INFORMATIQUE THÉORIQUE ET APPLICATIONS

MARIANNE MAKSIMENKO

Algorithme quadratique de calcul de la solution générale d'équations en mots à une variable

Informatique théorique et applications, tome 29, n° 4 (1995), p. 277-284

<http://www.numdam.org/item?id=ITA_1995__29_4_277_0>

© AFCET, 1995, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques

http://www.numdam.org/

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 29, n° 4, 1995, p. 277 à 284)

ALGORITHME QUADRATIQUE DE CALCUL DE LA SOLUTION GÉNÉRALE D'ÉQUATIONS EN MOTS À UNE VARIABLE (*)

par Marianne MAKSIMENKO ([1])

Communiqué par C. CHOFFRUT

Résumé. – *Nous proposons dans cet article un algorithme qui trouve toutes les solutions d'équations à une variable dans le monoïde libre avec une complexité quadratique.*

Abstract. – *In this paper we propose an algorithm computing all the solutions of word equations in one variable with quadratic complexity.*

1. INTRODUCTION

A. A. Markov (*voir* [5]) a commencé le premier à étudier les équations en mots. Il a prouvé la décidabilité de l'équation en mots à deux variables en 1954.

En 1971, J. I. Khmelevskiï (*voir* [4]) a prouvé la décidabilité de l'équation en mots à trois variable et a construit un algorithme qui cherche la solution générale de l'équation en mots à deux variables. En étudiant ces problèmes, il a indiqué la forme des solutions possibles d'équations à une variable et a montré que si une telle équation a une solution, elle doit avoir une solution de *longueur* inférieure ou égale à M, où M est une caractéristique de l'équation, calculée effectivement à partir de celle-ci. En considérant tous les mots de longueur inférieure à M, on peut décider s'il existe ou non une solution.

En 1992, W. Charatonic et L. Pacholski (*voir* [1]) ont posé le problème des algorithmes « rapides », en soulignant que la plupart des algorithmes contemporains ne peuvent s'appliquer en pratique à cause de leur complexité. Ils ont prouvé que la tâche qui consiste à trouver toutes les solutions d'une

(*) Reçu le 30 juillet 1993, accepté le 15 juillet 1994.
([1]) LIR, INSA de Rouen, B.P. 08, 76131 Mont-Saint-Aignan Cedex.

0988-3754/95/04/$ 4.00/© AFCET-Gauthier-Villars

équation à deux variables peut être résolue en temps polynomial (en ayant construit un algorithme). Ils n'ont pas considéré spécialement le cas d'une seule variable, mais ils ont rappelé les résultats de J. I. Khmelevskiï, dont ils avaient besoin dans leur travail. Ils ont aussi montré qu'à l'aide de cet algorithme on peut construire un algorithme calculant toutes les solutions d'équations à une variable en temps $O(\mathbf{l}^5)$, où $\mathbf{l}$ est la longueur de l'équation.

Ici nous proposons un algorithme qui trouve toutes les solutions d'équations à une variable avec une complexité quadratique. La recherche d'un algorithme optimal est un problème ouvert.

2. PRÉLIMINAIRES

Rappelons seulement les définitions les plus importantes et ajoutons-en quelques unes.

Soit $\mathbf{C} = \{a_1, a_2, \ldots, a_p\}$ un alphabet fini des constantes, soit $\mathbf{x}$ une variable.

Une équation à une variable dans le monoïde libre a la forme suivante :

$$\mathbf{z}_1(\mathbf{x}, a_1, a_2, \ldots, a_p) = \mathbf{z}_2(\mathbf{x}, a_1, a_2, \ldots, a_p), \tag{1}$$

où $\mathbf{z}_1$, $\mathbf{z}_2$ sont des mots de l'alphabet $\mathbf{C} \cup \{\mathbf{x}\}$.

On appelle *longueur* d'une équation de la forme (1) l'entier $\mathbf{l}$ défini comme suit : $|\mathbf{z}_1(\mathbf{x}, a_1, a_2, \ldots, a_n| + |\mathbf{z}_2(\mathbf{x}, a_1, a_2, \ldots, a_n)|$.

Lorsque la substitution de chaque $\mathbf{x}$ apparaissant dans l'équation par le mot $\mathbf{X} \in \mathbf{C}^*$ permet aux deux membres de l'équation d'être identiques, on appelle $\mathbf{X}$ *solution* de l'équation.

On appelle *longueur* de la solution $\mathbf{X}$ le nombre $|\mathbf{X}|$.

Une description de toutes les solutions sur l'alphabet $\mathbf{C}$ s'appelle *solution générale* de l'équation à une variable.

On dit qu'une équation est :

* *triviale* si ses deux membres sont mots vides;

* *réduite* si les premières lettres de ses membres sont différentes;

* *contradictoire* si les premières lettres ou les dernières lettres de ses membres sont différentes et appartiennent à l'alphabet $\mathbf{C}$.

J. I. Khmelevskiï ne considère que des équations non triviales, réduites et non contradictoires. Voilà pourquoi l'équation (1) peut s'écrire sous la forme

$$\mathbf{A}(\mathbf{x}\,\mathbf{A}_i)_{i=1}^n = (\mathbf{x}\,\mathbf{B}_i)_{i=1}^m, \tag{2}$$

où $\mathbf{A}$, $\mathbf{A}_i$, $\mathbf{B}_i$ sont des mots de l'alphabet $\mathbf{C}$, où $\mathbf{A} \neq \varepsilon$. Il est évident, qu'on peut réduire une équation (1) en temps linéaire et tester en $O(1)$, si elle est triviale ou contradictoire.

J. I. Khmelevskiĭ a aussi donné une formule explicite pour décrire toutes les solutions, en prouvant que chaque solution à la forme $\mathbf{A}^L \mathbf{B}$, où $\mathbf{L}$ est un entier et le mot $\mathbf{B}$ est un préfixe quelconque du mot $\mathbf{A}$. Il s'agit donc d'énumérer tous les mots de la forme $\mathbf{A}^L \mathbf{B}$, car la longueur du mot $\mathbf{A}^L \mathbf{B}$ est inférieure ou égale à $\mathbf{M}$, où $\mathbf{M}$ est le nombre calculé à partir de l'équation. De ce fait, si la solution existe, elle doit exister obligatoirement parmi un ensemble fini des mots (*voir* [4], 1.19).

On dit que le mot u est une *puissance* du mot v si u est égal à n concaténations du mot v, où $n > 1$. Notons cela $u = v^n$.

À l'inverse, le mot v est *racine* du mot u s'il existe un nombre $n \geq 1$, tel que $u = v^n$ et v est le plus court facteur ayant cette propriété.

Le mot u est dit *primitif* s'il n'est pas une puissance.

Deux mots quelconques qui sont de la forme uv et vu, sont dits *conjugués*.

Dire que λ est une *période* du mot $f = a_1 \dots a_n$ revient à dire que f est de la forme $(uv)^n u$ avec $|uv| = \lambda$ et $n \geq 0$, ou, de façon équivalente (*voir* [2], chapitre 1, § 1) :

$$f \text{ est de la forme } f = f' g = g f'' \qquad \text{avec} \quad |f'| = |f''| = \lambda. \tag{3}$$

LEMME DE LA COMMUTATION : *Si u et w sont deux mots primitifs, conjugués,* (i.e. $u = z_1 z_2$ *et* $w = z_2 z_1$), *alors cette factorisation est unique. (Cela veut dire, qu'il n'existe pas d'autres facteurs z_1 et z_2, ayant les mêmes propriétés.)*

Preuve (par l'absurde) : Soit $u = z_1 z_2 = z_3 z_4$, $w = z_2 z_1 = z_4 z_3$.

Sans restriction à la généralité, on peut supposer que z_3 est plus long que z_1, alors $z_3 = z_1 z_5$, $u = z_1 z_5 z_4 = z_1 z_2$, d'où $z_2 = z_5 z_4$, puis $w = z_5 z_4 z_1 = z_4 z_1 z_5$; on obtient que les deux mots $z_4 z_1$ et z_5 commutent. Comme w est primitif, z_5 est le mot vide (*voir* [2], 1.2'), et $z_3 = z_1$. ♦

Rappelons que n'importe quel conjugué d'un mot primitif est un mot primitif (*voir* [4], 1.8).

Disons que le préfixe d'un mot, qui est en même temps son suffixe, est un *bord*.

Disons que le mot f *se chevauche*, si l'ensemble de tous ses bords contient d'autres mots que f et le mot vide.

Si pour (3) il existe un mot g, qui n'est pas vide et n'est pas égal à f, (3) est équivalent à dire que le mot f se chevauche.

Notons *préfixe* $(u) \cap$ suffixe (w) l'ensemble de tous les facteurs non vides, qui sont en même temps préfixes de u et suffixes de w. Un algorithme cherchant en temps linéaire le plus long facteur, qui est en même temps préfixe de u et suffixe de w, est donné par Morris et Pratt (*voir* [6]).

J.-P. Duval a reformulé le théorème de Wilf, Fine (*voir* [2], [3]) de la manière suivante : Si un mot X a deux périodes λ et μ, et si $|X| \geq \lambda + \mu - pgcd\,(\lambda,\ \mu)$, alors $k \times pgcd\,(\lambda,\ \mu)$ est aussi une période, où k est n'importe quel nombre naturel.

LEMME (Goralcik) : *On peut tester, pour un mot X quelconque, s'il est une solution de l'équation en temps $O\,(|X|+1)$, où* 1 *est la longueur de l'équation.*

Preuve : Notons U et V les deux mots résultants de la substitution de x par X dans les deux membres $\mathbf{z_1}$ et $\mathbf{z_2}$ de (1). $|U| = O\,(|X| \times 1)$, ce qui donne le temps des comparaison naïves de U et V sur toutes les positions. Pour faire mieux, définissons les ensembles de *délais* de X dans U et V par

$$\mathrm{Del}\,(\mathbf{z}_1,\ X) = \{|\mathbf{A}\mathbf{A}_1 \ldots \mathbf{A_k}| + k|X|;\ 0 \leq k \leq n\}$$
$$\mathrm{Del}\,(\mathbf{z}_2,\ X) = \{|\mathbf{B}_1 \ldots \mathbf{B_k}| + k|X|;\ 1 \leq k \leq m\}$$

et appelons *X-position* de U (resp. de V) tout entier k tel que

$$i + 1 \quad \leq \quad k \quad \leq \quad i + |X|$$

pour un délai $i \in \mathrm{Del}\,(\mathbf{z_1},\ X)$ (resp. $i \in \mathrm{Del}\,(\mathbf{z_2},\ X)$) pour l'équation donnée dans la forme (2).

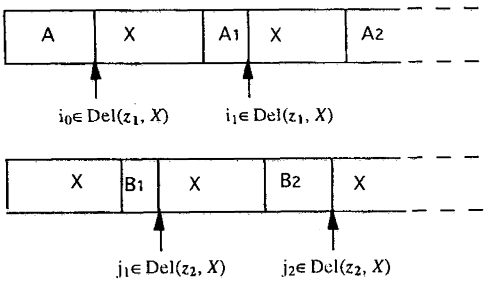

Figure 1.

Les X-positions communes de U et V sont réparties en au plus $n+m-1$ intervalles $\mathbf{I_{ij}} = [\max(i, j)+1, \min(i, j)+|X|]$, déterminés chacun par un couple de délais $i \in \mathrm{Del}(\mathbf{z_1}, X)$ et $j \in \mathrm{Del}(\mathbf{z_2}, X)$, tel que $|i-j| < |X|$. Les mots U et V s'accordent sur $\mathbf{I_{ij}}$ ssi $|i-j|$ est une période de X, cela se vérifie en $O(1)$ si l'on dispose de l'ensemble de périodes de X, donc en $O(n+m)$ pour tous les $\mathbf{I_{ij}}$ avec $|i-j| < |X|$. Il reste alors au plus $|\mathbf{A}\mathbf{A_1} \ldots \mathbf{A_n}\mathbf{B_1} \ldots \mathbf{B_m}|$ positions sur lesquelles il faut comparer U et V, ce qui donne un temps $O(1)$ pour tester si $U = V$ ou non, à condition que l'on connaisse les périodes de X. Mais ces dernières se calculent en $O(|X|)$ (par Morris et Pratt), donc la complexité en temps est $O(|X|+1)$. ♦

3. CALCUL DES SOLUTIONS

Si une équation n'est pas triviale ou contradictoire au début, elle a une des deux formes suivantes obtenues après la réduction des suffixes et préfixes communs :

$$u_1\, x u_2\, x \ldots u_{r1}\, x = x w_1\, x w_2 \ldots x w_{r2} \tag{4}$$

$$u_1\, x u_2\, x \ldots u_{r1}\, x u_{r1+1} = x w_1\, x w_2 \ldots x w_{r2-1}\, x, \tag{5}$$

où u_1 n'est pas vide et w_{r2} n'est pas vide dans (4) et u_{r1+1} n'est pas vide dans (5).

Soit $v = w_{r2}$ dans le cas (4), soit $v = u_{r1+1}$ dans le cas (5).

Soient $u = \mathrm{racine}(u_1)$, $w = \mathrm{racine}(v)$. Ces mots jouent un rôle très important, ils définissent des composants de la forme de solution.

On dit que la solution X est *courte* si $|X| < |u| + |w|$, *longue* sinon.

LEMME 1 (Condition nécessaire sur les solutions longues) : *Si une solution longue existe, alors u et w sont conjugués.*

Preuve : J. I. Khmelevskiĭ a montré, que $X = (s_1\, s_2)^s\, s_1$, où $u_1 = s_1\, s_2$. Il est évident, que $X = (z_1\, z_2)^n\, z_1$, où $u = z_1\, z_2$. En raisonnant d'une manière analogue à partir de la fin de X, on a toujours

$$X = z_3\,(z_4\, z_3)^m = (z_3\, z_4)^m\, z_3, \qquad \text{où} \qquad w = z_4\, z_3.$$

Comme X a des périodes $|u|$, $|w|$,

$$|X| \geq |u| + |w| \geq |u| + |w| - pgcd(|u|, |w|),$$

les conditions du théorème Wilf et Fine sont satisfaites, alors $pgcd(|u|, |w|)$ est une période. Si $s = |u|/pgcd(|u|, |w|)$, alors u est égal à son préfixe de la longueur $pgcd(|u|, |w|)$ à la puissance s. Mais u est primitif, donc $s = 1$ et $|u| = pgcd(|u|, |w|)$. D'une manière analogue on prouve que $|w| = pgcd(|u|, |w|)$, d'où $|u| = |w|$ et $u = z_3 z_4$, $z_1 = z_3$, donc, $w = z_2 z_1$. ♦

LEMME 2 : *Si une solution longue existe, alors* X *est de la forme* $(z_1, z_2)^n z_1$, *où* $u = z_1 z_2$ et z_1 *est défini d'une façon unique.*

Preuve : Suite au lemme 1, u et w sont conjugués. Comme u et w sont des mots primitifs, par le lemme de la commutation, la factorisation $u = z_1 z_2$, tel que $w = z_2 z_1$, est unique. Donc,

$$X = (z_1 z_2)^n z_1, \tag{6}$$

où z_1, est défini d'une façon unique. ♦

THÉORÈME 1 : *On peut trouver toutes les solutions longues ou tester si elles n'existent pas en temps quadratique.*

Preuve : Trouvons d'abord u et w, et vérifions s'ils sont conjugués. On peut le faire en temps linéaire de l'algorithme de Morris et Prat (*voir* [6]), car le plus long bord de uw coïncide avec z_1.

Si u et w ne sont pas conjugués, suite au lemme 1, il n'y a pas de solution longue. S'ils sont conjugués, chaque solution longue est de la forme $(z_1 z_2)^n z_1$ où z_1 est défini d'une façon unique (lemme 2) et peut être calculé en temps linéaire en testant la conjugaison de u et w.

Deux cas se présentent pour les solutions longues.

Cas 1. $r_1 \neq r_2$ (*i.e.* le nombre d'occurrences de x à gauche et à droite diffèrent).

La longueur d'une éventuelle solution X est déterminée par :

$$\begin{aligned}|X| = ((|u_1| + |u_2| + \cdots + |u_{r1}| + |u_{r1+1}|)\\ - (|w_1| + |w_2| + \cdots + |w_{r2}| + |w_{r2+1}|))/(r_2 - r_1).\end{aligned} \tag{7}$$

D'autre part, X est de la forme (6). On peut alors calculer immédiatement n en fonction de $|X|$ et $|u|$ et vérifier en temps linéaire (par le lemme de Goralcik), si X est effectivement une solution.

Cas 2. $r_1 = r_2$.

Nous employons ici une reformulation du théorème de J. I. Khmelevskiï (*voir* [4], 1.18), que voici :

THÉORÈME (Khmelevskiï) : *Soit* $\kappa = d/|C|+1$, *où* d *est un nombre calculé à l'aide de la formule donnée, tel que* $d \leq 1$, *où* 1 *est la longueur de l'équation et* $C \in \mathbf{C}^*$ *est un mot quelconque.*

Si $X = C^{\lambda} B$ est une solution de l'équation (2), où B est un préfixe propre de C et λ est un nombre tel que $\lambda \geq \kappa$, alors $\forall\, \mu \geq 0$ $C^{\mu} B$ est aussi une solution de l'équation (2). ♦

Suite au théorème de Khmelevskiï, nous pouvons vérifier, si tous les mots de cette forme sont des solutions. Vérifions cela pour $X_0 = (z_1 z_2)^{\kappa} z_1$. Comme

$$\begin{aligned} |(z_1 z_2)^{\kappa} z_1| &\leq \kappa\, |z_1 z_2| + |z_1| < |(\kappa + 1)\, |u| \\ &= (d/|u| + 2)|u| = d + 2\, |u|) < 3 1, \end{aligned}$$

où 1 est la longueur de l'équation, la longueur de X_0 est proportionnelle à 1; la substitution peut alors s'effectuer en temps linéaire suite au lemme de Goralcik.

Si X_0 est une solution, concluons que tous les mots de la forme $(z_1 z_2)^n z_1$ sont des solutions. Sinon, des solutions longues isolées X de la forme $(z_1 z_2)^{\lambda} z_1$ où $\lambda < \kappa$, peuvent avoir lieu. Chaque X a une longueur inférieure à celle de X_0, donc linéaire en 1.

La substitution de chaque X peut donc être faite en temps linéaire grâce au lemme de Goralcik. Le nombre de X étant proportionnel à la longueur de $(z_1 z_2)^n z_1$, il est proportionnel à 1, donc la complexité temporelle est quadratique. ♦

THÉORÈME 2 : *On peut trouver toutes les solutions courtes ou tester si elles n'extistent pas en temps quadratique.*

Preuve : Cas 1. $X \leq \min(|u|, |w|)$.

Il suffit de remplacer x par chaque mot de l'ensemble *préfixe* $(u) \cap$ *suffixe* (w).

Suite au lemme de Goralcik on peut tester si X est une solution de l'équation en temps $O(|X| + 1)$, où 1 est la longueur de l'équation. Mais ici la longueur de X est proportionnelle à 1, donc on peut le tester en temps $O(\mathbf{1})$.

Le cardinal de l'ensemble *préfixe* $(u) \cap$ *suffixe* (w) est proportionnel à la longueur de l'équation, et la substitution peut être réalisée en temps proportionnel à la longueur de l'équation, alors la complexité temporelle est quadratique.

Cas 2. $X > \min(|u|, |w|)$.

Quand $|u| \geq |w|$, X est de la forme $z_1 z_2 z_1$, où $u = z_1 z_2$, car $|X| < |u| + |w| < 2|u|$. On peut trouver alors toutes ces solutions en substituant tous les X de la forme $z_1 z_2 z_1$ dans l'équation. Le nombre de z_1 possibles est proportionnel à u, cela veut dire à l.

Quand $|u| < |w|$, X est de la forme $z_4 z_3 z_4$, où $w = z_3 z_4$, car $|X| < |u| + |w| < 2|w|$. On peut trouver alors toutes ces solutions en substituant tout X de la forme $z_4 z_3 z_4$ dans l'équation. Le nombre de z_4 possibles est proportionnel à w, cela veut dire à l.

Comme ci-dessus, chaque solution peut être testée en temps $O(1)$, alors la complexité temporelle est quadratique. ♦

THÉORÈME 3 : *On peut trouver toutes les solutions de l'équation à une variable ou tester si elles n'existent pas en temps quadratique.*

Preuve : L'équation peut avoir des solutions courtes ou longues. Suite aux théorèmes 1, 2, on peut trouver toutes ses solutions en temps quadratique. Donc, la complexité temporelle est quadratique. ♦

REMERCIEMENTS

Je remercie V. G. Dournev (l'Université de Jaroslavle de Russie), J.-P. Pécuchet, P. Goralcik, H. Abdulrab, J.-P. Duval pour les discussions que j'ai eues avec eux au sujet des idées développées dans cet article.

RÉFÉRENCES

1. W. CHARATONIC et L. PACHOLSKI, Solving Word Equations in Two Variables, *Lecture Notes in Computer Sciences*, IWWERT'91, Proceedings, Springer-verlag, 1991, p. 43-56.
2. J.-P. DUVAL, Contribution à la combinatoire du monoïde libre, Thèse, Université de Rouen, 1980.
3. N. J. FINE et H. S. WILF, Uniqueness Theorem for Periodic Function, *Proc. Am. Math. Soc.*, 1965, *16*.
4. J. I. KHMELEVSKIĬ, Equations in Free Semigroups, *Trudy Mat. Inst. Steklov*, 1971, *107*.
5. A. A. MARKOV, The Theory of Algorithms, *Trudy Mat. Inst. Steklov*, 1954, *42*.
6. J. H. MORRIS et V. R. PRATT, *A Linear Pattern Matching Algorithm*, Technical Report N° 40, Computing Center, University of California, Berkeley, 1970.