

HERMANN K.-G. WALTER

A simple proof of Valiant's lemma

Informatique théorique et applications, tome 20, n° 2 (1986),
p. 183-190

http://www.numdam.org/item?id=ITA_1986__20_2_183_0

© AFCET, 1986, 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/>

A SIMPLE PROOF OF VALIANT'S LEMMA (*)

by Hermann K.-G. WALTER ()

Communicated by J. BERSTEL

Abstract. – Valiant's algorithm for the recognition problem of contextfree languages uses the computation of matrix closures. The matrices in consideration are strictly upper triangular. The crucial point is that multiplication is nonassociative.

The main point is to prove a lemma concerning the computation of the transitive closure by dividing matrices into submatrices. We give a very simple proof of this lemma.

Résumé. – L'algorithme Valiant pour l'analyse de langages algébriques utilise le calcul de fermetures de matrices. Les matrices considérées sont nilpotentes. Le fait difficile est que la multiplication n'est pas associative.

Le point le plus important est la preuve d'un lemme concernant le calcul de la fermeture transitive en partitionnant les matrices en sous-matrices. Nous donnons une preuve très simple de ce lemme.

1. INTRODUCTION

Valiant's algorithm [2], to solve the wordproblem for contextfree languages uses a procedure to determine the transitive closure of a strictly upper triangular matrix. The crucial point of his approach is to design this procedure even in the case, where the product operation is non-associative. His algorithm uses several propositions on dividing a matrix into certain submatrices to obtain the transitive closure by recursiveness. One of these propositions, which is in fact the essential part of the correctness-proof, seems to be very hard to prove.

The reader may consult Harrison [1], where an elaborated version is given. We shall show that a real simple-minded proof can be given.

(*) Received in November 1984, revised in February 1985.

() Institut für Theoretische Informatik, FB Informatik, TH Darmstadt, Alexanderstr. 24, D-6100 Darmstadt, R.F.A..

2. PRELIMINARIES

We consider an algebraic structure with two operations $+$ and $*$. With respect to the addition $(R, +)$ is a semilattice, this means, we assume the following axiomes:

(A1) (Associativity):

$$(x + y) + z = x + (y + z).$$

(A2) (Commutativity):

$$x + y = y + x.$$

(A3) (Idempotence):

$$x + x = x.$$

(A4) (Neutral element). There exists $0 \in M$ with:

$$x + 0 = x.$$

As usual we introduce a partial ordering by:

(A5) (Absorption):

$$x \leq y \Leftrightarrow x + y = y.$$

With respect to the multiplication we assume:

(A6) (Distributivity):

$$x * (y + z) = x * y + x * z,$$

$$(x + y) * z = x * z + y * z.$$

and:

(A7) (Zero-element):

$$0 * x = x * 0 = 0.$$

By our axioms, multiplication and addition are monotonous operations:

(A8):

$$x \leq y \ \& \ u \leq v \Rightarrow x + u \leq y + v.$$

(A9):

$$x \leq y \ \& \ u \leq v \Rightarrow x * u \leq y * v.$$

By $M_{n,n}(R)$ we denote the set of (n, n) -matrices A over R .

By transferring the operations $+$, $*$ in the usual way to matrices, $M_{n,n}(R)$ again fulfills all our axioms. Especially, matrix product is defined by:

$$(A * B)[i, j] = \sum_{k=1}^n A[i, k] * B[k, j] \quad (1 \leq i, j \leq n).$$

A matrix $A \in M_{n,n}(R)$ is strictly upper triangular ($A \in M_{n,n}^{<}(R)$) if and only if:

$$A[i, j] = 0 \quad \text{if } j \leq i.$$

Especially, the null-matrix 0 containing only 0 -entries, is a strictly upper triangular matrix; hence $M_{n,n}(R)$ again fulfills our axioms.

Since associativity is not valid in general, the definition of exponentiation has to be altered. We define inductively for $A \in M_{n,n}(R)$:

$$A^1 = A,$$

$$A^{i+1} = \sum_{k=1}^i A^k * A^{i-k+1} \quad (i \geq 2).$$

The transitive closure of A is then defined by:

$$A^* = \sum_{k=1}^{\infty} A^k.$$

To assert existence, we assume the necessary completeness axiom for R . Since it is not necessary for $M_{n,n}^{<}(R)$ we omit the details. We summarize some facts on exponentiation.

PROPOSITION 1:

- (i) $A \leq B \Rightarrow A^i \leq B^i \quad (i=1, 2, \dots)$;
- (ii) $A \leq B \Rightarrow A^* \leq B^*$;
- (iii) $(A^*)^* = A^*$;
- (iv) $A \leq A^*$;
- (v) $A \in M_{n,n}^{<}(R) \Rightarrow A^i \in M_{n,n}^{<}(R) \quad (i=1, 2, \dots)$;
- (vi) $A \in M_{n,n}^{<}(R) \Rightarrow A^* \in M_{n,n}^{<}(R) \quad (i=1, 2, \dots)$;
- (vii) $A \in M_{n,n}^{<}(R) \Rightarrow A^{n+i} = 0 \quad (i=1, 2, \dots)$.

Given a matrix A we are interested in dividing A into submatrices. The most interesting division is into nine submatrices:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix},$$

where:

$$1, 5, 9 \quad \text{and} \quad \begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix} \times \begin{bmatrix} 5 & 6 \\ 8 & 9 \end{bmatrix}$$

are square matrices. Special cases are:

- 5 is not present (which implies 2, 4, 6 are not present);
- 9 (or 1) is not present [which implies 3, 6, 7, 8 (or 2, 3, 4, 7)] are not present.

It is easy to check the following proposition.

PROPOSITION 2 (Central submatrix lemma): If $A \in M_{n,n}^<(R)$ and $5^* = 5$ then:

$$A^* = \begin{bmatrix} 1' & 2' & 3' \\ 4 & 5 & 6' \\ 7 & 8 & 9' \end{bmatrix}$$

COROLLARY 1: If:

$$A = \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix} \in M_{n,n}^<(R), \quad 1^* = 1, \quad 9^* = 9,$$

then:

$$A^* = \begin{bmatrix} 1 & 3' \\ 7 & 9 \end{bmatrix}.$$

COROLLARY 2: If:

$$A = \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix} \in M_{n,n}^<(R) \quad \text{and} \quad A' = \begin{bmatrix} 1^* & 3' \\ 7 & 9^* \end{bmatrix},$$

then:

$$A^* = (A')^*.$$

3. VALIANT'S LEMMA

As indicated in the introduction Valiant's Lemma is the crucial point of the algorithm.

Valiant's Lemma

If:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \in M_{n,n}^<(R),$$

with:

$$\begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix}^* = \begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 5 & 6 \\ 8 & 9 \end{bmatrix}^* = \begin{bmatrix} 5 & 6 \\ 8 & 9 \end{bmatrix},$$

then:

$$A^* = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix},$$

where:

$$\begin{bmatrix} 1 & 3+2*6 \\ 7 & 9 \end{bmatrix}^* = \begin{bmatrix} 1 & 3' \\ 7 & 9 \end{bmatrix}.$$

Remark: Note, that by the central submatrix lemma the assumption of Valiant's lemma immediately yields:

$$1^* = 1, \quad 5^* = 5, \quad 9^* = 9.$$

The key to prove Valiant's lemma is to deal with matrix equations. Consider first A^* . We calculate:

$$\begin{aligned} A^* * A^* + A &= \left(\sum_{k=1}^{\infty} A^k \right) * \left(\sum_{l=1}^{\infty} A^l \right) + A \\ &= \sum_{k=1}^{\infty} \sum_{l=1}^{\infty} A^k * A^l + A \quad (\text{Distributivity}) \end{aligned}$$

$$\sum_{r=2}^{\infty} \sum_{l+k=r} A^k * A^l + A = \sum_{r=2}^{\infty} \sum_{k=1}^{r-1} A^k * A^{r-k} + A = \sum_{r=2}^{\infty} A^r + A = A^*,$$

hence A^* is a solution of the matrix equation:

$$X = X * X + A.$$

We claim that A^* is the unique minimal solution of this equations. To show this, we prove that, if X is a solution then

$$A^r \leq X \quad \text{for all } r=1, 2, \dots$$

and therefore:

$$A^* \leq X \quad (\text{Monotonicity of } +).$$

We proceed by induction. If $r=1$ we get:

$$A + X = A + A + X * X = A + X * X = X,$$

hence $A \leq X$.

Let $r > 1$. We assume $A^i \leq X$ for all $1 \leq i < r$. By the monotonicity of $*$, we get:

$$A^i * A^{r-i} \leq X * X.$$

Therefore:

$$A^r = \sum_{i=1}^{r-1} A^i * A^{r-i} \leq \sum_{i=1}^{r-1} X * X = X * X \leq X * X + A = X.$$

By this we have proven:

PROPOSITION3: A^* is the unique minimal solution of the equation:

$$X = X * X + A.$$

Now, we deal with the following situation. Consider a linear matrix equation of the form:

$$X = A_1 * X + X * A_2 + A_3,$$

where:

$$A_1^* = A_1, A_2^* = A_2, A_1, A_2$$

are strictly upper triangular.

To solve this equation we consider the transitive closure of:

$$\begin{bmatrix} A_1 & A_3 \\ 0 & A_2 \end{bmatrix}^* = \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix}$$

(by the central submatrix-lemma). Applying proposition 3 we get:

$$\begin{aligned} \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix} &= \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix}^* \times \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix} + \begin{bmatrix} A_1 & A_3 \\ 0 & A_2 \end{bmatrix} \\ &= \begin{bmatrix} A_1 * A_1 + A_1 & A_1 * B + B * A_2 + A_3 \\ 0 & A_2 * A_2 + A_2 \end{bmatrix} \\ &= \begin{bmatrix} A_1 & A_1 * B + B * A_2 + A_3 \\ 0 & A_2 \end{bmatrix} \text{ again by Proposition 3.} \end{aligned}$$

Hence B is a solution of the linear matrix equation. Let X be an arbitrary solution, then we can build:

$$\begin{bmatrix} A_1 & X \\ 0 & A_2 \end{bmatrix},$$

and show by the same calculation:

$$\begin{bmatrix} A_1 & X \\ 0 & A_2 \end{bmatrix} = \begin{bmatrix} A_1 & X \\ 0 & A_2 \end{bmatrix}^* \begin{bmatrix} A_1 & X \\ 0 & A_2 \end{bmatrix} + \begin{bmatrix} A_1 & A_3 \\ 0 & A_2 \end{bmatrix}.$$

Thus:

$$\begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_3 \\ 0 & A_2 \end{bmatrix}^* \leq \begin{bmatrix} A_1 & X \\ 0 & A_2 \end{bmatrix}.$$

This yields $B \leq X$.

PROPOSITION 4: *If B is determined by:*

$$\begin{bmatrix} A_1 & A_3 \\ 0 & A_2 \end{bmatrix}^* = \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix},$$

then B is the unique minimal solution of:

$$X = A_1 * X + X * A_2 + A_3,$$

provided A_1, A_2 are strictly upper triangular and $A_1^ = A_1$ and $A_2^* = A_2$.*

Now, consider Valiant's lemma. Let:

$$A = \begin{bmatrix} \bar{1} & 2 & \bar{3} \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad \text{and} \quad A^* = \begin{bmatrix} \bar{1} & 2 & \bar{X} \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Applying Proposition 3 we calculate:

$$A^* = \begin{bmatrix} 1 & 2 & 2 * 6 + 3 + 1 * X + X * 9 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Again we can use Proposition 3 to show that X is the unique minimal solution of:

$$1 * X + X * 9 + 2 * 6 + 3 = X.$$

Since 1, 9 are strictly upper triangular and $1^* = 1$, $9^* = 9$ we can apply Proposition 4. By this we get immediately Valiant's lemma.

REFERENCES

1. M. A. HARRISON, *Introduction to Formal Languages Theory*, Addison-Wesley Pub. Co., Reading, Mass. 1978.
2. L. VALIANT, *General Context-free Recognition In Less Than Cubic Time*, J. Comp. Syst. Sc., Vol. 10, 1975, pp. 308-315.