{-1}(C_1) = C_2 \\ &\implies C_2 \equiv C_1\ car\ l'inverse\ de\ T\ est\ monomiale. \end{aligned}$$

   d'où $\equiv$ est symétrique.

3. Soient C_1, C_2 et C_3 trois codes tels que $C_1 \equiv C_2$ et $C_2 \equiv C_3$.

$$\begin{aligned} C_1 \equiv C_2\ et\ C_2 \equiv C_3 &\implies \exists\, T\ et\ U\ telles\ que\ C_1 = T(C_2)\ et\ C_2 = U(C_3) \\ &\implies C_1 = T(U(C_3)) = T \circ U(C_3) \\ &\implies C_1 \equiv C_3 \end{aligned}$$

   d'où $\equiv$ est transitive.

Proposition 3.3.2. Soient C_1 et C_2 deux codes linéaires sur $\mathbb{F}_q$.
Si C_1 et C_2 sont équivalents alors $C_1^{\perp}$ et $C_2^{\perp}$ le sont aussi.

Preuve . Soient C_1 et C_2 deux codes équivalents montrons que $C_1^{\perp}$sont équivalents $C_2^{\perp}$.
C_1 et C_2 sont équivalents équivaut à dire qu'il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q^* \ /$

$$(c_1, \ldots, c_n) \in C_1 \iff (\alpha_1 c_1, \alpha_2 c_2, \ldots, \alpha_n c_n) \in C_2$$

cherchons $\beta_1, \ldots, \beta_n \in \mathbb{F}_q^* \ /$

$$x = (x, \ldots, x_n) \in C_1^{\perp} \iff (\beta_1 x_1, \ldots, \beta_n x_n) \in C_2^{\perp}$$

Soient $x = (x_1, \ldots, x_n) \in C_1^{\perp}$ et $y = (y_1, \ldots, y_n) \in C_2$ on a $(\alpha_1 y_1, \ldots, \alpha_n y_n) \in C_1$ car C_1 et C_2 sont équivalents. Posons $u = (\alpha_1 y_1, \ldots, \alpha_n y_n)$ il vient que
$< x, u >= \alpha_1 x_1 y_1 + \ldots + \alpha_n x_n y_n = 0$ car $x \in C_1^{\perp}$ et $u \in C_1$.
On a alors $< (\alpha_1 x_1, \ldots, \alpha_n x_n), y >= \alpha_1 x_1 y_1 + \ldots + \alpha_n x_n y_n = 0$
d'où $(\alpha_1 x_1, \ldots, \alpha_n x_n) \in C_2^{\perp}$ prendre $\beta_i = \alpha_i \ \forall i$ pour conclure.

Définition 3.3.3. Soit C un $[n,k]$-code linéaire sur $\mathbb{F}_q$, on dit que C est systématique s'il possède une matrice génératrice de la forme $G = \Big[I_k|A\Big]$, cette forme est appelée la forme standard où I_k est la matrice identité d'ordre k et A une matrice de taille $k \times (n-k)$ sur $\mathbb{F}_q$, plus précisément

$$G = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & e_{1k+1} & \dots & \dots & \dots & e_{1n} \\ 0 & 1 & 0 & \dots & 0 & \vdots & \ddots & \vdots & \vdots & \vdots \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & 1 & e_{kk+1} & \dots & \dots & \dots & e_{kn} \end{pmatrix}.$$

Proposition 3.3.3.

1. Un code linéaire reste inchangé si on permute les lignes de sa matrice génératrice.
2. Si on effectue cette opération sur les colonnes d'une matrice génératrice d'un code linéaire, on obtient un code linéaire qui lui est équivalent.

Preuve .

1. L'ordre des éléments dans une base importe peu donc permuter les lignes de la matrice génératrice d'un code ne change pas le code.
2. Soit C un $[n,k]$-code linéaire sur $\mathbb{F}_q$ engendré par :

$$G = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}$$

en permutant la première et la deuxième colonne on obtient la matrice

$$G' = \begin{pmatrix} a_{12} & a_{11} & \dots & a_{1n} \\ a_{22} & a_{21} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ a_{k2} & a_{k1} & \dots & a_{kn} \end{pmatrix}.$$

Désignons par C' le code donc la matrice génératrice est G' et α la permutation définie par :

$$\begin{array}{rccc} \alpha: & \{1,2,\ldots,n\} & \longrightarrow & \{1,2,\ldots,n\} \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 1 \\ & i & \longmapsto & i \end{array} \qquad \forall i \in \{3,4,\ldots,n\}$$

$\alpha_{1,1,\ldots,1}$ définie comme dans l'exemple 3.3.1 est une transformation monomiale et $\forall i \in \{1,\ldots,k\}$, on a

$$\begin{aligned} \alpha_{11\ldots1}(a_{i1},a_{i2},a_{i3},\ldots,a_{in}) &= (a_{i\alpha(1)},a_{i\alpha(2)},\ldots,a_{i\alpha(n)}) \\ &= (a_{i2},a_{i1},a_{i3},\ldots,a_{in}) \in C' \end{aligned}$$

ainsi $\alpha_{11\ldots1}(C) = C'$ d'où $C \equiv C'$. Lorsqu'on permute plus de deux colonnes on a le même résultat car $\equiv$ est une relation d'équivalence.

Proposition 3.3.4. Tout code linéaire est équivalent à un code systématique.

Preuve . Soit C un $[n,k,d]$-code linéaire sur $\mathbb{F}_q$.
Soit G une matrice génératrice de C.

- Si G est sous forme standard, alors C est systématique.
- Sinon, comme le rang de G est k, il existe un mineur de taille $k \times k$ non nul et en permutant les colonnes de G, on ramène ce mineur aux k premières colonnes et on obtient une matrice G' de la forme $G' = (X|Y)$ où $X \in \mathcal{M}_{k,k}(\mathbb{F}_q)$ et $Y \in \mathcal{M}_{k,n-k}(\mathbb{F}_q)$ avec $rang(X) = k$, X est donc inversible et en multipliant G' par à gauche par X^{-1}, on obtient la matrice $G'' = X^{-1}G = (I_k|X^{-1}Y)$ qui est sous forme standard. G'' est donc la matrice d'un code linéaire systématique C' équivalent à C d'où le résultat.

Proposition 3.3.5. Soit C un $[n,k]$-code linéaire sur $\mathbb{F}_q$.
Si C est systématique de matrice génératrice G=$\Big[I_k|A\Big]$ alors une matrice génératrice de $C^{\perp}$ est donnée par $H = \Big[-{}^tA|I_{n-k}\Big]$.

Preuve . En effet, si $H = [-{}^tA|I_{n-k}]$, alors $H^t = \begin{bmatrix} -A \\ I_{n-k} \end{bmatrix}$ et $GH^t = \Big[I_k|A\Big]\begin{bmatrix} -A \\ I_{n-k} \end{bmatrix} = -A + A = 0$ d'où le résultat.

3.4 Domaines d'applications des codes linéaires

Les codes linéaires s'appliquent dans plusieurs domaines de la vie à l'instar de :

1. La sécurité informatique.
2. La cryptographie qui est l'ensemble des techniques qui au moyen d'un code secret visent à rendre un message indéchiffrable pour toute autre personne que son émetteur ou son destinataire.
3. La télécommunication.
4. stéganographie qui est l'ensemble de techniques permettant de transmettre une information en la dissimulant au sein d'une autre information (Photo,vidéo,texte, etc)

⋆ ⋆ CHAPITRE QUATRE ⋆ ⋆

APPROCHE DE CONSTRUCTION DES CODES LINÉAIRES À PARTIR DES GRAPHES BIPARTIS

4.1 Introduction

De façon générale les codes linéaires sur un corps sont des sous-espaces vectoriels de dimension finie qui peuvent être entièrement déterminer par leurs matrices génératrices. Le problème dans l'approche de construction des codes linéaires à l'aide des graphes bipartis est de savoir si à partir de la matrice d'adjacence d'un graphe biparti on peut obtenir une matrice qui engendre un code linéaire. Le chapitre 4 de ce Mémoire apporte des solutions à ce problème.

Définition 4.1.1. Soit G un graphe biparti de matrice d'adjacence $A(G)$.
La matrice $\overline{A}(G)$ est la matrice obtenue de $A(G)$ en remplaçant progressivement les 0 de la diagonale inférieure de $A(G)$ par des 1.

4.2 Principe de construction.

L'objectif de cette partie est de construire des codes linéaires de distance minimale $d \geq 3$. La construction d'un code binaire à partir d'un graphe biparti se fait en plusieurs étapes qui sont :

Etape 1 : Déterminer la matrice d'adjacence du graphe notée $A(G)$.

Etape 2 : Déterminer la matrice $\overline{A}(G)$.

Etape 3 : Construire une matrice génératrice du code associé au graphe par ajout de l'identité d'ordre k (I_k) à la matrice $\overline{A}(G)$ qui est d'ordre k, on obtient alors une matrice

génératrice de la forme $(I_k|\overline{A}(G))$.

4.3 Construction d'un code linéaire sur $\mathbb{F}_2$ à partir d'un graphe biparti.

Soient $n \geq 4$ et $V = \{v_1, v_2, v_3, \ldots, v_n\}$ un ensemble à n éléments ,V_1 non vide tel que $V_1 \subset V$,

$V_2 = V \backslash V_1$ et $E \subseteq V_1 \times V_2$. Le graphe $G = (V, E)$ est biparti.

Pour n=4,

Soit $V = \{v_1, v_2, v_3, v_4\}$ l'ensemble des sommets du graphe, partitionnons V en deux sous-ensembles V_1 et V_2. Posons alors $V_1 = \{v_1\}$; $V_2 = \{v_2, v_3, v_4\}$ et $E = V_1 \times V_2$, le graphe $G = (V, E)$ est biparti complet.

La matrice d'adjacence de G est :

$$A(G) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

En remplaçant 0 par 1 et 1 par 0, on obtient la matrice

$$\overline{A}(G) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

La matrice $(I_4|\overline{A}(G))$ définie comme suit est la matrice génératrice d'un code C.

$$\mathcal{G} = (I_4|\overline{A}(G)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

On définit alors $C(\mathcal{G})$ par $C(\mathcal{G}) = \{u\mathcal{G}/u \in \mathcal{V}_4(\mathbb{F}_2)\}$.

Une matrice de contrôle de $C(\mathcal{G})$ est

$$\begin{aligned} H &= (-{}^t\overline{A}|I_4) \\ &= ({}^t\overline{A}|I_4) \\ &= \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

car $-1 = 1$ dans $\mathbb{F}_2$.

On définit le dual de $C(\mathcal{G})$ par $C^{\perp}(H) = \{uH/u \in \mathcal{V}_4(\mathbb{F}_2)\}$.

Le code C(G) et son dual $C^{\perp}(H)$ sont des $[8, 4, 3]$-code, ces codes peuvent détecter au plus deux erreurs et corriger une seule.

Pour n=5,

Soit $V = \{v_1, v_2, v_3, v_4, v_5\}$ posons $V_1 = \{v_1, v_2\}$ et $V_2 = \{v_3, v_4, v_5\}$ on a

$V_1 \times V_2 = \{(v_1, v_3), (v_2, v_3), (v_1, v_4), (v_2, v_4), (v_1, v_5), (v_2, v_5)\}$. Posons $E = \{(v_1, v_3), (v_2, v_4), (v_1, v_5)\}$, $G = (V, E)$ est un graphe biparti, sa matrice d'adjacence est :

$$A(G) = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\overline{A}(G) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

En ajoutant I_5 à $\overline{A}(G)$ on obtient une matrice génératrice de la forme $(I_5|\overline{A}(G))$ définie par :

$$\mathcal{G} = (I_5|\overline{A}(G)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Une matrice de contrôle est définie par :

$$\begin{aligned} H &= (-{}^t\overline{A}(G)|I_5) \\ &= ({}^t\overline{A}(G)|I_5) \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

$C(G)$ et $C^{\perp}(G)$ sont des $[10, 5, 3]$-code de capacité correctrice 1.

4.4 Graphes bipartis isomorphes et codes linéaires associés.

Dans cette partie on s'intéresse aux relations qui existent entre les codes linéaires associés à deux graphes bipartis isomorphes. Soient G^1 et G^2 deux graphes bipartis isomorphes de matrices d'adjacences respective $A(G_1)$ et $A(G_2)$ alors il existe une matrice de permutation P telle que $A(G^1) = PA(G^2)P^{-1}$, P est la matrice donc toutes les entrées sont nulles sauf les $(\varphi(i), i)$ qui sont égales à 1 où φ est l'isomorphisme G^1 et G^2.

Proposition 4.4.1. Soient G^1 et G^2 deux graphes bipartis isomorphes de matrices d'adjacences respectives $A(G_1)$ et $A(G_2)$, alors :

$$\overline{A}(G^1) = P\overline{A}(G^2)P^{-1} \tag{4.1}$$

$$(I_n|\overline{A}(G^1)) = (I_n|P\overline{A}(G^2)P^{-1}) \tag{4.2}$$

$$(-{}^t\overline{A}(G^1)|I_n) = (-{}^tP^{-1}\,{}^t\overline{A}(G^2){}^tP|I_n) \tag{4.3}$$

En remplaçant $\overline{A}(G^1_n)$ par $\overline{A}(G^2_n)$ on obtient un résultat similaire.

Proposition 4.4.2. Les codes linéaires associés à deux graphes bipartis isomorphes sont équivalents.

Preuve . En permutant les lignes puis les colonnes de la matrice génératrice d'un des codes on obtient la matrice génératrice de l'autre, or permuter les colonnes de la matrice génératrice d'un code permet d'obtenir un code qui lui est équivalent on déduit donc le résultat.

Exemple 4.4.1. Soient $V = \{v_1, v_2, v_3, v_4, v_5\}$ et N=$\{1, 2, 3, 4, 5\}$, posons $V_1 = \{v_1, v_2\}$, $V_2 = \{v_3, v_4, v_5\}$, $N_1 = \{3, 4\}$ et $N_2 = \{1, 2, 5\}$.
On a alors $V_1 \times V_2 = \{(v_1, v_3), (v_1, v_4), (v_1, v_5), (v_2, v_3), (v_2, v_4), (v_2, v_5)\}$ et
$N_2 \times N_1 = \{(3, 1), (3, 2), (4, 1), (4, 2), (3, 5), (4, 5)\}$;prenons $E = \{(v_1, v_3), (v_2, v_3), (v_1, v_5), (v_2, v_4)\}$ et $F = \{(3, 2), (4, 2), (3, 1), (4, 5)\}$, alors $G^1 = (V, E)$ et $G^2 = (N, F)$ sont des graphes bipartis isomorphes pour l'application φ définie par :

$$\begin{array}{rccc} \varphi : & V & \longrightarrow & N \\ & v_1 & \longmapsto & 3 \\ & v_2 & \longmapsto & 4 \\ & v_3 & \longmapsto & 2 \\ & v_4 & \longmapsto & 5 \\ & v_5 & \longmapsto & 1 \end{array}$$

Les matrices d'adjacences de (V, E) et (N, F) sont respectivement

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

La matrice $P = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

est une matrice de permutation.
c'est-à-dire : $A(G^2) = PA(G^1)P^{-1}$

$$\overline{A}(G^1) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ et } \overline{A}(G^2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

On vérifie aussi que $\overline{A}(G^2) = P\overline{A}(G^1)P^{-1}$.

Les matrices génératrices des codes associés à G^1 et G^2 sont respectivement :

$$(I_5|\overline{A}(G^1)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ et } (I_5|\overline{A}(G^2)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

4.4.1 Distribution de poids et Polynôme énumérateur de poids de C et $C^\perp$

On a $C = \{uG/u \in \mathcal{V}_3(\mathbb{F}_2)\}$. Les mots de C sont :

$$\begin{aligned} (0,0,0)G &= (0,0,0,0,0,0) \\ (1,0,0)G &= (1,0,0,0,1,1) \\ (0,1,0)G &= (0,1,0,0,0,0) \\ (0,0,1)G &= (0,0,1,0,0,0) \\ (0,1,1)G &= (0,1,1,0,0,0) \\ (1,1,1)G &= (1,1,1,0,1,1) \\ (1,0,1)G &= (1,0,1,0,1,1) \\ (1,1,0)G &= (1,1,0,0,1,1) \end{aligned}$$

Désignons par P_i le nombre de mots de poids i,on a alors $P_0 = 1$, $P_1 = 2$, $P_2 = 1$, $P_3 = 1$, $P_4 = 2$ et $P_5 = 1$; $(1,2,1,1,2,1)$ est le vecteur de distribution de poids de C et le polynôme énumérateur de poids de C est donnée par :

$$\begin{aligned} W_C(x,y) &= \sum_{i=0}^{5} P_i x^{6-i} y^i \\ &= x^6 + 2x^5y + x^4y^2 + 2x^3y^3 + 2x^2y^4 + y^6 \end{aligned}$$

De même $C^\perp = \{uH/u \in \mathcal{V}_3(\mathbb{F}_2)\}$, les mots de codes de $C^\perp$ sont donnés par :

$$(0,0,0)H = (0,0,0,0,0,0)$$
$$(0,0,1)H = (1,0,0,0,0,1)$$
$$(0,1,1)H = (0,0,0,0,1,1)$$
$$(1,0,0)H = (0,0,0,1,0,0)$$
$$(0,1,0)H = (1,0,0,0,1,0)$$
$$(1,1,0)H = (1,0,0,1,1,0)$$
$$(1,1,1)H = (0,0,0,1,1,1)$$
$$(1,0,1)H = (1,0,0,1,0,1)$$

Désignons par Q_i le nombre de mots de poids i, on alors $Q_0 = 1$,$Q_1 = 1$, $Q_2 = 3$, $Q_3 = 3$, $Q_4 = 0$, $Q_5 = 0$; $(1,1,3,3,0,0)$ est le vecteur distribution de poids de $C^{\perp}$ et le polynôme énumérateur de poids de $C^{\perp}$ est :

$$\begin{aligned} W_{C^{\perp}} &= \sum_{i=0}^{5} Q_i x^{6-i} y^i \\ &= x^6 + x^5 y + 3x^4 y^2 + 3x^3 y^3 \end{aligned}$$

Remarque 4.4.1. On peut aussi obtenir le polynôme énumérateur de poids de $C^{\perp}$ en utilisation l'identité de MACWILLIAMS.

♣ IMPLICATIONS PÉDAGOGIQUES ♣

Dans cette partie nous présentons les apports de ce travail à notre formation d'enseignant de mathématiques. La rédaction de ce mémoire m'a permis de :

- ☞ Approfondir mes connaissances sur les structures algébriques et leurs applications. Cet apport me permettra de bien enseigner les espaces vectoriels et les matrices au lycée et me permettra également de motiver les élèves à étudier les mathématiques.
- ☞ Renforcer mes aptitudes à faire l'analyse et la synthèse d'un document scientifique.
- ☞ Maitriser l'utilisation du logiciel latex qui me permettra de :
  - Saisir des épreuves de mathématiques ;
  - Confectionner des fiches de Travaux dirigés ;
  - Produire des documents (livres,fascicule,etc).
- ☞ Faire la connaissance de plusieurs sites de téléchargement de documents mathématiques.
- ☞ Développer l'esprit d'initiative et d'innovation.
- ☞ Renforcer mes aptitudes à faire la recherche.

♣ Conclusion et perspectives ♣

Dans ce mémoire, nous avons présenté une méthode de construction des codes linéaires à l'aide des graphes bipartis et de regarder les paramètres de ces codes. Les résultats que nous avons obtenus sont les suivantes :

- Les codes ainsi construits (appelés codes mères) n'ont pas une bonne capacité correctrice mais peuvent détecter une erreur.
- De ces codes mères, nous obtenons des codes induits qui ont une capacité correctrice plus intéressante.

Les résultats précédents n'ont pas été généralisé, il serait intéressant de voir dans quelle mesure étendre ces travaux à des graphes à n sommets $(n \geq 5)$ pour avoir des résultats plus généraux et pouvoir appliquer à ces codes des algorithmes de décodage .

Les codes construits dans ce mémoire sont essentiellement binaires, étudier les matrices d'adjacence des graphes k-partis $(k \geq 3)$ nous permettra d'étendre notre étude sur des corps finis plus grands et d'avoir des codes ayant des distance minimale plus grandes.

♣ Bibliographie ♣

[1] C. AUDERSET (2003) *Théorie des Graphes,* notes de cours, Université de Fribourg.

[2] C.BERGE (1970), *Graphes et hypergraphes,* dunod, Paris.

[3] H.BHERER (2000), *Théorie algébrique du codage,* Mémoire pour l'obtention du grade de maître ès sciences, Université de Laval.

[4] J.CALAIS (2006), *Extensions de corps,* ellipses, Paris.

[5] M.DEMAZURE (2008), *Cours d'algèbre,* Cassini, Paris.

[6] R.DONGMO (2016-2017), *Images Q-aires des codes constacycliques sur une extension d'un corps de GALOIS,* Mémoire de Master, Université de Yaoundé I.

[7] C.MOUAHA (2015-2016), *Algèbre commutative,* Cours de MA 203 de deuxième année, ENS Yaoundé I.

[8] D.NEKELEYAN (2015-2016),*Codes linéaires sur les anneaux finis,* Mémoire de DipesII Mathématiques, ENS Yaoundé I.

[9] S.NDJEYA (2014-2015) *Groupes et Anneaux,* Cours de MA 103, ENS Yaoundé I.

[10] M.RIGO (2009-2010) *Théorie des graphes,* notes de cours, Université de Liège.