UNIVERSITE MOHAMED BOUDIAF DE M'SILA

Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Algèbre et Mathématiques Discrètes

Par

OUCIF Halima Elsaadiya

Sujet

Quelques propriétés combinatoires sur le monoïde libre

Date de soutenance : 01/07/2019

Devant le jury :

Mr. MIHOUBI Douadi	Prof. Univ de M'sila	Président
Mr. GHADBANE Nacer	MCA. Univ de M'sila	Encadreur
Mr. HEBOUB Lakhdar	MAA. Univ de M'sila	Examinateur

Promotion : 2018 / 2019

Dédicace

C'est avec une très grande émotion et un immense plaisir que je dédie ce modeste travail :

Aux cœurs de mes parentes.

A tous les membres de ma famille pour leur soutien et sa patience durant ces années.

A tous mes amies.

A tous ceux que j'aime.

A tous les étudiants de ma promotion.

Avec l'expression de tous mes sentiments de respect.

A tous ceux qui sont proches de mon cœur et dont je n'ai pas cité le nom.

Je demande à Dieu de préserver leur vie.

Remerciements

Avant toute chose, je tiens à remercier **«Allah»** *, notre créateur de nos avoir donné la force, la volonté et le courage afin d'accomplir ce modeste travail.*

J'exprime le grand remerciement à mon encadreur de mémoire **Dr. N.GHADBANE***, pour avoir accepté de m'encadrer, pour ses conseils et son enseignement, son support, ses encouragements du début a la fin de ce travail .*

Je tiens également à remercier messieurs les membres de jury

Mr. D. MIHOUBI

Mr. L. HEBOUB

pour l'honneur qu'ils m'ont fait en acceptant de siéger à mon soutenance.

Mes sentiments de reconnaissance et mes remerciements chaleureux vont également au ma famille, mes amis et mes collègues, mes proches par leurs soutien et leurs encouragements.

Je tiens à remercier toute personne qui participé de prés ou de loi de réalisation ce modeste travail.

Notations

$Card$: cardinal d'un ensemble.
$\mathcal{A}_n^p$: arrangement.
$\mathcal{C}_n^p$: combinaison.
I : l'ensemble d'indice.
$\equiv$: congruence.
A **:** alphabet fini.
A^* : l'ensemble des mots sur A.
$|u|$: la longeur du mot u.
$|u|_a$: le nombre d'occurence de la lettre a dans le mot u.
L : langage sur l'alphabet A.
$\mathcal{P}(A)$: l'ensemble des langage sur A.
L^n : la puissance n-iéme d'un langage L
L^* : fermeture itérative d'un langage$L$.(ou fermeture de Kleen).
$\leq_l$: l'ordre lexicographique sur A^*.
$\leq_a$: l'ordre radiciel sur A^*.
A^ω : l'ensemble des mots infinis sur A
A^∞ : l'ensemble des mots finis ou infinis sur A
L^ω : l'étoile in...nie du langage L.
$F(w)$: l'ensemble des facteurs d'un mot w.
$f_X(z)$: la fonction génératrice de l'ensemble X.

Table des matières

Introduction

La combinatoire, l'étude des arrangements d'objets, est une partie importante des mathématiques discrètes. Ce sujet a été étudié dès le XVIIe siècle, lorsque des questions combinatoires se sont posées dans l'étude des jeux de hasard. Énumération, comptage d'objets avec certaines propriétés, est une partie importante de la combinatoire. Nous devons compter les objets à résoudre nombreux types de problèmes. Par exemple, le comptage est utilisé pour déterminer la complexité des algorithmes. Il est également nécessaire de compter pour déterminer s'il ya suffisamment de numéros de téléphone ou adresses de protocole Internet pour répondre à la demande. Récemment, il a joué un rôle clé en mathématiques biologie, en particulier dans le séquençage de l'ADN. En outre, les techniques de comptage sont largement utilisées lorsque les probabilités d'événements sont calculées.

Dans ce mémoire nous allons étudier quelques propriétés combinatoires sur le monoïde libre

Ce travail est composé de trois chapitres :

Le premier chapitre consiste à un rappel des notions élémentaires sur la combinatoire.

Dans le deuxième chapitre nous allons étudier le monoïde libre et leurs propriétés.

Dans le troisième chapitre nous intéressons à quelques propriétés combinatoires sur les mots et les langages.

Chapitre 1

Principes de combinatoire

Ce premier chapitre introduit quelques concepts fondamentaux de la combinatoire

1.1 Principe d'addition et principe de multiplication

Définition 1.1

Soit Ω un ensemble, E et F deux parties de Ω, on définit alors :

1.L'intersection de E et F par l'ensemble $E \cap F$ défini par :

$$E \cap F = \{x \in \Omega, x \in E \text{ et } x \in F\}.$$

2.L'union de E et F par l'ensemble $E \cup F$ défini par :

$$E \cup F = \{x \in \Omega, x \in E \text{ ou } x \in F\}.$$

Plus généralement, si I est un ensemble quelconque, et $(E_i)_{i \in I}$ une famille de parties de Ω, on définit :

1.L'intersection des E_i par l'ensemble $\bigcap_{i \in I} E_i$ défini par :

$$\bigcap_{i \in I} E_i = \{x \in \Omega, \forall i \in I, x \in E_i\}.$$

2.L'union des E_i par l'ensemble $\bigcup_{i \in I} E_i$ défini par :

$$\bigcup_{i\in I} E_i = \{x \in \Omega, \exists i \in I, x \in E_i\}.$$

Définition 1.2

Un ensemble Ω est fini, s'il existe un entier naturel non nul n tel que Ω soit en bijection avec $[1, n]$. Il ya alors unicité d'un tel entier n, que l'on appelle cardinal de Ω et on note $Card(\Omega)$. Par convention on dit que l'ensemble vide est de cardinal 0, et on note $Card(\varnothing) = 0$.

Exemple 1.1

$\Omega = \{0, 2, 4, 6, 8, 10\}$ est fini, mais $\bigcup_{i\in\mathbb{N}} \{-3i, 3i\}$ n'est pas fini.

Définition 1.3

Soit E et F deux ensembles, leurs produit cartésien noté $E \times F$ est l'ensemble :

$$E \times F = \{(x, y) : x \in E, y \in F\}.$$

En générale si $E_1, E_2, ..., E_n$, n ensembles leur produit cartésien est :

$$E_1 \times E_2 \times ... \times E_n = \{(e_1, e_2, ..., e_n) : \forall i = 1...n, e_i \in E_i\}.$$

$(e_1, e_2, ..., e_n)$ est dit un n-uplet .

Proposition 1.1

Si E et F deux ensembles finis disjoints (i.e, $E \cap F = \varnothing$), *alors :*

$$Card(E \cup F) = Card(E) + Card(F).$$

Soit $E_1, E_2, ..., E_n$, n ensembles deux à deux disjoints, alors :

$$Card(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} Card(E_i).$$

Autrement dit : si une procédure peut être divisée en k évenement ou cas dont les évenements sont indépendants (mutuellement exclusifs), avec la première pouvant se

faire de e_1 façons, la deuxième pouvant se faire de e_2 façons,..., la dernière de e_k façons, alors, le nombre total de résultats possibles est : $e_1 + e_2 + ... + e_k$.

Exemple 1.2

Dans une bibliothéque 50 livres de mathématiques en français et 40 livres de mathématiques en anglais (et aucun dans une autre langue). On peut donc choisir un livre de mathématiques de $50 + 40 = 90$ façons différentes.

Exemple 1.3

Soit C l'ensemble de tous les carrés dont les cotés sont matérialisés. Notons C_1, C_2, C_3 et C_4 l'ensemble des ces carrés ayant pour cotés respectifs 1, 2, 3 et 4 carreaux, les sous-ensembles C_1, C_2, C_3 et C_4 constituent une partition (deux à deux disjoints) de C . D'aprés le principe d'addition :

$$Card(C) = \sum_{i=1}^{4} Card(C_i) = 16 + 9 + 4 + 1 = 30.$$

Proposition 1.2

Soit E et F deux ensembles finis, alors :

$$Card(E \times F) = Card(E) \times Card(F).$$

Plus généralement, si *$F_1, F_2, ..., F_n$ sont des ensembles non vides, alors le nombre d'éléments de leur produit cartésien est* :

$$Card(\prod_{i=1}^{n} F_i) = \prod_{i=1}^{n} Card(F_i).$$

En particullier, soient n un entier naturel non nul, et F un ensemble fini, alors :

$$Card(F^n) = (Card(F))^n.$$

Autrement dit : Supposons que p expériences doivent être réalisées. Si l'expérience 1 peut produire l'un quelconque de n_1 résultats et si pour chacun d'entre eux, il y a n_2

résultats possibles pour l'expérience 2*, et ainsi de suite, alors il y'a* $n_1 \times n_2 \times ... \times n_p$ *résultats possibles pour les* p *expériences .*

Preuve.

Soit $F_1 = \{a_1, a_2, ..., a_n\}$ et $F_2 = \{b_1, b_2, ..., b_m\}$ deux ensembles finis, le produit cartésien $F_1 \times F_2$ peut être partitionnè comme suit : $(a_1 \times F_2) \cup (a_2 \times F_2) \cup ... \cup (a_n \times F_2)$ où $\forall i, j \in \overline{1...n}$, avec $i \neq j$ on a $(a_i \times F_2) \cap (a_j \times F_2) = \varnothing$. Par suite on a :

$$\begin{aligned} Card(F_1 \times F_2) &= Card(\bigcup_{i=1}^{n} \{a_i\} \times F_2) \\ &= \sum_{i=1}^{n} Card(\{a_i\} \times F_2) \\ &= \sum_{i=1}^{n} Card(\{a_i\} \times Card(F_2) \\ &= \sum_{i=1}^{n} Card(\{a_i\} \times m \\ &= m + m + ... + m \text{ (Le terme } m \text{ } n \text{ fois)} \\ &= n \times m. \end{aligned}$$

■

Exemple 1.4

Une plaque d'immatriculation de voitures est constitue de 3 lettres suive de 4 chiffres, on peut former $26 \times 26 \times 26 \times 10 \times 10 \times 10 \times 10$ plaques.

Exemple 1.5

Un menu offre comme choix

1. Entrée : Nachos ou Salade (2 choix).
2. Plat principal : Hamburger, cheese burger ou Fish & Chips (4 choix).
3. Breuvage : thé, lait, cola, ou jus.(4 choix).

Alors le nombre de différents repas est : $2 \times 4 \times 4 = 32$ repas différents.

Exemple 1.6

Sur une petite bibliothéque il ya 5 livres différents de calcul, 6 livres différents d'algèbre et 7 livres différents de combinatoire. On peut donc choisir une paire de livres de types différents de 107 façons différentes.

En effet, on a trois cas mutuellement exlusifs peuvent se produire, on peut choisir une paire algèbre-calcul, une paire algèbre-combinatoire, ou une paire combinatoire-calcul. Ainsi, d'aprés le principe de multiplication et le principe d'addition il existe $5 \times 6 + 6 \times 7 + 5 \times 7 = 107$ sélections de livres possibles.

1.2 Principe d'inclusion -Exclusion

Proposition 1.3

Pour compter le nombre total d'éléments de deux ensembles E et F, *on compte le nombre d'éléments de* E, *on lui ajoute le nombre d'éléments de* F *et on soustrait le nombre d'éléments que l'on* a *compté deux fois, à savoir ceux de* $E \cap F$. *Autrement dit, soit* E *et* F *deux ensembles finis quelconques (disjoints ou non), alors*

$$Card(E \cup F) = Card(E) + Card(F) - Card(E \cap F).$$

Plus généralement, partant de la somme $\sum_{i=1}^{n} Card(E_i)$, *on soustrait et on ajoute successivement le cardinal des intersections de ces ensembles, changeant de signe à chaque fois qu'on opère sur un plus* grand nombre *d'ensembles à la fois. En symboles, soit* $E_1, E_2, ..., E_n$ *sont des ensembles finis, alors :*

$$\begin{aligned} Card(\bigcup_{i=1}^{n} E_i) &= \sum_{i=1}^{n} Card(E_i) - \sum_{1 \le i < j \le n} Card(E_i \cap E_j) \\ &\quad + \sum_{1 \le i < j < k \le n} Card(E_i \cap E_j \cap E_k) - \\ &\quad ... + (-1)^{n+1} Card(\bigcap_{i=1}^{n} E_i). \end{aligned}$$

Preuve.

On a les égalites suivantes :

$$\begin{aligned} E \cup F &= (E \backslash F) \cup (F \backslash E) \cup (E \cap F) \\ E \backslash F &= E \backslash (E \cap F) \\ F \backslash E &= F \backslash (E \cap F) \end{aligned}$$

De même on a :

$$\begin{aligned} Card(E \backslash F) &= Card(E) - Card(E \cap F) \\ Card(F \backslash E) &= Card(F) - Card(E \cap F) \end{aligned}$$

Donc :

$$\begin{aligned} Card(E \cup F) &= Card(E \backslash F) + Card(F \backslash E) + Card(E \cap F) \\ &= Card(E) - Card(E \cap F) + Card(F) - Card(E \cap F) + Card(E \cap F) \\ &= Card(E) + Card(F) - Card(E \cap F). \end{aligned}$$

On utilise la récurrence sur $n \geq 2$ pour $n = 3$, soit E, F et G des ensembles finis

$$\begin{aligned} Card(E \cup F \cup G) &= Card((E \cup F) \cup G) \\ &= Card(E \cup F) + Card(G) - Card((E \cup F) \cap G) \\ &= Card(E) + Card(F) - Card(E \cap F) \\ &\quad + Card(G) - Card((E \cup F) \cap G). \quad (*) \end{aligned}$$

On a :

$$\begin{aligned}(E \cup F) \cap G &= (E \cap G) \cup (F \cap G).\\ Card((E \cup E) \cap F) &= Card((E \cap G) \cup (F \cap G))\\ &= Card(E \cap G) + Card(F \cap G) - Card(E \cap F \cap G) \quad (**)\end{aligned}$$

Donc de $(*)$ et $(**)$ on a :

$$\begin{aligned}Card(E \cup F \cup G) &= Card(E) + Card(F) + Card(G) - Card(E \cap F) - Card(E \cap G)\\ &\quad -Card(F \cap G) + Card(E \cap F \cap G).\end{aligned}$$

Supposons que la formule est vraie pour n et on la demontrons pour $n+1$, soit $E_1, E_2, ..., E_n, E_{n+1}$, $n+1$ ensembles finis.

$$\begin{aligned}Card(\bigcup_{i=1}^{n+1} E_i) &= Card((\bigcup_{i=1}^{n} E_i) \cup E_{n+1})\\ &= Card(\bigcup_{i=1}^{n} E_i) + Card(E_{n+1}) - Card(\bigcup_{i=1}^{n} E_i \cap E_{n+1})\\ &= \sum_{i=1}^{n} Card(E_i) - \sum_{1 \le i < j \le n} Card(E_i \cap E_j)\\ &\quad + \sum_{1 \le i < j < k \le n} Card(E_i \cap E_j \cap E_k) - .....\\ &\quad +(-1)^{n+1} Card(\bigcap_{i=1}^{n} E_i) + Card(E_{n+1}) - Card(\bigcup_{i=1}^{n} E_i \cap E_{n+1}).\end{aligned}$$

On applique l'hypothèse de réccurrence au dernier terme.

$Card((\bigcup_{i=1}^{n} E_i) \cap E_{n+1}) = \sum_{i=1}^{n} Card(E_i \cap E_{n+1}) - \sum_{1 \le i < j \le n} Card(E_i \cap E_j \cap E_{n+1}) +$
$.. + (-1)^{n+1} Card(\bigcap_{i=1}^{n} E_i \cap E_{n+1})$

Alors :

$$\begin{aligned} Card(\bigcup_{i=1}^{n+1} E_i) &= \sum_{i=1}^{n+1} Card(E_i) - \sum_{1\leq i<j\leq n+1} Card(E_i \cap E_j) \\ &+ \sum_{1\leq i<j<k\leq n+1}^{n+1} Card(E_i \cap E_j \cap E_k) - ... + (-1)^{n+2} Card(\bigcap_{i=1}^{n+1} E_i). \end{aligned}$$

■

Exemple 1.7

Dans un groupe de 67 étudiants, 47 sont inscrits à un cours d'Allemand, 35 à un cours d'Espagnol et 23 aux deux cours. Désignant par E et F les ensembles d'étudiants inscrits respectivement en Allemand et en Espagnol, on a

$$Card(E \cup F) = Card(E) + Card(F) - Card(E \cap F) = 47 + 35 - 23 = 59$$

Exemple 1.8

Soit D l'ensemble des entiers entre 1 et 12000 divisible par 4 ou 6, et D_4 et D_6 les ensembles des entiers divisible par 4 ou par 6(ou bien les deux).

On a $Card(D) = Card(D_4 \cup D_6) = Card(D_4) + Card(D_6) - Card(D_4 \cap D_6)$.

Il est claire que $Card(D_4) = \frac{12000}{4} = 3000$ et $Card(D_6) = \frac{12000}{6} = 2000$.

Et $D_4 \cap D_6$ l'ensemble des entiers qui divisible par 4 et 6 (un nombre qui divisible par 4 et 6 est divisible par le $ppcm(4, 6) = 12$)

Donc $Card(\ D_4 \cap D_6) = \frac{12000}{12} = 1000$.

Alors $Card(D) = 3000 + 2000 - 1000 = 4000$.

Corollaire 1.1

Si $E_i \cap E_j = \emptyset, \forall i \neq j$, alors $Card(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} Card(E_i)$.

1.3 Permutations, Arrangements, Combainaisons

Définition 1.4

Soit E un ensemble à n éléments. On appelle permutation de E une suite ordonnée de n éléments distincts de E.

Proposition 1.4

Le nombre de permutations d'un *ensemble à n éléments est* :

$$n! = n \times (n-1) \times (n-2) \times ... \times 3 \times 2 \times 1.$$

Exemple 1.9

Il ya $3! = 6$ de ranger l'une aprés l'autre les lettres A, B, C.

$$ABC \quad ACB \quad BCA \quad BAC \quad CAB \quad CBA.$$

Théorème 1.1

Le nombre d'applications d'un ensemble à p éléments dans un ensemble à n éléments est n^p.

Définition 1.5

Soit E un ensemble à n éléments est soit p tels que $1 \leq p \leq n$, on appelle un arrangement d'ordre p d'un ensemble E de n éléments est une suite ordonnée de p éléments de E.

Proposition 1.5

Le nombre d'arrangements avec répétition d'ordre p de E est n^P.

Le nombre des arrangements sans répétition d'ordre p sur un ensemble de n éléments est : $\mathcal{A}_n^p = n \times (n-1) \times (n-2) \times \cdots \times (n-p+1) = \frac{n!}{(n-p)!}$.

Théorème 1.2 .

Le nombre d'injections d'un ensemble à p éléments dans un ensemble à n éléments est $\mathcal{A}_n^p$.

Exemple 1.10

Soit $E = \{A, B, C\}$, le nombre des mots différentes de longeur 2 est $\mathcal{A}_3^2 = \frac{3!}{(3-2)!}$=6 : $AB \quad AC \quad BA \quad BC \quad CA \quad CB$.

Définition 1.6

Soit n et p deux entiers naturales avec $0 \leq p \leq n$, une combinaison de longueur p d'un ensemble E de n éléments est un sous-ensemble de p éléments de E. (Les éléments sont pris sans répétition et ne sont pas ordonnés). On note $\mathcal{C}_n^p$ ou $\binom{n}{p}$.

Proposition 1.6

Le nombre des combinaisons de longueur p sur un ensemble de n éléments :

$$\mathcal{C}_n^p = \frac{n!}{(n-p)!p!} = \frac{\mathcal{A}_n^p}{p!}.$$

Exemple 1.11

Les combinaisons à deux éléments de l'ensemble $\{1, 2, 3\}$ sont : $\mathcal{C}_3^2 = \frac{3!}{2!} = 3$: $\{1, 2\}, \{1, 3\}, \{2, 3\}$.

Proposition 1.7

Soient $n \in \mathbb{N} - \{0\}$ et $p \in \mathbb{N}, 1 \leq p \leq n$. On a les propriétés suivantes :
1. $\mathcal{C}_n^p = \mathcal{C}_n^{n-p} = \frac{n}{p}\mathcal{C}_{n-1}^{p-1}$.
2. $\mathcal{C}_n^p = \frac{n}{n-p}\mathcal{C}_{n-1}^p = \frac{n-p+1}{p}\mathcal{C}_n^{p-1}$.
3. $\mathcal{C}_n^p = \mathcal{C}_{n-1}^p + \mathcal{C}_{n-1}^{p-1}$.

Exemple 1.12

Le triangle de Pascal se construit via la formule : $\mathcal{C}_n^p = \mathcal{C}_{n-1}^p + \mathcal{C}_{n-1}^{p-1}$.

$n \setminus p$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Proposition 1.8

Un ensemble à n éléments a exactement 2^n sous-ensembles.

Proposition 1.9

$$(x+y)^n = \sum_{p=0}^{n} \mathcal{C}_n^p x^n y^{n-p} = \mathcal{C}_n^0 x^0 y^n + \mathcal{C}_n^1 x^1 y^{n-1} + ... + \mathcal{C}_n^n x^n y^0.$$

Proposition 1.10

Pour tout entier n, on a $(1+x)^n = \sum_{p=0}^{p=n} C_n^p x^{n-p}$.

Exemple 1.13

Soit $(1+3x)^{10}$, le terme qui contient x^7est $C_{10}^3 1^3 (3x)^7 = 3^7 C_{10}^3 x^7$, alors le coefficient de x^7est $3^7 C_{10}^3 = 262,440$.

1.4 Séries génératrices

Les séries génératrices sont des outils algébrique qui permet de reformuler des problèmes de combinatoire afin de les transformer en des problèmes de manipulation d'expressions algébriques. En particulier, en combinatoire, il s'agit souvent de déterminer le nombre d'objets d'un certain type qui sont de taille n, ce qui donne lieu à une suite $(a_n)_{n\in\mathbb{N}}$ dont on cherche à déterminer le $n-ième$ terme.

En particulier, la série génératrice d'une suite finie est un polynôme.

Définition 1.7

Soit $(a_n)_{n\in\mathbb{N}}$ une suite de réels ou complexs. On définit la série génératrice de $(a_n)_{n\in\mathbb{N}}$ comme la série formelle $\sum_{k\geq 0} a_k x^k \in K[x]$ où K est un corps.

Exemple 1.14

- Soit n un entier, si la suite $a_n = 1, \forall n \in \mathbb{N}$, on a alors
  $f(x) = \sum_{n\geq 0} x^n = 1 + x + x^2 + ... + x^n + ...$
  On remarque alors
  $xf(x) = \sum_{n\geq 0} x^n = x(1 + x + x^2 + ...) = x + x^2 + x^3 + ... = 1 - f(x),$

i.e, $xf(x) = 1 - f(x)$, par suit $(1 - x)f(x) = 1$. Donc

$$f(x) = \sum_{n\geq 0} x^n = \frac{1}{1-x}$$

- Soit la suite $(1, a, a^2, a^3, ...)$, on a $\sum_{n\geq 0} x^n = 1 + x + x^2 + ... = \frac{1}{1-x}$.....(1)
  On substitue x par ax dans (1), alors :
  $\sum_{n\geq 0}(ax)^n = 1 + ax + (ax)^2 + ... + (ax)^n + ... = \frac{1}{1-ax}$

$$f(x) = \sum_{n\geq 0}(ax)^n = \frac{1}{1-ax}$$

En particulier, si $a = -1$, Soit la suite $(1, -1, 1, -1, ...)$,
on a alors $g(x) = \sum_{n\geq 1}(-1)^n x^n = \frac{1}{1+x}$

Définition 1.8

- La somme de deux séries génératrices se définit de manière assez évidente en sommant les suites correspondantes.

$$(\sum_{n\geq 0} a_n x^n) + (\sum_{n\geq 0} b_n x^n) = \sum_{n\geq 0}(a_n + b_n)x^n.$$

- Le produit est un peu plus compliqué. Il se fait par analogie avec le produit des polynômes :

$$(\sum_{m\geq 0} a_m x^m)(\sum_{n\geq 0} b_n x^n) = \sum_{m,n\geq 0} a_m b_n x^{n+m} = \sum_{n\geq 0}(\sum_{k\geq 0} a_k b_{n-k})x^k.$$

Le produit est donc également une série génératrice, correspondant à la suite $(\sum_{k\geq 0} a_k b_{n-k})_n$

- La dérivée au sens formel d'une série génératrice se défnit sans trop de problèmes par analogie avec les polynômes :

$$(\sum_{n\geq 0} a_n x^n)' = (\sum_{n\geq 1} n a_n x^{n-1}).$$

Exemple 1.15

- Soit la somme $C(n,k) = \sum_{a_1+\ldots+a_k=n} a_1 \ldots a_k$, avec $S(x) = \sum_{n\geq 1} n x^n$. On peut calculer $C(n,k)$, donc comme $S(x)^k = \sum_{n\geq 1} C(n,k)\, x^n$ d'où $C(n,k) = C_{2k-1}^{n+k-1}$.
- La suite des entiers de Fibonacci est définie par :

$$F_0 = 0.$$

$$F_1 = 1.$$

$F_n = F_{n-1} + F_{n-2}$, pour $n \geq 2$.

Soit $F(x)$ la série géneratrice de la suite de des entiers de Fibonacci $F(x) = \sum_{n\geq 0} F_n x^n$.

On a : $F_n = F_{n-1} + F_{n-2}$, pour $n \geq 2$ donc $\sum_{n\geq 2} F_n x^n = \sum_{n\geq 2} F_{n-1} x^n + \sum_{n\geq 2} F_{n-2} x^n$, pour $n \geq 2$

$\sum_{n\geq 2} F_n x^n = F(x) - F_0 - F_1 x = F(x) - x$

$\sum_{n\geq 2} F_{n-1} x^n = x \sum_{n\geq 2} F_{n-1} x^{n-1} = x(F(x) - F_0) = xF(x)$

$\sum_{n\geq 2} F_{n-2} x^n = x^2 \sum_{n\geq 2} F_{n-2} x^{n-2} = x^2 F(x)$

$F(x) - x = xF(x) + x^2 F(x)$

Donc

$$F(x) = \frac{x}{1 - x - x^2} \quad .$$

Chapitre 2

Etude sur le monoïde libre

2.1 Monoïde

Dans ce qui suit, on donne quelques défnitions et notations concernant le monoïde libre.

Définition 2.1

Un monoïde est un ensemble M muni d'une loi interne, i.e, d'une application " $\cdot$ " : $M \times M \longrightarrow M$ qui satisfait aux conditions suivantes :

1. L'opération " $\cdot$ " est associative :

$$\forall x, y, z \in M : (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

2. Il existe un élément neutre $1_M \in M$ tel que

$$\forall x \in M : x \cdot 1_M = 1_M \cdot x = x.$$

Un élément $m^{'} \in M$ est dit le symétrique de l'élement $m \in M$ si $m \cdot m^{'} = m' \cdot m = 1_M$.

Exemple 2.1

1. $(\mathbb{R}, \times, 1), (\mathbb{N}, +, 0)$ et $(\mathbb{N}, \times, 1)$ sont des monoïdes, où $+$ et $\times$ dénotent respectivement l'addition et la multiplication usuelles.

2. L'ensemble des applications d'un ensemble Q vers lui même
   $Q^Q = \{f \ / \ Q \to Q\}$ muni de la composition des applications est un monoïde dont l'application identique noté 1_Q est l'élément neutre.
3. L'ensemble des parties d'un ensemble E , muni de l'union d'ensembles $(P(E), \cup)$ est un monoïde dont l'ensemble vide est l'élément neutre. Le même ensemble muni de l'intersection d'ensemble $(P(E), \cap)$ est aussi un monoïde, dont l'ensemble E est l'élément neutre.

Remarque 2.1

Un monoïde $(M, \cdot)$ qui est tel que tout élément de M posséde un symétrique est un groupe.

Remarque 2.2

Tout groupe est un monoïde mais l'inverse n'est pas toujours vrai.

Définition 2.2

Soit un monoïde $(M\ , \cdot,\ 1_M\ )$. Un sous-monoïde de M est un triplet $(N, \cdot', 1_N)$ tel que :

1. $N \subseteq M$.
2. $1_M = 1_N$.
3. $\forall m, m' \in N : m \cdot m' \in N$.

Exemple 2.2

Soit $(2\mathbb{N}, +, 0)$ l'ensemble des nombres paires et $(2\mathbb{N}+1, +, 0)$ l'ensemble des nombres impaires $(2\mathbb{N}, +, 0)$ est un sous-monoïde de $(\mathbb{N}, +, 0)$ engendré par $\{2\}$ tandis que $(2\mathbb{N}+1, +, 0)$ n'est pas un sous-monoïde de $(\mathbb{N}, +, 0)$.

Définition 2.3

Soit $(M, ., 1_M\ )$ un monoïde, une congruence sur $(M, ., 1_M\ )$ est une relation d'équivalence notée $\equiv$ stable par la multiplication à droite et à gauche, c'est-a-dire :

$$\forall x, y, z \in M : x \equiv y \implies x \cdot z \equiv y \cdot z \text{ et } z \cdot x \equiv z \cdot y$$

Exemple 2.3

On définit sur le monoïde $(\mathbb{Z}, +)$ la relation de congruence modulo n par :

$$x \equiv y[n] \iff \exists k \in \mathbb{Z}, x - y = k.n$$

- La relation est réflexive car $x \equiv x[n]$ puisque $x - x = 0.n, 0 \in \mathbb{Z}$
- La relation est symétrique car si $x \equiv y[n], \exists k \in \mathbb{Z}, x - y = k.n$
  $\implies y - x = (-k); n$, où $k \in \mathbb{Z}, (-k) \in \mathbb{Z}$ donc $y \equiv x[n]$.
- Enfin, la relation est transitive car $x \equiv y[n]$ et $y \equiv z[n]$,$\exists k \in \mathbb{Z}, x - y = k.n$ et $\exists l \in \mathbb{Z}, y - z = l.n$. On aditionnant memebre a membre on obtient
  $(x - z) = (k + l).n$,ou $(k + l) \in \mathbb{Z}$, donc $x \equiv z[n]$.
- La relation est compatible avec le loi de monoïde à he on $x \equiv x^{'}[n], \exists k \in \mathbb{Z}$, $x - x^{'} = k.n$,et $y \equiv y^{'}[n], \exists l \in \mathbb{Z}, y - y^{'}$. Alors par addition
  $x + y - (x^{'} + y^{'}) = (k + l).n$, donc $x + y \equiv (x^{'} + y^{'})[n]$.

Définition 2.4

Soit M un monoïde et une congruence $\equiv$ définie sur M. Le quotient $M/\equiv$ est le monoïde des classes de congruence de M pour la relation $\equiv$. La loi de composition de $M/\equiv$ est défnie de la manière suivante : $\overline{u} *_{M/\equiv} \overline{v} = \overline{u *_M v}$.

La projection naturelle (la surjection canonique) de M dans $M/\equiv$ est noté P.

2.2 Mot et langage

On introduit dans ce paragraphe quelques définitions, propriétés et notations concernant les mots et les langages.

Définition 2.5

Un alphabet (vocabulaire) est un ensemble fini quelconque. Les éléments d'un alphabet sont appelés lettres, caractères ou symboles. Ainsi $\Omega = \{a, .., z\}, \Sigma = \{0, 1\}$ sont des alphabets.

Définition 2.6

Soit A un alphabet. Un mot u sur A est une suite finie de lettres de A. Par exemple $\alpha\beta\alpha$ et $\beta\beta$ sont deux mots sur l'alphabet $\{\alpha, \beta\}$. La longueur d'un mot u est le nombre de lettres constituant ce mot, noté $\mid u \mid$. Ainsi $\mid \alpha\beta\alpha \mid = 3$ et $\mid \alpha\beta\alpha\alpha\beta \mid = 5$. L'unique mot de longueur 0 est le mot correspondant à la suite vide. Ce mot s'appelle le mot vide et on le note ϵ, ou bien 1.

L'ensemble des mots sur A est noté A^*, et l'ensemble des mots non vides noteé A^+ ($A^+ = A^* - \{\epsilon\}$) sur A.

Autrement dit,

$$A^* = \bigcup_{n=0}^{+\infty} A^n \text{ et } A^+ = \bigcup_{n=1}^{+\infty} A^n$$

Par exemple : $\{0,1\}^* = \{\epsilon, 0, 1, 00, 01, 10, 11, , 000, 001, ...\}$ (ϵ est le mot vide).

$$\{0,1\}^+ = \{0, 1, 00, 01, 10, 11, , 000, 001, ...\}.$$

Si a est une lettre de l'alphabet A, pour tout mot $u = a_1a_2...a_k \in A^*$, on note par

$$\mid u \mid_a = Card\{i \in \{1, 2, ..., k\} : a_i = a\}$$

le nombre d'occurrences de la lettre a dans le mot u et $u(i)$ sa i-ème lettre. Par exemple, $|\alpha\beta\beta\alpha\gamma|_\alpha = 2$ et $|\alpha\beta\beta\alpha\gamma|_\gamma = 1$. Ainsi, pour tout mot u et v de A^*, on a,

$$\mid u \mid = \sum_{a \in A} \mid u \mid_a \text{ et } \mid uv \mid_a = \mid u \mid_a + \mid v \mid_a .$$

Définition 2.7

Soient $u = a_1\alpha_2...a_n$ et $v = \beta_1\beta_2...\beta_m$ de mots A^*. La concatination de u et v est le mot noté $u \cdot v$ ou simplement uv et défini par : $uv = a_1a_2...a_n\beta_1\beta_2...\beta_m$. Par exemple la concaténation de 001 et 1111 est 0011111.

elle est une opération associative admettant le mots vide comme élément neutre.

$$\forall x, y, z \in A^* : (xy)z = x(yz).$$

$$\forall x \in A^* : x.\epsilon = \epsilon.x = x.$$

On notera u^n la concaténation de n copie de u avec bien sur $u^0 = \epsilon$.

Remarque 2.3

Il est utile de remarquer que si $Card(A) > 1$, alors A^*est un monoïde non commutatif, i.e, il existe $u, v \in A^*$ tels que $uv \neq vu$.

Proposition 2.1

Pour tous $u, v \in A^*$*, on a*

$|uv| = |u| + |v|$

$|u^n| = n.|u|, n \in \mathbb{N}$

Proposition 2.2

1. *L'ensemble* A^* *est infini* .
2. *L'ensemble* A^**est dénombrable.*

Preuve.

1. L'ensemble A^* est infini, en effet on a $A^* = \bigcup_{n=0}^{+\infty} A^n = A^0 \cup A^1 \cup ... \cup A^n \cup ...$

2. Montrons que A^* est dénombrable. Comme A est fini, on peut donc numéroter ses éléments, par exemple, si $A = \{\alpha, \beta, \gamma\}$, alors $n(\alpha) = 1, n(\beta) = 2, n(\gamma) = 3$. Ensuit, soit u un mot A^*, on considére les longueur $|u|$ premiers nombre premiers, par exemple si $|u| = 5$, on a les 5 premiers nombre premiers sont : $p(1) = 2$, $p(2) = 3$, $p(3) = 5$, $p(4) = 7$, $p(5) = 11$.

On forme le nombre $f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$, oú $u(i)$ désigne la i-éme lettre de u par exemple si $u = \alpha\gamma\beta\alpha\alpha$, alors

$f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))} = \prod_{i=1}^{i=5} p(i)^{n(u(i))} = 2^1 \times 3^3 \times 5^2 \times 7^1 \times 11^1$. Donc on peut définir une application $f : A^* \longrightarrow \mathbb{N}, u \longmapsto f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$ par l'unicité de la décomposition d'un entier en facteurs premier, l'application f est injective. Enfin, comme f est injective et l'ensemble $\mathbb{N}$ est dénombrable, alors A^* est dénombrable. ■

Proposition 2.3

Soit A un alphabet quelconque. Le monoïde possède les deux propriétés suivantes :

1. *Tout élément de* A^* *est une suite finie d'éléments de A.*
2. *Deux suites distinctes d'éléments définissent deux éléments distincts de* A^**.*

A^* est le seul monoïde satisfaisant les propriétés 1 et 2, on dit que A^* est le monoïde libre sur A.

Définition 2.8

Soit X une partie de A^*. Le sous- monoïde de A^* engendré, noté X^* est défini par :

$$X^* = \{x_1...x_n : n \geq 0, x_i \in X\}.$$

Proposition 2.4

Soit P et Q deux partitions de monoide libre A^*, on dit que P est plus fine que Q si :$\forall p \in P, \exists q \in Q$ tel que $p \subseteq q$ dans ce cas en dit que P et plus fine que Q ou bien Q plus grossière que P.

Exemple 2.4

Soit le monoïde $(\mathbb{Z}, +)$ On définit sur $(\mathbb{Z}, +)$ les deux congrunces $\equiv_1$et $\equiv_2$suivantes :

$$\begin{cases} x \equiv_1 y \iff x \equiv y\,[2] \text{ ,i.e,} \exists k \in \mathbb{Z} : x - y = 2k. \\ x \equiv_2 y \iff x \equiv y\,[4] \text{ ,i.e,} \exists k \in \mathbb{Z} : x - y = 4k. \end{cases}$$

Il est clair que $\equiv_2 \subset \equiv_1$. En effet, si $x \equiv_2 y$, i.e, $x \equiv y\,[4]$, alors $\exists k \in \mathbb{Z} : x-y = 4k$ et par conséquent $\exists k \in \mathbb{Z} : x-y = 2(2k)$ i.e, $x \equiv_1 y$. On a $P = \left\{[0]_{\equiv_2}, [1]_{\equiv_2}, [2]_{\equiv_2}, [3]_{\equiv_2}\right\}$ et $Q = \left\{[0]_{\equiv_1}, [1]_{\equiv_1}\right\}$ sont deux partitions de $\mathbb{Z}$. De plus , on a $[0]_{\equiv_2} \cup [2]_{\equiv_2} \subset [0]_{\equiv_1}$ et $[0]_{\equiv_2} \cup [3]_{\equiv_2} \subset [1]_{\equiv_1}$. Donc P plus fini que Q.

Définition 2.9

Soit A un alphabet. On appelle langage sur A toute partie (sous-ensemble) L de A^*. L'ensemble des langages sur A est donc :

$$\mathcal{P}(A^*) = \{L, L \subset A^*\}$$

Un langage sur un alphabet est donc un ensemble de mots sur cet alphabet.

Deux langages particuliers sont indépendants de l'alphabet A

– Le langage vide ($L = \varnothing$).

– Le langage contenant le seul mot vide($L = \{\epsilon\}$).

Proposition 2.5

- A^* est le plus grand langage sur A au sens de l'inclusion.
- $\mathcal{P}(A^*)$ est un monoïde libre pour la concaténation où $\{\epsilon\}$ est l'élement neutre.

Exemple 2.5

1. $L_1 = \{aa, ab, ba, bb\}$ est le langage sur l'alphabet $A = \{a, b\}$ composé des mots de longueur 2.
2. $L_2 = \{w \in \{\alpha, \beta\}^*, |w|_\alpha = |w|_\beta\}$ est le langage sur l'alphabet $A = \{\alpha, \beta\}$ composé des mots contenant autant de α que de β.
3. $L_3 = \{\epsilon, abc, aabbcc, aaabbbccc, ...\}$, soit tous les mots contenant n occurrences de la lettre a, suivies de n occurrences de la lettre b, suivies d'autant de fois la lettre c. Ce langage est noté $\{a^n b^n c^n | n \geq 0\}$.

Définition 2.10

Les langages étant des ensembles, on peut appliquer les opérations définies sur ces derniers :

- L'union de deux langages L_1et L_2, est le langage, noté $L_1 \cup L_2$ constitué des mots appartenant à L_1ou à L_2,

$$L_1 \cup L_2 = \{x | x \in L_1 \text{ou } x \in L_2\}.$$

- L'intersection de L_1 et L_2, est le langage, noté $L_1 \cap L_2$ constitué des mots appartenant à L_1 et à L_2,

$$L_1 \cap L_2 = \{x | x \in L_1 \text{et } x \in L_2\}.$$

- La différence de L_1 et L_2 est le langage, noté $L_1 - L_2$, constitué des mots appartenant à L_1 et n'appartenant pas à L_2

$$L_1 - L_2 = \{x | x \in L_1 \text{et } x \notin L_2\}.$$

- Le complémentaire de L est le langage

$$L^c = \{x : x \notin L\}.$$

Définition 2.11

Soient $L, K \subseteq A^*$, deux langages. La concaténation des langages L et K est le langage,

$$LK = \{uv : u \in L, v \in K\}.$$

En particulier, on peut définir la puissance n-iéme d'un langage L, $n > 0$, par :

$$L^n = \{w_1...w_n : \forall i \in \{1, ..., n\}, w_i \in L\}.$$

Et on pose $L^0 = \{\epsilon\}$

Exemple 2.6

– Considérons les deux langages $L = \{00, 11\}$ et $K = \{0, 1, 01\}$ définis sur $\{0, 1\}$.
$LK = \{000, 001, 0001, 110, 111, 1101\}$
– $M = \{00, 11\}$, alors $M^2 = \{0000, 0011, 1100, 1111\}$.

Définition 2.12 (Fermeture itérative d'un langage)

La fermeture itérative d'un langage L (ou fermeture de Kleene ou itéré de L) est l'ensemble des mots formés par une concaténation de mots de L :

$$L^* = \{w : \exists k \geq 0 \text{ et } w_1...w_k \in L\}.$$

Autrement dit, $L^* = \bigcup_{n \geq 0} L^i$. De même, on définit $L^+ = \bigcup_{n \geq 1} L^i$.

Proposition 2.6

$L^0 = \{\epsilon\}$.
$L^1 = L$.
$L^2 = LL$.
$L^i = LL...L$, la concaténation de i copies de L
$L^* = \bigcup_{n \geq 0} L^i$.

Exemple 2.7

Soient $A = \{a, b\}$ un alphabet, $L_1 = \{a\}$, $L_2 = \{ab\}$ et $L_3 = A$ trois langages sur A. On a $L_1^* = \{a^n, n \geq 0\}$, $L_2^* = \{(ab)^n\}$ et $L_3^* = A^*$.

Remarque 2.4

On voit facilement que L^* est le plus petit langage contenant L et le mot vide et qui soit stable par concaténation.

Définition 2.13

Soit L un langage sur un alphabet A, la congrunce syntaxique de L noteé $\equiv_L$est définie par :

$$\forall u, v \in A^*, (u \equiv_L v) \iff (\forall x, y \in A^*, xuy \in L \iff xvy \in L).$$

2.3 Homomorphisme de monoïdes

Dans ce paragraphe, nous donnerons quelques propriétés sur la notion d'un homomorphisme de monoïdes.

Définition 2.14

Soient $(M\ ,.,\ 1_M\ )$ et $(M', .', 1_{M'})$ deux monoïdes. Un morphisme (ou encore homomorphisme) de monoïdes de M dans M' est une application $f : M \to M'$ vérifiant :

- $\forall x, y \in M,\ f(x.y) = f(x).'f(y)$.
- $f(1_M) = 1_{M'}$.

Un isomorphisme de monoïdes est un homomorphisme bijectif de monoïdes.

Exemple 2.8

L'application : $h : (\mathbb{R}, +) \to (\mathbb{R}\backslash\{0\}, \times)$, $x \longmapsto a^x$, tel que a un élément fixé de $\mathbb{R}\backslash\{0\}$ est une homomorphisme de $(\mathbb{R}, +, 0)$ dans $(\mathbb{R}\backslash\{0\}, \times, 1)$.

Exemple 2.9

Soit $A = \{\alpha, \beta\}$, $f : \{\alpha, \beta\}^* \to (\mathbb{Z}, +)$ définie par : $f(\alpha) = 1$, $f(\beta) = -1$, $f(\epsilon) = 0$. Est est un homomorphisme de $\{\alpha, \beta\}^*$ dans $(\mathbb{Z}, +)$.

Définition 2.15

Un morphisme (*ou homomorphisme*) de monoïdes de A^* dans B^* est une application $\varphi : A^* :\to B^*$staisfait :

$$\forall x, y \in A^*, \varphi(xy) = \varphi(x)\varphi(y).$$

Remarque 2.5

- Un morphisme de monoïdes libres est entièrement défini par l'image des lettres :
  $h(\epsilon) = \epsilon$,
  $h(a_1...a_n) = h(a_1)...h(a_n)$.
- Un morphisme f sur A est effaçant s'il existe une lettre a tel $f(a) = \epsilon$ (ou de manière équivalente, s'il existe un mot non vide u tel que $f(u) = \epsilon$).
- Un morphisme f sur A est prolongeable en $a \in A$ s'il existe un mot non vide s tel que $f(a) = as$.
- Un mot w est un point fixe d'un morphisme f, si $f(w) = w$.
- Le morphisme identité sur A est noté Id_A.

Exemple 2.10

L'application longueur $|.| : A^* \to \mathbb{N}$ est un morphisme de monoïdes entre $(A^*, .)$ et $(\mathbb{N}, +)$. En effet,

$$\forall u, v \in A^* : |uv| = |u| + |v| \text{ et } |\epsilon| = 0.$$

Exemple 2.11

Fonction de Parikh : Soit un alphabet $A = \{a_1, a_2, ..., a_n\}$ de cardinal $n \geq 1$, et ordonné (avec $a_1 \leq a_2 \leq ... \leq a_n$). On définit alors la fonction de Parikh par :

$$\begin{aligned} \Psi &: A^* \longrightarrow \mathbb{N}^n \\ \Psi(w) &= (\mid w \mid_{a_1}, ..., \mid w \mid_{a_n}) \end{aligned}$$

est une morphisme de monoïde entre $(A^*, .)$ et $(\mathbb{N}^n, +)$.

La proposition suivante justife le fait que le monoïde A^* soit appelé monoïde libre. Cette propriété caractérise le monoïde libre engendré par A.

Proposition 2.7

Toute fonction $\psi : A \to M$ de A dans un monoïde M se prolonge de façons unique en un morphisme de A^* dans M.

Preuve.

L'existence : Posons

$\widetilde{\psi}(\epsilon) = 1_M$ et $\widetilde{\psi}(a_1a_2...a_n) = \psi(a_1)\psi(a_2)...\psi(a_n)$, $n \in \mathbb{N}$, $1 \leq i \leq n$, $a_i \in A$.

Et facile de voir $\widetilde{\psi}$ que est bien un homomorphisme.

L'Unicité :

Soient $\widetilde{\psi}$ et $\widetilde{\vartheta}$ deux homomorphismes de dans M tels que :

$\forall a \in A, \widetilde{\psi}(a) = \widetilde{\vartheta}(a)$

Alors $\widetilde{\psi}(\epsilon) = \widetilde{\vartheta}(\epsilon) = 1_M$ et pour tout mot $w = a_1a_2...a_n$

On a $\widetilde{\psi}(w) = \widetilde{\psi}(a_1a_2...a_n) = \psi(a_1)\psi(a_2)...\psi(a_n) = \widetilde{\vartheta}(a_1a_2...a_n) = \widetilde{\vartheta}(w)$. ■

Définition 2.16

Soit f un morphisme de monoïdes entre A^* et B^*. On remarque que f est complétement caractérisé par les images de f sur les symboles de A, si L est un langage sur A, alors l'image de L par le morphisme f est $f(L) = \{f(u) \in B^* : u \in L\}$.

de la même maniére, si M est un langage sur B, alors l'image inverse de M par le morphisme f est $f^{-1}(M) = \{u \in A^* : f(u) \in M\}$.

Chapitre 3

La combinatoire sur le monoïde libre

3.1 Opérations sur les mots

Définition 3.1

On dit que v est un facteur de u s'il existe deux mots $x, y \in A^*$ tels que $u = xvy$. Si $x = \epsilon$, alors on dit que v est un préfixe ou (facteur gauche). Si $y = \epsilon$, alors on dit que v est un suffixe ou (facteur droit).

Le mot v est un facteur (resp. préfixe, suffixe) propre d'un mot u si $v \neq u$ et v est un facteur (resp. préfixe, suffixe) de u.

Exemple 3.1

Soit l'alphabet $A = \{\alpha, \beta\}$ et le mot $u = \alpha\beta\beta\alpha\beta$, l'ensemble de ses facteurs est :

$$\{\epsilon, \alpha, \beta, \alpha\beta, \beta\alpha, \beta\beta, \alpha\beta\beta, \beta\alpha\beta, \beta\beta\alpha, \alpha\beta\beta\alpha, \beta\beta\alpha\beta, \alpha\beta\beta\alpha\beta\}\,.$$

L'ensemble de ses préfixes est :

$$\{\epsilon, \alpha, \alpha\beta, \alpha\beta\beta, \alpha\beta\beta\alpha, \alpha\beta\beta\alpha\beta\}\,.$$

Et l'ensemble de ses suffixes est :

$$\{\epsilon, \beta, \alpha\beta, \beta\alpha\beta, \beta\beta\alpha\beta, \alpha\beta\beta\alpha\beta\}.$$

Remarque 3.1

La relation "est préfixe de", souvent notée $\preceq$ est une relation d'ordre appelée ordre préfixiel.

1. $\forall \alpha \in A^*, \alpha \preceq \alpha$ (refléxivité).
2. $\forall \alpha, \beta, \gamma \in A^*$, si $\alpha \preceq \beta$ et $\beta \preceq \gamma$, alors $\alpha \preceq \gamma$ (transitivité).
3. $\forall \alpha, \beta \in A^*$, si $\alpha \preceq \beta$ et $\beta \preceq \alpha$, alors $\alpha = \beta$ (antisymétrie).

Définition 3.2

Soit L un langage de A^*, on définit,
Le langage des préfixes de L, noté $Pref(L)$ par :
$Pref(L) = \{u \in A^*, \exists v \in A^* : uv \in L\}$.
Le langage des suffixes de L, noté $Suff(L)$ par :
$Suff(L) = \{u \in A^*, \exists v \in A^* : vu \in L\}$.
Le langage des facteurs de L, noté $Fac(L)$ par :
$Fac(L) = \{u \in A^*, \exists v, w \in A^* : vuw \in L\}$.

Définition 3.3

Deux mots w_1 et w_2 sont dits conjugues s'il exsiste deux mots $x, y \in A^+$ tels que :

$$w_1 = xy \text{ et } w_2 = yx$$

Soit $u \in A^+$, La classe de conjuguaison de u est l'ensemble de ses conjugués.

Exemple 3.2

Soit le mot $v = \alpha\beta\beta\alpha\beta$, l'ensemble de ses conjugués est :

$$\{\alpha\beta\beta\alpha\beta, \beta\beta\alpha\beta\alpha, \beta\alpha\beta\alpha\beta, \alpha\beta\alpha\beta\beta, \beta\alpha\beta\beta\alpha\}.$$

Définition 3.4

- Soit $u = u_1u_2...u_k$ un mot de A^*. L'image miroir de u est le mot $u_ku_{k-1}...u_1$, noté $\widetilde{u}$, par exemple $\widetilde{\epsilon} = \epsilon$, si $u = 0101$, alors $\widetilde{u} = 1010$.
- Un mot w sur l'alphabet A est un palindrome si $w = \epsilon$ ou $w = w_1...w_n = w_n...w_1$ avec $n =\mid w \mid$, et $w_i \in A$, $1 \leq i \leq n$.

Définition 3.5 (puissance d'un mot)

Pour tout mot $u \in A^*$, on définit récursivement la puissance de u :
$u^0 = \epsilon$ et $\forall n \in \mathbb{N}, u^{n+1} = u^nu = uu^n$.

Définition 3.6

Un entier $p, 1 \leq p \leq \mid w \mid$, est une période de $w = a_1...a_n$, si, et seulement si $a_i = a_{i+p}$ pour tout entier i entre 1 et $\mid w \mid -p$. Par convention, la longueur de w est une période de w. On note $P(w)$ l'ensemble des périodes de w.

Définition 3.7

Un mot w est primitif s'il ne s'écrit pas $w = u^k$ avec $k \geq 2$. Autrement dit, un mot est primitif si sa longueur est l'unique période qui divise sa longueur. Tout mot w s'écrit de manière unique $w = u^k$ où l'entier k vérifie $k \geq 1$ et le mot u est primitif. L'entier k est égal à 1 quand w est primitif.

Exemple 3.3

Le mot $u = 010101$ a $P(u) = \{2, 4, 6\}$ pour ensemble de périodes. Il n'est pas primitif car il s'écrit $u = (01)^3$. Le mot $v = 01001010010$ a $P(v) = \{5, 8, 10, 11\}$.

Définition 3.8

On suppose que l'alphabet A est totalement ordonné. L'ordre lexicographique sur A^* noté $\leq_l$ est défini par $u \leq_l v$ ssi

1. Soit u est un préfixe de v.
2. Sinon $u = tu'$, $v = tv'$ avec $u' \neq \epsilon$ et $v' \neq \epsilon$, et le premier lettre de u' précède celui de v'.

Définition 3.9

L'ordre radiciel (ordre militaire) noté $\leq_a$ est défini comme suit : $u \leq_a v$ si, et seulement si,

1. $|u| \leq |v|$.
2. $|u| = |v|$ et $u \leq_l v$.

Exemple 3.4

1. $ab \leq_l abb$ et $ababb \leq_l abb$.
2. $ab \leq_a ba$ et $b \leq_a ab$.

Proposition 3.1

Sur un alphabet binaire, tout mot de longueur au moins 4 *contient un carré, i.e., un facteur de la forme* uu, $u \neq \epsilon$.

3.2 Mots infinis

Définition 3.10

Un mot infini sur un alphabet A est une suite infinie de lettres indicée par entiers naturels non nul. Il peut être vu comme une application de $\mathbb{N}^*$ dans A. La i ^{éme} lettre d'un mot infini w est notée $w(i)$.

L'ensemble des mots infinis sur A sera noté A^ω. On désignons $A^\infty = A^* \cup A^\omega$.

Définition 3.11

La concaténation sur A^* est étendue à A^∞ de la manière suivante :
$\forall f \in A^*, \forall u \in A^\omega$, pour tout $i \in \mathbb{N}^*$, $fu\,(i)$ est défini par :
$$\begin{cases} \text{si } i \leq |f|\text{, alors } fu\,(i) = f\,(i) \\ \text{si } i > |f|\text{, alors } fu\,(i) = u\,(i - |f|) \end{cases}$$
Et $\forall u \in A^\omega, \forall \alpha \in A^\infty$, on pose $u\alpha = u$.

Définition 3.12

On définit sur A^∞ une distance ultramètrique telle que, pour tous $f, g \in A^\infty$,

$$\begin{cases} d(f,g) = 2^{-Min\{i \in \mathbb{N}^* : f(i) \neq g(i)\}} \text{ si } f \neq g, \\ 0 \text{ si } \ f = g. \end{cases}$$

Relativement à cette métrique (A^∞, d) forme un espace complet.

Définition 3.13

Soit $L \subset A^*$ un langage, l'étoile infinie du langage L, noté L^ω est défini comme suit :

$L^\omega = \{u \in A^\omega : u = u_1 ... u_n ..., \ n \in \mathbb{N}^*, \ u_i \in L - \{\epsilon\}\}$.

Exemple 3.5

Pour $L = ba^*$, on a $L^\omega = (ba^*)^\omega$, l'ensemble des mots infinis qui contiennent un nombre infini de b.

Définition 3.14

Soit $L \subset A^*$ un langage. La limite de L notée $Lim(L)$ est l'ensemble de mots infinis sur A ayant une infinité de facteurs gauches dans L.

$Lim(L) = \{u \in A^\omega : Card(FG(u)) \cap L = \omega\}$.

Exemple 3.6

$Lim(ba^*) = \{u \in A^\omega : Card(FG(u)) \cap L = ba^*\} = ba^\omega$.

Définition 3.15

L'adherence d'un langage L, notée $Adh(L)$ est l'ensemble de mots infinis dont les facteurs gauches sont les facteurs gauches de L,

$Adh(L) = \{u \in A^\omega : FG(u) \subseteq FG(L)\}$.

Proposition 3.2 *(Maurice Nivat)*

Pour tous $L_1, L_2 \subseteq A^\infty$, on a les égalités suivantes :

1. $Adh(L_1 \cup L_2) = Adh(L_1) \cup Adh(L_2)$.
2. $Adh(L_1 \cdot L_2) = Adh(L_1) \cup L_1 \cdot Adh(L_2)$.
3. $Adh(L_1) = Adh(L_1^\omega) = L_1^* \cdot Adh(L_1) \cup L_1^\omega$.

Définition 3.16

- Un mot infini w est périodique s'il existe un entier $p > 0$ tel que, pour tout entier i, $w_i = w_{i+p}$. L'entier p appelé une période de w.
- Si w est périodique de période p et si u est le préfixe de longueur p de w, alors w sera noté u^ω (le mot u est aussi parfois appelé période de w).
- Un mot infini w est périodique s'il est de la forme uv^ωpour des mots u et v avec $v \neq \epsilon$.

Définition 3.17

Un mot fini u est facteur d'un mot infini w, s'il existe un mot fini p et un mot infini s tel que $w = pus$. Si $p = \epsilon$, u est un préfixe de w. L'ensemble des facteurs d'un mot w sera noté $F(w)$. L'ensemble des facteurs de longueur n sera noté $F_n(w)$.

Pour un sous-ensemble X de A^ω, on note par $F_X(w)$ L'ensemble des des facteurs des mots sur X.

Un mot infini s est un suffixe d'un mot infini w, s'il existe un mot fini p tel que $w = ps$. Le mot s est un suffixe propre de w si $p \neq \epsilon$.

Définition 3.18

Une suite $(u_n)_{n\geq 0}$ de mots finis sur A converge vers un mot infini w si tout préfixe de w est le préfixe de tous les u_n à l'exception d'un nombre fini. Ce mot w est unique Nous noterons

$$w = \lim_{n\to\infty} u_n$$

Définition 3.19

- Un mot fini u est récurrent dans un mot infini w s'il apparaît infiniment souvent dans w.
- Un mot infini est récurrent si tous ses facteurs sont récurrents.

Définition 3.20

Deux mots sont multiplicativement dépendants s'ils sont puissance d'un même troisième mot : u et v sont multiplicativement dépendants s'il existe un mot w et des entiers i, j tels que

$$u = w^i \text{ et } v = w^j.$$

Proposition 3.3

Deux mots commutent si et seulement si ils sont multiplicativement dépendants.

Preuve.

On procède par récurrence sur la longueur de uv. Si $|uv| = 0$, le résultat est immédiat. Supposons à présent le résultat satisfait pour $|uv| < n$. Soient u, v tels que $|uv| = n$. On peut même considérer que $u \neq \epsilon$ et $v \neq \epsilon$ car sinon, le résultat serait trivial. Si $|u| = |v|$, alors il est immédiat que $u = v$. Sinon, on peut supposer que $|u| < |v|$. Donc il existe $\acute{u}$ tel que $v = \acute{u}u$ et $|\acute{u}| < |v|$. Ainsi, $uv = u\acute{u}u = vu = \acute{u}uu$ et donc on trouve $\acute{u}u = u\acute{u}$. Puisque $|u\acute{u}| < |uv|$, on peut appliquer l'hypothése de récurence. Il existe un mot w et des entiers p, q tels que $u = w^p$ et $\acute{u} = w^q$. Pour conclure, On remarque que $v = \acute{u}u = w^{p+q}$ ■

Remarque 3.2

Noter que la réciproque du résultat ci-dessus est triviale.

Lemme 3.1 *(lemme de levi)*

$\forall u, v, x, y \in A^*$, $uv = xy \Rightarrow \exists t \in A^*$ tels que. soit $u = xt$ et $tv = y$, soit $x = ut$ et $v = ty$.

Preuve.

Posons $u = a_1a_2...a_n$, $v = a_{n+1}...a_m$ avec $a_i \in A$ et $1 \leq i \leq m$, de même $x = b_1b_2...b_k$, $y = b_{k+1}...b_q$ avec $b_i \in \Sigma$ et $1 \leq i \leq q$, comme $uv = xy$, nous avons $m = q$ (mais pas nécessairement $n = k$) et $a_i = b_i$ pour $i = 1, 2, ...m$, de sorte que $x = a_1a_2...a_k$ et $y = a_{k+1}...a_m$. Si $|x| = k \leq n = |u|$, posons $t = a_{k+1}...a_n$, alors $u = xt$ avec $tv = y$.

Si $|x| > |u|$ posons $t = a_{n+1}...a_k$ alors $ut = x$ et $v = ty$. ■

Corollaire 3.1

Soient $u, v, w, t \in A^*$.

1. *Si $uv = wt$ et $|u| = |w|$ alors $u = w$ et $v = t$.*

2. *Pour tout* $i \in \mathbb{N} - \{0\}$, $(u^i = v^i \implies u = v)$.

Lemme 3.2

Le monoïde libre A^* *est simplifiable C'est à dire pour tous mots* $u, v, w, t \in A^*$ *:*

1. $uv = uw \implies v = w$.
2. $uv = wv \implies u = w$.
3. $uvw = utw \implies v = t$.

Lemme 3.3

Soient A *un alphabet et* x, y *des mots sur* A*. Les propositions suivantes sont équivalentes :*

1. $xy = yx$.
2. *il existe deux entiers* n *et* m *non tous deux nuls tels que* $x^n = y^m$.
3. *il existe un mot* z *et deux entiers* p *et* q *tels que* $x = z^p$ *et* $y = z^q$.

Lemme 3.4

Pour tout mot w *non vide, il existe un unique mot primitif* z *tel que* $w = z^n$ *pour un entier* $n \geq 1$.

Lemme 3.5

Soient u *et* v *deux mots conjugués. Le mot* u *est primitif si et seulement si* v *est primitif.*

Théorème 3.1

Si $xy = yz$*, avec* $x \neq \epsilon$ *, alors* $\exists u, v \in A^*$ *et un entier* $k \geq 0$ *tels que :*

$$x = uv, y = (uv)^k u = u(vu)^k, z = vu.$$

Preuve.

Si $|x| \geq |y|$, alors le résultat précédent nous permet d'écrire directement $x = yt$, ce qui, en identifiant u et y, et v à t, nous permet de dériver directement les égalités voulues.pour $k = 0$.

Le cas où $|y| > |x|$ se traite par induction sur la longueur de y.

Le cas où $|y|$ vaut 1 étant immédiat, supposons la relation vraie pour tout y de longueur au moins n, et considérons y avec $|y| = n+1$. Il existe alors t tel que $y = xt$, d'où l'on dérive $xtz = xxt$, soit encore $tz = xt$, avec $|t| \leq n(\text{car } |x| > 0)$. L'hypothèse de récurrence garantit l'existence de u et v tels que $x = uv$ et $t = (uv)^k u$, d'où $y = uv(uv)^k u = (uv)^{k+1}u$. ■

Théorème 3.2

Si $xy = yx$, avec $x \neq \epsilon$,$y \neq \epsilon$, alors $\exists u \in A^*$ et deux indices i et j tels que $x = u^i$ et $y = u^j$.

Preuve.

Ce résultat s'obtient de nouveau par induction sur la longueur de xy. Pour une longueur égale à 2 le résultat vaut trivialement. Supposons le valable jusqu'à la longueur n, et considérons xy de longueur $n+1$. Par le théorème précédent, il existe u et v tels que $x = uv, y = (uv)^k u$, d'où on déduit : $uv(uv)^k u = (uv)^k uuv$, soit encore $uv = vu$. En utilisant l'hypothèse de récurrence il vient alors : $u = t^i, v = t^j$, puis encore $x = t^{i+j}$ et $y = t^{i+k(i+j)}$, qui est le résultat recherché. ■

Théorème 3.3 *(Fine et Wilf)*

Si un mot w posséde deux périodes p et q

et si $|w| \geq p + q - pgcd(p, q)$, alors $pgcd(p, q)$ est aussi une période de w.

Preuve.

Soit $d = p\gcd(p, q)$ le plus grand commun diviseur de p et q. On fixe d et on prouve le résultat par récurrence sur la valeur de $p+q$. Si $p+q \leq d$, c'est-à-dire $p = d$ et $q = 0$ ou $p = 0$ et $q = d$, le résultat est trivial et on suppose qu'il est vrai pour les entiers inférieurs à $p+q$. Soit w un mot tel que $|w| \geq p+q-d$ et ayant p et q comme périodes. Par symétrie, on peut supposer que $p \geq q$. Le mot w est alors factorisé $w = uv$ où u est de longueur $p-d$. Pour tout $1 \leq i \leq q-d$, on a $u_i = w_i = w_{i+p} = w_{i+p-q} = u_{i+p-q}$ et u a donc $p-q$ comme période. Comme u a aussi q comme période, l'hypothèse de récurrence implique que u a $d = p\gcd((p-q), q)$ comme période. Comme $|u| \geq q$, le préfixe de w de longueur q a aussi d comme période. Comme w a q comme période et que d divise q, alors w a aussi d comme période

■

Proposition 3.4

Les mots sans carré (Thue) : on dit qu'un mot contient un carré si il possède deux facteurs identiques successifs. Par exemple, le mot 011011001 *contient les carrés* 11 *et* 00*, ainsi que les carrés* 011011 *et* 110110*. Il est aisé de constater que les seuls mots en binaire n'ayant pas de carré sont* $0, 1, 01, 10, 010, 101$*. Des mots infinis sans carré peuvent être obtenus en considérant les points fixes de systèmes de substitution. Par exemple, Thue en* 1906 *donne des premiers mots sans carré sur un alphabet de* 4 *lettres en considérant la substitution* $a = abacb$*,* $b = abdcb$*,* $c = abcdb$ *et* $d = abcbd$*.*

3.3 La combinatoire des mots et les séries génératrices

Définition 3.21 (Mot de Fibonacci)

Les mots de Fibonacci sur l'alphabet $\{a, b\}$, que nous noterons $(f_n)_{n\geq 0}$, sont les mots définis par :

$$\begin{aligned} f_0 &= a. \\ f_1 &= ab. \\ f_{n+2} &= f_{n+1}f_n, \text{ pour } n \geq 0. \end{aligned}$$

Les premiers termes sont : $a, ab, aba, abaab, abaababa, abaababaabaab...$

Le mot infini de Fibonacci est $f = \lim_{n\to\infty} f_n$.

Définition 3.22 (Mot de Thue-Morse)

Les mots de Thue-Morse sur l'alphabet $\{a, b\}$, que nous noterons $(t_n)_{n\geq 0}$, sont les mots définis par : $t_0 = a$ et, pour $n \geq 1$, $t_n = t_{n-1}\overline{t_{n-1}}$, où $\overline{a} = b$ et $\overline{b} = a$.

Le mot infini $t = \lim_{n\to\infty} t_n$ est appelé le mot de Thue-Morse.

Définition 3.23

Un mot $l \in A^*$ est un mot de Lyndon si $l \in A^+$ et strictement plus petit, pour l'ordre lexicographique, que chacun de ses suffixes propres. Ainsi, le mot $v = abbab$ n'est pas un mot de Lyndon car il est plus grand que ab qui est un de ses facteurs droits propres. Par contre, le mot $aabab$ est un mot de Lyndon.

Proposition 3.5

Soit f un endomorphisme sur A non-effaçant et prolongeable en $a \in A$. Soit s le mot tel que $f(a) = as$.

Pour $n \geq 0$ entier, soit $u_n = f^n(a)$ et $v_n = f^n(s)$.

1. *Pour $n \geq 0$ entier, $u_{n+1} = u_n v_n$, et en particulier u_n est un préfixe de u_{n+1}.*
2. *Pour $n \geq 0$ entier, $u_{n+1} = a v_0 v_1 .... v_n$.*
3. *le mot infini $x = asf(s)f^2(s)..f^n(s)...est \lim_{n\to\infty} u_n$. De plus, il est l'unique mot commençant par a point fixe de f.*

Le mot x dans la proposition précédente est aussi noté $f^\omega(a)$ *et est appelé mot morphique.On dit aussi qu'il est engendré par morphisme*.

Preuve.

1.$u_{n+1} = f^{n+1}(a) = f^n(f(a)) = f^n(as) = f^n(a)f^n(s) = u_n v_n$.

2.pour $n = 0$, et par induction on a $u_{n+1} = u_n v_n = a v_0 v_1 ... v_{n-1} v_n$.

3. il est claire que x est limite , donc

$$f(x) = f(a)f(s)f^2(s)... = x.$$

■

Exemple 3.7

- Mot de Thue-Morse : mot engendré par le morphisme μ défini par $\mu \begin{cases} \mu(a) = ab. \\ \mu(b) = ba. \end{cases}$
- Mot de Fibonacci : mot engendré par le morphisme φ défini par $\varphi \begin{cases} \varphi(a) = ab. \\ \varphi(b) = b. \end{cases}$

Définition 3.24

Pour chaque ensemble $X \subseteq A^*$, la fonction génératrice ou la série génératrice de X est la série formelle : $f_X(z) = \sum_{n\geq 0} u_n z^n$ tel que $u_n = Card(X \cap A^n)$.

Avec $\begin{cases} A^0 = \{\epsilon\} \\ A^{n+1} = A^n A = AA^n \text{ pour } n \geq 0 \end{cases}$

Exemple 3.8

– L'ensemble $X = \{\beta, \alpha\beta\}$ sur l'aphabet $A = \{\alpha, \beta\}$. La série f_X est

$$f_X(z) = z + z^2.$$

Car, on a $f_X(z) = \sum_{n\geq 0} u_n z^n$ tel que $u_n = Card(X \cap A^n)$

$u_0 = Card(X \cap A^0) = |\{\beta, \alpha\beta\} \cap \{\epsilon\}| = |\{\varnothing\}| = 0.$

$u_1 = Card(X \cap A^1) = |\{\beta, \alpha\beta\} \cap \{\alpha, \beta\}| = |\{\beta\}| = 1.$

$u_2 = Card(X \cap A^2) = |\{\beta, \alpha\beta\} \cap \{\alpha\alpha, \alpha\beta, \beta\beta, \beta\alpha\}| = |\{\alpha\beta\}| = 1.$

$u_n = 0, \forall n \geq 3$

$f_X(z) = \sum_{n=0}^{2} u_n z^n = 0 + z + z^2 = z + z^2$

– L'ensemble $Y = \{\alpha\beta, \beta\gamma, \gamma\alpha\}$ sur l'aphabet $B = \{\alpha, \beta, \gamma\}$. La série f_Y est

$$f_Y(z) = 3z^2$$

Car :

$v_0 = Card(Y \cap B^0) = |\{\alpha\beta, \beta\gamma, \gamma\alpha\} \cap \{\epsilon\}| = |\{\varnothing\}| = 0.$

$v_1 = Card(Y \cap B^1) = |\{\alpha\beta, \beta\gamma, \gamma\alpha\} \cap \{\alpha, \beta, \gamma\}| = |\{\varnothing\}| = 0.$

$v_2 = Card(Y \cap B^2) = |\{\alpha\beta, \beta\gamma, \gamma\alpha\} \cap \{\alpha\alpha, \alpha\beta, \beta\beta, \beta\alpha, \gamma\alpha, \gamma\beta, \gamma\gamma\}| = |\{\alpha\beta, \beta\gamma, \gamma\alpha\}| = 3.$

$v_n = 0, \forall n \geq 3$

$$f_Y(z) = \sum_{n=0}^{2} v_n z^n = 0 + 0 + 3z^2 = 3z^2.$$

Conclusion

Au terme de ce travail, Nous avons donné une étude sur quelques propriétés combinatoires sur le monoïde libre.

Nous avons présenté dans le premier chapitre quelques concepts fondamentaux de la théorie de combinatoire. On introduire exactement aux principes de combinatoire.

Ensuite, nous avons étudié le monoïde libre et par conséquence les mots et les langages, morphismes de monoïde.

En fin, on s'intéressé a la combinatoire sur le monoïde libre qui l'étude des propriétés structurelles des mots, on présente principalement quelques opérations sur les mots, par suite on étudier les mots infinis et quelques propriétés, ainsi , on consacrée a la combinatoire des mots et les séries génératrices.

Bibliographie

[1] **R.B.J.T.Allenby et A.Slomson**, *How to count an introduction to combinatorics, S*econd édition, CRC Press, 2011.

[2] **P. Berlioux, M. Echenim et M. Lévy**, *Théorie des langage*s, Ècole nationale supérieure d'informatique et de mathématiques appliquées de France, 2009.

[3] **W.Bradley et Jackson,D.Thoro**, *Applied combinatorics with problems solving*, San jose state Université, 1990.

[4] **O. Carton**., *Langages formels,Calculabilité et Complexité*, Année 2007/2008.

[5] **C. Cusack et D.Santo**s, *An active introduction to discrete mathematics and algorithms*, 2015.

[6] **C.Deschamps et A.Warusfel**, *Mathématiques tout -en -*1^{re} *année cours et exercices corrigés* , Dunod.

[7] **N. Ghadbane**, *Cours Master1*, *Semi groupes et automates finis*, Université de M'sila, 2017-2018.

[8] **N. Ghadbane**, *Systèmes de réécriture et le problème du mot dans un monoïde*, Thèse de Doctorat, Université de M'sila, 2017.

[9] **L.Kane**, *Combinatoire et algorithmique des factorisations tangentes à l'identité*, Thèse de Doctorat, Université Paris, Sorbonne Paris cité, 2014.

[10] **S. Lipschutz et M. L. Lipson**, *Discrete Mathematics*, Temple University, University of Virginia.

[11] **S. Lombardy**, *Approche structuelle de quelques problémes de la théorie des automats* , Thèse de Doctorat, Ècole nationale supérieur des télecommunications, 2001.

[12] **M.Lothaire**, *Algebraic combinatorics on word*, May 30 2001.39

[13] **B. Margaret**, *Séries génératrices*, 2013.

[14] **D. Mihoubi**,*Cours Master1, La combinatoire 1,* Université de M'sila, 2017-2018.

[15] **C. Moulin**, *Théorie des langages*, Université de Technologie de Compiègne ,2013.

[16] **G. Richomme**, *Quelques éléments de Combinatoire des Mots*, 2014-2015.

[17] **M. Rigo**, *Théorie des automates et langages formels*, 2009–2010.

[18] **D. Santos**, *Discrete Mathematics Notes*, July 3, 2006.

[19] **S.Sarfat,** *Chapitre 12 , denombrement* , Master Class,

[20] **J. Vélu**., *Méthode mathématique pour l'informatique*, Paris, 2013.

[21] **F. Yvon, A. Demaille et P. Senellar**t, *Théorie des langages*, 2016.

Abstract :

This memory of master degree mathematics discrete lies within the scope of the theory of combinatorics on the free monoïd .In this work, we first give general notions about the principales of combinatorics , then we study the free monoïd.
On otherhand, we have studied the the words and the languages and some properties
In the end , we intersted in the cominatorics on the free monoïd.

Key words :
Principales of combinatorics, free monoïd, words, languages, morphism of monoids, generating functions.

Résumé :

Ce mémoire de master mathématiques discrètes s'inscrit dans le cadre de la théorie des combinatoires sur le monoïde libre. Dans ce travail, on donne tout d'abord des notions générales sur les principes de la combinatoire, par suite, on fait une étude sur le monoïde libre.
D'autre part, nous avons étudié les mots et les langages dans un monoïde libre et quelques propriétés
Enfin, on s'intéresse a la combinatoire sur le monoïde libre.

Mots clés :
Principes de combinatoire, monoïde libre, mots, langages, morphisme de monoïde, séries génératrices.

ملخص :

هذه مذكرة ماستر رياضيات متقطعة ، هي جزء من نظرية التوافقية على نصف الزمرة الحرة . في هذا العمل ، نقدم أولا مفاهيم عامة حول مبادئ التوافقية ، كما قمنا بدراسة حول نصف الزمرة الحرة، ومن ناحية أخرى درسنا الكلمات و اللغات على نصف الزمرة الحرة وبعض الخصائص.
في الأخير، إهتممنا بالتوافقية على نصف الزمرة الحرة.

الكلمات المفتاحية :
مبادئ التوافقية ، نصف الزمرة الحرة ، تماثل الزمرة الحرة ، كلمات ، لغات ، سلسلة مولدات.