

Ensembles de nombres non reconnaissables

Marvin Minsky et Seymour Papert

1966

1. Résumé

Quand est-ce qu'un ensemble A d'entiers positifs, représentés en nombres binaires, est "régulier" au sens où il s'agit d'un ensemble de séquences pouvant être reconnu par une machine à états finis ? Soit $\pi_A(n)$ le nombre de membres de A inférieurs à l'entier n . Il est démontré que le comportement asymptotique de $\pi_A(n)$ est soumis à de sévères contraintes si A est régulier. Ces contraintes sont violées par de nombreux ensembles numériques naturels importants dont les fonctions de distribution peuvent être calculées, au moins asymptotiquement. Ceux-ci incluent l'ensemble P des nombres premiers pour lesquels $\pi_P(n) \sim \frac{n}{\log n}$ pour n grand, l'ensemble des entiers $A(k)$ de la forme n^k pour lesquels $\pi_{A(k)}(n) \approx n^{1/k}$, et bien d'autres. Cependant, la technique ne peut pas fournir une procédure de décision pour la régularité, car pour tout ensemble régulier infini A , il existe un ensemble non régulier A' pour lequel $|\pi_A(n) - \pi_{A'}(n)| \leq 1$, de sorte que les comportements asymptotiques des deux fonctions de distribution sont essentiellement identiques.

2. Introduction

Soit A un certain ensemble d'entiers positifs écrits en notation binaire. Il est naturel de se demander quel genre de machine de calcul pourrait reconnaître l'ensemble au sens de décider si une séquence binaire donnée représente un nombre appartenant à A . La technique décrite dans cette note permet de montrer que certains ensembles ne peuvent pas être reconnus par des automates à états finis (c'est-à-dire que ces ensembles ne sont pas "réguliers"). L'idée essentielle est la suivante : soit $\pi_A(n)$ le nombre de membres de A inférieurs à l'entier n . Il est démontré que le comportement asymptotique de $\pi_A(n)$ est soumis à de sévères contraintes si A est régulier. Ces contraintes sont violées par de nombreux ensembles numériques naturels importants dont les fonctions de distribution peuvent être calculées, au moins asymptotiquement. Ceux-ci incluent l'ensemble P des nombres premiers, pour lesquels $\pi_P(n) \sim \frac{n}{\log n}$ pour n grand, l'ensemble des entiers $A(k)$ de la forme n^k , pour lesquels $\pi_{A(k)}(n) \approx n^{1/k}$, et bien d'autres. La technique ne peut cependant pas fournir de procédure de décision pour la régularité, car pour chaque ensemble régulier infini A , il existe un ensemble non régulier A' pour lequel $|\pi_A(n) - \pi_{A'}(n)| \leq 1$, de sorte que les comportements asymptotiques des deux fonctions de distribution sont essentiellement identiques.

Nous ne considérons ici que la représentation binaire, afin d'éviter des déclarations pompeuses, mais les mêmes résultats peuvent être obtenus pour toute base en remplaçant tous les 2 par des r dans la suite. Nous avertissons les lecteurs de ne pas confondre l'affirmation selon laquelle les nombres premiers écrits sous forme binaire ne constituent pas un ensemble régulier avec l'affirmation triviale selon laquelle l'ensemble des chaînes de longueur première n'est pas régulier.

3. Notation

1. Considérons l'ensemble des chaînes de 0 et de 1 dont le premier symbole est un 1, c'est-à-dire $N = 1(0 \vee 1)^*$, en utilisant la notation de Kleene.
2. De telles chaînes sont considérées de manière ambiguë comme des entiers en base 2 ou comme des chaînes de 0 et de 1. Les nombres sont présentés à la machine par les chiffres de poids fort en premier. (Cette convention est inoffensive puisque l'ensemble des chaînes inversées d'un ensemble régulier est régulier).
3. Pour tout entier x , $L(x)$ est le nombre de chiffres de x , c'est-à-dire $2^{L(x)-1} \leq x < 2^{L(x)}$.
4. Définissons la concaténation “.” par $x \cdot y = 2^{L(y)}x + y$.
5. A désigne toujours un ensemble d'entiers positifs et $\pi_A(n)$ la cardinalité de $\{x \mid 1 \leq x \leq n\}$.
6. Si A est régulier, soit M_A l'automate réduit (c'est-à-dire minimal) qui reconnaît A . Dans la discussion de tout automate particulier M , Q désigne son ensemble d'états, q_0 son état initial, Q_F son ensemble d'“états finaux” (dont l'apparition signifie l'acceptation d'une chaîne), et $\delta(q, x)$ la fonction de transition d'état, c'est-à-dire que la séquence x amène l'automate de l'état q à l'état $\delta(q, x)$.
7. Un état mort est un état q tel que $\delta(q, x) \in Q_F$ n'est satisfait par aucun x . (Si l'automate est réduit, cela équivaut à dire que $\delta(q, x) = q$ pour tout x , puisqu'il n'y a qu'un seul état mort dans une machine minimale).
8. Nous nous intéressons aux sous-ensembles de $N = 1(0 \vee 1)^*$ plutôt qu'aux sous-ensembles de $(0 \vee 1)^*$. Nous considérons comme triviale la partie de l'automate qui vérifie simplement que la séquence d'entrée commence par un 1. Nous nous écarterons de l'hypothèse de minimalité en autorisant un état mort spécial dans lequel la machine est poussée par un zéro initial. Dans la suite, “état mort” désigne un état mort autre que celui-ci.
9. Par commodité, la convention suivante est adoptée : pour tout ensemble A , et tout nombre réel x , $\pi_A(x) = \pi_A([x])$, où $[x]$ est la partie entière de x . Lorsque $\pi_A(n)$ est une fonction “naturelle”, telle que $\frac{n}{\log n}, \frac{x}{\log x}$ sera utilisé comme approximation de $\frac{[x]}{\log[x]}$ pour de très grandes valeurs de x .

4. Théorèmes

Tout d'abord, les conséquences du fait que M possède des états morts seront montrées.

Proposition 1. *Soit $M = M_A$ et supposons que :*

- (a) $\delta(q_0, \alpha)$ est un état mort,
- (b) $\lambda_0 = \frac{\alpha + 1}{\alpha}$, et
- (c) $\lim_{n \rightarrow \infty} \frac{\pi_A(n)}{\pi_A(\lambda_0 n)} = \theta$.

Alors $\theta = 1$.

Démonstration. Posons $n_m = 2^m \alpha$. Alors $\lambda_0 n_m = 2^m(\alpha + 1)$. Par l'hypothèse (a), il n'existe aucun β tel que $\alpha \cdot \beta \in A$. En d'autres termes, peu importe le choix de m , il n'existe aucun $n \in A$ tel que :

$$n_m = 2^m \alpha \leq n < 2^m \alpha + 2^m = \lambda_0 n_m$$

où $m = L(\beta)$.

Alors $\pi_A(n_m)/\pi_A(\lambda_0 n_m) = 1$ car il n'y a pas de membres de A entre n_m et $\lambda_0 n_m$. Mais $\{\pi_A(n_m)/\pi_A(\lambda_0 n_m)\}$ est une sous-suite infinie de la séquence, supposée par l'hypothèse (c) être convergente, $\{\pi_A(n)/\pi_A(\lambda_0 n)\}$. Il s'ensuit que la limite, θ , de cette séquence (si la limite existe) est 1.

Le fait sous-jacent est donc que les états morts produisent de grands écarts dans la suite de nombres reconnus par une machine. Ci-dessous, il est montré que s'il n'y a pas d'état mort, les écarts ne peuvent pas croître de la même manière.

Nous déduisons immédiatement la version affaiblie, mais plus facile à utiliser :

Proposition 2. *Si $\left(\frac{\pi_A(n)}{\pi_A(\lambda n)}\right) \rightarrow \theta(\lambda)$ pour tout λ réel et si $\theta(\lambda) = 1$ seulement si $\lambda = 1$, alors A ne peut pas être un ensemble régulier dont l'automate réduit possède un état mort.*

Dans certains cas intéressants (voir ci-dessous), $\pi(n)/\pi(\lambda n)$ ne converge pas. Nous pouvons parfois encore utiliser un critère plus strict mais moins élégant :

Proposition 3. *Soit a_r le r -ième membre de A par ordre de grandeur. Alors si :*

$$\lim_{r \rightarrow \infty} \frac{a_{r+1} - a_r}{a_r} = 0$$

A ne peut pas être un ensemble régulier dont l'automate réduit possède un état mort.

Démonstration. Supposons que A soit un ensemble régulier dont l'automate réduit possède un état mort, et soient α , λ_0 et n_m définis comme dans la démonstration de la Proposition 1. Désignons par k_m le nombre de membres de A inférieurs à n_m , c'est-à-dire que k_m est le plus grand entier tel que $a_{k_m} < n_m$. Puisqu'aucun membre de A ne peut se trouver entre n_m et $\lambda_0 n_m$, nous avons :

$$a_{k_m+1} \geq \lambda_0 n_m$$

Ainsi :

$$\frac{a_{k_m+1} - a_{k_m}}{a_{k_m}} \geq \frac{\lambda_0 n_m - n_m}{n_m} = \lambda_0 - 1 = \frac{1}{\alpha}$$

Il s'ensuit que $(a_{r+1} - a_r)/a_r$ ne peut pas converger vers 0 lorsque $r \rightarrow \infty$.

Enfin, examinons l'autre facette de la question : que se passe-t-il si M n'a pas d'état mort ?

Proposition 4. *Si A est régulier et que M_A n'a pas d'état mort, alors $\pi_A(n)/n \geq 2^{-2N}$, où N est le nombre d'états de M_A . Ainsi, la densité de A ne peut pas converger vers zéro.*

Démonstration. Pour chaque entier t , nous définissons une application injective g :

$$g : [2^{Nt}, 2^{Nt+1}) \rightarrow [2^{Nt}, 2^{Nt+N}) \cap A$$

où $[a, b)$ désigne l'intervalle $a \leq x < b$.

Pour tout $\alpha \in [2^{Nt}, 2^{Nt+1})$, soit β le plus petit entier pour lequel $\alpha \cdot \beta \in A$. Un tel β doit exister parce que $\delta(q_0, \alpha)$ n'est pas mort. De plus, $\beta < 2^N$ parce que le plus court chemin de $\delta(q_0, \alpha)$ à un membre de Q_F ne peut pas être plus long que $N - 1$. Il s'ensuit que $\alpha \cdot \beta < 2^{Nt+N}$ de sorte que $\alpha \cdot \beta \in [2^{Nt}, 2^{Nt+N}) \cap A$. Ainsi, si nous définissons $g(\alpha) = \min_{\beta} \{\beta \mid \alpha \cdot \beta \in A\}$, g a l'ensemble d'arrivée requis. Pour voir qu'il est injectif, remarquons simplement que α peut être récupéré comme les Nt premiers chiffres de $g(\alpha)$.

Il s'ensuit que $[2^{Nt}, 2^{Nt+N}) \cap A$ contient au moins autant de membres que $[2^{Nt}, 2^{Nt+1})$. Par conséquent, $\pi_A(2^{Nt+N}) \geq 2^{Nt+1} - 2^{Nt} = 2^{Nt}$. Considérons maintenant un nombre arbitraire n . Pour un certain t , $n \in [2^{Nt}, 2^{N(t+1)})$, et puisque $\pi_A(x)$ croît de manière monotone :

$$\frac{\pi_A(n)}{n} \geq \frac{\pi_A(2^{Nt})}{2^{N(t+1)}} \geq \frac{2^{N(t-1)}}{2^{N(t+1)}} = 2^{-2N}$$

En combinant ce résultat avec les conséquences des Propositions 2 et 3, on obtient le critère suivant.

Critère. Pour prouver qu'un ensemble A n'est pas régulier, il suffit de vérifier la condition 1 et la condition 2 ou 2'.

- **condition 1.** $\frac{\pi_A(n)}{n} \rightarrow 0$ lorsque $n \rightarrow \infty$.
- **condition 2.** $\frac{\pi_A(n)}{\pi_A(\lambda n)} \rightarrow \theta(\lambda)$ lorsque $n \rightarrow \infty$, et $\theta(\lambda) \neq 1$ pour tout $\lambda \neq 1$.
- **condition 2'.** $\frac{a_{n+1} - a_n}{a_n} \rightarrow 0$ lorsque $n \rightarrow \infty$.

Si A est régulier, d'après la Proposition 1, il possède un état mort, mais d'après la Proposition 2 ou 3, il n'en a aucun.

5. Applications

Tout d'abord, nous discutons de quelques exemples qui peuvent être résolus en utilisant le critère de la Section 3.

Exemple 1. $A = \{m^k \mid k \text{ entier fixe}\}$. Clairement $\pi_A(n) \approx n^{1/k}$ de sorte que :

1. $\pi_A(n)/n \approx n^{1/k-1} \rightarrow 0$ lorsque $n \rightarrow \infty$,
2. $\pi_A(n)/\pi_A(\lambda n) \rightarrow \lambda^{-1/k} \neq 1$ pour tout $\lambda \neq 1$.

Par conséquent, A n'est pas régulier.

Exemple 2. Soit P l'ensemble des nombres premiers. Il est bien connu que $\pi_P(n) \sim \frac{n}{\log n}$. Ainsi $\pi_P(n)/n \sim \frac{1}{\log n} \rightarrow 0$ lorsque $n \rightarrow \infty$, ce qui satisfait la condition 1. D'autre part :

$$\frac{\pi_P(n)}{\pi_P(\lambda n)} \sim \frac{n \log \lambda n}{\lambda n \log n} = \frac{\log \lambda + \log n}{\lambda \log n} \rightarrow \frac{1}{\lambda} \neq 1 \quad (\text{pour } \lambda \neq 1)$$

Encore une fois, les conditions 1 et 2 sont satisfaites ; par conséquent, P n'est pas régulier.

Exemple 3. Soit B l'ensemble de toutes les puissances de nombres premiers, c'est-à-dire $B = \{p^m \mid p \text{ premier}, m \text{ entier}\}$. Écrivons B sous la forme :

$$B = B_1 \cup B_2 \cup \dots \cup B_k \cup \dots$$

où $B_k = \{p^k \mid p \text{ premier}\}$. Alors pour chaque k nous avons, exactement, $\pi_{B_k}(n) = \pi_P(n^{1/k})$.

Pour calculer $\pi_B(n)$, remarquons d'abord que si $n_0 \in B$, $n_0 < n$; alors pour un seul k et p , $n_0 = p^k < n$, de sorte que :

$$k < \log_p n \leq \log_2 n$$

c'est-à-dire $n_0 \in B_1 \cup \dots \cup B_{\lfloor \log_2 n \rfloor}$. Il s'ensuit que :

$$\pi_B(n) = \pi_{B_1}(n) + \dots + \pi_{B_{\lfloor \log_2 n \rfloor}}(n) = \pi_P(n) + \pi_P(n^{1/2}) + \dots + \pi_P(n^{1/\lfloor \log_2 n \rfloor})$$

Ainsi :

$$\pi_B(n) \sim \frac{n}{\log_e n} + \frac{2n^{1/2}}{\log_e n} + \dots + \frac{\lfloor \log_2 n \rfloor n^{1/\lfloor \log_2 n \rfloor}}{\log_e n}$$

Puisque :

$$2n^{1/2} + \dots + \lfloor \log_2 n \rfloor n^{1/\lfloor \log_2 n \rfloor} < 2(\log_2 n)^2 n^{1/2}$$

et que $\frac{(\log_2 n)^2 n^{1/2}}{\log_e n} \rightarrow 0$ lorsque $n \rightarrow \infty$, nous avons :

$$\pi_B(n) \sim \frac{n}{\log_e n} \sim \pi_P(n)$$

Ainsi, l'ensemble B a la même densité asymptotique que P et n'est pas régulier. Un argument similaire montre que l'ensemble $\{n^m \mid n, m \text{ entiers}, m \geq 2\}$ n'est pas régulier.

Exemple 4. Nous illustrons maintenant l'utilisation du critère dans les cas où le rapport $\pi_A(n)/\pi_A(\lambda n)$ ne converge pas. Soit C l'ensemble des palindromes binaires, c'est-à-dire les séquences invariantes par inversion. Pour montrer que C n'est pas régulier, vérifions d'abord que la condition 1 est satisfaite. C'est facile ; puisque la première moitié des chiffres binaires d'un nombre palindromique à n chiffres est déterminée par la seconde moitié, en négligeant les petits effets de parité, $\pi_C(n)/n \approx (\sqrt{n})/n \rightarrow 0$. Ensuite, d'après la Proposition 1, si C est régulier, il doit être reconnu par un automate possédant un état mort. Mais c'est impossible puisque chaque séquence peut être complétée pour produire un palindrome de deux fois sa longueur.

On pourrait — bien que ce soit insensé dans ce cas — arriver à la même conclusion en utilisant la condition 2'. Pour ce faire, estimons la différence $a_{n+1} - a_n$ entre le n -ième palindrome et le suivant. Si a_n est de longueur paire, $2k$, il peut s'écrire $a_n = b_n 2^k + \tilde{b}_n$, où $\tilde{b}_n$ est la séquence de chiffres de b_n écrits dans l'ordre inverse. Si a_n est de longueur impaire, $2k+1$, il a la forme $a_n = b_n 2^{k+1} + \delta 2^k + \tilde{b}_n$, où δ vaut 0 ou 1. Il est facile de voir que b_{n+1} est soit b_n , soit $b_n + 1$, de sorte que dans chaque cas, $a_{n+1} - a_n$ ne peut pas être plus grand que l'ordre de $\sqrt{a_n}$. Il s'ensuit que $(a_{n+1} - a_n)/a_n \rightarrow 0$ lorsque $n \rightarrow \infty$.

Il est intéressant de comparer cela avec l'ensemble (régulier) de séquences de doublets, c'est-à-dire des séquences comme 00110011110011. Cet ensemble a à peu près le même type de distribution globale que les palindromes ; mais la structure fine de sa distribution d'écarts fait qu'il échappe (à juste titre) au critère.

Les exemples suivants montrent comment le critère peut ne pas fournir d'informations utiles.

Exemple 5. Soit $A(a)$ l'ensemble de toutes les puissances d'un entier fixe a , c'est-à-dire $A(a) = \{a^k \mid a \text{ fixe}\}$. Alors $\log_a(n) - 1 \leq \pi_A(n) < \log_a(n)$ de sorte que $\pi_A(n) \approx \log_a(n)$. La condition 1 est satisfaite. Cependant, $\pi_A(n)/\pi_A(\lambda n) \rightarrow \frac{\log_a n}{\log_a \lambda n} \rightarrow 1$ lorsque $n \rightarrow \infty$, donc la condition 2 échoue, tout comme la condition 2' : $\frac{a_{n+1} - a_n}{a_n} = a - 1$. Le critère ne donne aucune information dans ce cas. En fait, $A(2)$ est régulier (pour une machine binaire), tandis que $A(3)$ ne l'est pas (et vice versa pour une machine ternaire).

Exemple 6. Des séquences périodiques telles que 101, 101101, 101101101, ... ont $\pi(n) \sim k \log n$ de sorte que $\frac{\pi(n)}{\pi(\lambda n)} \rightarrow 1$. La condition 1 échoue. (Tous ces ensembles sont réguliers.)

6. Impossibilité d'une réciproque

Soit A un ensemble régulier infini quelconque avec un complémentaire infini et soit $\phi(x)$ une fonction non calculable prenant les valeurs 0 et 1. Soit A' le sous-ensemble de A défini par : $x \in A'$ si $x \in A$ et $(x+1) \notin A$. L'ensemble A' est infini. Soit $g(n)$ une énumération de A' sans répétitions, et définissons A'' par les conditions :

1. Si $x \in (A - A')$, alors $x \in A''$.
2. Si $x = g(n) \in A'$, alors mettez x dans A'' si $\phi(n) = 0$; sinon mettez $x+1$ dans A'' .

Il est clair que A'' n'est pas calculable, et a fortiori pas régulier ; sinon $\phi(n)$ pourrait être calculé en observant une machine qui reconnaît A'' , puisque $\phi(n) = 0$ si et seulement si $g(n) \in A''$. Mais $\pi_A(n)$ et $\pi_{A''}(n)$ diffèrent d'au plus 1. Ainsi, bien que les tests basés sur la densité asymptotique puissent fournir des indices contre la régularité, ils ne peuvent pas fournir des indices en faveur de la régularité.

7. Borne supérieure du taux de croissance des ensembles réguliers

Par souci d'exhaustivité, le résultat plus superficiel suivant est inclus.

Proposition 5. *Si A est régulier et infini, il existe un certain $K > 0$ tel que $\pi_A(n) > K \log n$.*

Démonstration. Supposons que A soit régulier et que M_A possède N états. Soit N_0 un entier quelconque. Alors il existe un certain $x \in A$ tel que $N_0 \leq L(x) \leq N_0 + N$. Pour voir cela, remarquons d'abord que si $\delta(q_0, y)$ était mort pour chaque y avec $L(y) = N_0$, alors A serait fini. Nous pouvons donc choisir un y avec $L(y) = N_0$ et pour lequel $y \cdot y_1 \in A$ pour un certain y_1 . Mais si y_1 est choisi pour produire le plus court chemin de $\delta(q_0, y)$ à $\delta(q_0, y \cdot y_1)$, alors $L(y_1) < N$. Ainsi $x = y \cdot y_1$ se trouve dans l'intervalle indiqué.

Il s'ensuit qu'il y a au moins un membre de A dans chacun des intervalles

$$(1, 2^N), (2^N, 2^{2N}), \dots, (2^{kN}, 2^{(k+1)N}).$$

Par conséquent, $\pi_A(2^{tN}) \geq t$, et par suite :

$$\pi_A(n) \geq \frac{\log n}{N} = K \log n$$

Exemple 7. Il découle de la Proposition 5 que des ensembles tels que $A = \{2^{t^2}\}$, qui croissent "plus vite qu'exponentiellement", ne peuvent pas être réguliers.

8. Discussion

De nombreuses questions demeurent. Dans quelle mesure le même type de méthodes fonctionnerait-il, disons, sur les machines à piles ? Les critères devront changer dans le détail (par exemple, les palindromes seraient désormais reconnaissables), mais nous sommes portés à supposer que les machines à piles ne parviendront pas non plus à reconnaître les exemples arithmétiquement intéressants, et que les arguments d'écart et de densité peuvent être affinés pour le montrer.

Nous sommes curieux de savoir si l'on peut montrer que $\{n \mid n \text{ est premier}\}$ n'est pas régulier par des moyens beaucoup plus élémentaires. Sinon, cela pourrait suggérer une relation non triviale entre la théorie des automates et des domaines de la théorie des nombres, tels que la théorie des approximations rationnelles.

[Reçu en décembre 1965]

Références

- [1] Rabin M., Scott D., Finite automata and their decision problems. *IBM J. Res. Develop.* 3 (1959), 114-125.

- [2] Kleene S. C., Representation of events in nerve nets and finite automata. In *Automata Studies*, Shannon, C. E., and McCarthy, J. (Eds.), Princeton U. Press, Princeton, N. J., 1956, pp. 3-41.
- [3] Ritchie R. W., Finite automata and the set of squares. *J. ACM* 10, 4 (Oct. 1963), 528-531.