

Automates finis et l'ensemble des carrés

Robert W. Ritchie

Université de Washington, Seattle, Washington

1. Introduction

La classe des ensembles acceptables par des automates finis a été étudiée de manière approfondie dans la littérature récente. Une caractérisation de cette classe en termes d'arithmétique du second ordre faible [1, 2] conjointement avec des résultats d'indécidabilité dans [4] montre que l'ensemble des carrés des entiers non négatifs n'est pas un ensemble acceptable (voir [1, p. 81]).

Une autre caractérisation des ensembles acceptables donnée, par exemple, dans [5] est purement combinatoire et évite l'utilisation de la logique mathématique. Cependant, il n'est pas facile de voir comment tirer des conclusions sur des ensembles théoriques des nombres usuels à partir de cette autre caractérisation.

Cette note procède directement des définitions des automates finis et des ensembles acceptables pour montrer que l'ensemble des carrés n'est pas acceptable. (Le lecteur peut noter que le même argument montre en fait que l'ensemble des carrés impairs n'est également pas acceptable, qu'un argument similaire montrera que l'ensemble des carrés pairs n'est pas acceptable, et que ces résultats peuvent être combinés pour montrer que des ensembles tels que l'ensemble des nombres de la forme $x(x - a)$ pour un a fixe quelconque ne sont pas acceptables.)

Le résultat principal repose sur le lemme de la Section 3 qui met en relation les carrés et les puissances de 2. Ce lemme et la simplicité de sa preuve peuvent présenter un intérêt indépendant puisque des problèmes étroitement liés semblent nécessiter des méthodes beaucoup plus puissantes pour leur solution (voir, par exemple, [3] et [6, Théorème 5]).

2. Préliminaires

Pour plus d'exhaustivité, nous incluons ici les définitions des automates finis et des ensembles acceptables de rubans. Nous suivons [5], et renvoyons le lecteur à cet article pour la motivation. Nous montrons également qu'un ensemble particulier est acceptable, qu'un autre ensemble ne l'est pas, et établissons la clôture de la classe des ensembles acceptables par intersection.

Définition. Étant donné un ensemble fini Σ , nous définissons un automate fini sur Σ comme étant un quadruplet $\mathfrak{A} = (S, M, s_0, F)$, où S est un ensemble fini (non vide) (les états de $\mathfrak{A}$), M est une fonction définie sur $S \times \Sigma$ à valeurs dans S (la fonction de transition de $\mathfrak{A}$), s_0 est un élément de S (l'état initial de $\mathfrak{A}$), et F est un sous-ensemble de S (les états finaux de $\mathfrak{A}$).

Reçu en janvier 1963. Ce travail a été soutenu en partie par la subvention Af SR-62-4 de l'Office of Scientific Research de l'U. S. Air Force.

Soit $\mathfrak{A}$ un automate fini sur Σ , soit T l'ensemble de toutes les chaînes finies de symboles de Σ , et soit Λ la chaîne vide. (Nous appelons T l'ensemble des rubans sur Σ , et incluons Λ dans T). Étendons M à $S \times T$ comme suit :

$$\begin{aligned} M(s, \Lambda) &= s \\ M(s, t\sigma) &= M(M(s, t), \sigma) \end{aligned}$$

pour tout $s \in S$, $t \in T$, $\sigma \in \Sigma$.

Définition. L'ensemble des rubans acceptés par l'automate fini $\mathfrak{A}$ sur Σ est l'ensemble de tous les rubans t dans T tels que $M(s_0, t)$ est dans F . (Un ensemble de rubans sur Σ est dit acceptable s'il existe un automate fini sur Σ qui accepte l'ensemble.)

Montrons maintenant que l'ensemble particulier A de rubans sur $\{0, 1\}$ est acceptable où

$$A = \{1^n 0^m 1 \mid n, m > 0, n + m \text{ est impair}\}.$$

L'automate (S, M, s_0, F) accepte A où $S = \{s_0, s_1, s_2, s_3, s_4, f, n\}$, $F = \{f\}$, et M est décrit par le tableau suivant :

M	s_0	s_1	s_2	s_3	s_4	f	n
0	n	s_3	s_4	s_4	s_3	n	n
1	s_1	s_2	s_1	n	f	n	n

Le lecteur peut facilement vérifier que

1. $M(s_0, t) = s_1$ si et seulement si $t = 1^n$, avec n impair,
2. $M(s_0, t) = s_2$ si et seulement si $t = 1^n$, avec n pair,
3. $M(s_0, t) = s_3$ si et seulement si $t = 1^n 0^m$, avec $n + m$ pair,
4. $M(s_0, t) = s_4$ si et seulement si $t = 1^n 0^m$, avec $n + m$ impair ;

et ainsi que $M(s_0, t) = f$ précisément lorsque t est dans A , comme souhaité.

Montrons maintenant que le sous-ensemble B de A n'est acceptable par aucun automate fini où

$$B = \{1^n 0^{n+1} 1 \mid n > 0\}.$$

Supposons par l'absurde que B soit accepté par l'automate fini $\mathfrak{A}$, et que $\mathfrak{A}$ ait k états. Il doit exister des entiers l et m , $0 \leq l < k$ et $0 < m \leq k$, tels que $M(s_0, 1^l) = M(s_0, 1^{l+m})$. Sinon les $k + 1$ états $M(s_0, 1^0), \dots, M(s_0, 1^k)$ seraient distincts, mais cela est impossible avec seulement k états disponibles. De plus, $M(s, tu) = M(M(s, t), u)$ pour tout s dans S et pour tous t et u dans T par induction sur la définition de M sur $S \times T$. Par conséquent, en particulier $M(s_0, 1^l 0^{l+1} 1) = M(M(s_0, 1^l), 0^{l+1} 1) = M(M(s_0, 1^{l+m}), 0^{l+1} 1) = M(s_0, 1^{l+m} 0^{l+1} 1)$. Puisque le ruban $1^l 0^{l+1} 1$ est accepté par $\mathfrak{A}$, il en va de même pour $1^{l+m} 0^{l+1} 1$, mais cela contredit l'hypothèse selon laquelle $\mathfrak{A}$ accepte précisément l'ensemble B .

Le dernier résultat préliminaire nécessaire est la clôture par intersection de la classe de tous les ensembles acceptables de rubans sur Σ . La preuve présentée ici est celle de [5, Théorème 6]. Soient

$\mathfrak{A} = (S, M, s_0, F)$ et $\mathfrak{B} = (S', M', s'_0, F')$ deux automates finis quelconques sur Σ . Considérons l'automate fini $\mathfrak{C} = (S \times S', N, (s_0, s'_0), F \times F')$ où $N((s, s'), \sigma) = (M(s, \sigma), M'(s', \sigma))$ pour tous s dans S , s' dans S' , et σ dans Σ . Alors $N((s_0, s'_0), t)$ est dans $F \times F'$ si et seulement si $M(s_0, t)$ est dans F et $M'(s'_0, t)$ est dans F' par une induction immédiate sur la longueur de t . Ainsi t est accepté par $\mathfrak{C}$ si et seulement s'il est accepté à la fois par $\mathfrak{A}$ et $\mathfrak{B}$. Par conséquent, $\mathfrak{C}$ accepte l'intersection des ensembles acceptés par $\mathfrak{A}$ et $\mathfrak{B}$ comme il fallait le démontrer.

3. Inacceptabilité de l'ensemble des carrés

Avant de pouvoir parler d'acceptation d'ensembles de nombres, nous devons choisir un codage des nombres en rubans sur un certain ensemble fini. Nous suivons la convention standard consistant à identifier un nombre avec son codage binaire sur l'ensemble $\{0, 1\}$. Pour rendre cette identification non ambiguë, spécifions que zéro est identifié au symbole 0 et que chaque entier positif est identifié à son codage binaire unique dont le symbole le plus à gauche est 1. Chaque entier non négatif est désormais identifié à une seule chaîne sur l'alphabet $\{0, 1\}$, et nous parlerons d'acceptabilité d'un ensemble de nombres (non négatifs) en entendant simplement l'acceptabilité de cet ensemble de chaînes.

Ayant adopté cette convention, nous pouvons interpréter les résultats de la section précédente comme suit. L'ensemble A de tous les nombres de la forme $(2^n - 1)2^l + 1$ où $n + l$ est pair est acceptable, tandis que le sous-ensemble B de A constitué de tous ces nombres de la forme $(2^n - 1)2^{n+2} + 1$ n'est pas acceptable ($n > 0$ et $l = m + 1 > 1$). Ce dernier ensemble est un ensemble de carrés, à savoir $B = \{(2^{n+1} - 1)^2 \mid n > 0\} = \{3^2, 7^2, 15^2, \dots\}$. Pour montrer que l'ensemble S de tous les carrés n'est pas acceptable, nous allons simplement montrer que B est l'intersection de S et A et faire appel à la clôture des ensembles acceptables par intersection.

Lemme 1. *Si $y^2 = (2^n - 1)2^l + 1$ avec y, n et l positifs et $n + l$ pair, alors $l = n + 2$ et $y = 2^{n+1} - 1$.*

Démonstration. Observons d'abord qu'exactlyement l'un de $y - 1$ et $y + 1$ est divisible par 2^{l-1} ; comme ils sont pairs, ils ne peuvent pas tous deux être divisibles par 4, et $(y - 1)(y + 1) = 2^l(2^n - 1)$. Puisque alors $y \pm 1 = 2^{l-1}q$ avec q impair, nous avons $(2^{l-1}q)(2^{l-1}q \pm 2) = 2^l(2^n - 1)$ et ainsi $q(2^{l-2}q \pm 1) = 2^n - 1$; donc $n \geq l - 2$. Avec n au moins aussi grand que $l - 2$, toute solution y de $y^2 = 2^{n+l} - 2^l + 1$ est légèrement inférieure à $2^{(n+l)/2}$ (puisque 2^{n+l} domine $2^l - 1$). Un calcul de routine montre en fait que $y = 2^{(l+n)/2} - 1$ est une solution si et seulement si $n = l - 2$, tandis que si $n > l - 2$ nous avons $(2^{(l+n)/2} - 1)^2 < (2^n - 1)2^l + 1 < (2^{(n+l)/2})^2$.

Ainsi, il n'y a pas de solution entière à moins que $l = n + 2$, ce qui devait être démontré. $\square$

Théorème 2. *L'ensemble de tous les carrés (non négatifs) n'est acceptable par aucun automate fini.*

Démonstration. L'intersection d'ensembles acceptables est à nouveau acceptable, et A est un ensemble acceptable. Mais le lemme montre que l'ensemble B est l'intersection de A avec l'ensemble S de tous les carrés. Puisque B n'est pas acceptable, S ne l'est pas non plus. $\square$

Remerciements. L'auteur tient à remercier le professeur D. L. Kreider du Dartmouth College et M. Robert Strichartz, étudiant à Dartmouth, pour les discussions préliminaires qui ont donné lieu à ce résultat.

Références

1. Büchi J. R., Weak second-order arithmetic and finite automata. *Zeit. Math. Logik und Grundlagen d. Math.*, 6 (1960), 66-92.
2. Elgot C. C., Decision problems of finite automata design and related arithmetics. *Trans. Amer. Math. Soc.* 98 (1961), 21-51.
3. Mordell L. J., The diophantine equation $2^a = x^2 + 7$. *Ark. Mat.* 4 (1962), 455-60.
4. Putnam H., Decidability and essential undecidability. *J. Symbolic Logic* 22 (1957), 39-54.
5. Rabin M., Scott D., Finite automata and their decision problems. *IBM J. Res. Develop.* 3 (1959), 114-25.
6. Shapiro H. S., Slotnick D. L., On the mathematical theory of error correcting codes. *IBM J. Res. Develop.* 3 (1959), 25-34.