

Le problème de la réalisation minimale dans le demi-anneau max-plus et le problème de Pisot sont NP-durs *

Vincent D. BLONDEL ^a, Natacha PORTIER ^b

^a Mathématiques appliquées, Université catholique de Louvain, avenue Georges Lemaître, 4, B-1348 Louvain-la-Neuve, Belgique

^b Laboratoire de l'informatique du parallélisme, École normale supérieure de Lyon, 46, allée d'Italie, 69364 Lyon cedex 07, France
Courriel : blondel@inma.ucl.ac.be; Natacha.Portier@ens-lyon.fr

(Reçu le 9 octobre 2000, accepté après révision le 5 novembre 2001)

Résumé. Nous montrons que deux problèmes sont NP-durs. Le premier est le problème bien connu de la réalisation minimale dans le demi-anneau max-plus. Le second problème, le problème de Pisot, consiste à savoir si une suite récurrente linéaire d'entiers a un zéro. © 2001 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

The minimal realization problem in the max-plus semiring and Pisot's problem are NP-hard

Abstract. We prove the NP-hardness of two problems. The first is the well-known minimal realization problem in the max-plus semiring. The second problem (Pisot's problem) is the problem of determining if a given integer linear recurrent sequence has a zero coefficient. © 2001 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

1. Introduction et définitions

Commençons par rappeler quelques définitions :

DÉFINITION. – La structure $(K, +, \times)$ est un *demi-anneau* si les deux opérations binaires $+$ et \times sont associatives, ont des éléments neutres, si $+$ est commutative, si le neutre de $+$ est absorbant pour \times et si \times est distributive par rapport à $+$.

Dans la suite, nous nous intéressons plus particulièrement au demi-anneau $(\mathbb{N} \cup \{-\infty\}, \max, +)$, que nous appelons demi-anneau max-plus.

Les demi-anneaux avec deux éléments seulement sont au nombre de deux. Le premier est un corps ; si nous notons par 0 et 1 les éléments neutres respectifs de $+$ et \times , nous avons $1 + 1 = 0$. Si nous imposons $1 + 1 = 1$, nous obtenons l'algèbre de Boole à deux éléments :

NOTATION. – L'algèbre de Boole B est le demi-anneau $(\{\bar{0}, \bar{1}\}, \vee, \wedge)$.

Note présentée par Etienne GHYS.

DÉFINITION. – Un *automate non-déterministe* sur l’alphabet $\Sigma = \{x\}$, à n états, où n est un entier naturel, est un ensemble de trois matrices à coefficients dans B : la matrice ligne b , la matrice carrée A et la matrice colonne c , toutes trois de dimension n . Si p est un entier naturel, le mot x^p est accepté par l’automate si et seulement si $bA^p c$ est égal à $\bar{1}$. Le *langage reconnu* par l’automate est l’ensemble des mots acceptés.

Cette notion se généralise à un demi-anneau quelconque :

DÉFINITIONS. – Soit $(K, +, \times)$ un demi-anneau. Une série sur l’alphabet $\Sigma = \{x\}$ et à coefficients dans K est une fonction de Σ^* dans K . Si p est un entier naturel, l’image de x^p est appelé son coefficient dans la série.

La série est *rationnelle* s’il existe un ensemble de trois matrices à coefficients dans K , la matrice ligne b , la matrice carrée A et la matrice colonne c , toutes trois de même dimension, et telles que si p est un entier naturel, le coefficient dans la série de x^p soit $bA^p c$. Le triplet est une *représentation linéaire* de la série, et sa dimension est la dimension commune des matrices.

Les représentations linéaires sont aussi appelées des K -automates. Si K est l’algèbre de Boole B nous retrouvons les automates non-déterministes.

Sur un alphabet à plusieurs lettres, on peut associer à chaque lettre une matrice carrée et définir des K -automates et des séries rationnelles sur plusieurs lettres.

DÉFINITION. – Le *problème de la minimisation* est le suivant : étant donnée une représentation linéaire d’une série rationnelle et un entier naturel N , la série a-t-elle une représentation linéaire de dimension au plus N ?

Nous nous intéressons au cas où les coefficients sont dans le demi-anneau max-plus. Une classe particulière de systèmes à événements discrets se décrit très naturellement par des systèmes linéaires sur le demi-anneau max-plus [1]. Dans le contexte de ces systèmes, le problème de la réalisation minimale est l’exacte transcription du problème fondamental d’identification. On cherche la plus petite dimension possible d’un système donnant lieu à une sortie donnée. Pour cette raison, le problème de la réalisation minimale dans le demi-anneau max-plus a donné lieu à de nombreux travaux [4,5,9–11]. Il reste néanmoins irrésolu. Nous montrons qu’il est *NP-dur*. Pour cela, nous utilisons un théorème de L.J. Stockmeyer et A.R. Meyer sur les expressions rationnelles [12].

DÉFINITION. – Les *expressions rationnelles* sur Σ sont définies par induction et chacune représente un langage, c’est-à-dire un sous-ensemble de Σ^* :

- Le mot vide ε et x sont des expressions rationnelles, et représentent respectivement les langages $\{\varepsilon\}$ et $\{x\}$.
- Si E_1 et E_2 sont des expressions rationnelles qui représentent les langages L_1 et L_2 , alors $E_1 \cup E_2$, $E_1.E_2$ et E_1^* , sont des expressions rationnelles et représentent les langages $L \cup L_2$, $L_1.L_2$ et $L_1^* = \{\varepsilon\} \cup L_1 \cup L_1.L_1 \cup L_1.L_1.L_1 \cup \dots$.

DÉFINITION. – La *taille* d’une expression rationnelle est le nombre de symboles x et ε qui apparaissent dans l’expression.

Dans [12], L.J. Stockmeyer et A.R. Meyer montrent le théorème suivant :

THÉORÈME 1. – *Savoir si une expression rationnelle sur une lettre représente le même langage que x^* est un problème NP-complet.*

S.C. Kleene a montré que les langages reconnaissables par un automate sont exactement ceux représentés par une expression rationnelle. Le résultat suivant est un corollaire du théorème 1 :

THÉORÈME 2. – *Savoir si un automate non-déterministe sur une seule lettre reconnaît x^* est un problème NP-complet.*

Ce problème est NP [12]. Pour prouver qu'il est NP-dur, nous utilisons le lemme suivant, qui nous montre que ce problème est plus compliqué que dans le cas des expressions rationnelles. Le lemme se montre facilement par induction sur les expressions rationnelles, voir par exemple [13].

LEMME 1. – Soit n un entier naturel et soit E une expression rationnelle sur une lettre de taille n . Il existe un automate non-déterministe de taille au plus $3n$ qui reconnaît le même langage. De plus, nous pouvons le construire en temps polynomialement borné en n .

2. Le problème de la réalisation minimale en max-plus

THÉORÈME 3. – Dans le demi-anneau max-plus, le problème de la minimisation est NP-dur.

Il suffit de montrer que ce problème est déjà NP-dur si nous nous restreignons à déterminer s'il existe une représentation de dimension un, et à des matrices à coefficients dans $\{0, -\infty\}$. En effet, nous pouvons montrer que si une série de $\{0, -\infty\}$ a une représentation linéaire, elle en a une de même taille à coefficients dans $\{0, -\infty\}$. En identifiant $(\{0, -\infty\}, \max, +)$ et l'algèbre de Boole $B = (\{\bar{0}, \bar{1}\}, \vee, \wedge)$ en posant $\bar{0} = -\infty$ et $\bar{1} = 0$, nous nous ramenons au problème de savoir si un automate reconnaît le même langage qu'un automate à un seul état.

Or un automate à un état reconnaît soit l'ensemble vide, soit le mot vide, soit x^* tout entier. Il est facile de savoir si un automate reconnaît l'ensemble vide ou le mot vide : il suffit de savoir s'il y a un état d'arrivée dans la composante connexe d'un état de départ. Nous sommes donc ramenés au théorème 2 et le théorème 3 est prouvé.

Nous pouvons en déduire que le problème de savoir si deux séries rationnelles à coefficients dans le demi-anneau max-plus sur une lettre sont différentes est NP-dur. D. Krob a montré [8] que ce problème avec deux lettres est indécidable, et il a montré avec M. Kanta [7] que ce problème est décidable sur une lettre.

3. Le problème de Pisot

Soit G un automate non-déterministe sur une seule lettre avec n états, où n est un entier naturel. Jusqu'à présent, nous avons considéré un automate comme un triplet de matrices à coefficients dans l'algèbre de Boole. Mais nous pouvons aussi voir les coefficients des matrices comme des éléments du sous-ensemble $\{0, 1\}$ de $(\mathbf{Z}, +, \times)$. Pour tout entier naturel p , l'automate G accepte x^p si et seulement si $bA^p c$ n'est pas nul, c'est-à-dire est un entier strictement positif. Nous en déduisons le :

THÉORÈME 4. – Le problème de savoir pour un entier naturel n et des éléments b de $\mathbf{Z}^{1 \times n}$, A de $\mathbf{Z}^{n \times n}$ et c de $\mathbf{Z}^{n \times 1}$ s'il existe un entier naturel p tel que $bA^p c = 0$ est NP-dur.

Considérons une suite récurrente linéaire ; c'est une suite $(u_n)_{n \in \mathbf{N}}$ d'entiers pour laquelle il existe un entier naturel h non nul et des entiers a_0, \dots, a_{h-1} tels que pour tout entier naturel n nous ayons $u_{n+h} = a_{h-1}u_{n+h-1} + \dots + a_0 u_n$. Le théorème de Skolem nous dit que l'ensemble des indices pour lesquels la suite s'annule est une union finie de progressions arithmétiques, et J. Berstel et M. Mignotte ont montré [2] que savoir si cet ensemble est fini ou infini est décidable. Cet ensemble est-il vide ? C'est le problème de Pisot ([3], p. 84). Nous ne savons pas s'il est décidable (voir [11] pour un commentaire sur la difficulté probable du problème).

THÉORÈME 5. – Le problème de Pisot est NP-dur.

Pour le prouver, nous montrons que c'est un problème équivalent à celui du théorème 4. Soient h un entier naturel et des éléments b de $\mathbf{N}^{1 \times h}$, A de $\mathbf{N}^{h \times h}$ et c de $\mathbf{N}^{h \times 1}$. Il existe des entiers a_{h-1}, \dots, a_0 tels que le polynôme caractéristique $p(s)$ de A soit égal à $s^h - a_{h-1}s^{h-1} - \dots - a_0$. Le théorème de Cayley-Hamilton nous prouve que $p(A)$ est nul. Si n est un entier naturel, en multipliant à gauche par bA^n , à droite

par c et en posant pour tout i entier naturel $\gamma_i = bA^i c$ nous obtenons la relation de récurrence suivante :

$$\gamma_{n+h} = a_{h-1}\gamma_{n+h-1} + \dots + a_0\gamma_n.$$

Comme le calcul de $p(s)$ est le calcul du déterminant $\det(sI_h - A)$, il peut être fait en temps polynomial, ce qui nous permet de conclure.

Réciproquement, soient un entier naturel non nul h , des entiers a_0, \dots, a_{h-1} et $(u_n)_{n \in \mathbf{N}}$ une suite d'entiers définie par la relation de récurrence : $u_{n+h} = a_{h-1}u_{n+h-1} + \dots + a_0u_n$ pour tout entier naturel n . Nous écrivons cette relation sous forme matricielle : pour tout entier naturel n , les lignes du vecteur colonne U_n sont u_{n+h-1}, \dots, u_n . Soit A la matrice carrée d'ordre n définie de la manière suivante : sa première ligne est $a_{h-1} \dots a_0$, il y a des 1 sous la diagonale principale, et tous les autres éléments sont nuls. Soit c le vecteur ligne de dimension n dont le dernier élément est égal à 1 et tous les autres à 0. Pour tout entier naturel n , nous avons l'égalité $u_n = cA^n U_0$, ce qui nous ramène au problème du théorème 4.

* Travail financé par la communauté européenne à travers le réseau de recherche ALAPEDES, the « Algebraic Approach to Performance Evaluation of Discrete Event Systems », contrat RB-FMRX-CT-96-0074.

Références bibliographiques

- [1] Baccelli F., Cohen G., Olsder G., Quadrat J.-P., Synchronization and Linearity. An Algebra for Discrete Event Systems, Wiley Ser. Probab. Math. Statist. Probab. Math. Statist., Wiley, Chichester, 1992.
- [2] Berstel J., Mignotte M., Deux propriétés décidables des suites récurrentes linéaires, Bull. Soc. Math. France 104 (2) (1976) 175–184.
- [3] Berstel J., Reutenauer C., Les séries rationnelles et leurs langages, Masson, Paris, 1984.
- [4] De Schutter B., De Moor B., Minimal realization in the max plus algebra is an extended linear complementary problem, Systems Control Lett. 25 (2) (1995) 103–111.
- [5] Gaubert S., On rational series in one variable over certain dioids, Technical report 2162, INRIA, 1994.
- [6] Gaubert S., Dutkovič P., Cuninghame-Green R., Minimal (max, +) realization of convex sequences, SIAM J. Control Optim. 36 (1) (1998).
- [7] Kanta M., Krob D., One-letter rational series with multiplicities in the tropical semiring: an algorithmic approach, Prépublication du LIAFA, Université Paris-7, 1997.
- [8] Krob D., The equality problem for rational series in the tropical semiring is undecidable, Internat. J. Algebra Comput. 3 (1994) 405–425.
- [9] Olsder G.-J., De Schutter B., de Vries R., The minimal state space realization problem in the max-plus algebra: An overview, Technical report 97-107, ESAT-SISTA, 1997.
- [10] Olsder G.-J., De Schutter B., The minimal realization problem in the max-plus algebra, in: Blondel V., Sontag E., Vidyasagar M., Willems J. (Eds.), Open Problems in Mathematical Systems and Control Theory, Springer, London, 1999.
- [11] Salomaa A., Soittola M., Automata-Theoretic Aspects of Formal Power Series, Springer, New York, 1978.
- [12] Stockmeyer L.J., Meyer A.R., Word problems requiring exponential time: preliminary report, in: Fifth Annual ACM Symposium on Theory of Computing, Assoc. Comput. Mach., New York, 1973.
- [13] Wolper P., Introduction à la calculabilité, InterEditions, Paris, 1991.