Astérisque

J. F. PERROT

Calcul dans un monoïde fini de transformations

Astérisque, tome 38-39 (1976), p. 203-211

<http://www.numdam.org/item?id=AST_1976__38-39__203_0>

© Société mathématique de France, 1976, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) 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/

Société Mathématique de France
Astérisque 38-39 (1976) p.203-211

CALCUL DANS UN MONOÏDE FINI DE TRANSFORMATIONS

par

J.F. PERROT

1.- INTRODUCTION

Considérons le problème élémentaire que voici : "Soit S un ensemble fini. On se donne une famille X de transformations de S (applications de S dans lui-même), et on désigne par T l'ensemble de toutes les transformations de S que l'on obtient par composition des transformations éléments de X (T est ainsi l'ensemble sous-jacent au monoïde de transformations de S engendré par X). On demande de décrire T à partir de X".

Notons que la taille de T peut être très grande : si S a n éléments, T peut en avoir de 1 à n^n sans que l'on connaisse de moyen général pour obtenir une meilleure approximation par simple inspection de l'ensemble X. On ne peut donc pas envisager de se donner la collection complète des éléments de T, sauf dans des cas très particuliers, et on est conduit à explorer T localement. Pour cela, il est naturel de faire intervenir la structure de monoïde fini dont est muni l'ensemble T relativement à l'opération de composition des transformations et de considérer que l'ordre imposé à l'exploration par le calcul à partir de X (produits de compositions de plus en plus longs) conduit, grosso modo, à parcourir en descendant le treillis des idéaux du monoïde ; en effet, les résultats de toutes les compositions où entre un élément $m \in T$ sont dans l'idéal $T\,m\,T$ engendré par m, et par conséquent, engendrent eux-mêmes des idéaux contenus dans $T\,m\,T$.

Les éléments de T voisins d'un élément m sont alors ceux qui engendrent le même idéal ; ils constituent, suivant la terminologie classique, la D-classe de m.

L'exploration locale de l'ensemble T conduit ainsi à poser le :

Problème : à partir de X et de $m \in T$, décrire la D-classe de m.

Malheureusement, il existe, en général, dans un monoïde fini, deux types de D-classes : celles qui contiennent au moins un élément idempotent, qu'on appelle régulières, et celles qui n'en contiennent point. Ces dernières, ou D-classes irrégulières, jouent la plupart du temps un rôle mal connu ; de notre point de vue, la connaissance d'une telle D-classe requiert celle de toute la partie du monoïde située au-dessus d'elle (au sens du treillis des idéaux), et fait échec à notre projet d'exploration locale. Nous nous bornerons donc, le cas échéant, à constater que la D-classe considérée est irrégulière.

Les D-classes régulières, en revanche, forment en quelque sorte l'ossature du monoïde, et c'est à elles que s'adressent la plupart des questions : par exemple, ce sont elles qui contiennent les sous-groupes du monoïde ; les D-classes sont toutes triviales (réduites à un seul élément) ssi les D-classes régulières le sont ; l'idéal minimal est toujours une D-classe régulière, etc... Or, chacune d'entre elles est pourvue d'une structure intrinsèque, entièrement décrite (à un isomorphisme près) par la donnée d'un groupe G, de deux entiers positifs p et q et d'une matrice Γ, de format $q \times p$, à éléments dans $G \cup \{0\}$, appelée matrice-sandwich. D'après le théorème de Rees, les éléments m de la D-classe régulière considérée D sont en bijection avec les triplets (g,i,j) pour $g \in G$ et $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$. Le produit de deux éléments m', $m'' \in D$ est encore dans D ssi l'élément $\gamma_{j',i''}$ de la matrice-sandwich est non nul, et en ce cas son triplet associé est donné par la règle $(g',i',j')\ (g'',i'',j'') = (g'\ \gamma_{j',i''}\ g'',i',j'')$, le produit dans la première

composante étant pris au sens du groupe G.

Nous donnons un procédé permettant, à partir d'un élément m et du système générateur X :

i) de décider si la $\underline{D}$-classe de m est régulière,

ii) si oui, de fournir les éléments de la description de la $\underline{D}$-classe en ne faisant appel qu'à $(p+q) \times n$ éléments de T (alors que la $\underline{D}$-classe elle-même contient $p \times q \times |G|$ éléments).

Ce procédé, développé à partir d'une technique employée de longue date par M.P. Schützenberger, est très facile à mettre en œuvre sur ordinateur et peut être adapté à divers problèmes particuliers : calcul de l'idéal minimal [6], calcul complet d'un monoïde régulier (i.e. ne possédant pas de $\underline{D}$-classe irrégulière) [3]. On trouvera en [5] des développements plus complets.

2.- RAPPEL SUR LA STRUCTURE D'UNE $\underline{D}$-CLASSE RÉGULIÈRE

Pour plus de détails, on se reportera à Clifford et Preston [2]. Dans un monoïde quelconque M, la relation d'équivalence $\underline{D}$ est définie comme la borne supérieure des équivalences $\underline{R}$ et $\underline{L}$ suivantes :

Pour $a, b \in M$, on note :

$a \ \underline{R} \ b$ ssi $aM = bM$ (a et b engendrent le même idéal à droite)

$a \ \underline{L} \ b$ ssi $Ma = Mb$ (a et b engendrent le même idéal à gauche).

Il est clair que $a \ \underline{D} \ b$ implique $MaM = MbM$, mais la réciproque n'est vraie que sous certaines hypothèses de finitude, vérifiées notamment quand M est fini. Dans un monoïde fini, on a donc :

$$MaM = MbM \Longleftrightarrow a \ \underline{D} \ b.$$

On note $\underline{H}$ l'équivalence $\underline{R} \cap \underline{L}$. Toute $\underline{D}$-classe peut être envisagée comme

réunion de R-classes, réunion de L-classes, ou réunion de H-classes.

Soit D une D-classe régulière du monoïde fini M, $\{R_i ; i = 1,2,\ldots,p\}$ (resp. $\{L_j ; j = 1,2,\ldots,q\}$) l'ensemble des R-classes (resp. L-classes) contenues dans D. La description de D que nous avons en vue est fondée sur les observations suivantes, dont on trouvera les preuves en [2].

1.- Chaque R-classe R_i coupe chaque L-classe L_j suivant une H-classe H_{ij}, et toutes les H-classes $H_{i,j}$ $(i = 1,2,\ldots,p,\ j = 1,2,\ldots,q)$ ont le même nombre d'éléments ;

2.- Chaque R-classe R_i (resp. chaque L-classe L_j) contient au moins un idempotent ;

3.- Chaque H-classe H_{ij} contient au plus un idempotent ; lorsqu'elle en contient un, la restriction de la multiplication dans M la munit d'une structure de groupe ayant pour élément neutre l'idempotent en question ; les différents groupes ainsi constitués à l'intérieur de D sont tous isomorphes entre eux ;

4.- On obtient une description de D du type annoncé en supposant que la H-classe H_{11} contient un idempotent et en désignant par G le groupe correspondant. La matrice-sandwich Γ est de format $q \times p$, on la définit à partir de deux familles quelconques r_i ; $i = 1,2,\ldots,p$ et $\overline{r}_j$; $j = 1,2,\ldots,q$ de représentants des H-classes $H_{i,1}$ et $H_{1,j}$ respectivement, en posant $\gamma_{j,i} = \overline{r}_j r_i$ lorsque ce produit figure dans H_{11}, $\gamma_{j,i} = 0$ sinon. Au triplet (g,i,j) correspond alors bijectivement l'élément $m = r_i g \overline{r}_j \in H_{ij}$.

Les indications ci-dessus, valables pour un monoïde quelconque, montrent clairement que la première information nécessaire pour décrire une D-classe est celle de son format (nombre de R-classes, nombre de L-classes). Nous l'obtiendrons en utilisant systématiquement le fait que notre monoïde M est représenté par transformations de l'ensemble fini S.

3.- ENSEMBLES-IMAGES, ÉQUIVALENCES D'APPLICATION ET FORMAT D'UNE D-CLASSE

Pour une transformation quelconque f de l'ensemble S, désignons par Im(f) le sous-ensemble image Sf, par Ker(f) l'équivalence d'application de f et par rg(f) le rang de f, qui est égal à l'index de Ker(f) et au cardinal de Im(f).

Pour deux éléments quelconques a et b de notre monoïde de transformations, il est facile de voir que :

$$a \underline{R} b \Rightarrow \mathrm{Ker}(a) = \mathrm{Ker}(b)$$
$$a \underline{L} b \Rightarrow \mathrm{Im}(a) = \mathrm{Im}(b).$$

Les implications réciproques ne sont pas vraies en général, mais elles le sont sous l'hypothèse que a et b appartiennent à une même D-classe régulière, d'où la :

PROPOSITION 1.- Pour une D-classe régulière D du monoïde de transformations M, les R-classes (resp. les L-classes) de D sont en bijection avec l'ensemble d'équivalences $\underline{K} = \{\mathrm{Ker}(a) ; a \in D\}$ (resp. avec l'ensemble d'images $\underline{I} = \{\mathrm{Im}(b) ; b \in D\}$).

Il suffit donc, pour déterminer le format de D, de calculer les ensembles I et K. En fait, ces deux ensembles nous fournissent en sus un critère pour décider si un élément quelconque $f \in M$ appartient ou non à la D-classe D:

Remarque.- Pour tout $f \in M$ on a $f \in D$ ssi $\mathrm{Ker}(f) \in \underline{K}$ et $\mathrm{Im}(f) \in \underline{I}$.

La vérification de ces énoncés utilise essentiellement l'observation 2 ci-dessus relative à la présence d'au moins un idempotent par R-classe et par L-classe. Or, les idempotents sont faciles à repérer par examen du couple Im, Ker : en effet, pour un sous-ensemble J de S et une équivalence θ d'index $|J|$ sur S, il existe une transformation idempotente e telle que $\mathrm{Im}(e) = J$ et $\mathrm{Ker}(e) = \theta$ ssi J constitue un système complet de représentants des classes mod. θ ;

l'idempotent e est alors unique ; en ce cas, nous disons simplement que le couple (J,θ) repère un idempotent.

Il suit donc de l'observation 2 que pour tout $J \in \underline{I}$, il existe au moins un $\theta \in \underline{K}$, et pour tout $\theta \in K$, il existe au moins un $J \in \underline{I}$, tels que le couple (J,θ) repère un idempotent.

Pour calculer effectivement $\underline{I}$ et $\underline{K}$ à partir d'un élément m de D donné et du système générateur X, notons d'abord que l'observation 1 permet de restreindre le choix des représentants a et b dans la définition de $\underline{I}$ et de $\underline{K}$ et d'écrire :

$$\underline{K} = \{Ker(a) \ ; \ a \, \underline{L} \, m\} \quad \text{et} \quad \underline{I} = \{Im(b) \ ; \ b \, \underline{R} \, m\}$$

de sorte qu'en définissant :

$$\underline{K}' = \{Ker(a) \ ; \ a \in Mm \ , \ rg(a) = rg(m)\}$$

et

$$\underline{I}' = \{Im(b) \ ; \ b \in mM, \ rg(b) = rg(m)\}$$

on a $\underline{K} \subseteq \underline{K}'$ et $\underline{I} \subseteq \underline{I}'$.

On peut alors énoncer le critère suivant :

PROPOSITION 2.- Soit $J \in \underline{I}'$ (resp. $\theta \in \underline{K}'$) : on a $J \in \underline{I}$ (resp. $\theta \in \underline{K}$) ssi il existe $\chi \in \underline{K}'$ (resp. $P \in \underline{I}'$) tel que le couple (J,χ) (resp. (θ, P)) repère un idempotent.

Comme par définition on doit avoir $m \in D$ donc $Ker(m) \in \underline{K}$ et $Im(m) \in \underline{I}$, on voit que si D est régulière, l'un au moins des $J \in \underline{I}'$ (resp. l'un au moins des $\theta \in \underline{K}'$) doit avec Ker(m) (resp. avec Im(m)) repérer un idempotent, et que réciproquement l'une de ces deux conditions est suffisante pour assurer que la $\underline{D}$-classe de m est régulière.

La détermination du format de la $\underline{D}$-classe de m est ainsi ramenée au calcul des ensembles $\underline{I}'$ et $\underline{K}'$. Ce dernier se fait sans difficulté par un processus arborescent classique à partir de l'élément m et du système généra-

teur X : pour calculer $\underline{I}'$, on répète à partir de M des compositions à droite par les éléments de X, en ne conservant à chaque pas que les transformations dont l'image est de rang rg(m) et n'a pas encore été rencontrée, jusqu'à ce que toute nouvelle opération donne, soit une image déjà répertoriée, soit une transformation de rang inférieur ; on obtient ainsi l'ensemble $\underline{I}'$ et pour chaque $J \in \underline{I}'$, un élément $r_j \in mM$ tel que $Im(r_j) = J$. De même, en opérant à gauche, on obtient l'ensemble d'équivalences K' et pour chaque $\theta \in \underline{K}'$ un élément $\overline{r}_\theta \in Mm$ vérifiant $Ker(\overline{r}_\theta) = \theta$.

Le calcul se déroule donc ainsi :

- Génération de l'ensemble $\underline{I}'$ à partir de m et de X ; la $\underline{D}$-classe est régulière ssi I' contient une image J qui, avec Ker(m), repère un idempotent.
- Si la $\underline{D}$-classe est régulière, génération de $\underline{K}'$ à partir de m et de X.
- Extraction des sous-ensembles $\underline{I}$ et $\underline{K}$ de $\underline{I}'$ et $\underline{K}'$ grâce à la proposition 2.

4.- MATRICE-SANDWICH ET GROUPE D'UNE D-CLASSE RÉGULIÈRE

Le calcul du format de la $\underline{D}$-classe de m effectué au paragraphe précédent nous a fourni tous les éléments nécessaires à la description complète de la $\underline{D}$-classe.

Pour construire la matrixe-sandwich, il faut d'abord choisir une $\underline{H}$-classe contenant un idempotent pour jouer le rôle de H_{11} de l'observation 4, ainsi que les familles r_i et $\overline{r}_j$ correspondantes. On peut choisir H_{11} dans la $\underline{R}$-classe de m, ce qui permet de prendre pour famille r_i la famille des représentants r_j calculés en même temps que l'ensemble $\underline{I}$. Il suffit alors de connaître une transformation f telle que $mf \in H_{11}$ pour avoir la famille $\overline{r}_j$ sous la forme $\overline{r}_\theta f$, où les $\overline{r}_\theta$ ont été calculés en même temps que $\underline{K}$. Si on ne dispose pas de cette information (notamment lors d'un calcul par ordinateur), il suffit de calculer $\underline{K}'$ à partir du représentant $mf \in H_{11}$ pour obtenir la famille cherchée. La matrice-sandwich se déduit

donc immédiatement du calcul précédent.

La détermination du groupe G pose un autre problème : ce groupe apparaît, dans la perspective de notre calcul, comme un groupe de permutations sur l'ensemble-image de H_{11} ; il peut être, comme le monoïde M lui-même, de trop grande taille pour être manipulé dans son ensemble, aussi n'en proposerons-nous qu'un système générateur, déduit de X par le biais de la représentation de Schützenberger du monoïde M sur la D-classe D. On sait que cette représentation associe à chaque élément $f \in M$ une matrice $\mu(f)$ de format $q \times q$ monomiale en lignes, à éléments dans $G \cup \{0\}$, qui décrit l'action de f à droite sur la D-classe D. Commme l'ensemble X engendre M, les éléments non nuls des matrices $\mu(x)$, pour $x \in X$, engendrent G. Il suffit donc de calculer les matrices $\mu(x)$, ce qui se fait,à partir des familles de représentants déjà utilisés pour construire la matrice-sandwich,par simple traduction des définitions données en [2].

Il est clair que ce procédé n'est pas toujours satisfaisant : il reste à décrire le groupe G à partir de son système générateur ; mais ce problème est d'une autre nature, et, conformément à une tradition bien ancrée en théorie des monoïdes, nous nous contentons ici de décrire la D-classe "modulo ses sous-groupes".

5.- CONCLUSION

Ceci achève la description de la D-classe d'un élément m à condition qu'elle soit régulière. On voit que la quantité de mémoire utilisée pour le calcul est proportionnelle à la taille n de l'ensemble S et à la somme des tailles des ensembles I' et K' ; en admettant que ces derniers sont du même ordre que I et K , on obtient pour une D-classe de format (p,q) un encombrement de l'ordre de $(p + q) \times n$.

Notre technique permet donc de traiter, à la main ou par ordinateur, des monoïdes de grande taille qui resteraient inaccessibles aux méthodes re-

posant sur l'énumération complète des éléments [1] [4].

On peut chercher à appliquer le même principe à la description de toutes les D-classes régulières du monoïde M en évitant l'énumération de tous ses éléments. Cette extension se fait sans difficulté lorsque M ne contient que des D-classes régulières (monoïde régulier), et on trouvera en [3] des programmes réalisant ce calcul sur ordinateur. Ces programmes sont également utilisables pour des monoïdes irréguliers, mais alors on ne peut plus assurer que toutes les D-classes régulières du monoïde seront effectivement calculées, en raison de pertes d'information dues aux D-classes irrégulières. Le problème de la description de toutes les D-classes régulières en présence de D-classes irrégulières et sans énumération exhaustive des éléments du monoïde n'est donc pas résolu.

BIBLIOGRAPHIE

[1] CANNON J.J. : Computing the ideal structure of finite semigroups, Num. Mathematik 18 (1971) 254-266.

[2] CLIFFORD A.H. and PRESTON G.B : The Algebraic Theory of Semigroups, Vol. I, Amer. Math. Soc. 1961.

[3] COUSINEAU F.G ; PERROT J.F, and RIFFLET J-M : APL Programs for Direct Computation of a Finite Semigroup, in APL Congress'73, North-Holland 1973, p. 67-74.

[4] HENNEMAN W. : The Automata Theorist's Helper, in Mc Naughton and Papert, Counter-Free Automata, MIT Press 1971, p. 147-154.

[5] PERROT J-F : Contribution à l'étude des monoïde syntaxiques et de certains groupes associés aux automates finis, Thèse Sc.Math. Paris 1972.

[6] PERROT J-F : Utilisation d'APL pour calculer des monoïdes finis, Journées SMF sur l'utilisation des calculateurs en Math. pures, Limoges 1975, à paraître.

Jean-François PERROT
Institut de Programmation
Université de Paris VI
4 place Jussieu
75005 PARIS