FAMILLES INFINIES DE BOUCLES INCASSABLES

par

Louis Marchand

Mémoire présenté au Département d'informatique
en vue de l'obtention du grade de maître ès sciences (M.Sc.)

FACULTÉ DES SCIENCES

UNIVERSITÉ DE SHERBROOKE

Sherbrooke, Québec, Canada, 24 février 2010

Your file Votre référence
ISBN: 978-0-494-61493-8
Our file Notre référence
ISBN: 978-0-494-61493-8

Le 26 février 2010

le jury a accepté le mémoire de Monsieur Louis Marchand dans sa version finale.

Membres du jury

Professeur Martin Beaudry
Directeur de recherche
Département d'informatique

Professeur Shiping Liu
Membre
Département d'informatique

Professeur Richard St-Denis
Président rapporteur
Département d'informatique

Sommaire

Une boucle incassable est une boucle ne contenant aucune sous-boucle propre. Ce mémoire propose la construction de quatre familles de boucles incassables caractérisées par leur commutativité et par leur groupe de multiplication. La première famille est tout simplement une famille de boucles incassables de tout ordre. La seconde famille est une famille de boucles incassables commutatives d'ordre premier dont le groupe de multiplication est le groupe symétrique. La troisième famille élargit la seconde à tous les ordres impairs. La dernière famille est une famille de boucles incassables commutatives d'ordre impair dont le groupe de multiplication est le groupe alterné.

Remerciements

J'aimerais remercier mes parents de m'avoir soutenu et encouragé dans tous mes projets. Puisqu'ils ont toujours cru en moi et ont fait de moi la personne que je suis aujourd'hui, ce mémoire est autant le leur que le mien.

Je tiens également à remercier ma conjointe Myriam qui m'a fait l'honneur de partager ma vie depuis plus de 6 ans. Je lui dois une grande partie de la motivation et de l'inspiration qui m'ont permis de réaliser ce travail et de me rendre là où je suis.

Je remercie mon frère et ma soeur qui partagent mes passions et qui me permettent de discuter sans arrêt de tout et de rien. Ils me connaissent comme personne d'autre et lorsque je vois qu'ils ont confiance en moi, je ne peux qu'avoir confiance également.

J'exprime ma gratitude à mes amis qui m'ont toujours permis d'avoir du plaisir et de me sentir important. En particulier Alexei et Philippe, à qui je dois la majorité des moments de relaxation (voire procrastination) que j'ai eus durant la création et la rédaction de ce travail.

Finalement, j'aimerais remercier mon directeur Martin Beaudry pour m'avoir permis de me dépasser. Il m'a accueilli à bras ouverts et m'a donné les ressources nécessaires à mon essor. Il a toujours cru à mes capacités, dans les bons moments comme dans les moins bons.

Table des matières

Table des figures

Liste des tableaux

Liste des algorithmes

Introduction

Les quasigroupes et les boucles ont attiré l'attention de plusieurs chercheurs, notamment dans le domaine de la théorie des langages formels. La notion de boucles incassables (boucles ne contenant aucune sous-boucle propre) a émergé de ces recherches. Le but de ce mémoire est de montrer l'existence de boucles incassables de tout ordre ainsi que de présenter des familles infinies de boucles incassables.

Le premier chapitre de cet ouvrage permettra au lecteur de réviser les connaissances de base nécessaires à la bonne compréhension des chapitres qui suivront. Les notions qui seront vues dans ce chapitre portent sur l'algèbre en général, sur les groupes de permutations ainsi que sur la théorie des langages formels.

Dans le second chapitre, nous présenterons les motivations qui nous ont poussé à étudier les boucles incassables. Nous présenterons également notre première famille de boucles. Cette famille a été construite par Martin Beaudry et François Lemieux pour un article qui n'est pas encore publié. L'utilité de cette famille est de montrer que, peu importe l'ordre supérieur ou égal à 5, il existe une boucle incassable de cet ordre. Enfin, nous donnerons certains résultats expérimentaux préliminaires qui ont orienté notre recherche.

Dans le troisième chapitre, nous présenterons une famille infinie de boucles incassables commutatives d'ordre premier supérieur ou égal à 13 dont le groupe de multiplication est le groupe symétrique. De plus, nous présenterons les données expérimentales qui nous ont permis de construire cette famille.

Dans le quatrième chapitre, nous commencerons par montrer de nouvelles données

expérimentales basées sur celles du troisième chapitre qui nous permettront de construire les deux prochaines familles de boucles incassables. Ensuite, nous décrirons une famille infinie de boucles incassables commutatives d'ordre impair supérieur ou égal à 21 dont le groupe de multiplication est le groupe symétrique.

Dans le cinquième chapitre, nous présenterons une famille infinie de boucles incassables commutatives d'ordre impair supérieur ou égal à 43 dont le groupe de multiplication est le groupe alterné. Ensuite, nous donnerons des exemples de boucles incassables commutatives d'ordre impair compris entre 25 et 41 dont le groupe de multiplication est le groupe alterné.

Plusieurs travaux ont déjà été réalisés sur des sujets connexes. Voici quelques uns de ces travaux. Jean-Pierre Guy s'est penché sur les groupes isomorphes aux groupes de multiplication des quasigroupes [11]. Également, Jörg Schwenk a effectué une classification de quasigroupes commutatifs [21]. Ensuite, Wanless a présenté une méthode pour construire un carré latin ne contenant aucun carré latin autre que lui-même [24]. Il a utilisé cette méthode pour montrer l'existence de ce type de carrés latins pour plusieurs ordres. Cette méthode a ensuite été étendue à tous les ordres impairs par Wanless, Maenhaut et Webb [13]. Le contenu du présent travail se distingue des recherches déjà effectuées par le fait que nous imposons à nos quasigroupes d'avoir un élément identité (boucles) et un groupe de multiplication bien précis.

En plus de fournir des familles infinies de boucles incassables pouvant servir à démontrer de nouvelles théories ou bien à construire des exemples, notre mémoire présente une grande quantité d'outils (expérimentation, algorithme, etc.) qui, nous l'espérons, seront utiles pour construire de nouvelles familles infinies de boucles.

Chapitre 1

Notions de base et définitions

Dans ce premier chapitre, nous passerons en revue les éléments théoriques de base qui seront utilisés tout au long de l'ouvrage. Nous débuterons par un survol de la théorie des quasigroupes et des boucles. Ensuite, nous verrons quelques bases de la théorie des permutations et des groupes de permutations. Enfin, nous verrons certains éléments de la théorie des langages formels qui sont pertinents à notre travail.

1.1 Notions d'algèbre

Les quasigroupes et les boucles sont des structures algébriques dont la loi de composition interne n'est pas nécessairement associative. Pour présenter plus précisément ce qu'est un quasigroupe et une boucle nous aurons besoin de certaines notions de base de la théorie des ensembles. Pour plus d'information sur les quasigroupes et les boucles, voir [15]. Sauf lorsque le contraire sera spécifié, les ensembles utilisés dans ce travail seront toujours des ensembles finis.

Les notations de la théorie des ensembles utilisées dans ce documents sont classiques. Pour les ensembles A, B et C, on note $f : A \to B$ une application (ou fonction) de A dans B, où A est le domaine de f et B est son codomaine. Pour $a \in A$ et $b \in B$, on note $f(a) = b$ le fait que l'application de la fonction f sur l'élément a résulte en l'élément b. Prenons $g : B \to C$, on note la composition de fonctions $(g \circ f)(a) = g(f(a))$. Le produit

cartésien est noté $A \times B$ et les éléments d'un produit cartésien sont notés $(a, b) \in A \times B$. Le produit $A \times A$ peut être notée A^2. La cardinalité de A est notée $|A|$. Nous utiliserons les opérations booléennes suivantes :

1. L'union de A et de B : $A \cup B = \{x | x \in A \text{ ou } x \in B\}$
2. L'intersection de A et de B : $A \cap B = \{x | x \in A \text{ et } x \in B\}$
3. La soustraction de A par B : $A \backslash B = \{x | x \in A \text{ et } x \notin B\}$

Définition 1.1.1 Soit $f : A \rightarrow B$ une application, on dit que f est *surjective* si tout élément du codomaine est l'image d'au moins un élément du domaine. Formellement, $\forall b \in B, \exists a \in A, f(a) = b$. On appelle *surjection* une application surjective.

Définition 1.1.2 Soit $f : A \rightarrow B$ une application, on dit que f est *injective* si tout élément du codomaine est l'image d'au plus un élément du domaine. Formellement, $\forall (a, b) \in A^2, f(a) = f(b) \Rightarrow a = b$. On appelle *injection* une application injective.

Définition 1.1.3 Soit $f : A \rightarrow B$ une application, on dit que f est *bijective* si f est injective et surjective. On appelle *bijection* une application bijective.

Proposition 1.1.1 Soit $f : A \rightarrow B$ une application. Si les ensembles A et B sont finis et de même cardinalité, alors les affirmations suivantes sont équivalentes :

1. f est injective,
2. f est surjective,
3. f est bijective.

Preuve : Voir [19]. ■

Définition 1.1.4 On appelle *loi de composition interne* sur un ensemble A une application $\star$ de $A \times A$ dans A. Pour tout $(a, b) \in A^2$ et $c \in A$, on notera $a \star b = c$ ou $ab = c$ au lieu de $\star(a, b) = c$.

Définition 1.1.5 On appelle *groupoïde* un ensemble non vide A muni d'une loi de composition interne $\star$. Nous noterons ce groupoïde $(A, \star)$. Lorsque cela n'induit aucune ambiguïté, nous utilisons A pour représenter le groupoïde $(A, \cdot)$.

	0	1	2
0	0	1	2
1	1	2	0
2	1	1	0

figure 1.1 – Exemple : Table de Cayley

Définition 1.1.6 On appelle *table de Cayley* la table de l'opération d'un groupoïde.

Définition 1.1.7 Chacune des lignes (resp. des colonnes) d'une table de Cayley d'un groupoïde A représente une application de A vers A. Cette application est appelée *translation à gauche* (resp. *à droite*) et on la note L_a (resp. R_a) pour tout $a \in A$. Plus formellement, on a $L_a(x) = a \cdot x$ (resp. $R_a(x) = x \cdot a$) pour tout $x \in A$.

Définition 1.1.8 Un groupoïde A est dit *commutatif* si $x \cdot y = y \cdot x$ pour tout $x, y \in A$.

Proposition 1.1.2 Soit A un groupoïde. A est commutatif si et seulement si $L_a = R_a$ pour tout $a \in A$.

Preuve : Voir [15] ■

Définition 1.1.9 Un groupoïde A est dit *associatif* si $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, pour tout $x, y, z \in A$.

Proposition 1.1.3 Soit A un groupoïde, les affirmations suivantes sont équivalentes :

1. A est associatif,
2. $R_{(a \cdot b)} = R_b \circ R_a$ pour tout $a, b \in A$,
3. $L_{(a \cdot b)} = L_a \circ L_b$ pour tout $a, b \in A$.

Preuve : Voir [15] ■

Définition 1.1.10 On appelle *semigroupe* un groupoïde associatif.

Définition 1.1.11 Un *quasigroupe* A est un groupoïde où, pour tout $a \in A$, L_a et R_a sont des bijections.

Remarque : Par la proposition 1.1.1, si le groupoïde A est fini, alors l'injectivité ou la surjectivité de L_a et R_a sont suffisantes pour qu'on ait un quasigroupe.

Définition 1.1.12 Un *carré latin* d'ordre n ($n \geq 1$) est un carré de n lignes par n colonnes contenant n éléments distincts et où chaque élément apparaît une et une seule fois dans chaque ligne et dans chaque colonne.

$$\begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

figure 1.2 – Exemple : Carré latin d'ordre 3

Définition 1.1.13 Un *rectangle latin* d'ordre n de taille r par s est un rectangle de r lignes par s colonnes pour $r \leq n$ et $s \leq n$ tel que chacun des n éléments apparaît au plus une fois dans chacune des lignes et chacune des colonnes. On peut considérer un rectangle latin comme un sous-rectangle d'un carré latin.

$$\begin{array}{cccc} 0 & 1 & 2 & 4 \\ 2 & 4 & 1 & 3 \\ 4 & 3 & 0 & 1 \end{array}$$

figure 1.3 – Exemple : Rectangle latin d'ordre 5 de taille 3 par 4

Proposition 1.1.4 Soit A, un groupoïde fini. Alors les affirmations suivantes sont équivalentes :

1. A est un quasigroupe,
2. Pour $a, x, y \in A$, on a $a \cdot x = a \cdot y \Rightarrow x = y$ (loi d'annulation à gauche) et $x \cdot a = y \cdot a \Rightarrow x = y$ (loi d'annulation à droite),
3. La table de Cayley de A est un carré latin.

Preuve :
1→2 : Puisque L_a est injective, pour tout $a \in A, L_a(x) = L_a(y) \Rightarrow x = y$. De manière similaire, puisque R_a est injective, pour tout $a \in A, R_a(x) = R_a(y) \Rightarrow x = y$.
2→3 : Par la loi d'annulation à gauche, $\forall a, x, y \in A, L_a(x) = L_a(y) \Rightarrow x = y$. Également, par la loi d'annulation à droite, $\forall a, x, y \in A, R_a(x) = R_a(y) \Rightarrow x = y$. Puisque les L_a correspondent aux lignes de la table de Cayley et les R_a correspondent aux colonnes, toutes les lignes et toutes les colonnes ne contiendront qu'une et une seule fois chaque élément de A. Donc, la table de Cayley de A est un carré latin.
3→1 : Posons que M, la table de Cayley de A, est un carré latin. Chacune des lignes et colonnes de M contient au moins une fois chacun des éléments de A. Puisque les lignes de M correspondent aux L_a, on voit que $\forall a, c \in A, \exists b \in A$ tel que $L_a(b) = c$. De manière similaire, puisque les colonnes de M correspondent aux R_a, on voit que $\forall a, c \in A, \exists b \in A$ tel que $R_a(b) = c$. Donc, L_a et R_a sont surjectives. ■

Corollaire 1.1.5 Soit A, un quasigroupe. Alors pour $(a, b) \in A \times A$, il existe un unique $(x, y) \in A \times A$ tel que $a \cdot x = y \cdot a = b$.

Définition 1.1.14 Soit A, un groupoïde. On appel *élément identité à gauche* (resp. *à droite*) de A un élément $e \in A$ tel que $L_e(a) = a$ (resp. $R_e(a) = a$) pour tout $a \in A$. Si un élément $e \in A$ est à la fois un élément identité à gauche et à droite de A, on le nomme *élément identité* de A.

Proposition 1.1.6 Quand il existe, l'élément identité d'un groupoïde est toujours unique.

Preuve : Voir [15] ■

Définition 1.1.15 Un *monoïde* est un semigroupe avec un élément identité.

Définition 1.1.16 Une *boucle* est un quasigroupe avec un élément identité.

·	0	1	2	3	4
0	0	1	2	3	4
1	1	2	0	4	3
2	2	3	4	0	1
3	3	4	1	2	0
4	4	0	3	1	2

(a) Ordre 5

·	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	4	5	3
2	2	0	3	5	1	4
3	3	4	5	1	0	2
4	4	5	1	2	3	0
5	5	3	4	0	2	1

(b) Ordre 6

figure 1.4 – Exemple : Boucles d'ordre 5 et 6

À partir de maintenant, même s'il n'est pas directement spécifié, l'élément 0 d'une boucle sera toujours l'élément identité.

Définition 1.1.17 On appelle *groupe* un monoïde $(A, \cdot)$ dans lequel pour chaque élément $a \in A$, il existe un inverse $a^{-1} \in A$ tel que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Proposition 1.1.7 Soit A un quasigroupe fini. Si A est associatif, alors il possède un élément identité.

Preuve : Puisque A est non vide, il possède un élément $a \in A$. Puisque L_a est une bijection, il existe un unique $e \in A$ tel que $L_a(e) = a$. Maintenant, prenons $b \in A$ un élément de A. Puisque R_a est une bijection, il existe un unique $y \in A$ tel que $R_a(y) = b$. Donc, on a $R_e(b) = b \cdot e = (y \cdot a) \cdot e = y \cdot (a \cdot e) = y \cdot a = R_a(y) = b$ (par associativité). Donc, $R_e(b) = b$ pour tout $b \in A$ implique que e est un élément identité à droite dans A.

Maintenant, prenons $b \in A$, un élément de A. Nous avons donc $b \cdot b = (b \cdot e) \cdot b = b \cdot (e \cdot b)$ (par associativité). Par la loi d'annulation à gauche (proposition 1.1.4), on a que $b \cdot b = b \cdot (e \cdot b)$ implique $b = e \cdot b$. Donc, $L_e(b) = b$ pour tout $b \in A$ implique que e est un élément identité à gauche dans A. Puique e est un élément identité à gauche et à droite de A, e est l'élément identité de A. ■

Corollaire 1.1.8 Soit A un quasigroupe fini. Si A est associatif, alors A est une boucle.

Proposition 1.1.9 Soit A un quasigroupe fini. Si A est associatif, alors A est un groupe.

Preuve : On sait que A est associatif et que par la proposition 1.1.7, A possède un identité e unique. On doit montrer que pour tout $a \in A$, il existe un inverse $a^{-1} \in A$ tel que $a \cdot a^{-1} = a^{-1} \cdot a = e$. Puisque A est un quasigroupe, alors par le corollaire 1.1.5, il existe un élément $(b, c) \in A^2$ tel que $a \cdot b = c \cdot a = e$. Donc : $a \cdot b = c \cdot a \Rightarrow c \cdot (a \cdot b) = c \cdot (c \cdot a) \Rightarrow (c \cdot a) \cdot b = c \cdot (c \cdot a) \Rightarrow e \cdot b = c \cdot e \Rightarrow b = c$. Donc, $b = c = a^{-1}$ est l'inverse de a. ■

Proposition 1.1.10 Tout groupe est une boucle.

Preuve : Soit A un groupe. On sait que A possède un élément identité. On doit montrer que A est un quasigroupe. Soit $x \in A$ et $(a, b, c, d) \in A^4$ tels que $L_x(a) = L_x(b)$ et $R_x(c) = R_x(d)$. On a $x \cdot a = x \cdot b \Rightarrow x^{-1} \cdot (x \cdot a) = x^{-1} \cdot (x \cdot b) \Rightarrow (x^{-1} \cdot x) \cdot a = (x^{-1} \cdot x) \cdot b \Rightarrow a = b$. Similairement, $c \cdot x = d \cdot x \Rightarrow c \cdot x \cdot x^{-1} = d \cdot x \cdot x^{-1} \Rightarrow c = d$. Donc, L_x et R_x sont injectives pour tout $x \in A$. ■

La figure 1.5 permet de bien voir les relations entre les structures algébriques définies jusqu'ici.

Définition 1.1.18 Soit $(A, \cdot)$ un quasigroupe (resp. boucle, groupe) et B un sous-ensemble de A. On dit que $(B, \cdot)$ est un *sous-quasigroupe* (resp. *sous-boucle*, *sous-groupe*) de $(A, \cdot)$ si $(B, \cdot)$ est un quasigroupe (resp. boucle, groupe).

Proposition 1.1.11 (Théorème de Lagrange) Si H est un sous-groupe du groupe G, alors $|H|$ divise $|G|$.

Preuve : Voir theorème 4.11 de [1]. ■

Définition 1.1.19 Soit A une boucle (resp. groupe) et 0, l'élément identité de A. On voit que $\{0\}$ et A sont toujours des sous-boucles (resp. sous-groupes) de A. On appelle ces sous-boucles (resp. sous-groupes) les sous-boucles (resp. sous-groupes) *impropres* de A. Une sous-boucle (resp. sous-groupe) qui n'est pas impropre est dite *propre*.

Définition 1.1.20 Soit A une boucle. On dit que A est *incassable* si elle ne contient aucune sous-boucle propre.

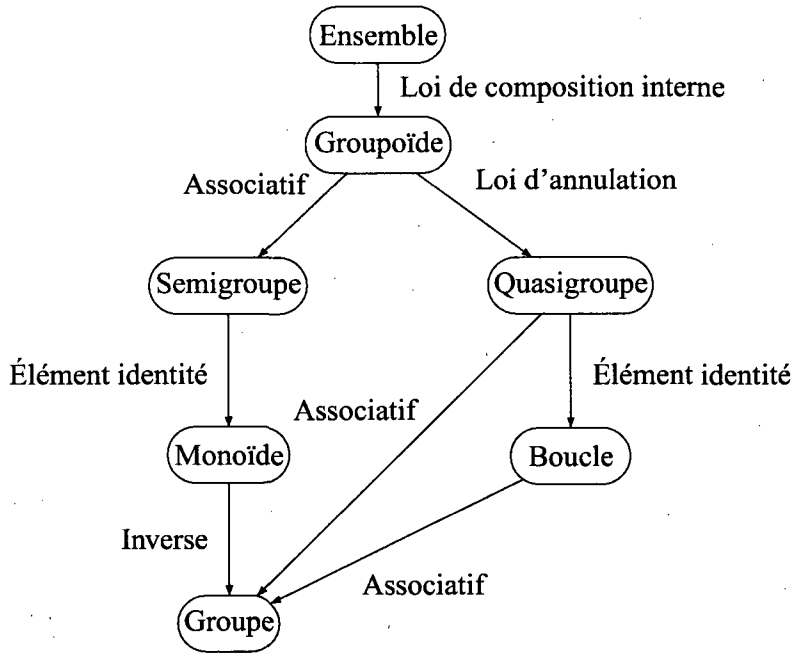

figure 1.5 – Hiérarchie des structures algébriques finies

Définition 1.1.21 Soit $(A, \bullet)$ et $(B, \circ)$, deux quasigroupes (resp. boucles, groupes). On appel *morphisme* ou *homomorphisme* de $(A, \bullet)$ dans $(B, \circ)$ une application f de A dans B telle que $f(x \bullet y) = f(x) \circ f(y)$ pour tout $x, y \in A$.

Définition 1.1.22 Soit $(A, \bullet)$ et $(B, \circ)$, deux quasigroupes (resp. boucles, groupes). On appelle *isomorphisme* de $(A, \bullet)$ dans $(B, \circ)$ un morphisme bijectif de $(A, \bullet)$ dans $(B, \circ)$. Intuitivement, un isomorphisme de $(A, \bullet)$ dans $(B, \circ)$ correspond au renommage de chacun des éléments de A par les éléments de B. On appelle *classe d'isomorphisme* d'un quasigroupe (resp. boucle, groupe) $(A, \bullet)$ l'ensemble des quasigroupes (resp. boucles, groupes) isomorphes à $(A, \bullet)$. Lorsque $(A, \bullet)$ et $(B, \circ)$ sont isomorphes, on note $(A, \bullet) \cong (B, \circ)$ ou $A \cong B$.

Exemple : Soit l'ensemble $A = 0, 1, 2, 3$, les deux boucles $(A, \bullet)$ et $(A, \circ)$ suivantes sont

isomorphes (l'élément 1 a été renommé 2 et 2 renommé 1) :

$\bullet$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cong$

$\circ$	0	2	1	3
0	0	2	1	3
2	2	1	3	0
1	1	3	0	2
3	3	0	2	1

$=$

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	1	0
3	3	2	0	1

figure 1.6 – Exemple : Boucles isomorphes

Définition 1.1.23 Soit $(A, \cdot)$ un quasigroupe (resp. boucle, groupe) et soit $\emptyset \neq S \subseteq A$. Prenons T l'ensemble de tous les sous-quasigroupes (resp. sous-boucles, sous-groupes) contenant les éléments de S. L'intersection des éléments de T est notée $\langle S \rangle$ et est appelée *sous-quasigroupe* (resp. *sous-boucle*, *sous-groupe*) *engendré* par S.

Pour trouver tous les éléments d'un groupe engendré par un ensemble d'éléments, il suffit d'utiliser l'algorithme 1.

Entrée : S : Ensemble générateur.
$\cdot$: Loi de composition interne de $\langle S \rangle$
Sortie : le quasigroupe (resp. boucle, groupe) $\langle S \rangle$ engendré par S

FERMETURE_ENSEMBLE(S,$\cdot$) **début**
  Copier les éléments de S dans un nouvel ensemble $\langle S \rangle$
  $fin := Faux$
  tant que $fin = Faux$ **faire**
    pour tout $(a, b) \in \langle S \rangle \times \langle S \rangle$ **faire**
      $c := a \cdot b$
      si $c \notin \langle S \rangle$ **alors**
        Ajouter c dans $\langle S \rangle$
        $fin := Faux$
      fin si
    fin pour tout
  fin tant que
  retourne $\langle S \rangle$
fin

Algorithme 1 : Effectue la fermeture d'un ensemble

1.2 Groupes de permutations

Maintenant que nous avons les bases nécessaires concernant les quasigroupes et les boucles, nous sommes intéressés à séparer ces boucles incassables en plusieurs classes. Pour ce faire, nous allons utiliser les groupes de permutations isomorphes aux groupes de multiplication de ces boucles.

Une grande partie des notions de cette section sont prises du livre de la série Schaum sur la théorie des groupes [1].

Définition 1.2.1 On appelle *permutation* d'ordre n une bijection de l'ensemble X vers X pour $|X| = n$.

Notation : La notation standard d'une permutation place sur une première ligne les éléments dans leur ordre naturel et sur une deuxième ligne les images correspondantes.

Exemple : Considérons l'ensemble $X = \{1, 2, 3, 4\}$ et l'application σ telle que $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 1$ et $\sigma(4) = 3$. L'application σ est une permutation de X.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

figure 1.7 – Exemple : Permutation, notation standard (ou matricielle)

Définition 1.2.2 La *permutation identité* est la permutation P_I qui ne change pas l'ordre initial des éléments.

$$P_I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

figure 1.8 – Exemple : Permutation identité

Le *produit de deux permutations* P_1P_2 correspond à la composition de fonctions $P_2 \circ P_1$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

figure 1.9 – Exemple : Produit de permutations

Pour trouver *l'inverse d'une permutation*, nous avons qu'à inverser le domaine et l'image comme dans l'exemple de la figure 1.10.

Définition 1.2.3 Soit P, la permutation d'ordre n sur X. Soit $a_1, \cdots, a_k \in X$ des éléments de X tels que $1 \leq k \leq n$ et que $P(a_1) = a_2, P(a_2) = a_3, \cdots, P(a_{k-1}) = a_k$ et que $P(a_k) = a_1$. On appelle *cycle* de P la suite d'éléments $a_1, \cdots, a_k$ et on note ce cycle $(a_1 \ \cdots \ a_k)$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

figure 1.10 – Exemple : Inverse d'une permutation

Par exemple, la permutation $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ peut être décomposée en 2 cycles : $(1\ 3\ 5)$ et $(2\ 4)$.

Notation : Certaines fois, il peut être utile de représenter les permutations en donnant la liste de leurs cycles de longueur supérieure ou égale à 2. On parle de la *notation canonique* d'une permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\,3\,5)(2\,4)$$

figure 1.11 – Exemple : Notation canonique d'une permutation

Définition 1.2.4 On appelle *transposition* une permutation qui déplace seulement deux éléments.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2\,4)$$

figure 1.12 – Exemple : Transposition

Proposition 1.2.1 Toute permutation peut être écrite comme un produit de transpositions.

Preuve : Voir [22] ■

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 3\ 5)(2\ 4) = (1\ 3)(3\ 5)(2\ 4)$$

figure 1.13 – Exemple : Permutation comme produit de transpositions

Définition 1.2.5 On appelle *permutation paire* (resp. *impaire*) une permutation qui peut être écrite comme un produit d'un nombre pair (resp. impair) de transpositions.

Définition 1.2.6 On appelle *signature* d'une permutation P la fonction :

$$sng(P) = \begin{cases} 1 & \text{si } P \text{ est paire} \\ -1 & \text{si } P \text{ est impaire} \end{cases}$$

Pour calculer cette fonction, prenons $X = 0, ..., n-1$ les n éléments ordonnés de P et $\sigma : X \to X$ la fonction de P qui prend i et l'envoie sur $\sigma(i)$. Le calcul de la fonction se fait de la manière suivante :

$$sng(P) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

On dit que deux éléments i et j forment une *inversion* si $i < j$ et que $\sigma(i) > \sigma(j)$. On peut donc voir que la formule ci-dessus calcule le nombre d'inversions dans la permutation. Le nombre d'inversions permet donc de savoir la parité de la permutation. Pour calculer le nombre d'inversions par rapport à un élément x à la position y, on regarde le nombre d'éléments inférieurs à x dans les positions supérieures à y. Le nombre total d'inversions dans une permutation est la somme des nombres d'inversions par rapport à chacun des éléments de la permutation. Une permutation est paire si et seulement si le nombre d'inversions dans la permutation est pair. La figure 1.2 montre un exemple de calcul de parité d'une permutation.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$$

Nombre d'inversions par rapport à	5	:	5 3 2 4 1	$\rightarrow$	4	$5>3, 5>2, 5>4, 5>1$
	3	:	3 2 4 1	$\rightarrow$	2	$3>2, 3>1$
	2	:	2 4 1	$\rightarrow$	1	$2>1$
	4	:	4 1	$\rightarrow$	1	$4>1$
Nombre d'inversions dans α		:			8	

Puisque le nombre d'inversions dans α est pair, alors α est paire.

figure 1.14 – Exemple : Parité d'une permutation par nombre d'inversions

Définition 1.2.7 On appelle *groupe symétrique* de degré n le groupe constitué de toutes les permutations de n symboles. Ce groupe contient $n!$ permutations et on le note $\mathcal{S}(n)$.

Définition 1.2.8 On appelle *groupe alterné* de degré n le groupe contenant toutes les permutations paires de n symboles. Ce groupe contient $\frac{n!}{2}$ permutations, il est un sous-groupe de $\mathcal{S}(n)$ et on le note $\mathcal{A}(n)$.

Définition 1.2.9 Soit A un quasigroupe et $a \in A$ un élément de A. Puisque L_a et R_a sont des bijections de A vers A, L_a et R_a sont des permutations. On appelle *groupe de multiplication* de A, noté $\mathcal{M}(A)$, le groupe de permutations engendré par les permutations L_a et R_a. Formellement, $\mathcal{M}(A) = \langle \{L_a, a \in A\} \cup \{R_a, a \in A\} \rangle$.

Proposition 1.2.2 Si G et H sont deux boucles isomorphes, alors $\mathcal{M}(G) \cong \mathcal{M}(H)$.

Preuve : voir Théorème III.2.7 dans [15] ■

1.3 Les langages

L'étude algébrique des langages permet d'étudier ceux-ci avec une approche différente de l'approche utilisant les grammaires, automates et expressions régulières. Les notions de cette section sont principalement tirées de [12].

1.3. LES LANGAGES

Définition 1.3.1 On appelle *alphabet* A un ensemble non vide de symboles.

Définition 1.3.2 Le *semigroupe libre* A^+ est l'ensemble de tous les *mots* qu'il est possible de former avec l'alphabet A en utilisant la concaténation (pour tout $x, y \in A^+$, $xy \in A^+$).

Définition 1.3.3 On appelle mot vide ϵ l'unique mot tel que $\forall x \in A^+$, $\epsilon x = x\epsilon = x$. Il s'agit de l'élément identité de la concaténation.

Définition 1.3.4 Soit A un alphabet. Si on ajoute le mot vide ϵ au semigroupe libre A^+, on obtient le monoïde libre A^*. Formellement, $A^* = A^+ \cup \{\epsilon\}$.

Définition 1.3.5 On appelle *langage* sur l'alphabet A un sous-ensemble des mots du monoïde libre A^* (semigroupe libre A^+ si le mot vide est exclu).

Le premier pas pour en arriver à une représentation algébrique d'un langage est de trouver une équivalence entre les langages et une structure algébrique. On y arrive en montrant qu'un automate peut représenter un langage régulier et qu'un semigroupe peut représenter un automate.

Définition 1.3.6 Soit A un alphabet et ϵ le mot vide. Les *langages réguliers* sur A sont définis récursivement :

- Base : $\emptyset$, $\{\epsilon\}$ et $\{a\}$ pour $a \in A$, sont des langages réguliers.
- Récursion : Soit X et Y deux langages réguliers sur A, alors les langages suivants sont réguliers sur A :
  - $X \cup Y = \{w \in A^* | w \in X \text{ ou } w \in Y\}$
  - $XY = \{w_1 w_2 \in A^* | w_1 \in X \text{ et } w_2 \in Y\}$
  - $X^* = \bigcup_{i \geq 0} X^i$ où $X^0 = \{\epsilon\}$ et $X^{n+1} = XX^n$.
- Clôture : X est un langage régulier sur A si et seulement si il peut être obtenu à partir de langages de base en effectuant un nombre fini de récursions.

Définition 1.3.7 Un *automate fini* est un quintuplet $M = (Q, A, \delta, q_0, F)$, où Q est un ensemble fini d'états, A est un alphabet, $q_0 \in Q$ est l'état initial de l'automate, $F \subset Q$ est l'ensemble des états accepteurs de l'automate et $\delta : Q \times A^* \rightarrow Q$ est la fonction de transition. On a que $\delta(q, w_1w_2) = \delta(\delta(q, w_1), w_2)$ et $\delta(q, \epsilon) = q$. Un mot $w \in A^*$ est accepté par M si et seulement si $\delta(q_0, w) \in F$. Le langage accepté par M, noté $L(M)$, est l'ensemble des mots de A^* acceptés par M.

Exemple : Soit l'automate fini $M = (Q, A, \delta, q_0, F)$ avec $Q = \{q_0, q_1, q_2\}$, $A = \{a, b\}$, $F = \{q_3\}$ et δ est représentée par la figure 1.15.

δ	a	b
q_0	q_1	q_0
q_1	q_2	q_0
q_2	q_2	q_2

figure 1.15 – Exemple : Table de la fonction de transition δ de l'automate M

Pour ceux qui connaissent la représentation d'un automate sous forme de diagramme de transition (voir [12]), l'automate décrit par la figure 1.15 est représenté par le diagramme de transition de la figure 1.16.

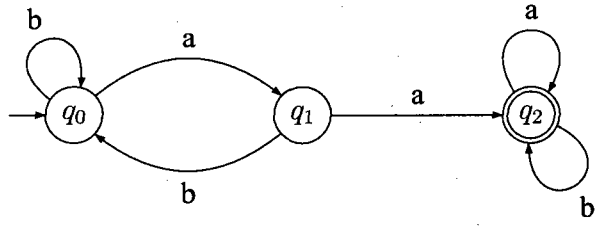

figure 1.16 – Exemple : Diagramme de transition de l'automate M

Le langage accepté par cet automate est celui des mots finis contenant aa. Formellement, $L(M) = \{uaav | u \in A^* \text{ et } v \in A^*\}$. □

Proposition 1.3.1 (Théorème de Kleene) Un langage L est régulier si et seulement s'il existe un automate fini M tel que $L = L(M)$.

Preuve : Voir [12]. ■

Maintenant, remarquons que chaque mot w de A^+ (resp. A^*) définit une application α_w de Q dans Q telle que $\alpha_w : q \mapsto \delta(q, w)$. La composition des applications est associative, ce qui implique que les α_w engendrent un semigroupe appelé semigroupe de transition (ce semigroupe est un monoïde si on tient compte du mot vide). Par contre, ce semigroupe ne prend en compte que la structure de l'automate fini (c'est-à-dire les ensembles Q, A et les transitions δ). La définition suivante montre comment un semigroupe peut reconnaître un langage. Noter que l'état initial est intrinsèque dans le semigroupe S et que le sous-ensemble F correspond aux états finaux.

Définition 1.3.8 Soit A un alphabet, $L \subseteq A^*$ un langage sur l'alphabet A et S un semigroupe. On dit que S reconnaît L s'il existe un morphisme $\phi : A^* \to S$ et un sous-ensemble $F \subseteq S$ tel que $L = \phi^{-1}(F)$.

Exemple : Soit $L = \{uaav | u \in A^* \text{ et } v \in A^*\}$, un langage sur l'alphabet $A = \{a, b\}$. Soit $S = \{a, b, a^2, ab, ba\}$, le semigroupe engendré par toutes les transitions de l'automate (induites par la fonction de transition comme dans l'exemple de la définition 1.3.7). Pour construire ce semigroupe, on utilise le tableau 1.1.

mot	q_0	q_1	q_2	Élément
a	q_1	q_2	q_2	a
b	q_0	q_0	q_2	b
a^2	q_2	q_2	q_2	a^2
bb	q_0	q_0	q_2	b
ab	q_0	q_2	q_2	ab
ba	q_1	q_1	q_2	ba
a^3	q_2	q_2	q_2	a^2
a^2b	q_2	q_2	q_2	a^2
aba	q_1	q_2	q_2	a
abb	q_0	q_2	q_2	ab
baa	q_2	q_2	q_2	a^2
bab	q_0	q_0	q_2	b

tableau 1.1 – Exemple : Inventaire des éléments du semigroupe S

La table de Cayley de S est :

	a	b	a^2	ab	ba
a	a^2	ab	a^2	a^2	a
b	ba	b	a^2	b	ba
a^2	a^2	a^2	a^2	a^2	a^2
ab	a	ab	a^2	ab	a
ba	a^2	b	a^2	a^2	ba

figure 1.17 – Exemple : Table de Cayley du semigroupe S

On reconnaît L avec $\phi(a) = a$, $\phi(b) = b$ et $F = \{a^2\}$. Noter qu'on confond $a \in S$ et $a \in A$. Ainsi, si on prend un mot exemple $abbaabab$ qui fait partie du langage L, on voit que $\phi(abbaabab) = a^2$. Puisque $a^2 \in F$, le mot $abbaabab$ est accepté par le semigroupe. Par contre, si on prend le mot $abbabab$ qui ne fait pas partie du langage, on obtient $\phi(abbabab) = ab$. Puisque $ab \notin F$, le mot $abbabab$ n'est pas accepté par le semigroupe. □

Cette notion de reconnaissance de langages par les semigroupes ainsi que le théorème de Kleene nous permettent d'énoncer un des théorèmes majeurs dans l'étude algébrique des langages.

Proposition 1.3.2 Un langage est régulier si et seulement si il est accepté par un semigroupe fini.

Preuve : Voir section 2.3 de [18]. ■

Ce théorème a permis de faire l'étude des langages réguliers en utilisant la théorie des semigroupes. Il est possible d'avoir l'équivalent au niveau des langages hors contexte. Pour y arriver, nous avons besoin d'une structure algébrique plus puissante que les semigroupes. Les groupoïdes ont donc été étudiés. Cette étude a porté fruit puisqu'il a été montré que les langages reconnus par les groupoïdes sont exactement les langages hors contexte.

Définition 1.3.9 Une *grammaire hors contexte* est un quadruplet $G = (V, A, P, S)$, où V est un ensemble fini de variables, A est un alphabet, P est un sous-ensemble de $V \times (V \cup A)^*$ représentant les règles et $S \in V$ est le symbole de départ (V et A doivent être disjoints). Un règle de P est écrite $X \to w$, où $X \in V$ et $w \in (V \cup A)^*$.

Définition 1.3.10 Soit $G = (V, A, P, S)$ une grammaire hors contexte et $v \in (V \cup A)^*$. L'ensemble des *mots dérivables* à partir de v est défini récursivement :

- Base : v est dérivable à partir de v.
- Récursion : Si $u = yXz$ est dérivable à partir de v et $(X \to w) \in P$, alors ywz est dérivable à partir de v.
- Clôture : un mot est dérivable à partir de v si et seulement si il peut être dérivé à partir de v par un nombre fini d'étapes de récursion.

Lorsqu'un mot u est dérivable à partir de v, on note $v \overset{*}{\Rightarrow} u$ ($v \Rightarrow u$ si la dérivation n'utilise qu'une étape de récursion).

Définition 1.3.11 Soit $G = (V, A, P, S)$ une grammaire hors contexte. Le langage engendré par G (noté $L(G)$) est l'ensemble $\{w \in A^* | S \overset{*}{\Rightarrow} w\}$. Un *langage hors contexte* est un langage engendré par une grammaire hors contexte.

Exemple : Soit $G = (V, A, P, S)$ une grammaire hors contexte avec $V = \{S, X, Y\}$, $A = \{a, b\}$ et P, l'ensemble des règles suivantes :

$$\begin{aligned} S &\rightarrow XSY \\ S &\rightarrow \epsilon \\ X &\rightarrow a \\ Y &\rightarrow b \end{aligned}$$

figure 1.18 – Exemple : Règles de la grammaire G

Le langage engendré par cette grammaire est $L(G) = \{vw | v = a^n, w = b^n \text{ et } n \geq 0\}$. Par exemple, si on prend le mot $aabb$, on peut faire la dérivation suivante :

$$S \Rightarrow XSY \Rightarrow aSY \Rightarrow aXSYY \Rightarrow aaSYY \Rightarrow aaYY \Rightarrow aabY \Rightarrow aabb$$

Ainsi, on a $S \overset{*}{\Rightarrow} aabb$, ce qui implique que $aabb \in L(G)$. □

Définition 1.3.12 Une grammaire hors contexte $G = (V, A, P, S)$ est sous la forme normale de Chomsky si chaque règle de P est sous une des formes suivantes :

1. $X \rightarrow YZ$
2. $X \rightarrow a$

où $X, Y, Z \in V$ et $a \in A$.

Proposition 1.3.3 Tout langage hors contexte ne contenant pas le mot vide peut être généré par une grammaire hors contexte sous la forme normale de Chomsky.

Preuve : Voir Théorème 4.5 dans [12]. ■

La forme normale de Chomsky permet une gestion binaire (deux à deux) des variables de la grammaire. De cette manière, on peut représenter une dérivation sous forme d'arbre binaire ou même sous forme de parenthésage du mot engendré. Avec cet outil, nous pouvons définir la reconnaissance d'un langage par un groupoïde. En effet, puisqu'un groupoïde n'est pas associatif, le parenthésage des éléments dans une expression doit être géré. Voici comment on définit la reconnaissance d'un langage par un groupoïde.

Définition 1.3.13 Soit $L \subseteq A^*$ un langage, G un groupoïde et $\phi : A^* \to G^*$ le morphisme induit par la fonction $\phi : A \to G$. Pour tout $w \in A^*$, notons $\eta_G(w)$ l'ensemble des éléments $g \in G$ tel que w peut être évalué à g en utilisant le morphisme ϕ et un certain parenthésage. On dit que G reconnaît L s'il existe un sous-ensemble $F \subseteq G$ tel que pour tout $w \in A^*$ nous avons $w \in L$ si et seulement si $\eta_G(w) \cap F \neq \emptyset$.

Exemple : Nous allons voir un exemple de groupoïde acceptant le langage hors contexte L vu lors de l'exemple de la définition 1.3.11. Pour cela, nous allons transformer un peu notre grammaire pour qu'elle soit sous la forme normale de Chomsky. Prenons la grammaire $Q' = (V', A, P', B)$ avec $V' = \{B, C, X, Y\}$, $A = \{a, b\}$ et P' contient les règles suivantes :

$$\begin{aligned} B &\to XC \\ B &\to XY \\ C &\to BY \\ X &\to a \\ Y &\to b \end{aligned}$$

Nous voyons que cette grammaire est sous la forme normale de Chomsky et que $L(Q') = L\backslash\{\epsilon\}$ (sans le mot vide). Pour gérer le mot vide, nous allons prendre une nouvelle grammaire $Q = (V, A, P, S)$ avec $V = V' \cup \{S\}$ et les règles de P sont :

$$\begin{aligned} S &\to B \\ S &\to \epsilon \\ B &\to XC \\ B &\to XY \\ C &\to BY \\ X &\to a \\ Y &\to b \end{aligned}$$

On voit maintenant que $L(Q) = L$ (incluant le mot vide), mais cette grammaire n'est plus sous la forme normale de Chomsky. Nous allons donc créer un groupoïde qui utilisera la structure de Q' pour calculer, mais contiendra un élément identité 1 qui permettra de gérer le mot vide. Prenons donc le groupoïde $G = \{0, 1, \hat{B}, \hat{C}, \hat{X}, \hat{Y}\}$. Les éléments de G avec un chapeau sont en lien avec les éléments de V. L'élément 0 sert à remplir la table de Cayley

du groupoïde. Si cet élément est utilisé lors du calcul d'un mot, le résultat de ce calcul ne sera jamais accepté (0 ne fait jamais partie de F). La table de Cayley de notre groupoïde est la suivante :

	0	1	$\hat{B}$	$\hat{C}$	$\hat{X}$	$\hat{Y}$
0	0	0	0	0	0	0
1	0	1	$\hat{B}$	$\hat{C}$	$\hat{X}$	$\hat{Y}$
$\hat{B}$	0	$\hat{B}$	0	0	0	$\hat{C}$
$\hat{C}$	0	$\hat{C}$	0	0	0	0
$\hat{X}$	0	$\hat{X}$	0	$\hat{B}$	0	$\hat{B}$
$\hat{Y}$	0	$\hat{Y}$	0	0	0	0

Posons le morphisme $\phi : A^* \rightarrow G^*$ tel que $\phi(a) = \hat{X}$, $\phi(b) = \hat{Y}$, $\phi(\epsilon) = 1$ et l'ensemble $F = \{1, \hat{B}\}$ correspondant aux éléments acceptés (F contient la correspondance des variables pointées par S). Prenons le mot $aabb$; on a $\phi(aabb) = \hat{X}\hat{X}\hat{Y}\hat{Y}$. Donc la fonction η_G qui retourne l'ensemble des parenthésages donnera :
$\eta_G(aabb) = \{(((\hat{X}\hat{X})\hat{Y})\hat{Y}), ((\hat{X}(\hat{X}\hat{Y}))\hat{Y}), ((\hat{X}\hat{X})(\hat{Y}\hat{Y})), ...\}$.
Si on prend le parenthésage $(\hat{X}((\hat{X}\hat{Y})\hat{Y}) \in \eta_G(aabb)$, le calcul du résultat donne :
$(\hat{X}((\hat{X}\hat{Y})\hat{Y}) = (\hat{X}(\hat{B}\hat{Y})) = (\hat{X}\hat{C}) = \hat{B}$.
Puisque $\hat{B} \in F$, on a $\eta_G(aabb) \cap F \neq \emptyset$, d'où on en déduit que $aabb \in L$ □

La démarche utilisée dans le précédent exemple est à la base de la démonstration de la proposition suivante.

Proposition 1.3.4 Un langage est hors contexte si et seulement si il est reconnu par un groupoïde fini.

Preuve : Voir [6]. ■

Chapitre 2

Préliminaires

Dans ce chapitre, nous présenterons les motivations principales qui nous ont poussé à étudier les boucles incassables. Ensuite, nous présenterons une preuve que, peu importe l'ordre (fini) supérieur à 5, il existe une boucle incassable de cet ordre. Cette preuve nous permettra de savoir que nous pouvons continuer d'étudier les boucles incassables sans risquer d'avoir un ordre où il n'existe aucune boucle incassable à étudier. Enfin, à la fin du chapitre, nous donnerons les résultats expérimentaux préliminaires qui ont orienté notre recherche.

2.1 Motivation

Comme nous l'avons vu dans la dernière section, nous pouvons maintenant utiliser la théorie des groupoïdes pour étudier les langages hors contexte. Par contre, le fait que le groupoïde soit une structure algébrique très générale rend son étude très difficile. On se restreint alors à étudier les groupoïdes ayant certaines propriétés algébriques en commun. L'utilisation du monoïde de multiplication (similaire au groupe de multiplication des quasigroupes) comme outil de caractérisation donne des résultats intéressants. Voir [2, 3, 4, 5] pour des exemples.

L'intérêt des quasigroupes, du point de vue des langages, est le fait que le monoïde

de multiplication d'un quasigroupe est toujours un groupe. Ce qui est également intéressant à propos des quasigroupes et des boucles, c'est que ce sont des structures qui ont déjà été significativement étudiées par les algébristes. On a donc pu en faire l'étude en utilisant les bases déjà existantes. Le premier résultat qui est ressorti de cette étude est que tous les langages reconnus par un quasigroupe sont réguliers [8]. Dans ce sens, on sait que les quasigroupes ne sont pas plus puissants que les semigroupes en terme de reconnaissance de langages. D'un autre côté, les quasigroupes ont en commun avec les groupoïdes qu'ils ne sont pas associatifs. Donc, l'étude des quasigroupes peut fournir une certaine compréhension de la reconnaissance d'un langage par une structure algébrique non associative. Cette compréhension de la non-associativité sera utile pour l'étude future des groupoïdes.

Ensuite, le résultat principal est sorti à propos des langages reconnus par les boucles. On a démontré dans [4] qu'un langage est reconnu par une boucle finie si et seulement si ce langage est un polynôme de langages à groupe. Un polynôme de langages à groupe est une union finie de langages de la forme $L_0 a_1 L_1 \cdots L_{k-1} a_k L_k$, où $k \geq 0$, a_i est une lettre et L_i est un langage à groupe (langage reconnu par un groupe). On appelle aussi langage régulier ouvert un polynôme de langages à groupe.

Une autre classe de langages a été étudiée à partir d'un cas particulier de boucles. En effet, l'étude des boucles qui ne possèdent aucun sous-groupe propre a permis de constater qu'un langage L est reconnu par ce type de boucle si et seulement si L est un langage régulier ouvert et sans étoile (voir [5] et [3]).

La classe des langages sans étoile sur l'alphabet A (notée $SE(A)$) est le plus petit ensemble de langages vérifiant les conditions :

1. $\emptyset, A^*, \{a\} \in SE(A)$ pour tout $a \in A$
2. $SE(A)$ est stable pour l'union : $X \cup Y = \{w \in A^* | w \in X \text{ ou } w \in Y\}$
3. $SE(A)$ est stable pour la soustraction : $X \backslash Y = \{w \in A^* | w \in X \text{ et } w \notin Y\}$
4. $SE(A)$ est stable pour la concaténation : $XY = \{w \in A^* | \exists u \in X \text{ et } v \in Y \text{ tel que } w = uv\}$.

Un léger problème entre en ligne de compte. Construire des exemples de boucles ne contenant pas de sous-groupes propres est très difficile. Nous savons par contre qu'un groupe est un cas particulier de boucles respectant l'associativité (voir proposition 1.1.10). Donc, en construisant des boucles incassables, on obtient des exemples de boucles ne contenant aucun sous-groupe propre.

Donc, le but de cette étude est de construire des exemples de boucles incassables dont le groupe de multiplication est connu. La première étape consiste à montrer qu'au moins une boucle incassable existe pour tout ordre. Ensuite, on doit examiner quels sont les groupes de multiplication des boucles incassables de petite taille. Enfin, trouver des familles infinies de boucles incassables ayant ces groupes de multiplication.

2.2 Boucles incassables d'ordre $n \geq 5$

Dans cette section, nous montrerons que peu importe l'entier $n \geq 7$, il existe une boucle incassable d'ordre n. Pour les ordres 5 et 6, il suffit de voir les boucles de la figure 1.4 pour voir qu'elles sont incassables. La preuve présentée dans cette section a été construite par Martin Beaudry et François Lemieux pour un article qui n'est pas encore publié. Elle est basée sur la propriété suivante des rectangles latins.

Proposition 2.2.1 Soit T un rectangle latin d'ordre n de taille r par s basé sur les éléments $0, \cdots, n-1$. Soit $N(i)$, le nombre de fois où l'élément i apparaît dans le rectangle latin. T peut être étendu à un carré latin d'ordre n si et seulement si, pour tout $i \in \{0, \cdots, n-1\}$, $N(i) \leq r + s - n$.

Preuve : Voir [20]. ■

Théorème 2.2.2 Pour tout $n \geq 7$, il existe une boucle incassable d'ordre n.

Preuve :
Cas où n est impair : Soit $H = \{0, 1, \cdots, 2p\}$, un ensemble de n éléments avec $n = 2p + 1$ et $p \geq 3$. Prenons $E = \{0, 1, \cdots, p\}$ et $F = \{p+1, p+2, \cdots, 2p\}$. Nous allons construire un rectangle latin de hauteur $r = p + 1$ et de largeur $s = n$.

Nous noterons $[i, j]$ pour $i \in E$ et $j \in H$ l'élément du rectangle latin à la ligne i et à la colonne j. À chaque étape de la construction de notre rectangle latin, nous allons voir un exemple pour $n = 9$ ($p = 4$).
En premier lieu, nous voulons imposer la présence de l'identité dans notre rectangle latin. Pour cela, nous mettons $[i, 0] = i$ et $[0, j] = j$ pour tout $i \in E$ et $j \in H$. On obtient le résultat de la figure 2.1.

0	1	2	3	4	5	6	7	8
1								
2								
3								
4								

figure 2.1 – Exemple : Rectangle latin partiel avec identité

Pour assigner un élément aux $2p^2$ positions restantes, nous allons séparer les colonnes 1 à $2p$ en deux parties que nous appellerons partie gauche G, de largeur p, et partie droite D, de largeur p. Les traits dans les exemples servent à mettre en évidence l'identité ainsi que les parties G et D.

0	1	2	3	4	5	6	7	8
1								
2			G				D	
3								
4								

figure 2.2 – Exemple : Rectangle latin partiel - Parties G et D

Nous allons maintenant remplir le carré G avec les éléments de F et D avec les éléments de E de la manière suivante :

$$G = \begin{array}{ccccccc} p+1 & 2p & 2p-1 & 2p-2 & \cdots & p+3 & p+2 \\ p+2 & p+1 & 2p & 2p-1 & \cdots & p+4 & p+3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2p-1 & 2p-2 & 2p-3 & 2p-4 & \cdots & p+1 & 2p \\ 2p & 2p-1 & 2p-2 & 2p-3 & \cdots & p+2 & p+1 \end{array}$$

et :

$$D = \begin{array}{cccccc} 2 & 3 & \cdots & p-1 & p & 0 \\ 3 & 4 & \cdots & p & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ p & 0 & \cdots & p-4 & p-3 & p-2 \\ 0 & 1 & \cdots & p-3 & p-2 & p-1 \end{array}$$

Les deux carrés sont de taille $p \times p$. La figure 2.3 contient le résultat de notre exemple.

0	1	2	3	4	5	6	7	8
1	5	8	7	6	2	3	4	0
2	6	5	8	7	3	4	0	1
3	7	6	5	8	4	0	1	2
4	8	7	6	5	0	1	2	3

figure 2.3 – Exemple : Rectangle latin partiel

Il ne nous reste qu'à permuter les éléments de $[p, p]$ et de $[p, 2p]$ pour obtenir le rectangle latin final.

0	1	2	3	4	5	6	7	8
1	5	8	7	6	2	3	4	0
2	6	5	8	7	3	4	0	1
3	7	6	5	8	4	0	1	2
4	8	7	6	3	0	1	2	5

figure 2.4 – Exemple : Rectangle latin, ordre impair

Dans ce rectangle latin, chaque élément de H apparaît exactement $p + 1$ fois. Donc, on a $N(i) = p + 1$ pour tout $i \in H$. Pour utiliser la proposition 2.2.1, on doit montrer que $N(i) \leq r + s - n$. Puisque $s = n$, on a $r + s - n = r = p + 1$. D'où, $N(i) = p + 1 \leq r + s - n = p + 1$. Par la proposition 2.2.1, il est possible de compléter un carré latin de taille $n \times n$ à partir de ce rectangle latin. Pour s'assurer d'avoir l'identité dans la colonne 0, on peut permuter les lignes $p + 1$ à $2p$ de manière à ce que

$[i, 0] = i$ pour tout $i \in H$.

Par la proposition 1.1.4, le carré latin que nous avons est la table de Cayley d'un quasigroupe $(H, *)$ et, puisque 0 est un élément identité, $(H, *)$ est une boucle. Il ne reste qu'à montrer que cette boucle est incassable. Nous montrerons cela en démontrant que pour tout $i \neq 0$, i engendre tous les éléments de la boucle.

En premier lieu, observons la colonne $p + 1$. On voit que, pour tout $1 \leq i \leq p - 1$, on a $i * (p + 1) = i + 1$ et que $p * (p + 1) = 0$. Observer également que, toujours pour $1 \leq i \leq p - 1$, on a $i * i = p + 1$. En d'autres mots, tous les éléments i tels que $1 \leq i \leq p - 1$ engendrent tous les éléments de i à p ainsi que l'identité 0.

Maintenant, observons que la colonne $2p$ effectue le processus inverse. En effet, on voit que pour tout $1 \leq i \leq p - 1$, on a $i * 2p = i - 1$. Également, observons que, toujours pour $1 \leq i \leq p - 1$, on a $i * i = p + 1$, $i * (p + 1) = i + 1$ et que $i * (i + 1) = 2p$. Ensuite, $i * 2p = i - 1$, $(i - 1) * 2p = i - 2, \cdots, 1 * 2p = 0$. En d'autres mots, tous les éléments i tels que $1 \leq i \leq p - 1$ engendrent tous les éléments x de 0 à i.

Nous obtenons donc que chaque élément de 0 à $p - 1$ engendre tous les éléments de 0 à p. Ensuite, puisque $p * p = p - 1$, il en est de même pour p. Observons maintenant qu'avec tous les éléments de 1 à p, on peut engendrer tous les éléments de $p + 1$ à $2p$. En effet, on voit que $1 * 1 = p + 1$, $1 * 2 = p + 2, \cdots, 1 * p = 2p$. En d'autres mots, chaque élément de 1 à p engendre tous les éléments de la boucle.

Il nous reste à montrer que les éléments $p + 1$ à $2p$ engendrent tous les éléments de la boucle. Pour montrer cela, supposons qu'il existe une sous-boucle propre de $(H, *)$ notée $(B, *)$. Alors B contient 0 et certains éléments de F. Soit $j \in B$ avec $j \neq 0$, un élément de la sous-boucle différent de 0. Par le corollaire 1.1.5, il existe un élément $k \in B$ tel que $j * k = 0$. Cela implique dans la table de Cayley de $(H, *)$ que l'élément de $[j, k]$ est 0. Mais, puisque $p + 1 \leq k \leq 2p$ et que toutes les colonnes de $p + 1$ à $2p$ contiennent déjà un 0, on obtient qu'il ne s'agit pas d'un carré latin. Donc, par contradiction, il n'y a aucune sous-boucle propre dans $(H, *)$. Ainsi, on en conclut que la boucle est incassable.

Cas où n est pair :

La preuve du cas n pair est très similaire à la preuve du cas n impair. Donc, certaines étapes de la construction seront expliquées plus rapidement. Nous allons donner un

exemple pour chaque étape en utilisant $n = 10$ ($p = 5$).
Soit $H = \{0, 1, \cdots, 2p-1\}$, un ensemble de n éléments avec $n = 2p$ et $p \geq 3$. Prenons $E = \{0, 1, \cdots, p-1\}$ et $F = \{p, p+1, \cdots, 2p-1\}$. Nous allons créer un rectangle latin de hauteur $r = p+1$ et de largeur $s = n$. Tout comme pour le cas n impair, nous commençons par imposer l'élément identité comme étant 0, ensuite, on sépare les colonnes 1 à $2p-1$ en deux parties G et D avec G de largeur p et D de largeur $p-1$.

0	1	2	3	4	5	6	7	8	9
1									
2									
3				G			D		
4									
5									

figure 2.5 – Exemple : Rectangle latin, parties G et D

Nous allons maintenant remplir le carré G avec les éléments de F et le rectangle D avec les éléments de E de la manière suivante :

$$G = \begin{array}{ccccccc} p & 2p-1 & 2p-2 & 2p-3 & \cdots & p+2 & p+1 \\ p+1 & p & 2p-1 & 2p-2 & \cdots & p+3 & p+2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2p-2 & 2p-3 & 2p-4 & 2p-5 & \cdots & p & 2p-1 \\ 2p-1 & 2p-2 & 2p-3 & 2p-4 & \cdots & p+1 & p \end{array}$$

et :

$$D = \begin{array}{cccccc} 2 & 3 & \cdots & p-2 & p-1 & 0 \\ 3 & 4 & \cdots & p-1 & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ p-1 & 0 & \cdots & p-5 & p-4 & p-3 \\ 0 & 1 & \cdots & p-4 & p-3 & p-2 \\ 1 & 2 & \cdots & p-3 & p-2 & p-1 \end{array}$$

La figure 2.6 contient le résultat de notre exemple.

0	1	2	3	4	5	6	7	8	9
1	5	9	8	7	6	2	3	4	0
2	6	5	9	8	7	3	4	0	1
3	7	6	5	9	8	4	0	1	2
4	8	7	6	5	9	0	1	2	3
5	9	8	7	6	5	1	2	3	4

figure 2.6 – Exemple : Rectangle latin partiel, après parties G et D

Sans toucher à la ligne et à la colonne identité (ligne et colonne 0), nous allons interchanger toutes les occurrences de p et de $p+1$ ainsi que toutes les occurrences de 0 et de 1. La figure 2.7 contient le résultat.

0	1	2	3	4	5	6	7	8	9
1	6	9	8	7	5	2	3	4	1
2	5	6	9	8	7	3	4	1	0
3	7	5	6	9	8	4	1	0	2
4	8	7	5	6	9	1	0	2	3
5	9	8	7	5	6	0	2	3	4

figure 2.7 – Exemple : Rectangle latin partiel, après changements de 1 et de 0

Ce résultat intermédiaire n'est pas un rectangle latin. En effet, on voit que l'élément 1 se retrouve deux fois dans la ligne 1. Donc, nous allons effectuer deux modifications. En premier lieu, nous permutons les valeurs des positions $[p, p]$ et $[p, 2p-1]$. Ensuite, nous assignons $[p, p-1] = 1$, $[1, p] = 0$ et $[1, 2p-1] = p$. La figure 2.8 contient le résultat.

0	1	2	3	4	5	6	7	8	9
1	6	9	8	7	0	2	3	4	5
2	5	6	9	8	7	3	4	1	0
3	7	5	6	9	8	4	1	0	2
4	8	7	5	6	9	1	0	2	3
5	9	8	7	1	4	0	2	3	6

figure 2.8 – Exemple : Rectangle latin, ordre pair

Ceci est un rectangle latin dans lequel chaque élément de H apparaît exactement $p+1$ fois. Donc, on a $N(i) = p+1$ pour tout $i \in H$. Puisque $s = n$, on a $r+s-n = r = p+1$. D'où, $N(i) = p+1 \leq r+s-n = p+1$. Par la proposition 2.2.1, il est possible de compléter un carré latin de taille $n \times n$ à partir de ce rectangle latin. Pour s'assurer d'avoir l'identité, on permute les lignes comme dans le cas impair.

Par la proposition 1.1.4, nous avons la table de Cayley d'un quasigroupe $(H, *)$ et, puisque 0 est un élément identité, $(H, *)$ est une boucle. Il ne reste qu'à montrer que cette boucle est incassable. Nous montrerons cela en montrant que pour tout $i \neq 0$, i engendre tous les éléments de la boucle.

En premier lieu, montrons que l'élément 1 engendre tous les éléments de la boucle. On a d'abord $1 * 1 = p+1$. Ensuite, pour i de 1 à $p-2$, $i * (p+1) = i+1$. En d'autres mots, 1 engendre tous les éléments de 1 à $p-1$. L'élément p est engendré à partir de 1 puisque 2 est déjà engendré (car $p \geq 3$) et $2 * 1 = p$. Donc, les éléments 1 à $p+1$ peuvent être engendrés à partir de 1. Pour engendrer les autres éléments, observons que : $3*1 = p+2, 4*1 = p+3, \cdots, p*1 = 2p-1$. Nous obtenons donc que l'élément 1 engendre tous les éléments de la boucle.

Maintenant, pour i de 1 à $p-1$, on a $i * i = p+1$ et on sait que pour j de 1 à $p-2$, $j*(p+1) = j+1$. Puisque $(p-1)*(p+1) = 1$, on en déduit que tous les i engendrent l'élément 1, et donc tous les éléments de la boucle.

L'élément p engendre également tous les éléments de la boucle puisque $p * p = p-1$.

Enfin, en utilisant exactement la même preuve par l'absurde que dans le cas n impair, on peut montrer que les éléments de $F \cup \{0\}$ ne peuvent pas engendrer de sous-boucle propre. ■

2.3 Résultats expérimentaux

Maintenant que nous savons qu'il vaut la peine d'étudier les boucles incassables, nous devons savoir comment se comporte le groupe de multiplication de ces boucles. Pour étudier le groupe de multiplication des boucles incassables de petit ordre, nous les avons traitées exhaustivement.

Nous avons d'abord commencé par créer un fichier informatique contenant un élément de chaque classe d'isomorphisme de boucles pour les ordres de 5 à 8. Pour effectuer cette tâche nous avons utilisé un logiciel de calcul de groupoïdes dont l'implémentation et les algorithmes sont décrits dans le mémoire [10]. Comme résultat, nous avons obtenu six boucles d'ordre 5, 109 boucles d'ordre 6, 23 746 boucles d'ordre 7 et 106 228 849 boucles d'ordre 8. Nous n'avons pas généré les boucles d'ordre 9 et plus car nous n'avions pas une puissance de calcul suffisante pour les calculer (voir tableau 2.1). Ensuite, pour extraire les boucles incassables de ces fichiers, nous avons utilisé l'algorithme 2.

Grâce à cet algorithme, nous avons obtenu deux boucles incassables d'ordre 5, 28 boucles incassables d'ordre 6, 9 906 boucles incassables d'ordre 7 et 43 803 136 boucles incassables d'ordre 8 (voir tableau 2.1).

Maintenant, il est très possible que dans les boucles contruites, il s'y cache des groupes. Mais, nous savons que si G est un groupe, alors $\mathcal{M}(G) = G$. Donc nous avons utilisé l'algorithme 3 pour ne garder que des boucles qui ne sont pas des groupes. Cet algorithme a enlevé une boucle d'ordre 5 et une boucle d'ordre 7 ($\mathbb{Z}_5$ et $\mathbb{Z}_7$). Le tableau 2.1 donne un compte rendu des résultats.

Il nous reste maintenant à calculer le groupe multiplicatif de chacune de ces boucles. Pour ce faire, nous allons utiliser l'algorithme 1 vu plus tôt ainsi que les algorithmes 4 et 5.

Lorsque nous avons obtenu le groupe de multiplication d'une de nos boucles, nous devons savoir s'il s'agit du groupe symétrique, du groupe alterné ou bien d'un autre groupe. Pour ce faire, il suffit de regarder la taille (nombre d'éléments) du groupe de multiplication.

Ordre	N^{bre} total de boucles [14]	N^{bre} de boucles incassables	N^{bre} de boucles associatives	N^{bre} de boucles restantes
5	6	2	1*	1
6	109	28	0	28
7	23 746	9 906	1*	9 905
8	106 228 849	43 803 136	0	43 803 136
9	9 365 022 303 540	Non calculé	0	Non calculé

* $\mathbb{Z}_n$ est une boucle incassable pour n premier.

tableau 2.1 – Résultat de la génération des boucles

Si le groupe de multiplication d'une boucle d'ordre n est de taille $n!$, il s'agit du groupe symétrique $\mathcal{S}_n$, si la taille est $n!/2$, il s'agit du groupe alterné $\mathcal{A}_n$ et si la taille du groupe n'est aucune des deux, il s'agit d'un autre groupe. Après avoir exécuté ces algorithmes sur chacune des boucles incassables que nous avions, nous avons obtenu des résultats surprenants. En premier lieu, toutes les boucles d'ordre 5 et 6 ont le groupe symétrique comme groupe de multiplication. Dans les 9 905 boucles d'ordre 7, une seule boucle a le groupe alterné comme groupe de multiplication (voir figure 2.9). Toutes les autres boucles d'ordre 7 ont le groupe symétrique comme groupe multiplicatif. Dans les boucles d'ordre 8, 43 799 370 boucles (soit 99,99% des boucles d'ordre 8) ont le groupe symétrique comme groupe de multiplication, 3 765 ont le groupe alterné et une dernière boucle a un autre groupe comme groupe de multiplication (voir 2.10). Le tableau 2.2 donne un compte rendu des résultats.

Ordre n	N^{bre} de Boucles	Groupe de multiplication		
		$\mathcal{S}_n$	$\mathcal{A}_n$	Autres
5	1	1	0	0
6	28	28	0	0
7	9 905	9 904	1	0
8	43 803 136	43 799 370	3 765	1

tableau 2.2 – Groupe de multiplication des boucles incassables

Nous voyons que la très grande majorité des boucles incassables calculées ont le groupe symétrique comme groupe de multiplication. Il y a toutefois certains cas plus particuliers

que nous n'aborderons que brièvement durant ce travail. Ces cas particuliers sont les suivants.

Le premier cas observé est la boucle incassable d'ordre 7 de la figure 2.9.

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	0	4	3	6	5
2	2	0	3	5	6	4	1
3	3	4	5	6	1	2	0
4	4	3	6	1	5	0	2
5	5	6	4	2	0	1	3
6	6	5	1	0	2	3	4

figure 2.9 – Boucle d'ordre 7 avec $\mathcal{M} \cong \mathcal{A}_7$

Cette boucle est la seule boucle incassable d'ordre 7 à avoir le groupe alterné comme groupe de multiplication. On remarque en plus que la boucle est commutative.

L'autre résultat surprenant est la boucle incassable d'ordre 8 de la figure 2.10.

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	0	5	6	7	4
2	2	4	7	6	1	3	0	5
3	3	6	1	5	2	7	4	0
4	4	0	5	7	6	2	3	1
5	5	7	0	4	3	1	2	6
6	6	5	4	2	7	0	1	3
7	7	3	6	1	0	4	5	2

figure 2.10 – Boucle d'ordre 8 avec $\mathcal{M} \ncong \mathcal{S}_8$ et $\mathcal{M} \ncong \mathcal{A}_8$

Cette boucle est la seule boucle des 43 803 136 boucles incassables d'ordre 8 dont le groupe de multiplication n'est pas le groupe symétrique ni le groupe alterné. La cardinalité du groupe de multiplication de cette boucle est de 1 344, soit $8!/30$. À l'aide du logiciel GAP (GAP-Groups, Algorithms, and programming version 4.4.10, www.gap-system.org), nous avons établi qu'il s'agit d'un groupe isomorphe au groupe Galois G_{1344} (également noté $AL(8)$), qui consiste en un produit semidirect du groupe $\mathbb{Z}_2^3$ et du groupe $PSL(2,7)$ ($G_{1344} = \mathbb{Z}_2^3 \rtimes PSL(2,7)$) [7]. Le fait de savoir s'il existe une famille infinie de boucles incassables dont le groupe multiplicatif est un groupe isomorphe à un groupe Galois est hors de la portée de ce travail. Il est cependant à noter qu'aucun groupe Galois isomorphe à $PSL(2,q)$ ne peut être isomorphe au groupe de multiplication d'une boucle [23].

Ces résultats nous permettent d'établir un plan d'action pour la suite du travail. En premier lieu, il est clair que le nombre de boucles incassables augmente significativement lorsqu'on prend des ordres plus élevés. Il est donc probable que le nombre de boucles commutatives augmente également significativement lorsqu'on prend des ordres de boucles plus élevés. En plus, il est plus facile de travailler avec des boucles commutatives puisque leur table de Cayley est symétrique autour de la diagonale ($L_a = R_a$ pour tout a). Également, on constate que la très grande majorité des boucles incassables ont le groupe symétrique comme groupe de multiplication. Donc, la première étape consiste à extraire les boucles commutatives des boucles que nous avons produites dans cette section et de les examiner pour voir s'il est possible construire une famille infinie de boucles incassables commutatives dont le groupe de multiplication est le groupe symétrique.

Entrée : A : Ensemble des éléments contenus dans la boucle
($0 \in A$ est l'élément indentité de la boucle).
$\cdot$: loi de composition interne de la boucle.
Sortie : $vrai$ si la boucle $(A, \cdot)$ est incassable, sinon $faux$.

EST_INCASSABLE(A,$\cdot$) **début**
  $resultat = vrai$
  pour tout $x \in A \setminus \{0\}$ **faire**
    $changement := vrai$
    $B := \{x\}$
    tant que $|B| < |A|$ *et* $changement = vrai$ **faire**
      $C := B$
      $changement = faux$
      pour tout $(x, y) \in B \times B$ **faire**
        $C := C \cup \{x \cdot y\}$
      fin pour tout
      si $|C| \neq |B|$ **alors**
        $changement = vrai$
      fin si
    fin tant que
    si $|B| \neq |A|$ **alors**
      $resultat = faux$
    fin si
  fin pour tout
  retourne $resultat$
fin

Algorithme 2 : Vérifie si la boucle est incassable

Entrée : A : Un ensemble
$\cdot$: loi de composition interne de l'ensemble.
Sortie : $vrai$ si $(A, \cdot)$ est associatif, sinon $faux$.

EST_ASSOCIATIF(A,$\cdot$) **début**
  $resultat = vrai$
  pour tout $(x, y, z) \in A \times A \times A$ **faire**
    si $(x \cdot y) \cdot z \neq x \cdot (y \cdot z)$ **alors**
      $resultat = faux$
    fin si
  fin pour tout
  retourne $resultat$
fin

Algorithme 3 : Valide si le groupoïde est associatif

Entrée : $perm1$: Première permutation sous forme de vecteur.
$perm2$: Seconde permutation sous forme de vecteur.
(Les vecteurs sont indexés de 0 à $n-1$).
Sortie : Permutation sous forme de vecteur résultante du produit des deux permutations.

OPER_PERM($perm1$,$perm2$) **début**
  $n = |perm1|$
  $resultat$ =Vecteur(n)
  pour i **de** 0 **à** $n-1$ **faire**
    $resultat[i] = perm2[perm1[i]]$
  fin pour
  retourne $resultat$
fin

Algorithme 4 : Calcule le produit de deux permutations (sous forme de vecteur)

Entrée : n : Ordre du quasigroupe Q.
T : Table de dimension $n \times n$ représentant la table de Cayley du quasigroupe Q (indexé de $T[0,0]$ à $T[n-1, n-1]$).
Sortie : Ensemble contenant tous les éléments de $\mathcal{M}(Q)$

GROUPE_MULT(n,T) **début**
  $P := \emptyset$
  pour i **de** 0 **à** $n-1$ **faire**
    $permCol$:=Vecteur(n)
    $permLig$:=Vecteur(n)
    pour j **de** 0 **à** $n-1$ **faire**
      $permCol[j] := T[i,j]$
      $permLig[j] := T[j,i]$
    fin pour
    $P := P \cup \{permCol, permLig\}$
  fin pour
  $resultat$:=FERMETURE_ENSEMBLE(P,OPER_PERM)
  retourne $resultat$
fin

Algorithme 5 : Calcule le groupe de multiplication d'un quasigroupe

Chapitre 3

Famille de boucles incassables commutatives d'ordre premier dont le groupe de multiplication est le groupe symétrique

Dans la section précédente, nous avons vu que pour tout $n \geq 5$, il y avait toutes les chances pour qu'il existe une boucle incassable B d'ordre n dont le groupe de multiplication est le groupe symétrique ($\mathcal{M}(B) \cong \mathcal{S}_n$). Également, le fait d'avoir une boucle commutative semble nous faciliter la tâche lors de l'analyse des L_a et R_a puisque $L_a = R_a$ pour tout $a \in B$. À l'origine, la preuve faite dans ce présent chapitre avait pour but de montrer l'existence d'une boucle incassable commutative pour tous les ordres impairs. Par contre, après certaines expérimentations, nous avons remarqué que notre solution fonctionnait seulement pour les boucles d'ordre premier. Mais, puisque la boucle est très simple à construire et que le résultat est tout de même intéressant, nous le présentons.

3.1 Résultat expérimental

La commutativité permet de réduire le travail à faire lors de la création de boucles. Sachant cela, nous avons commencé à étudier les boucles incassables commutatives. La pre-

mière chose qui a été faite est de ressortir de nos données expérimentales précédemment calculées les boucles incassables commutatives. Pour ce faire, nous avons utilisé l'algorithme 6.

En exécutant cet algorithme, nous avons seulement trouvé huit boucles incassables commutatives d'ordre 7. L'absence de boucles incassables commutatives d'ordre 8 s'explique par la proposition suivante (voir [9], Chapitre 8).

Proposition 3.1.1 Il n'existe aucune boucle incassable commutative d'ordre pair.

Preuve : Soit $(B, *)$ une boucle incassable d'ordre n pair et soit 0, son élément identité. Puisque $(B, *)$ est incassable, il n'existe aucun élément $a \in B$ tel que $a * a = 0$ (sauf bien sûr si $a = 0$) : si tel était le cas, $(\{0, a\}, *)$ formerait une sous-boucle de $(B, *)$. Décrivons les 0 dans la table de Cayley de $(B, *)$ de manière constructive en respectant la commutativité. Posons H, l'ensemble des lignes $b \neq 0$ n'ayant pas encore de 0 assigné (pas encore de c tel que $b * c = 0$). Initialement, H contient $n - 1$ éléments (puisque $0 * 0 = 0$) qui est un nombre impair. Lorsqu'on assigne un 0 à un élément b parce que $b * c = 0$, on assigne également un 0 à l'élément c puisque $c * b = 0$ (par commutativité). Donc, lorsqu'on assigne un 0 à un élément, on enlève deux éléments de l'ensemble H. Puisque H possède un nombre impair d'éléments, en enlevant de H des éléments deux à deux, on voit qu'avant d'être vide, H contiendra un seul élément x. Donc pour assigner un 0 à x, nous devons faire que $x * x = 0$. Mais nous savons que si $x * x = 0$, la boucle $(B, *)$ n'est pas incassable. Ainsi, il est impossible de respecter la commutativité pour assigner tous les 0 lors de la création d'une boucle incassable d'ordre pair. De ce fait, on conclut qu'il n'existe aucune boucle incassable commutative d'ordre pair. ■

Par expérimentation, nous savons que pour les ordres $n < 9$, seul l'ordre 7 contient des boucles incassables commutatives. Mais, il y a toutes les possibilités pour qu'il existe un grand nombre de boucles incassables commutatives d'ordre 9. Par contre, nous n'avons pas la puissance de calcul nécessaire pour les chercher exhaustivement.

Maintenant le but est de trouver, avec ce que nous avons, une structure de boucle incassable commutative qui soit facile à comprendre et facilement généralisable. Le problème est que nous n'avons que huit boucles incassables commutatives connues et qu'il s'agit d'un

très petit échantillon à étudier. Pour corriger ce manque, nous avons utilisé l'algorithme 7 pour produire toutes les boucles isomorphes aux huit boucles incassables commutatives que nous avions. La fonction ISOMORPHISME permet d'obtenir le groupoïde résultant de l'échange de l'étiquetage de i et de j. Cette fonction s'implémente avec l'algorithme 8.

L'utilisation de ces algorithmes sur chacune des boucles incassables commutatives d'ordre 7 nous a donné 720 nouvelles tables de Cayley par boucle, soit 5 760 boucles. Nous nous retrouvons donc avec trop de boucles pour une analyse exhaustive. Nous devons donc établir des restrictions pour éliminer des boucles. La première restriction sera de garder seulement les boucles dont le groupe de multiplication est le groupe symétrique. Cette restriction élimine 720 boucles, mais ce n'est pas suffisant. La seconde restriction consiste à garder seulement les boucles où L_1 forme la permutation $(0\,1\,2\,3\,4\,5\,6)$. Cette restriction est intéressante parce que le produit d'une permutation sous cette forme avec une autre permutation effectue une rotation circulaire sur les éléments de cette autre permutation.

Exemple : Dans le produit de permutations suivant (figure 3.1), on voit que la permutation résultante est une rotation circulaire de 1 vers la gauche par rapport à la seconde permutation du produit.

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 6 & 3 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 0 & 4 & 2 \end{pmatrix}$$

figure 3.1 – Permutation permettant une rotation circulaire d'une autre permutation

Une fois ces restrictions appliquées sur les 5 720 boucles incassables produites plus haut, nous obtenons 16 boucles incassables. Ainsi, nous avons pu examiner chacune d'elle et en choisir une qui semble intéressante. La figure 3.2 représente la table de Cayley de la boucle qui a été choisie. La boucle a été choisie parce qu'elle semble facile à décrire. En effet, plus de 50% de la table de Cayley de la boucle est identique à celle du groupe Z_n.

Pour généraliser cette boucle nous devons commencer par avoir certains exemples

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	1	5	6	0	4
3	3	4	5	6	0	1	2
4	4	5	6	0	3	2	1
5	5	6	0	1	2	4	3
6	6	0	4	2	1	3	5

figure 3.2 – Boucle incassable modèle pour la première famille

d'ordre supérieur à 7. Pour construire ces exemples, nous utiliserons une boucle trouée comme celle de la figure 3.3 (exemple pour l'ordre 9). Un point d'interrogation (?) représente une position dont le contenu n'est pas fixé d'avance. Pour compléter cette boucle, on utilise l'algorithme 9.

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	0	7	0
2	2	3	1	5	6	7	8	0	4
3	3	4	5	6	7	8	0	?	?
4	4	5	6	7	8	0	?	?	?
5	5	6	7	8	0	?	?	?	?
6	6	7	8	0	?	?	?	?	5
7	7	8	0	?	?	?	?	5	6
8	8	0	4	?	?	?	5	6	7

figure 3.3 – Table de Cayley trouée pour la production de boucles

Pour s'assurer que les résultats sont des boucles, il suffit de s'assurer que chaque ligne et colonne ne contient qu'une seule fois chaque élément de 0 à $n-1$. Pour valider que le résultat n'est pas un groupe, on peut utiliser l'algorithme EST_ASSOCIATIF (algorithme 3). De plus, pour s'assurer qu'il s'agit d'une boucle incassable, on peut utiliser l'algorithme EST_INCASSABLE (algorithme 2). Enfin, pour s'assurer que la boucle incassable

est commutative, on peut utiliser l'algorithme EST_COMMUTATIF (algorithme 6).

En utilisant ces algorithmes nous avons produit des boucles incassables commutatives dont le groupe de multiplication est le groupe symétrique pour les ordres n premiers jusqu'à l'ordre 31. En utilisant ces exemples, nous avons réussi à construire une famille infinie de boucles incassables commutatives d'ordre n premier avec $n \geq 13$, dont le groupe de multiplication est le groupe symétrique.

Entrée : n : Ordre du groupoïde
T : Table de dimension $n \times n$ représentant la table de Cayley du groupoïde (les éléments de T sont 0 à $n-1$).
Sortie : $Vrai$ si le groupoïde est commutative, $faux$ sinon

EST_COMMUTATIF(n, T) **début**
  $resultat := Vrai$
  pour i **de** 0 **à** $n-1$ **faire**
    pour j **de** 0 **à** $n-1$ **faire**
      si $T[i][j] \neq T[j][i]$ **alors**
        $resultat := Faux$
      fin si
    fin pour
  fin pour
  retourne $resultat$
fin

Algorithme 6 : Décide si un groupoïde est commutatif

Entrée : n : Ordre de la boucle
T : Une boucle sous forme de table de dimension $n \times n$ représentant la table de Cayley (les éléments de T sont 0 à $n-1$).
Sortie : Ensemble des boucles isomorphes à T (incluant T)

```
GEN_ISOMORPHISME(n, T) début
    R := {T}
    fin := Faux
    tant que fin = Faux faire
        fin := vrai
        pour tout B ∈ R faire
            pour tout i ∈ B\{0} faire
                pour tout j ∈ B\{0, i} faire
                    N :=ISOMORPHISME(n, B, i, j)
                    si N ∉ R alors
                        R := R ∪ {N}
                        fin := faux
                    fin si
                fin pour tout
            fin pour tout
        fin pour tout
    fin tant que
    retourne R
fin
```

Algorithme 7 : Retourne tous les isomorphismes d'une boucle (garde l'identité à 0)

Entrée : n : Ordre du groupoïde
T : Table de dimension $n \times n$ représentant la table de Cayley du groupoïde (les éléments de T sont 0 à $n-1$).
x : L'index du premier élément à échanger
y : L'index du deuxième élément à échanger
Sortie : L'isomorphisme de T avec x et y échangés

```
ISOMORPHISME(n, T, x, y) début
    R := T
    pour i de 0 à n − 1 faire
        pour j de 0 à n − 1 faire
            si T[i][j] = x alors
                R[i][j] := y
            fin si
            si T[i][j] = y alors
                R[i][j] := x
            fin si
        fin pour
    fin pour
    permuter les lignes x et y dans R
    permuter les colonnes x et y dans R
    retourne R
fin
```

Algorithme 8 : Applique l'isomorphisme sur le groupoïde

Entrée : n : Ordre du groupoïde
T : Table de dimension $n \times n$ représentant la table de Cayley incomplète du quasigroupe (les éléments de T sont 0 à $n-1$ et ?).
H : L'ensemble des quasigroupes déjà calculés (initialement vide)
Sortie : L'ensemble des quasigroupes que l'on peut construire avec T
GEN_QUASIGROUPE(n, T, H) **début**
  $Q := T$; $trouve := Faux$; $i := 0$; $j := 0$
  tant que $j < n-1$ **faire**
    si $T[i][j] =?$ **alors**
      $trouve := Vrai$
      pour k **de** 0 **à** $n-1$ **faire**
        $ok := Vrai$
        pour l **de** 0 **à** $n-1$ **faire**
          si $T[i][l] = k$ **ou** $T[l][j] = k$ **alors**
            $ok := Faux$
          fin si
        fin pour
        si $ok = Vrai$ **alors**
          $Q[i][j] := k$
          $H := H \cup$ GEN_QUASIGROUPE(n, Q, H)
        fin si
      fin pour
    fin si
    $i := i + 1$
    si $i = n$ **alors**
      $i := 0$; $j := j + 1$
    fin si
  fin tant que
  si $trouve = Faux$ **alors**
    $H := H \cup \{Q\}$
  fin si
  retourne H
fin

Algorithme 9 : Remplace les ? par des éléments afin d'obtenir un quasigroupe

3.2 Construction et preuve

Dans cette section, nous allons montrer comment construire des boucles incassables commutatives d'ordre premier dont le groupe de multiplication est le groupe symétrique. La construction sera faite dans la proposition suivante. À chaque étape, je ferai un exemple à l'aide d'une boucle d'ordre 13. La notation $[i, j]$ représente la cellule à la ligne i et à la colonne j dans la table de Cayley. La première ligne (resp. colonne) de la table de Cayley est 0 et la dernière est $n-1$. Cette construction fonctionne pour tout ordre premier supérieur ou égal à 13.

Construction 3.2.1 Dans toute notre construction, nous décrirons comment remplir les cellules $[i, j]$ pour $i \leq j$; il sera partout sous-entendu que la cellule $[j, i]$ aura le même contenu que $[i, j]$. Donc, la boucle sera commutative par construction.

Soit n, un nombre premier tel que $n \geq 13$ et $p = \frac{n+1}{2}$. En premier lieu, pour i et j tel que $0 \leq i \leq n-1$ et $0 \leq j \leq i+1$, prenons $[i, j] = i + j(mod\ n)$. Ensuite, pour i et j tel que $i \geq 6$ et $n - i + 5 \leq j \leq n - 1$, prenons $[i, j] = i + j(mod\ n)$. Enfin, pour tout $0 \leq i \leq 3$ et $0 \leq j \leq n - 1$, prenons $[i, j] = i + j(mod\ n)$ et $[j, i] = j + i(mod\ n)$. Ceci construit la portion de la table de Cayley dont le contenu est identique à celui de la table de Z_n. La figure 3.4 représente la table après cette étape. La ligne tracée sous la diagonale permet de bien voir que la table est symétrique. Nous allons remplir la partie supérieure droite de la table ; la partie inférieure gauche est remplie par symétrie.

Maintenant, assignons les valeurs $[2, 2] = 1$ et $[2, n-1] = 4$.

Les trous restants doivent être remplis avec des éléments entre 1 et 4. Donc, assignons $[5, n-1] = 1$, $[p, p] = 3$, $[p+1, p+1] = 4$, $[p, p+1] = 1$, $[p-1, p+1] = 2$ et $[p+1, p+2] = 3$. Dans la figure 3.5, les éléments modifiés depuis la figure 3.4 sont en caractères gras.

Il reste encore une zone incomplète. Cette zone sera nommée escalier. On voit que l'escalier du haut et l'escalier du bas n'ont aucune ligne ni colonne en commun, ce qui nous permet de travailler sur un seul d'entre eux, l'autre étant construit par symétrie. Nous travaillerons donc seulement avec l'escalier des lignes 5 à p. Un escalier est formé d'une marche incomplète de taille 3 sur la ligne 5, suivi de $p - 7$ marches complètes de taille 4

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	4	5	6	7	8	9	10	11	12	0	1
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	?	?	?	?
6	6	7	8	9	10	11	12	0	?	?	?	?	5
7	7	8	9	10	11	12	0	?	?	?	?	5	6
8	8	9	10	11	12	0	?	?	?	?	5	6	7
9	9	10	11	12	0	?	?	?	?	5	6	7	8
10	10	11	12	0	1	?	?	?	5	6	7	8	9
11	11	12	0	1	2	?	?	5	6	7	8	9	10
12	12	0	1	2	3	?	5	6	7	8	9	10	11

figure 3.4 – Portion Z_n de carré latin

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	**1**	5	6	7	8	9	10	11	12	0	**4**
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	?	?	?	**1**
6	6	7	8	9	10	11	12	0	**2**	?	?	?	5
7	7	8	9	10	11	12	0	**3**	**1**	?	?	5	6
8	8	9	10	11	12	0	**2**	**1**	**4**	**3**	5	6	7
9	9	10	11	12	0	?	?	?	**3**	5	6	7	8
10	10	11	12	0	1	?	?	?	5	6	7	8	9
11	11	12	0	1	2	?	?	5	6	7	8	9	10
12	12	0	**4**	2	3	**1**	5	6	7	8	9	10	11

figure 3.5 – Carré latin incomplet - sans les escaliers

sur les lignes 6 à $p-2$, puis d'une marche incomplète de taille 3 sur la ligne $p-1$ et enfin d'une marche incomplète de taille 2 sur la ligne p. La figure 3.6 donne une représentation visuelle de l'escalier.

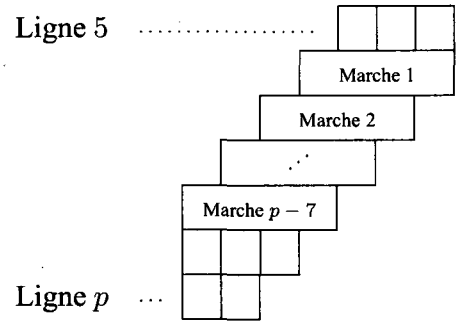

figure 3.6 – Généralisation de l'escalier

Pour remplir cet escalier, nous séparerons deux cas.

Cas où p est impair : Dans ce cas, nous mettrons les éléments 2, 3 et 4 (en ordre de gauche à droite) dans les trous de la ligne 5. On se souvient qu'on a $[5, n-1] = 1$, donc L_5 est une permutation. Ensuite, nous mettrons les éléments 1, 4, 3 (toujours dans cet ordre) dans les trous de la ligne $p-1$. Puisque $[p-1, p+1] = 2$, L_{p-1} est une permutation. Enfin, les trous de la ligne p contiendront (en ordre) 4 et 2. Puisque $[p, p] = 3$ et $[p, p+1] = 1$, L_p est une permutation. Nous obtenons l'escalier de la figure 3.7.

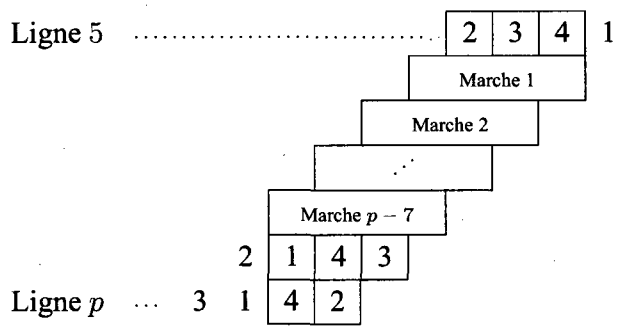

figure 3.7 – Généralisation de l'escalier pour p impair après la première étape

Pour les marches en tant que tel, nous allons placer les éléments 1, 4, 2 et 3 (en ordre) dans toutes les marches des lignes paires et les éléments 2, 3, 1 et 4 (en ordre) dans toutes les marches des lignes impaires. Donc, la première marche sera toujours (1, 4, 2, 3) et la dernière marche sera toujours (2, 3, 1, 4). On obtient l'escalier final de la figure 3.8.

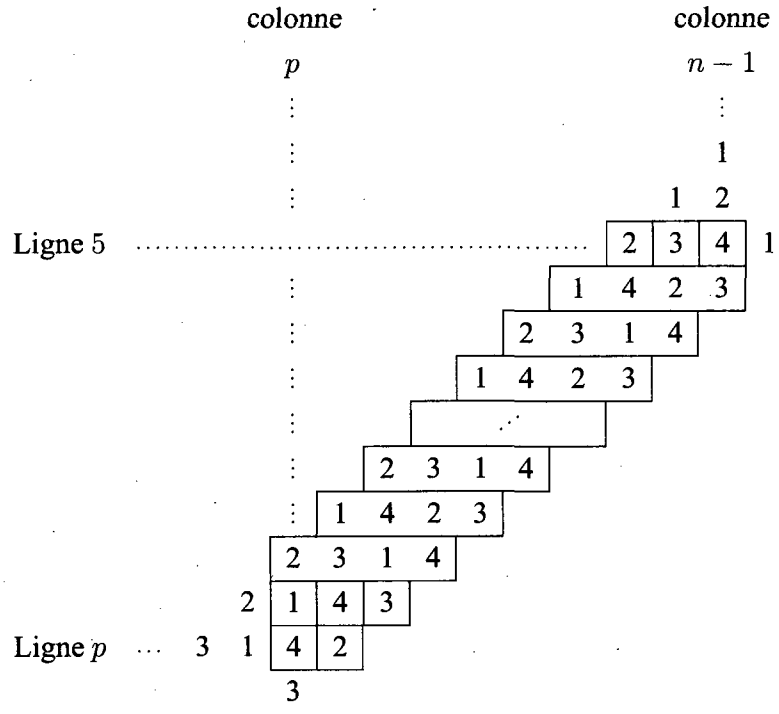

figure 3.8 – Généralisation de l'escalier pour p impair

Puisque pour $n = 13$ et $n = 17$, les marches des lignes 5 et $p - 1$ croisent des colonnes communes, nous traiterons ces cas particulier plus tard. Pour $n > 17$, on voit que les colonnes affectées par les lignes $p - 1$ et p sont les colonnes p, $p + 1$ et $p + 2$. Mais, ces colonnes seront toujours identiques à celles de la figure 3.8. Sur cette figure, on voit que R_p, R_{p+1} et R_{p+2} sont des permutations. La même méthode est utilisée pour montrer que les colonnes R_{n-1}, R_{n-2} et R_{n-3} qui croisent la ligne 5 sont également des permutations. Pour les colonnes $p + 2$ à $n - 4$, la figure 3.9 montre que l'alternance des marches (1, 4, 2, 3) et (2, 3, 1, 4) permet de toujours avoir une et une seule fois les éléments de 1 à 4 sur chaque ligne et sur chaque colonne.

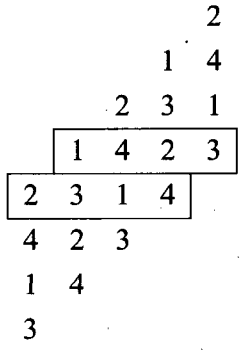

figure 3.9 – Alternance des marches pour p impair

En ce qui concerne les cas particuliers des ordres $n = 13$ (a) et $n = 17$ (b), la construction nous donne les résultats présentés dans la figure 3.10. On vérifie que chaque ligne et chaque colonne ne contient qu'une et une seule fois chaque élément de 1 à 4.

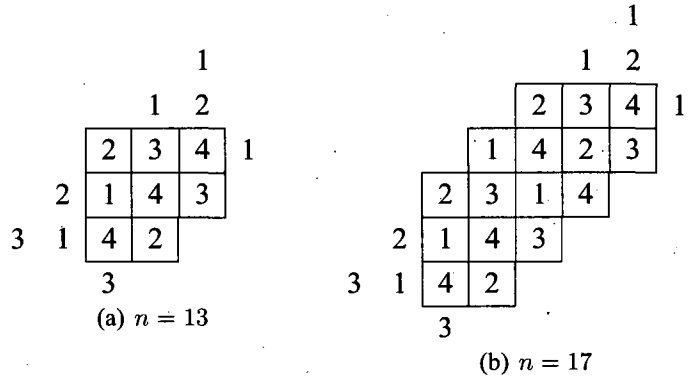

figure 3.10 – Cas particulier pour escalier avec $n = 13$ et $n = 17$

Ainsi, on a montré que la table de Cayley est un carré latin ; on a donc une boucle.

Cas où p est pair : La construction pour p pair est très similaire. La figure 3.11 présente les éléments à placer sur les lignes 5, p et $p - 1$. On voit que dans ces trois lignes, les éléments de 1 à 4 n'interviennent qu'une seule fois.

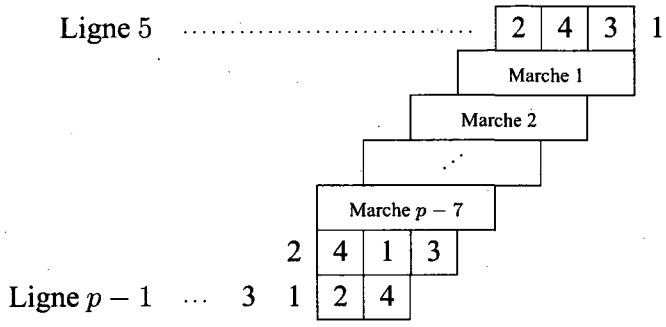

figure 3.11 – Généralisation de l'escalier pour p pair après la première étape

Les marches des lignes paires contiendront la suite (1, 3, 2, 4) et les marches des lignes impaires la suite (2, 4, 1, 3). La première et la dernière marche contiendront donc la suite (1, 3, 2, 4). La figure 3.12 représente l'escalier complété.

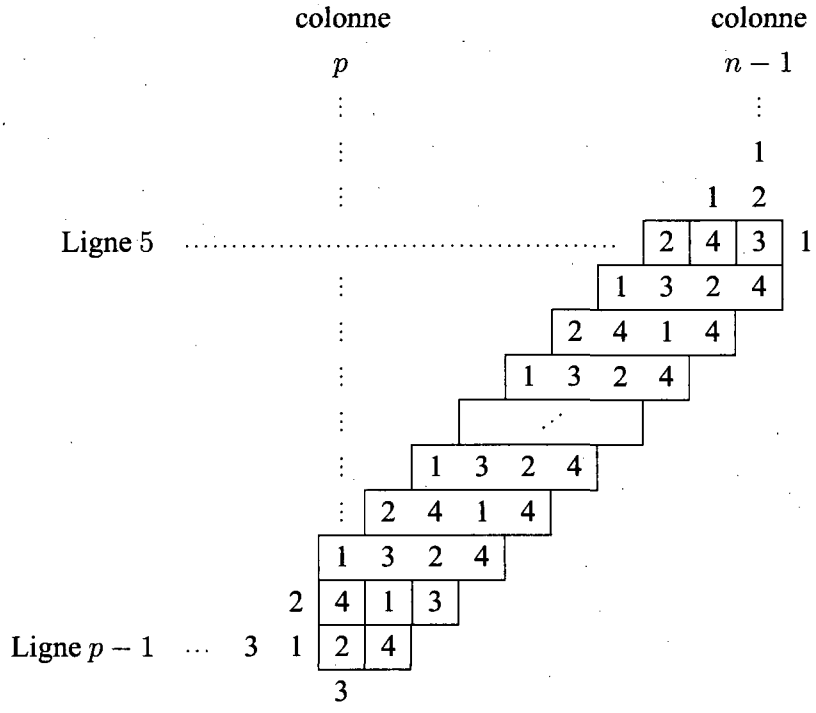

figure 3.12 – Généralisation de l'escalier pour p pair

De la même manière que dans le cas impair (sans exception puisque $n > 17$), la figure

3.12 permet de voir que les colonnes p, $p+1$, $p+2$, $n-3$, $n-2$ et $n-1$ forment des permutations. Pour les colonnes $p+3$ à $n-4$, la figure 3.13 montre que l'alternance des lignes paires et impaires fait en sorte que les éléments de 1 à 4 ne se retrouvent qu'une seule fois sur chaque ligne et colonne de l'escalier.

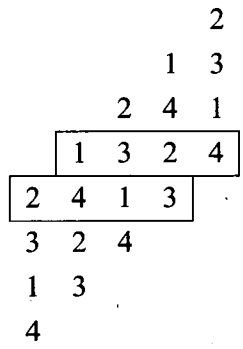

figure 3.13 – Alternance des marches pour p pair

Ainsi, nous obtenons nos boucles commutatives pour tout n premier avec $n \geq 13$.

Maintenant que notre construction est faite, montrons que la boucle résultante est incassable.

Proposition 3.2.2 Pour tout n premier tel que $n \geq 13$, la boucle construite par la construction 3.2.1 est incassable.

Preuve : Soit B la boucle d'ordre n premier construite avec la construction 3.2.1. Dans cette preuve, lorsqu'un élément $a \in B$ engendre tous les éléments de la boucle, nous noterons $\langle a \rangle = B$. En premier lieu, on a $1 \star 1 = 2, 1 \star 2 = 3, 1 \star 3 = 4, \cdots, 1 \star n-1 = 0$. Donc, on a $\langle 1 \rangle = B$. Également, puisque $2 \star 2 = 1$, on a $\langle 2 \rangle = B$.
Maintenant, effectuons une récurrence sur i : on suppose que pour un $i \in B \backslash \{0\}$, on a $\langle j \rangle = B$ pour tout $j < i$.
Prenons i de 3 à $p-1$. On obtient la suite d'opérations : $i \star i = 2i$, $i \star 2i = 3i$, $\cdots$, $i \star xi = (x+1)i$. Cette suite d'opérations correspond à des bonds de taille i sur la ligne L_i. La suite d'opérations dure jusqu'à ce que $xi \leq n - i$ et que $(x+1)i > n - i$ (le bond passe par dessus le 0). Il est à noter que, puisque n est premier, il est impossible que $xi = n - i$. Ainsi, si on prend $i \star (x+1)i = j$, on voit que $j < i$ (puisque tous les

éléments à gauche du 0 sont inférieurs à i). Par hypothèse, $\langle i \rangle = B$.
Prenons maintenant i de p à $n-1$. On voit que $i \star i = j$ avec un $j < i$. Par hypothèse, $\langle i \rangle = B$.
Ainsi, on en conclut que B est incassable. ■

Enfin, il nous reste à montrer que le groupe de multiplication de la boucle incassable commutative est le groupe symétrique. Pour faire cette preuve, nous allons avoir besoin de la proposition suivante.

Proposition 3.2.3 Quel que soit le nombre premier $n > 1$, la permutation $a_0, a_1, \cdots, a_n - 1$ des nombres $0, 1, \cdots, n-1$ et les deux entiers distincts a et b compris entre 0 et $n-1$, les deux permutations sous forme de cycles $S = (a_1 \ a_2 \ \cdots \ a_{n-1})$ et $T = (a \ b)$ constituent une base du groupe symétrique.

Preuve : Voir corollaire 4 de [17]. ■

Théorème 3.2.4 Pour tout n premier tel que $n \geq 13$, il existe une boucle incassable commutative d'ordre n dont le groupe de multiplication est le groupe symétrique.

Preuve : Soit B la boucle d'ordre n premier construite avec la construction 3.2.1. Prenons les deux permutations L_1 et L_2.

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-2 & n-1 \\ 1 & 2 & 3 & \cdots & n-1 & 0 \end{pmatrix} = (0 \ 1 \ 2 \ 3 \ \cdots \ n-2 \ n-1)$$

$$L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & \cdots & n-4 & n-3 & n-2 & n-1 \\ 2 & 3 & 1 & 5 & 6 & \cdots & n-2 & n-1 & 0 & 4 \end{pmatrix}$$

Rappelons que le produit d'une permutation de la forme $(0 \ 1 \ 2 \ 3 \ \cdots \ n-2 \ n-1)$ avec une autre permutation a l'effet d'une rotation circulaire à gauche des éléments dans cette autre permutation. Donc, l'opération suivante permet d'obtenir une transposition :

$$L_1^{n-2}L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \cdots & n-2 & n-1 \\ 0 & 4 & 2 & 3 & 1 & 5 & 6 & \cdots & n-2 & n-1 \end{pmatrix} = (1\ 4)$$

Ainsi, nous avons une permutation de la forme $(0\ 1\ 2\ 3\ \cdot\ n-2\ n-1)$ et une transposition $(1\ 4)$. Puisque n est premier, la proposition 3.2.3 permet de dire que la permutation L_1 et la transposition $L_1^{n-2}L_2$ engendrent le groupe symétrique. ■

Chapitre 4

Famille de boucles incassables commutatives d'ordre impair dont le groupe de multiplication est le groupe symétrique

Dans le chapitre précédent, nous avons décrit une famille infinie de boucles incassables commutatives dont le groupe de multiplication est le groupe symétrique. Par contre, cette construction ne fonctionne que pour les ordres premiers. Le but maintenant est de trouver une famille infinie dont la construction fonctionne pour tous les ordres impairs.

4.1 Résultat expérimental

Pour réussir à construire notre famille infinie, nous devons avoir des exemples de petite taille permettant de nous orienter. Également, pour avoir des exemples valables, nous utiliserons des boucles qui ne sont pas d'ordre premier. Ensuite, l'ordre des boucles devra être supérieur à 9 puisque, comme nous l'avons remarqué dans le chapitre précédent, les boucles d'ordre 7 sont difficilement généralisables. Enfin, le groupe de multiplication des boucles produites devra être le groupe alterné. En effet, nous savons qu'il est très facile de faire de légères modifications à la boucle afin d'obtenir le groupe symétrique. Donc, les

exemples construits de la sorte pourront servir autant pour le groupe symétrique que pour le groupe alterné.

Pour contruire nos exemples, nous avons encore utilisé l'algorithme 9 pour la complétion de quasigroupe troué ainsi que les algorithmes 2, 6 et 5. Lors de la construction de la première famille, nous avons remarqué que la position des 0, fixée d'avance, empêchait les boucles d'ordre non premier d'être incassables. Pour la construction de nos nouvelles boucles, nous avons donc laissé les éléments 0 à des emplacements non spécifiés.

Après la construction de plusieurs exemples d'ordre 15, 21 et 25, nous avons construit le modèle illustré par la figure 4.1. Nous avons mis la diagonale en évidence.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	0	4	5	6	7	8	9	10	11	12	3	14	15	16	17	18	19	20	13
2	2	0	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	3
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	0
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10
12	12	3	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	5
15	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	1	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	1	2	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	13	3	0	?	?	?	6	7	8	9	10	11	12	5	14	15	16	17	18	19

figure 4.1 – Table de Cayley trouée pour modèle d'ordre 21

Ce modèle nous a semblé intéressant car il ressemble à celui du chapitre précédent. Grâce à ce modèle, nous avons réussi à construire des boucles incassables commutatives

dont le groupe de multiplication est le groupe alterné pour tout ordre n impair tel que $21 \leq n \leq 39$. De plus, le nombre de boucles semble augmenter lorsque l'ordre de la boucle augmente. Nous avons donc basé la construction de notre famille sur ce modèle.

4.2 Construction et preuve

La construction de cette famille de boucles ressemble beaucoup à celle de la famille précédente. Ainsi, certains détails déjà expliqués dans le chapitre précédent ne seront pas expliqués de nouveau. Tout au long de la construction, une boucle d'ordre 21 sera utilisée comme exemple.

Construction 4.2.1 Puisque la boucle doit être commutative, nous décrirons comment remplir les cellules $[i, j]$ pour $i \leq j$. Il est sous-entendu que $[i, j]$ aura le même contenu que $[j, i]$ pour tout i et j. Soit n, un nombre impair tel que $n \geq 21$ et posons p tel que $n = 2p + 1$.
En premier lieu, pour i et j tels que $0 \leq i \leq n-1$ et $0 \leq j \leq i$, prenons $[i, j] = i + j(mod\ n)$. Ensuite, pour i et j tels que $7 \leq i \leq n-1$ et $n-i+6 \leq j \leq n-1$, prenons $[i, j] = i + j(mod\ n)$. Ceci construit une portion de table de Cayley dont le contenu est identique à celui de la table de Z_n. La figure 4.2 représente cette portion de table.

On effectue les modifications suivantes : $[1, 2] = 0$, $[1, p+2] = 3$ et $[1, n-1] = p+3$. Puisque l'ancienne valeur de $[1, 2]$ était de 3, celle de $[1, p+2]$ était de $p+3$ et que seul 0 pouvait être dans $[1, n-1]$, on en déduit que L_1* est toujours une permutation. Par contre, R_{n-1} ne peut plus être une permutation puisque l'élément $p+3$ s'y trouve deux fois. Prenons donc $[p+4, n-1] = 5$. Maintenant, puisque $[2, 1] = 0$, il ne manque que les éléments 1 et 3 sur la ligne 2 pour que L_2 soit une permutation. Prenons dont $[2, n-2] = 1$ et $[2, n-1] = 3$. Sur la ligne 3, il manque les élément 0, 1 et 2 pour que L_3 soit une permutation. Prenons donc $[3, n-3] = 1$, $[3, n-2] = 2$ et $[3, n-1] = 0$. Nous obtenons alors le modèle de la figure 4.3. Les positions concernées sont mises en caractères gras.

Les cases restantes doivent contenir des éléments de 0 à 5, sauf $[p+2, p+4]$ qui

*Rappel : L_k est l'action à gauche de k et est spécifiée par la ligne k de la table. Similairement, R_k est l'action à droite de k et est spécifiée par la colonne k de la table.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10
12	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13
15	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17	18	19

figure 4.2 – Table de Cayley - Portion Z_n

doit contenir $p + 3$. Ces cases ne seront pas remplies explicitement. Nous allons simplement montrer qu'il est possible d'assigner des valeurs à chacune des cases pour obtenir une boucle commutative. Pour ce faire, nous allons commencer par construire un triangle de départ de la ligne (resp. colonne) $p + 1$ à la ligne (resp. colonne) $p + 5$. Les positions de ce triangle sont identifiées par des astérisques $(*)$ dans la figure 4.3.

Pour plus de lisibilité, nous ne travaillerons qu'avec les triangles à partir de maintenant. La figure 4.4 représente un tel triangle.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	**0**	4	5	6	7	8	9	10	11	12	**3**	14	15	16	17	18	19	20	**13**
2	2	**0**	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	**1**	**3**
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	**1**	**2**	**0**
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	?	*	*	*	*	*	6	7	8	9	10
12	12	**3**	14	15	16	17	18	19	20	?	?	*	*	*	*	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	?	?	?	*	*	*	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	?	?	?	?	*	*	6	7	8	9	10	11	12	**5**
15	15	16	17	18	19	20	?	?	?	?	?	*	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	**1**	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	**1**	**2**	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	**13**	**3**	**0**	?	?	?	6	7	8	9	10	11	12	**5**	14	15	16	17	18	19

figure 4.3 – Table de Cayley - Triangle

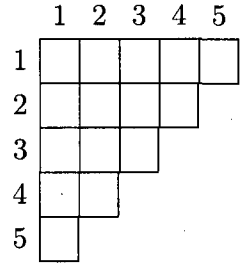

figure 4.4 – Triangle type

Il est clair que les positions $[p+2, p+4]$ et $[p+4, p+2]$ devront contenir la valeur $p+3$. Mais, il est à noter que puisque $[p+4, n-1] = 5$ et que $[1, p+2] = 3$, nous traiterons par la suite le triangle comme s'il y avait la valeur 5 sur la ligne $p+4$ et la valeur 3 sur la colonne $p+2$. Nous raisonnerons donc comme si les cellules $[p+2, p+4]$ et $[p+4, p+2]$ contenaient une valeur différente si vues par une ligne ou par une colonne. La figure 4.5 montre ce triangle de base.

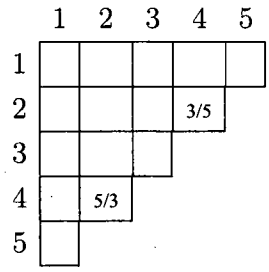

figure 4.5 – Triangle de base

Le triangle de départ qui sera utilisé a été choisi après avoir observé les résultats des exemples que nous avons produits avec la technique de la section précédente. Ce triangle de départ est présenté à la figure 4.6. Les cases notées $*$ contiennent la valeur $p+3$.

	1	2	3	4	5
1	3	0	5	4	2
2	0	5	4	$*$	
3	5	4	1		
4	4	$*$			
5	2				

figure 4.6 – Triangle de départ

Posons S_i le contenu de la colonne i du triangle avec $S_i \subseteq \{1,..,5\}$. Également, posons ρ_j pour $j \in \{0,\cdots,5\}$ le nombre d'occurrences de j dans le triangle. En considérant qu'un des symboles $*$ vaut 3 et que l'autre vaut 5, dans notre triangle on a $\rho_0 = \rho_2 = \rho_3 = 2$, $\rho_1 = 1$ et $\rho_4 = \rho_5 = 4$.

Remplissons maintenant la ligne située directement au dessus du triangle (ligne p du carré latin). Posons P_i avec $1 \leq i \leq 6$ de manière à ce que pour $i \in \{1,..,5\}$, P_i soit la case au dessus de S_i ; P_6 est une nouvelle case complètement à droite. On voit que la valeur $p+3$ des cases notées $*$ n'a aucun impact sur la création de la nouvelle ligne. Par contre, les valeurs des cellules $[1,p+2] = 3$ et $[n-1,p+4] = 5$ empêchent P_2 d'avoir 3 et

P_4 d'avoir 5. Nous allons donc représenter notre triangle de départ comme illustré dans la figure 4.7 ($3 \in S_2$ et $5 \in S_4$).

P_1	P_2	P_3	P_4	P_5	P_6
3	0	5	4	2	
0	5	4	5*		
5	4	1			
4	3*				
2					

figure 4.7 – Triangle de départ - vue par colonne

Pour remplir la nouvelle ligne, on utilise la règle : $P_i \notin S_i \cup \{P_j | j < i\}$ pour $1 \leq i \leq 5$ et $P_i \notin \{P_j | j < i\}$ pour $i = 6$. Nous obtenons alors un nouveau triangle.

1	2	0	3	4	5
3	0	5	4	2	
0	5	4	5*		
5	4	1			
4	3*				
2					

figure 4.8 – Exemple - nouveau triangle

Formellement, les cellules de la nouvelle ligne doivent être remplies selon la règle : $P_i \notin S_i \cup \{P_j | j < i\}$ pour $1 \leq i \leq 6$.

On voit qu'il est toujours possible de compléter la ligne suivante puisque chaque cellule de la ligne a un maximum de cinq valeurs interdites sur six valeurs possibles. En effet, $|S_i| = 6 - i$ et $|\{P_j | j < i\}| = i - 1$ pour tout $1 \leq i \leq 6$. Donc $S_i \cup \{P_j | j < i\}$ a un maximum de $6 - i + i - 1 = 5$ éléments. De plus, on voit que tous les éléments de S_1 sont redistribués sur les cellules de la première ligne du nouveau triangle (P_i avec $2 \leq i \leq 6$),

ce qui signifie que le nombre d'occurrences de chaque élément dans le nouveau triangle est identique au nombre d'occurrences de cet élément dans le triangle précédent. Ainsi, dans tous les triangles construits par la suite, les contraintes $\rho_0 = \rho_2 = \rho_3 = 2$, $\rho_1 = 1$ et $\rho_4 = \rho_5 = 4$ seront toujours respectées.

On répète l'étape précédente jusqu'à ce que la ligne à remplir soit la ligne 8 de la table de Cayley. On obtient la configuration présentée à la figure 4.9.

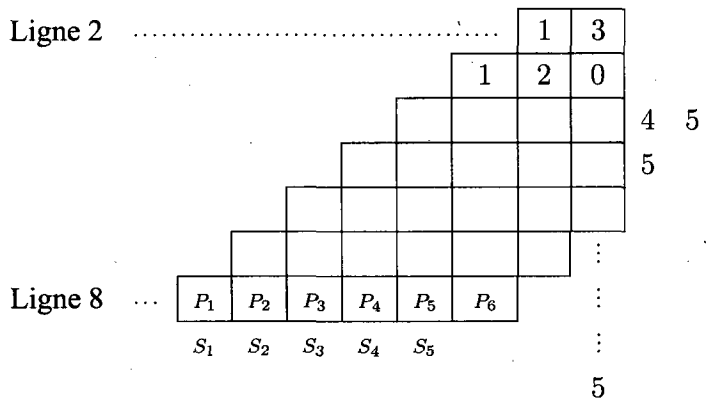

figure 4.9 – Extrémité du bandeau

On voit que, pour remplir la ligne 8, nous devons nous assurer de ne pas placer l'élément 1 dans P_6. Par la contrainte $\rho_1 = 1$, on sait qu'il n'y a qu'un seul élément 1 dans les S_i. Donc, si on a $1 \notin S_1$, alors on peut faire $P_1 = 1$. Si $1 \in S_1$, alors $1 \notin S_2 \cup \{P_1\}$ et donc on peut faire $P_2 = 1$. De cette manière, P_6 n'égalera jamais 1.

Maintenant, pour remplir la ligne 7, nous devons nous assurer de ne pas placer l'élément 1 dans P_5 ni dans P_6. Également, nous devons nous assurer de ne pas placer l'élément 2 dans P_6. Puisque S_1 contient cinq éléments sur les six éléments possibles, il est clair que S_1 contient au moins un des deux éléments 1 et 2. Si $1 \in S_1$, alors on fait $P_1 = 2$ et $P_2 = 1$ (possible puisque 1 n'est que dans S_1). Dans le cas où $2 \in S_1$, on place $P_1 = 1$. Ensuite, on sait qu'il y a deux éléments 2 dans les quatre S_i avec $2 \leq i \leq 5$. On place donc l'élément 2 dans le premier P_i tel que $2 \notin S_i$. Nous obtenons ainsi notre nouveau triangle.

Pour remplir les lignes 6, 5 et 4, nous avons utilisé l'algorithme 10 pour calculer tous les ensembles S_i possibles à ce niveau. L'algorithme a ressorti 125 ensembles S_i et, en enlevant les ensembles où $1 \in S_4$ ou $1 \in S_5$ ou encore $2 \in S_5$, nous avons obtenu 108 ensembles S_i. Ensuite, l'algorithme 11 nous a permis de produire toutes les complétions de bandeau possibles à partir de chacun des ensembles S_i. Pour chaque ensemble S_i, au minimum deux complétions pour les lignes 6, 5 et 4 sont possibles par triangle. Nous savons donc qu'il est toujours possible de terminer le carré latin. Ainsi, cette boucle commutative existe pour tout ordre n supérieur ou égal à 21.

Proposition 4.2.2 Pour tout n impair tel que $n \geq 21$, la boucle de la construction 4.2.1 est incassable.

Preuve : Soit B, une boucle commutative d'ordre impair n construite à l'aide de la technique de la construction 4.2.1. Posons également p tel que $n = 2p + 1$. Nous utiliserons la table de Cayley partielle après l'étape du triangle de base (voir figure 4.10).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	**0**	4	5	6	7	8	9	10	11	12	**3**	14	15	16	17	18	19	20	**13**
2	2	**0**	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	**1**	**3**
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	**1**	**2**	**0**
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	?	?	?	?	?	?	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	**1**	?	?	?	?	?	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	**1**	**3**	**0**	**5**	**4**	**2**	6	7	8	9	10
12	12	**3**	14	15	16	17	18	19	20	?	?	**0**	**5**	**4**	**13**	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	?	?	?	**5**	**4**	**1**	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	?	?	?	?	**4**	**13**	6	7	8	9	10	11	12	**5**
15	15	16	17	18	19	20	?	?	?	?	?	**2**	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	**1**	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	**1**	**2**	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	**13**	**3**	**0**	?	?	?	6	7	8	9	10	11	12	**5**	14	15	16	17	18	19

figure 4.10 – Table de Cayley - Incassable

En premier lieu, montrons que $\langle 2 \rangle = B$. Nous voyons que $[2, i] = i + 2$ pour $2 \leq i \leq n - 3$. Ainsi, nous pouvons obtenir tous les nombres pairs entre 2 et $n - 1$ à partir de 2. Ensuite, $[2, n - 1] = 3$. À partir de 3, nous pouvons obtenir tous les nombres impairs de 3 à $n - 2$. Pour obtenir 1 et 0, on voit que $[2, n - 2] = 1$ et que $[2, 1] = 0$. Nous avons obtenu tous les éléments de la boucle, on en déduit que $\langle 2 \rangle = B$. Également, puisque $[1, 1] = 2$, on a $\langle 1 \rangle = B$.

Montrons maintenant que $\langle n - 1 \rangle = B$. On voit que $[n - 1, i] = i - 1$ pour $p + 5 \leq i \leq n - 1$. Ainsi, à partir de $n - 1$, on peut obtenir 5. Ensuite, on voit que $[n - 1, 5]$ est une valeur manquante. Mais, nous voyons que la valeur doit être 1, 2 ou 4. Si $[n - 1, 5] = 1$ ou $[n-1, 5] = 2$, on obtient que $\langle n-1 \rangle = B$. Si $[n-1, 5] = 4$, on voit que $[n-1, 4] = 1$ ou $[n - 1, 4] = 2$, d'où on obtient que $\langle n - 1 \rangle = B$. Nous voyons également très facilement que $\langle p \rangle = B$ puisque $[p, p] = n - 1$.

Montrons maintenant que $\langle 3 \rangle = B$. On voit que $[3, i] = i + 3$ pour $3 \leq i \leq n - 4$. Ainsi, à partir de l'élément 3, il est possible d'obtenir tous les multiples de 3 entre 3 et $n - 1$. Si $n - 1$ est un multiple de 3, nous obtenons que $\langle 3 \rangle = B$ puisque $\langle n - 1 \rangle = B$. Puisque $[3, n - 2] = 2$ et $[3, n - 3] = 1$, alors si $n - 2$ ou $n - 3$ est un multiple de 3, on a $\langle 3 \rangle = B$.

Nous avons donc que $\langle 1 \rangle = B$, $\langle 2 \rangle = B$, $\langle 3 \rangle = B$, $\langle p \rangle = B$ et $\langle n - 1 \rangle = B$. Maintenant, montrons par induction que $\langle k \rangle = B$ pour tout $k \geq 4$. Posons comme hypothèse d'induction que pour tout i tel que $1 \leq i < k$ on a $\langle i \rangle = B$. Tout ce qui nous reste à montrer est que nous pouvons obtenir un élément non nul inférieur à k à partir de k. Séparons en deux cas :

Cas où $4 \leq k < p$: En premier lieu, remarquons que $[k, x] = x + k$ pour $k \leq x < n - k$. En d'autres mots, tous les $tk \leq n - 1$ peuvent être obtenus à partir de k. Également, les positions $[k, n - k]$, $[k, n - k + 1]$, $\cdots$, $[k, n - 1]$ forment une permutation des éléments $\{0, \cdots, k - 1\}$. Deux cas se présentent à nous : le cas où k est un diviseur de n et celui où k n'est pas un diviseur de n.

Si k est un diviseur de n, alors nous allons ajouter une contrainte à l'étape de remplissage du bandeau de la construction 4.2.1. En effet, lorsqu'une nouvelle ligne est construite, nous ne permettrons jamais à P_1 de contenir 0. De cette manière, $[k, n - k]$ ne sera jamais nul. Pour ce faire, nous devons nous assurer que S_1 contienne toujours 0. On sait que $\rho_0 = 2$. La méthode est simple, nous allons toujours placer l'élément

0 dans P_3. Il est toujours possible d'effectuer cette opération. En effet, puisque 0 est toujours contenu dans S_1 et S_2, lors du remplissage de P_1 et P_2, nous ne pouvons pas y placer de 0 et S_3 ne peut pas contenir de 0. Par contre, cette technique ne fonctionne que pour les lignes supérieures à 6. Donc, le cas $k = 5$ sera traité à part (4 et 6 ne peuvent être diviseur de n puisque n est impair). Pour $k > 6$, puisque k divise n, k divise aussi $n - k$. D'où, il existe un entier t tel que $tk = n - k$. Ainsi, tk est obtenu à partir de k et $[k, tk] < k$ est non nul. Donc $\langle k \rangle = B$. Si 5 est un diviseur de n, on sait qu'il existe un t tel que $n = 5t$. Si on pose $t = 2s + 1$, on obtient $n = 10s + 5$. Sachant que $n = 2p + 1$, on obtient que $2p + 1 = 10s + 5$ ou $p = 5s + 2$. De là, on voit que $p + 3 = 5s + 5$ ou $p + 3 = 5(s + 1)$. D'où on déduit que $p + 3 \in \langle 5 \rangle$. Puisque $[p + 3, p + 3] = 1$ et que $\langle 1 \rangle = B$, on en arrive à $\langle 5 \rangle = B$.
Dans le cas où k n'est pas un diviseur de n, on prend t tel que $n - k + 1 \leq tk \leq n - 1$ ($tk = n - k$ est impossible). Si $[k, tk] \neq 0$ alors $\langle k \rangle = B$ puisque $[k, tk] < k$. Si $[k, tk] = 0$, on prend un s tel que $p < sk < n-1$. On a que $[sk, sk] = r = sk + sk (\text{mod } n)$. On voit que r n'est pas un multiple de k puisque k n'est pas un diviseur de n. Donc si $n - k \leq r \leq n - 1$, on prend $[k, r]$ qui est non nul et inférieur à k. Si $r < n - k$, on prend $[k, r] = r + k$, $[k, r + k] = r + 2k, \cdots$, jusqu'à ce que $r + ik$ soit supérieur à $n - k$. Ensuite, on prend $[k, r + ik]$ qui est inférieur à k et non nul (puisque $[k, tk] = 0$ et $tk \neq r + ik$). D'où, par hypothèse d'induction, on obtient que $\langle k \rangle = B$.
Cas où $p < k < n - 1$ **:** Pour ces cas, nous voyons que $[k, k] = i$ avec $1 \leq i < k$. Donc, par hypothèse d'induction, on a $\langle k \rangle = B$. ■

Maintenant que nous avons une boucle incassable commutative pour tout ordre impair, montrons que cette boucle peut avoir le groupe symétrique comme groupe de multiplication. Pour ce faire, nous allons utiliser les définitions et propositions suivantes.

Définition 4.2.1 Soit $n > 1$, un entier et a, b deux nombres distincts de la suite $0, 1, \cdots n - 1$. On note $\overline{ab}$ la distance entre a et b calculée avec l'équation $a + \overline{ab} \equiv b (\text{mod } n)$.

Proposition 4.2.3 Quels que soient le nombre impair $n \geq 4$ et les trois nombres distincts a, b, c de la suite $0, 1, 2, \cdots, n - 1$, une condition nécessaire et suffisante pour que les deux permutations en représentation canonique $S = (0\ 1\ \cdots\ n-1)$ et $T = (a\ b\ c)$ constituent une base du groupe alterné, c'est que $PGCD(\overline{ab}, \overline{ac}, n) = 1$, où $PGCD(x, y, z)$ est le plus

grand commun diviseur de x, y et z.

Preuve : voir la proposition 5 de [16]. ■

Proposition 4.2.4 Pour tout n impair tel que $n \geq 21$, il existe une boucle incassable commutative B d'ordre n tel que $\mathcal{A}(n)$ est un sous-groupe du groupe de multiplication de B.

Preuve : Posons donc B une boucle construite à l'aide de la construction 4.2.1 et de la proposition 4.2.2. Pour cette preuve, nous utiliserons les permutations L_2 et L_3. Le but est d'obtenir une permutation contenant un seul cycle de trois éléments à partir de ces deux permutations afin d'utiliser la proposition 4.2.3. Les permutations sont présentées par la figure 4.11.

$$L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & \cdots & n-4 & n-3 & n-2 & n-1 \\ 2 & 0 & 4 & 5 & 6 & \cdots & n-2 & n-1 & 1 & 3 \end{pmatrix}$$
$$L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & \cdots & n-5 & n-4 & n-3 & n-2 & n-1 \\ 3 & 4 & 5 & 6 & \cdots & n-2 & n-1 & 1 & 2 & 0 \end{pmatrix}$$

figure 4.11 – Permutations L_2 et L_3

Si on analyse ces permutations on voit que pour L_2, l'image de x est $x+2$ sauf pour $x \in \{1, n-2, n-1\}$. Également, pour L_3 on voit que l'image de x est $x+3$ sauf pour $x \in \{n-3, n-2, n-1\}$. Donc si on prend les permutations $\alpha = L_2 * L_3$ et $\beta = L_3 * L_2$, on obtient les permutations de la figure 4.12.

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & \cdots & n-7 & n-6 & n-5 & n-4 & n-3 & n-2 & n-1 \\ 5 & 3 & 7 & 8 & 9 & \cdots & n-2 & n-1 & 1 & 2 & 0 & 4 & 6 \end{pmatrix}$$
$$\beta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & \cdots & n-7 & n-6 & n-5 & n-4 & n-3 & n-2 & n-1 \\ 5 & 6 & 7 & 8 & 9 & \cdots & n-2 & n-1 & 1 & 3 & 0 & 4 & 2 \end{pmatrix}$$

figure 4.12 – Permutations α et β

On voit que les permutations α et β se comportent très similairement. En effet, l'image de x est $x+5$ sauf pour $x \in \{1, n-5, n-4, n-3, n-2, n-1\}$. Ce qui est intéressant de voir est que α et β diffèrent seulement sur les éléments 2, 3 et 6. Donc, dans la

permutation $\gamma = \alpha^{-1} * \beta$, β annulera l'effet de α^{-1} pour tous les éléments sauf 2, 3 et 6. La permutation $\gamma = \alpha^{-1} * \beta = (L_2 * L_3)^{-1} * L_3 * L_2$ ainsi que son calcul sont présentés à la figure 4.13. La première ligne de cette figure correspond aux éléments de la boucle, la seconde ligne correspond à leur image par α^{-1}, la troisième ligne correspond à leur image par β et la dernière ligne correspond à leur image par γ. Par exemple, dans la première colonne, on a en ordre de ligne l'élément 0, $\alpha^{-1}(0) = n - 3$, $\beta(0) = 5$ et $\gamma(0) = 0$

$$\left(\begin{array}{cccccccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots & n-6 & n-5 & n-4 & n-3 & n-2 & n-1 \\
\hline\hline
n-3 & n-5 & n-4 & 1 & n-2 & 0 & n-1 & 2 & 3 & \cdots & n-11 & n-10 & n-9 & n-8 & n-7 & n-6 \\
* & & & & & & & & & & & & & & & \\
5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & \cdots & n-1 & 1 & 3 & 0 & 4 & 2 \\
\hline
0 & 1 & 3 & 6 & 4 & 5 & 2 & 7 & 8 & \cdots & n-6 & n-5 & n-4 & n-3 & n-2 & n-1
\end{array}\right)$$

figure 4.13 – Calcul de $\gamma = (L_2 * L_3)^{-1} * L_3 * L_2$

Nous vérifions que dans la permutation γ, seul les éléments 2, 3 et 6 sont permutés. Dans la représentation canonique, on a : $\gamma = (2\ 3\ 6)$.
Pour utiliser la proposition 4.2.3, nous devons aussi avoir une permutation dont la représentation canonique est $(0\ \ 1\ \ 2\ \ \cdots\ \ n-1)$. Nous allons pour cela utiliser un isomorphisme. Cet isomorphisme est un simple renommage des éléments qui permettra à la permutation L_2 d'avoir la forme requise. Puisque les groupes de multiplication de deux boucles isomorphes sont également isomorphes (voir 1.2.2), le résultat obtenu avec l'isomorphisme s'applique également dans notre boucle B. Donc la permutation L_2 sous forme de cycle est présentée à la figure 4.14.

$$L_2 = (0\ 2\ \cdots\ n-3\ n-1\ 3\ 5\ \cdots\ n-4\ n-2\ 1)$$

figure 4.14 – Permutation L_2

Si on renomme chacun des éléments de L_2 pour obtenir la permutation $\hat{L_2} = (0\ 1\ \cdots\ n-1)$, on obtient l'isomorphisme (le renommage) présenté par le tableau 4.1. La colonne *éléments utilisés i* montre que tous les éléments ne sont utilisés qu'une seul fois.

Éléments	Isomorphisme	Éléments utilisés i
0	0	0
1	$n-1$	$n-1$
Éléments pairs x	$\frac{x}{2}$	$1 \leq i \leq p$
Éléments impairs x ($x \neq 1$)	$\frac{x-1}{2}+p$	$p+1 \leq i \leq n-2$

tableau 4.1 – Isomorphisme

Maintenant, si nous utilisons l'isomorphisme sur la permutation $\gamma = (2\ \ 3\ \ 6)$, nous obtenons la permutation $\hat{\gamma} = (1\ \ p+1\ \ 3)$.
Avec nos permutations $\hat{L}_2 = (0\ \ 1\ \ \cdots\ \ n-1)$ et $\hat{\gamma} = (1\ \ p+1\ \ 3)$, nous pouvons utiliser la proposition 4.2.3. Ainsi, posons $a = 1$, $b = p+1$ et $c = 3$. Puisque n est impair et que $\overline{ac} = 2$, on en déduit que $PGCD(\overline{ab}, \overline{ac}, n) = 1$. Donc, la proposition 4.2.3 permet d'affirmer que $\hat{L}_2 = (0\ \ 1\ \ \cdots\ \ n-1)$ et $\hat{\gamma} = (1\ \ p+1\ \ 3)$ sont des bases du groupe alterné.
Ainsi, on en conclut que le groupe alterné $\mathcal{A}(n)$ est un sous-groupe du groupe de multiplication de B. ■

Pour en arriver à notre théorème principal, il nous faut une dernière proposition.

Proposition 4.2.5 Si P est une permutation impaire d'ordre n, alors $\langle \mathcal{A}(n) \cup \{P\} \rangle = \mathcal{S}(n)$.

Preuve : Soit $H = \langle \mathcal{A}(n) \cup \{P\} \rangle$. Il est clair que H est un sous-groupe de $\mathcal{S}(n)$. On sait que $|\mathcal{S}(n)| = n!$ et que $|\mathcal{A}(n)| = \frac{n!}{2}$. Il est clair que le plus petit diviseur de $n!$ qui est supérieur à $\frac{n!}{2}$ est $n!$. Par le théorème de Lagrange (voir proposition 1.1.11), on en déduit que $|\langle \mathcal{A}(n) \cup \{P\} \rangle| = n!$ et donc que $\langle \mathcal{A}(n) \cup \{P\} \rangle = \mathcal{S}(n)$. ■

Nous pouvons maintenant énoncer notre théorème principal.

Théorème 4.2.6 Pour tout n impair tel que $n \geq 21$, il existe une boucle incassable commutative d'ordre n dont le groupe de multiplication est le groupe symétrique.

Preuve : Posons donc B une boucle construite à l'aide de la construction 4.2.1 et de la proposition 4.2.2. Avec la proposition 4.2.4, on sait que le groupe alterné est un sous-groupe du groupe de multiplication de B. Donc, par la proposition 4.2.5 si on montre que nous pouvons avoir une permutation impaire parmis les L_i, on montre que le groupe

de multiplication de B est le groupe symétrique. Prenons $L_{p,1}$ comme étant L_p avec les P_i contenant les valeurs $1, 2, 0, 3, 4, 5$ et $L_{p,2}$ comme étant L_p avec les P_i contenant les valeurs $1, 2, 0, 3, 5, 4$. On voit qu'autant $L_{p,1}$ que $L_{p,2}$ sont des permutations. Mais, puisque $L_{p,1} = L_{p,2} \cdot (4\ \ 5)$, on voit que leurs parités sont inversées. Donc une des permutations $L_{p,1}$ ou $L_{p,2}$ est impaire. ■

Entrée : S : Liste des ensembles S_i (initialement, tous les S_i sont vides)
i : Le i du S_i en traitement dans cette itération (initialement à 1).
ρ : Liste contenant les contraintes (initialement, $\rho[0] = 2, \rho[1] = 1, \rho[2] = 2, \rho[3] = 2, \rho[4] = 4$ et $\rho[5] = 4$).
$total$: Ensemble contenant toutes les listes S_i calculées jusqu'à maintenant (initialement vide).
Sortie : Ensemble contenant toutes les listes S_i

```
CALCUL_ENSEMBLES_S(S,i,ρ,total) début
    si i > 5 alors
        Ajouter S dans total
    sinon
        si |S_i| = 6 − i alors
            total =CALCUL_ENSEMBLES_S(S,i + 1,ρ,total)
        sinon
            pour j de max(S_i) à 5 faire
                si ρ[j] > 0 alors
                    Ajouter j dans S_i
                    ρ[j] = ρ[j] − 1
                    total =CALCUL_ENSEMBLES_S(S,i,ρ,total)
                    Enlever j de S_i
                    ρ[j] = ρ[j] + 1
                fin si
            fin pour
        fin si
    fin si
    retourne total
fin
```

Algorithme 10 : Construit tous les ensembles S_i possibles

Entrée : S : Un ensemble S_i (On ajoute un S_6 aux ensembles et on ajoute les valeurs : $1 \in S_4$, $1, 2 \in S_5$ et $0, 3, 5 \in S_6$)
T : Ensemble T_j similaire à S_i mais pour les lignes (initialement : $4, 5 \in T_1$ et $5 \in T_2$)
i : Le i du S_i représente la colonne du bandeau à construire. (initialement 1)
j : Le j du T_j représente la ligne du bandeau à construire. (initialement 1)
bandeau : Tableau de trois lignes et six colonnes représentant le reste du bandeau (cellules $[1, 1]$, $[1, 2]$, $[2, 1]$ jamais utilisées)
total : Ensemble contenant tous les bandeaux finaux calculés jusqu'à maintenant (initialement vide).
Sortie : Tous les bandeaux (lignes 4, 5 et 6) possibles.

```
FINALISER_BANDEAU(S,T,i,j,bandeau,total) début
    si [i, j] ∈ {[1, 1], [1, 2], [2, 1]} alors
        total :=FINALISER_BANDEAU(S,T,i + 1,j,bandeau,total)
    sinon
        si i > 6 alors
            si j = 3 alors
                Ajouter bandeau à total
            sinon
                total :=FINALISER_BANDEAU(S,T,1,j + 1,bandeau,total)
            fin si
        sinon
            pour k de 0 à 5 faire
                si k ∉ S_i et k ∉ L_i alors
                    bandeau[j, i] := k
                    Ajouter k dans S_i et dans T_j
                    total :=FINALISER_BANDEAU(S,T,i + 1,j,bandeau,total)
                    Enlever k de S_i et de T_j
                fin si
            fin pour
        fin si
    fin si
    retourne total
fin
```

Algorithme 11 : Construit tous les bandeaux possibles à partir d'ensembles S_i

Chapitre 5

Famille de boucles incassables commutatives d'ordre impair dont le groupe de multiplication est le groupe alterné

La famille de boucles qui sera présentée dans ce chapitre est basée sur les exemples et la construction du chapitre précédent. En effet, tous les exemples de boucles que nous avons créés ont comme groupe de multiplication le groupe alterné. Pour avoir le groupe symétrique, nous avons montré que nous pouvions avoir une permutation impaire dans $\mathcal{M}(B)$ (voir la preuve du théorème 4.2.6). Maintenant, nous allons montrer qu'il y a moyen de n'avoir que des permutations paires. Cette construction fonctionne pour des boucles d'ordre impair supérieur ou égal à 43. Des boucles d'ordre inférieur à 43 seront présentées dans la seconde section du chapitre.

5.1 Construction et preuve

Pour construire cette famille de boucles, nous allons nous baser sur la méthode vue au chapitre précédent. Nous utiliserons une boucle d'ordre 43 pour illustrer la construction. Dans cette section, nous ne montrerons que la partie supérieure droite de la table de Cayley,

soit les lignes 0 à $p+5$ (ligne 26) et les colonnes $p+1$ (colonne 22) à $n-1$ (colonne 42). Puisque les parties supérieure gauche et inférieure droite sont déjà entièrement spécifiées et que la partie inférieure droite est construite par commutativité à partir de la partie supérieure droite, on voit que cette dernière est entièrement suffisante pour décrire la boucle.

Construction 5.1.1 Le début de cette construction est identique au début de la construction 4.2.1 du chapitre précédent. Nous débuterons donc lors du remplissage du bandeau, juste après avoir placé le triangle de départ. Nous avons donc une boucle incomplète similaire à la boucle de la figure 4.10. Maintenant, nous allons remplir les deux lignes suivantes avec les valeurs (dans l'ordre) $1, 2, 0, 3, 4, 5$. Nous poursuivons en assignant les valeurs $[p-2, p+3] = 3$, $[p-2, p+4] = 1$, $[p-2, p+5] = 5$, $[p-3, p+4] = 2$, $[p-3, p+5] = 0$, $[p-4, p+5] = 1$. Maintenant que nous avons nos éléments de départ (milieu du bandeau), nous devons placer les éléments d'arrivée (extrémités du bandeau). Donc assignons (dans l'ordre) à la ligne 4 les valeurs $1, 0, 3, 2$, à la ligne 5 les valeurs $2, 0, 3, 4, 1$, à la ligne 6 les valeurs $3, 1, 5, 2, 0, 4$ et à la ligne 7 les valeurs $1, 2, 0, 3, 4, 5$. Enfin, assignons les valeurs $[8, n-4] = 4$, $[8, n-3] = 5$, et $[9, n-4] = 2$. Dans notre exemple, on obtient la boucle présentée par la figure 5.1. Les zones mises en évidence par des traits sont nommées *papillons de liaison*. Il est important de remarquer que les deux papillons sont identiques. Ces papillons de liaison nous serviront un peu plus loin.

Pour remplir le restant du bandeau (lignes 8 à $p-2$), nous utiliserons des sous-bandeaux. Un sous-bandeau correspond à une partie de bandeau qui commence (en bas à gauche du sous-bandeau) et termine (en haut à droite du sous-bandeau) par un papillon de liaison. Le papillon de liaison le plus en bas d'un sous-bandeau sera appelé *papillon de liaison initial* tandis que le papillon de liaison le plus en haut d'un sous-bandeau sera appelé *papillon de liaison final*. La taille d'un sous-bandeau correspond au nombre de lignes complètes (de six éléments) que le sous-bandeau contient, diminué de 1*. Les papillons de liaison initial et final permettent de concaténer deux sous-bandeaux afin d'en obtenir un troisième. Soit B_x un sous-bandeau de taille x et B_y un sous-bandeau de taille y, il nous suffit de faire chevaucher le papillon de liaison initial de B_y avec le papillon de liaison final de B_x ; on obtient un nouveau sous-bandeau de taille $x+y$ que nous appellerons B_{x+y}. Par exemple, si on concatène le sous-bandeau B_{10} de la figure 5.12 avec le sous-bandeau B_{13}

*Par exemple, le sous-bandeau de la figure 5.12 possède 11 lignes complètes. Donc sa taille est de 10.

	⋯	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
0	⋯	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
1	⋯	23	**3**	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**24**
2	⋯	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**1**	**3**
3	⋯	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**1**	**2**	**0**
4	⋯	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**1**	**0**	**3**	**2**
5	⋯	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**2**	**0**	**3**	**4**	**1**
6	⋯	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**3**	**1**	**5**	**2**	**0**	**4**
7	⋯	29	30	31	32	33	34	35	36	37	38	39	40	41	42	**1**	**2**	**0**	**3**	**4**	**5**	6
8	⋯	30	31	32	33	34	35	36	37	38	39	40	41	42	?	?	?	?	**4**	**5**	6	7
9	⋯	31	32	33	34	35	36	37	38	39	40	41	42	?	?	?	?	?	**2**	6	7	8
10	⋯	32	33	34	35	36	37	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9
11	⋯	33	34	35	36	37	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9	10
12	⋯	34	35	36	37	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9	10	11
13	⋯	35	36	37	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9	10	11	12
14	⋯	36	37	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9	10	11	12	13
15	⋯	37	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14
16	⋯	38	39	40	41	42	?	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15
17	⋯	39	40	41	42	**1**	?	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16
18	⋯	40	41	42	**2**	**0**	?	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17
19	⋯	41	42	**3**	**1**	**5**	?	?	?	6	7	8	9	10	11	12	13	14	15	16	17	18
20	⋯	42	**1**	**2**	**0**	**3**	**4**	**5**	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	⋯	**1**	**2**	**0**	**3**	**4**	**5**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	⋯	**3**	**0**	**5**	**4**	**2**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
23	⋯	**0**	**5**	**4**	**24**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
24	⋯	**5**	**4**	**1**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
25	⋯	**4**	**24**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	5
26	⋯	**2**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
⋮	⋱	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

figure 5.1 – Table de Cayley

de la figure 5.13, on obtient le sous-bandeau présenté par la figure 5.2. Il est à noter que B_{x+y} et B_{y+x} on la même taille, mais peuvent être différents.

Nous utiliserons les dix sous-bandeaux présentés par les figures 5.12 à 5.21 à la fin de la présente section. Dans ces figures, les chiffres en italiques représentent le nombre d'inversions dans chacune des lignes et des colonnes du sous-bandeau. Cette information nous sera utile plus tard. Maintenant, nous voyons que pour tout i de 0 à 9, il existe un B_x présenté par une des figures 5.12 à 5.21 tel que $i = x \pmod{10}$. Donc, si nous avons besoin d'un sous-bandeau de longueur k pour terminer la table de Cayley, nous prenons le x tel que $x = k \pmod{10}$ et nous concaténons B_x avec $k \div 10$ fois B_{10} pour obtenir le sous-bandeau de longueur k (avec $\div$ une division entière). On voit donc qu'on peut obtenir un sous-bandeau pour toute longueur supérieure ou égale à 13.

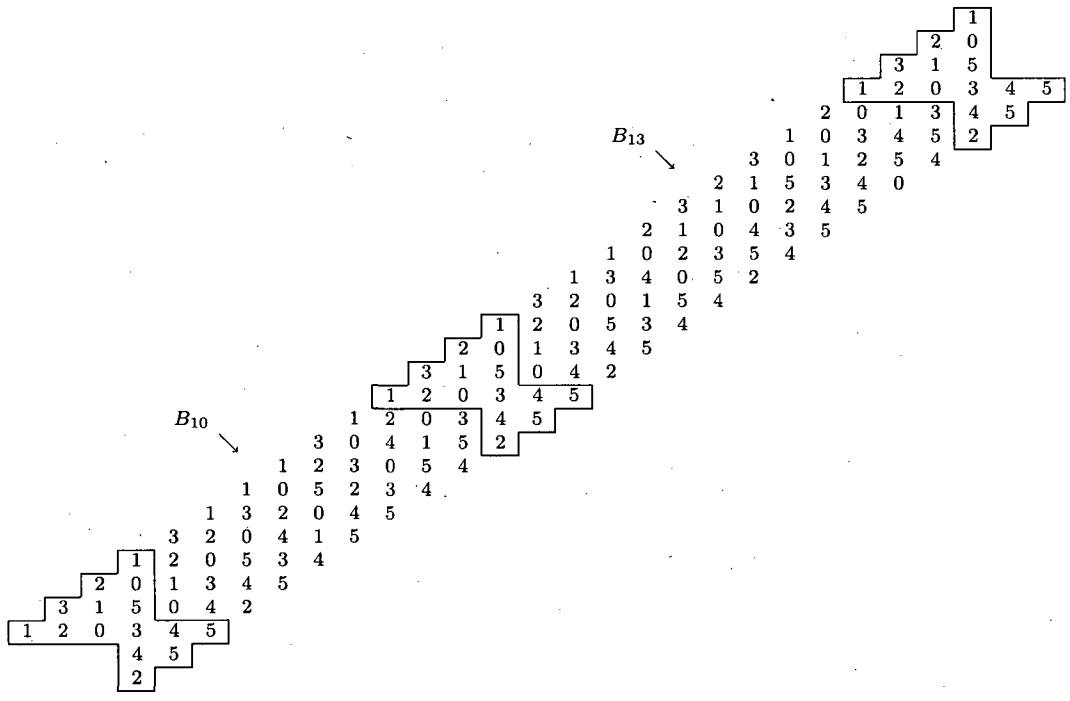

figure 5.2 – B_{10+13} : Sous-bandeau de taille 23 - Concaténation de B_{10} et B_{13}

Maintenant, nous allons calculer la taille de sous-bandeau nécessaire pour remplir une table de Cayley pour une boucle d'ordre n. Si on considère que le papillon de liaison de la table de Cayley des lignes $p-4$ à $p+1$ est en fait le papillon de liaison initial du sous-bandeau, nous voyons que nous devons remplir les lignes 8 à $p-1$ (inclusivement) à l'aide d'un sous-bandeau. Donc notre sous-bandeau devra être de taille $p-8$. Puisque les sous-bandeaux doivent être de taille supérieure ou égale à 13 et que $21-8=13$, on obtient que la plus petite boucle pouvant utiliser cette construction est d'ordre 43 ($n=2p+1$).

Proposition 5.1.2 Pour tout n impair tel que $n \geq 43$, une boucle résultante de la construction 5.1.1 est incassable.

Preuve : Puisque les constructions 4.2.1 et 5.1.1 sont identiques mise à part la manière de remplir le bandeau, la preuve de la proposition 4.2.2 s'applique. Nous devons tout simplement nous assurer que pour chaque ligne, le 0 ne soit pas sur la diagonale en

dessous des $n-1$. De fait, en regardant les sous-bandeaux des figures 5.12 à 5.21, on voit que les 0 ne sont jamais sur la diagonale problématique. De plus, les éléments fixés dans la table de Cayley n'ont pas non plus de 0 sur la diagonale en dessous des $n-1$. ■

Théorème 5.1.3 Pour tout n impair tel que $n \geq 43$, il existe une boucle incassable commutative B d'ordre n dont le groupe de multiplication de B est le groupe alterné $\mathcal{A}(n)$.

Preuve :
$\mathcal{A}(n) \subseteq \mathcal{M}(B)$: Puisque les permutations L_2 et L_3 n'ont pas changé entre la construction 4.2.1 et la construction 5.1.1, avec la preuve de la proposition 4.2.4, on peut déduire $\mathcal{A}(n) \subseteq \mathcal{M}(B)$.

$\mathcal{M}(B) \subseteq \mathcal{A}(n)$: Il suffit de montrer que $\mathcal{M}(B)$ ne contient que des permutations paires. Puisque le produit de deux permutations paires donne une toujours permutation paire, et que la boucle est commutative, on peut se contenter de montrer que tous les L_a de la boucle sont pairs. Pour ce faire, nous utiliserons la technique du nombre d'inversions vue dans l'exemple 1.2. Il faut montrer que le nombre d'inversions est pair.

Commençons par montrer que L_i est pair pour tout $i \in [6, n-2] \backslash \{p+2, p+4\}$. Tous ces L_i sont construits de la même manière. La figure 5.3 montre une permutation L_i.

$$L_i = \begin{pmatrix} 0 & 1 & \cdots & n-i-1 & n-i & n-i+1 & \cdots & n-i+5 & n-i+6 & n-i+7 & \cdots & n-1 \\ i & i+1 & \cdots & n-1 & ? & ? & \cdots & ? & 6 & 7 & \cdots & i-1 \end{pmatrix}$$

figure 5.3 – L_i pour $i \in [6, n-2] \backslash \{p+2, p+4\}$

Ce qu'il faut remarquer dans cette figure, c'est que les éléments des positions 0 à $n-i-1$ sont en ordre croissant ainsi que les éléments aux positions $n-i-6$ à $n-1$. Par contre, les éléments aux positions 0 à $n-i-1$ sont tous plus grand que les éléments aux positions $n-i$ à $n-1$. On en déduit que chaque élément des positions $n-i$ à $n-1$ fera une inversion pour chaque élément des positions 0 à $n-i-1$. Donc, si on considère que les

éléments manquants (les ?) sont toujours les éléments en ordre $0, 1, 2, 3, 4, 5$, on a que la permutation a $i(n-i)$ inversions. Puisque n est impair, on a que soit i ou $(n-i)$ est pair. Donc le nombre d'inversions pour une permutation L_i dans lequel nous n'avons pas mélangé les éléments de 0 à 5 est pair. Nous devons maintenant placer les éléments de 0 à 5 correctement en gardant toujours un nombre pair d'inversions. On voit que mélanger ces éléments n'a aucun impact sur le nombre d'inversions par rapport aux éléments des positions 0 à $n-i-1$ ou $n-i-6$ à $n-1$. Également, on a que tous les éléments des positions $n-i-6$ à $n-1$ sont supérieurs à 5. Donc, si la permutation des éléments 0 à 5 est paire, la permutation L_i restera paire.

Dans les sous-bandeaux des figures 5.12 à 5.21, nous avons mis en italiques le nombre d'inversions pour chaque ligne (pour la partie supérieure droite de la table de Cayley) et chaque colonne (pour la partie inférieure gauche de la table de Cayley) du sous-bandeau. Il est facile de voir que toutes ces lignes et colonnes ont un nombre pair d'inversions. Il reste les lignes 6, p, $p+1$ et $p+3$ qui ne sont pas formées par des sous-bandeaux (ou en partie seulement). Le tableau 5.1 montre ces lignes avec la permutation des éléments de 0 à 5 ainsi que le nombre d'inversions pour chacune de ces lignes.

Ligne	**Permutation**	**nombre d'inversions**
6	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 0 & 4 \end{pmatrix}$	8
p	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 3 & 4 & 5 \end{pmatrix}$	2
$p+1$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 0 & 5 & 4 & 1 \end{pmatrix}$	6
$p+3$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 0 & 5 & 4 & 1 \end{pmatrix}$	8

tableau 5.1 – Nombre d'inversions pour les lignes 6, p, $p+1$ et $p+3$

Nous nous intéressons maintenant aux permutations qui ne sont pas sous la forme présentée à la figure 5.3. Il s'agit des lignes 0 à 5, $p+2$, $p+4$ et $n-1$. La ligne 0 est

la permutation identité qui est toujours paire. Pour les autres permutations, nous allons présenter chacune d'entre elles avec son nombre d'inversions. Débutons par la permutation L_1 présentée par la figure 5.4.

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & \cdots & p+1 & p+2 & p+3 & \cdots & n-2 & n-1 \\ 1 & 2 & 0 & 4 & \cdots & p+2 & 3 & p+4 & \cdots & n-1 & p+3 \end{pmatrix}$$

figure 5.4 – L_1

Dans cette permutation, on peut voir que tous les éléments sont en ordre croissant sauf 0, 3 et $p+3$. On voit que les éléments 1 et 2 (deux éléments) feront chacun une inversion avec 0, les éléments 4 à $p+2$ ($p+1$ éléments) feront chacun une inversion avec 3 et les éléments $p+4$ à $n-1$ ($p-3$ éléments) feront chacun une inversion avec $p+3$. Nous obtenons donc $2+(p+1)+(p-3) = 2p$ inversions, ce qui est forcément pair. Passons maintenant à la permutation L_2 présentée par la figure 5.5.

$$L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & \cdots & n-4 & n-3 & n-2 & n-1 \\ 2 & 0 & 4 & 5 & \cdots & n-2 & n-1 & 1 & 3 \end{pmatrix}$$

figure 5.5 – L_2

Dans cette permutation, on a 2 (un élément) qui fera une inversion avec 0 et 1 et ensuite, toutes les valeurs de 4 à $n-1$ ($n-4$ éléments) feront une inversion avec 1 et 3. On a donc $2 \times 1 + 2(n-4) = 2(n-3)$ inversions, ce qui est pair. Ensuite, la permutation L_3 présentée par la figure 5.6.

$$L_3 = \begin{pmatrix} 0 & 1 & \cdots & n-5 & n-4 & n-3 & n-2 & n-1 \\ 3 & 4 & \cdots & n-2 & n-1 & 1 & 2 & 0 \end{pmatrix}$$

figure 5.6 – L_3

Dans cette permutation, tous les éléments de 3 à $n-1$ ($n-3$ éléments) feront une inversion avec 1, 2 et 0. Également, 1 et 2 (deux éléments) feront une inversion avec 0. On obtient donc $3(n-3)+2 = 3n+11$ inversions. Puisque n est impair, on obtient que

$3n$ est également impair et que $3n + 11$ est donc pair. Poursuivons avec la permutation L_4 qui est présentée par la figure 5.7.

$$L_4 = \begin{pmatrix} 0 & 1 & \cdots & n-6 & n-5 & n-4 & n-3 & n-2 & n-1 \\ 4 & 5 & \cdots & n-2 & n-1 & 1 & 0 & 3 & 2 \end{pmatrix}$$

figure 5.7 – L_4

Dans cette permutation, tous les éléments de 4 à $n-1$ ($n-4$ éléments) feront une inversion avec les quatre éléments de 0 à 3. Ensuite, l'élément 1 fera une inversion avec 0 et l'élément 3 fera une inversion avec 2. On a donc $4(n-4)+2$ inversions dans L_4, ce qui est forcément pair. Ensuite, la permutation L_5 présentée par la figure 5.8.

$$L_5 = \begin{pmatrix} 0 & 1 & \cdots & n-7 & n-6 & n-5 & n-4 & n-3 & n-2 & n-1 \\ 5 & 6 & \cdots & n-2 & n-1 & 2 & 0 & 3 & 4 & 1 \end{pmatrix}$$

figure 5.8 – L_5

Dans cette permutation, tous les éléments de 5 à $n-1$ ($n-5$ éléments) feront une inversion avec les cinq éléments de 0 à 4. Ensuite, l'élément 2 fera une inversion avec 0 et avec 1. De plus, les éléments 3 et 4 feront une inversion avec 1. On a donc $5(n-5)+4 = 5n-21$ inversions dans L_5. Puisque n est impair alors $5n$ l'est également, d'où on sait que $5n-21$ est pair.

Passons maintenant aux permutations L_{p+2}, L_{p+4} et L_{n-1}. La permutation L_{p+2} est présentée par la figure 5.9.

$$L_{p+2} = \begin{pmatrix} 0 & 1 & 2 & \cdots & p-2 & p-1 & p & p+1 & p+2 & p+3 & p+4 & p+5 & \cdots & n-1 \\ p+2 & 3 & p+4 & \cdots & n-1 & 1 & 2 & 0 & 5 & 4 & p+3 & 6 & \cdots & p+1 \end{pmatrix}$$

figure 5.9 – L_{p+2}

Dans cette permutation, $p+2$ fera une inversion avec tous les éléments de 0 à $p+1$ ($p+2$ éléments). Ensuite, l'élément 3 fera une inversion avec les éléments 0, 1, 2 (3

éléments). Ensuite, les éléments $p+3$ à $n-1$ ($p-2$ éléments) feront une inversion avec les éléments 0 à $p+1$ ainsi qu'avec $p+3$ ($p+3$ éléments). Les éléments 1 et 2 (deux éléments) feront une inversion avec l'élément 0 et l'élément 5 fera une inversion avec l'élément 4. Enfin, l'élément $p+3$ fera une inversion avec les éléments 6 à $p+1$ ($p-4$ éléments). On obtient donc $(p+2)+3+(p-2)(p+3)+3+(p-4) = p^2+3p-2$ inversions dans L_{p+2}. On voit que p^2 et $3p$ ont la même parité. Donc p^2+3p+2 est toujours pair. Ensuite, la permutation L_{p+4} est présentée par la figure 5.10.

$$L_{p+4} = \begin{pmatrix} 0 & \cdots & p-4 & p-3 & p-2 & p-1 & p & p+1 & p+2 & p+3 & \cdots & n-2 & n-1 \\ p+4 & \cdots & n-1 & 2 & 1 & 0 & 3 & 4 & p+3 & 6 & \cdots & p & 5 \end{pmatrix}$$

figure 5.10 – L_{p+4}

Dans cette permutation, les éléments $p+4$ à $n-1$ ($p-3$ éléments) feront une inversion avec les éléments 0 à $p+3$ ($p+4$ éléments). Ensuite, l'élément 2 fera une inversion avec les éléments 1 et 0. Également, l'élément 1 fera une inversion avec l'élément 0. L'élément $p+3$ fera une inversion avec les éléments 5 à p ($p-4$ éléments). Enfin, chacun des éléments 6 à p ($p-5$ éléments) feront une inversion avec l'élément 5. On obtient donc $(p-3)(p+4)+3+(p-4)+(p-5) = (p-3)(p+4)+2p-6$ inversions. Puisque $(p-3)$ ou bien $(p+4)$ est pair et que $2p-6$ est forcément pair, on obtient que la permutation est paire. Passons finalement à notre dernière permutation. Il s'agit de L_{n-1} et elle est présentée par la figure 5.11.

$$L_{n-1} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots & p+3 & p+4 & p+5 & \cdots & n-1 \\ n-1 & p+3 & 3 & 0 & 2 & 1 & 4 & 6 & 7 & \cdots & p+2 & 5 & p+4 & \cdots & n-2 \end{pmatrix}$$

figure 5.11 – L_{n-1}

Dans cette permutation, on a que $n-1$ fera une inversion avec les éléments 0 à $n-2$ ($n-1$ éléments). Ensuite, l'élément $p+3$ fera une inversion avec les éléments 0 à $p+2$ ($p+3$ éléments). L'élément 3 fera une inversion avec 0, 2 et 1. Également, l'élément 2 fera une inversion avec l'élément 1. Enfin, les éléments 6 à $p+2$ ($p-3$ éléments) feront une inversion avec l'élément 5. On a donc $(n-1)+(p+3)+4+(p-3) = 4p+4$

inversions, ce qui est forcément pair.

On a donc montré que toutes les permutations de la boucle sont paires. Donc, $\mathcal{M}(B) \subseteq \mathcal{A}(n)$. ■

Dans le reste de cette section, nous présentons les dix sous-bandeaux que nous avons utilisés ainsi que le nombre d'inversions pour chaque ligne et colonne de ces sous-bandeaux.

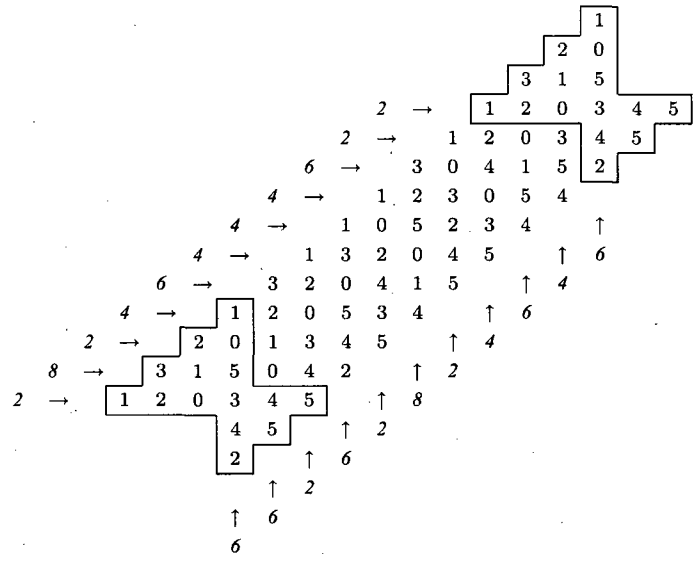

figure 5.12 – B_{10} : Sous-bandeau de taille 10

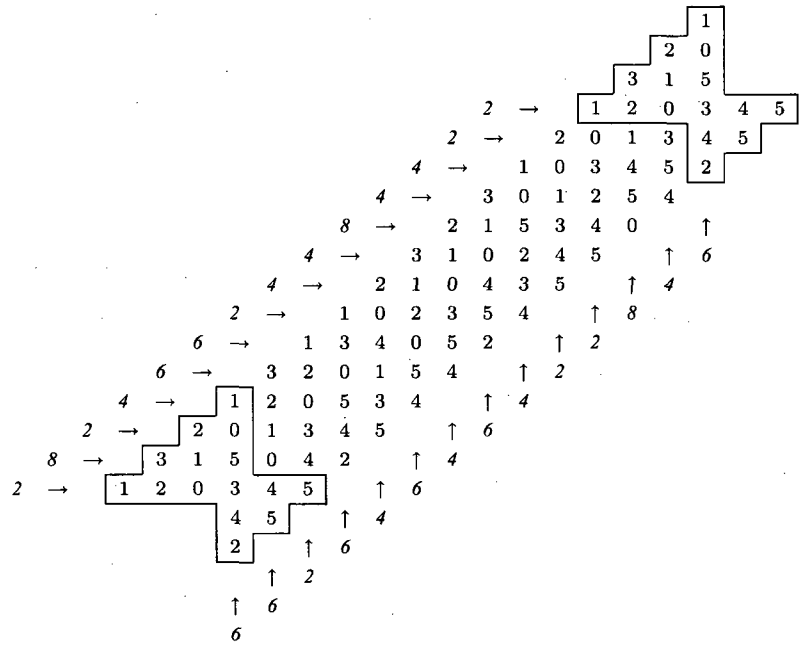

figure 5.13 – B_{13} : Sous-bandeau de taille 13

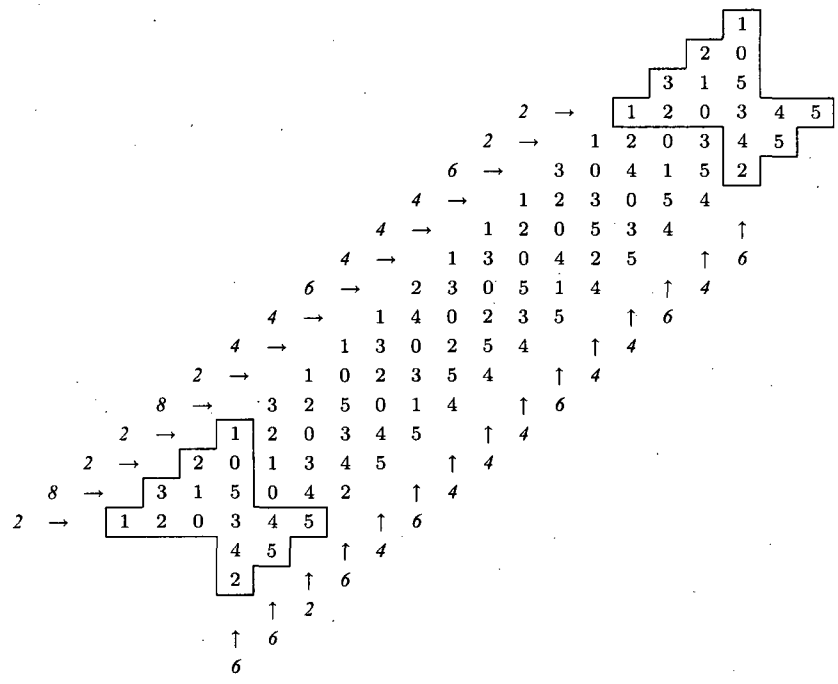

figure 5.14 – B_{14} : Sous-bandeau de taille 14

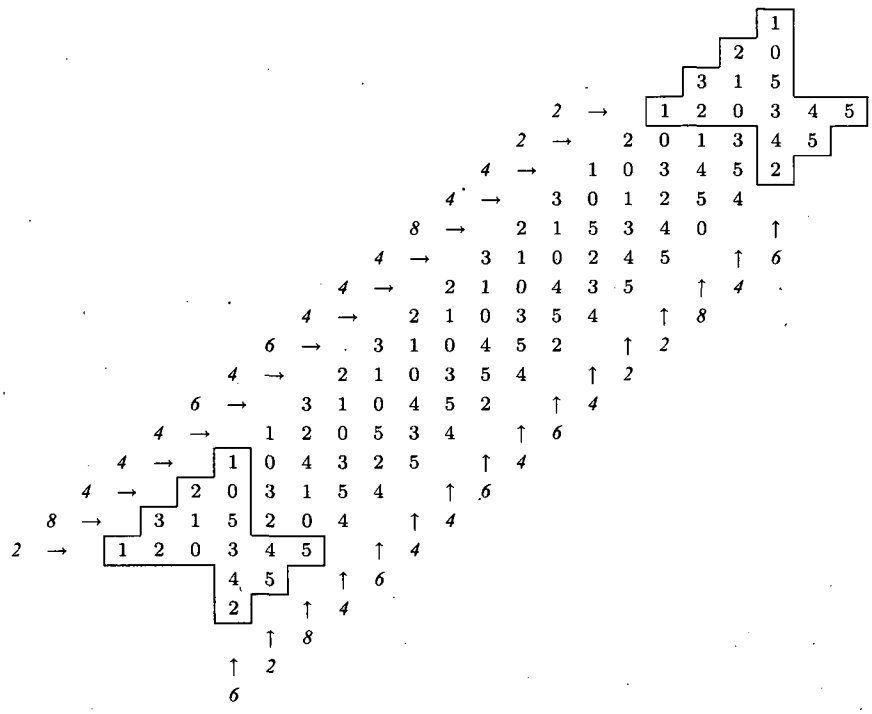

figure 5.15 – B_{15} : Sous-bandeau de taille 15

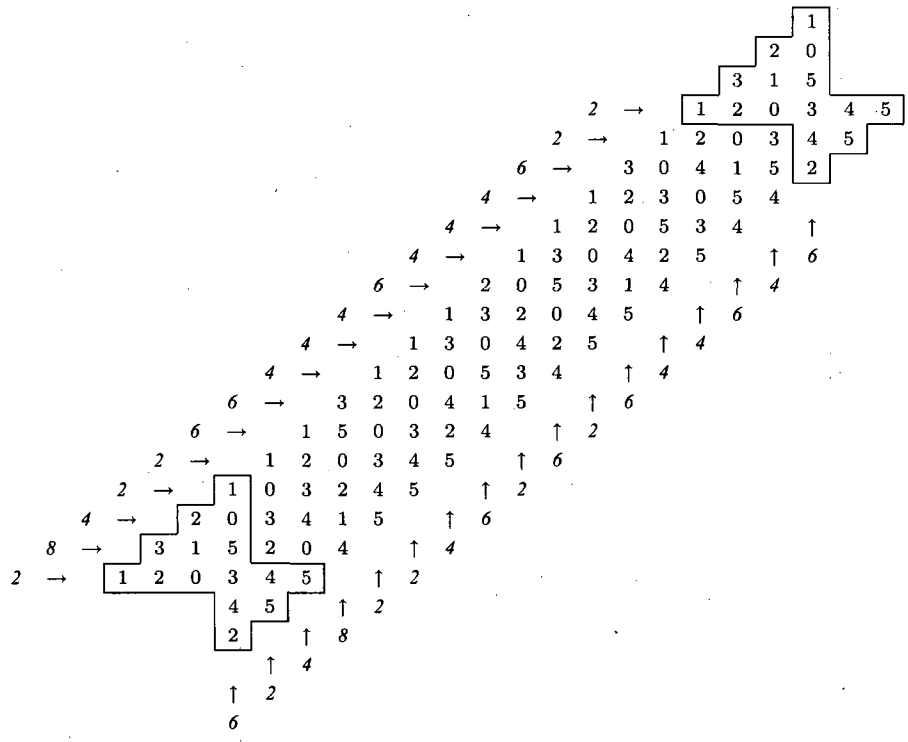

figure 5.16 – B_{16} : Sous-bandeau de taille 16

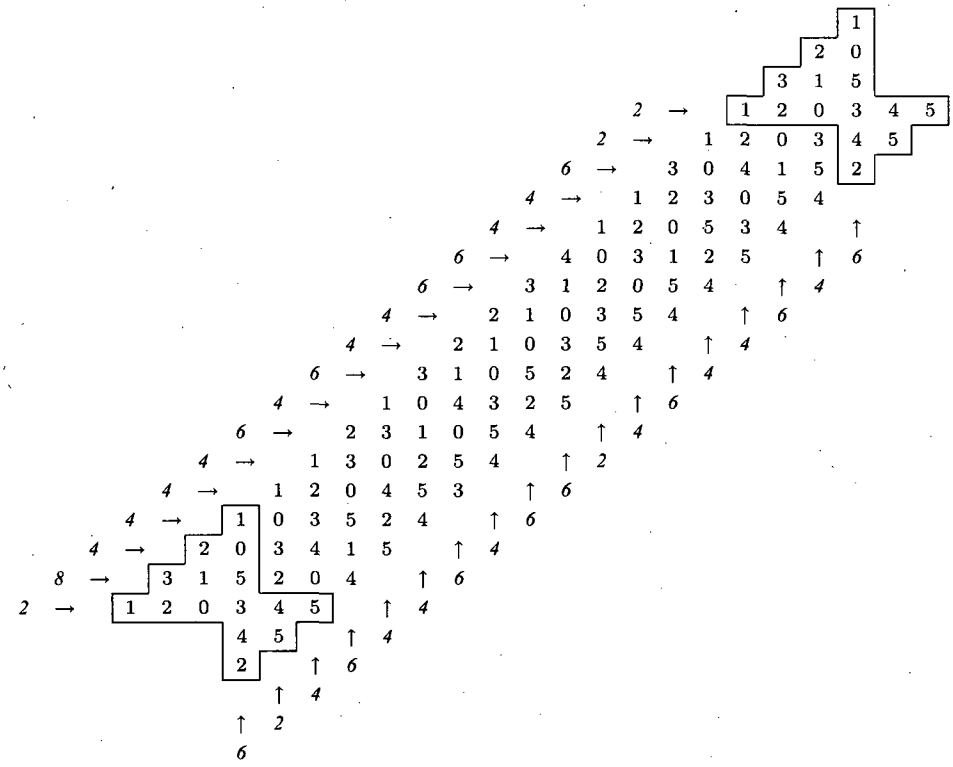

figure 5.17 – B_{17} : Sous-bandeau de taille 17

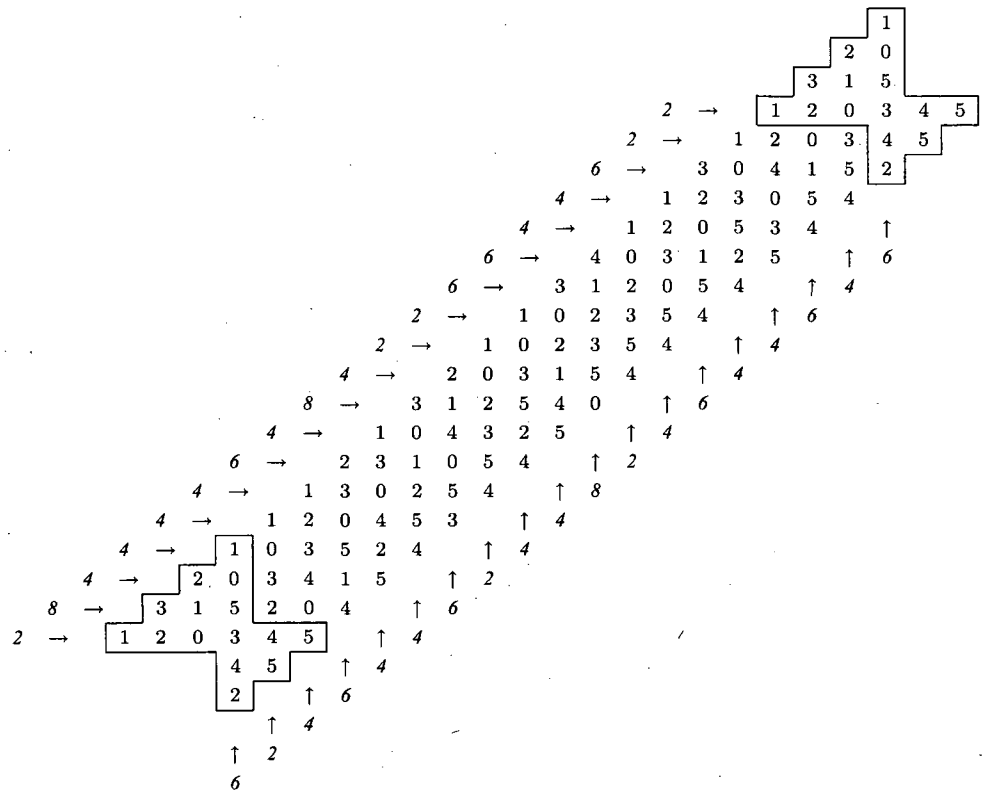

figure 5.18 – B_{18} : Sous-bandeau de taille 18

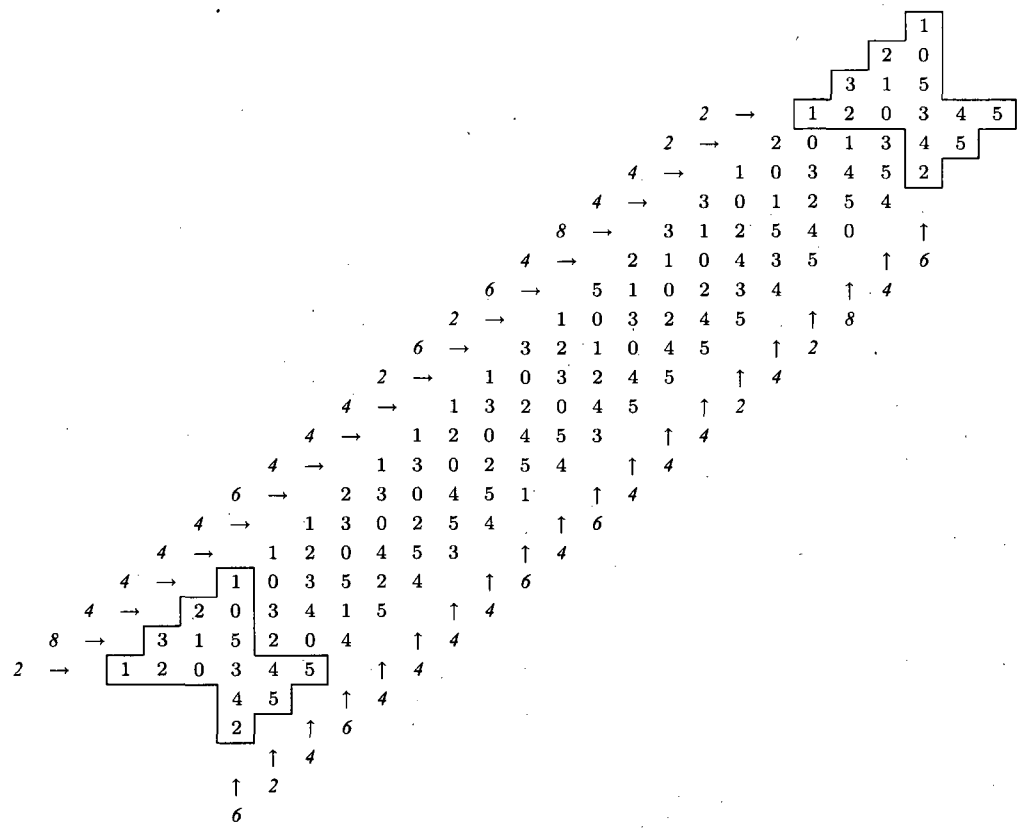

figure 5.19 – B_{19} : Sous-bandeau de taille 19

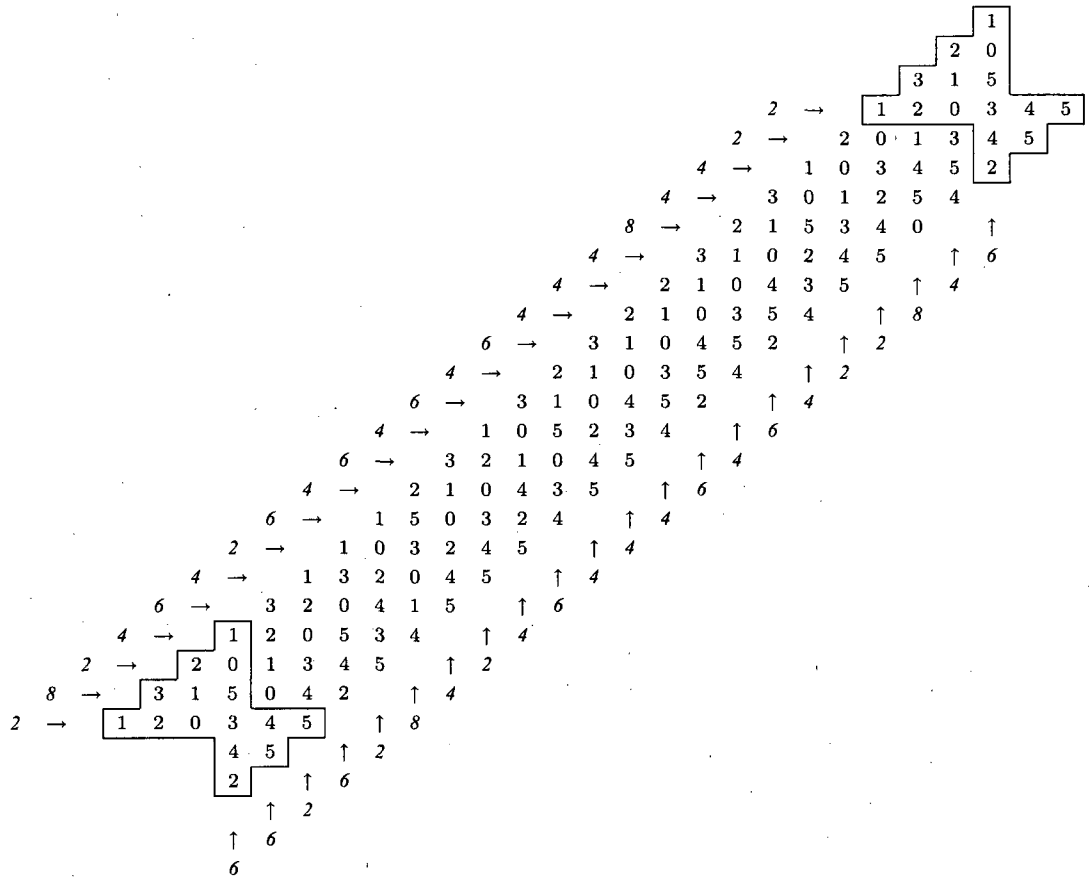

figure 5.20 – B_{21} : Sous-bandeau de taille 21

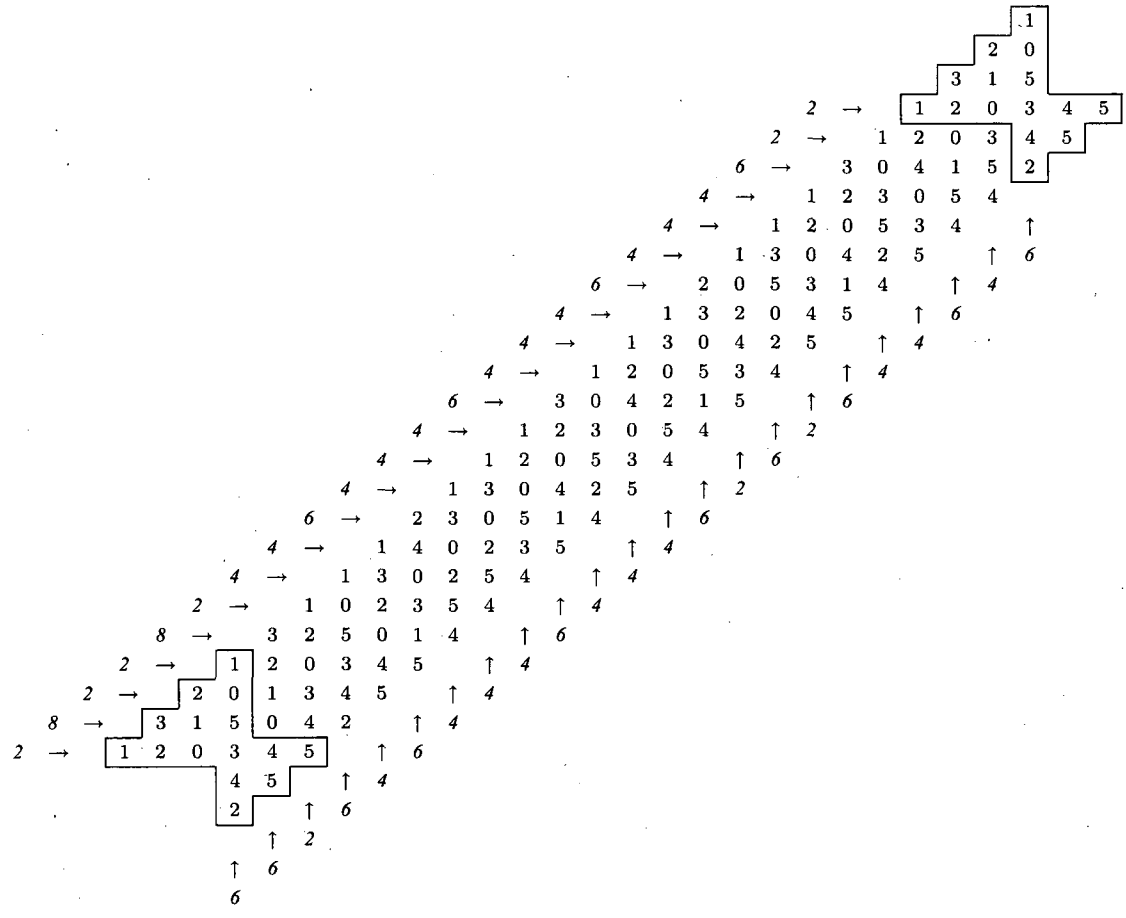

figure 5.21 – B_{22} : Sous-bandeau de taille 22

5.2 Exemples de boucles d'ordre 25 à 41

Puisque la construction présentée dans la section précédente ne fonctionne que pour des boucles d'ordre supérieur à 43, nous allons donner des exemples de boucles incassables commutatives d'ordre impair de 25 à 41 dont le groupe de multiplication est le groupe alterné.

Pour donner un exemple de boucle d'ordre 37, nous pouvons directement utiliser le sous-bandeau B_{10} de la figure 5.12 avec la construction 5.1.1. Pour les autres boucles, nous utiliserons le début de la construction 4.2.1, jusqu'après l'étape du triangle de départ (avant le remplissage du bandeau) tel que montré dans la figure 4.10. Seul le bandeau sera donné. Celui-ci contiendra la première ligne du triangle de départ (ligne $p+1$) ainsi que la dernière ligne du petit triangle d'arrivée (ligne 3). Ce qu'il faut remarquer, c'est que s'il y a un élément 0 sur la diagonale en dessous de la diagonale de $n-1$, ce 0 est placé sur une ligne dont le numéro n'est pas un diviseur de n. De cette façon, la boucle reste incassable. Également, le lecteur pourra valider que le groupe de multiplication de ces boucles est bel et bien le groupe alterné en vérifiant que, pour tout élément a de la boucle, la permutation L_a est paire. En effet, puisque les lignes L_2 et L_3 ne sont pas touchées, la preuve du théorème 5.1.3 s'applique. Les figures 5.22 à 5.29 à la fin de la section illustrent ces bandeaux.

Il est possible d'obtenir des boucles commutatives d'ordre impair inférieur à 25 dont le groupe de multiplication est le groupe alterné. Par contre, nous ne pouvons pas utiliser les constructions présentées dans ce mémoire pour les produire. Néanmoins, les algorithmes présentés dans les précédents chapitres permettent de construire ces boucles.

Ligne 3	⋯⋯											1	2	0
											1	0	3	2
										2	0	3	4	1
									1	3	2	5	0	4
								1	3	0	4	2	5	
							5	0	2	1	3	4		
						2	1	3	0	4	5			
					3	1	0	2	4	5				
				1	2	0	3	4	5					
			1	2	0	3	4	5						
Ligne $p+1=13$	⋯	1	3	0	5	4	2							

figure 5.22 – Bandeau d'une boucle d'ordre 25

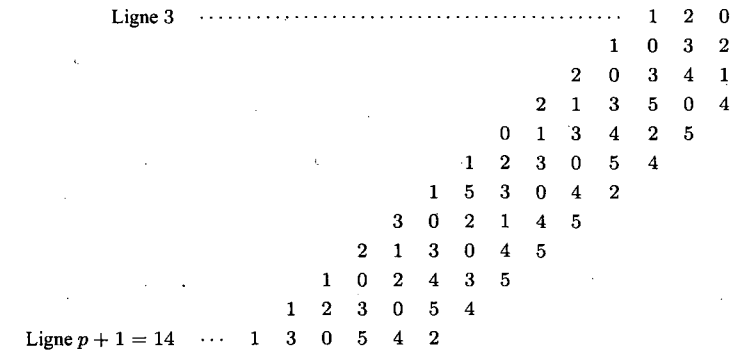

figure 5.23 – Bandeau d'une boucle d'ordre 27

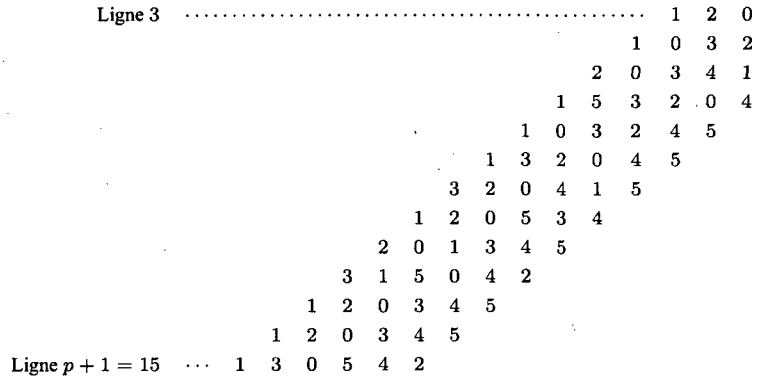

figure 5.24 – Bandeau d'une boucle d'ordre 29

5.2. EXEMPLES DE BOUCLES D'ORDRE 25 À 41

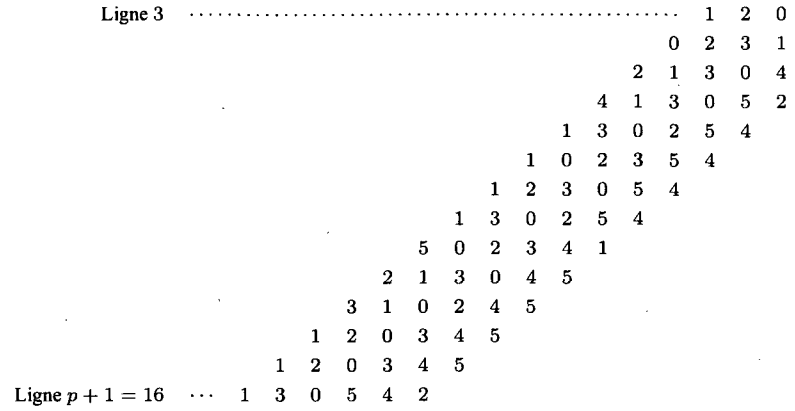

figure 5.25 – Bandeau d'une boucle d'ordre 31

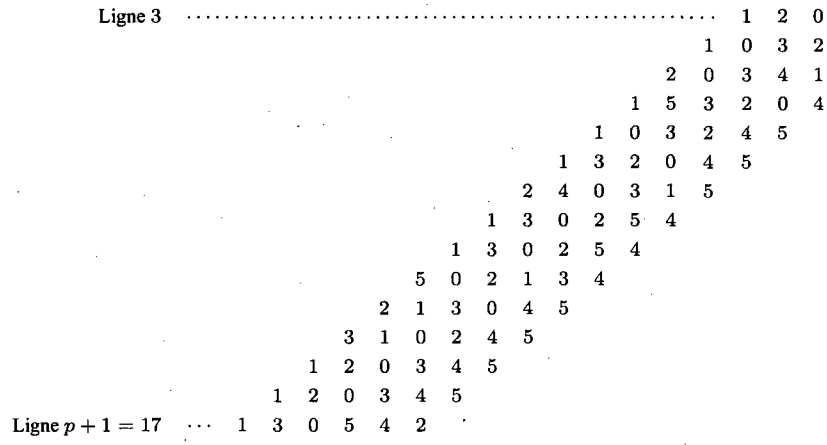

figure 5.26 – Bandeau d'une boucle d'ordre 33

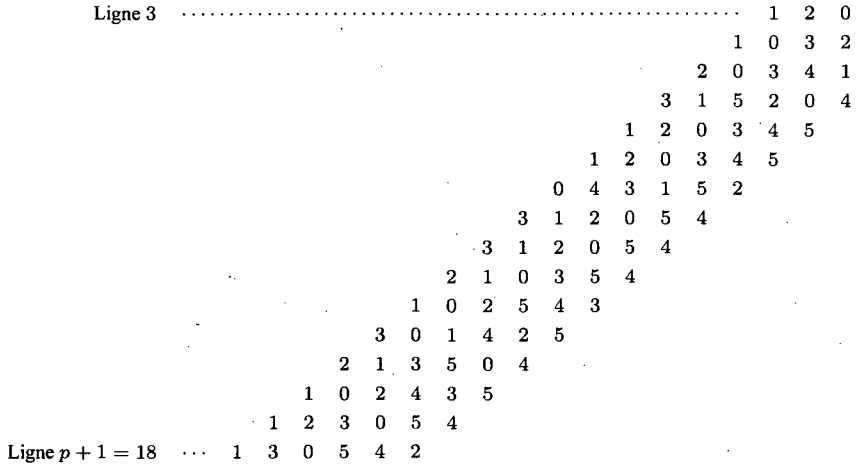

figure 5.27 – Bandeau d'une boucle d'ordre 35

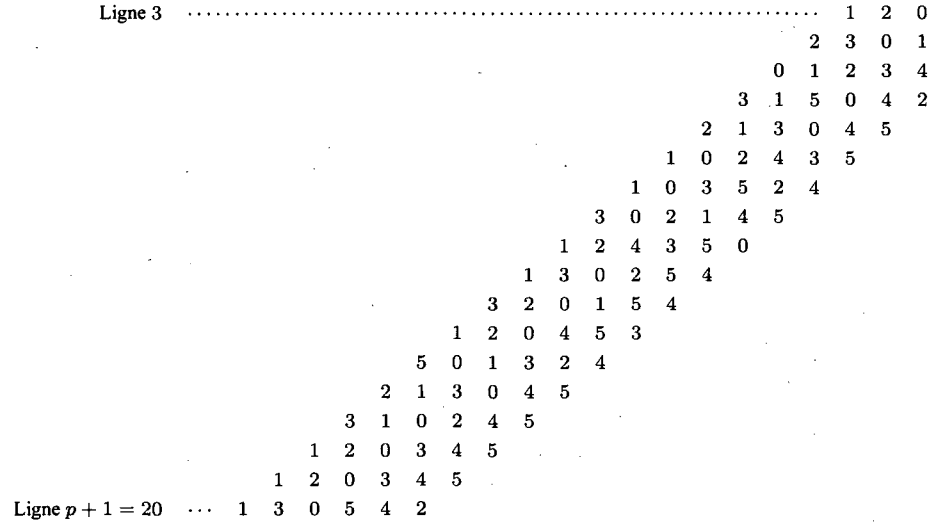

figure 5.28 – Bandeau d'une boucle d'ordre 39

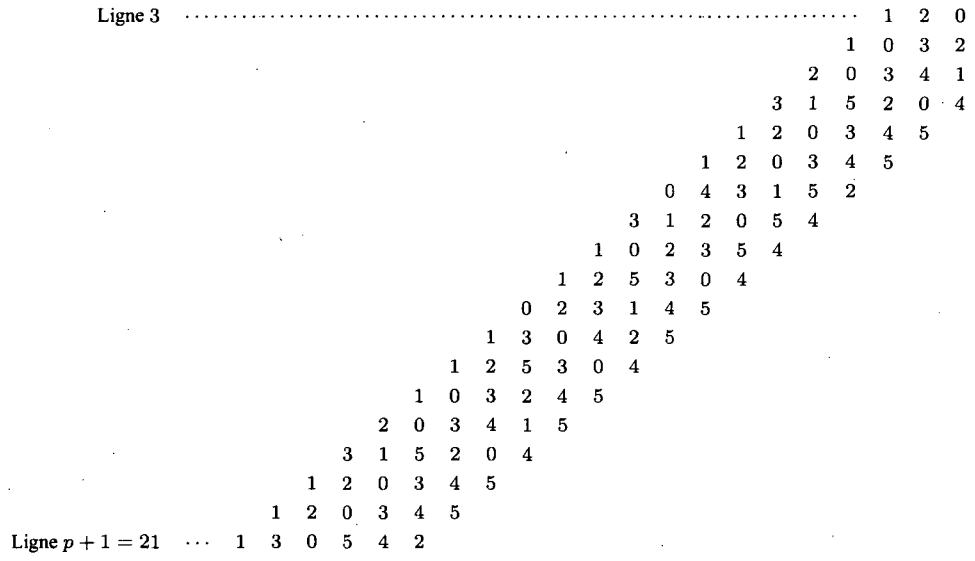

figure 5.29 – Bandeau d'une boucle d'ordre 41

Conclusion

Il va de soi que la recherche de familles infinies de boucles incassables n'en est qu'à ses débuts. La matière présentée dans ce mémoire constitue néanmoins une bonne introduction à ce domaine. En effet, nous avons présenté les motivations nous poussant à construire des familles infinies de boucles incassables. Également, les expérimentations ainsi que la première famille infinie de boucles incassables que nous avons construite suggèrent que le nombre de boucles incassables augmente significativement lorsque l'ordre des boucles augmente. Nous savons donc que beaucoup d'autres familles de boucles peuvent être construites à partir de boucles de grande taille. Ces familles peuvent être définies à partir de plusieurs propriétés de boucles. Pour notre part, les propriétés auxquelles nous nous sommes attaqués sont le groupe de multiplication et la commutativité des boucles. Ainsi, nous avons construit notre première famille infinie de boucles incassables commutatives dont le groupe de multiplication est le groupe symétrique. Par contre, cette famille ne contenait que des boucles d'ordre premier. Ce résultat nous a poussé à l'étendre à toutes les boucles d'ordre impair. Après avoir obtenu cette nouvelle famille de boucles, nous avons décidé de nous en inspirer pour construire une famille de boucles incassables commutatives d'ordre impair dont le groupe de multiplication est le groupe alterné.

En terminant, nous pensons que la construction de familles de boucles incassables sera utile pour de futures recherches. En effet, en se basant sur les familles déjà construites, nous pourrions tâcher de construire des familles de boucles incassables d'ordre pair dont le groupe de multiplication est le groupe symétrique ou le groupe alterné. Également, en voulant aller plus loin, la boucle d'ordre 8 trouvée lors des expérimentations dont le groupe de multiplication est isomorphe au groupe Galois peut donner une piste pour explorer de nouvelles familles de boucles incassables dont le groupe de multiplication n'est pas le groupe

symétrique ni le groupe alterné.

Bibliographie

[1] B. BAUMSLAG et B. CHANDLER. Schaum's Outline of Theory and Problems of Group Theory. McGraw-Hill, 1968.

[2] M. BEAUDRY. « Languages Recognized by Finite Aperiodic Groupoids ». Theoretical Computer Science, 209 :299–317, 1998.

[3] M. BEAUDRY et F. LEMIEUX. « Faithful Loops for Aperiodic E-Ordered Monoids ». Dans Proceedings of the 36th International Colloquium on Automata, Languages and Programming, volume 5556 de Lecture Notes in Computer Science, pages 55–66, 2009.

[4] M. BEAUDRY, F. LEMIEUX et D. THÉRIEN. « Finite Loops Recognize Exactly the Regular Open Languages ». Dans Proceedings of the 24th International Colloquium on Automata, Languages and Programming, volume 1256 de Lecture Notes in Computer Science, pages 110–120, 1997.

[5] M. BEAUDRY, F. LEMIEUX et D. THÉRIEN. « Star-free Open Languages and Aperiodic Loops ». Dans 18th Annual Symposium on Theoretical Aspects of Computer Science, volume 2010 de Lecture Notes in Computer Science, pages 87–98, 2001.

[6] F. BÉDARD, F. LEMIEUX et P. MCKENZIE. « Extensions to Barrington's M-Program Model ». Theoretical Computer Science, 107 :31–61, 1993.

[7] N. BRUIN et N. D. ELKIES. « Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois Groups of Order 168 and $8 \cdot 168$ ». Dans Algorithmic Number Theory, 5th International Symposium, ANTS-V, volume 2369 de Lecture Notes in Computer Science, pages 172–188, 2002.

[8] H. CAUSSINUS et F. LEMIEUX. « The Complexity of Computing over Quasigroups ». Dans Proceeding of the 14th Annual FST&TCS Conference, volume 880 de Lecture Notes in Computer Science, pages 36–47, 1994.

[9] J. DÉNES et A. D. KEEDWELL. Latin Squares and Their Applications. Academic Press Inc, 1974.

[10] P. GUÉRIN. « Génération des classes d'isomorphisme des boucles d'ordre 8 ». Mémoire de maîtrise, Université du Québec à Chicoutimi, 2003.

[11] J. P. GUY et L. BENETEAU. « Groupes isomorphes au groupe de multiplication d'un quasigroupe ». Thèse de doctorat, Université de Toulouse 3, 1993.

[12] J. E. HOPCROFT et J. D. ULLMAN. Introduction to Automata Theory, Languages, and Computation. Addison-Wesley, 1979.

[13] B. MAENHAUT, I. M. WANLESS et B. S. WEBB. « Subsquare-Free Latin Squares of Odd Order ». European Journal of Combinatorics, 28(1) :322–336, 2007.

[14] B. D. MCKAY, A. MEYNERT et W. MYRVOLD. « Small Latin Squares, Quasigroups, and Loops ». Journal of Combinatorial Designs, 15(2) :98–119, 2006.

[15] H. O. PFLUGFELDER. Quasigroups and Loops : Introduction (Sigma Series in Pure Mathematics Vol 7). Heldermann Verlag, 1990.

[16] S. PICCARD. « Quelques propositions concernant les bases du groupe symétrique et du groupe alterné ». L'Enseignement mathématique, 38 :276–286, 1942.

[17] S. PICCARD. Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier. Libraire Vuibert, 1946.

[18] J. E. PIN. Variétés de langages formels. Masson, 1984.

[19] K. H. ROSEN. Discrete Mathematics and its Applications, Second Edition. McGraw-Hill, 1991.

[20] H. J. RYSER. « A Combinatorial Theorem with an Application to Latin Rectangle ». Proceedings of the American Mathematical Society, 2(4) :550–552, 1951.

[21] J. SCHWENK. « A Classification of Abelian Quasigroups ». Rendiconti di Matematica e delle sue Applicazioni, Serie VII, 15(2) :161–172, 1995.

[22] M. SUZUKI. Group Theory I. Springer-Verlag, 1982.

[23] A. VESANEN. « The Group PSL(2,q) is not the Multiplication Group of a Loop ». Communications in Algebra, 22(4) :1177–1195, 1994.

[24] I. M. WANLESS. « Atomic Latin Squares Based on Cyclotomic Orthomorphisms. ». Electronic Journal of Combinatorics, 12 :22–23, 2005.