THÉORÈME DE COBHAM

BRUNO LE FLOCH

Le but de ce document est de présenter une démonstration du théorème de Cobham ne nécessitant que des connaissances de base sur les automates finis. On introduira pour ce faire quelques notions (entiers multiplicativement indépendants, sous-mots récursifs de mots infinis, ensembles s-automatiques, et ensemble syndétiques) dans les quatre premières sections, avant de donner la preuve proprement dite du théorème dans la cinquième section.

Théorème 1. *(Cobham, 1969) Soient $s, t \geq 2$ deux entiers multiplicativement indépendants. Si une partie X de $\mathbb{N}$ est s- et t-automatique, alors elle est ultimement périodique.*

1. E

Définition 2. *Deux entiers $s, t \geq 2$ sont dits multiplicativement indépendants lorsque $\frac{\log t}{\log s} \notin \mathbb{Q}$.*

La définition est clairement symétrique. On commence par rappeler une propriété classique.

Proposition 3. *Soient $s, t \geq 2$ multiplicativement indépendants. L'ensemble*

$$\left\{ \frac{t^\beta}{s^\alpha} \middle| \alpha, \beta \in \mathbb{N} \right\}$$

est dense dans $\mathbb{R}_+^*$.

Preuve. Les réels $\log s$ et $\log t$ sont positifs et de rapport irrationnel, donc

$$\left\{ \alpha \log t - \beta \log s \middle| \alpha, \beta \in \mathbb{N} \right\}$$

est dense dans $\mathbb{R}$. On conclut en invoquant la continuité de l'exponentielle. □

On montre ensuite un lemme qui nous sera utile dans la section (4).

Lemme 4. *Soient $m, n, \alpha, \beta, \gamma, \delta \in \mathbb{N}^*$ tels que $n < m$, et soient $s, t \geq 2$ des entiers mulitiplicativement indépendants. Alors il existe des entiers $i, j \geq 1$ tels que*

$$nt^{\gamma+\delta j} \leq ms^{\alpha+\beta i} < (m+1)s^{\alpha+\beta i} \leq (n+1)t^{\gamma+\delta j}.$$

Preuve. La propriété recherchée se réécrit

$$\frac{nt^\gamma}{ms^\alpha} \leq \frac{\left(s^\beta\right)^i}{\left(t^\delta\right)^j} \leq \frac{(n+1)t^\gamma}{(m+1)s^\alpha}.$$

L'existence de i et j est alors une conséquence de la proposition précédente (car s^β et t^δ sont encore multiplicativement indépendants). □

2. S - ´ ’

Définition 5. *Un mot infini* $\mathbf{w}$ *sur un alphabet fini* Σ *est une suite infinie* $(w_n)_{n\in\mathbb{N}}$ *d'éléments de* Σ. *On note* $\mathbf{w} = w_0w_1w_2\cdots$. *Le mot infini* $\mathbf{w}$ *est dit ultimement périodique lorsqu'il existe deux entiers* $T > 0$ *et* $N \geq 0$ *tels que pour tout* $n \geq N$ *on ait* $w_{n+T} = w_n$.

Définition 6. *Soit* $\mathbf{w}$ *un mot infini.*

On dit qu'un mot fini v *est un sous-mot de longueur* l *de* $\mathbf{w}$ *lorsqu'il existe un entier* $n \geq 0$ *tel que* $v = w_nw_{n+1}\cdots w_{n+l-1}$. *On dit que ce sous-mot est récurrent lorsqu'il existe une infinité de tels* n.

Pour chaque entier $l \geq 0$, *on pose* $r_l(\mathbf{w})$ *le nombre de sous-mots récurrents de longueur* l *de* $\mathbf{w}$. *En particulier,* $r_0(\mathbf{w}) = 1$, *car le mot vide est l'unique mot récurrent de longueur nulle.*

Proposition 7. *Soit* $\mathbf{w} = w_0w_1w_2\cdots$ *un mot infini sur l'alphabet fini* Σ. *La suite* $(r_l(\mathbf{w}))_{l\in\mathbb{N}}$ *est croissante.*

Preuve. Soit $l \in \mathbb{N}$. Soit $X = \left\{x_0, x_1, \ldots, x_{j-1}\right\}$ l'ensemble des sous-mots récurrents de longueur l de $\mathbf{w}$. Pour $0 \leq i < j$, comme le mot x_i apparait une infinité de fois dans $\mathbf{w}$, et Σ est fini, il existe une infinité d'occurrences de x_i dans $\mathbf{w}$ suivies par la même lettre $a_i \in \Sigma$. Le mot x_ia_i est alors un sous-mot récurrent de longueur $l + 1$ de $\mathbf{w}$. Ainsi $r_{l+1}(\mathbf{w}) \geq r_l(\mathbf{w})$, et la suite est croissante. □

Proposition 8. *Soit* $\mathbf{w} = w_0w_1w_2\cdots$ *un mot infini sur l'alphabet fini* Σ. *Les propriétés suivantes sont équivalentes :*

- *(a) La suite* $(r_l(\mathbf{w}))_{l\in\mathbb{N}}$ *est bornée.*
- *(b) La suite* $(r_l(\mathbf{w}))_{l\in\mathbb{N}}$ *est stationnaire.*
- *(c) Il existe* $k \geq 0$ *tel que* $r_k(\mathbf{w}) \leq k$.
- *(d) Il existe* $m \geq 0$ *tel que* $r_{m+1}(\mathbf{w}) = r_m(\mathbf{w})$.
- *(e)* $\mathbf{w}$ *est ultimement périodique.*

Preuve. Les implications *(a)* $\Rightarrow$ *(b)* , *(b)* $\Rightarrow$ *(c)* et *(c)* $\Rightarrow$ *(d)* sont conséquence rapide de $r_0(\mathbf{w}) = 1$ et de la croissance de $(r_l(\mathbf{w}))_{l\in\mathbb{N}}$. Par ailleurs, si $\mathbf{w}$ est ultimement périodique de période $T > 0$, la suite $(r_l(\mathbf{w}))_{l\in\mathbb{N}}$ est bornée par T, donc *(e)* $\Rightarrow$ *(a)*.

Il reste donc à montrer que *(d)* $\Rightarrow$ *(e)*. Soit $X = \left\{x_0, x_1, \ldots, x_{j-1}\right\}$ l'ensemble des sous-mots récurrents de longueur m de $\mathbf{w}$. Comme $r_{m+1}(\mathbf{w}) = r_m(\mathbf{w})$, la lettre a_i construite dans la preuve de la proposition précédente est unique. Ainsi, à partir d'un certain rang N_i, toute occurrence de x_i est suivie de a_i. En posant $N = \max N_i$, on obtient que pour tout $n \geq N$, w_{n+m} est entièrement déterminé par $w_nw_{n+1}\cdots w_{n+m-1}$. On considère alors les mots $w_nw_{n+1}\cdots w_{n+m-1}$ pour $N \leq n \leq N + |\Sigma|^m$. Par le principe des tiroirs, deux d'entre eux sont égaux, par exemple ceux correspondant à n_1 et à $n_2 > n_1$, et d'après ce qui précède, on a : $\forall i \geq 0, w_{n_1+i} = w_{n_2+i}$. Donc $\mathbf{w}$ est ultimement périodique, de période $n_2 - n_1$. □

3. E *t*- ’

Soit $t \geq 2$ un entier. On note $\Sigma_t = \{0, \ldots, t-1\}$. Pour chaque entier naturel n, on note $(n)_t \in \Sigma_t^*$ la représentation en base t de n, sans 0 initiaux, et pour chaque mot $w \in \Sigma_t^*$, commençant éventuellement par des 0, on note $[w]_t \in \mathbb{N}$ l'entier qu'il représente (en base t). On définit alors pour $X \subset \mathbb{N}$ le langage $(X)_t = \{(x)_t, x \in X\}$ sur Σ_t, et pour $L \subset \Sigma_t^*$ la partie $[L]_t = \{[w]_t, w \in L\}$ de $\mathbb{N}$.

On remarque qu'avec ces définitions, $[(.)_t]_t$ est l'identité sur $\mathbb{N}$, tandis qu'appliquer $([.]_t)_t$ à un mot sur Σ_t supprime ses zéros initiaux.

Définition 9. *Une partie* X *de* $\mathbb{N}$ *est dite* t*-automatique lorsque* $(X)_t$ *est reconnaissable par un automate fini. Autrement dit,* t *est reconnaissable si il existe un automate qui est capable de reconnaître les écritures en base* t *des éléments de* X.

On rappelle que :

Lemme 10. *(Lemme du miroir) Si un langage L sur un alphabet Σ est reconnaissable, son langage miroir*

$$L^M = \{w_{n-1}w_{n-2}\cdots w_0 | w_0 w_1 \cdots w_{n-1} \in L\}$$

est reconnaissable.

Preuve. Il suffit de « retourner »toutes les transitions de l'automate et déchanger états finaux et initiaux (on perd son éventuel caractère déterministe). □

Lemme 11. *Soit L un langage sur l'alphabet Σ, et $a \in \Sigma$ telle qu'aucun mot de L ne commence par a. L est automatique si et seulement si a^*L l'est.*

Preuve. Si L est reconnaissable, soit $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ un automate le reconnaissant. L'automate $\mathcal{A}'$ obtenu à partir de $\mathcal{A}$ en ajoutant une transition de l'état initial q_0 vers lui-même, étiquetée par a, reconnait a^*L.

Réciproquement, si $\mathcal{A} = (Q, \Sigma_q, \delta, q_0, F)$ reconnait a^*L, on considère l'automate $\mathcal{A}'$, obtenu à partir de $\mathcal{A}$ en lui ajoutant un état puits $\bullet$ et en remplaçant toutes les transitions partant de q_0 avec la lettre a par une unique transition de q_0 vers $\bullet$ étiquetée par a. Cet automate reconnaît L. □

Ainsi le sens de lecture des nombres écrits en base t, ainsi que le fait d'autoriser les nombres à commencer ou non par des 0 n'ont aucune incidence dans la définition d'être t-automatique.

On va finir cette section en montrant que la classe des ensembles t-automatiques est stable par une transformation un peu plus élaborée, ce qui va nous servir dans la preuve du théorème de Cobham, dans la section 5.

Lemme 12. *(Stabilité par transformation affine réciproque) Si X est t-automatique, alors pour tout $A > 0$, et $B \geq 0$, l'ensemble $E = \{y \in \mathbb{N} | Ay + B \in X\}$ est t-automatique.*

Preuve. D'après les lemmes précédents, X est t-automatique si et seulement si $(X)_t^M 0^*$ est rationnel, et de même, E est t-automatique si et seulement si $(E)_t^M 0^*$ est rationnel. On va donc construire un automate reconnaissant ce second langage à partir d'un automate reconnaissant le premier : on calcule successivement les chiffres de $Ay + B$, en partant de celui de poids faible, en mémorisant la retenue, et on simule l'automate de départ en parallèle sur le résultat du calcul.

Soit $\mathcal{A} = (Q, \Sigma_t, \delta, q_0, F)$ un automate déterministe reconnaissant $(X)_t^M 0^*$. On écrit B en base t : $B = b_0 + tb_1 + \ldots + t^k b_k$. On considère l'automate déterministe $\mathcal{A}' = (Q', \Sigma_t, \delta', q_0', F')$ défini par :

$$\begin{cases} Q' = Q \times \{0, 1, \ldots, A\} \times \{0, 1, \ldots, k, \infty\}, \\ \delta'((q, r, i), c) = \left(\delta\left(q, (Ac + b_i + r \pmod t)\right), \left\lfloor \frac{Ac + b_i + r}{t} \right\rfloor, i + 1\right), \\ q_0' = (q_0, 0, 0), \\ F' = \left\{(q, r, i) \,\middle|\, \delta\left(q, \left(r + b_i + tb_{i+1} + \ldots + t^{k-i} b_k\right)_t^M\right) \in F\right\}, \end{cases}$$

où $b_\infty = 0$, $i + 1$ vaut ∞ si $i = k$ ou $i = \infty$.

Un état de cet automate est déterminé par un état de $\mathcal{A}$, une retenue, et un indice qui compte le numéro du chiffre que l'on traite, jusqu'à ce qu'on ait fini de traiter l'addition de B, après quoi la troisième composante vaut ∞.

Effectuer une transition consiste à calculer l'état suivant de l'automate $\mathcal{A}$ après une transition étiquetée par le chiffre de $Ay + B$ que l'on calcule en prenant en compte la retenue, à retenir la nouvelle retenue, et à incrémenter de 1 le compteur. On vérifie par récurrence que comme $c \leq t - 1$ et $b_i \leq t - 1$, la retenue ne dépasse jamais A, donc que l'automate était bien défini.

On commence sans retenue, et au 0^{e} chiffre.

Lorsqu'on a épuisé l'entrée, le calcul se termine, alors qu'on doit encore traiter la retenue restante. Ainsi les états acceptants ne sont pas simplement $F \times \{0\} \times \{\infty\}$, mais forment l'ensemble un peu plus compliqué F'.

On vérifie facilement que le nouvel automate reconnaît $(E)_t^M 0^*$. □

4. S ´ ´

Définition 13. *Soit X une partie de $\mathbb{N}$. Si il existe un entier $d > 0$ tel que pour tout $x \in X$ il existe $y \in X$ tel que $x < y \leq x + d$, alors X est dite d-syndétique.*

Le but de cette section est de montrer le théorème qui suit.

Théorème 14. *Soient $s, t \geq 2$ des entiers multiplicativement indépendants. Si une partie X de $\mathbb{N}$ est à la fois s- et t-automatique, alors elle est syndétique.*

Pour montrer ce résultat, on va établir quelques lemmes. Le premier est un résultat classique.

Lemme 15. *Soit $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ un automate déterministe, de fonction de transition étendue $\tilde{\delta} : Q \times \Sigma^* \to Q$. Pour chaque état $q \in Q$, l'ensemble*

$$L_q = \{|w| \in \mathbb{N} | w \in \Sigma^*, \tilde{\delta}(q, w) \in F\}$$

est ultimement périodique (sa fonction caractéristique est ultimement périodique).

Preuve. Pour chaque état $q \in Q$ l'ensemble L_s est un langage reconnu par l'automate $(Q, \Sigma, \delta, q, F)$, donc rationnel (par le théorème de Kleene), donc il suffit de montrer que l'ensemble des longueurs des mots d'un langage défini par une expression rationnelle est ultimement périodique. On va procéder par induction structurelle sur les expressions rationnelles.

Pour les parties de Σ, la propriété est immédiate.

Même si l'ensemble E des longueurs des mots du langage L n'est pas ultimement périodique, les longueurs des mots du langage L^* forment un ensemble E' ultimement périodique. En effet, soit $u \in L$, et soit $T = |u|$. Pour tout $w \in L^*$, $wu \in L^*$ et $|wu| = |w| + T$, donc l'ensemble E' est T-périodique. Ainsi E' est ultimement périodique de période le pgcd des éléments de E.

Il n'est pas difficile non plus de montrer que le produit de deux langages et la réunion conservent le caractère ultimement périodique de l'ensemble des longueurs (dans les deux cas on obtient une période égale au ppcm des périodes initiales). □

Lemme 16. *Soient $s \geq 2$ et X une partie s-automatique infinie de $\mathbb{N}$. Alors il existe des entiers $m, \alpha, \beta \geq 1$ tels que pour tout $k \in \mathbb{N}$, l'ensemble $X \cap \left[ms^{\alpha+\beta k}, (m+1)s^{\alpha+\beta k}\right[$ soit non vide. De plus, on peut choisir m arbitrairement grand.*

Preuve. Soit $\mathcal{A} = (Q, \Sigma_s, \delta, q_0, F)$ un automate déterministe reconnaissant $(X)_s$. Comme X est infini, il existe un entier m arbitrairement grand tel que $(m)_s$ soit préfixe d'un nombre infini d'éléments de $(X)_s$.

D'après le lemme précédent, appliqué à l'état $q = \tilde{\delta}(q_0, (m)_s)$, il existe $a \geq 0$ et $\beta > 0$ tels que L_q soit β-périodique à partir du rang a.

Or $((m)_s \Sigma_s^*) \cap (X)_s$ est infini, donc il existe un mot v tel que $(m)_s v \in (X)_s$ et $|v| > a$. Posons $\alpha = |v|$. Par β-périodicité, on a, pour chaque $k \geq 0$ qu'il existe un mot v_k de longueur $\alpha + \beta k$ tel que $(m)_s v_k \in (X)_s$, i.e. tel que $[(m)_s v_k]_s \in X$, autrement dit $ms^{\alpha+\beta k} + [v_k]_s \in X$.

Comme $0 \leq [v_k]_s < s^{\alpha+\beta k}$ on a trouvé $\alpha \geq 0$ et $\beta > 0$ tels que pour tout k, $\left[ms^{\alpha+\beta k}, (m+1)s^{\alpha+\beta k}\right[\cap X$ soit non-vide. □

Lemme 17. *Soient $s \geq 2$ et X une partie s-automatique infinie de $\mathbb{N}$. Soit $\mathcal{A} = (Q, \Sigma_s, \delta, q_0, F)$ l'automate minimal (déterministe) de $(X)_s$. Si l'état q est tel que $\mathbb{N}\backslash L_q$ est infini, alors il existe des entiers $m, \alpha, \beta \geq 1$ tels que pour tout $k \in \mathbb{N}$ l'ensemble $X \cap \left[ms^{\alpha+\beta k}, (m+1)s^{\alpha+\beta k}\right[$ soit vide.*

Preuve. Soit q un état tel que $\mathbb{N}\backslash L_q$ est infini. On peut supposer $q \neq q_0$ car si $\mathbb{N}\backslash L_{q_0}$ est infini, il existe un autre état q vérifiant la même propriété. Comme l'automate minimal est émondé, on peut fixer $m \in \mathbb{N}$ tel que $q = \delta(q_0, (m)_s)$. Par l'avant-dernier lemme, on a existence de $a \geq 0$ et $\beta > 0$ tels que L_q soit β-périodique à partir du rang a. Comme $\mathbb{N}\backslash L_q$ est infini, il existe $\alpha > a$ tels qu'il n'y ait aucun mot v de longueur α tel que $(m)_s v \in (X)_s$. Pour chaque $k \geq 0$, on déduit qu'il n'y a pas non plus de mot de la forme $(m)_s u$ dans $(X)_s$ vérifiant $|u| = \alpha + \beta k$, c'est-à-dire que $X \cap \left[ms^{\alpha+\beta k}, (m+1)s^{\alpha+\beta k}\right[$ est vide. □

On a enfin un dernier lemme.

Lemme 18. *Soient $t > s \geq 2$ deux entiers multiplicativement indépendants, et X une partie infinie s- et t-automatique de $\mathbb{N}$. Si $\mathcal{A} = (Q, \Sigma_t, \delta, q_0, F)$ est l'automate minimal de $(X)_t$, alors pour tout état $q \in Q$, L_q est cofini.*

Preuve. Supposons le contraire. Alors par les lemmes précédents il existe $n, \gamma, \delta \geq 1$ tels que pour tout $l \in \mathbb{N}$, $X \cap [nt^{\gamma+\delta l}, (n+1)t^{\gamma+\delta l}[$ soit vide, et il existe aussi $m, \alpha, \beta \geq 1$ tels que pour tout $k \in \mathbb{N}$, $X \cap [ms^{\alpha+\beta k}, (m+1)s^{\alpha+\beta k}[$ soit non-vide, avec de plus $m > n$.

Pour obtenir une contradiction, on applique un lemme 4, qui affirme l'existence de $K, L \geq 1$ tels que

$$nt^{\gamma+\delta L} \leq ms^{\alpha+\beta K} < (m+1)s^{\alpha+\beta K} \leq (n+1)t^{\gamma+\delta L}.$$

□

Preuve du Théorème. On suppose $t > s$. Soit $\mathcal{A} = (Q, \Sigma_t, \delta, q_0, F)$ est l'automate minimal de $(X)_t$. Pour chaque $q \in Q$ le lemme précédent affirme que L_q est cofini, donc qu'il existe un entier C_q tel que si $k \geq C_q$, alors $k \in L_q$. En posant $C = \max C_q$, il vient que pour tout état $q \in Q$ il existe un mot w_q de longueur C tel que $\delta(q, w_q) \in F$. Alors, pour chaque $n \in \mathbb{N}$, en posant $q_n = \delta(q_0, (n)_t)$, il vient $\delta(q_0, (n)_t w_{q_n}) = \delta(q_n, w_{q_n}) \in F$, c'est-à-dire $nt^C + [w_{q_n}]_t \in X$. Comme $0 \leq [w_{q_n}]_t < t^C$, on obtient que tout intervalle de longueur $2t^C$ contient un élément de X. C'est la conclusion recherchée. □

5. T ´ ` C

Les quatre premières sections de ce document ont présenté les différentes notions qui entrent en jeu dans la preuve du théorème de Cobham. La cinquième et dernière se charge de combiner toutes les remarques des sections précédentes pour montrer le théorème de Cobham, dont nous rappelons l'énoncé :

Théorème 19. *(Cobham) Soient $s, t \geq 2$ deux entiers multiplicativement indépendants. Si une partie X de $\mathbb{N}$ est s- et t-automatique, alors elle est ultimement périodique.*

Preuve. Les parties finies de $\mathbb{N}$ sont ultimement périodiques, donc on peut supposer X infinie.

On définit la relation d'équivalence ρ_s sur $\mathbb{N}$ par $\forall (x, y) \in \mathbb{N}^2$,

$$x \sim y \pmod{\rho_s} \Leftrightarrow \forall w \in \Sigma_s^*, ((x)_s w \in (X)_s \Leftrightarrow (y)_s w \in (X)_s).$$

Lemme 20. *Les classes d'équivalence pour ρ_s sont t-automatiques.*

Preuve. Pour chaque $u \in \Sigma_s^*$ on pose $E_u = \{y \in \mathbb{N} \mid ys^{|u|} + [u]_s \in X\}$. D'après le lemme 12 (stabilité par transformation affine réciproque), comme X est t-automatique, E_u l'est aussi. Or

$$E_u = [(E_u)_s]_s = [\{v \in (\Sigma_s \backslash \{0\})\Sigma_s^* \mid vu \in (X)_s\}]_s = [\{v \in \Sigma_s^* \mid vu \in (X)_s\}]_s = [(X)_s / u]_s,$$

donc on a montré que $\forall u \in \Sigma_s^*$, $[(X)_s/u]_s$ est t-automatique.

Soit $y_0 \in \mathbb{N}$.

Pour chaque $y \in \mathbb{N}$ tel que $y \nsim y_0$, on choisit $u_y \in \Sigma_s^*$ tel qu'on ait soit $(y_0)_s u_y \in (X)_s$ et $(y)_s u_y \notin (X)_s$, soit $(y_0)_s u_y \notin (X)_s$ et $(y)_s u_y \in (X)_s$. On pose ensuite

$$\mathcal{B}_y = \begin{cases} \overline{[(X)_s/u_y]_s} & \text{si } (y_0)_s u_y \notin (X)_s, \\ [(X)_s/u_y]_s & \text{si } (y_0)_s u_y \in (X)_s, \end{cases}$$

où le complémentaire est pris dans $\mathbb{N}$. Chacun des $\mathcal{B}_y$ est t-automatique. Montrons que $\{y' \in \mathbb{N} \mid y' \sim y_0\} = \bigcap_{y \nsim y_0} \mathcal{B}_y$, ce qui conclut, car le classe des langages rationnels, donc la classe des ensembles t-automatiques, est stable par intersection finie.

Si $y' \sim y_0$, pour chaque $y \nsim y_0$, on a l'équivalence

$$\begin{aligned} y' \in [(X)_s/u_y]_k &\Leftrightarrow (y')_s \in (X)_s/u_y \\ &\Leftrightarrow (y')_s u_y \in (X)_s \\ &\Leftrightarrow (y_0)_s u_y \in (X)_s, \end{aligned}$$

donc $y' \in \mathcal{B}_y$, puis $y' \in \bigcap_{y \nsim y_0} \mathcal{B}_y$.

Si $y' \nsim y_0$, on a l'équivalence

$$\begin{aligned} y' \in [(X)_s/u_{y'}]_k &\Leftrightarrow (y')_s \in (X)_s/u_{y'} \\ &\Leftrightarrow (y')_s u_{y'} \in (X)_s \\ &\Leftrightarrow (y_0)_s u_{y'} \notin (X)_s, \end{aligned}$$

donc $y' \notin \mathcal{B}'_y$, puis $y' \notin \bigcap_{y \nsim y_0} \mathcal{B}_y$. □

Un résultat classique sur les automates affirme que les classes d'équivalence de ρ_s sont en bijection naturelle avec les états de l'automate déterministe minimal reconnaissant $(X)_s$, donc il y en a un nombre fini. Comme chacune est t-automatique, on peut construire un automate $\mathcal{A} = (Q, \Sigma_t, \delta, q_0, \emptyset)$ qui s'arrête dans des états différents sur deux entrées non-équivalentes pour ρ_s (peu importent les états finaux de cet automate, car ce qui va nous intéresser est l'état précis où il s'arrête). On associe à cet automate la relation d'équivalence θ_t sur $\mathbb{N}$, définie par : $\forall (x, y) \in \mathbb{N}^2$,

$$x \sim y \pmod{\theta_t} \Leftrightarrow \delta(q_0, (x)_t) = \delta(q_0, (y)_t).$$

Cette relation est plus fine que ρ_s (i.e. les classes d'équivalence de ρ_s sont réunions de classes de θ_t), et est t-stable, c'est-à-dire vérifie

$$\forall j \geq 0, \forall 0 \leq n < t^j, x \sim y \pmod{\theta_t} \Rightarrow (xt^j + n) \sim (yt^j + n) \pmod{\theta_t}.$$

On pose c le nombre de classes d'équivalence pour θ_t, $\mathbf{v} = v_0 v_1 v_2 \cdots$ le mot infini tel que pour chaque $n \in \mathbb{N}$, v_n soit la classe d'équivalence de n pour ρ_s, et de même $\mathbf{u} = u_0 u_1 u_2 \cdots$ le mot infini tel que pour chaque $n \in \mathbb{N}$, u_n soit la classe d'équivalence de n pour θ_t.

Comme X est réunion de classes d'équivalence de ρ_s, il suffit de montrer que $\mathbf{v}$ est ultimement périodique pour montrer le théorème, donc, d'après la proposition 8, il suffit de montrer qu'il existe un entier m tel que le nombre de sous-mots récurrents de longueur m de $\mathbf{v}$ est borné par m. Pour ce faire, nous allons considérer un réel $\varepsilon > 0$, et construire des entiers $K = s^p$, $L = t^q$ et m bien choisis, puis montrer que tous les sous-mots récurrents de longueur m de $\mathbf{v}$ ont une occurrence qui est entièrement contenue dans un mot de la forme $\mathbf{v}[yL..(y+1)L-1] = v_{yL} v_{yL+1} \cdots v_{(y+1)L-1}$, pour un $y \in \mathbb{N}$ et qui, qui plus est, commence en l'une des $K\varepsilon$ premières lettres de ce mot. Comme la relation ρ_s est moins fine que θ_t, le mot $\mathbf{v}[yL..(y+1)L-1]$ est déterminé uniquement par le mot $\mathbf{u}[yL..(y+1)L-1]$, et comme θ_t est t-stable, et que L est une puissance de t, le mot $\mathbf{u}[yL..(y+1)L-1]$ est uniquement

déterminé par la lettre u_y, qui prend au plus c valeurs. Ainsi il y a au plus $c(K\varepsilon + 1)$ mots récurrents de m lettres. Si on parvient à rendre cette quantité plus petite que m, on a prouvé le théorème.

Pour chaque sous-mot récurrent $w = w_1w_2$ de longueur 2 de $\mathbf{v}$, l'ensemble des indices $n \in \mathbb{N}$ tels que $v_n = w_1$ et $v_{n+1} = w_2$ est à la fois s- et t-automatique, donc syndétique (par le théorème 14). Comme il y a un nombre fini $r_2(\mathbf{v}) \leq |\Sigma|^2 \leq c^2$ de tels mots w, il existe $d \in \mathbb{N}^*$ tel que tout sous-mot récurrent de longueur 2 de $\mathbf{v}$ a une autre occurrence au plus d lettres plus loin.

Soit $0 < \varepsilon < 1$. Par la proposition 3, il existe $\alpha, \beta \geq 0$ tels que

$$1 < \frac{t^\beta}{s^\alpha} < 1 + \frac{\varepsilon}{d}.$$

Soient $K = s^\alpha$, $L = t^\beta$, et $m = \lfloor K(1-\varepsilon) \rfloor$. Comme $L > K$ sont des entiers, $L \geq K + 1$, puis $1 + \frac{1}{K} \leq \frac{L}{K} < 1 + \frac{\varepsilon}{d}$, donc $K > \frac{d}{\varepsilon}$.

ρ_s est s-stable, et K est une puissance de s, donc $\mathbf{v}[xK..(x+2)K-1]$ est entièrement déterminé par $\mathbf{v}[x..x+1]$. Soit w un sous-mot récurrent de longueur m de $\mathbf{v}$. Comme $m < K$, chacune de ses occurrences apparait dans un sous-mot de $\mathbf{v}$ de la forme $\mathbf{v}[xK..(x+2)K-1]$, qui correspond au mot $\mathbf{v}[x..x+1]$ de longueur 2. Comme chaque mot de la forme $\mathbf{v}[xK..(x+2)K-1]$ contient au plus un nombre fini d'occurrences de w, et que w a une infinité d'occurrences dans $\mathbf{v}$, on déduit qu'il existe un sous-mot récurrent de longueur 2 de $\mathbf{v}$ tel que le mot de longueur $2K$ qu'il détermine contient w. Par définition de d, on peut alors construire une suite strictement croissante $(x_n)_{n\geq 1}$ d'entiers tels que

$$\forall n \in \mathbb{N}, x_{n+1} - x_n \leq d,$$

et $\mathbf{v}[x_n..x_n+1]$ est un mot constant, tel que le mot constant $\mathbf{v}[x_nK..(x_n+2)K-1]$ contienne w.

On peut alors écrire $\mathbf{v}[x_nK..(x_n+2)K-1] = w'ww''$. On pose $h = |w'|$. Soit $r \in \mathbb{N}$ minimal tel que $rK + h < rL$. Pour tout $1 \leq i \leq d$ on a, par minimalité de r, $(r-i)L \leq (r-i)K + h$, et par ailleurs

$$\begin{aligned}(r-i)K + h &\leq (rK + h) - iK \\ &< rL - iK \\ &< rL - i(L - K\frac{\varepsilon}{d}) \\ &\leq (r-i)L + K\varepsilon,\end{aligned}$$

donc en ajoutant jKL à chacun des membres, il vient : $\forall j \in \mathbb{N}$, $\forall 1 \leq i \leq d$,

$$(jK + r - i)L \leq (jL + r - i)K + h < (jK + r - i)L + K\varepsilon.$$

Comme $\{x_0, x_1, x_2, \ldots\}$ est syndétique, on a, pour j assez grand, qu'il existe $1 \leq i \leq d$ tel que $jL + r - i = x_n$ pour un certain $n \in \mathbb{N}$. On a alors, en notant $y = jK + r - i$, que

$$yL \leq x_nK + h < yL + K\varepsilon.$$

Comme

$$\begin{aligned}x_nK + h + m &< yL + K\varepsilon + \lfloor K(1-\varepsilon) \rfloor \\ &\leq yL + K \\ &< (y+1)L,\end{aligned}$$

et comme $\mathbf{v}[x_nK + h..x_nK + h + m - 1] = w$, w est un sous-mot de $\mathbf{v}[yL..(y+1)L-1]$, et on peut écrire $\mathbf{v}[yL..(y+1)L-1] = swt$, avec $|s| = x_nK + h - yL < K\varepsilon$.

Ainsi on a réussi à « capturer »une occurrence de w dans un sous-mot de $\mathbf{v}$ de la forme $\mathbf{v}[yL..(y+1)L-1]$, à une distance au plus $K\varepsilon$ du début. Un sous-mot récurrent w de $\mathbf{v}$ est donc entièrement déterminé par la lettre v_y et la longueur du mot s, donc

$$r_m(\mathbf{v}) \leq c(1 + K\varepsilon).$$

On veut que cette dernière expression soit plus petite que $K(1-\varepsilon)-1 \leq m$. Pour cela, il suffit d'avoir pris $\varepsilon < \frac{1}{2(c+1)}$, car alors $K > \frac{d}{\varepsilon} > 2(c+1)$, et on a

$$K\varepsilon(c+1) \leq \frac{K}{2} \leq K - c - 1,$$

d'où $c + K\varepsilon c \leq K - K\varepsilon - 1$, soit l'inégalité voulue.

Ainsi on obtient que $r_m(\mathbf{v}) \leq m$, donc que $\mathbf{v}$ est ultimement périodique, donc que X est ultimement périodique. □