ENS — Math Info 2007

1. Préliminaires

Question 1.1

1. De façon classique, on a $\varphi(1_M) = 1_N$ donc $\varphi^{-1}(1_N) = 1_M$. De même, pour $x, y \in N$, en écrivant $u = \varphi^{-1}(x)$ et $v = \varphi^{-1}(y)$, on a
$$\varphi\big(\varphi^{-1}(x) \odot \varphi^{-1}(y)\big) = \varphi(u \odot v) = \varphi(u) \otimes \varphi(v) = x \otimes y,$$
et donc en composant par φ^{-1},
$$\varphi^{-1}(x) \odot \varphi^{-1}(y) = u \odot v = \varphi^{-1}(x \otimes y).$$
2. De plus, pour $x \in N$, on a $\varphi(x) \otimes \varphi(x^{-1}) = \varphi(x \odot x^{-1}) = \varphi(1_M) = 1_N$, et de même pour $\varphi(x^{-1}) \otimes \varphi(x)$, ce qui prouve que $\varphi(x^{-1})$ est l'inverse de $\varphi(x)$.

Question 1.2

1. Prouvons tout d'abord que $R^\star$ est stable par composition. Pour u et v dans $R^\star$, on peut écrire
$$u = r_1 \odot \cdots \odot r_n \qquad v = r'_1 \odot \cdots \odot r'_p,$$
avec chacun des r_i et des r'_j appartenant à R. On a alors
$$u \odot v = r_1 \odot \cdots \odot r_n \odot r'_1 \odot \cdots \odot r'_p$$
qui appartient lui aussi à $R^\star$, étant lui aussi un produit fini d'éléments de R.
Cela prouve, puisque de plus $1_M \in R^\star$, que $R^\star$ est un sous-monoïde.

   Soit maintenant N un sous-monoïde de M contenant R. Par définition, $1_M \in N$ et $R \subseteq N$ et, puisque N est stable par produits finis, il contient donc $R^\star$. Cela prouve que $R^\star$ est le plus petit sous-monoïde de N contenant R.
2. Si maintenant M est un groupe, comme $R \cup R^{-1}$ est une partie de M, cela prouve que $\big(R \cup R^{-1}\big)^\star$ est le plus petit sous-monoïde de M contenant $R \cup R^{-1}$.
Pour prouver qu'il s'agit en fait du plus petit sous-groupe de M contenant $R \cup R^{-1}$, il suffit donc de montrer que $\big(R \cup R^{-1}\big)^\star$ est stable par passage à l'inverse. Mais, si $u = r_1 \odot \cdots \odot r_n$ est un élément de $\big(R \cup R^{-1}\big)^\star$ (avec chacun des r_i appartenant à $R \cup R^{-1}$), on a r_i^{-1} qui appartient aussi à $R \cup R^{-1}$, et donc $u^{-1} = r_n^{-1} \odot \cdots \odot r_1^{-1}$ appartient à $\big(R \cup R^{-1}\big)^\star$.
Notons enfin qu'un sous-groupe de M contient R si, et seulement si il contient $R \cup R^{-1}$, étant stable par inverse. Ainsi, $\big(R \cup R^{-1}\big)^\star$ est bien le plus petit sous-groupe de M contenant R.

2. Mots réduits

Question 2.1 On peut prouve ce résultat classiquement par récurrence sur la longueur du mot considéré. En effet, tout mot u de longueur 0 étant réduit, il existe alors bien un mot réduit v tel que $u \xrightarrow{\infty} v$ (ayant $u = v = 1$). Si, maintenant, la propriété est vrai à un rang $n \in \mathbf{N}$ quelconque, étant donné un mot u de longueur $n+1$, deux cas sont possibles : soit u est lui-même réduit auquel cas la propriété voulue est vérifiée, soit il existe v tel que $u \xrightarrow{1} v$. Comme alors $|v| \leq n$ (on a en fait $|v| = n-1$), par hypothèse de récurrence, il existe w réduit tel que $v \xrightarrow{\infty} w$. On a alors $u \xrightarrow{\infty} w$.

Une autre manière de procéder est la suivante : étant donné un mot u quelconque, on considère l'ensemble $E_u = \left\{ v \in \tilde{A}^\star \;\middle|\; u \xrightarrow{\infty} v \right\}$. Cet ensemble est non vide (il contient u) et admet un élément de longueur minimale w. Le mot w est alors nécessairement réduit (car si il existe un w' tel que $w \xrightarrow{1} w'$, on aurait $|w'| < |w|$ et $u \xrightarrow{\infty} w'$) et il vérifie $u \xrightarrow{\infty} w'$.

L'exemple donné se réduit ainsi :
$$ab\overline{a}a\overline{bb}aab\overline{b}\overline{aa}aab\overline{b}\overline{a}ab \xrightarrow{\infty} a\overline{b}aab.$$

Question 2.2 Soient u, x et y tels que $u \xrightarrow{1} x$ et $u \xrightarrow{1} y$. On peut écrire :
$$u = v_1 a\overline{a} v_2 \qquad x = v_1 v_2$$
$$v = w_1 b\overline{b} w_2 \qquad y = w_1 w_2$$

Plusieurs cas sont possibles (on suppose ici que $|v_1| \leq |w_1|$) :

1. Si $v_1 = w_1$ et $v_2 = w_2$, alors $x = y$ et $a = b$. En posant $z = x = y$, on a $x \xrightarrow{0} z$ et $y \xrightarrow{0} z$.
2. Si $w_1 = v_1 a$ (et donc $v_2 = \overline{b} w_2$), alors $a = \overline{b}$ et, comme précédemment, $x = y$.
3. Si, enfin, $v_1 a\overline{a}$ est un prefixe de w_1 (et, de façon équivalent, $b\overline{b}w_2$ est un suffixe de v_2), il existe un mot z tel que $w_1 = v_1 a\overline{a}z$ et $v_2 = zb\overline{b}w_2$. Dans ce cas, on a $u = v_1 a\overline{a}zb\overline{b}w_2$, $x = v_1 zb\overline{b}w_2$ et $y = v_1 a\overline{a}zw_2$ et donc $x \xrightarrow{1} v_1 zw_2$ et $y \xrightarrow{1} v_1 zw_2$.

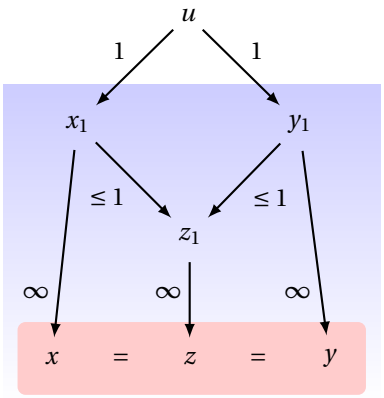
Question 2.3 D'après la question 2.1, tout mot de $\tilde{A}^\star$ admet au moins un réduit. Montrons maintenant que celui-ci est unique, par récurrence sur la longueur. Notons tout d'abord que ce résultat est bien vérifié pour tous les mots de longueur 0.

Considérons maintenant n un entier quelconque, et supposons que tout mot de longueur au plus n admet un unique réduit, et soit enfin un mot u de longueur $n+1$. Si u est réduit, on a bien unicité, puisque $u \xrightarrow{\infty} v$ implique $u = v$. Si, par contre, u n'est pas réduit, soient x et y deux mots réduits tels que $u \xrightarrow{\infty} x$ et $u \xrightarrow{\infty} y$. En définissant x_1 et y_1

tels que $u \xrightarrow{1} x_1 \xrightarrow{\infty} x$ et $u \xrightarrow{1} y_1 \xrightarrow{\infty} y$, il existe d'après la question précédente un mot z_1 tel que $x_1 \xrightarrow{\leq 1} z_1$ et $y_1 \xrightarrow{\leq 1} z_1$. Notons enfin z l'unique mot réduit tel que $z_1 \xrightarrow{\infty} z$ (son unicité est assuré par l'hypothèse de récurrence, puisque $|z| \leq n$).

Puisque $x_1 \xrightarrow{\leq 1} z_1 \xrightarrow{\infty} z$ et $x_1 \xrightarrow{\infty} x$ et que x et z sont tous deux réduits, on en déduit par hypothèse de récurrence que $x = z$. En considérant de même y_1, on en déduit que $y = z$ et donc que $x = y$. On a donc montré que u admet exactement un seul réduit, ce qui achève la démonstration.

On peut résumer la situation par le diagramme suivant :



Domaine d'application de l'hypothèse de récurrence : unicité d'un mot réduit

Mots réduits

Question 2.4 Un algorithme pour réduire un mot est le suivant :

1. On note $u = a_1 \cdots a_n$ le mot en entrée, en supposant que $n \geq 2$ (sinon, le mot est déjà réduit), et on considère deux pointeurs i et j, initialisés respectivement à 1 et 2.
2. Si a_i et a_j sont complémentaires l'un de l'autre, on barre ces deux lettres, puis on change la position des pointeurs de la façon suivate :
   (a) si il existe au moins une lettre non barrée à gauche de i et une autre à la droite de j (cette dernière étant forcément en position $j+1$), alors on positionne i et j sur ces lettres, et on recommence le point courant ;
   (b) si toutes les lettres à gauche de i sont barrées et si il existe au moins de lettres non barrées à la droite de j (en position $j+1$ et $j+2$), alors on positionne i et j sur ces lettres, et on recommence le point courant ;
   (c) sinon, on va au point 3.

   Sinon, si a_i et a_j ne sont pas complémentaires l'une de l'autre,
   (a) si $j < n$, on "avance" les pointeurs, en faisant pointer i sur a_j et j sur a_{j+1}, et l'on recommence le point courant ;
   (b) sinon, on va au point 3.
3. On a fini, le mot réduit s'obtient en le prenant que les lettres non marquées.

Illustrons cet algorithme en l'appliquant à l'exemple précédent. Le déroulement est représenté figure 1.

Remarque 1 Il ne faut bien sûr par, durant un écrit de concours, dérouler un exemple aussi long. Par contre, illustrer un algorithme à l'aide d'un exemple (de taille bien choisie) est une bonne idée. En effet, cela peut clarifier un algorithme dont le principe n'est pas forcément aisé à comprendre.

Remarque 2 Quitte à faire ce qui n'est pas demandé, voici une implémentation en OCaml de l'algorithme précédent, où un mot est représenté par une liste, et où l'on fournit une fonction « `complementaire` » pour dire si deux lettres sont complémentaires l'un de l'autre ou non. Le programme est donné figure 2. La fonction principale, nommée « `aux` » prends quatre arguments en entrée : d'une part les lettres pointées par i et j, nommées « `li` » et « `lj` », ainsi que les mots à gauche de i (nommé « `mi` ») et à droite de j (nommé « `mj` »), sachant que le mot « `mi` » est représenté en sens inverse. À la fin de l'algorithme, le mot réduit obtenu est donc « `mi` » remis dans le bon sens.

Plus sérieusement, on remarque que le mot retourne par l'algorithme est bien réduit, puisque pour chaque couple de lettres consécutives du mot obtenu aura été testé lors de l'exécution. De plus, l'algorithme se déroule en temps linéaire en fonction de la longueur du mot, puisque le pointeur j avance strictement à chaque itération.

3. Groupes libres

Question 3.1 On a $u \odot (v \odot w) = \rho(u\rho(vw))$. Or, puisque d'une part $uvw \xrightarrow{\infty} \rho(uvw)$, et d'autre part $uvw \xrightarrow{\infty} u\rho(vw) \xrightarrow{\infty} \rho(u\rho(vw))$, on en déduit par unicité du mot réduit que $u \odot (v \odot w) = \rho(u\rho(vw)) = \rho(uvw)$.

Cela implique que la loi de composition interne $\odot$ est associative :

$$u \odot (v \odot w) = \rho(u\rho(vw)) = \rho(uvw) = \rho(\rho(uv)w) = (u \odot v) \odot w$$

Bien sûr, pour tout u réduit, on a $u \odot 1 = 1 \odot u = u$, donc 1 est élément neutre pour $\odot$, ce qui prouve que $(F(A), \odot, 1)$ est un monoïde.

De plus, pour tout mot $u \in \tilde{A}^\star$, on a clairement $\rho(u\overline{u}) = 1$, donc tout mot réduit u a pour inverse $\rho(\overline{u})$, ce qui fait que l'on a en fait bien une structure de groupe.

Finalement, on remarque que le mot $\overline{u}$ contient deux lettres consécutives de la forme $a\overline{a}$, il en est de même puisque $\overline{a\overline{a}} = a\overline{a}$. Cela montre que u est réduit si, et seulement si $\overline{u}$ l'est aussi, et donc si u est réduit, alors $u^{-1} = \overline{u}$.

Question 3.2 Si A contient au moins deux lettres (notons les a et b), alors $F(A)$ n'est pas commutatif puisque $\mathtt{a} \odot \mathtt{b} = \mathtt{ab} \neq \mathtt{ba} = \mathtt{b} \odot \mathtt{a}$.

Maintenant, si $A = \{\mathtt{a}\}$, il est clair que $F(A) = \left\{ \mathtt{a}^k \;\middle|\; k \in \mathbf{Z} \right\}$ (où $\mathtt{a}^0 = 1$ et, si $k < 0$, $\mathtt{a}^k = \overline{\mathtt{a}}^{|k|}$), et qu'alors

$$\mathtt{a}^{k_1} \odot \mathtt{a}^{k_2} = \mathtt{a}^{k_1+k_2}.$$

Cela prouve que $F(A)$ est un groupe commutatif (il est même isomorphe à $\mathbf{Z}$).

Ainsi, $F(A)$ est commutatif si, et seulement si A est réduit à un unique élément.

Question 3.3 Étant donné un groupe $(G, \otimes)$ et $\varphi : A \to G$, on prolonge d'abord φ à $\tilde{A}$ en posant :

$$\forall\, a \in A,\ \varphi\left(\overline{a}\right) = \left(\varphi(a)\right)^{-1}.$$

Maintenant, définissons $\psi : \tilde{A}^\star \to G$ en posant :

$$\psi(a_1 \cdots a_n) = \varphi(a_1) \otimes \cdots \otimes \varphi(a_n).$$

Pour tous u et v dans $\tilde{A}^\star$, on a $\psi(uv) = \psi(u) \otimes \psi(v)$. De plus, si $a \in \tilde{A}$, alors

$$\psi\left(ua\overline{a}v\right) = \psi(u) \otimes \varphi(a) \otimes \left(\varphi(a)\right)^{-1} \otimes \psi(v) = \psi(u) \otimes \psi(v) = \psi(uv).$$

Cela implique que pour tout $u \in \tilde{A}^\star$, on a $\psi(\rho(u)) = \psi(u)$. On en déduit que pour tout u et v dans $F(A)$, on a :

$$\psi(u \odot v) = \psi(\rho(uv)) = \psi(uv) = \psi(u) \otimes \psi(v).$$

Ainsi, la restriction de ψ à $F(A)$ est un morphisme de monoïde. Il reste à montrer que pour tout $u \in F(A)$, $\psi\left(\overline{u}\right) = \left(\psi(u)\right)^{-1}$. Mais en écrivant $u = a_1 \cdots a_n$, on a :

$$\begin{aligned}
\psi\left(\overline{u}\right) &= \psi\left(\overline{a}_n \cdots \overline{a}_1\right) \\
&= \varphi\left(\overline{a}_n\right) \otimes \cdots \otimes \varphi\left(\overline{a}_1\right) \\
&= \left(\varphi(a_n)\right)^{-1} \otimes \cdots \otimes \left(\varphi(a_1)\right)^{-1} \\
&= \left(\varphi(a_1) \otimes \cdots \otimes \varphi(a_n)\right)^{-1} \\
&= \left(\psi(u)\right)^{-1}.
\end{aligned}$$

Ainsi, $\psi|_{F(A)}$ est un morphisme de groupe de $F(A)$ dans G.

Soit maintenant ψ' un autre morphisme de groupe de $F(A)$ dans G tels que $\psi'(a) = \varphi(a)$ pour tout $a \in A$, autrement dit tel que ψ' et ψ coïncident sur A. On en déduit que les images par ψ et ψ' de tout produit fini d'éléments de $\tilde{A}$ sont égales, et donc que ψ et ψ' coïncident sur $F(A)$, ce qui assure l'unicité.

Question 3.4 Soient $A = \{a_1, \ldots, a_n\}$ et $B = \{b_1, \ldots, b_n\}$ deux alphabets de même cardinal et définissons $\varphi : A \to B$ par $\varphi(a_i) = b_i$. L'application φ peut être vue comme ayant son image dans $F(B)$, et on peut donc définir le morphisme $\varphi_A : F(A) \to F(B)$ induit par φ. De même, considérons de même le morphisme $\varphi_B : F(A) \to F(B)$ induit par φ^{-1}.

Puisque pour tout $a \in A$, on a $\varphi_B \circ \varphi_A(a) = a$, on en déduit que $\varphi_B \circ \varphi_A$ est l'unique endomorphisme induit par l'identité sur A (vue comme une fonction de A dans $F(A)$), c'est donc l'identité de $F(A)$, et on a :

$$\forall\, u \in F(A),\ \varphi_B \circ \varphi_A(u) = u.$$

De façon similaire, on prouve que $\forall\, v \in F(B)$, $\varphi_A \circ \varphi_B(v) = v$. On en déduit que φ_A et φ_B sont deux isomophismes de groupes, réciproques l'un de l'autre, et donc que $F(A)$ et $F(B)$ sont isomorphes.

4. Rang d'un groupe libre

Question 4.1 Il est claire que A est une base de $F(A)$, puisque l'application identité Id_A de A induit un morphisme bijectif sur $F(A)$, qui n'est autre que $\mathrm{Id}_{F(A)}$.

Supposons maintenant que l'on a un alphabet B, une partie X de $F(A)$ et une bijection $\varphi : B \to X$ induisant un isomorphisme de $F(B)$ dans $F(A)$ (ce qui prouve donc que X est une base de A). Soit C un autre alphabet de même cardinal que B et que X et soit ψ une bijection quelconque de C sur X, et montrons que le morphisme ψ_F induit par ψ est aussi un isomorphisme.

Pour cela, soit $f : C \to B$ défini par $f = \varphi^{-1} \circ \psi$. Il est clair que le morphisme f_F de $F(C)$ dans $F(B)$ induit par f est un isomorphisme (la réciproque étant le morphisme induit par $\psi^{-1} \circ \varphi$). On a de plus, pour tout $c \in C$, $f_F(c) = f(c) \in B$ et donc :

$$\forall\, c \in C,\ \varphi_F \circ f_F(c) = \varphi_F \circ f(c) = \varphi \circ f(c) = \psi(c).$$

Par unicité du morphisme induit par ψ, on en déduit que $\psi_F = \varphi_F \circ f_F$, et donc que ψ_F est un isomorphisme.

Cela montre que la preuve que X est une base de $F(A)$ ne dépend ni du choix de B, ni du choix de la bijection φ.

Question 4.2

1. Si $x = ab\overline{a}$ et $y = ab$, on a $a = x^{-1} \odot y$ et $b = y^{-1} \odot x \odot y$. Considérons alors l'alphabet $B = \{c, d\}$ et définissons φ par $\varphi(c) = x = ab\overline{a}$ et $\varphi(d) = y = ab$ et le morphisme φ_F induit par φ. Définissons maintenant $\psi : A \to F(B)$ par $\psi(a) = \overline{c}d$ et $\psi(b) = \overline{d}cd$ et le morphisme induit ψ_F.

   Par construction, on a $\psi_F \circ \varphi_F(c) = c$ et $\psi_F \circ \varphi_F(d) = d$ ce qui implique que $\psi_F \circ \varphi_F$

est le morphisme induit par l'application identité sur B :

$$\psi_F \circ \varphi_F = \mathrm{Id}_{F(B)}.$$

De même, on a $\varphi_F \circ \psi_F = \mathrm{Id}_{F(A)}$, ce qui prouve que φ_F est bien un isomorphisme, et donc X est une base de $F(A)$.

2. En notant $|u|$ la longueur d'un mot u, il est clair que si $u \xrightarrow{1} v$ et, plus généralement, qu si $u \xrightarrow{\infty} v$, alors $|u| \equiv |v|\,[2]$. Ayant de plus, pour tous u et v, $|uv| \equiv |u| + |v|\,[2]$ et $|\overline{u}| \equiv |u|\,[2]$. Puisque l'on a $|ab\overline{a}\overline{b}| \equiv |\overline{b}\overline{a}ba| \equiv 0\,[2]$, on en déduit que tous les mots appartenant au sous-monoïde engendré par $\{ab\overline{a}\overline{b}, \overline{b}\overline{a}ba\}$ est de longueur paire.
Ainsi, si l'on note φ_F le morphisme induit par $\varphi : B \to F(A)$ défini par $\varphi(c) = ab\overline{a}\overline{b}$ et $\varphi(d) = \overline{b}\overline{a}ba$, alors pour tout $u \in F(B)$, on a $|\varphi_F(u)| \equiv 0\,[2]$ ce qui implique que φ_F n'est pas surjectif (en particulier, ni a ni b ne sont dans son image).
Cela prouve que $\{ab\overline{a}\overline{b}, \overline{b}\overline{a}ba\}$ n'est pas une base de $F(A)$.

Question 4.3

1. Définissons l'application linéaire $\hat{\varphi}$ en spécifiant les images de vecteurs de la base E_A :
$$\forall\, e \in E_A,\ \hat{\varphi}(e) = \rho_F \circ \varphi \circ \sigma^{-1}(e).$$
Les morphismes de groupe $\hat{\varphi} \circ \sigma$ et $\rho_F \circ \sigma$ coïncident sur A, ils sont donc égaux.
2. Si φ est surjectif, alors $\hat{\varphi}$ l'est aussi. En effet, pour tout $f \in E_B$, il existe $u \in F(A)$ tel que $\varphi(u) = \rho^{-1}(f)$. On a alors $\hat{\varphi}\big(\sigma_F(u)\big) = \rho_F \circ \varphi(u) = f$ et donc $E_B \subseteq \mathrm{Im}\,\hat{\varphi}$.
On en déduit donc que $\dim V(B) \leq \dim V(A)$. Mais $\dim V(B) = \mathrm{Card}\,E_B = \mathrm{Card}\,B$ et de même pour A, d'où $\mathrm{Card}\,B \leq \mathrm{Card}\,A$.
3. Soit maintenant X une base de A et B un alphabet et φ une bijection entre B et X. Comme φ induit un isomorphisme φ_F entre $F(B)$ et $F(A)$, cela implique d'après la question précédente que $\mathrm{Card}\,A = \mathrm{Card}\,B$. Or, comme $\mathrm{Card}\,B = \mathrm{Card}\,X$, on a donc $\mathrm{Card}\,X = \mathrm{Card}\,A$ pour toute base X de A.

Question 4.4

1. Ce résultat se montre directement par récurrence, puisque :
$$a^i b^k \overline{a}^i \odot a^i b \overline{a}^i = a^i b^{k+1} \overline{a}^i \quad \text{et} \quad a^i b^k \overline{a}^i \odot a^i \overline{b} \overline{a}^i = a^i b^{k-1} \overline{a}^i.$$
2. Tout mot de u non vide de $\rho(C)$ peut s'écrire de façon unique sous la forme ${c_{i_1}}^{p_1} {c_{i_2}}^{p_2} \cdots {c_{i_n}}^{p_n}$ avec $i_k \neq i_{k+1}$. On a alors
$$\varphi(u) = a^{i_1} b^{p_1} a^{i_2 - i_1} b^{p_2} \cdots b^{p_{n-1}} a^{i_n - i_{n-1}} b^{p_n} a^{-i_n}.$$
Ainsi, si $n \neq 1$, alors $\varphi(u) \neq 1$. Maintenant, si $n = 1$, alors $\varphi\big({c_i}^p\big) = a^i b^p \overline{a}^i$ donc $\varphi\big({c_i}^p\big) = 1$ si, et seulement si $p = 0$ et donc $u = 1$. Ainsi, on a montré que
$$\forall\, u \in F(C),\ \varphi(u) = 1 \iff u = 1,$$
autrement dit que $\mathrm{Ker}\,\varphi = \{1\}$, ce qui signifie que φ est injective.
3. L'image de φ est un sous-groupe de $F\big(\{a,b\}\big)$ qui est d'ordre 2. Or, puisque φ est injectif, cela signifie que $F(C)$ est en bijection avec $\mathrm{Im}\,\varphi$, on en déduit que $\mathrm{Im}\,\varphi$ est un groupe libre de même ordre que C, autrement dit d'ordre n, et ce pour un $n \in \mathbf{N}^\star$ quelconque.
Cela prouve donc que $F(A)$ et, de façon plus générale tout groupe libre de rang 2, admet comme sous-groupe un groupe libre d'ordre $n \in \mathbf{N}^\star$ quelconque.

5. Mots cycliquement réduits et conjugaison

Question 5.1 Étant donné un mot $u \in F(A)$, considérons l'ensemble
$$E = \big\{\, w \in F(A) \;\big|\; \exists\, v \in F(A) : u = \overline{w} v w \,\big\}.$$

Il est clair que cet ensemble est fini, non vide (il contient 1), et que pour tous mots w et w' de E, le plus court des deux est préfixe de l'autre. En particulier, si $|w'| = |w| + 1$, en écrivant $u = \overline{w} v w$ et $u = \overline{w}' v' w'$, il existe un lettre a telle que $w' = aw$ et donc que $v = \overline{a} v' v$, ce qui prouve que v n'est pas cycliquement réduit.

Soit maintenant w le mot de E de longueur maximale et soit v tel que $u = \overline{w} v w$. D'après le résultat précédent, c'est la seule décomposition de u pour laquelle v est susceptible d'être cycliquement réduit. Or, si ce n'était pas le cas, en écrivant $v = \overline{a} v' a$, alors on aurait $aw \in E$ ce qui n'est pas le cas.

Ainsi, la décomposition $u = \overline{w} v w$ est bien l'unique telle que v est cycliquement réduit.

Ainsi, si u n'est pas le mot vide, alors v non plus (car si $v = 1$, alors $u = \overline{w} w = 1$) et, pour tout $n > 0$, on aalors
$$u^n = \underbrace{\overline{w} v w\ \overline{w} v w\ \cdots\ \overline{w} v w}_{n \text{ fois}} = \overline{w} v^n w \neq 1.$$

Question 5.2 Montrons que $\equiv$ est un relation d'ordre. Tout d'abord, elle est réflexive, puisque pour tout $u \in F(A)$, $u = \overline{1} \odot u \odot 1$. Maintenant, si $u \equiv v$ et $v \equiv w$, en écrivant $u = \overline{x} \odot v \odot x$ et $v = \overline{y} \odot w \odot y$, on a $u = \overline{(y \odot x)} \odot w \odot (y \odot x)$, ce qui assure la transitivité de $\equiv$. Pour la symétrie, avec les notations précédentes, on a $v = \overline{\overline{x}} \odot u \odot \overline{x}$.

Question 5.3 Si u et v cycliquement réduits sont conjugués, il existe un mot $w \in F(A)$ tel que $u = \overline{w} \odot v \odot w$, et considérons un tel mot w de longueur minimale (il est en particulier réduit). Comme la première lettre de $\overline{w}$ et la dernière lettre de w sont complémentaires l'une de l'autre et que u est réduit, cela signifie que lors de la réduction de $\overline{w} v w$, l'une ou l'autre lettre doit disparaître, ce qui signifie que $\overline{w}$ ou w doit "disparaître entièrement".

Supposons par exemple que $\overline{w}$ "disparaisse" lors de la réduction. Cela signifie que l'on peut écrire v sous la forme $v = wv'$ et qu'alors $u = v' \odot w$. Or, puisque v est cycliquement

réduit, la première lettre de w et la dernière lettre de v' ne sont par complémentaires l'un de l'autre, et donc $v' \odot w = v'w$.

Le raisonnement est similaire si l'on suppose que c'est w qui disparaît lors de la réduction de $\overline{w}vw$, et dans les deux cas, on a pu trouver deux mots (réduits) r et s tels que $u = rs$ et $v = sr$.

Question 5.4 Soient maintenant deux mots réduits u et u'. Décomposons les comme à la question 5.1 :

$$u = \overline{w}vw, \qquad u' = \overline{w}'v'w'.$$

Il est clair que $u \equiv v$ et $u' \equiv v'$ et que, par transitivité, $u \equiv u'$ si, et seulement si $v \equiv v'$. Mais comme v et v' sont cycliquement réduits, on peut appliquer la question précedente.

En résumé, cela nous indique un algorithme simple pour déterminer si deux mots réduits sont conjugués :

1. on décompose u et u' à la manière de la question 5.1. En particulier, w se détermine simplement en étant le plus grand préfixe commun à u et $\overline{u}$.
2. on regarde si les mots v et v' obtenus sont permutation cyclique l'un de l'autre. En effet, u et u' sont conjugués si, et seulement si v et v' sont permutation cyclique l'un de l'autre.

6. Groupe fondamental d'un graphe

Question 6.1 Considérons l'étiquette u d'un chemin. Cette étiquette n'est pas réduite si et seulement si elle contient deux lettres successives de la forme $a\overline{a}$. Cela se traduit par l'existence de trois sommets p, q et r tels que le chemin comporte deux arêtes consécutives $(p,a,q)(q,\overline{a},r)$. Mais, le graphe étant réduit, cela n'est possible que si $p = r$. Ainsi, l'étiquette n'est pas réduit si et seulement si le chemin correspondant n'est pas réduit.

Question 6.2 Procédons par récurrence, et supposons que pour $n \in \mathbf{N}$, de tout chemin de s à t de longueur au plus n et d'étiquette x, on peut déduire un chemin réduit de s à t d'étiquette $\rho(x)$. Considérons l'étiquette x d'un chemin p de s à t de longueur $n+1$. Si x est réduite, alors d'après la question précédente, le chemin est réduit. Sinon, on peut écrire $x = ya\overline{a}z$ et trouver deux états u et v tels que y est l'étiquette d'un chemin p_1 de s à u, z celle d'un chemin p_2 de u à t, et que le graphe contient l'arête (p,a,q). Dans ce cas, le chemin p_1p_2 d'étiquette yz relie s à t. On en déduit par récurrence qu'il existe un chemin réduit p' de s à t d'étiquette $\rho(yz) = \rho(x)$.

Question 6.3 L'ensemble $G(\Gamma, s_0)$ contient le mot vide, étiquette du chemin vide. De plus, si x est l'étiquette d'un chemin p de s_0 à s_0, alors il en est de même pour $\overline{x}$ qui est l'étiquette du chemin obtenu à partir de p en inversant l'ordre des sommets traversés. Enfin, si x et y sont les étiquettes de deux chemins réduits p et q, alors xy est l'étiquette du chemin concaténé xy dont on déduit, à l'aide de la question précédente, que $x \odot y = \rho(xy)$ est l'étiquette d'un chemin réduit de s_0 à s_0.

Question 6.4 Si Γ est une forêt, alors pour tout sommet s_0, il existe au plus un chemin réduit de s_0 à s_0. Or, le chemin vide en s_0 est réduit, c'est donc l'unique possible, et on en déduit qu'alors $G(\Gamma, s_0) = \{1\}$.

Question 6.5 Commençons par décrire l'algorithme, qui est une forme de parcours de graphe. On procède ainsi :

1. Étant donné le sommet $s_0 \in V$, on définit $V' = \{s_0\}$, $E' = \emptyset$ et $F = \mathrm{Vois}(s_0)$ où la fonction de voisinage Vois est définit par :

$$\mathrm{Vois}(s) = \{\, t \in V \mid \exists a \in A \colon (s,a,t) \in E \,\}.$$

2. Tant que $F \neq \emptyset$, faire :
   (a) choisir $t \in F$ et ainsi que $s \in V'$ et $a \in A$ tel que $(s,a,t) \in E$ (de tels éléments existent par construction de F) ;
   (b) effectuer les affectations :

$$\begin{aligned} V' &\leftarrow V' \cup \{t\}, \\ E' &\leftarrow E' \cup \{(s,a,t)\}, \\ F &\leftarrow F \setminus \{t\} \cup \left\{\, t' \in \mathrm{Vois}(t) \;\middle|\; t' \notin V' \,\right\} ; \end{aligned}$$

3. Retourner le graphe $\Gamma' = (E', V')$.

Il est clair qu'à chaque entrée et sortie de la boucle, (E', V') est un sous-arbre de Γ. En effet, c'est le cas au début de l'algorithme, est si cette propriété est vérifiée en entrée de la boucle, on ajoute à l'intérieur de la boucle un nouveau sommet au graphe ainsi qu'une arête d'un sommet déjà présent au sommet ajouté. Cela assure d'une part que le sous-graphe ne contient pas de cycle (c'est donc une forêt) et qu'il est connexe.

Vérifions qu'en fin d'algorithme, on a $V' = V$. Supposons par l'absurde que ce n'est pas le cas, et soit $t_0 \in V \setminus V'$. Par connexité de Γ, il existe un chemin réduit de s_0 à t_0. En particulier, sur ce chemin, il existe une arête (s_1, a, t_1) telle que $s_1 \in V'$ et $t_1 \in V \setminus V'$. On aboutit alors à une absurdité, puisque à l'étape où s_1 a été ajouté à V', puisque $t_1 \in \mathrm{Vois}(s_1)$, t_1 a été ajouté à F à cette même étape. Or, à la fin de l'algorithme, on a $F = \emptyset$ et le seul moyen de supprimer un sommet de F est de l'incorporer à E'. Nous aboutissons alors à une absurdité, puisque $t_1 \notin V'$.

En conclusion, on a bien $V' = V$ et donc le graphe Γ' retourné par l'algorithme est bien un sous-arbre couvrant de Γ. On remarque au passage que l'algorithme (avec la preuve de sa correction) consistue une preuve constructive de l'existence d'un sous-arbre de Γ.

Question 6.6 Soit un élément $x \in G(\Gamma, s_0)$, et p un chemin réduit de s_0 à s_0 d'étiquette x. On peut bien sûr décomposer ce chemin comme suggéré dans l'énoncé, en écrivant

$$p = p_0 e_1 p_1 \cdots e_r p_r,$$

de telle sorte que les chemins réduits p_i ne comportent que des arêtes de $\tilde{E}_T$ et les arêtes e_i appartiennent à $\tilde{E} \setminus \tilde{E}_T$. Notons $e_i = (s_i, a_i, t_i)$. Pour i tel que $0 < i < r$, le chemin réduit p_i va de t_i à s_{i+1}. Par unicité, son étiquette est égale à $\overline{x}_{t_i} \odot x_{s_{i+1}}$. De plus, l'étiquette de p_0 est x_{s_1}, et celle de p_r est $\overline{x}_{t_r}$, d'où :

$$\begin{aligned} x &= x_{s_1} a_1 \left(\overline{x}_{t_1} \odot x_{s_2}\right) a_2 \left(\overline{x}_{t_2} \odot x_{s_3}\right) a_3 \cdots a_{r-1} \left(x_{t_{r-1}} \odot x_{s_r}\right) a_r \overline{x}_{t_r} \\ &= \left(x_{s_1} a_1 \overline{x}_{t_1}\right) \odot \left(x_{s_2} a_2 \overline{x}_{t_2}\right) \odot \cdots \odot \left(x_{s_r} a_r \overline{x}_{t_r}\right) \\ &= b_{e_1} \odot b_{e_2} \odot \cdots \odot b_{e_r}. \end{aligned}$$

Bien sûr, pour $e = (s, a, t) \in E \setminus E_T$, on pose $b_{\overline{e}} = x_t \overline{a} x_s = \overline{b_e}$.

Question 6.7 La question précédente montre que le morphisme $\varphi_F : F(E \setminus E_T) \to F(A)$ défini par $\varphi(e) = b_e$ vérifie $\operatorname{Im} \varphi_F = G(\Gamma, s_0)$.

Pour montrer que $G(\Gamma, s_0)$ est libre de rang r, il reste à montrer que φ_F est injectif. Pour cela, montrons par récurrence sur la taille des mots de $F(E \setminus E_F)$ que pour tout mot $u = e_1 e_2 \dots e_n$ (pour $n \geq 1$, et où l'on note $e_i = (s_i, a_i, t_i)$), $\varphi_F(u)$ peut s'écrire sous la forme

$$x_{s_1} a_1 v_1 a_2 v_2 a_3 \cdots a_n \overline{x_{t_n}}$$

avec $v_1, \dots, v_{n-1}$ des mots réduits.

Pour $n = 1$, si $e = (s, a, t)$, on a $\varphi(e) = b_e = x_s a \overline{x}_t$, donc l'hypothèse de récurrence est bien vérifiée.

Si maintenant l'hypothèse de récurrence est supposée est vérifiée au rang $n \geq 1$, soit $u = e_1 \dots e_{n+1}$ un mot réduit de longueur $n+1$. Avec les notations précédentes, on a

$$\varphi_F(e_1 \dots e_n) = x_{s_1} a_1 v_1 a_2 v_2 a_3 \cdots a_n \overline{x_{t_n}},$$

et donc

$$\varphi_F(e_1 \dots e_{n+1}) = x_{s_1} a_1 v_1 a_2 v_2 a_3 \cdots a_n \overline{x_{t_n}} \odot x_{s_{n+1}} a_{n+1} \overline{x}_{t_{n+1}}.$$

Maintenant, deux cas sont possibles :

– si $s_{n+1} \neq t_n$, alors $\overline{x_{t_n}} \odot x_{s_{n+1}}$ est l'étiquette de l'unique chemin réduit allant de t_n à s_{n+1}. En particulier, ce n'est pas le mot vide et l'on a alors

$$\varphi_F(e_1 \dots e_{n+1}) = x_{s_1} a_1 v_1 a_2 v_2 a_3 \cdots a_n \underbrace{\left(\overline{x_{t_n}} \odot x_{s_{n+1}}\right)}_{v_{n+1}} a_{n+1} \overline{x}_{t_{n+1}} ;$$

– sinon, $s_{n+1} = t_n$. Dans ce cas, $\overline{x_{t_n}} \odot x_{s_{n+1}}$ est le mot vide. Mais puisque u est supposé réduit, on a alors $a_n \neq \overline{a}_{n+1}$, et donc $a_n a_{n+1}$ est réduit. On a alors la décomposition voulue, avec $v_{n+1} = 1_A$.

Cette récurrence montrer que pour tout $u \in F(E \setminus E_T)$, $\left|\varphi_F(u)\right| \geq \left|u\right|$. En particulier, on a $\varphi_F(u) = 1_A$ si, et seulement si $u = 1_{E \setminus E_T}$, ce qui prouve l'injectivité de φ_F.

En conclusion, φ_F réalise un isomorphisme entre $F(E \setminus E_T)$ et $G(\Gamma, s_0)$, ce qui montre que ce dernier est un groupe libre de rang $\operatorname{Card}(E \setminus E_T) = n$.

7. Sous-groupes d'un groupe libre

Question 7.1 Soit x un élément de $L(\mathscr{A})$, et soit p le chemin de Γ allant de s_0 à s_0 et d'étiquette x. Si l'on modifie le chemin p en un chemin q de Δ en effectuant la même manipulation de sommets que celle utilisée pour passer de Γ à Δ, le chemin q obtenu est une chemin de t_0 à t_0 d'étiquette x. Cela montre que l'on a « $x \in L(\mathscr{A}) \implies x \in L(\mathscr{B})$ », autrement dit que $L(\mathscr{A}) \subseteq L(\mathscr{B})$.

Cela implique en particulier que $\rho(L(\mathscr{A})) \subseteq \rho(L(\mathscr{B}))$.

Soit maintenant un chemin q de t_0 à t_0 étiquetté par un mot y. On peut décomposer q sous la forme $q = q_1 q_2 \cdots q_n$ de telle sorte que :

– chacun des q_i s'obtient à partir d'un chemin p_i de Γ en renumérotant les sommets comme précédemment ;

– pour $0 \leq i < n$, p_i aboutit à v et p_{i+1} part de v', ou réciproquement.

Dans ce cas, on peut définir un chemin p de Γ allant de s_0 à s_0 de la forme

$$p = p_1 r_1 p_2 r_2 p_3 \cdots p_{n-1} r_{n-1} p_n$$

où r_i est soit $(v, a, u)(u, \overline{a}, v')$ ou $(v', a, u)(u, \overline{a}, v)$ (ou les deux possibilités restant en échangeant a et $\overline{a}$). Si l'on note x l'étiquette de p, il est clair que $\rho(x) = \rho(y)$.

Cela achève de prouver que $\rho(L(\mathscr{A})) = \rho(L(\mathscr{B}))$.

Question 7.2 Soit G le sous-groupe engendré par les mots $h_1, \dots, h_n$ de $F(A)$. Or, par définition, il s'agit précisément

Considérons un automate $\mathscr{A}$ construit par récurrence de la façon suivante :

1. $V = \{s_0\}$ et $E = \emptyset$;
2. pour chaque mot $h_i = a_1 \cdots a_{n_i}$ de longueur $n_i \geq 1$,
   (a) on ajoute à V $n_i - 1$ nouveaux sommets $t_1, \dots, t_{n_i - 1}$;
   (b) en notant $t_0 = t_{n_i} = s_0$, on ajoute à E les arêtes $(t_0, a_1, t_1), \dots, (t_{n_i - 1}, a_{n_i}, t_{n_i})$.

Par construction, les seuls chemins simples de $\mathscr{A}$ reliant s_0 à s_0 sont étiquettés soit par l'un des h_i, soit par l'un des $\overline{h}_i$.

Ainsi, l'ensemble $L(\mathscr{A})$ est égal à l'ensemble des produits finis des h_i et des $\overline{h}_i$ et donc $G = \rho(L(\mathscr{A}))$.

Maintenant, construisons une suite finie d'automates de la façon suivante :

1. on pose $\mathscr{A}_0 = \mathscr{A}$ et $n = 0$, et
2. tant que le graphe correspondant à $\mathscr{A}_n$ n'est pas réduit, soit $\mathscr{B}$ tel que $\mathscr{A}_n \xrightarrow{1} \mathscr{B}$, définir $\mathscr{A}_{n+1} = \mathscr{B}$ et incrémenter n.

Notons $\mathscr{A}_n = (\Delta, t_0)$. D'après la question précédente, il est claire que $G = \rho(L(\mathscr{A}_n))$. De plus, comme Δ est réduit, on a $\rho(L(\mathscr{A}_n)) = G(\Gamma, t_0)$. En particulier, c'est un groupe libre.

Cela montre donc que le sous-groupe engendré par un nombre fini de mots est un groupe libre.

Question 7.3 L'algorithme pour trouver une base d'un groupe libre finiment engendré est maintenant clair :

1. on commence par engendrer l'automate comme expliqué précédemment ;
2. on réduit cet automate ;
3. on en détermine un arbre couvrant, et on en déduit une base.

Pour en mesurer la complexité, il est clair qu'il faut prendre comme mesure du problème la somme des longueurs des mots :

$$n = \sum_i |h_i|$$

Ainsi, l'automate créé comporte $O(n)$ sommets et arêtes, et sa création se fait en temps linéaire.

Pour la réduction (qui s'effectue en au plus $O(n)$ étapes, le nombre de sommets diminuant de 1 à chaque fois), la recherche d'une paire d'arêtes à réduire s'effectue en temps linéaire, et il en est de même pour la réduction proprement dite. Pour que cela soit faisable, il faut cependant une représentation convenable des données. On propose par exemple d'associer à chaque sommet s et chaque lettre a l'ensemble des sommets t tels que (s, a, t) est une arête, cet ensemble pouvant par exemple être représenté par une liste. On associe de plus l'ensemble des sommets t tels que (t, a, s) soit une arête. La détermination d'une paire à réduire se faire alors simplement en parcourant ces tableaux à la recherche d'un ensemble comportant au moins 2 éléments. Le coût total est donc en $O(n^2)$.

Ensuite, la détermination d'un sous-arbre couvrant se fait en $O(n^2)$, et de même pour celle d'une base (qui revient à lister les arêtes e non retenus dans l'arbre couvrant et de calculer les étiquettes b_e des chemins correspondants).

Au total, l'algorithme s'effectue donc en $O(n^2)$.

8. Représentations des groupes libres

Question 8.1 L'existence d'un morphisme de groupes de $F(A)$ dans $\mathrm{GL}_2(\mathbf{R})$ découle de questions précédentes (où il était appelé φ_F). Montrons son caractère injectif. Pour cela, considérons les images par $\varphi(a)$ des Y_a, $Y_{\overline{a}}$, Y_b et $Y_{\overline{b}}$.

Remarquons tout d'abord que $Y_a \cup Y_{\overline{a}} \cup Y_b \cup Y_{\overline{b}} = \mathbf{R}^2$.

Maintenant, soit $\vec{u} = \binom{x}{y} \in \mathbf{R}^2$. Posons $\vec{v} = \binom{x'}{y'} = \alpha \binom{x}{y} = \binom{x+2y}{y}$.

Si $\vec{u} \in Y_a$, on a $x'y' = xy + 2y^2 \geq 0$ et

$$\begin{aligned} x'^2 - y'^2 &= (x' + y')(x' - y') \\ &= (x + 3y)(x + y) = x^2 + 4xy + 3y^2 \\ &\geq 0 \end{aligned}$$

En particulier, $x'^2 \geq y'^2$ et donc $|x'| \geq |y'|$ et donc $\alpha\vec{u} \in Y_a$.

Si $\vec{u} \in Y_b \cup Y_{\overline{b}}$, on a $|x| \leq |y|$ (et, donc, $x^2 \leq y^2$), d'où :

$$\begin{aligned} x'^2 - y'^2 &= x^2 + 4xy + 3y^2 \\ &\geq 2x^2 + 4xy + 2y^2 \\ &= 2(x + y)^2 \geq 0 \end{aligned}$$

Ainsi, si $\vec{u} \in Y_a \cup Y_b \cup Y_{\overline{b}}$, alors $\alpha\vec{u} \in Y_a$ (cela implique, bien sûr, que ce n'est pas le cas si $\vec{u} \in Y_{\overline{a}}$, puisque α est une matrice inversible qui, donc, réalise une bijection de $\mathbf{R}^2$ dans lui-même).

Par symétrie, on en déduit que pour toutes lettres a et b, si $a \neq \overline{b}$, alors $\varphi(a)(Y_b) \subseteq Y_a$.

Soit maintenant $u = a_1 a_2 \dots a_n$ un mot réduit non vide. En particulier, on peut remarquer que $a_{i+1} \neq \overline{a}_i$.

Posons $E_{n+1} = \mathbf{R}^2 \setminus Y_{\overline{a_n}}$ et, pour tout k compris entre 1 et n,

$$E_k = \varphi(a_k)(E_{k+1}).$$

D'après la remarque précédente, on a $E_n \subseteq Y_{a_n}$, et pour tout k, si $E_{k+1} \subseteq Y_{a_{k+1}}$, alors comme $a_k \neq \overline{a}_{k+1}$, on en déduit que $E_k = \varphi(a_k)(E_{k+1}) \subseteq Y_{a_k}$. Ainsi, par récurrence, on a :

$$E_1 = \varphi_F(u)(E_{n+1}) \subseteq Y_{a_1}.$$

On a donc finalement $\varphi_F(u)\left(\mathbf{R}^2 \setminus Y_{\overline{a_n}}\right) \subseteq Y_{a_1}$, ce qui prouve que $\varphi_F(u)$ n'est pas l'application linéaire identité, et donc que φ_F n'est injective.

Question 8.2 Posons $R = \sum_{k=0}^{\infty} (-1)^n a^n = 1 - a + a^2 - a^3 + \cdots$. On a alors $R(1 + a) = 1$ puisque pour $k \geq 1$, le coefficient associé à a^k est $(-1)^k + (-1)^{k-1} = 0$. De plus, on a bien sûr $(1 + a)R = R(1 + a) = 1$.

Ainsi, $1+a \in U(A)$.

Question 8.3 À nouveau, il n'est nécessaire que de se pencher sur l'injectivité, l'existence ayant été discutée précédemment.

Notons tout d'abord, d'après la question précédente, que le coefficient de a de $(1+a)^k$ est égal à k pour $k \geq 1$ et que cette relation se généralise aussi au cas $k = 0$ et $k \leq -1$ (puisque il vaut -1 pour l'inverse de $1+a$).

Soit maintenant un mot non vide u écrit, comme suggéré par l'énoncé :

$$u = a_1^{r_1} a_2^{r_2} \cdots a_n^{r_n},$$

avec $a_i \neq a_{i+1}$ (et, u étant réduit, $a_i \neq \overline{a}_{i+1}$) et $r_i \neq 0$. En particulier, le mot $\sqrt{u} = a_1 a_2 \cdots a_n$ est réduit et on montre facilement par récurrence sur n que le coefficient de $\sqrt{u}$ est égal à $r_1 \times r_2 \times \cdots \times r_n$.

En particulier, il est non nul, et donc si u n'est pas le mot nul, alors $\varphi_F(u)$ n'est pas égal à 1. Ainsi, φ_F est injectif.

$\underleftarrow{a}\,\underrightarrow{b}\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,\underleftarrow{b}\,\underrightarrow{\overline{a}}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\underleftarrow{\overline{a}}\,\underrightarrow{a}\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\underleftarrow{\overline{b}}\,\underrightarrow{\overline{b}}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$\underleftarrow{a}\,b\,\overline{a}\,a\,\overline{b}\,\underrightarrow{\overline{b}}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\underleftarrow{\overline{b}}\,\underrightarrow{a}\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,\underleftarrow{a}\,\underrightarrow{a}\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,\underleftarrow{a}\,\underrightarrow{b}\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,\underleftarrow{b}\,\underrightarrow{\overline{b}}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\underleftarrow{\overline{a}}\,\underrightarrow{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\underleftarrow{a}\,\underrightarrow{\overline{a}}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\underleftarrow{\overline{b}}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,\underrightarrow{a}\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,\underleftarrow{a}\,\underrightarrow{a}\,b\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,\underleftarrow{a}\,\underrightarrow{b}\,\overline{b}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,\underleftarrow{b}\,\underrightarrow{\overline{b}}\,\overline{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\underleftarrow{\overline{a}}\,\underrightarrow{a}\,a\,b$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,\underleftarrow{a}\,\underrightarrow{b}$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\underleftarrow{\overline{a}}\,\underrightarrow{b}$

$a\,b\,\overline{a}\,a\,\overline{b}\,\overline{b}\,a\,a\,b\,\overline{b}\,\overline{a}\,\overline{a}\,a\,a\,b\,\overline{b}\,\overline{a}\,a\,b$

FIGURE 1 – Déroulement de l'algorithme

```
let reduire complementaire mot = begin
  let rec aux mi li lj mj = begin
    if complementaire li lj
    then begin
      match mi with
      | li' :: mi' -> begin
        match mj with
        | lj' :: mj' -> aux mi' li' lj' mj'
        | [] -> List.rev mi
      end
      | [] -> begin
        match mj with
        | a :: b :: mj' -> aux [] a b mj'
        | _ -> mj
      end
    end
    else begin
      match mj with
      | [] -> List.rev (lj :: li :: mi)
      | a :: mj' -> aux (li :: mi) lj a mj'
    end
  end in
  match mot with
  | a :: b :: mot' -> aux [] a b mot'
  | _ -> mot
end ;;
```

FIGURE 2 – Algorithme programmé en OCaml