CORRECTION DE L'ÉPREUVE INFORMATIQUE DU CONCOURS ENS 2001

J. CASSAIGNE, G. HANROT ET P. LESCANNE

Première partie

1.1. Si le mot $x = x_1 \dots x_n$ est non vide, alors on prouve facilement par récurrence sur n que nécessairement $f(x) = f(x_1) \dots f(x_n)$; $f(x)$ est donc bien défini.

Pour $f(\varepsilon)$, noter qu'on a $f(\varepsilon\varepsilon) = f(\varepsilon) = f(\varepsilon)f(\varepsilon)$, d'où $f(\varepsilon) = \varepsilon$.

1.2. Il suffit de prendre $G_2 = (A_2, (a \mapsto bb, b \mapsto a), b)$. On a alors

$$S(G_2) = (b, a, bb, aa, bbbb, \dots) \neq S(G_1),$$

tandis que par récurrence sur n on peut prouver que si $f = (a \mapsto bb, b \mapsto a)$, $f^{2n}(b) = b^{2^n}$, $f^{2n+1}(b) = a^{2^n}$, donc $L(G_2) = L(G_1)$.

1.3. Les 5 premiers termes de $S(T)$ sont a, ab, $abba$, $abbabaab$, $abbabaabbaababba$. Considérons alors le morphisme i comme dans la question 1.2. Il est facile de voir que $\theta\iota = \iota\theta$; comme le composé de deux morphismes est manifestement un morphisme, en vertu de 1.1, cela découle de $\theta\iota(a) = ba = \iota\theta(a)$ et $\theta\iota(b) = ab = \iota\theta(b)$.

On peut alors montrer par récurrence que $\theta^{n+1}(a) = \theta^n(a)i(\theta^n(a))$. C'est vrai pour $n = 1$, et si c'est vrai au rang $k-1$, on a $\theta^{k+1}(a) = \theta(\theta^k(a)) = \theta(\theta^{k-1}(a))\theta(i(\theta^{k-1}(a))) = \theta^k(a)i(\theta^k(a))$. Comme il est clair que $|i(x)| = |x|$, on a $|\theta^k(a)| = 2^k$.

Si $L(T)$ est rationnel et infini, en vertu du lemme de l'étoile il existe $(u, v, w) \in A^* \times A^+ \times A^*$ tels que $uv^n w \in L$ pour tout entier n. Or $|uv^n w| = n|v| + |u| + |w|$. Si cette quantité est une puissance de 2 pour tout $n > 0$, il existe $k < k' < k''$ tels que $|u| + |v| + |w| = 2^k$, $|u| + 2|v| + |w| = 2^{k'}$, $|u| + 3|v| + |w| = 2^{k''}$, soit $2^{k'} - 2^k = 2^{k''} - 2^{k'}$, ou encore $2^{k'+1} - 2^k = 2^{k''}$, d'où $k'' < k' + 1$, contradiction.

On voit donc que $L(T)$ n'est pas rationnel.

1.4. Il est aisé de montrer (par récurrence) que $L(A_2, (a \mapsto ab, b \mapsto b), a) = \{ab^n, n \geq 0\}$. Par suite, $L(H) = \{a^n, n \geq 1\} = A_1^+$. S'il existe un $D0L$-système G tel que $L(G) = L(H)$, on a forcément $u_0 = a^k$ pour un certain k, et $f(a) = a^l$ pour un certain l. Il vient $L(G) = \{a^{kl^i}, i \geq 0\}$, ce qui ne peut être égal à A_1^+ pour aucune valeur de (k, l).

Corrigé rédigé par G. Hanrot en partie à l'aide de notes et suggestions de J. Cassaigne et P. Lescanne. G. Hanrot est seul responsable des erreurs ou imprécisions éventuelles de ce corrigé.

Deuxième partie

2.1. Notons tout d'abord que l'alphabet A étant fini, l'ensemble des mots sur A de longueur inférieure à un entier l donné est fini. Il s'ensuit que L, qui est infini, contient des mots de longueur arbitrairement grande.

Soient $\mathbf{y}$ et $\mathbf{z}$ deux mots infinis engendrés par L. Montrons que $y_l = z_l$ pour tout entier l : il existe un mot m de L de longueur $> l$; ce mot est préfixe de $\mathbf{y}$, ce qui impose $m_l = y_l$, et de même il est préfixe de $\mathbf{z}$, ce qui impose $m_l = z_l$, d'où $y_l = z_l$, et donc $\mathbf{y} = \mathbf{z}$.

À l'inverse, il est facile de voir que l'ensemble des préfixes d'un mot infini $\mathbf{y}$ est infini (on construit une bijection de $\mathbb{N}$ dans cet ensemble en associant à un entier k le préfixe de longueur k correspondant), et que cet ensemble engendre donc le mot infini $\mathbf{y}$.

2.2. Si L engendre un mot infini $\mathbf{y}$, L est infini par la partie (i) de la définition. En outre, si $u, v \in L$, on sait que u et v sont tous deux préfixes de $\mathbf{y}$; supposons sans perte de généralité que $|u| \geq |v|$; alors que pour tout $j \leq |u|$, $u_j = \mathbf{y}_j = v_j$, donc v est préfixe de u.

Réciproquement, on va construire le mot correspondant lettre par lettre. Soit l un entier ; L étant infini, il existe un mot $m^{(l)}$ de L de longueur $> l$, on choisit le mot de longueur minimale ayant cette propriété ; ce dernier est unique, car deux mots de même longueur dont l'un est préfixe de l'autre sont égaux. On pose alors $y_l = m_l^{(l)}$.

Montrons que $\mathbf{y}$ est bien engendré par L. Soit m un mot de L ; pour chaque $k \leq |m|$, $m^{(k)}$ est préfixe de m ; il s'ensuit que $m_k^{(k)} = m_k$, et donc que m est préfixe de $\mathbf{y}$, ce qui prouve que L engendre bien un mot infini (unique d'après 2.1).

2.3. Il suffit de prendre le $D0L$-système $G = (A_2, (a \mapsto ab, b \mapsto ab), a)$, pour lequel $L(G) = \{a\} \cup \{(ab)^{2^k}, k \in \mathbb{N}\}$, dont on vérifie aisément qu'il engendre le mot $\mathbf{q}$.

2.4. Si G engendre un mot infini, en vertu de 2.2, soit u_0 est préfixe de $f(u_0)$, soit l'inverse. Dans ce second cas, $u_0 = f(u_0)v$ et donc $f^k(u_0) = f^{k+1}(u_0)f^k(v)$, donc la suite $|f^k(u_0)|$ est positive décroissante, donc stationnaire. Il s'ensuit que la suite $f^k(u_0)$ est elle-même stationnaire, et donc que $L(G)$ est fini, impossible. Donc u_0 est bien préfixe de $f(u_0)$. Réciproquement, si u_0 est préfixe de $f(u_0)$, une récurrence facile montre que $f^k(u_0)$ est préfixe de $f^l(u_0)$ pour $k \leq l$; on conclut alors en appliquant 2.2 à $L(G)$.

2.5. Il suffit de prendre $K_1 = (A_3, (a \mapsto b, b \mapsto c, c \mapsto \varepsilon), a)$, pour lequel $L(K_1) = A_3$. Comme $L(K_1)$ est fini, K_1 n'engendre pas de mot infini.

2.6. Pour $K_2 = (A_2, (a \mapsto ab, b \mapsto c, c \mapsto \varepsilon), a)$ on a $u_0 = a$, $u_1 = ab$, $u_k = abc$ pour $k \geq 2$, et donc $L(K_2) = \{a, ab, abc\}$ et K_2 n'engendre pas de mot infini car $L(K_2)$ est fini.

2.7. Il suffit par exemple de prendre G_1 donné dans la page 1 de l'énoncé, car $f(u_0)$ n'est pas préfixe de u_0. En revanche, on a bien $L(G_1)$ infini.

2.8. Dans 2.6, la seule lettre immortelle est a : en effet, $f^2(b) = f(c) = \varepsilon$, tandis que $|f^k(a)| = |f^{k-1}(a)| + |f^{k-1}(b)| \geq |f^{k-1}(a)|$, d'où $|f^k(a)| \geq 1$ pour tout k.

Si $f(u_0) = u_0 v$, on a par récurrence

$$f^k(u_0) = u_0 v f(v) f^2(v) \ldots f^{k-1}(v).$$

Si toutes les lettres de v sont mortelles, pour toute lettre x de v, il existe j_x tel que $f^{j_x}(x) = \varepsilon$; posant $j = \max_{x \text{ lettre de } v} j_x$, on a $f^j(x) = \varepsilon$ pour toute lettre x de v, et par suite $f^j(v) = \varepsilon$. Il s'ensuit que la suite $f^k(u_0)$ est stationnaire pour $k \geq j$, et donc $L(G) = \{u_0, f(u_0), \ldots, f^j(u_0)\}$ est fini.

Inversement, si v contient au moins une lettre immortelle, on a $|f^j(v)| \geq 1$ pour tout j, et donc $|f^k(u_0)| \geq |f^{k-1}(u_0)| + 1 \geq k$, et $L(G)$ contient des mots arbitrairement longs, donc est infini.

2.9. L'élément $N[x, y]$ de la matrice N mesure le nombre d'occurrences de la lettre x dans $f(y)$.

La terminaison de l'algorithme est claire, car dans la boucle **tant que**, x peut prendre au plus une fois la valeur d'une lettre donnée de l'alphabet. La boucle **tant que** est donc exécutée au plus Card A fois.

Au début de chaque itération de la boucle **tant que**, $T \cup M$ est l'ensemble des lettres y telles que $L[y] = 0$, et $L[y]$ est la longueur du mot $f(y)$ dans lequel on a effacé toutes les lettres de M :
- c'est vrai initialement ($M = \emptyset$, T est l'ensemble des lettres telles que $f(y) = \varepsilon$, et $L[y]$ est la longueur de $f(y)$) ;
- la boucle consiste à faire passer un x de T dans M, mettre à jour les $L[y]$ en effaçant les occurrences de x, et ajouter les y tels que $L[y]$ dans T, ce qui fait qu'en fin de boucle, la propriété ci-dessus reste vérifiée.

Toute lettre x de $T \cup M$ est mortelle. En effet, soit i l'indice de l'étape où x est ajoutée dans $T \cup M$. Si $i = 0$ (x initialement dans T, c'est clair). Si c'est vrai pour les lettres ajoutées avant la i-ème it eration, et si x est ajoutée à la i-ème itération, on a alors $L[x] = 0$, ce qui implique que $f(x)$ ne contient que des lettres déjà dans $T \cup M$ à la fin de la $(i - 1)$-ème itération, donc mortelles par récurrence.

Inversement, toute lettre mortelle finit par se trouver dans T, donc dans M ; soit i le plus petit indice tel que $f^i(x) = \varepsilon$, on le prouve par récurrence sur i. Si $i = 0$, la lettre est initialement dans T ; sinon $f(x)$ est constitué de lettres z telles que $f^{i-1}(z) = \varepsilon$, donc toutes ces lettres finissent par se trouver dans M, et à ce stade, $L[x] = 0$, donc x est ajouté à T.

La complexité de la première boucle est $O(k^2)$, celle de la seconde $O(m)$. La troisième boucle est effectuée au plus k fois, et la boucle intérieure fait alors au plus k itérations, d'où une complexité de $O(k^2)$ pour la troisième boucle, et une complexité totale de $O(k^2 + m)$.

2.10. Il suffit de vérifier que u_0 est préfixe de $f(u_0)$, et que le suffixe correspondant n'est pas constitué uniquement de lettres mortelles, puis ensuite d'itérer f.

MOT-INFINI(A, f, u_0, ℓ)
- $z = f(u_0)$
- si $|z| \leq |u_0|$ renvoyer « G n'engendre pas de mot infini ».
- pour x de 0 à $|u_0| - 1$ faire
  - si $z[x] \neq u_0[x]$ renvoyer « G n'engendre pas de mot infini ».
- $M \leftarrow$ LETTRES-MORTELLES(A, f).
- $x \leftarrow |u_0|$.
- tant que $x < |z|$ et $z[x] \in M$ faire $x \leftarrow x + 1$.
- si $x = |z| + 1$ renvoyer « G n'engendre pas de mot infini ».
- Tant que $|z| \leq \ell$ faire

– $z \leftarrow f(z)$
– Pour k de 0 à $\ell - 1$ faire $t[k] = z[k]$.
– Renvoyer t.

2.11. Le mot $\mathbf{q}$ de la question 2.3. est point fixe non trivial de ζ ; en effet, les préfixes de $\mathbf{q}$ étant tous de la forme $(ab)^l$ ou $(ab)^l a$, on a

$$\{\zeta(w), w\text{préfixe de } \mathbf{y}\} = \{\zeta((ab)^l), \zeta((ab)^l a), l \geq 0\} = \{(ab)^{2l}, (ab)^{2l+1}, l \geq 0\}.$$

Ce dernier ensemble est infini, et tous ses éléments sont préfixes de $\mathbf{q}$; il engendre donc $\mathbf{q}$, et $\zeta(\mathbf{q}) = \mathbf{q}$.

Inversement, tout point fixe non trivial $\mathbf{y}$ pour ζ commence par a, sans quoi et b et $f(b) = ab$ doivent tous deux être préfixes de $\mathbf{y}$, impossible. Mais alors $f(a)$ est aussi préfixe de $\mathbf{y}$, et aussi $f^l(a)$ pour tout l, donc tout élément de $\{(ab)^{2^l}, l \geq 0\}$ est préfixe de $\mathbf{y}$. Or cet ensemble engendre $\mathbf{q}$, ce qui implique $\mathbf{y} = \mathbf{q}$ par 2.1.

2.12. Montrons que $\mathbf{q}$ est à nouveau point fixe non trivial de η ; on a

$$\{\eta(w), w\text{préfixe de } \mathbf{q}\} = \{\eta((ab)^l), \eta((ab)^l a), l \geq 0\} = \{(abab)^l, (abab)^l aba, l \geq 0\},$$

dont tous les éléments sont préfixes de $\mathbf{q}$. Le mot $b\mathbf{q}$ est lui aussi point fixe non trivial de η, car $\{\eta(w), w\text{préfixe de } b\mathbf{q}\} = \{\eta(b(ab)^l), \eta(b(ab)^l a), l \geq 0\} = \{b(abab)^l, b(abab)^l aba, l \geq 0\}$, qui sont tous préfixes de $b\mathbf{q}$. De la même façon, $b^l\mathbf{q}$ est point fixe non trivial de η pour tout l (on peut montrer qu'il n'y en a pas d'autre).

2.13. Le point fixe $\mathbf{y}$ étant non trivial, il existe une lettre x de $\mathbf{y}$ telle que $f(x) \neq x$. Soit u_0 le plus court préfixe de $\mathbf{y}$ contenant une telle lettre x, c'est-à-dire que $u_0 = sx$, avec $f(s) = s$.

On sait que $f(u_0)$ est un préfixe de $\mathbf{y}$, et, f étant non-effaçant, $|f(u_0)| \geq |u_0|$. Par suite, d'après 2.2, u_0 est préfixe de $f(u_0)$. Comme $f(u_0) \neq u_0$ par construction de u_0, on a $f(u_0) = u_0 v$, avec v non vide. Le morphisme f étant non-effaçant, toutes les lettres sont immortelles, et v contient donc au moins une lettre immortelle pour f.

D'après 2.4. et 2.8. le $D0L$ système (A, f, u_0) engendre bien un mot infini. Il est facile de montrer par récurrence que $f^k(u_0)$ est bien préfixe de $\mathbf{y}$ pour tout k, donc le mot infini en question est $\mathbf{y}$.

Si $f(x) \neq x$ pour tout $x \in A$, la construction précédente revient à prendre pour u_0 la première lettre de $\mathbf{y}$. Noter qu'une fois u_0 choisi, le point fixe $\mathbf{y}$ correspondant est caractérisé de façon unique : il est engendré par (A, f, u_0) ; on a donc une injection de l'ensemble des points fixes non triviaux dans A, d'où le résultat. Plus précisément, f a un point fixe non trivial pour chaque lettre x telle que $f(x)$ commence par x.

2.14. Le $D0L$-système de la question 2.3 engendre un mot infini ultimement périodique (et même périodique). Si $\mathbf{y}$ est un mot sur B ultimement périodique, avec les paramètres (i_0, p), on peut considérer le $HD0L$-système $(A_2, (a \mapsto ab, b \mapsto b), a, B, (a \mapsto y_0 \ldots y_{i_0-1}, b \mapsto y_{i_0} \ldots y_{i_0+p-1}))$. Le $D0L$ système sous-jacent a pour langage $\{ab^l, l \geq 0\}$, et le $HD0L$-système a donc pour langage $\{y_0 \ldots y_{i_0-1}(y_{i_0} \ldots y_{i_0+p-1})^l, l \geq 0\} = \{y_0 \ldots y_{i_0+pl-1}, l \geq 0\}$ puisque $\mathbf{y}$ est ultimement périodique. Le $HD0L$-système donné engendre donc bien $\mathbf{y}$.

2.15. Pour montrer que T engendre un mot infini $\mathbf{t}$, il suffit d'appliquer 2.4. et 2.8.

Notons σ l'application qui associe à un entier l la somme modulo 2 de ses chiffres binaires. Remarquons que si $x \in [2^k, 2^{k+1}[$, $\sigma(x) = 1 + \sigma(x - 2^k)$.

Pour calculer t_i, on utilise la remarque de la question 1.3, qui permet de montrer par récurrence sur k que pour $i \in [2^k, 2^{k+1}[, t_i = a$ si et seulement $\sigma(i) = 1$.

Cette propriété est vraie pour $k = 0$, car $t_1 = a$ et $\sigma(1) = 1$. Supposons la vraie jusqu'à un certain entier k ; alors $\theta^{k+1}(a) = \theta^k(a)\iota\theta^k(a)$; en vertu de cette formule, si $i \in [2^{k+1}, 2^{k+2}[$, on a $i = 2^{k+1} + l$, avec $l \in [1, 2^{k+1}$, et $t_i = a$ si et seulement si $t_l = b$, c'est-à-dire, par récurrence, $\sigma(l) = 0$. Mais $\sigma(i) = 1 + \sigma(l)$, donc $t_i = a$ si et seulement si $\sigma(i) = 1$, ce qui prouve le résultat par récurrence.

Supposons maintenant que pour deux entiers i_0 et p, on ait pour tout $n \geq i_0$, $t_{n+p} = t_n$. Si $\sigma(p) = 1$, on choisit $n = 2^k$ tel que $n > \max(i_0, p)$. On a alors $\sigma(n + p) = 1 + \sigma(p) = 0$, tandis que $\sigma(n) = 1$, d'où $t_n \neq t_{n+p}$.

Si $\sigma(p) = 0$, on définit l par $2^l \leq p < 2^{l+1}$, et on prend $n = 2^k + 2^l$ tel que $k > l + 1$, $n > \max(i_0, p)$. On a alors $\sigma(n) = 0$, tandis que $n+p = 2^k + 2^{l+1} + (p - 2^l)$. Le choix de k et de l montre que $\sigma(n+p) = \sigma(2^k) + \sigma(2^{l+1}) + \sigma(p - 2^l) = 1 + 1 + (\sigma(p) - 1) = \sigma(p) + 1 = 1$.

On constate encore que $\sigma(n) \neq \sigma(n + p)$. Contradiction, et $\mathbf{t}$ ne peut être ultimement périodique.

2.16. Commençons par observer que $\theta\psi = \psi\mu$, identité qu'il suffit de vérifier sur les lettres (cf. 1.1). Soit $\mathbf{y}$ le mot infini engendré par $T'' = (A_3, \mu, a)$. On a alors $\theta\psi(\mathbf{y}) = \psi\mu(\mathbf{y}) = \psi(\mathbf{y})$, et comme $\psi(\mathbf{y})$ commence par a, en vertu de 2.13, on a $\mathbf{y} = \mathbf{t}$.

2.17. La preuve de 2.8. montre alors que $\forall k < l$, $f^{nk}(u_0)$ est un préfixe strict de $f^{nl}(u_0)$. Il s'ensuit que $L(G_{mn})$ est infini, et, u_0 étant préfixe de $f^{mn}(u_0)$, engendre un mot infini. Comme $L(G_{mn}) \subset L(G_n)$, on a $W(G_n) = W(G_{mn})$ (la preuve de 2.1. montre qu'un sous-ensemble infini quelconque de L engendre le même mot infini que L), et de même $W(G_m) = W(G_{mn})$.

Troisième partie

3.1. Remarquons d'abord, comme le suggère l'énoncé, qu'en effaçant les c dans $W(J_1)$ on retrouve $\mathbf{t}$. Pour prouver cela, notons $\delta_c = (a \mapsto a, b \mapsto b, c \mapsto \varepsilon)$ et $\nu = (a \mapsto abccc, b \mapsto baccc, c \mapsto \varepsilon)$. On vérifie que $\theta\delta_c = \delta_c\nu = (a \mapsto ab, b \mapsto ba, c \mapsto \varepsilon$. Comme $\nu(W(J_1)) = W(J_1)$, on a $\theta(\delta_c(W(J_1))) = \delta_c(W(J_1))$; de plus $\delta_c(W(J_1))$ commence par a, et $\mathbf{t}$ est le seul point fixe de θ commençant par a, soit $\mathbf{t} = \delta_c(W(J_1))$.

Remarquons quelques faits sur $W(J_1)$. Soit $\tilde{\iota} = (a \mapsto b, b \mapsto a, c \mapsto c)$. Alors $\nu\tilde{\iota} = i\tilde{ota}\nu$, donc comme en 1.3, pour $n \geq 2$, $\nu^n(a) = \nu^{n-1}(a)\nu^{n-1}(b)\nu^{n-1}(ccc) = \nu^{n-1}(a)\tilde{\iota}(\nu^{n-1}(a))$. On montre ainsi facilement par récurrence que

- que $\nu^n(a)$ se termine toujours par ccc,
- $\nu^n(a)$ ne contient pas plus de trois c consécutifs (remarquer que $\tilde{\iota}(\nu^{n-1}(a))$ commence par b) ;
- que tout facteur de longueur 3 de $\nu^n(a)$ contient un c.
- que ccc est toujours précédé dans $\nu^n(a)$ de ab ou de ba.

Supposons maintenant que $W(J_1)$ est engendré par un $PD0L$-système $J_2 = (A_3, f, u_0)$. Le mot $W(J_2) = W(J_1)$ contient des facteurs ccc; par suite $\mathbf{t} = \delta_c(W(J_1))$ contient $\delta_c(f(c))^3$; en vertu de la proposition 1, on voit que $\delta_c(f(c)) = \varepsilon$, soit $f(c) = c^l$ pour un certain l. Si $l \geq 2$, $f(W(J_2)) = W(J_2)$ contient $f(c)^3$, donc contient c^6. Or pour tout mot w, $\nu(w)$ ne peut contenir plus de trois c consécutifs.

Si maintenant $l = 1$, $f(abccc) = f(a)f(b)ccc$ est préfixe de $W(J_1)$; si $f(a) = a$, $|f(b)| \geq 2$, et donc $f(b)$ se termine par ab ou ba, qui sont les seuls facteurs de longueur 2 à pouvoir être suivis de ccc. Sinon, $f(a)$ commence par ab et $f(b)$ se termine par a ou b, car il est suivi de ccc. Dans les deux cas, le mot $W(J_1)$ contient $f(ba) = f(b)f(a)$ qui contient lui-même aba, baa, aab, bab, impossible car tout facteur de longueur 3 de $W(J_1)$ contient c.

3.2. La relation $W(J_2) = \varphi(\mathbf{t})$ vient de la définition de J_2. Le calcul des premières lettres de $\varphi(\mathbf{t})$ donne $aabbbbaabbaaaabb$, qui contient a^4 et b^4. Supposons que $\varphi(\mathbf{t})$ soit engendré par un D0L-système (A_2, f, u_0).

Si $|f(a)| = |f(b)| = 1$, $|u_0| = |f(u_0)|$ et on ne peut engendrer de mot infini.

Comme $\varphi(\mathbf{t})$ contient a^4 et b^4, il contient v^4, avec $|v| = |f(a)|$ou $|f(b)| \geq 2$.

Si $v \in \{a^n, b^n, n \in \mathbb{N}\}$, alors a^8 ou b^8 est facteur de $\varphi(\mathbf{t})$, donc a^4 ou b^4 apparaît dans $\mathbf{t}$, impossible (proposition 1).

On dira dans la suite qu'un facteur v de $\varphi(\mathbf{t})$ apparaît en position paire s'il existe j pair tel que $v_j = \varphi(\mathbf{t})_j$ pour $j = 1, \ldots, |v|$. En particulier, remarquons que les motifs ab ou ba ne peuvent apparaître qu'à des positions paires, vu la forme de φ. En outre, un facteur v de $\varphi(\mathbf{t})$ qui commence et termine à une position impaire est de la forme $\varphi(w)$ pour un unique w facteur de $\mathbf{t}$, défini par $w_i = v_{2i-1}$.

Si v contient ab ou ba, v ne peut apparaître simultanément à une position paire ou impaire dans $\varphi(\mathbf{t})$ (ab et ba n'apparaissent qu'à des positions paires), donc comme v^2 apparaît dans $\varphi(\mathbf{t})$, $|v|$ est pair.

- si v^4 apparaît à une position impaire, on a $v = \varphi(w)$, et donc $v^4 = \varphi(w^4)$ et $\mathbf{t}$ contient w^4, impossible.
- si v apparaît à une position paire, on a $v = x\varphi(w)y$, et $v^4 = x(\varphi(w)yx)^3\varphi(w)y$; le y de yx apparaît en position impaire, donc $x = y$, et $v^4 = x(\varphi(wx)^3)x$, et $(wx)^3$ apparaît dans $\mathbf{t}$, impossible.

3.3. Supposons que $\mathbf{y} = W(A, f, u_0)$, avec f effaçant. Soit alors $x \in A$ tel que $f(x) = \varepsilon$ Considérons alors $B = A - \{x \in A, f(x) = \varepsilon\}$, $\delta_x : A^* \to B^*$, défini par $x \mapsto \varepsilon$, $y \neq x \mapsto y$. Soit $\tilde{f}$ la restriction de $\delta_x f$ à B^*, et $\tilde{u}_0 = \delta_x(u_0)$.

On a alors $\delta_x f = \tilde{f}\delta_x$, donc $\delta_x f^n = \tilde{f}^n \delta_x$, soit encore $\delta_x f^n(u_0) = \tilde{f}^n(\tilde{u}_0)$.

Si maintenant $\tilde{g}$ est la restriction de f à B^*, on a $\tilde{g}\delta_x = f$. Donc $\tilde{g}(\tilde{f}^n(\tilde{u}_0)) = f^{n+1}(u_0)$. Par suite, $L(A, f, u_0) = \{u_0\} \cup L(B, \tilde{f}, \tilde{u}_0, A, \tilde{g})$. La preuve n'est pas tout à fait finie : si par exemple on avait $f(y) = x$ avec $f(x) = \varepsilon$, on a $y \in B$ et $\tilde{f}(y) = \varepsilon$, donc $\tilde{f}$ peut être effaçant.

On conclut par récurrence sur le cardinal de A. Si A est de cardinal 1, f est non effaçant et le résultat est trivial. Si l'on suppose l'assertion vraie pour tout alphabet de cardinal $\leq k$, et si A est de cardinal $k+1$, on peut appliquer l'hypothèse de récurrence à $(B, \tilde{f}, \tilde{u}_0)$ et obtenir $(C, \overline{f}, \overline{u}_0, B, \overline{g})$ tel que $W(B, \tilde{f}, \tilde{u}_0) = W(C, \overline{f}, \overline{u}_0, B, \overline{g})$. Par suite, $W(A, f, u_0) = W(C, \overline{f}, \overline{u}_0, A, \tilde{g}\overline{g})$, et l'hypothèse de récurrence est prouvée. Par suite, $\mathcal{W}_A(D0L) \subset \mathcal{W}_A(NPD0L)$.

Si $\mathbf{y} = W(B, f, u_0, A, g)$ avec g non effaçant, on sait que $\mathbf{y} = g(W(B, f, u_0))$; mais on peut trouver $(C, \tilde{f}, \tilde{u_0}, B, \tilde{g})$ un NPD0L-système tel que $W(B, f, u_0) = W(C, \tilde{f}, \tilde{u_0}, B, \tilde{g})$. Mais alors $\mathbf{y} = W(C, \tilde{f}, \tilde{u_0}, A, g\tilde{g}) \in \mathcal{W}_A(NPD0L)$, car $g\tilde{g}$ non effaçant.

Le même argument conduit à $\mathcal{W}_A(HD0L) \subset \mathcal{W}_A(HPD0L)$, et les inclusions inverses sont déjà connues.

3.4. L'application α de $P(B)$ dans $P(B)$ qui associe à une partie E l'ensemble

$$\alpha(E) = \cup_{x\in E} \operatorname{Alph}(f(x))$$

est une fonction de $P(B)$ dans lui-même, ainsi que toutes ses itérées ; l'ensemble des fonctions de $P(B)$ dans lui-même étant fini, il existe $n < m$ tels que $\alpha^n = \alpha^m$ pour toute lettre x. Posant $p = m - n$, on a $\alpha^{j+p} = \alpha^j$, pour tout $j \geq n$. Soit N l'entier de l'intervalle $[j, j+p[$ divisible par p. Alors $N \geq n$ et $p|(2N - N)$, donc $\alpha^{2N} = \alpha^N$. En particulier, pour toute lettre x, $\operatorname{Alph}(f^N(x)) = \alpha^N(\{x\}) = \alpha^{2N}(\{x\}) = \operatorname{Alph}(f^{2N}(x))$.

Posons alors $\tilde{f} = f^N$, $\tilde{g} = gf^N$. D'après 2.8, si (B, f, u_0) engendre un mot infini, (B, f^N, u_0) engendre également un mot infini, et d'après 2.17 il s'agit du même. Par suite, $W(B, f, u_0, A, g) = W(B, f^N, u_0, A, g)$, qui est engendré par le langage $\{gf^{Nk}(u_0), k \geq 0\}$, donc aussi par $\{gf^{Nk}(u_0), k \geq 1\} = L(B, f^N, u_0, A, gf^N)$. Par suite $W(B, f, u_0, A, g) = W(B, \tilde{f}, u_0, A, \tilde{g})$.

En outre,

$$\begin{aligned} \tilde{g}(\tilde{f}(x)) = \varepsilon \quad &\Leftrightarrow \quad \operatorname{Alph}(f^{2N}(x)) \subset \{y, g(y) = \varepsilon\} \\ &\Leftrightarrow \quad \operatorname{Alph}(f^{N}(x)) \subset \{y, g(y) = \varepsilon\} \\ &\Leftrightarrow \quad \tilde{g}(x) = \varepsilon. \end{aligned}$$

On pose alors $\overline{B} = \{x \in B, \tilde{g}(x) \neq \varepsilon\}$, et $\delta : B \to \overline{B}$ qui envoie x sur x si $\tilde{g}(x) \neq \varepsilon$, sur ε sinon. Enfin, soit $\overline{f} = \delta\tilde{f}$ restreint à $\overline{B}^*$, $\overline{u}_0 = \delta(u_0)$, $\overline{g}$ la restriction de $\tilde{g}$ à $\overline{B}^*$; on a alors $\tilde{g} = \overline{g}\delta$.

Montrons que $\delta\tilde{f} = \overline{f}\delta$:

– Si $x \notin \overline{B}, \tilde{g}(x) = \varepsilon$, donc $\tilde{g}(\tilde{f}(x)) = \varepsilon$; par suite $\delta(\tilde{f}(x)) = \varepsilon = \delta(x)$;

– Si $x \in \overline{B}$, $\overline{f}(\delta(x)) = \overline{f}(x) = \delta(\tilde{f}(x))$, par définition de $\overline{f}$.

Par suite, $\delta\tilde{f}^n = \overline{f}^n\delta$, et $\overline{g}(\delta\tilde{f}^n) = (\overline{g}\delta)\tilde{f}^n = \tilde{g}\tilde{f}^n$ est égal à $\overline{g}\overline{f}^n\delta$.

Notons alors que le mot $W(B, \tilde{f}, u_0, A, \tilde{g})$ est engendré par le langage $\{\tilde{g}(\tilde{f}^n(u_0)), n \in \mathbb{N}\} = \{\overline{g}(\overline{f}^n(\overline{u}_0))\}$, donc $W(B, f, u_0, A, g) = W(B, \tilde{f}, u_0, A, \tilde{g}) = W(\overline{B}, \overline{f}, \overline{u}_0, A, \overline{g})$.

Notons enfin que $\overline{f}$ est non effaçant ; en effet, si $x \in \overline{B}$, on a $\overline{g}(\overline{f}(x)) = \tilde{g}(\tilde{f}(x)) \neq \varepsilon$, car $\tilde{g}(x) \neq \varepsilon$ par définition de $\overline{B}$.

En outre, $\overline{g}$ est de même non effaçant, car pour $x \in \overline{B}$, $\overline{g} = \tilde{g}(x) \neq \varepsilon$.

Par suite, $(\overline{B}, \overline{f}, \overline{u}_0, A, \overline{g})$ est bien un $NPD0L$-système, et engendre le même mot que (B, f, u_0, A, g), donc $\mathcal{W}_A(HPD0L) \subset \mathcal{W}_A(NPD0L)$.

3.5. Soit $H = (B, f, u_0, A, g)$ un NPD0L-système.

Supposons tout d'abord qu'il existe y dans B tel que $f(y) \neq y$ et $L(B, f, y)$ fini. Remarquons que cela implique que y n'apparaît pas dans $f(y)$, sans quoi comme f est non-effaçante, la suite $|f^n(y)|$ est strictement croissante.

On pose alors $B' = B - \{y\}$, et $\delta_y : B \to B'$, avec $\delta_y(y) = f(y)$, $\delta_y(x) = x$ pour $x \neq y$. Soit alors $\tilde{f}$ la restriction de δf à B'^*, $\tilde{g}$ la restriction de gf à B', et $\tilde{u}_0 = \delta(u_0)$. On a alors $W(H) = W(B', \tilde{f}, \tilde{u}_0, A, \tilde{g})$.

En itérant ce procédé, on peut supposer que pour tout $y \in B$, soit $f(y) = y$, soit $L(B, f, y)$ infini.

Pour tout y dans la deuxième catégorie, il existe n_y tel que $|f^{n_y}(y)| \geq |g(y)|$. Soit N un entier plus grand que tous les n_y. Quitte à remplacer f par f^N, ce qui ne change pas le mot engendré, on peut donc supposer que $|f(y)| \geq |g(y)|$ ou $f(y) = y$ pour tout $y \in B$.

On pose maintenant $\tilde{B} = \{(x,i), x \in B, 1 \le i \le |g(x)|\}$, $\beta : B^* \to \tilde{B}^*$ qui envoie x sur $(x,1)\dots(x,|g(x)|)$, et $\tilde{g} : \tilde{B}^* \to A^*$, qui envoie (x,i) sur la i-ème lettre de $g(x)$. Alors $\tilde{g}$ est lettre-à-lettre, et $g = \tilde{g}\beta$.

Définissons $\tilde{f}((x,i))$ = la i-ème lettre de $\beta(f(x))$ pour $i < |g(x)|$, $\tilde{f}((x,|g(x)|)$ étant le suffixe de $\beta(f(x))$ commençant en position $|g(x)|$. Le fait que $\tilde{f}$ est non effaçant découle de $|\beta f(x)| \ge |f(x)| \ge |g(x)|$.

Il est facile enfin de voir, par construction, que $\tilde{f}\beta = \beta f$.

Posant $\tilde{u}_0 = \beta(u_0)$, on voit alors comme dans les questions précédentes que $W(H) = W(\tilde{B}, \tilde{f}, \tilde{u}_0, A, \tilde{g})$; $W(H)$ peut donc être engendré par un CPD0L-système.

3.6. Si Card(A) vaut 1, il n'existe qu'un seul mot infini sur A, à savoir le mot $aaaaa$.... Par suite, $\mathcal{W}_A(PD0L) = \mathcal{W}_A(HD0L)$, donc tous les ensembles sont égaux.

En vertu des questions 3.3, 3.4 et 3.5, on a

$$\mathcal{W}_A(CPD0L) = \mathcal{W}_A(NPD0L) = \mathcal{W}_A(ND0L) = \mathcal{W}_A(HD0L) = \mathcal{W}_A(HPD0L).$$

Par suite, nécessairement, $\mathcal{W}_A(CPD0L) = \mathcal{W}_A(CD0L) = \mathcal{W}_A(ND0L)$.

Par 3.2, on sait que $\mathcal{W}_A(NPD0L) \not\subset \mathcal{W}_A(D0L)$ dès que l'alphabet a au moins deux lettres. Cela implique automatiquement $\mathcal{W}_A(PD0L) \ne \mathcal{W}_A(CPD0L)$ dans ce cas. et $\mathcal{W}_A(D0L) \ne \mathcal{W}_A(CD0L)$.

Enfin, on a $\mathcal{W}_A(D0L) = \mathcal{W}_A(PD0L)$ ssi Card$(A) \le 2$.

En résumé, si Card$(A) = 2$:

$$\begin{array}{ccccccc} \mathcal{W}_A(D0L) & \subset & \mathcal{W}_A(CD0L) & = & \mathcal{W}_A(ND0L) & = & \mathcal{W}_A(HD0L) \\ \| & & \| & & \| & & \| \\ \mathcal{W}_A(PD0L) & \subset & \mathcal{W}_A(CPD0L) & = & \mathcal{W}_A(NPD0L) & = & \mathcal{W}_A(HPD0L) \end{array} \tag{1}$$

Si Card$(A) = 3$:

$$\begin{array}{ccccccc} \mathcal{W}_A(D0L) & \subset & \mathcal{W}_A(CD0L) & = & \mathcal{W}_A(ND0L) & = & \mathcal{W}_A(HD0L) \\ \cup & & \| & & \| & & \| \\ \mathcal{W}_A(PD0L) & \subset & \mathcal{W}_A(CPD0L) & = & \mathcal{W}_A(NPD0L) & = & \mathcal{W}_A(HPD0L) \end{array} \tag{2}$$

Dans ces deux diagrammes, les inclusions notées $\subset$ sont strictes.

Quatrième partie

4.1. Une énumération montre que l'ensemble des mots de longueur ≤ 4 sans carré est $\{\varepsilon, a, b, ab, ba, aba, bab\}$. Par suite tout mot de longueur 4, et donc a fortiori de longueur ≥ 4, contient un carré, et $E^2(A_2) = \{\varepsilon, a, b, ab, ba, aba, bab\}$.

4.2. On énumère les positions de début j possibles pour le carré et la longueur l possible pour le carré ; il reste alors à tester si les deux facteurs de longueur l commençant en j et $j + l$ sont égaux.

CARRE(w)
- $n \leftarrow |w|$.
- pour j de 0 à $n - 2$
  - pour l de 1 à $\lfloor (n - i)/2 \rfloor$ faire
    - test $\leftarrow$ vrai.
      - pour j de 0 à $l - 1$ faire

  - si $w[i+j] \neq w[i+l+j]$ alors test $\leftarrow$ faux.
  - si test = vrai renvoyer « w contient un carré ».
- Renvoyer « w est sans carré ».

La complexité de cet algorithme est manifestement $O(n^3)$.

4.3. Si w est un mot sans carré, son préfixe de longueur $|w|-1$ n'en a pas non plus, et il n'a pas de suffixe de la forme vv. Inversement, si w contient un carré, soit ce carré est un suffixe de w, auquel cas il existe v tel que vv suffixe de w, soit le carré ne contient pas la dernière lettre de w, auquel cas c'est un carré du préfixe de longueur $|w|-1$.

Ceci une fois remarqué, on procède de la façon suivante : pour obtenir les mots de longueur $\leq \ell$, on construit itérativement la liste des mots L'_i sans carré de longueur $< i$, et la liste L_i des mots sans carré de longueur i, sachant que $L_0 = \{\varepsilon\}$, et que L_{i+1} s'obtient en testant pour chaque mot w de L_i et pour chaque lettre x de A si wx n'a pas de suffixe carré.

On obtient l'algorithme :

LISTE_SANS_CARRE(A, ℓ)
- $L' \leftarrow \emptyset$, $L \leftarrow \{\varepsilon\}$.
- pour j de 0 à $\ell - 1$
- $S \leftarrow \emptyset$.
- pour $l \in L$ faire
  - pour $a \in A$ faire
    - $w \leftarrow la$.
    - carre $\leftarrow$ faux.
    - pour j de 1 à $\lfloor |w|/2 \rfloor$ faire
    - test $\leftarrow$ vrai.
    - pour i de 0 à j faire
    - si $w_{|w|-i} \neq w_{|w|-i-j}$ alors test $\leftarrow$ faux.
    - si test $\leftarrow$ vrai faire carre $\leftarrow$ vrai.
    - si carre = faux faire $S \leftarrow S \cup \{w\}$.
- $L' \leftarrow L' \cup L$, $L \leftarrow S$.
- Renvoyer $L' \cup L$.

La boucle centrale sur a et j est effectuée au plus une fois pour chaque mot retourné (une fois exactement pour les mots de longueur $< \ell$, aucune fois pour les mots de longueur ℓ). Son coût est manifestement de $O(k\ell^2)$, d'où la complexité annoncée.

4.4. Supposons que $x \neq y$; en ce cas
- soit l'un des deux est préfixe de l'autre, par exemple $x = yv$ et $\mu(x) = \mu(y)\mu(v)$ et donc $\mu(x) \neq \mu(y)$;
- dans le cas contraire, il existe j tel que $x_j \neq y_j$, et soit n le plus petit tel indice. Alors $\mu(x_1 \dots x_n)$ est un préfixe de $\mu(x)$ et $\mu(y_1 \dots y_n)$ un préfixe de $\mu(y)$. Si $\mu(x) = \mu(y)$, $\mu(x_n)$ est un préfixe de $\mu(y_n)$ ou l'inverse. C'est impossible dans les deux cas.

Par suite, μ est bien injective.

4.5. On remarque que si un facteur interdit est dans $\mu(w)$, alors il apparaît dans $\mu(v)$, avec v facteur de w de longueur au plus 3 (les motifs interdits recouvrent au plus l'image de 3 lettres). Il suffit donc de prouver le résultat pour les w de longueur au plus 3, et c'est alors un calcul simple.

4.6. L'existence est simple ; si v commence au début de l'image d'une lettre de w, on prend $x = \varepsilon$; dans le cas contraire, v commence par un suffixe strict de $\mu(a)$, ou de $\mu(b)$, soit c ou bc, que l'on note x, suivi de l'image d'un facteur de w, noté y, suivi éventuellement d'un préfixe strict de $\mu(a)$ ou $\mu(b)$, soit $\{ab, a\}$ que l'on note z.

Pour l'unicité, supposons que $x\mu(y)z = x'\mu(y')z'$; alors

- si $x \neq x'$, on a par exemple x préfixe de x', donc $x = \varepsilon$ et $x' \in \{c, bc\}$. Mais alors x' est préfixe d'un $\mu(y)$, ou de z si y est vide, impossible dans les deux cas.
- si $z \neq z'$, le même type de raisonnement s'applique.

Donc $\mu(y) = \mu(y')$, et on conclut par 4.4.

4.7. Supposons que $\mu(w)$ contient vv. Si $v = b$, on applique 4.6 à $vv = bb = \varepsilon\mu(cc)\varepsilon$, donc w contient cc.

Sinon, on écrit v sous la forme $x\mu(y)z$, et on a alors $\mu(w)$ contient $x\mu(y)zx\mu(y)z$. On a $zx \in \{\varepsilon, a, ac, ab, ac, bc, abc, abbc\}$.

- si $zx \in \{\varepsilon, ac, abc\}$, on a $zx = \mu(t)$ pour un certain t, $v = x\mu(yty)z$. Par unicité de 4.6, w contient yty ;
  - soit $t = \varepsilon$ et w contient un carré ;
  - soit $t = a$ et
    - $x = c$, $z = ab$, d'où $vv = c\mu(yay)ab$, qui est nécessairement suivi de c, donc $vvc = c\mu(yaya)$ est facteur de w, et par 4.6, $yaya$ (carré) est facteur de w.
    - $x = bc$, et $z = a$, et alors de la même façon $avv = \mu(ayay)a$ est facteur de w.
  - soit $t = b$, et alors $x = c$, $z = a$.
    - si vv est précédé de a, $byby$ est facteur de w ;
    - si vv est suivi de a, $ybyb$ est facteur de w ;
    - sinon vv est précédé de ab et suivi de bc, et $aybya$ est facteur de w.
- si $zx = a$, alors $vv = \mu(y)a\mu(y)a$ ou $a\mu(y)a\mu(y)$. Dans les deux cas, $\mu(y)$ doit commencer par bc ou c, ce qui est impossible. On conclut de la même façon pour les cas restants.

Cela conclut la preuve.

4.8. Si c'était le cas, ay ne peut commencer par aa ni aba, ni contenir bb, donc y doit commencer par c ou bc. De plus by ne doit par contenir bb, donc y doit commencer par c. Maintenant, ybc ne peut contenir ni bb, ni cbc, donc y finit par a, mais alors ya contient aa, contradiction.

4.9. En vertu de 4.5, $\mu(V) \subset V$. En vertu de 4.7 et 4.8, $\mu(V \cap E^2(A_3)) \subset E^2(A_3)$, donc $\mu(V \cap E^2(A_3)) \subset V \cap E^2(A_3)$. Le mot a est dans $V \cap E^2(A_3)$, donc $L(A_3, \mu, a) \subset V \cap E^2(A_3)$, et ce langage est infini ; en effet, $\mu(a) = abc$ avec b et c immortelles, cf. question 2.8.

4.10. Montrons que les mots de $L(A_3, \mu, a)$ sont indéfiniment prolongeables. En effet, $\mu^2(a) = abcacb$, et donc $\mu^{n+2}(a) = \mu^n(abc)\mu^n(a)\mu^n(cb)$. Par suite, pour tout k et pour tout $n \geq k$, $u\mu^k(a)$ est sans carré , avec $u = \mu^n(abc)$ et v la concaténation de w et de $\mu^n(cb)$, où w est défini par $\mu^n(a) = \mu^k(a)w$. En prenant n assez grand, on peut avoir $|u|$ et $|v|$ arbitrairement grands.

Supposons donné un mot w tel que

- $wcw \in V \cap E^2(A_3)$;
- w admet un préfixe de la forme $ybya$, où y commence par a, et un suffixe de la forme $axbx$, où x se termine par a.

– $a^{-1}wcwc \in V \cap E^2(A_3)$, où la notation a^{-1} signifie que l'on enlève la première lettre a de $wcwc$.

Notons qu'une conséquence facile des deux premières propriétés est que wcw est non prolongeable.

On a alors $\mu(wcw) = \mu(w)b\mu(w) = w'bw'$, avec les propriétés suivantes :

– $w'bw' \in V \cap E^2(A_3)$ (4.9) ;
– w' admet un préfixe de la forme $y'cy'b$, où y' commence par a ($y' = \mu(y)a$), et un suffixe de la forme $bx'ax'$, où x' termine par c ($x' = c\mu(x)$) ;
– $a^{-1}w'bw'b \in V \cap E^2(A_3)$:
  – comme $a^{-1}w'bw'$ est facteur de l'image par μ d'un mot de V, il est dans V. Les motifs interdits ne peuvent donc apparaître dans $a^{-1}w'bw'b$ qu'en suffixe, et w' se terminant par c, bb n'est pas suffixe de $a^{-1}w'bw'b$, qui est donc bien dans V.
  – si maintenant zz est un carré de $a^{-1}w'bw'b$, alors, $w'bw'$ étant sans carré, zz est un suffixe de $w'bw'b$. Comme zz est un facteur de $a^{-1}w'bw'b$, z est un suffixe strict de $w'b$. Enfin, si $|z| = |w'b| - 1$, $zz = b^{-1}a^{-1}w'bw'b$ commence par c, tandis que $z = a^{-1}w'b$ commence par b. Par suite, la longueur de z est au plus $|w'b|-2$. Comme $\mu(a^{-1}wcwc)$ est un préfixe de $a^{-1}w'bw'b$ de longueur $|w'bw'b|-3$, on voit que zz est suffixe de $\mu(a^{-1}wcwc)$. Comme $a^{-1}wcwc$ est dans V et sans carré, c'est impossible par 4.9.

On voit, là encore, que $w'bw'$ est non prolongeable. On a $\mu(w'bw') = \mu(w')ac\mu(w')$; on pose $w'' = \mu(w')a$.

On a alors

– $w''cw'' \in V \cap E^2(A_3)$; en effet, w' se termine par c, donc par bc ou ac, donc $\mu(w')$, qui est dans V se termine par acb ou bcb, et les motifs interdits n'apparaissent pas dans $\mu(w')a$. En outre, si $w''cw''$ contient un carré zz, celui-ci est un suffixe de w'', car $w''cw''a^{-1}$ est sans carré. Comme $|zz| = 2|z| \leq 2|w''| + 1$, on a $|z| \leq |w''|$. En cas d'égalité, alors $zz = a^{-1}w''cw''$, d'où $z = a^{-1}w''c$, impossible car z, suffixe de w'', se termine par a. Par suite, $|z| < |w''|$, et donc zz est un suffixe de longueur au plus $2|w''| - 2$ de $w''cw'' = \mu(w'bw')a$, donc un suffixe de $\mu(a^{-1}w'bw')a$. Par suite, $\mu(a^{-1}w'bw')ac = \mu(a^{-1}w'bw'b)$ contient un carré, impossible car $a^{-1}w'bw'b$ est dans $V \cap E^2(A_3)$.
– w'' admet un préfixe de la forme $y''by''a$ avec y'' commençant par a ($y'' = \mu(y')$), et un suffixe de la forme $ax''bx''$, où x'' se termine par a ($x'' = c\mu(x)a$).
– $a^{-1}w''cw''c \in V \cap E_2(A_3)$.
  – Notons que $w'bw'b$ est dans V ; en effet, $w'bw'$ est dans V et $a^{-1}w'bw'b$ est dans V. Tout facteur de $w'bw'b$ qui n'est pas un préfixe est facteur de $a^{-1}w'bw'b$, et tout facteur de $w'bw'b$ qui n'est pas un suffixe est facteur de $w'bw'$. Il ne peut donc y avoir de motif interdit dans $w'bw'b$, ni donc dans $w''cw''c$, ce qui montre que $a^{-1}w''cw''c \in V$.
  – Si zz est un carré de $a^{-1}w''cw''c$, par le même raisonnement que pour $a^{-1}w'bw'b$, on voit que z est suffixe strict de $w''c$ de longueur $\leq |w''c| - 2$. Comme $\mu(a^{-1}w'bw'b)$ est un suffixe de $a^{-1}w''cw''c$ de longueur $2|w'| + 1 = 2|w''| - 1 = 2|w''c| - 3$, il s'ensuit que zz est un facteur de $\mu(a^{-1}w'bw'b)$; ceci est impossible en vertu du fait que $a^{-1}w'bw'b$ est dans $V \cap E^2(A_3)$ (4.9).

Partant du mot sans carré non prolongeable wcw, on a donc construit un mot $w''cw''$ vérifiant les mêmes propriétés, avec $w'' = \mu^2(w)a$, soit $|\mu(w'')| = 1 + |\mu(w)| > |w|$, et donc $|w''cw''| > |wcw|$.

En itérant ce procédé, on peut construire une infinité de mots sans carrés non prolongeables. Reste à produire un w qui convient.

On pourrait penser à partir de $w = bab$, car $babcbab$ est bien sans carré non prolongeable, mais w ne vérifie pas les hypothèses. En revanche, $w'' = \mu(\mu(w))a = abcbabcacbabcbac$ vérifie toutes les hypothèses.

On a donc bien construit une suite infinie de mots sans carrés non prolongeables.

4.11. Supposons qu'on a une occurrence du type vvv dans $\mathbf{t}$. Si v commence par b, on sait que $\iota(vvv)$ est aussi un cube, qui apparaît aussi dans $\mathbf{t}$. Il s'ensuit que l'on peut supposer que $\mathbf{t}$ commence par a.

On sait que $\mathbf{t} = \psi(\mathbf{y})$ (question 2.16). Comme v commence par a, et que a n'apparaît qu'en tête des images par ψ de $\{a, b, c\}$, on voit que chaque occurrence de v est préfixe de l'image d'un facteur de $\mathbf{y}$. Dans une occurrence vv, il s'ensuit donc que le premier v est image d'un facteur de $\mathbf{y}$. Appliqué aux deux premiers v du facteur vvv, cela montre que $\mathbf{y}$ admet un facteur w_1w_2 avec $\psi(w_1) = \psi(w_2) = v$. On peut prouver que ψ est injective comme en 4.4, donc $w_1 = w_2$, et $\mathbf{y}$ contient un carré, ce qui contredit 4.9. D'où le résultat.