Sur la façon dont les ensembles de nombres reconnaissables par des automates finis dépendent de la base

Alan Cobham

1. Résumé

C'est un fait connu que l'ensemble des puissances de deux est reconnaissable par un automate fini si la base de numération utilisée pour représenter les nombres est elle-même une puissance de deux, mais qu'il est non reconnaissable dans toutes les autres bases. D'un autre côté, l'ensemble des multiples de deux est reconnaissable quelle que soit la base de numération. Il est montré que la dernière situation est l'exception, et la première la règle : les seuls ensembles reconnaissables indépendamment de la base sont ceux qui sont ultimement périodiques ; les autres, si jamais ils sont reconnaissables, ne le sont que dans des bases qui sont des puissances d'un certain entier positif fixe.

2. Introduction

Un ensemble d'entiers non négatifs est ultimement périodique s'il est, à un nombre fini d'exceptions près, l'union d'un système de classes de résidus modulo un entier positif fixe. Tous ces ensembles sont reconnaissables par des automates finis indépendamment de la base de numération. En d'autres termes, pour chaque $m \geq 2$, il existe un automate fini qui peut distinguer les représentations en base m des membres d'un tel ensemble de celles de ses non-membres. En contraste, comme Büchi l'a montré [1], l'ensemble des puissances entières d'un entier $n \geq 2$ n'est reconnaissable en notation en base m que si m et n sont multiplicativement dépendants, c'est-à-dire seulement si $m^p n^q = 1$ possède une solution non triviale en entiers p et q. Il sera montré ici que ce dernier cas reflète la situation générale : à l'exception des ensembles ultimement périodiques, la reconnaissabilité est une notion dépendante de la base. Cela apporte un témoignage supplémentaire, d'un genre différent de celui présenté par Minsky et Papert [3], selon lequel, pour ce qui est de la reconnaissance d'ensembles de nombres, les automates finis sont faibles et quelque peu non naturels.

Théorème 1. *Soit S un ensemble d'entiers non négatifs et soient m et n des entiers positifs multiplicativement indépendants. Alors S est reconnaissable par des automates finis à la fois en notation en base m et en base n si et seulement s'il est ultimement périodique.*

Un théorème un peu plus faible, à savoir qu'un ensemble reconnaissable en notation en base n pour tout $n \geq 2$ est nécessairement ultimement périodique, a été établi indépendamment par J. Nievergelt en utilisant des arguments plus simples que ceux utilisés ici. La démonstration du théorème énoncé fournie ici constitue elle-même une simplification substantielle par rapport à une démonstration antérieure de ma part parue sous la forme d'une note de recherche IBM (IBM Research

IBM Watson Research Center
Yorktown Heights, New York.

Référence : A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems Theory 3 (1969) 186–192.

Note NC-577, "Sets Definable by Finite Automata-III", janv. 1966). La seconde formulation du théorème a été signalée par le reviewer.

Étant donné que les ensembles reconnaissables en notation unaire sont exactement ceux qui sont ultimement périodiques, cela peut être reformulé de la manière suivante.

Théorème 2. *Un ensemble S est reconnaissable à la fois en notation en base m et en base n pour certains m et n multiplicativement indépendants si et seulement s'il est reconnaissable en notation en base d pour tout $d \geq 1$.*

Le résultat connexe, à savoir que pour des m et n multiplicativement dépendants, tout ensemble reconnaissable dans une notation est reconnaissable dans l'autre, ne devrait poser aucun problème au lecteur.

3. Notation et terminologie

Pour $n \geq 2$, l'ensemble des chiffres en base n $\{0, 1, \ldots, d_{n-1}\}$ sera noté D_n et les éléments de D_n^*, c'est-à-dire les chaînes de chiffres en base n, seront appelés des n-chaînes. Nous désignons par $l(x)$ le nombre de chiffres dans la chaîne x et posons que x est propre si $l(x) > 0$ et que son premier symbole n'est pas 0.

Si p est un entier positif, $(p)_n$ est la n-chaîne propre que nous regardons ordinairement comme la représentation en base n de p ; par exemple, $(\text{cinq})_2$ est la 2-chaîne 101 ; nous ne nous écartons de la notation standard qu'en représentant zéro par la chaîne vide : $(\text{zéro})_n = \Lambda$.

Si x est une n-chaîne, $[x]_n$ est le nombre que x, une fois les zéros non significatifs supprimés, représente en notation en base n ; par exemple, $[0101]_2$ est le nombre cinq ; si x est vide ou ne contient que des 0, $[x]_n$ vaut zéro.

Un automate fini qui lit des n-chaînes, c'est-à-dire qui a D_n pour alphabet, sera appelé un n-automate. Un n-automate est caractérisé par la spécification d'un ensemble fini d'états G, d'une fonction de transition $\delta : G \times D_n \to G$, d'un état initial $s_0 \in G$, et d'un ensemble d'états d'acceptation $F \subset G$. Les états n'appartenant pas à F seront appelés états de rejet.

La fonction δ possède une extension naturelle au domaine $G \times D_n^*$ déterminée par la condition $\delta(s, xy) = \delta(\delta(s, x), y)$ où $s \in G$, $x, y \in D_n^*$ et xy désigne la concaténation de x et y. Nous disons qu'une chaîne x est acceptée ou rejetée selon que $\delta(s_0, x)$ est un état d'acceptation ou de rejet.

Un ensemble S d'entiers non négatifs est dit reconnaissable en notation en base n, ou brièvement n-reconnaissable, s'il existe un n-automate qui accepte exactement les n-chaînes x pour lesquelles $[x]_n \in S$. Selon cette convention, les zéros non significatifs doivent être ignorés pour déterminer l'acceptation ou le rejet d'une chaîne. Un ensemble reconnaissable à la fois en notation en base m et en base n est dit m-n-reconnaissable.

Nous disons que la chaîne x appartient à l'état s, $x \in s$, si $\delta(s_0, x) = s$. Un état est récurrent si $\delta(s, x) = s$ pour une certaine chaîne non vide x, et proprement récurrent si, de plus, $\delta(s_0, y) = s$

pour une certaine chaîne propre y ; ainsi, un état proprement récurrent est un état qui peut survenir plus d'une fois lors de la lecture d'une chaîne propre.

Nous ne nous intéresserons qu'aux automates réduits, c'est-à-dire ceux pour lesquels, premièrement, tous les états peuvent être atteints à partir de l'état initial et, deuxièmement, les états distincts s, s' sont inéquivalents au sens où pour une certaine chaîne x, l'un des états $\delta(s, x)$, $\delta(s', x)$ est dans F et l'autre en est à l'extérieur.

Une certaine familiarité avec les résultats et techniques de base des références [1] et [4], cette dernière en particulier, est supposée. Nous rappelons spécifiquement que, pour n fixe, la classe des ensembles n-reconnaissables est fermée par complémentation et intersection finie [4], et que si S est n-reconnaissable et a, b sont des entiers non négatifs fixes, alors l'ensemble $\{p \mid ap + b \in S\}$ est n-reconnaissable [1]. De plus, si l'on écrit $x \sim y$ lorsque x et y sont des n-chaînes appartenant au même état, alors $\sim$ est une relation d'équivalence invariante à droite : $x \sim y$ implique que $xz \sim yz$ pour toute n-chaîne z [4].

4. Démonstration du théorème

Tout au long de cette section, m et n sont des entiers positifs fixes et multiplicativement indépendants. Comme indiqué ci-dessus, tout ensemble ultimement périodique est m-n-reconnaissable ; ainsi, nous devons seulement montrer que tous les ensembles m-n-reconnaissables sont ultimement périodiques.

Lemme 3. *Soit $\mathfrak{N}$ un n-automate qui reconnaît un ensemble m-n-reconnaissable S, et soit s un état quelconque de $\mathfrak{N}$. Alors l'ensemble $\{p \mid (p)_n \in s\}$ est m-n-reconnaissable.*

Démonstration. Le remplacement de l'ensemble des états d'acceptation de $\mathfrak{N}$ par l'ensemble $\{s\}$ produit un automate qui n-reconnaît l'ensemble indiqué. Pour montrer sa m-reconnaissabilité, soit s' un état quelconque de $\mathfrak{N}$ distinct de s. Puisque $\mathfrak{N}$ est réduit par hypothèse, il existe une chaîne fixe z telle que l'un des couples $\delta(s, z), \delta(s', z)$ est un état d'acceptation et l'autre un état de rejet. Si $\delta(s, z)$ est l'état d'acceptation, posons $T(s') = \{p \mid pn^{l(z)} + [z]_n \in S\}$; sinon, posons $T(s') = \{p \mid pn^{l(z)} + [z]_n \notin S\}$. Dans les deux cas, $T(s')$ est un ensemble m-reconnaissable puisque S l'est. Pour $x \in s$, nous avons $\delta(s_0, xz) = \delta(\delta(s_0, x), z) = \delta(s, z)$, de sorte que $[xz]_n \in S$ ou $[xz]_n \notin S$ selon que $\delta(s, z)$ est ou n'est pas un état d'acceptation. Par conséquent, puisque $[xz]_n = [x]_n n^{l(z)} + [z]_n$, dans les deux cas $[x]_n \in T(s')$. De même, si $x \in s'$, alors $[x]_n \notin T(s')$. Si maintenant nous prenons l'intersection, $T = \bigcap_{s' \neq s} T(s')$, sur les (en nombre fini) états s' distincts de s, nous obtenons un ensemble qui est m-reconnaissable et qui a la propriété que $[x]_n \in T$ si et seulement si $x \in s$. Le lemme découle de l'observation que $[(p)_n]_n = p$. □

C'est un fait familier qu'on ne peut pas déterminer grand-chose concernant, disons, les chiffres initiaux d'un nombre décimal en lisant les chiffres initiaux du nombre binaire correspondant ; en fait, étant données deux chaînes, l'une de chiffres décimaux et l'autre de chiffres binaires, il est toujours possible de les étendre de telle sorte que les extensions représentent le même nombre. L'argument qui sous-tend cette observation peut être utilisé pour montrer que si S est un ensemble infini de nombres reconnaissables dans l'une ou l'autre notation, alors une chaîne dans l'une ou l'autre peut être étendue pour représenter un nombre dans S. De plus, le nombre de chiffres qui doivent être ajoutés peut, dans certaines limites, être préspécifié.

Lemme 4. *Soit $\mathfrak{N}$ un n-automate qui reconnaît un ensemble m-n-reconnaissable infini S, soit x une n-chaîne, et soient c et d des entiers avec $d > c \geq 0$. Alors il existe une n-chaîne y telle que xy soit accepté par $\mathfrak{N}$ et $l(y) \equiv c \pmod{d}$.*

Démonstration. Nous avons besoin du résultat suivant : Soient a et b des entiers positifs multiplicativement indépendants et soient k_1 et k_2 des nombres réels avec $k_2 > k_1 \geq 0$. Alors il existe des entiers positifs p et q arbitrairement grands tels que $k_1 < a^p b^{-q} < k_2$.

Cela peut s'établir en observant que l'indépendance multiplicative de a et b implique l'indépendance linéaire sur les rationnels de leurs logarithmes et en utilisant des techniques standard de la théorie des approximations rationnelles [2].

Soit $\mathfrak{M}$ un m-automate qui reconnaît S. Puisque S est infini, il existe des m-chaînes t, u, v telles que t est propre, $l(u) > 0$ et toutes les chaînes de la forme $tu^i v$, où u^i désigne la concaténation de i copies de u, sont acceptées par $\mathfrak{M}$ [4]. Posons $g = l(u)$, $h = l(v)$, et dans le résultat susmentionné, prenons $a = m^g$, $b = n^d$, $k_1 = ([x]_n + \frac{1}{4})/k$, $k_2 = ([x]_n + \frac{1}{2})/k$, où $k = \frac{m^h}{n^c}([t]_m + \frac{[u]_m}{m^g - 1})$.

Nous en concluons qu'il existe des entiers p et q arbitrairement grands tels que

$$[x]_n + \frac{1}{4} < \left([t]_m + \frac{[u]_m}{m^g - 1}\right) \frac{m^{gp+h}}{n^{dq+c}} < [x]_n + \frac{1}{2}$$

Clairement, pour tout q suffisamment grand,

$$-\frac{1}{4} < \frac{1}{n^{dq+c}} \left([v]_m - \frac{m^h [u]_m}{m^g - 1}\right) < \frac{1}{2}$$

En additionnant ces deux inégalités terme à terme, nous trouvons qu'il existe des entiers positifs spécifiques p et q pour lesquels

$$[x]_n n^{dq+c} < [t]_m m^{gp+h} + [u]_m \frac{m^{gp} - 1}{m^g - 1} m^h + [v]_m < ([x]_n + 1) n^{dq+c}.$$

Maintenant, pour le terme central de cette inégalité, nous avons

$$[t]_m m^{gp+h} + [u]_m \frac{m^{gp} - 1}{m^g - 1} m^h + [v]_m = [t]_m m^{gp+h} + [u]_m (m^{g(p-1)} + \cdots + m^g + 1) m^h + [v]_m = [tu^p v]_m$$

par conséquent, il existe un entier j avec $0 < j < n^{dq+c}$ tel que $[x]_n n^{dq+c} + j \equiv [tu^p v]_m$. À ce j correspond une n-chaîne y, peut-être impropre, telle que $j = [y]_n$, $l(y) = dq + c$ et

$$[tu^p v]_m = [x]_n n^{dq+c} + [y]_n = [xy]_n$$

Puisque $\mathfrak{M}$ accepte $tu^p v$, $\mathfrak{N}$ doit accepter xy et, puisque $l(y) \equiv c \pmod{d}$, le lemme s'ensuit. □

Lemme 5. *À tout n-automate $\mathfrak{N}$ qui reconnaît un ensemble m-n-reconnaissable infini correspond une constante $\lambda = \lambda(\mathfrak{N})$ ayant la propriété que pour tout entier $L \geq \lambda$, tout état proprement récurrent s de $\mathfrak{N}$, et toute n-chaîne x, il existe une n-chaîne z pour laquelle $l(z) = L$ et $xz \in S$.*

Démonstration. Pour tout état proprement récurrent s de $\mathfrak{N}$, soit $S_s = \{p \mid (p)_n \in s\}$. Clairement, S_s est infini et, d'après le lemme 1, il est m-n-reconnaissable. Soit y_1 une chaîne dans s et soit d_s le plus grand commun diviseur des longueurs de toutes les chaînes y pour lesquelles $\delta(s, y) = s$. D'après le lemme 2, appliqué à un automate qui n-reconnaît S_s, il existe une chaîne y_2 telle que $y_1 y_2 \in S_s$ et $l(y_2) \equiv 1 \pmod{d_s}$. Puisque, cependant, $\delta(s, y_2) = s$, cela implique que $d_s = 1$, et il s'ensuit aisément qu'il existe une constante λ_s telle que pour tout $L \geq \lambda_s$, il existe une chaîne y pour laquelle $l(y) = L$ et $\delta(s, y) = s$. Nous posons $\lambda(\mathfrak{N}) = Q + \max \lambda_s$, où Q est le nombre d'états de $\mathfrak{N}$ et le maximum est pris sur l'ensemble de ses états proprement récurrents.

Maintenant, soit x une n-chaîne arbitraire et s un état proprement récurrent arbitraire de $\mathfrak{N}$. Une autre application des lemmes 1 et 2 montre l'existence d'une certaine chaîne z_1 telle que $xz_1 \in S$. Mais l'existence d'une telle chaîne implique [4] l'existence d'une chaîne pour laquelle, de plus, $l(z_1) \leq Q$. Alors, pour $L \geq \lambda(\mathfrak{N})$, nous avons $\lambda_s \leq \lambda(\mathfrak{N}) - Q \leq L - l(z_1)$, de sorte que, d'après ce que nous avons établi ci-dessus, il existe une chaîne z_2 avec $\delta(s, z_2) = s$ et $l(z_2) = L - l(z_1)$. En posant $z = z_1 z_2$, nous avons $l(z) = L$ et $xz \in s$, ce qui établit le lemme. □

C'est un corollaire simple que sous les hypothèses du lemme, seuls des états proprement récurrents peuvent suivre des états proprement récurrents. Car si s est un tel état et x une n-chaîne quelconque, il existe une chaîne non vide y telle que $s = \delta(\delta(s, x), y) = \delta(s, xy)$. Alors $\delta(\delta(s, x), yx) = \delta(\delta(s, xy), x) = \delta(s, x)$, de sorte que $\delta(s, x)$ est proprement récurrent. À son tour, cela implique que pour toute chaîne propre x de longueur au moins égale au nombre d'états de $\mathfrak{N}$, $\delta(s_0, x)$ est proprement récurrent.

D'après le lemme 1, à chaque état s_i d'un n-automate $\mathfrak{N}$ qui reconnaît un ensemble m-n-reconnaissable correspond un m-automate $\mathfrak{M}_i$ qui reconnaît l'ensemble $\{p \mid (p)_n \in s_i\}$. Supposons que p_1 et p_2 soient des nombres dont les représentations en base m ont des parties initiales qui sont indiscernables (au sens où elles appartiennent au même état) par l'un quelconque des $\mathfrak{M}_i$ et des parties terminales consistant en des chaînes de 0 de longueur égale. Alors les représentations de $p_1 + r$ et $p_2 + r$ seront indiscernables par l'une quelconque de ces machines, pourvu que r soit suffisamment petit pour que son addition à p_1 ou p_2 ne provoque pas de retenue au-delà de la chaîne terminale de 0 dans leurs représentations. De ceci nous inférons que les représentations en base n correspondantes doivent appartenir au même état de $\mathfrak{N}$. Utilisé conjointement avec le lemme 3, cet argument nous permet de montrer l'existence d'un nombre g tel que pour tout état proprement récurrent s donné de $\mathfrak{N}$, $\delta(s, z)$ ne dépend que de la longueur de z et de la classe de résidus de $[z]_n$ modulo g.

Nous introduisons la notation additionnelle suivante. Pour q un entier positif, $e(q)$ est le plus grand entier tel que $n^{e(q)}$ divise m^q, $f(q)$ est le plus grand entier tel que $n^{f(q)}$ soit inférieur à m^q, et $R(q)$ est le nombre de classes de résidus distinctes modulo $n^{f(q)}$ dans lesquelles tombent les valeurs de la forme $(km + 1)m^q$ lorsque k varie sur les entiers positifs.

Lemme 6. $\lim_{q\to\infty} R(q) = \infty$.

Démonstration. Pour chaque q, $d(q) = m^q/n^{e(q)}$ est un entier, et l'indépendance multiplicative de m et n implique clairement que $d(q) \neq d(q')$ chaque fois que $q \neq q'$. Par conséquent, $\lim_{q\to\infty} d(q) = \infty$. Par définition, $n^{f(q)+1} \geq m^q = d(q)n^{e(q)}$, de sorte que $n^{f(q)-e(q)} \geq d(q)/n$ et il s'ensuit que $\lim_{q\to\infty}(f(q) - e(q)) = \infty$.

Supposons que k_1 et k_2 soient des entiers avec $k_1 > k_2$, et que $(k_1m+1)m^q \equiv (k_2m+1)m^q \pmod{n^{f(q)}}$. Alors $(k_1-k_2)m^{q+1} = (k_1-k_2)d(q)mn^{e(q)} \equiv 0 \pmod{n^{f(q)}}$; par conséquent, $n^{f(q)-e(q)}$ doit diviser $(k_1-k_2)d(q)m$. Puisque n ne divise pas $d(q)$, il existe un nombre premier p qui divise n à une puissance supérieure à celle à laquelle il divise $d(q)$, de sorte que $p^{f(q)-e(q)}$ doit diviser $(k_1-k_2)m$. Ainsi $k_1-k_2 \geq p^{f(q)-e(q)}/m$ de sorte que $R(q) \geq p^{f(q)-e(q)}/m$ également, et la relation limite sur l'exposant $f(q)-e(q)$ dérivée ci-dessus implique le résultat souhaité. □

Lemme 7. *Associé à chaque n-automate $\mathfrak{N}$ qui reconnaît un ensemble m-n-reconnaissable, il existe un entier positif g ayant la propriété que pour tout état proprement récurrent s de $\mathfrak{N}$ et toutes n-chaînes z_1 et z_2 telles que $l(z_1) = l(z_2)$ et $[z_1]_n \equiv [z_2]_n \pmod{g}$, on a $\delta(s, z_1) = \delta(s, z_2)$.*

Démonstration. Soit Q le nombre d'états de $\mathfrak{N}$, soit $\mathfrak{M}_i$ le m-automate associé à l'état s_i de $\mathfrak{N}$ de la manière décrite ci-dessus ($i = 0, 1, \ldots, Q-1$) et soit Q_i le nombre d'états de $\mathfrak{M}_i$. D'après le lemme 4, nous pouvons sélectionner un entier q pour lequel $R(q) > n^{\lambda+1}Q\prod_{i=0}^{Q-1} Q_i$, où $\lambda = \lambda(\mathfrak{N})$ est la constante du lemme 3.

Il est aisé de vérifier que pour tout entier positif k, le nombre $(km+1)m^q$ possède des représentations de la forme $((km+1)m^q)_m = u10^q$, $((km+1)m^q)_n = xy$ où u est une m-chaîne propre, x est une n-chaîne propre, et y est une n-chaîne pour laquelle $l(y) = f(q)$. Sur la base de ces représentations, nous partargeons l'ensemble des nombres de la forme $(km+1)m^q$ en $Q\prod_{i=0}^{Q-1} Q_i$ classes comme suit. Soit $\sim$ la relation d'équivalence sur les n-chaînes déterminée par $\mathfrak{N}$ et, pour $i = 0, \ldots, Q-1$, soit $\sim_i$ la relation d'équivalence sur les m-chaînes déterminée par $\mathfrak{M}_i$. Pour des entiers positifs k_1 et k_2, soient u_1, x_1, y_1 et u_2, x_2, y_2 les chaînes associées, comme ci-dessus, aux représentations de $(k_1m+1)m^q$ et $(k_2m+1)m^q$, respectivement. Nous plaçons maintenant deux tels nombres dans la même classe si et seulement si $x_1 \sim x_2$ et $u_1 \sim_i u_2$ pour $i = 0, \ldots, Q-1$.

En raison de la manière dont nous avons choisi q, l'une des classes ainsi construites doit contenir au moins $n^{\lambda+1}$ nombres qui sont distincts modulo $n^{f(q)}$. En observant que $[y]_n < n^{f(q)}$ et $(km+1)m^q \equiv [y]_n \pmod{n^{f(q)}}$, nous voyons qu'il existe deux nombres, $p_1 = (k_1m+1)m^q$ et $p_2 = (k_2m+1)m^q$, qui appartiennent à la même classe et pour lesquels $0 < [y_1]_n - [y_2]_n < n^{f(q)-\lambda-1}$.

En fixant une paire quelconque p_1, p_2 pour laquelle cette relation tient, nous posons $g = [y_1]_n - [y_2]_n$. Supposons que z_1 et z_2 soient des n-chaînes avec $g = [z_1]_n - [z_2]_n$ et $l(z_1) = l(z_2) = l \leq f(q) - \lambda$ et que s soit un état proprement récurrent de $\mathfrak{N}$. D'après le lemme 3, il existe une n-chaîne w avec $l(w) = f(q) - l$ telle que $x_1w \in S$. Alors, puisque $x_1 \sim x_2$, $x_2w \in S$ également. Soit $r = [x_1wz_1]_n - p_1$. Alors

$$\begin{aligned} r &= ([x_1]_n n^{f(q)} + [w]_n n^l + [z_1]_n) - ([x_1]_n n^{f(q)} + [y_1]_n) \\ &= [w]_n n^l + [z_1]_n - [y_1]_n = [w]_n n^l + [z_2]_n - [y_2]_n \\ &= [x_2wz_2]_n - p_2, \end{aligned}$$

de sorte que p_1+r et p_2+r ont pour représentations en base n $(p_1+r)_n = x_1wz_1$ et $(p_2+r)_n = x_2wz_2$. Puisque $|r| < n^{f(q)} < m^q$, leurs représentations en base m ont la forme $(p_1+r)_m = u_1dt$ et $(p_2+r)_m = u_2dt$, où t est une n-chaîne avec $l(t) = q$ et d est le chiffre 1 ou le chiffre 0 selon que $r \geq 0$ ou $r < 0$. Du fait que $u_1 \sim_i u_2$, il découle par l'invariance à droite de $\sim_i$ que $u_1dt \sim_i u_2dt$ pour chaque $i = 0, \ldots, Q-1$. De la propriété fondamentale des $\mathfrak{M}_i$ nous inférons immédiatement que $x_1wz_1 \sim x_2wz_2$. Ainsi, puisque $x_1w \in S$ et $x_2w \in S$, $\delta(s, z_1) = \delta(s, z_2)$. Nous remarquons que si

deux chaînes de même longueur représentent des nombres différant d'un multiple entier de g, alors l'une peut être transformée en l'autre par une succession de changements préservant la longueur, chacun modifiant la magnitude du nombre correspondant exactement de g. Par conséquent, cette conclusion vaut également si la condition $[z_1]_n - [z_2]_n = g$ est remplacée par la condition $[z_1]_n \equiv [z_2]_n \pmod{g}$, et nous avons établi le lemme sous la restriction $l(z_1) = l(z_2) \leq f(q) - \lambda$.

Le cas général est démontré par récurrence sur la longueur commune des z_i. En supposant que le lemme vaut pour un $l \geq f(q) - \lambda$ donné, soient z_1 et z_2 des n-chaînes avec $l(z_1) = l(z_2) = l + 1$ et $[z_1]_n \equiv [z_2]_n \pmod{g}$, et soit s un état proprement récurrent. Alors z_1 et z_2 ont la forme $z_1 = d_1 v_1 w_1$ et $z_2 = d_2 v_2 w_2$, où d_1 et d_2 sont des chiffres isolés, $l(v_1) = l(v_2) = f(q) - \lambda - 1$, $l(w_1) = l(w_2) = l - f(q) + \lambda + 1$. Puisque $g < n^{f(q)-\lambda-1}$, il existe une chaîne v_1' avec $l(v_1') = l(v_1)$ telle que $[d_1 v_1]_n \equiv [d_2 v_1']_n \pmod{g}$ de sorte que, puisque $l(d_1 v_1) = f(q) - \lambda$, par le cas particulier établi ci-dessus, $\delta(s, d_1 v_1) = \delta(s, d_2 v_1')$. Alors $\delta(s, z_1) = \delta(\delta(s, d_1 v_1), w_1) = \delta(\delta(s, d_2 v_1'), w_1) = \delta(\delta(s, d_2), v_1' w_1)$. Aussi $\delta(s, z_2) = \delta(\delta(s, d_2), v_2 w_2)$. Cependant, $l(v_1' w_1) = l(v_2 w_2) = l$ et $[v_1' w_1]_n \equiv [v_2 w_2]_n \pmod{g}$, de sorte que par l'hypothèse de récurrence, $\delta(\delta(s, d_2), v_1' w_1) = \delta(\delta(s, d_2), v_2 w_2)$, où nous avons utilisé le fait, noté précédemment, que $\delta(s, d_2)$ doit être proprement récurrent puisque s l'est. Il s'ensuit que $\delta(s, z_1) = \delta(s, z_2)$, ce qui achève la démonstration du lemme. □

En venant maintenant à la démonstration du théorème lui-même, nous supposons que S est un ensemble m-n-reconnaissable, et $\mathfrak{N}$ un n-automate qui le reconnaît. Pour montrer que S est ultimement périodique, il suffit de montrer que, pour chaque entier h, $0 \leq h < g$, où g est la constante du lemme précédent, si S contient une infinité de nombres équivalents à h modulo g, alors il contient tous ces nombres à un nombre fini près. En fixant h, nous posons $S_h = S \cap \{p \mid p \equiv h \pmod{g}\}$ et supposons que S_h est infini. Puisqu'il est l'intersection de deux ensembles m-n-reconnaissables, il est lui-même m-n-reconnaissable. Soit $\mathfrak{N}_h$ un n-automate qui reconnaît S_h, soit $\lambda = \lambda(\mathfrak{N}_h)$ la constante associée à $\mathfrak{N}_h$ comme dans le lemme 3, et soit Q le nombre d'états de $\mathfrak{N}$. Pour nos besoins, il suffit maintenant de montrer que si $p \equiv h \pmod{g}$ et $p \geq n^{Q+\lambda}$, alors $p \in S$.

Supposons que p possède ces propriétés. Alors il admet une représentation $(p)_n = xy$ où $l(x) = Q$ et $l(y) > \lambda$. Puisque S_h est infini, $\mathfrak{N}_h$ doit posséder un état d'acceptation proprement récurrent, disons s. D'après le lemme 3, il existe une n-chaîne z telle que $l(z) = l(y)$ et $xz \in s$. Par conséquent, $[xz]_n \equiv h \pmod{g}$ et, puisque $[xy]_n \equiv h \pmod{g}$ également, $[y]_n \equiv [z]_n \pmod{g}$. D'un autre côté, puisque $l(x) = Q$, $\delta(s_0, x)$ est un état proprement récurrent de $\mathfrak{N}$ (ici s_0 est l'état initial de $\mathfrak{N}$), et il découle du lemme 5 que $\delta(s_0, xy) = \delta(\delta(s_0, x), y) = \delta(\delta(s_0, x), z) = \delta(s_0, xz)$. Ainsi, xy est accepté par $\mathfrak{N}_h$ et par suite également par $\mathfrak{N}$. Par conséquent, $p = [xy]_n \in S$.

Ceci achève la démonstration.

Références

1. J. R. Büchi, Weak second-order arithmetic and finite automata, Z. Math. Logik Grundlagen Math. 6 (1960), 66–92.
2. J. W. S. Cassels, An Introduction to Diophantine Approximation, Cambridge University Press, 1957.

3. M. Minsky et S. Papert, Unrecognizable sets of numbers, J. Assoc. Comput. Mach. 13 (1966), 281–286.
4. M. O. Rabin and D. Scott, Finite automata and their decision problems, IBM J. Res. Develop. 3 (1959), 114–125.