DECOMPOSITION POLYNOMIALE DES FONCTIONS RATIONNELLES

M.P. Schützenberger

Nous considérons une fonction rationnelle $\alpha : A^* \to B^*$ d'un monoïde libre dans un autre. Dans le cas le plus général, elle est donnée par un transducteur (μ, λ, ρ) constitué par un morphisme μ de A^* dans un monoïde de matrices à entrées dans $B^* \cup \{0\}$ et deux vecteurs fixes (à entrées dans le même monoïde) λ et ρ ; l'image par α d'un mot w de A^* étant l'élément $\lambda.w\mu.\rho$ de $B^* \cup \{0\}$, ce qui implique des restrictions sévères sur les supports des matrices $w\mu$ et des vecteurs λ et μ : si β est le morphisme de $B^* \cup \{0\}$ dans $\mathbb{Z}$ envoyant B^* sur 1 on doit avoir identiquement $\lambda\beta.w\mu\beta.\rho\beta \in \{0,1\}$.

Comme on le sait, les rapports entre une fonction α donnée et les différents transducteurs susceptibles de la réaliser sont encore fort obscurs bien que l'on sache décider si deux transducteurs réalisent ou non la même fonction.

La théorie est beaucoup plus avancée dans le cas de fonctions dites *séquentielles* ou *sous-séquentielles* qui sont d'ailleurs les plus communément considérées. Ayant fait choix d'un sens de lecture (disons gauche-droite, si on nous l'autorise encore) du mot d'entrée w, ce sont les fonctions α pour lesquelles le mot de sortie $w\alpha$ peut être calculé au fur et à mesure de la lecture sans avoir besoin de connaître le reste du mot.

Ceci correspond à la possibilité de réaliser α au moyen d'un transducteur (μ, λ, ρ) tel que d'une part toutes les matrices $w\mu$ soient monomiales par ligne, et, d'autre part, le vecteur initial λ n'ait qu'une seule entrée non nulle. Le cas séquentiel strict est celui où, de plus, le vecteur final ρ a toutes ses entrées égales à 0 ou à 1. C'est le cas classique, et sa généralisation "sous séquentielle" n'en diffère que par la possibilité de faire intervenir dans les dernières lettres du mot de sortie le fait que l'on a ou non atteint la fin du mot d'entrée.

Nous avons considéré dans [1] une généralisation assez immédiate, consistant à suposer que le domaine de α est l'union (finie, disjointe) de parties reconnaissables X_i et que sur chacune de celles-ci, α est réalisable par un transducteur sous séquentiel.

L'exemple le plus simple serait peut être la fonction $\alpha : A^* \to A^*$ envoyant chaque mot w sur lui-même quand sa première et sa dernière lettre sont différentes et sinon sur la lettre figurant à la fois à l'initiale et à la finale de w.

Une description approximative de ces fonctions serait de dire qu'elles peuvent être réalisées de façon séquentielle moyennant l'acquisition préalable d'une quantité *bornée* d'informations, à savoir la connaissance de celui des sous-domaines X_i qui contient le mot d'entrée w que l'on doit transducter. Il est bien facile de voir que cette condition n'est pas satisfaite par l'exemple type de la fonction rationnelle qui est l'inverse d'un morphisme injectif correspondant à un code (complet, fini) quand ce dernier n'est pas un code préfixe. Considérons en effet un tel code Y et supposons même qu'il est synchronisant. Il existe des mots arbitrairement longs $v \in A^*$ et des facteurs droits d,d' de mots de Y tels que wd et wd' aient respectivement les factorisations $wd = y_1 \ldots y_n$, $wd' = y'_1 \ldots y'_{n'}$ avec $y_1 \neq y'_1$ ($y_1, \ldots, y_n, y'_1, \ldots, y'_{n'} \in Y$). Donc si v est le facteur gauche d'un mot $w \in Y^*$, le transducteur décodeur ne peut commencer à écrire la première lettre y que s'il possède l'information correspondant au fait que v est suivi par d ou par d' dans w, c'est-à-dire très exactement que $y_1^{-1} w \in Y^*$ ou que $y'^{-1}_1 w \in Y^*$. Comme nous avons supposé Y synchronisant, il existe des mots $u_1, u_2, \ldots, u_k, \ldots$ tels que si $w = vu_1vu_2 \ldots vu_k \ldots$ la même situation se retrouve au début de chaque facteur v. En conclusion, le décodage séquentiel de w ne peut être effectué que si une exploration préalable de w a fourni un nombre d'informations indépendantes croissant linéairement avec k, c'est-à-dire avec la longueur de w puisque les u_k peuvent être pris à l'intérieur d'un ensemble fini de mots.

Le cas que je propose d'examiner est intermédiaire entre les extrêmes : celui du décodage, (qui est le cas générique) où l'information préalable indispensable pour toute implémentation déterministe de la transduction croît linéairement avec la longueur du mot d'entrée w et le cas séquentiel où la même tâche peut être accomplie "en temps réel" sans nulle connaissance de la partie de w à droite (ou dans le futur) de chaque lettre successive soumise à l'algorithme.

Le premier de ces cas est bien un cas extrême puisque pour toute fonction rationnelle $\alpha : A^* \rightarrow B^*$ on peut trouver un alphabet fini A' et une transduction $\alpha' : A^* \rightarrow (A \times A')^*$ telle que :

d'une part α' soit "séquentielle retournée" c'est-à-dire réalisable séquentiellement de DROITE à GAUCHE ; d'autre part $\alpha = \alpha' \alpha''$ où $\alpha'' : (A \times A)^* \rightarrow B^*$ est une fonction sous séquentielle ordinaire.

Je propose un nouveau cas intermédiaire sous le nom de *polyséquentiel* dont voici la définition formelle.

Fonctions Polyséquentielles.

Définition. Une fonction rationnelle $\alpha : A^* \rightarrow B^*$ est *polyséquentielle* ssi son domaine est une union finie disjointe de produits (finis, évidemment) non ambigus de parties reconnaissables $X_{i,j}$ telles que la restriction de α à chaque $X_{i,j}$ soit une fonction sous-séquentielle.

Le cas évoqué plus haut est le cas particulier où le domaine D est une union finie de produits triviaux, $X_i = X_{i_1}$ et non pas de produits $X_{i_1} X_{i_2} \ldots X_{i_{r_i}}$.

Montrons d'abord que l'information sur w qui est requise pour pouvoir déterminiser sa transduction ne croît pas aussi vite que dans le cas générique bien qu'elle ne puisse pas être bornée a priori. Soit donc α une fonction polyséquentielle et w un mot de son domaine. Puisque les parties reconnaissables $X_{i,j}$ sont en nombre fini nous pouvons effectuer une exploration préparatoire de w qui en donne une factorisation $w = w_1 w_2 \ldots w_r$ où, pour un certain i, on a identiquement $w_j \in X_{i,j}$ ($j = 1,2,\ldots, r_i = r$). Les hypothèses de non ambiguité impliquent que cette factorisation est unique. Introduisant de nouvelles lettres $a_{i,j}$ (dont le nombre est fini) et l'alphabet auxiliaire $A' = \{1\} \cup \{a_{i,j}\}$, on associe à w le mot $w\gamma$ sur $A \times A'$ en remplaçant dans w chaque lettre a par $(a, a_{i,j})$ ou par (a,1) selon qu'elle est ou non la première lettre de l'un des facteurs w_j. On verra plus loin que γ est une fonction rationnelle d'un type très particulier mais pour l'instant nous examinons seulement la quantité d'informations ajoutée à w par la transformation $w \rightarrow w\gamma$.

Par définition chaque lettre a_{ij} n'y figure qu'une fois au plus et la seule donnée réellement importante est la place qu'elle occupe dans w', c'est-à-dire un entier $n_{i,j} \geq 1$ borné supérieurement par la longueur n de w. La quantité correspondante d'informations est donc bornée supérieurement par $Log_2 n + K_i'$ où K_i' ne dépend que de la taille de A'. Par conséquent $w \rightarrow w\gamma$ requiert au maximum $K'' + KLog_2 n$ bits où K et K" sont des constantes finies déterminées a priori par la donnée de la représentation du domaine D comme polynôme non ambigü (en des parties reconnaissables).

De nouveau on peut facilement montrer que K est nul si et seulement si α est une somme de fonctions sous-séquentielles et que $K = K'' = 0$ correspond au cas séquentiel.

Venons-en maintenant à l'implémentation de γ. Une autre manière de présenter un transducteur μ est de lui associer un morphisme σ de A* sur un monoïde fini S' et une fonction $\alpha_1 : S \times A \times S \rightarrow B^*$. A un détail près (concernant l'image de 1) c'est la description en terme de ce que S. Eilenberg a bien voulu appeler *"bimachine"*. Pour chaque factorisation $w = w'aw''$ $(w',w'' \in A^*, a \in A)$ du mot d'entrée w, la bimachine fournit le facteur correspondant $(w'\sigma, a, w''\sigma)\ \alpha_1 \in B^*$ du mot de sortie.

Ceci étant rappelé, et α étant toujours un transducteur polyséquentiel, nous pouvons certainement trouver un morphisme $\sigma : A^+ \rightarrow S'$, semigroupe fini, et, pour chaque (i,j) une partie C_{ij} de $S \times A \times S$ telle que $(w'\sigma, a, w''\sigma) \in C_{ij}$ si et seulement si $w'aw'' \in X_{i_1} X_{i_2} \ldots X_{i_r}$ - où a est la première lettre du facteur dans $X_{i,j}$ - ce qui montre que g est bien une fonction rationnelle. Cette construction n'a pas d'autre mérite puisque l'on aurait aussi bien pu construire d'emblée une bimachine réalisant α au lieu de passer par l'étape intermédiaire de γ avant de terminer la transduction par l'opération séquentielle évidente $w\gamma \rightarrow w\alpha$.

J'indique donc très brièvement comment on pourrait concevoir une machine particulière, simple et économique pour effectuer l'opération γ. Disons un *arpenteur*.

Les arpenteurs.

Nous considérons un automate fini déterministe qui lira le mot d'entrée w de façon progressive de DROITE à GAUCHE.

L'aspect nouveau est que la machine dispose d'un ensemble *fini* $\{a_k\}$ $(k \in K)$ de marqueurs et qu'en fonction de son état et de la lettre lue elle peut effectuer l'une ou l'une et l'autre des deux opératiohns suivantes sur la bande portant le mot d'entrée :

(1) retirer un marqueur qu'elle a déjà posé (c'est-à-dire qui est à droite de la lettre qu'elle est en train de lire)

(2) poser sous cette lettre un marqueur a_j, à condition que ce marqueur ne soit pas déjà posé ailleurs (auquel cas il faudrait d'abord le retirer).

Ces opérations sont effectuées en fonction de l'état de l'automate et il est licite, pour chaque lettre lue d'en accomplir un nombre (fini) quelconque. A la fin de la lecture du mot d'entrée w, on dispose donc d'un mot $w\gamma$ sur l'alphabet produit $A \times (\{1\} \cup \{a_k : k \in K\})$ dans lequel chacun des symboles a_k apparaît une fois au plus. Des considérations bimachinistes simples montrent que l'opération $w \rightarrow w\gamma$ réalisée par l'arpenteur est une transduction rationnelle ajoutant à w une quantité d'informations qui ne croît pas plus vite qu'une fonction linéaire du logarithme de la longueur de w.

Examinons d'un peu plus près les règles de pose et d'enlèvement des marqueurs. Dans le cas le plus général il existe un morphisme $\tau : A^* \rightarrow T$ fini tel qu'à chaque lettre lue l'état de l'automate contienne à la fois l'ordre dans lequel les marqueurs ont été posés et la valeur par τ du segment de w entre la lettre lue et celles où ils se trouvent. Tout ceci ne requiert qu'une quantité *bornée* d'informations et le contenu de la mémoire peut être décrit comme étant une partir K' de K, un ordre total sur K' et une application de K' dans T.

Ce genre d'appareil a déjà été rencontré sous une forme à peine différente par McNaughton dans sa théorie des mots infinis. Montrons en l'application à notre problème et soient X et Y deux parties reconnaissables par τ telles que le produit $D = XY$ soit non ambigu. Par commodité nous désignons par P l'ensemble des facteurs droits des mots de X et nous observons le

Lemme . *Pour chaque mot w de A* le nombre de ses factorisations w = py (p ∈P, y ∈Y) est au plus égal à Card(T).*

Preuve. Supposons w = phy' où h ≠ 1, p, ph ∈ P, y', hy' ∈ Y. Les éléments pτ et phτ sont différents car sinon prenant f tel que fp ∈ X le mot fw = (fp)(hy') = (fph)(y') aurait deux XY-factorisations distinctes. □

Ceci permet de construire un arpenteur donnant la factorisation des mots : le nombre des marqueurs est K = 1 + Card (T) et on ne pose l'un d'eux sous la lettre lue que si le mot appartient à Y. D'autre part, le mot lu étant w et un marqueur a_j se trouvant posé sous la première lettre (à gauche) de son facteur droit y' ∈ Y, soit w = gy', on enlève ce marqueur ssi g ∉ P. Le lemme ci-dessus montre qu'avec ces règles on aura toujours assez de marqueurs. A la fin de la lecture, si w ∈ XY il existe exactement un d'entre eux dont le facteur associé est dans X. On enlève les autres et l'on a obtenu wγ.

Revenant au cas général, on voit que la non ambiguité d 'un produit $X_{i1} X_{i2}...X_{ir}$ entraîne celle de chacun des facteurs et la construction de l'arpenteur fournissant un mot wγ indiquant la factorisation de w est un simple exercice.

Un exemple.

Soit σ : A* → S un morphisme sur un monoide fini J-trivial et soit α la transduction définie par une bimachine dont les transitions sont régies par σ, c'est-à-dire dont l'ensemble Q des états peut être identifié à S de façon naturelle. L'hypothèse que S est J-trivial signifie que pour chaque (w',a) ∈ A* x A on a w'σ = (w'a) σ sauf si l'idéal bilatère engendré par (w'a) σ est strictement inférieur à celui engendré par w'σ et qu'il en est de même pour tout (a,w") ∈ A x A. Il en résulte que si $\{D_i : i \in I\}$ est l'ensemble des J-classes de S il existe pour chaque i,j ∈ I un morphisme $\varphi_{i,j}$ de A* dans B* ∪ 0 et un sous alphabet A_{ij} de A tel que w'σ ∈ D_i, w"σ ∈ D_j, u ∈ A^*_{ij} entraîne (w', u, w")μ = uφij. Comme d'autre part chaque mot a au plus un facteur gauche de longueur minimale dans chaque D_i et que la propriété correspondante vaut pour les facteurs droits, on voit que ces facteurs permetent de construire une décomposition polynomiale non ambigüe de

A^* telle que α se réduise à un morphisme φ_{ij} sur chacun de ses facteurs X_{ij}. Les morphismes étant des fonctions séquentielles ceci achève de montrer que les transducteurs à support J-trivial sont des fonctions polyséquentielles.

Je mentionne ici pour terminer une condition remarquable satisfaite par ces transducteurs. Il est vraisemblable qu'elle suffit pour garantir qu'une fonction rationnelle α puisse être implémentée par un transducteur J-trivial mais je n'ai pas terminé la preuve.

Il existe des constantes finies r, k_0, k_1 telles que tout mot w de A^* admette une factorisation $w = u_0v_1u_1 ...w_ju_j$ $(1 \leq r)$ pour laquelle

$$w\alpha = \bar{u}_0(v_1\varphi_1)\ \bar{u}_1(v_2\varphi_2) ...(v_1\varphi_1)\ \bar{u}_1$$

où $|\ \bar{u}_0\ \bar{u}_1 ...\ \bar{u}_1\ | \leq k_0$ et où chaque φ_i est un morphisme $A^* \rightarrow B^* \cup \{0\}$ satisfaisant $|\ a\varphi_i\ | \leq k_i$ pour tout $a \in A$.

Un problème de décision.

Il reste à trouver des conditions permettant de décider si une fonction rationnelle α est ou non susceptible d'être réalisée par un transducteur polyséquentiel indépendamment du transducteur (μ, λ, ρ) par laquelle elle est originellement donnée. La méthode employée est celle de [1].

Soit Q l'ensemble des états de μ, c'est-à-dire que chaque $w\mu$ est une $Q \times Q$ matrice. On peut supposer sans perte de généralité que q est l'unique état pour lequel le vecteur λ a une coordonnée non nulle et que chaque état q est accessible et coaccessible.

On a définit dans [1] un *branchement* comme un triple (q, q_1, q_2) tel que $u\mu_{q,q_1} \neq x_1 \neq \emptyset$ pour au moins un $u \in A^*$, ce branchement étant *fort* ssi pour chaque $k > 0$ on peut choisir un mot u_k tel que la distance préfixe entre x_1 et x_2 excède k. On a également montré que α est sous séquentielle ssi elle n'a pas de branchements forts et qu'elle est une union disjointe (finie) de fonctions sous séquentielles ssi pour chaque branchement fort (q, q_1, q_2) l'état q est inaccessible à partir de q_1 *et* à partir de q_2 c'est-à-dire que $v\mu_{q_1,q} = v\mu_{q_2,q} = \emptyset$ pour tout $v \in A^*$.

Propriété. *Une condition nécessaire et suffisante pour que* α *soit polyséquentielle est que pour tout branchement fort* (q, q_1, q_2) q *ne soit acessible qu'à partir de l'un au plus des deux états* q_1 *et* q_2.

Preuve. Supposons que cette condition ne soit pas satisfaite c'est-à-dire qu'il existe v_1, v_2 satisfaisant $v_i\mu_{q_i,q} = y_i \neq \emptyset$ $(1 = 1,2)$. Prenant u_k comme ci-dessus et considérant les mots de $f\{u_kv_1, u_kv_2\}g$ où $f\mu_{q\text{-}q} \neq \emptyset$ et $q\mu_{qq_+} \neq \emptyset$ on vérifie facilment que la quantité d'information nécessaire pour déterminiser x croît linéairement avec d.

Dans la direction opposée la condition que par exemple q ne soit accessible qu'à partir de q_1 équivaut à l'hypothèse que Q admet une partition $Q = Q_1 \cup Q_2$ telle que, $q, q_1 \in Q_1$, $q_2 \in Q_2$ et $v\mu_{q'',q'} = \emptyset$ pour tout $v \in A^*$, $q' \in Q_1$, $q'' \in Q_2$. Par induction on en déduit l'existence d'une partition finie $Q = \Sigma\, Q_i$ ayant les deux propriétés suivantes :

(a) aucun état de Q_i n'est accessible à partir d'un état d'un Q_j où $j > i$;

(b) la restrction μ_{ij} de μ a chaque $Q_i \times Q_j$ n'admet aucun branchement fort.

La première de celles-ci entraîne comme on le sait l'existence d'une décomposition polynomiale non ambigue de A^* telle que chaque $X_{i,j}$ soit le domaine d'un $\mu_{i,j}$; la seconde que chacun des $\mu_{i,j}$ soit sous-séquentiel. Ceci achève la preuve et marque le point d'orgue où je remercie Dominique qui a su retenir votre très patiente attention.

[1] C. Choffrut et M.P. Schützenberger, Décomposition des fonctions rationnelles, 3rd STACS, Lecture Notes in Computer Science **210** (1986) 213-226.