Sur la complexité des mots substitutifs

François Nicolas

3 juillet 2001

Table des matières

Première partie

Préliminaires

Chapitre 1

Introduction

1.1 But

Dans ce mémoire, on va étudier deux aspects des mots substitutifs.

La partie II concerne leurs images par des morphismes. On va, en particulier, démontrer un théorème de réduction, le théorème de COBHAM, utile dans le dernier chapitre.

La partie III constitue une étude du comportement asymptotique de la complexité des mots substitutifs. Elle est essentiellement due à PANSIOT [8].

Dans la suite de la partie I, on va fixer les notations et démontrer un certain nombre de résultats techniques utiles dans la partie III.

1.2 Comportements asymptotiques des suites

Définition 1 *Soient* f*,* $g : \mathbf{N} \to \mathbf{R}$.

On dira que g domine f *(ce que l'on notera* $f \preceq g$*) lorsqu'il existe* $C \in \mathbf{R}_+^*$ *et* $N \in \mathbf{N}$ *tels que pour tout entier* $n \geq N$*, on ait* $f(n) \leq Cg(n)$*.*

On dira que f *et* g *ont le* même comportement asymptotique *(ce que l'on notera* $f \asymp g$*) lorsque on a* $f \preceq g$ *et* $g \preceq f$*.*

On dira que f *et* g *sont* équivalents *(ce que l'on notera* $f \sim g$*) lorsque pour tout* $\epsilon \in \mathbf{R}_+^*$*, il existe* $N \in \mathbf{N}$ *tel que pour tout entier* $n \geq N$*, on ait* $(1-\epsilon)f(n) \leq g(n) \leq (1+\epsilon)f(n)$*.*

On définit ainsi trois relations $\preceq$, $\asymp$ et $\sim$ sur $\mathbf{R}^{\mathbf{N}}$. On remarque que $\preceq$ est une relation d'ordre et que $\asymp$ et $\sim$ sont des relations d'équivalence. De plus, la valeur de vérité de $f \preceq g$ (resp. $f \asymp g$, resp. $f \sim g$) ne dépend que des valeurs prises par f et g au voisinage de ∞. Dans la suite, on pourra noter "$f(n) \preceq g(n)$ (resp. $f(n) \asymp g(n)$, resp. $f(n) \sim g(n)$) lorsque $n \to \infty$" pour $f \asymp g$ (resp. $f \preceq g$, resp. $f \sim g$).

Notons quelques propriétés élémentaires de ces trois relations :

- $f \sim g \Longrightarrow f \asymp g$,

- $f(n) \preceq 1$ (resp. $f(n) \succeq 1$) lorsque $n \to \infty$ si et seulement si f est majorée (resp. minorée),
- si $f \asymp g$ et si f et g ne s'annulent jamais alors, il existe c, $C \in \mathbf{R}_+^*$ tels que :

$$\forall n \in \mathbf{N} \qquad cf(n) \leq g(n) \leq Cf(n)$$

1.3 Mots

Les références pour cette section sont [6] et [5] dont on garde à une exception près les notations.

1.3.1 Notations

On fixe tout d'abord quelques notations concernant les mots finis et infinis.

On note :

- ε le mot vide,
- $|w|$ la longueur du mot w,
- $\overleftarrow{w}$ l'image miroir du mot w (voilà l'exception),
- L^+ le plus petit langage contenant L et stable par concaténation,
- $L^\star := L^+ \cup \{\varepsilon\}$,
- $L^\omega := \{w_1 w_2 w_3 \ldots : w_1, w_2, w_3, \ldots \in L\}$,
- $L^\infty := L^\omega \cup L^\star$.

pour tout mot w fini, tout entier $n \in \mathbf{N}$, et tout langage L.

De plus, pour tout mot w de longueur $\geq n$, on note $\mathtt{pref}_n\, w$ (resp. $\mathtt{suff}_n\, w$) le préfixe (resp. suffixe) de longueur n de w. Par convention, on pose $\mathtt{pref}_n\, w := w$ (resp. $\mathtt{pref}_n\, w := w$) pour tout mot w de longueur $< n$.

1.3.2 Facteurs, Complexité

Soient $\mathtt{A}$ un alphabet et $u \in \mathtt{A}^\infty$.

On appelle *facteur* de u tout $w \in \mathtt{A}^\star$ tel qu'il existe $x \in \mathtt{A}^\star$ et $y \in \mathtt{A}^\infty$ vérifiant $u = xwy$. On note $\mathtt{F}(u)$ l'ensemble des facteurs de u et pour tout $n \in \mathbf{N}$, $\mathtt{F}_n(u)$ l'ensemble des facteurs de u de longueur n.

On appelle *fonction de complexité* de u l'application :

$$\begin{array}{rccc} \mathtt{p}_u : & \mathbf{N} & \longrightarrow & \mathbf{N} \\ & n & \longmapsto & \#\,\mathtt{F}_n(u) \end{array}$$

On appelle *facteur intérieur* de u tout $w \in \mathtt{A}^\star$ tel qu'il existe $x \in \mathtt{A}^+$ et $y \in \mathtt{A}^\omega \cup \mathtt{A}^+$ vérifiant $u = xwy$.

1.4 Morphismes

Soient $\mathtt{A}$ et $\mathtt{B}$ deux alphabets.

1.4.1 Définitions

On appelle *morphisme* de $\mathtt{A}^\star$ dans $\mathtt{B}^\star$ toute application $f : \mathtt{A}^\star \to \mathtt{B}^\star$ telle que pour tous x, $y \in \mathtt{A}^\star$, on ait $f(xy) = f(x)f(y)$. On note $\hom(\mathtt{A}^\star, \mathtt{B}^\star)$ l'ensemble des morphismes de $\mathtt{A}^\star$ dans $\mathtt{B}^\star$. On dit que f est un *endomorphisme* de $\mathtt{A}^\star$ lorsque f est un morphisme de $\mathtt{A}^\star$ dans lui-même. On abrège $\hom(\mathtt{A}^\star, \mathtt{A}^\star)$ en $\hom(\mathtt{A}^\star)$.

Une remarque fondamentale est : tout $f \in \hom(\mathtt{A}^\star, \mathtt{B}^\star)$ est déterminé de manière unique par sa rectriction à $\mathtt{A}$.

On dit que $f \in \hom(\mathtt{A}^\star, \mathtt{B}^\star)$ est *non effaçant* lorsque $\varepsilon \notin f(\mathtt{A})$. On dit que f est *lettre à lettre* lorsque $f(\mathtt{A}) \subseteq \mathtt{B}$. On étend f en une application $\mathtt{A}^\infty \to \mathtt{B}^\infty$ en posant $f(\mathtt{a}_1\mathtt{a}_2\mathtt{a}_3\ldots) := f(\mathtt{a}_1)f(\mathtt{a}_2)f(\mathtt{a}_3)\ldots$ pour tout $(\mathtt{a}_j)_{j\in\mathbf{N}^\star} \in \mathtt{A}^{\mathbf{N}}$.

1.4.2 Mots substitutifs

Pour tout $f \in \hom(\mathtt{A}^\star)$ et tout $\mathtt{u}_0 \in \mathtt{A}$ tels que $f(\mathtt{u}_0) \in \mathtt{u}_0\mathtt{A}^\star$, on pose :

$$f^\omega(\mathtt{u}_0) := \mathtt{u}_0 s f(s) f^2(s) f^3(s) \ldots$$

où $s \in \mathtt{A}^\star$ est tel que $f(\mathtt{u}_0) = \mathtt{u}_0 s$. On remarque que pour tout $n \in \mathbf{N}$, on a $f^n(\mathtt{u}_0) = \mathtt{u}_0 s f(s) f^2(s) \ldots f^n(s)$ et que $f\left(f^\omega(\mathtt{u}_0)\right)$.

On dit qu'un endomorphisme f est *prolongeable* sur une lettre $\mathtt{u}_0$ lorsque :

– $f(\mathtt{u}_0)$ commence par $\mathtt{u}_0$,

– $\lim_{n\to\infty} |f^n(\mathtt{u}_0)| = \infty$.

Ceci force $f^\omega(\mathtt{u}_0)$ à être infini.

On dit qu'un mot infini u est *engendré* par un endomorphisme f lorsque f est prolongeable sur la première lettre $\mathtt{u}_0$ de u et lorsque $u = f^\omega(\mathtt{u}_0)$.

On appelle *mot substitutif* tout mot infini engendré par un endomorphisme.

Chapitre 2

Généralités sur la fonction de complexité des mots infinis

Dans ce chapitre, $\mathtt{A}$ et $\mathtt{B}$ désignent deux alphabets quelconques.

2.1 Facteurs spéciaux

Soit $u \in \mathtt{A}^\omega$.

Définition 2 (Extensions) *Pour $w \in \mathtt{A}^\star$ on note :*

$$\underset{u}{\mathtt{ext}}(w) := \{\mathtt{a} \in \mathtt{A} : w\mathtt{a} \in \mathtt{F}(u)\}$$

et on appelle extensions *de w dans u les éléments de $\mathtt{ext}_u(w)$.*

On remarque que pour tout $w \in \mathtt{F}(u)$, on a $\mathtt{ext}_u(w) \neq \emptyset$.

Définition 3 (Facteurs spéciaux) *On note :*

$$\mathtt{R}(u) := \left\{w \in \mathtt{A}^\star : \#\underset{u}{\mathtt{ext}}(w) \geq 2\right\}$$

et on appelle les éléments de $\mathtt{R}(u)$ facteurs spéciaux *de u.*

On définit également $\mathtt{R}_n(u) := \mathtt{R}(u) \cap \mathtt{A}^n$ pour tout $n \in \mathbf{N}$ et :

$$\begin{array}{rccc} \mathtt{r}_u : & \mathbf{N} & \longrightarrow & \mathbf{N} \\ & n & \longmapsto & \#\,\mathtt{R}_n(u) \end{array}$$

Lemme 4

$$\forall n \in \mathbf{N} \qquad \mathtt{r}_u(n) \leq \mathtt{p}_u(n+1) - \mathtt{p}_u(n) \leq (\#\,\mathtt{A} - 1)\,\mathtt{r}_u(n)$$

Preuve : On a :

$$\mathtt{F}_{n+1}(u) = \bigcup_{w \in \mathtt{F}_n(u)} w \underset{u}{\mathtt{ext}}(w)$$

donc comme la réunion ci-dessus est disjointe, on obtient en passant aux cardinaux :

$$\mathtt{p}_u(n+1) = \sum_{w \in \mathtt{F}_n(u)} \# \Big(w \underset{u}{\mathtt{ext}}(w) \Big) = \sum_{w \in \mathtt{F}_n(u)} \# \underset{u}{\mathtt{ext}}(w)$$

puis :

$$\mathtt{p}_u(n+1) - \mathtt{p}_u(n) = \sum_{w \in \mathtt{F}_n(u)} \Big(\# \underset{u}{\mathtt{ext}}(w) - 1 \Big)$$

Or pour tout $w \in \mathtt{F}(u)$, on a :
- $\# \mathtt{ext}_u(w) \leq \# \mathtt{A}$,
- $\# \mathtt{ext}_u(w) \neq 1$ si et seulement si $w \in \mathtt{R}(u)$.

Il en résulte que :

$$\mathtt{p}_u(n+1) - \mathtt{p}_u(n) = \sum_{w \in \mathtt{R}_n(u)} \Big(\# \underset{u}{\mathtt{ext}}(w) - 1 \Big)$$

et les $\mathtt{r}_u(n)$ termes de cette dernière somme sont tous compris entre 1 et $\# \mathtt{A} - 1$.

■

Proposition 5

$$\forall N \in \mathbf{N}^* \qquad 1 + \sum_{n=0}^{N-1} \mathtt{r}_u(n) \leq \mathtt{p}_u(N) \leq 1 + (\# \mathtt{A} - 1) \sum_{n=0}^{N-1} \mathtt{r}_u(n)$$

Preuve : Il suffit de prendre la somme sur n variant de 0 à $N-1$ de l'encadrement démontré dans le lemme 4. ■

Théorème 6 (Morse-Hedlund) *On a équivalence entre :*

1. *v n'est pas ultimement périodique,*
2. *$\mathtt{p}_v$ est non bornée,*
3. *$\mathtt{r}_v$ ne s'annule jamais,*
4. *pour tout $n \in \mathbf{N}$, on a $\mathtt{p}_v(n) \geq n+1$.*

En particulier, on a :

$$\mathtt{p}_u(n) \begin{cases} \asymp & 1 \quad \text{si } f \text{ est ultimement périodique} \\ \succeq & n \quad \text{sinon} \end{cases}$$

lorsque $n \to \infty$.

On admettra la démonstration de ce théorème, que l'on trouvera dans [7] ou dans [5]. Il constitue le premier (et le moins fin) des deux instruments que nous allons mettre en oeuvre pour minorer des complexités. Le deuxième instrument est le lemme suivant.

Lemme 7 *Soient* $v \in \{\mathtt{0},\mathtt{1}\}^\omega$, $(w_k)_{k\in\mathbf{N}}$ *une suite d'éléments de* $\{\mathtt{0},\mathtt{1}\}^\star$ *et* $(e_k)_{k\in\mathbf{N}}$ *une suite d'entiers naturels tels que pour tout* $k \in \mathbf{N}$*, on ait :*

– w_k *suffixe de* w_{k+1}*,*
– $e_k < e_{k+1}$*,*
– $w_k\mathtt{1}\mathtt{0}^{e_k}\mathtt{1}$ *facteur de* v*.*

Alors, pour tout $n \in \mathbf{N}$*, on a* $\mathtt{r}_v(n) \geq \# E_n$ *avec :*

$$E_n := \{k \in \mathbf{N} : 1 + e_k \leq n \leq 1 + e_k + |w_k|\}$$

Preuve : Notons :

$$\begin{array}{rccl} \varphi_n : & E_n & \longrightarrow & \{\mathtt{0},\mathtt{1}\}^n \\ & k & \longmapsto & \underset{n}{\mathtt{suff}}\, w_k\mathtt{1}\mathtt{0}^{e_k} \end{array}$$

D'une part, on voit que pour $k \in E_n$:

– $\varphi_n(k)\mathtt{1}$ est suffixe de $w_k\mathtt{1}\mathtt{0}^{e_k}\mathtt{1}$ et donc facteur de v,
– $\varphi_n(k)\mathtt{0}$ est suffixe de $w_k\mathtt{1}\mathtt{0}^{e_k+1}$ donc facteur de $w_{k+1}\mathtt{1}\mathtt{0}^{e_{k+1}}$ donc facteur de v,
– $\varphi_n(k)$ admet $\mathtt{1}\mathtt{0}^{e_k}$ pour suffixe.

Il résulte des deux premiers points que $\varphi_n(E_n) \subseteq \mathtt{R}_n(u)$.

D'autre part, pour k, $l \in E_n$ avec $k < l$ le troisième point garantit que les suffixes de longueur $e_k + 1$ de $\varphi_n(k)$ et $\varphi(l)$ sont respectivement $\mathtt{1}\mathtt{0}^{e_k}$ et $\mathtt{0}^{e_k+1}$ d'où $\varphi_n(k) \neq \varphi_n(l)$: φ est injective. ■

2.2 Image de mots infinis par des morphismes

Soient $f \in \hom(\mathtt{A}^\star, \mathtt{B}^\star)$ et $u \in \mathtt{A}^\omega$.

Proposition 8 *Il suffit que* f *soit non effaçant pour avoir :*

$$\forall n \in \mathbf{N} \qquad \mathtt{p}_{f(u)}(n) \leq |f|\, \mathtt{p}_u(n)$$

Preuve : Supposons f non effaçant et fixons $n \in \mathbf{N}^*$.

Notant :

$$\begin{array}{rccl} \varphi_n : & \mathtt{F}_n(u) \times \{1, \ldots, |f|\} & \longrightarrow & \mathtt{F}(f(u)) \\ & (x, j) & \longmapsto & \underset{n}{\mathtt{pref}} \left(\underset{|f(x)|-(j-1)}{\mathtt{suff}} f(x) \right) \end{array}$$

il suffit de montrer que l'image de φ_n contient $\mathtt{F}_n(f(u))$.

Soit $y \in \mathtt{F}_n(f(u))$.

Soient :

– q un préfixe de $f(u)$ tel que qy soit préfixe de $f(u)$,
– p le préfixe de u de longueur maximale tel que $|f(p)| \leq |q|$,
– $w \in \mathtt{B}^\star$ tel que $q = f(p)w$,
– $\mathtt{a} \in \mathtt{A}$ et $x \in \mathtt{A}^{n-1}$ tels que $p\mathtt{a}x$ soit préfixe de u : $\mathtt{a}x \in \mathtt{F}_n(u)$.

Par maximalité de $|p|$, on a $|f(p\mathtt{a})| \geq |q| + 1$ d'où :

$$\underbrace{|f(p)| + |w|}_{|q|} + 1 \leq \underbrace{|f(p)| + |f(\mathtt{a})|}_{|f(p\mathtt{a})|} \leq |f(p)| + |f|$$

puis :

$$|w| < |f| \tag{2.1}$$

De plus, comme f est non effaçant, on a $|f(x)| \geq n - 1$ d'où :

$$|f(p\mathtt{a}x)| = |f(p\mathtt{a})| + |f(x)| \geq |q| + 1 + n - 1 = |qy|$$

Ainsi, comme $f(p\mathtt{a}x)$ et qy sont tous les deux préfixes de $f(u)$, il existe $w' \in \mathtt{B}^\star$ tel que $f(p\mathtt{a}x) = qyw' = f(p)wyw'$. On en déduit que :

$$f(\mathtt{a}x) = wyw' \tag{2.2}$$

On tire alors de (2.1) et (2.2) que $y = \varphi_n(\mathtt{a}x, |w| + 1)$: ce qu'on voulait. ■

Proposition 9 *Il suffit que u n'admette qu'un nombre fini de facteurs effacés par une puissance de f pour avoir :*

$$\forall n \in \mathbf{N} \qquad \mathtt{p}_{f(u)}(n) \leq |f|\, \mathtt{p}_u\left((M+1)n - M\right)$$

où :

$$M := \sup_{\substack{x \in \mathtt{F}(u) \\ f(x) = \varepsilon}} |x|$$

Preuve : Soient $\tilde{\mathtt{A}} := \{\mathtt{a} \in \mathtt{A} : f(\mathtt{a}) \neq \varepsilon\}$, $\chi \in \hom\left(\mathtt{A}^\star, \tilde{\mathtt{A}}^\star\right)$ défini en posant :

$$\chi(\mathtt{a}) := \begin{cases} \mathtt{a} & \text{si } \mathtt{a} \in \tilde{\mathtt{A}} \\ \varepsilon & \text{sinon} \end{cases}$$

pour tout $\mathtt{a} \in \mathtt{A}$ et $\tilde{f} \in \hom\left(\tilde{\mathtt{A}}^\star, \mathtt{B}^\star\right)$ la restriction de f à $\tilde{\mathtt{A}}^\star$.

Par construction, on a $f = \tilde{f} \circ \chi$ et $\tilde{f}$ est non effaçant avec $\left|\tilde{f}\right| = |f|$ donc par la proposition 8, il suffit de montrer que :

$$\forall n \in \mathbf{N} \qquad \mathtt{p}_{\chi(u)}(n) \leq \mathtt{p}_u((M+1)n - M)$$

Pour cela, on écrit :

$$u = w_0\mathtt{u}_0w_1\mathtt{u}_1w_2\mathtt{u}_2w_3\mathtt{u}_3w_4\mathtt{u}_4\ldots$$

avec $\mathtt{u}_j \in \tilde{\mathtt{A}}$ et $w_j \in \left(\mathtt{A} \setminus \tilde{\mathtt{A}}\right)^\star$ tel que $|w_j| \leq M$ pour $j \in \mathbf{N}$:

$$\chi(u) = \mathtt{u}_0\mathtt{u}_1\mathtt{u}_2\mathtt{u}_3\mathtt{u}_4\ldots$$

Soit alors $y \in \mathtt{F}_n(\chi(u))$: il existe $p \in \mathbf{N}$ tel que $y = \mathtt{u}_p\mathtt{u}_{p+1}\ldots\mathtt{u}_{p+n-1}$. Ainsi, $y = \chi(x)$ avec :

$$x := \mathtt{u}_pw_{p+1}\mathtt{u}_{p+1}\ldots w_{p+n-1}\mathtt{u}_{p+n-1}$$

et comme on a :

$$|x| = \underbrace{\sum_{j=0}^{n-1} |u_{p+j}|}_{n} + \sum_{j=0}^{n-2} \underbrace{|w_{p+j}|}_{\leq M} \leq (M+1)n - M$$

il existe $x' \in \mathtt{F}_{(M+1)n-M}(u)$ admettant x pour préfixe :

$$y = \underset{n}{\mathtt{pref}}\, \chi(x')$$

On a ainsi démontré que l'image de l'application :

$$\begin{array}{ccc} \mathtt{F}_{(M+1)n-M}(u) & \longrightarrow & \mathtt{F}(\chi(u)) \\ x & \longmapsto & \underset{n}{\mathtt{pref}}\, \chi(x) \end{array}$$

contenait $\mathtt{F}_n(\chi(u))$ d'où l'inégalité recherchée. ■

Chapitre 3

Un peu d'analyse

3.1 Minoration de sommes de logarithmes itérés

Dans la suite, on aura besoin des minorations :

$$\begin{aligned} \sum_{n=1}^{N} \ln N &\succeq N \ln N \\ \sum_{n=3}^{N} \ln \ln N &\succeq N \ln \ln N \end{aligned}$$

lorsque $N \to \infty$. Le but de cette section est d'établir ces minorations.

Lemme 10

$$\forall x \in \mathbf{R}_+^* \qquad x > 4 \iff \ln\left(\frac{1}{2}x\right) > \frac{1}{2}\ln x \tag{3.1}$$

$$\forall y \in \mathbf{R} \qquad y > \ln 4 \iff \exp\left(\frac{1}{2}y\right) < \frac{1}{2}\exp y \tag{3.2}$$

Preuve : Il est évident que (3.1) et (3.2) sont équivalents.

Notant :

$$\begin{aligned} f: \quad \mathbf{R}_+^* &\longrightarrow \mathbf{R} \\ x &\longmapsto \ln\left(\frac{1}{2}x\right) - \frac{1}{2}\ln x \end{aligned}$$

on calcule que pour tout $x > 0$, on a $f'(x) = (2x)^{-1} > 0$ donc f est strictement croissante et comme $f(4) = 0$ on obtient (3.1). ∎

Pour $k \in \mathbf{N}^*$ on note :

$$\begin{aligned} \exp^k &:= \underbrace{\exp \circ \cdots \circ \exp}_{k} \\ \ln^k &:= \underbrace{\ln \circ \cdots \circ \ln}_{k} \end{aligned}$$

et on convient que $\ln^0 = \exp^0 =$ l'identité sur $\mathbf{R}$. Pour $k \in \mathbf{N}^*$, la fonction $\ln^k$ est définie sur $\left]\exp^{k-1} 0, \infty\right[$ et strictement positive sur $\left]\exp^k 0, \infty\right[$

Lemme 11 *Pour tout $k \in \mathbf{N}^*$ on a :*

$$\exp^{k-1} 4 \quad > \quad \exp^k 0 \tag{3.3}$$

$$\forall x \in \left]\exp^{k-1} 4, \infty\right[\qquad \ln^k\left(\frac{1}{2}x\right) \quad > \quad \frac{1}{2}\ln^k x \tag{3.4}$$

Preuve : On démontre par récurrence en utilisant (3.2) que pour tout $k \in \mathbf{N}^*$, on a :

$$\frac{1}{2}\exp^{k-1} 4 \geq \exp^{k-1} 2$$

d'où :

$$\frac{1}{2}\exp^{k-1} 4 \geq \exp^{k-1} 1 = \exp^k 0$$

ce qui démontre (3.3) et garantit que (3.4) à un sens.

On démontre alors facilement (3.4) par récurrence sur k en utilisant (3.1). ■

Proposition 12 *Pour tout $k \in \mathbf{N}^*$ et tout entier $N \geq \lceil \exp^k 0 \rceil$, on a :*

$$\sum_{n=\lceil \exp^k 0\rceil}^{N} \ln^k n \geq \frac{1}{\exp^{k-1} 4} N \ln^k N$$

Preuve : Le lemme 11 garantit que pour tout entier $N \geq \exp^{k-1} 4$, on a $\lceil N/2 \rceil \geq \lceil \exp^k 0 \rceil$ et :

$$\begin{aligned}
\sum_{n=\lceil \exp^k 0\rceil}^{N} \ln^k n &\geq \sum_{n=\lceil N/2\rceil}^{N} \ln^k n \\
&\geq \left(N - \left\lceil \frac{N}{2} \right\rceil + 1\right) \ln^k \left\lceil \frac{N}{2} \right\rceil \\
&\geq \frac{N}{2} \ln^k \left(\frac{N}{2}\right) \\
&\geq \frac{N}{4} \ln^k N \\
&\geq \frac{1}{\exp^{k-1} 4} N \ln^k N
\end{aligned}$$

Enfin, pour tout entier N, $\lceil \exp^k 0 \rceil \leq N \leq \exp^{k-1} 4$, on a :

$$\sum_{n=\lceil \exp^k 0\rceil}^{N} \ln^k n \geq \ln^k N \geq \frac{1}{\exp^{k-1} 4} N \ln^k N$$

■

On pourrait montrer que pour tout $k \in \mathbf{N}^*$, on a :

$$\sum_{n=\lceil \exp^k 0 \rceil}^{N} \ln^k n \sim N \ln^k N$$

lorsque $N \to \infty$ mais on n'en a pas besoin.

3.2 Un comportement asymptotique fondamental

Proposition 13 *Soient $\beta_1,\ \beta_2 \in]1,\infty[$, $\alpha_1,\ \alpha_2 \in \mathbf{N}$ et $\varphi_1,\ \varphi_2 : \mathbf{N} \to \mathbf{R}^*$ tels que $\varphi_j(n) \asymp n^{\alpha_j}\beta_j^n$ lorsque $n \to \infty$ $(j \in 1,2)$.*

Alors, on a :

$$\#\left\{k \in \mathbf{N} : \varphi_1(k) \leq n \leq \varphi_2(k)\right\} \begin{cases} \preceq & 1 & \text{si } \alpha_1 = \alpha_2 \text{ et } \beta_1 = \beta_2 \\ \sim & \frac{\alpha_2 - \alpha_1}{\ln \beta_1} \ln \ln n & \text{si } \beta_1 = \beta_2 \text{ et } \alpha_1 < \alpha_2 \\ \sim & \left(\frac{1}{\ln \beta_1} - \frac{1}{\ln \beta_2}\right) \ln n & \text{si } \beta_1 < \beta_2 \end{cases}$$

lorsque $n \to \infty$.

Preuve : Soient $c_1, c_2, C_1, C_2 \in \mathbf{R}_+^*$ tels que pour tout $k \in \mathbf{N}^*$ et tout $j \in \{1,2\}$ on ait $c_j k^{\alpha_j}\beta_j^k \leq \varphi_j(k) \leq C_j k^{\alpha_j}\beta_j^k$.

Posant :

$$\begin{array}{rcl} E_n & := & \{k \in \mathbf{N}^* : \varphi_1(k) \leq n \leq \varphi_2(k)\} \\ F_n & := & \left\{k \in \mathbf{N}^* : C_1 k^{\alpha_1}\beta_1^k \leq n \leq c_2 k^{\alpha_2}\beta_2^k\right\} \\ G_n & := & \left\{k \in \mathbf{N}^* : c_1 k^{\alpha_1}\beta_1^k \leq n \leq C_2 k^{\alpha_2}\beta_2^k\right\} \end{array}$$

pour tout $n \in \mathbf{N}^*$, on a $F_n \subseteq E_n \subseteq G_n$.

Ceci nous pousse à minorer $\# F_n$ et à majorer $\# G_n$ pour n au voisinage de ∞ donc à introduire les fonctions :

$$\psi_{\alpha,\beta} : \begin{array}{rcl} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^\alpha \beta^x \end{array}$$

pour $\alpha \in \mathbf{N}$ et $\beta > 1$. On remarque que si $\alpha \neq 0$ (resp. $= 0$) alors $\psi_{\alpha,\beta}$ induit une bijection de $\mathbf{R}_+^* \to \mathbf{R}_+^*$ (resp. $\mathbf{R} \to \mathbf{R}_+^*$) dont on note (abusivement) $\psi_{\alpha,\beta}^{-1}$ l'inverse.

Lemme 14 *On a le développement assymptotique :*

$$\psi_{\alpha,\beta}^{-1}(y) = \frac{1}{\ln \beta} \ln y - \frac{\alpha}{\ln \beta} \ln \ln y + \frac{\alpha \ln \ln \beta}{\ln \beta} + \mathrm{o}(1)$$

lorsque $y \to \infty$.

Preuve : En faisant $x := \psi^{-1}_{\alpha,\beta}(y)$ et $y \to \infty$, on a $y = x^\alpha \beta^x$ et $x \to \infty$ d'où :

$$\begin{aligned}
\psi^{-1}_{\alpha,\beta}(y) - \frac{1}{\ln\beta}\ln y + \frac{\alpha}{\ln\beta}\ln\ln y &= x - \frac{1}{\ln\beta}\ln(x^\alpha\beta^x) - \frac{\alpha}{\ln\beta}\ln\ln(x^\alpha\beta^x) \\
&= \frac{\alpha}{\ln\beta}\ln\left(\ln\beta + \alpha\frac{\ln x}{x}\right) \\
&\to \frac{\alpha\ln\ln\beta}{\ln\beta}
\end{aligned}$$

ce qu'on voulait. ■

Lemme 15 *Pour A, $B \in \mathbf{R}^*_+$, on a :*

$$\psi^{-1}_{\alpha_1,\beta_1}\left(\frac{n}{A}\right) - \psi^{-1}_{\alpha_2,\beta_2}\left(\frac{n}{B}\right) \begin{cases} \to & \textit{une limite finie} & \textit{si } \beta_1 = \beta_2 \textit{ et } \alpha_1 = \alpha_2 \\ \sim & \frac{\alpha_2-\alpha_1}{\ln\beta_1}\ln\ln n & \textit{si } \beta_1 = \beta_2 \textit{ et } \alpha_1 < \alpha_2 \\ \sim & \left(\frac{1}{\ln\beta_1} - \frac{1}{\ln\beta_2}\right)\ln n & \textit{si } \beta_1 < \beta_2 \end{cases}$$

lorsque $n \to \infty$.

Preuve : C'est une simple application du lemme 14 où on a remarqué que $\ln\ln\left(\frac{n}{C}\right) = \ln\ln n + o(1)$ lorsque $n \to \infty$ pour $C \in \{A, B\}$. ■

Remarquons que pour tous a, $b \in \mathbf{R}$, on a :

$$b - a \le \#\{k \in \mathbf{N} : a \le k \le b\} \le \max\{b - a + 1, 0\}$$

en tenant compte qu'il est possible que $b < a$.

Ainsi, en écrivant que :

$$\begin{aligned}
F_n &= \left\{k \in \mathbf{N}^* : \psi^{-1}_{\alpha_2,\beta_2}\left(\frac{n}{c_2}\right) \le k \le \psi^{-1}_{\alpha_1,\beta_1}\left(\frac{n}{C_1}\right)\right\} \\
G_n &= \left\{k \in \mathbf{N}^* : \psi^{-1}_{\alpha_2,\beta_2}\left(\frac{n}{C_2}\right) \le k \le \psi^{-1}_{\alpha_1,\beta_1}\left(\frac{n}{c_1}\right)\right\}
\end{aligned}$$

on obtient :

$$\begin{aligned}
\# E_n \ge \# F_n &\ge \psi^{-1}_{\alpha_1,\beta_1}\left(\frac{n}{C_1}\right) - \psi^{-1}_{\alpha_2,\beta_2}\left(\frac{n}{c_2}\right) \\
\# E_n \le \# G_n &\le \max\left\{\psi^{-1}_{\alpha_1,\beta_1}\left(\frac{n}{c_1}\right) - \psi^{-1}_{\alpha_2,\beta_2}\left(\frac{n}{C_2}\right) + 1, 0\right\}
\end{aligned}$$

On conclut grâce au lemme 15. ■

Chapitre 4

Un peu de technique pure

Le lemme suivant sera utilisé plusieurs fois par la suite.

Lemme 16 *Soient E un ensemble* fini *et $\varphi : E \to E$.*
Alors, pour tout $k \in \mathbf{N}^*$, on a $\varphi^{k(\# E)!} = \varphi^{(\# E)!}$.

Preuve : Soient $N := \# E$ et $x \in E$. L'application :

$$\begin{array}{ccc} \{0, 1, \ldots, N\} & \longrightarrow & E \\ n & \longmapsto & \varphi^n(x) \end{array}$$

ne peut pas être injective, donc il existe p, $q \in \{0, 1, \ldots, N\}$ tels que $p < q$ et $\varphi^p(x) = \varphi^q(x)$. Posant $n := q - p$ ($1 \leq n \leq N$), on a $\varphi^{p+n}(x) = \varphi^p(x)$ donc par récurrence sur j, on montre que :

$$\forall j \in \mathbf{N} \qquad \varphi^{p+jn}(x) = \varphi^p(x)$$

En particulier pour $j = (k-1)\frac{N!}{n}$, on a :

$$\forall k \in \mathbf{N}^* \qquad \varphi^{p+(k-1)N!}(x) = \varphi^p(x)$$

donc en prenant l'image des deux membres par $\varphi^{N!-p}$, il vient :

$$\forall k \in \mathbf{N}^* \qquad \varphi^{kN!}(x) = \varphi^{N!}(x)$$

ce qu'on voulait. ■

Soient $\mathtt{A}$ un alphabet, $f \in \hom(\mathtt{A}^\star)$ et $\mathtt{B}$, $\mathtt{C} \subseteq \mathtt{A}$ vérifiant les quatre conditions suivantes notées $(*)$:

$$\begin{array}{rcl} \mathtt{B} \cup \mathtt{C} & = & \mathtt{A} \\ \mathtt{B} \cap \mathtt{C} & = & \emptyset \\ f(\mathtt{B}) & \subseteq & \mathtt{B}^\star \\ f(\mathtt{C}) & \subseteq & \mathtt{A}^\star\mathtt{C}\mathtt{A}^\star \end{array}$$

On aura l'occasion, dans la suite, de se retrouver plusieurs fois dans une situation de ce type.

Proposition 17 *Soit* $\mathtt{u}_0 \in \mathtt{A}$ *tel que* $f(\mathtt{u}_0) \in \mathtt{u}_0(\mathtt{A}^\star \setminus \mathtt{B}^\star)$.
Alors, $f^\omega(\mathtt{u}_0)$ *contient une infinité d'occurences de lettres appartenant à* $\mathtt{C}$.

Preuve : Par hypothèse, on peut écrire $f(\mathtt{u}_0) = \mathtt{u}_0 s$ avec $s \in \mathtt{A}^\star \setminus \mathtt{B}^\star$. Ainsi, au moins une lettre de s est dans $\mathtt{C}$ donc il en est de même pour $f^n(s)$ quel que soit $n \in \mathbf{N}$. Comme $f^\omega(\mathtt{u}_0) = \mathtt{u}_0 s f(s) f^2(s) f^3(s) f^4(s) \ldots$, $f^\omega(\mathtt{u}_0)$ contient bien une infinité de d'occurences de lettres appartenant à $\mathtt{C}$. ■

Lemme 18 *Il existe* $N \in \mathbf{N}^*$ *tel que pour tout* $\mathtt{c} \in \mathtt{C}$*, il existe* $\mathtt{c}' \in \mathtt{C}$ *vérifiant :*
- $f^N(\mathtt{c}) \in \mathtt{B}^\star\mathtt{c}'\mathtt{A}^\star$ *(resp.* $\in \mathtt{A}^\star\mathtt{c}'\mathtt{B}^\star$*),*
- $f^N(\mathtt{c}') \in \mathtt{B}^\star\mathtt{c}'\mathtt{A}^\star$ *(resp.* $\in \mathtt{A}^\star\mathtt{c}'\mathtt{B}^\star$*).*

Preuve : Soient $N := (\#\,\mathtt{C})!$ et $\gamma : \mathtt{C} \to \mathtt{C}$ la fonction qui à tout $\mathtt{c} \in \mathtt{C}$ associe la lettre appartenant à $\mathtt{C}$ apparaissant le plus à gauche possible dans $f(\mathtt{c})$:

$$\forall \mathtt{c} \in \mathtt{C} \qquad f(\mathtt{c}) \in \mathtt{B}^\star\gamma(\mathtt{c})\mathtt{A}^\star$$

Fixons $\mathtt{c} \in \mathtt{C}$ et posons $\mathtt{c}' := \gamma^N(\mathtt{c})$.
L'astuce consiste à remarquer que :

$$\forall n \in \mathbf{N} \qquad f^n(\mathtt{c}) \in \mathtt{B}^\star\gamma^n(\mathtt{c})\mathtt{A}^\star$$

ce qui peut se vérifier par exemple par récurrence.

On a ainsi $f^N(\mathtt{c}) \in \mathtt{B}^\star\mathtt{c}'\mathtt{A}^\star$ et comme par le lemme 16, $\gamma^{2N} = \gamma^N$, on a $f^{2N}(\mathtt{c}) \in \mathtt{B}^\star\gamma^{2N}(\mathtt{c})\mathtt{A}^\star = \mathtt{B}^\star\mathtt{c}'\mathtt{A}^\star$ ce qui force $f^N(\mathtt{c}') \in \mathtt{B}^\star\mathtt{c}'\mathtt{A}^\star$.

On démontre de même la conclusion alternative du lemme. ■

Proposition 19 *Soit* $\mathtt{u}_0 \in \mathtt{A}$ *tel que* $f(\mathtt{u}_0) \in \mathtt{u}_0\mathtt{A}^\star$.
Alors, pour tout y *facteur de* $f^\omega(\mathtt{u}_0)$ *appartenant à* $\mathtt{CB}^\star\mathtt{C}$*, il existe* $n \in \mathbf{N}$*,* $\mathtt{c}$*,* $\mathtt{c}_1$*,* $\mathtt{c}_2 \in \mathtt{C}$*, et* $b \in \mathtt{B}^\star$ *tels que :*
- $\mathtt{c}_1 b \mathtt{c}_2$ *est facteur de* $f(\mathtt{c})$*,*
- y *est la concaténation d'un suffixe de* $f^n(\mathtt{c}_1)$*, de* $f^n(b)$ *et d'un préfixe de* $f^n(\mathtt{c}_2)$*.*

Preuve : On va montrer par récurrence sur $n \in \mathbf{N}$ que tout facteur de $f^n(\mathtt{u}_0)$ appartenant à $\mathtt{CB}^\star\mathtt{C}$ est de la forme souhaitée.

Pour $n = 0$, il n'y a aucun facteur de $f^n(\mathtt{u}_0)$ appartenant à $\mathtt{CB}^\star\mathtt{C}$ donc tout va bien au rang 0. Supposons maintenant le résultat acquis à un rang $n \in \mathbf{N}$ donné.

Soit y un facteur de $f^{n+1}(\mathtt{u}_0)$ appartenant à $\mathtt{CB}^\star\mathtt{C}$: y est facteur de $f\left(f^n(\mathtt{u}_0)\right)$ donc on peut trouver un facteur x de $f^n(\mathtt{u}_0)$ de longueur minimale tel que y soit facteur de $f(x)$. L'astuce consiste à remarquer que $x \in \mathtt{C}$ ou que $x \in \mathtt{CB}^\star\mathtt{C}$.

En effet, supposons tout d'abord $|x| = 1$. Comme $y \notin \mathtt{B}^\star$, on a $x \in \mathtt{C}$ donc il suffit de poser $n := 0$, $\mathtt{c} := x$ et de prendre $\mathtt{c}_1$, $\mathtt{c}_2 \in \mathtt{C}$, $b \in \mathtt{B}^\star$ tels que $y = \mathtt{c}_1 b \mathtt{c}_2$.

Supposons maintenant $|x| \geq 2$. Alors, on peut écrire $x = \mathtt{a}_1\mathring{x}\mathtt{a}_2$ avec $\mathtt{a}_1$, $\mathtt{a}_2 \in \mathtt{A}$ et $\mathring{x} \in \mathtt{A}^\star$ et $y = y_1 f(\mathring{x}) y_2$ avec y_1 suffixe non vide de $f(\mathtt{a}_1)$, y_2 préfixe non vide de $f(\mathtt{a}_2)$. La première (resp. dernière) lettre de y est dans y_1 (resp. y_2) donc dans $f(\mathtt{a}_1)$ (resp. $f(\mathtt{a}_2)$) et comme cette lettre est dans $\mathtt{C}$, on a nécessairement $\mathtt{a}_1 \in \mathtt{C}$ (resp. $\mathtt{a}_2 \in \mathtt{C}$). De plus, $f(\mathring{x})$ n'est ni suffixe, ni préfixe de y donc $f(\mathring{x}) \in \mathtt{B}^\star$

et par suite, $\mathring{x} \in \mathtt{B}^\star$. On en déduit que $x \in \mathtt{CB}^\star\mathtt{C}$ ce qui permet d'appliquer à x l'hypothèse de récurrence : il existe $m \in \mathbf{N}$, $\mathtt{c}$, $\mathtt{c}_1$, $\mathtt{c}_2 \in \mathtt{C}$, et $b \in \mathtt{B}^\star$ tels que $\mathtt{c}_1 b \mathtt{c}_2 \in \mathtt{F}(f(\mathtt{c}))$ et que x soit la concaténantion d'un suffixe de $f^m(\mathtt{c}_1)$, de $f^m(b)$ et d'un préfixe de $f^m(\mathtt{c}_2)$. On termine en posant $n := m + 1$. ■

Deuxième partie

Images de mots substitutifs par des morphismes

Etant donneé un alphabet $\mathtt{B}$, on a cherche dans cette partie à comparer les quatres classes de mots infinis sur $\mathtt{B}$ suivantes :

(PD0L) les mots infinis sur engendré par un endomorphisme *non effaçant*,

(D0L) les mots engendrés par un endomorphisme quelconque,

(HD0L) les images par des morphismes quelconques de mots infinis engendrés par des endomorphismes quelconques,

(CD0L) les images par des morphismes *lettre à lettre* de mots infinis engendrés par des endomorphismes *non effaçants*.

On a trivialement :

$$\mathrm{PD0L} \subseteq \mathrm{D0L} \subseteq \mathrm{HD0L} \subseteq \mathrm{CD0L}$$

mais on va montrer que :

$$\mathrm{PD0L} \subset \mathrm{D0L} \subset \mathrm{HD0L} = \mathrm{CD0L}$$

Chapitre 5

Thèorèmes de factorisation

Dans ce chapitre, $\mathtt{A}$ et $\mathtt{B}$ désignent deux alphabets quelconques.

5.1 Suites d'entiers naturels

Lemme 20 *De toute suite d'entiers naturels, on peut extraire une sous-suite strictement croissante ou une sous-suite constante.*

Preuve : Soit $\nu : \mathbf{N} \to \mathbf{N}$.

Etudions tout d'abord le cas où ν est majorée. Posant :

$$\begin{aligned} M &:= \max_{n=0}^{\infty} \nu(n) \\ I_m &:= \nu^{-1}(\{m\}) \end{aligned}$$

pour $m \in \mathbf{N}$, on a :

$$\mathbf{N} = \bigcup_{m=0}^{M} I_m \tag{5.1}$$

ce qui force l'existence d'un $m \in \{0, 1, \ldots, M\}$ tel que I_m soit infini (sinon, on aurait écrit en (5.1) que l'ensemble infini $\mathbf{N}$ est réunion finie d'ensembles finis).

Alors, on a :

$$\forall N \in \mathbf{N} \qquad I_m \not\subseteq \{0, 1, \ldots, N\}$$

ce qui permet de construire par récurrence $\varphi : \mathbf{N} \to \mathbf{N}$ telle que $\varphi(0) = \min I_m$ et :

$$\forall n \in \mathbf{N} \qquad \varphi(n+1) \in I_m \setminus \{0, 1, \ldots, \varphi(n)\}$$

Ainsi, φ est strictement croissante et $\nu \circ \varphi \equiv m$: ce qu'on voulait.

Etudions maintenant le cas où ν n'est pas majorée, i.e. le cas où :

$$\forall M \in \mathbf{R}\ \exists m \in \mathbf{N} \qquad \nu(m) > M$$

On peut alors construire par récurrence $\varphi : \mathbf{N} \to \mathbf{N}$ telle que $\varphi(0) = 0$ et :

$$\forall n \in \mathbf{N} \qquad \nu(\varphi(n+1)) > \max_{k=0}^{\varphi(n)} \nu(k)$$

Ainsi φ et $\nu \circ \varphi$ sont strictement croissantes : ce qu'on voulait. ■

Lemme 21 *Soit* $(\nu_{\mathtt{a}})_{\mathtt{a} \in \mathtt{A}} \in \left(\mathbf{N}^{\mathbf{N}}\right)^{\mathtt{A}}$.

Alors, il existe $\varphi : \mathbf{N} \to \mathbf{N}$ *strictement croissante telle que pour tout* $\mathtt{a} \in \mathtt{A}$, $\nu_{\mathtt{a}} \circ \varphi$ *soit strictement croissante ou constante.*

Preuve : On procède par récurrence sur $\# \mathtt{A}$.

Si $\# \mathtt{A} = 1$ il suffit d'appliquer le lemme 20. Supposons maintenant $\# \mathtt{A} \geq 2$.

Fixons $\mathtt{a}_0 \in \mathtt{A}$.

D'une part, en appliquant le lemme 20 à $\nu_{\mathtt{a}_0}$, on obtient $\varphi_0 : \mathbf{N} \to \mathbf{N}$ strictement croissante telle que $\nu_{\mathtt{a}_0} \circ \varphi_0$ soit strictement croissante ou constante.

D'autre part, en appliquant l'hypothèse de récurrence à la famille $(\nu_{\mathtt{a}} \circ \varphi_0)_{\mathtt{a} \in \mathtt{A} \setminus \{\mathtt{a}_0\}}$ on obtient $\varphi_1 : \mathbf{N} \to \mathbf{N}$ strictement croissante telle que pour tout $\mathtt{a} \in \mathtt{A} \setminus \{\mathtt{a}_0\}$, $\nu_{\mathtt{a}} \circ \varphi_0 \circ \varphi_1$ soit strictement croissante ou constante.

Posant $\varphi := \varphi_0 \circ \varphi_1$, on voit que φ est strictement croissante et que pour tout $\mathtt{a} \in \mathtt{A}$, $\nu_{\mathtt{a}} \circ \varphi$ est strictement croissante ou constante : ce qu'on voulait. ■

5.2 Le théorème de Cobham

Le théorème suivant, but de ce chapitre, est dû à Cobham [2].

Théorème 22 (Cobham) *Soient* $f \in \hom(\mathtt{A}^\star)$, $g \in \hom(\mathtt{A}^\star, \mathtt{B}^\star)$ *et* $\mathtt{u}_0 \in \mathtt{A}$ *tels que* f *soit prolongeable sur* $\mathtt{u}_0$ *et* $g\left(f^\omega(\mathtt{u}_0)\right)$ *soit infini.*

Alors, il existe un alphabet $\tilde{\mathtt{A}}$, $\tilde{\mathtt{u}}_0 \in \tilde{\mathtt{A}}$, $\tilde{f} \in \hom\left(\tilde{\mathtt{A}}^\star\right)$ non effaçant *et* $\tilde{g} \in \hom\left(\tilde{\mathtt{A}}^\star, \mathtt{B}^\star\right)$ lettre à lettre *tels que* $\tilde{f}$ *soit prolongeable sur* $\tilde{\mathtt{u}}_0$ *et* $\tilde{g}\left(\tilde{f}^\omega(\tilde{\mathtt{u}}_0)\right) = g\left(f^\omega(\mathtt{u}_0)\right)$.

Preuve : Posons $u := f^\omega(\mathtt{u}_0)$ et $v := g\,(u)$.

Lemme 23 *Il existe* $p \in \mathbf{N}^*$ *et* $q \in \mathbf{N}$ *tels que :*

$$\begin{array}{lrcl} \forall \mathtt{a} \in \mathtt{A} & \left|(g \circ f^q)\left(f^p(\mathtt{a})\right)\right| & \geq & \left|(g \circ f^q)(\mathtt{a})\right| \\ & \left|(g \circ f^q)\left(f^p(\mathtt{u}_0)\right)\right| & > & \left|(g \circ f^q)(\mathtt{u}_0)\right| \end{array}$$

Preuve : Soit :

$$\begin{array}{rccl} \nu_{\mathtt{a}} : & \mathbf{N} & \longrightarrow & \mathbf{N} \\ & n & \longmapsto & \left|g\left(f^n(\mathtt{a})\right)\right| \end{array}$$

pour tout $\mathtt{a} \in \mathtt{A}$. Par le lemme 21, il existe $\varphi : \mathbf{N} \to \mathbf{N}$ tel que pour tout $\mathtt{a} \in \mathtt{A}$, $\nu_{\mathtt{a}} \circ \varphi$ soit strictement croissante ou constante.

Posant $p := \varphi(1) - \varphi(0)$ et $q := \varphi(0)$, on a pour tout $\mathtt{a} \in \mathtt{A}$:

$$\left|(g \circ f^q)\left(f^p(\mathtt{a})\right)\right| = \nu_{\mathtt{a}}(\varphi(1)) \geq \nu_{\mathtt{a}}(\varphi(0)) = \left|(g \circ f^q)(\mathtt{a})\right| \tag{5.2}$$

De plus, lorsque $n \to \infty$, $f^n(\mathtt{u}_0) \to u$ donc $g\left(f^n(\mathtt{u}_0)\right) \to v$ et par suite $\nu_{\mathtt{u}_0}(n) \to \infty$. Ceci force $\nu_{\mathtt{u}_0} \circ \varphi$ à être strictement croissante. Ainsi, l'inégalité (5.2) est stricte dès que $\mathtt{a} = \mathtt{u}_0$. ∎

Dans toute la suite, on suppose avoir remplacé f par f^p (ce qui ne change ni u ni la prolongeabilité de f sur $\mathtt{u}_0$) et g par $g \circ f^q$ (ce qui ne change pas v donc ne nuit pas à la généralité).

On note :

$$\tilde{\mathtt{A}} := \{(\mathtt{a}, j) \in \mathtt{A} \times \mathbf{N} : 1 \leq j \leq |g(\mathtt{a})|\}$$

et :

$$\tilde{\mathtt{u}}_0 := (\mathtt{u}_0, 1)$$

On définit $\alpha \in \hom\left(\mathtt{A}^\star, \tilde{\mathtt{A}}^\star\right)$ et $\tilde{g} \in \hom\left(\tilde{\mathtt{A}}^\star, \mathtt{B}^\star\right)$ par :

$$\forall \mathtt{a} \in \mathtt{A} \qquad \alpha(\mathtt{a}) = (\mathtt{a}, 1)(\mathtt{a}, 2)\ldots(\mathtt{a}, |g(\mathtt{a})|)$$

avec la convention que $\alpha(\mathtt{a}) = \varepsilon$ dès que $g(\mathtt{a}) = \varepsilon$ et :

$$\forall (\mathtt{a}, j) \in \tilde{\mathtt{A}} \qquad \tilde{g}(\mathtt{a}, j) = \text{la } j\text{-ème lettre de } g(\mathtt{a})$$

Par construction, $\tilde{g}$ est lettre à lettre et :

$$\tilde{g} \circ \alpha = g \tag{5.3}$$

Lemme 24 *Il existe $\tilde{f} \in \hom\left(\tilde{\mathtt{A}}^\star\right)$ non effaçant, prolongeable sur $\tilde{\mathtt{u}}_0$ et tel que $\tilde{f} \circ \alpha = \alpha \circ f$.*

Preuve : Pour tout $\mathtt{a} \in \mathtt{A}$, on a $|\alpha(\mathtt{a})| = |g(\mathtt{a})|$ donc pour tout $w \in \mathtt{A}^\star$, $|\alpha(w)| = |g(w)|$. Compte tenu des changements effectués sur f et g, il vient :

$$|\alpha(f(\mathtt{a}))| = |g(f(\mathtt{a}))| \quad \geq \quad |g(\mathtt{a})| \tag{5.4}$$

$$|\alpha(f(\mathtt{u}_0))| = |g(f(\mathtt{u}_0))| \quad > \quad |g(\mathtt{u}_0)| \tag{5.5}$$

L'inégalité (5.4) garantit que, pour tout $\mathtt{a} \in \mathtt{A}$ tel que $g(\mathtt{a}) \neq \varepsilon$, il existe $w_{\mathtt{a},1}$, $w_{\mathtt{a},2}$, …, $w_{\mathtt{a},|g(\mathtt{a})|} \in \tilde{\mathtt{A}}^+$ tels que :

$$\alpha(f(\mathtt{a})) = w_{\mathtt{a},1} w_{\mathtt{a},2} \ldots w_{\mathtt{a},|g(\mathtt{a})|}$$

et l'inégalité (5.5) garantit que l'on peut supposer $|w_{\mathtt{u}_0,1}| \geq 2$, i.e. $w_{\mathtt{u}_0,1} \in \tilde{\mathtt{u}}_0 \tilde{\mathtt{A}}^+$ car $f(\mathtt{u}_0)$ commence par $\mathtt{u}_0$ donc $\alpha(f(\mathtt{u}_0))$ commence par $\alpha(\mathtt{u}_0)$ qui lui-même commence par $\tilde{\mathtt{u}}_0$.

On peut maintenant définir $\tilde{f}$ en posant $\tilde{f}(\mathtt{a}, j) := w_{\mathtt{a},j}$ pour tout $(\mathtt{a}, j) \in \tilde{\mathtt{A}}$: $\tilde{f}$ est bien non effaçant, prolongeable sur $\tilde{\mathtt{u}}_0$ et $\tilde{f} \circ \alpha = \alpha \circ f$. ∎

Soit $n \in \mathbf{N}$. En appliquant plusieurs fois le lemme 24, on obtient $\tilde{f}^n \circ \alpha = \alpha \circ f^n$ donc, par (5.3), $\tilde{g} \circ \tilde{f}^n \circ \alpha = g \circ f^n$ et par suite :

$$\tilde{g}\left(\tilde{f}^n(\alpha(\mathtt{u}_0))\right) = g\left(f^n(\mathtt{u}_0)\right) \tag{5.6}$$

Or, $\tilde{f}^n(\tilde{\mathtt{u}}_0)$ est préfixe de $\tilde{f}^n(\alpha(\mathtt{u}_0))$ et $\tilde{f}^\omega(\tilde{\mathtt{u}}_0)$ est infini car $\tilde{f}$ est prolongeable sur $\tilde{\mathtt{u}}_0$ et non effaçant. Ainsi, en faisant $n \to \infty$, on a $\tilde{f}^n(\alpha(\mathtt{u}_0)) \to \tilde{f}^\omega(\tilde{\mathtt{u}}_0)$, d'où (5.6) devient :

$$\tilde{g}\left(\tilde{f}^\omega(\tilde{\mathtt{u}}_0)\right) = v$$

ce qu'on voulait. ■

5.3 Un exemple d'application

Dans la preuve du théorème de Cobham on construit de manière *effective*, $\tilde{\mathtt{A}}$, $\tilde{\mathtt{u}}_0$, $\tilde{f}$ et $\tilde{g}$. On va appliquer la méthode décrite sur un exemple.

On prend $\mathtt{A} = \mathtt{B} = \{\mathtt{0}, \mathtt{1}, \mathtt{2}\}$, $\mathtt{u}_0 = \mathtt{0}$, pour g l'identité et :

$$f: \begin{array}{lcl} \mathtt{0} & \longmapsto & \mathtt{01} \\ \mathtt{1} & \longmapsto & \mathtt{202} \\ \mathtt{2} & \longmapsto & \varepsilon \end{array}$$

On calcule que :

a	$g(f(\mathtt{a}))$	$g(f^2(\mathtt{a}))$	$g(f^3(\mathtt{a}))$
0	01	01202	0120201
1	202	01	01202
2	ε	ε	ε

donc $p := 1$ et $q := 2$ conviennent. On remplace donc g par :

$$g: \begin{array}{lcl} \mathtt{0} & \longmapsto & \mathtt{01202} \\ \mathtt{1} & \longmapsto & \mathtt{01} \\ \mathtt{2} & \longmapsto & \varepsilon \end{array}$$

et on ne change pas f. Ainsi (pour mémoire), on a :

$$\begin{array}{rcl} \tilde{\mathtt{A}} & = & \{(\mathtt{0},1),\ldots,(\mathtt{0},5),(\mathtt{1},1),(\mathtt{1},2)\} \\ \tilde{\mathtt{u}}_0 & = & (\mathtt{0},1) \\ \alpha(\mathtt{0}) & = & (\mathtt{0},1)\ldots(\mathtt{0},5) \\ \alpha(\mathtt{1}) & = & (\mathtt{1},1)(\mathtt{1},2) \\ (\tilde{g}(\mathtt{0},1),\ldots,\tilde{g}(\mathtt{0},5)) & = & (\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{0},\mathtt{2}) \\ (\tilde{g}(\mathtt{1},1),\tilde{g}(\mathtt{1},2)) & = & (\mathtt{0},\mathtt{1}) \end{array}$$

On définit alors $\tilde{f}$ en prenant (par exemple) :

$$\begin{array}{rcl} \alpha(f(\mathtt{0})) & = & \overbrace{(\mathtt{0},1)(\mathtt{0},2)}^{\tilde{f}(\mathtt{0},1)}\overbrace{(\mathtt{0},3)(\mathtt{0},4)}^{\tilde{f}(\mathtt{0},2)}\overbrace{(\mathtt{0},5)}^{\tilde{f}(\mathtt{0},3)}\overbrace{(\mathtt{1},1)}^{\tilde{f}(\mathtt{0},4)}\overbrace{(\mathtt{1},2)}^{\tilde{f}(\mathtt{0},5)} \\ \alpha(f(\mathtt{1})) & = & \overbrace{(\mathtt{0},1)(\mathtt{0},2)(\mathtt{0},3)}^{\tilde{f}(\mathtt{1},1)}\overbrace{(\mathtt{0},4)(\mathtt{0},5)}^{\tilde{f}(\mathtt{1},2)} \end{array}$$

Chapitre 6

Exemples et contre-exemples

On démontre dans ce chapitre que les inclusions PD0L $\subseteq$ D0L et D0L $\subseteq$ HD0L sont strictes grâce à deux contre-exemples. Pour construire ces deux contre-exemples, on va tout d'abord construire un mot substitutif très particulier, le mot de Thue-Morse [10], qui va avoir la propriété d'être sans facteurs cubiques non vides.

6.1 Le mot de Thue-Morse

Les résultats démontrés dans cette section se trouvent aussi dans [6].

Définition 25 (Chevauchement) *Soient* $\mathtt{A}$ *un alphabet et* $w \in \mathtt{A}^\infty$.

On dit que w *est* sans chevauchement *lorsque :*

$$\forall x \in \mathtt{A}^\star\ \forall \mathtt{a} \in \mathtt{A} \qquad \mathtt{a}x\mathtt{a}x\mathtt{a} \notin \mathtt{F}(w)$$

Proposition 26 *Un mot fini est sans chevauchement si et seulement s'il en est de même pour son image miroir.*

Preuve : Evidente ! ■

Pour tout $w \in \{\mathtt{0},\mathtt{1}\}^\star$, on note $\bar{w}$ l'image de w par l'endomorphisme :

$$\begin{array}{ccc} \{\mathtt{0},\mathtt{1}\}^\star & \longrightarrow & \{\mathtt{0},\mathtt{1}\}^\star \\ \mathtt{0} & \longmapsto & \mathtt{1} \\ \mathtt{1} & \longmapsto & \mathtt{0} \end{array}$$

Définition 27 (Substitution de Thue-Morse) *On appelle* substitution de Thue-Morse *l'endomorphisme* μ *de* $\{\mathtt{0},\mathtt{1}\}^\star$ *donné par* $\mu(\mathtt{a}) := \mathtt{a}\bar{\mathtt{a}}$ *pour* $\mathtt{a} \in \{\mathtt{0},\mathtt{1}\}$.

Proposition 28

$$\forall w \in \{\mathtt{0},\mathtt{1}\}^\star \qquad \mu(\overleftarrow{w}) = \overleftarrow{\mu(w)}$$

Preuve : On procède par récurrence sur $|w|$.

Si $|w| = 0$ alors $\mu(\overleftarrow{w}) = \varepsilon = \overleftarrow{\mu(w)}$ donc tout va bien.

Supposons maintenant $|w| \geq 1$. On peut alors écrire $w = \mathtt{a}v$ avec $v \in \{\mathtt{0},\mathtt{1}\}^\star$ et $\mathtt{a} \in \{\mathtt{0},\mathtt{1}\}$:

- $\overleftarrow{w} = \mathtt{a}\overleftarrow{v}$ (immédiat),
- $\mu(\overleftarrow{v}) = \overleftarrow{\mu(v)}$ (hypothèse de récurrence),
- $\mu(\mathtt{a}) = \overleftarrow{\mu(\mathtt{a})}$ (immédiat)

d'où :

$$\overleftarrow{\mu(w)} = \overleftarrow{\overline{\mu(v)}\,\overline{\mu(\mathtt{a})}} = \overleftarrow{\mu(\mathtt{a})}\,\overleftarrow{\mu(v)} = \mu(\mathtt{a})\mu(\overleftarrow{v}) = \mu(\mathtt{a}\overleftarrow{v}) = \mu(\overleftarrow{w})$$

ce qu'on voulait. ■

Lemme 29

$$\forall w \in \{\mathtt{0},\mathtt{1}\}^\star \;\; \forall \mathtt{a} \in \{\mathtt{0},\mathtt{1}\} \qquad \{w, \mathtt{a}w\mathtt{a}\} \nsubseteq \{\mathtt{01},\mathtt{10}\}^\star$$

Preuve : On procède par récurrence sur $|w|$.

Si $|w| = 0$ alors $\mathtt{a}w\mathtt{a} = \mathtt{aa} \notin \{\mathtt{01},\mathtt{10}\}^\star$ donc tout va bien.

Si $|w| = 1$ alors $w \notin \{\mathtt{01},\mathtt{10}\}^\star$ donc tout va bien aussi.

Supposons maintenant (absurde) qu'il existe $w \in \{\mathtt{0},\mathtt{1}\}^\star$ avec $|w| \geq 2$ tel que $\{w, \mathtt{a}w\mathtt{a}\} \subseteq \{\mathtt{01},\mathtt{10}\}^\star$. On peut alors écrire $w = \mathtt{a}_1 v \mathtt{a}_2$ avec $v \in \{\mathtt{0},\mathtt{1}\}^\star$ et $\mathtt{a}_1$, $\mathtt{a}_2 \in \{\mathtt{0},\mathtt{1}\}$.

Comme $\mathtt{aa}_1 v \mathtt{a}_2\mathtt{a} = \mathtt{a}w\mathtt{a} \in \{\mathtt{01},\mathtt{10}\}^\star$ on a :

- $\{\mathtt{aa}_1, \mathtt{a}_2\mathtt{a}\} \subseteq \{\mathtt{01},\mathtt{10}\}$ donc $\mathtt{a}_1 = \mathtt{a}_2 = \bar{\mathtt{a}}$,
- $v \in \{\mathtt{01},\mathtt{10}\}^\star$.

On a ainsi $|v| < |w|$ et $\{v, \bar{\mathtt{a}}v\bar{\mathtt{a}}\} = \{v, w\} \subseteq \{\mathtt{01},\mathtt{10}\}^\star$ ce qui contredit l'hypothèse de récurrence. ■

Théorème 30 *Pour tout $w \in \{\mathtt{0},\mathtt{1}\}^\star$ sans chevauchement, $\mu(w)$ est sans chevauchement.*

Preuve : Comme $\{\mathtt{01},\mathtt{10}\}$ est un code sur $\{\mathtt{0},\mathtt{1}\}^\star$, on peut définir $\mu^- \in \hom\left(\{\mathtt{01},\mathtt{10}\}^\star, \{\mathtt{0},\mathtt{1}\}^\star\right)$ en posant $\mu^-(\mathtt{a}\bar{\mathtt{a}}) := \mathtt{a}$ pour tout $\mathtt{a} \in \{\mathtt{0},\mathtt{1}\}$ et par construction, on a $\mu^-(\mu(w)) = w$ pour tout $w \in \{\mathtt{0},\mathtt{1}\}^\star$.

Soit $w \in \{\mathtt{0},\mathtt{1}\}^\star$ tel que $\mu(w)$ ne soit pas sans chevauchement : il existe $\mathtt{a} \in \{\mathtt{0},\mathtt{1}\}$ et u, x, $v \in \{\mathtt{0},\mathtt{1}\}^\star$ tels que $\mu(w) = u\mathtt{a}x\mathtt{a}x\mathtt{a}v$. Il s'agit de montrer que w n'est pas sans chevauchement.

Lemme 31 *Les entiers $|u|$ et $|v|$ sont de parités distinctes.*

Preuve : On a :

$$|u| + |v| + 2\,|x| + 3 = |\mu(w)| = 2\,|w|$$

donc :

$$|u| + |v| = 2(|w| - |x| - 2) + 1 \in 2\mathbf{N} + 1$$

ce qui donne le résultat. ■

Pour montrer que w n'est pas sans chevauchement, il suffit de montrer que $\overleftarrow{\overline{w}}$ n'est pas sans chevauchement (proposition 26). Or, par la proposition 28 :

$$\mu(\overleftarrow{\overline{w}}) = \overline{\overleftarrow{v}}\,\bar{\mathtt{a}}\,\overline{\overleftarrow{x}}\,\bar{\mathtt{a}}\,\overline{\overleftarrow{x}}\,\bar{\mathtt{a}}\,\overline{\overleftarrow{u}}$$

donc montrer que $\overleftarrow{\overline{w}}$ n'est pas sans chevauchement revient à montrer que w contient un chevauchement en changeant $(u, \mathtt{a}, x, v)$ en $\left(\overline{\overleftarrow{v}}, \bar{\mathtt{a}}, \overline{\overleftarrow{x}}, \overline{\overleftarrow{u}}\right)$.

Ainsi, comme $\left|\overline{\overleftarrow{v}}\right| = |v|$, le lemme 31 permet de supposer que dans la suite on a $|u| \in 2\mathbf{N}$ et $|v| \in 2\mathbf{N}+1$.

Lemme 32 *L'entier $|x|$ est impair.*

Preuve : Supposons (absurde) que $|x| \in 2\mathbf{N}$.

Alors, on a :

$$\{|u|, |\mathtt{a}x\mathtt{a}|, |x|, |\mathtt{a}v|\} \subseteq 2\mathbf{N}$$

donc, comme :

$$u(\mathtt{a}x\mathtt{a})x(\mathtt{a}v) = \mu(w) \in \{\mathtt{01}, \mathtt{10}\}^\star$$

on a :

$$\{\mathtt{a}x\mathtt{a}, x\} \subseteq \{u, \mathtt{a}x\mathtt{a}, x, \mathtt{a}v\} \subseteq \{\mathtt{01}, \mathtt{10}\}^\star$$

ce qui contredit le lemme 29. ■

Le lemme 32 donne :

$$\{|u|, |\mathtt{a}x|, |\mathtt{a}v|\} \subseteq 2\mathbf{N}$$

donc, comme :

$$u(\mathtt{a}x)(\mathtt{a}x)(\mathtt{a}v) = \mu(w) \in \{\mathtt{01}, \mathtt{10}\}^\star$$

il vient :

$$\{u, \mathtt{a}x, \mathtt{a}v\} \subseteq \{\mathtt{01}, \mathtt{10}\}^\star$$

De plus, $\mu^-(\mathtt{a}x) = \mathtt{a}y$ et $\mu^-(\mathtt{a}v) = \mathtt{a}v'$ avec y, $v' \in \{\mathtt{0}, \mathtt{1}\}^\star$. On peut ainsi, écrire :

$$w = \mu^-(\mu(w)) = \mu^-(u)\mu^-(\mathtt{a}x)\mu^-(\mathtt{a}x)\mu^-(\mathtt{a}v) = u'\mathtt{a}y\mathtt{a}y\mathtt{a}v'$$

avec $u' := \mu^-(u)$ donc w contient un chevauchement. ■

Définition 33 (Mot de Thue-Morse) *On appelle* mot de Thue-Morse*, le mot infini $t := \mu^\omega(\mathtt{0})$.*

Théorème 34 *Le mot de* Thue-Morse *est sans chevauchement.*

Preuve : Le théorème 30 permet de montrer par récurrence que pour tout $n \in \mathbf{N}$, $\mu^n(\mathtt{0})$ est sans chevauchement.

Comme tout facteur de t est facteur d'un $\mu^N(\mathtt{0})$ pour $N \in \mathbf{N}$ assez grand, on obtient que t est sans chevauchement. ■

Corollaire 35

$$\forall w \in \{\mathtt{0}, \mathtt{1}\}^+ \qquad w^3 \notin \mathtt{F}(t)$$

Autrement dit, le mot de Thue-Morse est sans cube.

6.2 Applications

6.2.1 Problèmes d'effacement

On va montrer dans cette sous-section que l'inclusion PD0L $\subseteq$ D0L est stricte.

Soit $\tilde{\mu}$ l'endomorphisme :

$$\begin{array}{rccl} \tilde{\mu}: & \{\mathtt{0},\mathtt{1},\mathtt{2}\}^\star & \longrightarrow & \{\mathtt{0},\mathtt{1},\mathtt{2}\}^\star \\ & \mathtt{0} & \longmapsto & \mathtt{01222} \\ & \mathtt{1} & \longmapsto & \mathtt{10222} \\ & \mathtt{2} & \longmapsto & \varepsilon \end{array}$$

On voit que $\tilde{\mu}$ est effaçant et engendre deux mots non vides : $\tilde{\mu}^\omega(\mathtt{0})$ et $\tilde{\mu}^\omega(\mathtt{1})$. On veut montrer qu'aucun de ces deux mots n'est engendré par un endomorphisme *non effaçant*. On pose $\tilde{t} := \tilde{\mu}^\omega(\mathtt{0})$.

Lemme 36

$$\begin{aligned} \{\mathtt{0},\mathtt{1}\}^+ \cap \mathtt{F}(\tilde{t}) &= \{\mathtt{0},\mathtt{1},\mathtt{01},\mathtt{10}\} && (6.1) \\ \{\mathtt{2}\}^+ \cap \mathtt{F}(\tilde{t}) &= \{\mathtt{2},\mathtt{22},\mathtt{222}\} && (6.2) \end{aligned}$$

Preuve : On a $\tilde{t} = \tilde{\mu}(\tilde{t})$ donc $\tilde{t} \in \{\mathtt{01222},\mathtt{10222}\}^\omega$ ce qui fournit le résultat. ■

Lemme 37 *Le mot de* Thue-Morse *est l'image de $\tilde{t}$ par l'endomorphisme :*

$$\begin{array}{rccl} \chi: & \{\mathtt{0},\mathtt{1},\mathtt{2}\}^\star & \longrightarrow & \{\mathtt{0},\mathtt{1},\mathtt{2}\}^\star \\ & \mathtt{0} & \longmapsto & \mathtt{0} \\ & \mathtt{1} & \longmapsto & \mathtt{1} \\ & \mathtt{2} & \longmapsto & \varepsilon \end{array}$$

Preuve : On a :

$$\mu \circ \chi = \chi \circ \tilde{\mu}$$

donc par récurrence :

$$\forall n \in \mathbf{N} \qquad \mu^n \circ \chi = \chi \circ \tilde{\mu}^n$$

puis en appliquant les deux membres à $\mathtt{0}$, on obtient :

$$\forall n \in \mathbf{N} \qquad \mu^n(\mathtt{0}) = \chi(\tilde{\mu}^n(\mathtt{0}))$$

et enfin, en faisant $n \to \infty$, il vient :

$$t = \chi(\tilde{t})$$

■

En particulier, $\tilde{t}$ est infini.

Lemme 38

$$\{w^3\}_{w\in\{\mathtt{0},\mathtt{1},\mathtt{2}\}^+} \cap \mathtt{F}(\tilde{t}) = \{\mathtt{222}\}$$

Preuve : Pour tout $w \in \{\mathtt{0},\mathtt{1},\mathtt{2}\}^+$ tel que $w^3 \in \mathtt{F}(\tilde{t})$, on a :

$$\chi(w)^3 = \chi(w^3) \in \mathtt{F}(\chi(\tilde{t})) = \mathtt{F}(t)$$

donc, par le corollaire 35, $\chi(w)^3 = \varepsilon$ i.e. $w \in \{\mathtt{2}\}^+$. Ainsi, (6.2) force $w^3 = \mathtt{222}$: ce qu'on voulait. ■

Théorème 39 (Cassaigne) *Les mots infinis $\tilde{\mu}^\omega(\mathtt{0})$ et $\tilde{\mu}^\omega(\mathtt{1})$ ne sont engendrés par aucun endomorphisme non effaçant.*

Preuve : Supposons (absurde) qu'il existe $f \in \hom(\{\mathtt{0},\mathtt{1},\mathtt{2}\}^\star)$ non effaçant et engendrant $\tilde{t}$.

Tout d'abord, $\tilde{\mu}(\mathtt{0}) = \mathtt{01}$ et $f(\mathtt{0})$ sont préfixes de $\tilde{t}$ et comme $f^\omega(\mathtt{0}) = \tilde{t}$ est infini, on a $|f(\mathtt{0})| \geq 2$ d'où :

$$\mathtt{01} \textit{ est préfixe de } f(\mathtt{0}) \tag{6.3}$$

Or, on calcule que :

$$\tilde{\mu}^2(\mathtt{0}) = \mathtt{0122210222}$$

est préfixe de $\tilde{t}$ donc en particulier $f(\mathtt{2})^3 = f(\mathtt{222})$ $(\neq \varepsilon)$ est facteur de $f(\tilde{t}) = \tilde{t}$ et par suite, le lemme 38 force $f(\mathtt{2}) = \mathtt{2}$. Ainsi :

$$f(\mathtt{0})\underbrace{f(\mathtt{1})\mathtt{222}}\underbrace{f(\mathtt{1})f(\mathtt{0})}\mathtt{222} = f\left(\tilde{\mu}^2(\mathtt{0})\right)$$

est préfixe de $\tilde{t}$. Ceci garantit que :

– $f(\mathtt{1})\mathtt{222}$ est facteur de $\tilde{t}$ donc, par (6.2) :

$$\textit{la dernière lettre de } f(\mathtt{1}) \textit{ est } \mathtt{0} \textit{ ou } \mathtt{1} \tag{6.4}$$

– $f(\mathtt{1})f(\mathtt{0})$ est facteur de $\tilde{t}$ donc (6.3) et (6.4) forcent $\mathtt{001}$ ou $\mathtt{101}$ à être facteurs de $\tilde{t}$.

On débouche ainsi sur une contradiction avec (6.1). On démontre de même que $\tilde{\mu}^\omega(\mathtt{1})$ n'est engendré par aucun endomorphisme non effaçant. ■

6.2.2 Images de mots substitutifs par des morphismes

On va montrer dans cette sous-section que l'inclusion D0L $\subseteq$ HD0L est stricte.

Lemme 40 *Soient $x \in \{\mathtt{0},\mathtt{1}\}^\star$, $y \in \{\mathtt{0},\mathtt{1}\}^\infty$ et $\mathtt{a} \in \{\mathtt{0},\mathtt{1}\}$.*

Alors, on a :

$$x\mathtt{a}\bar{\mathtt{a}}y \in \{\mathtt{00},\mathtt{11}\}^\infty \iff \{x\mathtt{a}, \bar{\mathtt{a}}y\} \subseteq \{\mathtt{00},\mathtt{11}\}^\infty$$

Preuve : L'implication $\Longleftarrow$ est triviale.

Réciproquement, supposons que $x\mathtt{a}\bar{\mathtt{a}}y \in \{\mathtt{00},\mathtt{11}\}^\infty$.

Si (absurde) $|x|$ était pair alors $x\mathtt{a}\bar{\mathtt{a}}$ serait un préfixe de longueur paire d'un élément de $\{\mathtt{00},\mathtt{11}\}^\infty$ d'où $x\mathtt{a}\bar{\mathtt{a}}$ serait dans $\{\mathtt{00},\mathtt{11}\}^\infty$: contradition.

On en déduit que que $|x|$ est impair donc $x\mathtt{a}$ est un préfixe de longueur paire d'un élément de $\{\mathtt{00},\mathtt{11}\}^\infty$. Il s'en suit que $x\mathtt{a} \in \{\mathtt{00},\mathtt{11}\}^\star$ puis que $\bar{\mathtt{a}}y \in \{\mathtt{00},\mathtt{11}\}^\infty$.

On a ainsi démontré $\Longrightarrow$. ■

Contre-exemple 41 (Cassaigne) *L'image du mot de* Thue-Morse *par le morphisme :*

$$\begin{array}{rccc} q: & \{\mathtt{0},\mathtt{1}\}^\star & \longrightarrow & \{\mathtt{00},\mathtt{11}\}^\star \\ & \mathtt{0} & \longmapsto & \mathtt{00} \\ & \mathtt{1} & \longmapsto & \mathtt{11} \end{array}$$

n'est engendrée par aucun endomorphisme.

Preuve : Supposons (absurde) que $q(t)$ soit engendré par un $f \in \hom\left(\{\mathtt{0},\mathtt{1}\}^\star\right)$.

Lemme 42 *Il existe $s \in \{\mathtt{0},\mathtt{1}\}^\star$ tel que $f(\mathtt{0}) = \mathtt{001}s$.*

Preuve : Comme $\mathtt{01} = \mu(\mathtt{0})$ est préfixe de t, $\mathtt{0011} = q(\mu(\mathtt{0}))$ est préfixe de $q(t)$. Or, $f(\mathtt{0})$ est également préfixe de $q(t)$.

Ainsi, si on avait $|f(\mathtt{0})| \leq 2$ alors on aurait $f(\mathtt{0}) \in \{\varepsilon, \mathtt{0}, \mathtt{00}\}$ d'où $q(t) = f^\omega(\mathtt{0}) \in \{\varepsilon, \mathtt{0}, \mathtt{0}^\omega\}$ ce qui ne se peut pas.

On en déduit $|f(\mathtt{0})| \geq 3$ donc $\mathtt{001}$ est préfixe de $f(\mathtt{0})$: ce qu'on voulait. ■

Soient $u \in \{\mathtt{0},\mathtt{1}\}^\omega$ tel que $t = \mathtt{0}u$, $v = f(q(\mu^3(u)))$ et $w := \mathtt{0011110011}$:

$$\begin{array}{rcl} q(t) & = & f(q(\mu^3(t))) \\ & = & f(q(\mu^3(\mathtt{0})))v \\ & = & f(w\mathtt{000011})v \\ & = & f(w)f(\mathtt{0})^4 f(\mathtt{11})v \\ & = & f(w)\left(\mathtt{001}s\right)^4 f(\mathtt{11})v \\ & = & f(w)\mathtt{00}\left(\mathtt{1}s\mathtt{00}\right)^3 \mathtt{1}s f(\mathtt{11})v \end{array}$$

Comme $q(t) \in \{\mathtt{00},\mathtt{11}\}^\omega$, on obtient successivement, en appliquant plusieurs fois le lemme 40 que $f(w)\mathtt{00}$, $\mathtt{1}sf(\mathtt{11})v$, $f(w)\mathtt{00}\left(\mathtt{1}s\mathtt{00}\right)^3$ et $\mathtt{1}s\mathtt{00}$ sont dans $\{\mathtt{00},\mathtt{11}\}^\star$.

Remarquant que q est bijectif et que $q^{-1} \in \hom\left(\{\mathtt{00},\mathtt{11}\}^\star, \{\mathtt{0},\mathtt{1}\}^\star\right)$, on peut alors écrire :

$$t = q^{-1}(q(t)) = q^{-1}\left(f(w)\mathtt{00}\right) q^{-1}\left(\mathtt{1}s\mathtt{00}\right)^3 q^{-1}\left(\mathtt{1}sf(\mathtt{11})v\right)$$

et la présence de $q^{-1}\left(\mathtt{1}s\mathtt{00}\right)^3$ comme facteur de t contredit le corollaire 35. ■

Troisième partie

Sur la complexité des mots substitutifs

Etant donné un alphabet $\mathtt{A}$, $\mathtt{u}_0 \in \mathtt{A}$ et $f \in \hom(\mathtt{A}^\star)$ prolongeable sur $\mathtt{u}_0$, on cherche à démontrer dans cette partie que lorsque $n \to \infty$, on a $\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \asymp p(n)$ où $p : \mathbf{N} \setminus \{0,1,2\} \to]0,\infty[$ est l'une des cinq fonctions suivantes :

$$\begin{array}{rcl} n & \longmapsto & n^2 \\ n & \longmapsto & n \ln n \\ n & \longmapsto & n \ln \ln n \\ n & \longmapsto & n \\ n & \longmapsto & 1 \end{array}$$

Ce résultat est essentiellement dû à Pansiot [8]. On note $u := f^\omega(\mathtt{u}_0)$ et quitte à restreindre f, on suppose que $\mathtt{A} = \mathtt{F}\left(f^\omega(\mathtt{u}_0)\right)$.

Chapitre 7

Mots croissants

7.1 Mots croissants, endomorphismes croissants

Définition 43 *Soit $w \in \mathtt{A}^\star$.*

On dit que w est croissant *(resp.* borné*) pour f lorsque* $\sup_{n\in\mathbf{N}} |f^n(w)| = \infty$ *(resp. $< \infty$).*

Proposition 44 *Pour tout $w \in \mathtt{A}^\star$, la suite $(f^n(w))_{n\in\mathbf{N}}$ est ultimement périodique* ou $|f^n(w)| \to \infty$ *lorsque $n \to \infty$.*

Preuve : Supposons que $|f^n(w)| \not\to \infty$ lorsque $n \to \infty$.

Ceci signifie qu'on peut trouver $M \in \mathbf{N}$ tel que pour tout $N \in \mathbf{N}$, il existe un entier $n \geq N$ pour lequel on a $|f^n(w)| \leq M$.

Posant :

$$\begin{array}{rcl} F & := & \bigcup_{n=0}^{M} \mathtt{A}^n \\ I & := & \{n \in \mathbf{N} : |f^n(w)| \leq M\} \end{array}$$

on voit que l'application :

$$\begin{array}{rcl} \mathbf{N} & \longrightarrow & \mathtt{A}^\star \\ n & \longmapsto & f^n(w) \end{array}$$

ne peut pas être injective car elle envoie I (infini) dans F (fini). Ainsi, il existe $p, q \in \mathbf{N}$ tels que $p < q$ et $f^p(w) = f^q(w)$.

Ainsi, pour tout $n \in \mathbf{N}$, on a :

$$f^{n+p+(q-p)}(w) = f^{n+q}(w) = f^n\left(f^q(w)\right) = f^n\left(f^p(w)\right) = f^{n+p}(w)$$

donc pour tout entier $n \geq p$, on a $f^{n+(q-p)}(w) = f^n(w)$ ce qui démontre que la suite $(f^n(w))_{n\in\mathbf{N}}$ est ultimement périodique. ■

On tire de la proposition précédente que l'on ne change pas l'ensemble des mots croissants pour f en élevant f à une puissance strictement positive.

Définition 45 (Endomorphismes croissants)

- *On dit que f est* croissant *lorsque :*

$$\forall \mathtt{a} \in \mathtt{A} \qquad \lim_{n\to\infty} |f^n(\mathtt{a})| = \infty$$

- *On dit que f est* strictement croissant *lorsque :*

$$\forall \mathtt{a} \in \mathtt{A} \qquad |f(\mathtt{a})| \geq 2$$

L'endomorphisme f est croissant si et seulement si toutes les lettres appartenant à $\mathtt{A}$ sont croissantes pour f.

Proposition 46

- *Tout endomorphisme strictement croissant est croissant.*
- *Tout endomorphisme croissant de $\mathtt{A}^\star$ élévé à la puissance $\#\mathtt{A}$ est strictement croissant.*

Preuve : Si f est strictement croissant alors, pour tout $w \in \mathtt{A}^\star$, on a $|f(w)| \geq 2\,|w|$ donc par récurrence on a $|f^n(\mathtt{a})| \geq 2^n$ pour tout $\mathtt{a} \in \mathtt{A}$ et tout $n \in \mathbf{N}$: f est bien croissant. On a ainsi prouvé le premier point.

Supposons maintenant f croissant. Notons $N := \#\mathtt{A}$ et fixons $\mathtt{a} \in \mathtt{A}$ quelconque. Comme f est en particulier non effaçant on a :

$$1 = |\mathtt{a}| \leq |f(\mathtt{a})| \leq \left|f^2(\mathtt{a})\right| \leq \cdots \leq \left|f^N(\mathtt{a})\right|$$

Ainsi, si on avait (absurde) $\left|f^N(\mathtt{a})\right| \leq 1$ alors l'application :

$$\begin{array}{ccc} \{0, 1, \dots N\} & \longrightarrow & \mathtt{A}^\star \\ k & \longmapsto & f^k(\mathtt{a}) \end{array}$$

serait à valeurs dans $\mathtt{A}$ donc, pour des raisons de cardinalité, elle ne pourrait pas être injective. Par suite, il existerait i, $j \in \{0, 1, \dots, N\}$ tels que $i < j$ et $f^i(\mathtt{a}) = f^j(\mathtt{a})$. On aurrait ainsi $f^{k(j-i)+i}(\mathtt{a}) = f^i(\mathtt{a})$ pour tout $k \in \mathbf{N}$ donc $f^n(\mathtt{a}) \not\to \infty$ lorsque $n \to \infty$: contradiction.

On en déduit $\left|f^N(\mathtt{a})\right| \geq 2$ et le second point. ■

7.2 Ordre de croissance

Théorème 47 (Berstel) *Soit $w \in \mathtt{A}^\star$ tel que pour tout $n \in \mathbf{N}$, on ait $f^n(w) \neq \varepsilon$.*

Alors, il existe $\alpha \in \mathbf{N}$ et $\beta \in [1, \infty[$ tels que $|f^n(w)| \asymp n^\alpha \beta^n$ lorsque $n \to \infty$.

On admettra la démonstration de ce théorème (plutôt difficile), on la trouvera dans [9] et dans [1].

Pour tout $w \in \mathtt{A}^\star$, on appelle *ordre de croissance* pour f de w la classe d'équivalence de $(|f^n(w)|)_{n\in\mathbf{N}}$ pour la relation $\asymp$.

Définition 48 (Classes d'endomorphismes) *On dit que f est :*

1. quasi-uniforme *lorsqu'il existe* $\beta \in [1, \infty[$ *tel que pour tout* $\mathtt{a} \in \mathtt{A}$ *croissant pour* f*, on ait* $|f^n(\mathtt{a})| \asymp \beta^n$*,*

2. polynômialement divergent *lorsqu'il n'est pas quasi-uniforme et lorsqu'il existe* $\beta \in [1, \infty[$ *tel que pour tout* $\mathtt{a} \in \mathtt{A}$ *croissant pour* f*, il existe* $\alpha_{\mathtt{a}} \in \mathbf{N}$ *vérifiant* $|f^n(\mathtt{a})| \asymp n^{\alpha_{\mathtt{a}}}\beta^n$ *lorsque* $n \to \infty$*,*

3. exponentiellement divergent *lorsqu'il existe* $\mathtt{a}_1$*,* $\mathtt{a}_2 \in \mathtt{A}$ *croissants pour* f*,* β_1*,* $\beta_2 \in [1, \infty[$*, et* α_1*,* $\alpha_2 \in \mathbf{N}$ *vérifiant* $\beta_1 \neq \beta_2$ *et pour* $j \in \{1, 2\}$*,* $|f^n(\mathtt{a}_j)| \asymp n^{\alpha_j}\beta_j^n$ *lorsque* $n \to \infty$*.*

Par définition, tout endomorphisme de $\mathtt{A}^\star$ entre dans l'une des trois classes décrites ci-dessus.

On remarque l'on ne change pas la nature d'un endomorphisme en l'élevant à un puissance positive mais aussi que la classe d'un endomorphisme ne dépend que de sa matrice.

Définition 49 (Module, endomorphisme uniforme) *On appelle* module *de* f *l'entier :*

$$|f| := \max_{\mathtt{a} \in \mathtt{A}} |f(\mathtt{a})|$$

On dit que f *est* uniforme *lorsque :*

$$\forall \mathtt{a} \in \mathtt{A} \qquad |f(\mathtt{a})| = |f|$$

On remarque que pour tout $w \in \mathtt{A}^\star$, on a $|f(w)| \leq |f|\,|w|$ donc pour tout $n \in \mathbf{N}$, on a $|f(w)| \leq |f|^n\,|w|$.

Exemple 50 *Tout endomorphisme uniforme est quasi-uniforme.*

Preuve : Si f est uniforme alors on a :

$$\forall \mathtt{a} \in \mathtt{A}\ \forall n \in \mathbf{N} \qquad |f^n(\mathtt{a})| = |f|^n$$

■

Proposition 51 *Si* f *est croissant alors pour tout* $\mathtt{a} \in \mathtt{A}$*, on a* $|f^n(\mathtt{a})| \asymp n^\alpha\beta^n$ *lorsque* $n \to \infty$ *avec* $\alpha \in \mathbf{N}$ *et* $\beta \in]1, \infty[$*.*

Preuve : Si (absurde) il existait $n_0 \in \mathbf{N}$ tel que $f^{n_0}(\mathtt{a}) = \varepsilon$ alors pour tout entier $n \geq n_0$, on aurait $f^n(\mathtt{a}) = \varepsilon$ et par suite $|f^n(\mathtt{a})| \to 0 \neq \infty$ lorsque $n \to \infty$: contradiction avec l'hypothèse f croissant. Ainsi, par le théorème 47, il existe $\alpha \in \mathbf{N}$ et $\beta \in [1, \infty[$ tels que $|f^n(\mathtt{a})| \asymp n^\alpha\beta^n$ lorsque $n \to \infty$.

Or, par la proposition 46, il existe $N \in \mathbf{N}$ tel que f^N soit strictement croissant.

On en déduit :

$$n^\alpha \left(\beta^N\right)^n \asymp (Nn)^\alpha\beta^{Nn} \asymp \left|f^{Nn}(\mathtt{a})\right| \geq 2^n$$

lorsque $n \to \infty$. Or, ceci n'est possible que si $\beta^N \geq 2$ ce qui force $\beta > 1$. ■

Exemple 52 *L'endomorphisme :*

$$\begin{array}{rccc} f: & \{\mathtt{0},\mathtt{1}\}^\star & \longrightarrow & \{\mathtt{0},\mathtt{1}\}^\star \\ & \mathtt{0} & \longmapsto & \mathtt{0101} \\ & \mathtt{1} & \longmapsto & \mathtt{11} \end{array}$$

est polynômialement divergent.

Preuve : Il est immédiat que :

$$M := \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$$

est une matrice de f et on vérifie facilement par récurrence que :

$$M^n = \begin{pmatrix} 2^n & 0 \\ n2^n & 2^n \end{pmatrix}$$

donc :

$$\begin{aligned} |f^n(\mathtt{0})| &= \begin{pmatrix} 1 & 1 \end{pmatrix} M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (n+1)2^n \\ |f^n(\mathtt{1})| &= \begin{pmatrix} 1 & 1 \end{pmatrix} M^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 2^n \end{aligned}$$

■

Chapitre 8

Endomorphismes croissants

On veut dans ce chapitre montrer le théorème suivant.

Théorème 53 *Si f est croissant et $f^\omega(\mathtt{u}_0)$ non ultimement périodique alors, on a :*

$$\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \asymp \begin{cases} n & \text{si } f \text{ est quasi-uniforme} \\ n \ln\ln n & \text{si } f \text{ est polynômialement divergent} \\ n \ln n & \text{si } f \text{ est exponentiellement divergent} \end{cases}$$

lorsque $n \to \infty$.

8.1 Majoration

Les références pour cette section sont [8], [3] et [4].

Lemme 54 *Soient $\varphi_1,\ \varphi_2 : \mathbf{N}^* \to \mathbf{R}_+^*$ tels que :*

$$\forall k \in \mathbf{N}\ \forall \mathtt{a} \in \mathtt{A} \qquad \varphi_1(k) \leq \left|f^k(\mathtt{a})\right| \leq \varphi_2(k)$$

Alors, lorsque $n \to \infty$, on a :

$$\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \preceq n\,(\#\, I_n)$$

avec $I_n := \{k \in \mathbf{N} : \varphi_1(k) \leq n \leq 2\,|f|\,\varphi_2(k)\}$.

Preuve : Fixons un entier $n \geq 3$. On va montrer que l'image de l'application :

$$\begin{array}{ccc} \mathtt{A} \times \mathtt{A}^{2|f|-1} \times I_n \times \{1, \ldots, n\} & \longrightarrow & \mathtt{A}^\star \\ (\mathtt{a}, s, k, l) & \longmapsto & \left(\underset{l}{\mathtt{suff}}\, f^k(\mathtt{a})\right)\left(\underset{n-l}{\mathtt{pref}}\, f^k(s)\right) \end{array}$$

contient $\mathtt{F}_n(u)$ ce qui démontrera le théorème.

Soit $w \in \mathtt{F}_n(u)$: il existe $K \in \mathbf{N}$ tel que w soit facteur de $f^K(\mathtt{u}_0)$. On construit alors par récurrence une suite $(w_0, w_1, \ldots, w_K)$ d'éléments de $\mathtt{A}^\star$:

– en posant $w_0 := w$,
– en choisissant, pour $j \in \{1, \ldots, K\}$, un facteur w_j de $f^{K-j}(\mathtt{u}_0)$ de longueur minimale tel que w_{j-1} soit facteur de $f(w_j)$.

On a $|w_0| \geq 3$ donc on peut poser :

$$k := \max \{j \in \{0, 1, \ldots, K\} : |w_j| \geq 3\}$$

et comme $w_K = \mathtt{u}_0$, on a $k < K$ ce qui permet d'écrire $|w_k| \geq 3 > 2 \geq |w_{k+1}|$. Par suite, il vient $3 \leq |w_k| \leq |f(w_{k+1})| \leq 2\,|f|$ donc il existe $\mathtt{a}, \mathtt{b} \in \mathtt{A}$ et $s' \in \mathtt{A}^+$ tels que $w_k = \mathtt{ab}s'$ et $s \in \mathtt{A}^{2|f|-1}$ admettant $\mathtt{b}s'$ pour préfixe. On vérifie alors par récurrence que pour tout entier j, $0 \leq j \leq k$:
– $f^j(\mathtt{b})$ est un facteur intérieur de w_{k-j},
– w_{k-j} est la concaténation d'un suffixe non vide de $f^j(\mathtt{a})$ et d'un préfixe non vide de $f^j(s)$.

En particulier, ceci est vrai pour $j = k$ donc $f^k(\mathtt{b})$ est facteur de w lui même facteur de $f^k(w_k)$ et par suite, on a :

$$\varphi_1(k) \leq \left|f^k(\mathtt{b})\right| \leq n \leq \left|f^k(w_k)\right| \leq 2\,|f|\,\varphi_2(k)$$

i.e. $k \in I_n$. De plus, il existe x suffixe non vide de $f^k(\mathtt{a})$ et y préfixe non vide de $f^k(s)$ tels que $w = xy$. Posant $l := |x|$ on a construit un quadruplet $(\mathtt{a}, s, k, l)$ s'envoyant sur w par l'application décrite ci-dessus. ∎

Théorème 55 *Si f est croissant et si $f^\omega(\mathtt{u}_0)$ n'est pas ultimement périodique alors on a :*

$$\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \preceq \begin{cases} n & \text{si } f \text{ est quasi-uniforme} \\ n \ln\ln n & \text{si } f \text{ est polynômialement divergent} \\ n \ln n & \text{si } f \text{ est exponentiellement divergent} \end{cases}$$

lorsque $n \to \infty$.

Preuve : Soit $\mathtt{a}_1$ (resp. $\mathtt{a}_2$) $\in \mathtt{A}$ d'ordre de croissance pour f minimal (resp. maximal). Pour $j \in \{1, 2\}$, soient $\lambda_j \in]0, \infty[$, $\alpha_j \in \mathbf{N}$ et $\beta_j \in [1, \infty[$ tels que $|f^n(\mathtt{a}_j)| \asymp n^{\alpha_j}\beta_j^n$ lorsque $n \to \infty$ et :

$$\begin{array}{rccc} \varphi_j : & \mathbf{N} & \longrightarrow & \mathbf{R}^* \\ & n & \longmapsto & \lambda_j n^{\alpha_j} \beta_j^n \end{array}$$

Quitte à ajuster les constantes λ_1 et λ_2, on peut supposer que φ_1 et φ_2 vérifient les hypothèses permettant d'appliquer l lemme précédent.

Or, par la proposition 51, on a $\beta_j > 1$ donc on peut appliquer la proposition 13 et on obtient le résultat recherché. ∎

8.2 Minorations

Lemme 56 *Soient $w \in \mathtt{A}^\star$, $\alpha \in \mathbf{N}$ et $\beta \in]1, \infty[$ tels que $|f^n(w)| \asymp n^\alpha \beta^n$ lorsque $n \to \infty$.*

Alors, on a :

$$\sum_{k=0}^{n} \left|f^k(w)\right| \asymp n^\alpha \beta^n$$

lorsque $n \to \infty$.

Preuve : Il existe c, $C \in \mathbf{R}_+^*$ tels que :

$$\forall n \in \mathbf{N} \qquad cn^\alpha \beta^n \leq |f^n(w)| \leq Cn^\alpha \beta^n$$

donc on a trivialement :

$$\sum_{k=0}^{n} \left|f^k(w)\right| \geq |f^n(w)| \geq cn^\alpha \beta^n$$

mais aussi :

$$\sum_{k=0}^{n} \left|f^k(w)\right| \leq \sum_{k=0}^{n} Ck^\alpha \beta^k \leq \sum_{k=0}^{n} Cn^\alpha \beta^k = Cn^\alpha \frac{\beta^{n+1}-1}{\beta-1} \leq \frac{C\beta}{\beta-1} n^\alpha \beta^n$$

■

Théorème 57 *Si f est croissant alors, on a :*

$$\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \succeq \begin{cases} n \ln\ln n & \textit{si } f \textit{ est polynômialement divergent} \\ n \ln n & \textit{si } f \textit{ est exponentiellement divergent} \end{cases}$$

lorsque $n \to \infty$.

Preuve : Quitte à élever f à une puissance convenable, on peut, par la proposition 46, supposer f strictement croissant. Soient $\alpha_0 \in \mathbf{N}$ et $\beta_0 \in \,]1, \infty[$ tels que $|f^n(\mathtt{u}_0)| \asymp n^{\alpha_0} \beta_0^n$ lorsque $n \to \infty$.

Soit $\mathtt{C}$ l'ensemble des $\mathtt{a} \in \mathtt{A}$ tels que :

$$|f^n(\mathtt{a})| \succeq \begin{cases} n^{\alpha_0} \beta_0^n & \text{si } f \text{ est polynômialement divergent} \\ \beta_0^n & \text{si } f \text{ est exponentiellement divergent} \end{cases}$$

lorsque $n \to \infty$ et $\mathtt{B} := \mathtt{A} \setminus \mathtt{C}$. On remarque que pour tout $\mathtt{b} \in \mathtt{B}$, $|f^n(b)|$ est négligeable devant $n^{\alpha_0} \beta_0^n$ lorsque $n \to \infty$ et que $\mathtt{B}$ et $\mathtt{C}$ vérifient les conditions $(*)$.

On définit $\chi \in \hom(\mathtt{A}^\star, \{\mathtt{0}, \mathtt{1}\}^\star)$ en posant :

$$\chi(\mathtt{a}) := \begin{cases} \mathtt{1} & \text{si } \mathtt{a} \in \mathtt{C} \\ \mathtt{0} & \text{si } \mathtt{a} \in \mathtt{B} \end{cases}$$

pour tout $\mathtt{a} \in \mathtt{A}$ et $v := \chi(u)$. Pour tout $n \in \mathbf{N}$, on a $\chi(\mathtt{F}_u(u)) = \mathtt{F}_n(v)$ donc $\mathtt{p}_u(n) \geq \mathtt{p}_v(n)$ et par suite il suffit de minorer $\mathtt{p}_v$.

Lemme 58 *Il existe dans u une infinité d'occurences de lettres appartenant à $\mathtt{C}$.*

Preuve : Soit $s \in \mathtt{A}^\star$ tel que $f(\mathtt{u}_0) \in \mathtt{u}_0\mathtt{A}^\star$, $\alpha \in \mathbf{N}$ et $\beta \in]1, \infty[$ tels que $|f^n(s)| \asymp n^\alpha \beta^n$ lorsque $n \to \infty$.

Par la proposition 17, il suffit de montrer que $s \notin \mathtt{B}^\star$.

Pour tout $n \in \mathbf{N}$, on a :

$$f^{n+1}(\mathtt{u}_0) = \mathtt{u}_0 s f(s) f^2(s) \dots f^n(s)$$

donc par le lemme 56, il vient :

$$\left|f^{n+1}(\mathtt{u}_0)\right| = 1 + \sum_{k=0}^{n} \left|f^k(s)\right| \asymp n^\alpha \beta^n \asymp |f^n(s)|$$

lorsque $n \to \infty$. On en déduit qu'au moins une lettre de s est de même ordre croissance pour f que $\mathtt{u}_0$ donc cette lettre est dans $\mathtt{C}$. ∎

Lemme 59 *Il existe dans u une infinité d'occurences de lettres appartenant à* $\mathtt{B}$.

Preuve : Pour tout $n \in \mathbf{N}$ et tout $\mathtt{b} \in \mathtt{B}$, $f^n(\mathtt{b})$ est un facteur de u et $|f^n(\mathtt{b})| \to \infty$ lorsque $n \to \infty$. Ainsi, il suffit de montrer que $\mathtt{B}$ est non vide pour démontrer le lemme. Si f est exponentiellement divergent, c'est par définition. Etudions donc le cas où f est polynômialement divergent.

Supposons (absurde) que $\mathtt{B} = \emptyset$ i.e. que $\mathtt{A} = \mathtt{C}$. On peut alors associer à chaque $\mathtt{a} \in \mathtt{A}$ un réel $c_\mathtt{a} > 0$ tel que pour tout $n \in \mathbf{N}$, on ait $|f^n(\mathtt{a})| \geq c_\mathtt{a} n^{\alpha_0} \beta_0^n$. Ainsi, posant $c := \min_{\mathtt{a} \in \mathtt{A}} c_\mathtt{a}$, on a :

$$\forall \mathtt{a} \in \mathtt{A}\ \forall n \in \mathbf{N} \qquad |f^n(\mathtt{a})| \geq c n^{\alpha_0} \beta_0^n$$

puis :

$$\forall x \in \mathtt{A}^\star\ \forall n \in \mathbf{N} \qquad |f^n(x)| \geq c\,|x|\, n^{\alpha_0} \beta_0^n$$

Fixons alors $\mathtt{a} \in \mathtt{A}$ quelconque. Il existe $N \in \mathbf{N}$ tel que $\mathtt{a}$ apparaisse dans $f^N(\mathtt{u}_0)$ donc pour tout $n \in \mathbf{N}$, $f^n(\mathtt{a})$ est facteur de $f^{N+n}(\mathtt{u}_0)$ et on a :

$$\left|f^{2n}(\mathtt{a})\right| = |f^n\left(f^n(\mathtt{a})\right)| \geq c\,|f^n(\mathtt{a})|\, n^{\alpha_0} \beta_0^n \geq c(cn^{\alpha_0}\beta_0^n) n^{\alpha_0} \beta_0^n = c^2 n^{2\alpha_0} \beta_0^{2n}$$

On en déduit que lorsque $n \to \infty$, on a :

$$n^{2\alpha_0} \beta_0^{2n} \preceq \left|f^{2n}(\mathtt{a})\right| \leq \left|f^{N+2n}(\mathtt{u}_0)\right| \asymp (N+2n)^{\alpha_0} \beta_0^{N+2n} \preceq n^{\alpha_0} \beta_0^{2n}$$

ce qui force $\alpha_0 = 0$ et $\left|f^{2n}(\mathtt{a})\right| \asymp \beta_0^{2n}$. On a ainsi démontré que f^2 était quasi-uniforme : contradiction car f ne l'est pas. ∎

Lemme 60 *Il existe $N \in \mathbf{N}$, $a \in \mathtt{A}^\star$, $b \in \mathtt{B}^+$, b_1, $b_2 \in \mathtt{B}^\star$ et $\mathtt{c}_1$, $\mathtt{c}_2 \in \mathtt{C}$ tels que :*

- $\mathtt{c}_1 b \mathtt{c}_2$ *est facteur de u,*
- $f^N(\mathtt{c}_1) = a \mathtt{c}_1 b_1$,
- $f^N(\mathtt{c}_2) \in b_2 \mathtt{c}_2 \mathtt{A}^\star$.

Preuve : Par les lemmes 58 et 59, il existe $b' \in \mathtt{B}^+$ et $\mathtt{c}_1'$, $\mathtt{c}_2' \in \mathtt{C}$ tels que $\mathtt{c}_1' b' \mathtt{c}_2'$ soit facteur de u. Or, par le lemme 18, il existe $N \in \mathbf{N}$, $a \in \mathtt{A}^\star$, β_1, β_2, b_1, $b_2 \in \mathtt{B}^\star$ et $\mathtt{c}_1$, $\mathtt{c}_2 \in \mathtt{C}$ tels que $f^N(\mathtt{c}_1') \in \mathtt{A}^\star \mathtt{c}_1 \beta_1$, $f^N(\mathtt{c}_1) = a\mathtt{c}_1 b_1$, $f^N(\mathtt{c}_2') \in \beta_2 \mathtt{c}_2 \mathtt{A}^\star$, $f^N(\mathtt{c}_2) \in b_2 \mathtt{c}_2 \mathtt{A}^\star$. Posant $b := \beta_1 f(b') \beta_2$, on voit que $\mathtt{c}_1 b \mathtt{c}_2$ est facteur de $f^N(\mathtt{c}_1' b' \mathtt{c}_2')$ donc de u. ∎

Lemme 61 *Lorsque $n \to \infty$, on a :*

$$\mathtt{r}_v(n) \succeq \begin{cases} \ln \ln n & \textit{si } f \textit{ est polynômialement divergent} \\ \ln n & \textit{si } f \textit{ est exponentiellement divergent} \end{cases}$$

Preuve : Posant $g := f^N$ et $s_k := g^k(a) \dots g^2(a) g(a) a$ on voit que :

$$\underbrace{s_k \mathtt{c}_1 b_1 g(b_1) g^2(b_1) \dots g^k(b_1)}_{g^{k+1}(\mathtt{c}_1)} g^{k+1}(b) g^k(b_2) \dots g^2(b_2) g(b_2) b_2 \mathtt{c}_2$$

est préfixe de $g^{k+1}(\mathtt{c}_1 b \mathtt{c}_2)$ donc facteur de u. Ainsi, posant :

$$\begin{array}{rcl} w_k & := & \chi(s_k) \\ e_k & := & \left| b_1 g(b_1) g^2(b_1) \dots g^k(b_1) g^{k+1}(b) g^k(b_2) \dots g^2(b_2) g(b_2) b_2 \right| \\ & = & \left| g^{k+1}(b) \right| + \displaystyle\sum_{j=0}^{k} \left| g^j(b_1 b_2) \right| \\ \varphi_1(k) & := & 1 + e_k \\ \varphi_2(k) & := & 1 + e_k + |w_k| \end{array}$$

on voit que $w_k \mathtt{1} \mathtt{0}^{e_k} \mathtt{1}$ est facteur de v, que w_k est suffixe de w_{k+1}. De plus, comme f est strictement croissant, la suite $\left(g^{k+1}(b)\right)_k$ est strictement croissante donc il en est de même pour la suite $(e_k)_k$. On peut maintenant appliquer le lemme 7 qui donne :

$$\mathtt{r}_v(n) \geq \# \{ k \in \mathbf{N} : \varphi_1(k) \leq n \leq \varphi_2(k) \}$$

Pour conclure la démonstration de ce lemme, on cherche à appliquer le lemme 13. Or, par le lemme 56, on a :

$$\begin{array}{rcl} \varphi_1(k) & \asymp & \left| g^{k+1}(b) \right| + \left| g^k(b_1 b_2) \right| \\ & = & \left| g^k(g(b) b_1 b_2) \right| \\ \varphi_2(k) & = & g^{k+1}(\mathtt{c}_1) + \left| g^{k+1}(b) \right| + \displaystyle\sum_{j=0}^{k} \left| g^j(b_2) \right| \\ & \asymp & g^k(g(\mathtt{c}_1) g(b) b_2) \end{array}$$

lorsque $k \to \infty$.

On en déduit qu'il existe α_1, $\alpha_2 \in \mathbf{N}$ et β_1, $\beta_2 \in]1, \infty[$ tels que pour tout $j \in \{1, 2\}$, on ait $\varphi_j(k) \asymp k^{\alpha_j} \beta_j^k$ lorsque $k \to \infty$. De plus, comme toutes les lettre de $g(b) b_1 b_2$ sont dans $\mathtt{B}$ et comme $g(\mathtt{c}_1) g(b) b_2$ contient une lettre appartenant à $\mathtt{C}$, on a :

– $\beta_1 = \beta_0 = \beta_2$ et $\alpha_1 < \alpha_0 = \alpha_2$ si f est polynômialement divergent.
– $\beta_1 < \beta_0 = \beta_2$ si f est exponentiellement divergent.

■

La proposition 5, le lemme précédent et la proposition 12 donnent successivement :

$$\mathtt{p}_u(n) \geq \mathtt{p}_v(n) \geq \sum_{k=0}^{n-1} \mathtt{r}_v(n) \geq \sum_{k=0}^{n-1} \ln^k n \succeq n \ln^k n$$

lorsque $n \to \infty$ avec $k = 1$ si f est polynômialement divergent, 2 si f est exponentiellement divergent. ■

Chapitre 9

Mots substitutifs de complexité non quadratique

Notant $\mathtt{B}$ (resp. $\mathtt{C}$) l'ensemble des lettres bornées (resp. croissantes) pour f, on cherche à généraliser le théorème 53 en affaiblissant l'hypothèse "f est croissant" en "$\mathtt{B}^\star \cap \mathtt{F}\,(f^\omega(\mathtt{u}_0))$ est fini". *On suppose donc dans ce chapitre que* $\mathtt{B}^\star \cap \mathtt{F}\,(f^\omega(\mathtt{u}_0))$ *est fini.* Ceci permet de poser :

$$M := \max_{w \in \mathtt{B}^\star \cap \mathtt{F}(u)} |w|$$

On définit $\chi_c \in \hom(\mathtt{A}^\star, \mathtt{C}^\star)$ et $f_c \in \hom(\mathtt{C}^\star)$ en posant :

$$\chi_c(\mathtt{a}) := \begin{cases} \mathtt{a} & \text{si } \mathtt{a} \in \mathtt{C} \\ \varepsilon & \text{sinon} \end{cases}$$

pour tout $\mathtt{a} \in \mathtt{A}$ et :

$$f_c(\mathtt{c}) := \chi_c(f(\mathtt{c}))$$

pour tout $\mathtt{c} \in \mathtt{C}$.

Lemme 62

$$f_c \circ \chi_c = \chi_c \circ f$$

Preuve : Il suffit de montrer que pour tout $\mathtt{a} \in \mathtt{A}$, on a $f_c(\chi_c(\mathtt{a})) = \chi_c(f(\mathtt{a}))$:

- si $\mathtt{a} \in \mathtt{B}$ alors $f(\mathtt{a}) \in \mathtt{B}^\star$ donc $(f_c \circ \chi_c)(\mathtt{a}) = \varepsilon = (\chi_c \circ f)(\mathtt{a})$,
- si $\mathtt{a} \in \mathtt{C}$ alors, $(f_c \circ \chi_c)(\mathtt{a}) = f_c(\mathtt{a}) = (\chi_c \circ f)(\mathtt{a})$.

■

Lemme 63 *Pour tout* $\mathtt{c} \in \mathtt{C}$*, on a* $|f^n(\mathtt{c})| \asymp |f_c^n(\mathtt{c})|$ *lorsque* $n \to \infty$*.*

Preuve : Trivialement, on a :

$$|f^n(\mathtt{c})| \geq |\chi_c\,(f^n(\mathtt{c}))|$$

D'autre part on peut effectuer la division euclidienne de $|f^n(\mathtt{c})|$ par $M+1$. On récolte $(q, r) \in \mathbf{N} \times \mathbf{N}$ tel que $|f^n(\mathtt{c})| = (M+1)q + r$ et $r \leq M$ donc il existe x_1, ..., $x_q \in \mathtt{A}^{M+1}$ et $x_{q+1} \in \mathtt{A}^r$ tels que $f^n(\mathtt{c}) = x_1 \dots x_q x_{q+1}$. Or, pour $j \in \{1, \dots, q\}$, x_j est facteur de $f^n(\mathtt{c})$ qui est lui-même facteur de u donc il est impossible que $x_j \in \mathtt{B}^{M+1}$: on en déduit que x_j contient au moins une lettre de $\mathtt{C}$. Par suite, on a :

$$|\chi_c(f^n(\mathtt{c}))| \geq q = \frac{1}{M+1}|f^n(\mathtt{c})| - \frac{r}{M+1} \geq \frac{1}{M+1}|f^n(\mathtt{c})| - 1$$

On a ainsi démontré que l'on avait :

$$|f^n(\mathtt{c})| \asymp |\chi_c(f^n(\mathtt{c}))|$$

lorsque $n \to \infty$.

Or, on vérifie facilement par récurrence en utilisant le lemme 62 que :

$$\forall n \in \mathbf{N} \qquad f_c^n \circ \chi_c = \chi_c \circ f^n$$

d'où :

$$\forall n \in \mathbf{N} \qquad |f_c^n(\mathtt{c})| = |\chi_c(f^n(\mathtt{c}))|$$

et le résultat recherché est démontré. ■

Théorème 64 *L'endomorphisme f_c de $\mathtt{C}^\star$:*
- *engendre le mot obtenu en effaçant de $f^\omega(\mathtt{u}_0)$ les lettres de $\mathtt{B}$,*
- *est quasi-uniforme (resp. polynômialement divergent, resp. exponentiellement divergent) en même temps que f.*

Preuve : Le lemme 62 garantit que $f_c(\chi_c(u)) = \chi_c(f_c(u)) = \chi_c(u)$. Or, le lemme 63 garantit que f_c est croissant et de même nature que f d'où le résultat. ■

Théorème 65 *Il existe :*
- *un alphabet $\tilde{\mathtt{A}}$,*
- $\tilde{\mathtt{u}}_0 \in \tilde{\mathtt{A}}$,
- $\tilde{f} \in \hom\left(\tilde{\mathtt{A}}^\star\right)$ croissant *prolongeable sur* $\tilde{\mathtt{u}}_0$,
- $g \in \hom\left(\tilde{\mathtt{A}}^\star, \mathtt{A}^\star\right)$ non effaçant

tels que :
- $f^\omega(\mathtt{u}_0) = g\left(\tilde{f}^\omega(\tilde{\mathtt{u}}_0)\right)$,
- *$\tilde{f}$ est quasi-uniforme (resp. polynômialement divergent, resp. exponentiellement divergent) en même temps que f.*

Preuve : Ecrivons :

$$u = \mathtt{u}_0 w_1 \mathtt{u}_1 w_2 \mathtt{u}_2 w_3 \mathtt{u}_3 w_4 \mathtt{u}_4 \dots$$

avec $\mathtt{u}_j \in \mathtt{C}$ et $w_j \in \mathtt{B}^\star$ pour $j \in \mathbf{N}^*$ et posons :

$$\begin{aligned}
\tilde{\mathtt{A}} &:= \left\{(\mathtt{c}, b, \mathtt{c}') \in \mathtt{C} \times \mathtt{B}^\star \times \mathtt{C} : \mathtt{c}b\mathtt{c}' \in \mathtt{F}(u)\right\} \\
\tilde{\mathtt{u}}_0 &:= (\mathtt{u}_0, w_1, \mathtt{u}_1) \\
\tilde{u} &:= (\mathtt{u}_0, w_1, \mathtt{u}_1)(\mathtt{u}_1, w_2, \mathtt{u}_2)(\mathtt{u}_2, w_3, \mathtt{u}_3)(\mathtt{u}_3, w_4, \mathtt{u}_4) \dots
\end{aligned}$$

en remarquant que $\tilde{\mathtt{A}}$ est fini.

On définit $\tilde{f} \in \hom\left(\tilde{\mathtt{A}}^\star\right)$ en posant pour tout $(\mathtt{c}, b, \mathtt{c}') \in \tilde{\mathtt{A}}^\star$:

$$\tilde{f}(\mathtt{c}, b, \mathtt{c}') := (\mathtt{c}_1, b_1, \mathtt{c}_2)(\mathtt{c}_2, b_2, \mathtt{c}_3) \dots (\mathtt{c}_{n-1}, b_{n-1}, \mathtt{c}_n)(\mathtt{c}_n, b_n b'_n, \mathtt{c}_{n+1})$$

où :

$$\begin{array}{rcl} f(\mathtt{c}b) & = & b_0 \mathtt{c}_1 b_1 \mathtt{c}_2 b_2 \dots \mathtt{c}_{n-1} b_{n-1} \mathtt{c}_n b_n \\ f(\mathtt{c}') & \in & b'_n \mathtt{c}_{n+1} \mathtt{A}^\star \end{array}$$

avec $n \in \mathbf{N}^*$ (l'image d'une lettre croissante contient u moins une lettre croissante), $b_j \in \mathtt{B}^\star$ $(0 \leq j \leq n)$, $b'_n \in \mathtt{B}^\star$ et $\mathtt{c}_j \in \mathtt{C}^\star$ $(1 \leq j \leq n+1)$. Par construction, $\tilde{f}(\tilde{u}) = \tilde{u}$ (utiliser $\mathtt{u}_0 \in \mathtt{C}$).

On définit $g \in \hom\left(\tilde{\mathtt{A}}^\star, \mathtt{A}^\star\right)$ et $h \in \hom\left(\tilde{\mathtt{A}}^\star, \mathtt{C}^\star\right)$ en posant :

$$\begin{array}{rcl} g(\mathtt{c}, b, \mathtt{c}') & := & \mathtt{c}b \\ h(\mathtt{c}, b, \mathtt{c}') & := & \mathtt{c} \end{array}$$

pour tout $(\mathtt{c}, b, \mathtt{c}') \in \tilde{\mathtt{A}}$. Par construction, g est non effaçant, $g\left(\tilde{u}\right) = u$.

Il ne reste donc plus qu'à vérifier que $\tilde{f}$ est croissant et de même nature que f. Or, lorsque $\tilde{\mathtt{a}}$ décrit $\tilde{\mathtt{A}}$, $h(\tilde{\mathtt{a}})$ décrit $\mathtt{C}$ donc le lemme suivant permet de conclure.

Lemme 66 *Pour tout* $\tilde{\mathtt{a}} \in \tilde{\mathtt{A}}$*, on a* $\left|\tilde{f}^n(\tilde{\mathtt{a}})\right| \asymp |f^n(h(\tilde{\mathtt{a}}))|$ *lorsque* $n \to \infty$*.*

Preuve : En remarquant que $h \circ \tilde{f} = f_c \circ h$ on obtient par récurrence que :

$$h \circ \tilde{f}^n = f_c^n \circ h$$

puis, comme h est lettre à lettre :

$$\left|\tilde{f}^n(\tilde{\mathtt{a}})\right| = \left|h\left(\tilde{f}^n(\tilde{\mathtt{a}})\right)\right| = \left|f_c^n\left(h(\tilde{\mathtt{a}})\right)\right|$$

Il suffit maintenant d'appliquer le lemme 63 pour obtenir ce qu'on voulait. ■ ■

Théorème 67 *Si* $f^\omega(\mathtt{u}_0)$ *n'est pas ultimement périodique alors on a :*

$$\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \asymp \begin{cases} n & \textit{si } f \textit{ est quasi-uniforme} \\ n \ln\ln n & \textit{si } f \textit{ est polynômialement divergent} \\ n \ln n & \textit{si } f \textit{ est exponentiellement divergent} \end{cases}$$

lorsque $n \to \infty$*.*

Preuve : On va appliquer le théorème 53.

Par la proposition 8, on a :

$$\forall n \in \mathbf{N} \quad \mathtt{p}_u(n) \leq |g|\, \mathtt{p}_{\tilde{f}^\omega(\tilde{\mathtt{u}}_0)}(n)$$

Or, par la proposition 9 on a aussi :

$$\forall n \in \mathbf{N} \qquad \mathtt{p}_u((M+1)n - M) \geq \mathtt{p}_{f_c^\omega(\mathtt{u}_0)}(n)$$

d'où :

$$\forall n \in \mathbf{N} \qquad \mathtt{p}_u(n) \geq \mathtt{p}_{f_c^{\omega}(\mathtt{u}_0)}\left(\left\lfloor \frac{n}{M+1} \right\rfloor\right)$$

Comme f_c et $\tilde{f}$ sont croissants et de même nature que f, on a bien le résultat recherché. ■

Chapitre 10

Mots substitutifs de complexité quadratique

On va dans ce chapitre démontrer le théorème suivant.

Théorème 68 *On suppose que $f^\omega(\mathtt{u}_0)$ n'est pas ultimement périodique et que $\mathtt{B}^\star \cap \mathtt{F}(f^\omega(\mathtt{u}_0))$ est* infini, $\mathtt{B}$ *désignant l'ensemble des lettres bornées pour f.*

Alors, on a $\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \asymp n^2$ lorsque $n \to \infty$.

On aura ainsi déterminé le comportement asymptotique de la complexité des mots substitutifs dans tous les cas possibles.

10.1 Majoration

Théorème 69 *On a $\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \preceq n^2$ lorsque $n \to \infty$.*

Preuve : Par le théorème de Cobham, on peut supposer que f est non effaçant. De plus, en appliquant le lemme 18 avec $\mathtt{B} := \emptyset$ et $\mathtt{C} = \mathtt{A}$, on voit que, quitte à élever f à une puissance convenable, on peut supposer que pour tout $\mathtt{a} \in \mathtt{A}$, il existe $\mathtt{a}' \in \mathtt{A}$ tel que $f(\mathtt{a}) \in \mathtt{a}'\mathtt{A}^\star$ et $f(\mathtt{a}') \in \mathtt{a}'\mathtt{A}^\star$ (resp. $f(\mathtt{a}) \in \mathtt{A}^\star\mathtt{a}'$ et $f(\mathtt{a}') \in \mathtt{A}^\star\mathtt{a}'$).

Lemme 70

$$\forall w \in \mathtt{A}^\star \qquad |w| = \left|f^2(w)\right| \Longrightarrow f(w) = f^2(w)$$

Preuve : Posons $n = |w|$ et écrivons $w = \mathtt{a}_1\mathtt{a}_2 \ldots \mathtt{a}_n$ avec $\mathtt{a}_1$, $\mathtt{a}_2$, …, $\mathtt{a}_n \in \mathtt{A}$.

Il existe w_j, $w'_j \in \mathtt{A}^\star$ et $\mathtt{a}'_j \in \mathtt{A}$ tel que $f(\mathtt{a}_j) = \mathtt{a}'_j w_j$ et $f(\mathtt{a}'_j) = \mathtt{a}'_j w'_j$ pour $j \in \{1, \ldots, n\}$.

Ainsi, on a :

$$\begin{aligned} f(w) &= \mathtt{a}'_1 w_1 \mathtt{a}'_2 w_2 \ldots \mathtt{a}'_n w_n \\ f^2(w) &= \mathtt{a}'_1 w'_1 f(w_1) \mathtt{a}'_2 w'_2 f(w_2) \ldots \mathtt{a}'_n w'_n f(w_n) \end{aligned}$$

Supposons que $|w| = \left|f^2(w)\right|$. Ceci force, pour $j \in \{1, \dots, n\}$, que $w'_j f(w_j) = \varepsilon$ donc, comme f est non effaçant, $w'_j = w_j = \varepsilon$. On en déduit que $f(w) = \mathtt{a}'_1 \mathtt{a}'_2 \dots \mathtt{a}'_n = f^2(w)$. ■

Fixons un entier $n \geq 2$ et notons :

$$S := \bigcup_{k=1}^{|f|-1} \mathtt{A}^k$$

On va montrer que l'image de l'application :

$$\begin{array}{ccc} \mathtt{A} \times S \times \{1, \dots, n\} \times \{0, 1, \dots, 2n\} & \longrightarrow & \mathtt{A}^\star \\ (\mathtt{a}, s, k, l) & \longmapsto & \left(\underset{l}{\mathtt{pref}}\, f^k(\mathtt{a})\right) \left(\underset{n-l}{\mathtt{suff}}\, f^k(s)\right) \end{array}$$

contient $\mathtt{F}_n(u)$.

Soient $w \in \mathtt{F}_n(u)$ quelconque et :

$$K := \min \left\{k \in \mathbf{N} : w \in f^k(\mathtt{u}_0)\right\}$$

Comme dans le lemme 54, on construit par récurrence une suite $(w_0, w_1, \dots, w_K)$ d'éléments de $\mathtt{A}^\star$:

- en posant $w_0 := w$,
- en choisissant, pour $j \in \{1, \dots, K\}$, un facteur w_j de $f^{K-j}(\mathtt{u}_0)$ de longueur minimale tel que w_{j-1} soit facteur de $f(w_j)$.

Posant :

$$k := \max \{j \in \{0, 1, \dots, K\} : |w_j| \geq 2\}$$

on a $k < K$ car $w_K = \mathtt{u}_0$, ce qui permet d'écrire :

$$2 \leq |w_k| \leq |f(w_{k+1})| \leq |f|$$

puis $w = \mathtt{a}s$ avec $\mathtt{a} \in \mathtt{A}$ et $s \in S$. En utilisant le fait que f est non effaçant, on vérifie alors par récurrence que pour tout entier j, $0 \leq j \leq k$, w_{k-j} est la concaténation d'un suffixe non vide de $f^j(\mathtt{a})$ et d'un préfixe non vide de $f^j(s)$. En particulier, il existe $l \in \{1, \dots, n\}$ tel que :

$$w = \left(\underset{l}{\mathtt{pref}}\, f^k(\mathtt{a})\right) \left(\underset{n-l}{\mathtt{suff}}\, f^k(s)\right)$$

Lemme 71 *La suite* $(|w_0|, |w_1|, \dots |w_k|)$ *est décroissante.*

Preuve : Soit un entier j, $1 \leq j \leq k$: w_{j-1} est un facteur de $f(w_j)$ et w_{j-1} n'est facteur de l'image par f d'aucun facteur propre de w_j.

Ainsi, on peut écrire :

- $w_j = \mathtt{a}x\mathtt{b}$ avec $\mathtt{a}, \mathtt{b} \in \mathtt{A}$ et $x \in \mathtt{A}^\star$,
- $w_{j-1} = \sigma f(x) \pi$ avec σ suffixe non vide de $f(\mathtt{a})$, π préfixe non vide de $f(\mathtt{b})$.

Comme f est non effaçant, on a $|f(x)| \geq |x|$ puis :

$$|w_{j-1}| = |\sigma| + |f(x)| + |\pi| \geq 1 + |x| + 1 = |w_j|$$

■

Lemme 72 *Il n'existe pas de $j \in \{0, 1, \ldots, k-2\}$ tel que $|w_j| = |w_{j+1}| = |w_{j+2}|$.*

Preuve : On écrit :

$$\begin{array}{rcl} w_j & = & \sigma_0 x \pi_0 \\ w_{j+1} & = & \sigma_1 f(x) \pi_1 \\ w_{j+2} & = & \sigma_2 f^2(x) \pi_2 \end{array}$$

avec σ_0, $\pi_0 \in \mathtt{A}$, $x \in \mathtt{A}^\star$, σ_i suffixe non vide de $f(\sigma_{i-1})$ et π_i préfixe non vide de $f(\pi_{i-1})$ pour $i \in \{1, 2\}$.

Supposons (absurde) que $|w_j| = |w_{j+1}| = |w_{j+2}|$. Pour $i \in \{1, 2\}$, on a $|\sigma_i| \geq 1$, $|\pi_i| \geq 1$ et $\left|f^i(x)\right| \geq |x|$ car f est non effaçant d'où :

$$|w_{j+i}| \geq |\sigma_i| + \left|f^i(x)\right| + |\pi_i| \geq 1 + |x| + 1 = |w_i|$$

On en déduit que $\left|f^i(x)\right| = |x|$ et que $|\sigma_i| = |\pi_i| = 1$: σ_i et π_i sont respectivement la dernière lettre de $f(\sigma_{i-1})$ et la première lettre de $f(\pi_{i-1})$. Le lemme 70 garantit alors que $f(x) = f^2(x)$ et, compte tenu des hypothèses faites sur f, on a $\sigma_1 = \sigma_2$ et $\pi_1 = \pi_2$. Il en résulte que $w_{j+1} = w_{j+2}$ ce qui contredit la minimalité de K. ■

Ainsi, la suite $(|w_0|, |w_1|, \ldots |w_k|)$ décroit de n vers un entier ≥ 1 sans que jamais ne se présente trois termes consécutifs égaux. Ceci force $k \leq 2n$ donc le quadruplet $(\mathtt{a}, s, k, l)$ s'envoie bien sur w par l'application décrite ci-dessus. ■

10.2 Minoration

Lemme 73 (Nicolas) *Soient $v \in \{\mathtt{0}, \mathtt{1}\}^\omega$, $p \in \mathbf{N}$ et $q \in \mathbf{N}^*$ tels que pour tout $k \in \mathbf{N}$, $\mathtt{1}\mathtt{0}^{p+qk}\mathtt{1}$ soit facteur de v.*

Alors, on a $\mathtt{p}_v(n) \succeq n^2$ lorsque $n \to \infty$.

Preuve : Posons $z := \mathtt{1}^{-\omega} v$.

Le mot biinfini z vérifie pour tout $n \in \mathbf{N}$:

$$\mathtt{F}_n(z) = \mathtt{F}_n(v) \cup \left\{ \mathtt{1}^k \underset{n-k}{\mathtt{pref}}\, v \right\}_{0 \leq k \leq n}$$

donc on a :

$$\mathtt{p}_v(n) \geq \mathtt{p}_z(n) - (n+1)$$

et par suite, il suffit de montrer que $\mathtt{p}_z(n) \succeq n^2$ lorsque $n \to \infty$.

L'hypothèse faite sur v garantit que pour tout $k \in \mathbf{N}$, il existe $\pi_k \in \{\mathtt{0},\mathtt{1}\}^{-\omega}$ et $\sigma_k \in \{\mathtt{0},\mathtt{1}\}^{\omega}$ tels que :

$$z = \pi_k \mathtt{1}\mathtt{0}^{p+qk}\mathtt{1}\sigma_k$$

ce qui permet de poser pour tout $j \in \mathbf{N}$:

$$\begin{array}{rcl} \pi_{k,j} & := & \underset{j}{\mathtt{suff}}\, \pi_k \\ \sigma_{k,j} & := & \underset{j}{\mathtt{pref}}\, \sigma_k \end{array}$$

Fixons $n \in \mathbf{N}$ et posons :

$$E_n := \left\{ k \in \mathbf{N} : \frac{n}{2} \leq p + qk \leq \frac{3n}{4} - 2 \right\}$$

Pour tout $(k,j) \in E_n \times ([0, n/4] \cap \mathbf{N})$, on a $p+qk+2+j \leq 3n/4-2+2+n/4 = n$ donc on peut poser :

$$w_{k,j} := \pi_{k,j}\mathtt{1}\mathtt{0}^{p+qk}\mathtt{1}\sigma_{k,n-(p+qk+2+j)}$$

et, bien sûr, $w_{k,j} \in \mathtt{F}_n(z)$.

De plus, (là est l'astuce) les $w_{k,j}$ $((k,j) \in E_n \times ([0,n/4] \cap \mathbf{N}))$ sont deux à deux distincts car un mot de longueur n donné admet au plus une occurence de facteur de la forme $\mathtt{1}\mathtt{0}^l\mathtt{1}$ avec $l \geq n/2$.

On en déduit :

$$\mathtt{p}_z(n) \geq (\# E_n)\,(\#[0, n/4] \cap \mathbf{N}) \geq \left(\frac{n}{2q} - \frac{2}{q}\right)\frac{n}{4}$$

ce qu'on voulait. ∎

Proposition 74 *Il existe $N \in \mathbf{N}^*$ tel que :*

$$\forall k \in \mathbf{N}^* \ \forall b \in \mathtt{B}^\star \qquad f^{kN}(b) = f^N(b) \tag{10.1}$$

Preuve : L'ensemble :

$$E := \bigcup_{\mathtt{b} \in \mathtt{B}} \{f^n(\mathtt{b}) : n \in \mathbf{N}\}$$

est fini donc on peut poser $N := (\# E)!$ et est stable par f donc f induit une application :

$$\begin{array}{rccc} \varphi : & E & \longrightarrow & E \\ & x & \longmapsto & f(x) \end{array}$$

à laquelle on peut appliquer le lemme 16 : pour tout $k \in \mathbf{N}^*$, on a $\varphi^{kN} = \varphi^N$ donc pour tout $\mathtt{b} \in \mathtt{B}$, on a $f^{kN}(\mathtt{b}) = f^N(\mathtt{b})$. ∎

Proposition 75 *Le mot infini $f^\omega(\mathtt{u}_0)$ contient une infinité d'occurences de lettres appartenant à $\mathtt{C}$ ou est ultimement périodique.*

Preuve : Quitte à élever f à une puissance convenable, on peut supposer que (10.1) est vraie pour $N = 1$.

Soit alors $s \in \mathtt{A}^\star$ tel que $f(\mathtt{u}_0) = \mathtt{u}_0 s$. Comme $u = \mathtt{u}_0 s f(s) f^2(s) f^3(s) \ldots$, $s \in \mathtt{B}^\star$ donnerait $u = \mathtt{u}_0 s f(s)^\omega$ et par suite u serait ultimement périodique. On en déduit que si u n'est pas ultimement périodique alors $s \in \mathtt{A}^\star \setminus \mathtt{B}^\star$ et par suite la proposition 17 garantit que u contient une infinité d'occurences de lettres appartenant à $\mathtt{C}$. ∎

Théorème 76 *On note* $\mathtt{B}$ *(resp.* $\mathtt{C}$*) l'ensemble des lettres bornées (resp. croissantes) pour* f *et on suppose que l'ensemble* $\mathtt{B}^\star \cap \mathtt{F}(f^\omega(\mathtt{u}_0))$ *est infini et que* $f^\omega(\mathtt{u}_0)$ *n'est pas ultimement périodique.*

Alors, on a $\mathtt{p}_{f^\omega(\mathtt{u}_0)}(n) \succeq n^2$ *lorsque* $n \to \infty$.

Preuve : Soit $\chi \in \hom\left(\mathtt{A}^\star, \{\mathtt{0},\mathtt{1}\}^\star\right)$ défini en posant :

$$\chi(\mathtt{a}) := \begin{cases} \mathtt{0} & \text{si } \mathtt{a} \in \mathtt{B} \\ \mathtt{1} & \text{si } \mathtt{a} \in \mathtt{C} \end{cases}$$

pour tout $\mathtt{a} \in \mathtt{A}$. Soit $v := \chi(u)$. Comme pour tout $n \in \mathbf{N}$, on a $\mathtt{p}_u(n) \geq \mathtt{p}_v(n)$, il suffit, pour conclure, d'être en mesure d'appliquer le lemme **??** à v.

Lemme 77

$$\mathtt{B}^+ \cap \mathtt{F}(u) \subseteq \bigcup_{w \in \mathtt{CB}^\star\mathtt{C} \cap \mathtt{F}(u)} \mathtt{F}(w)$$

Preuve : Soit $b \in \mathtt{B}^+ \cap \mathtt{F}(u)$.

Il existe $a_1 \in \mathtt{A}^\star$ et $a_2 \in \mathtt{A}^\omega$ tels que $a_1 b a_2 = u$.

Soit b_1 le plus long suffixe de a_1 appartenant à $\mathtt{B}^\star$: $\mathtt{u}_0 \in \mathtt{C}$ donc il est impossible que $\mathtt{u}_0$ soit la première lettre de b donc il est impossible que $a_1 = \varepsilon$. On en déduit que $a_1 \neq \varepsilon$ puis que $\mathtt{u}_0$ est la première lettre de a_1 puis que $a_1 \notin \mathtt{B}^\star$. Par suite, on a $a_1 \neq b_1$ d'où il existe $\mathtt{c}_1 \in \mathtt{C}$ et $a_1' \in \mathtt{A}^\star$ tels que $a_1 = a_1' \mathtt{c}_1 b_1$.

Soit b_2 le plus long préfixe de a_2 appartenant à $\mathtt{B}^\infty$. La proposition 75 garantit que u contient une infinité d'occurences de lettres appartenant à $\mathtt{C}$ donc il en est de même pour tout ses suffixes. En particulier, a_2 contient des lettres appartenant à $\mathtt{C}$. Il en résulte que $b_2 \neq a_2$ donc b_2 est de longueur finie et il existe $\mathtt{c}_2 \in \mathtt{C}$ et $a_2' \in \mathtt{A}^\omega$ tels que $a_2 = b_2 \mathtt{c}_2 a_2'$.

On en déduit que $u = a_1' \mathtt{c}_1 b_1 b b_2 \mathtt{c}_2 a_2'$ donc $b \in \mathtt{F}(\mathtt{c}_1 b_1 b b_2 \mathtt{c}_2)$ et $\mathtt{c}_1 b_1 b b_2 \mathtt{c}_2 \in \mathtt{CB}^\star\mathtt{C} \cap \mathtt{F}(u)$. ∎

Lemme 78 *Il existe* $\mathtt{c}_1, \mathtt{c}_2 \in \mathtt{C}$ *et* $b \in \mathtt{B}^\star$ *tels que* $\mathtt{c}_1 b \mathtt{c}_2$ *est facteur de* u *et que lorsque* k *décrit* $\mathbf{N}$*, la longueur de la concaténation (notée* $\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k)$*) :*

- *du suffixe de* $f^k(\mathtt{c}_1)$ *appartenant à* $\mathtt{CB}^\star$*,*
- *de* $f^k(b)$*,*
- *du préfixe de* $f^k(\mathtt{c}_2)$ *appartenant à* $\mathtt{B}^\star\mathtt{C}$

est non bornée.

Preuve : Notant :

$$X := \bigcup_{\mathtt{c} \in \mathtt{C}} \{(\mathtt{c}_1, b, \mathtt{c}_2) \in \mathtt{C} \times \mathtt{B} \times \mathtt{C} : \mathtt{c}_1 b \mathtt{c}_2 \in \mathtt{F}(f(\mathtt{c}))\}$$

le lemme 19, donne :

$$\mathtt{CB}^\star\mathtt{C} \cap \mathtt{F}(u) = \bigcup_{(\mathtt{c}_1,b,\mathtt{c}_2)\in X} \{\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k) : k \in \mathbf{N}\}$$

Or, comme $\mathtt{B}^\star \cap \mathtt{F}(u)$ est infini, le lemme 77 force $\mathtt{CB}^\star\mathtt{C} \cap \mathtt{F}(u)$ à être infini. Par suite, comme X est fini, il existe $(\mathtt{c}_1, b, \mathtt{c}_2) \in X$ tel que $\{\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k) : k \in \mathbf{N}\}$ soit infini i.e. tel que $\sup_{k\in\mathbf{N}} |\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k)| = \infty$. ∎

Dans la suite de la démonstration, on supposera que f a été élevé à une puissance suffisante pour que les conclusions des lemmes 18 et 74 soient vraies pour $N = 1$. Ainsi, il existe b_1, b_2, b'_1, $b'_2 \in \mathtt{B}^\star$ et $\mathtt{c}'_1$, $\mathtt{c}'_2 \in \mathtt{C}$ tels que $f(\mathtt{c}_1) \in \mathtt{A}^\star\mathtt{c}'_1 b_1$, $f(\mathtt{c}_2) \in b_2\mathtt{c}'_2\mathtt{A}^\star$, $f(\mathtt{c}'_1) \in \mathtt{A}^\star\mathtt{c}'_1 b'_1$, $f(\mathtt{c}'_2) \in b'_2\mathtt{c}'_2\mathtt{A}^\star$. Pour tout $k \in \mathbf{N}$, on a :

$$\begin{array}{rcl}
\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(0) & = & \mathtt{c}_1 b \mathtt{c}_2 \\
\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(1) & = & \mathtt{c}'_1 b_1 f(b) b_2 \mathtt{c}'_2 \\
\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(2) & = & \mathtt{c}'_1 b'_1 f(b_1) f(b) f(b_2) b'_2 \mathtt{c}'_2 \\
\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k+2) & = & \mathtt{c}'_1 b'_1 f(b'_1)^k f(b_1) f(b) f(b_2) f(b'_2)^k b'_2 \mathtt{c}'_2
\end{array}$$

donc posant :

$$\begin{array}{rcl}
p & := & |\mathtt{c}'_1 b'_1 f(b_1)| + |f(b)| + |f(b_2) b'_2 \mathtt{c}'_2| \\
q & := & |f(b'_1)| + |f(b'_2)|
\end{array}$$

il vient :

$$|\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k+2)| = p + qk$$

et comme la quantité ci-dessus est non bornée lorsque k décrit $\mathbf{N}$, on a forcément $q \neq 0$. Enfin, $\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k+2)$ est facteur $f^{k+2}(\mathtt{c}_1 b \mathtt{c}_2)$ donc de u donc $\mathtt{1}\mathtt{0}^{p+qk}\mathtt{1} = \chi\left(\beta_{\mathtt{c}_1,b,\mathtt{c}_2}(k+2)\right)$ est facteur de v : tout va bien. ∎

Exemple 79 *En prenant* $\mathtt{A} := \{\mathtt{0}, \mathtt{1}\}$, $\mathtt{u}_0 := \mathtt{0}$ *et :*

$$f : \begin{array}{rcl} \mathtt{0} & \longmapsto & \mathtt{001} \\ \mathtt{1} & \longmapsto & \mathtt{1} \end{array}$$

on a $f^\omega(\mathtt{u}_0)$ *non ultimement périodique et* $\mathtt{B}^\star \cap \mathtt{F}\left(f^\omega(\mathtt{u}_0)\right)$ *infini.*

Preuve : On a trivialement $\mathtt{B} = \{\mathtt{1}\}$ et on vérifie facilement par récurrence que pour tout $n \in \mathbf{N}$, $\mathtt{01}^n$ est facteur de $f^n(\mathtt{u}_0)$. ∎

Bibliographie

[1] Jean Berstel and Christophe Reutenauer. *Rational Series and Their Languages.* Number 12 in EATCS Monographs on Theoretical Computer Science. Springer-Verlag, 1988.

[2] A. Cobham. On the Hartmanis-Stearns problem for a class of tag machines. *IEEE Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory*, 1968.

[3] Andrzej Ehrenfeucht, K. P. Lee, and Grzegorz Rozenberg. Subword complexities of various classes of deterministic developmental languages without interaction. *Theoret. Comput. Sci.*, 1 :59–75, 1975.

[4] Andrzej Ehrenfeucht and Grzegorz Rozenberg. On subword complexities of homomorphic images of langages. *R.A.I.R.O Informatique théorique*, 16 :108–113, 1982.

[5] M. Lothaire. *Algebraic Combinatorics on Words.* Cambridge University Press. To appear. Available online at `http ://www-igm.univ-mlv.fr/~berstel/Lothaire/`.

[6] M. Lothaire. *Combinatorics on Words*, volume 17 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley, 1983. Reprinted in the *Cambridge Mathematical Library*, Cambridge University Press, 1997.

[7] Marston Morse and Gustav A. Hedlund. Symbolic dynamics. *American J. Math.*, 60 :815–866, 1938.

[8] Jean-Jacques Pansiot. Complexité des facteurs des mots infinis engendrés par morphismes itérés. In *ICALP '84*, number 172 in Lect. Notes Comput. Sci., pages 380–389. Springer-Verlag, 1984.

[9] Arto Salomaa and Matti Soittola. *Automata-Theoretic Aspects of Formal Power Series.* Springer-Verlag, 1978.

[10] A. Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. *Kra. Vidensk. Selsk. Skrifter, I. Mat. Nat. Kl.*, 1 :1–67, 1912.