femmes & mathématiques

Forum des jeunes mathématiciennes et des jeunes informaticiennes

Institut Henri Poincaré, Paris, vendredi 8 et samedi 9 mars 2002

6ème Forum

Résumés des exposés présentés par les jeunes mathématiciennes et des jeunes informaticiennes

Avec le soutien de :

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

Société Mathématique de France SMF

SMAI

specif

FEMMES & SCIENCES association

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

#

Sommaire

Comportement à distance finie des tests fondés sur les graphes PP

Naïma Bessah

Résumé : Désignons par F_m et G_n les fonctions de répartition empiriques de deux échantillons indépendants de tailles respectives m et n et soient F_m^{-1} et G_n^{-1} les fonctions quantiles empiriques correspondantes. La statistique de test de Bahadur Kiefer est définie par :

$$BK(F_m,G_n) = Sup_{0<s<1} \left| F_m G_n^{-1}(s) + G_n F_m^{-1}(s) - 2s \right|$$

Nous nous intéressons à la comparaison de ce test avec le test classique de Kolmogorov- Smirnov, par une approche finie et sous l'hypothèse de contiguité des distributions.

Introduction: Les tests d'hypothèses (ou tests statistiques) nous permettent de décider si une hypothèse (appelée hypothèse nulle et notée H_0) est acceptée ou rejetée avec un taux d'erreur α.
Parmi ces tests, celui de Kolmogorov Smirnov à deux échantillons nous permet de décider si deux échantillons indépendants provenant de deux populations différentes ont même fonction de distribution ou pas.
Le but de cette étude est d'introduire le test de Bahadur Kiefer et de le comparer au test de Kolmogorov Smirnov.

Définitions: Soient X_1,X_2,...,X_m et Y_1,Y_2,...Y_n deux échantillons indépendants de lois respectives F et G inconnues
Les fonctions de répartition empiriques sont définies par

$$F_m(x) = \frac{1}{m}\#\{1 \leq i \leq m, X_i \leq x\} \text{ et } G_n(y) = \frac{1}{n}\#\{1 \leq i \leq n, Y_i \leq y\}$$

le symbole # désigne le cardinal de l'ensemble.
Les fonctions inverses sont appelées fonctions empiriques quantiles et définies par : $F_m^{-1}(s) = inf\ \{x, F_m(x) \geq s\}$ et $G_n^{-1}(s) = inf\{y, G_n(y) \geq s\ \}$ *pour* $0 \leq s \leq 1$ **Notation :** On pose $N = \frac{mn}{m+n}$

Le processus P-P plot empirique de F contre G est défini par :

$$A_{mn}(s) = N^{1/2} \left(F_m(G_n^{-1}(s)) - F(G^{-1}(s)) \right)$$

Sous l'hypothèse nulle d'égalité des deux distributions : $H_0 : F = G$,

$$A_{mn}(s) = N^{1/2} \left(F_m(G_n^{-1}(s)) - s \right)$$

Remarque : La statistique de test de Kolmogorov Smirnov est définie par

$$\| \left(F_m(G_n^{-1}(s)) - s\right) \| = \sup_{0<s<1} | \left(F_m(G_n^{-1}(s)) - s\right) |$$

Le processus de type Bahadur Kiefer à deux échantillons est fondé sur les graphes P-P; il est défini par :

$$R_{mn} = \sqrt{N} \{F_m(G_n^{-1}(s) + G_n(F_m^{-1}(s) - 2s\}$$

Théorème (P.DEHEUVELS et D.M MASON 1990b)
Supposons que $F = G$ *est continue et que* $m \longrightarrow \infty$ *et* $n \longrightarrow \infty$. *Alors* $N^{1/4}(\log(N))^{-1/2} \| R_{mn} \| \longrightarrow_d \| B \|^{1/2}$
où B *désigne un pont brownien et* $\| f \| = \sup_{0\leq x\leq 1} | f(x) |$

La statistique de test de Bahadur Kiefer est définie par $\| F_m(G_n^{-1}(s) + G_n(F_m^{-1}(s) - 2s \|$, sa loi est donc connue d'aprés le théorème précédent .

Niveau de signification d'un test : Un niveau de signification, noté α,est la probabilité maximum de rejeter une hypothèse nulle vraie.
L' hypothèse nulle d'égalité des deux distributions $H_0 : F = G$ est rejetée au niveau de signification α pour chacun des tests si

$$P(\| \left(F_m(G_n^{-1}(s)) - s\right) \| > c_1) = P(\| F_m(G_n^{-1}(s) + G_n(F_m^{-1}(s) - 2s\| > c_2) = \alpha$$

$$c_1 = k_\alpha N^{-1/2} \;\; et \; c_2 = \sqrt{k_\alpha} N^{-3/4} (LogN)^{1/2}$$

La valeur de k_α est lue sur la table de Kolmogorov Smirnov pour α donné (par exemple $\alpha = 0.05$ $k_\alpha = 1.36$)

Puissance d'un test
Définition La puissance d'un test, notée β , est la probabilité de rejeter une hypothèse nulle fausse.

Comparaison des deux tests : On a comparé les puissances β_{KS} et β_{BK}, obtenues par simulation, des deux tests de Kolmogorov Smirnov et de Bahadur Kiefer respectivement; on s'est interessé, en particulier au cas où la loi de F est uniforme sur [0,1] et au cas où la loi est gaussienne, l'alternative G sera contigue à F par translation, dilatation ou contamination pour des tailles d'éechantillons égales ($n = m = 200$) ou différentes ($m = 100$ *et* $n = 80$)

Quelques résultats de simulation

Tableau 1 : $n = m = 200 F\tilde{}U[0,1]$ et $G\tilde{}U[a_m, 1 - a_m]$

a_m	β_{KS}	β_{BK}	β_{BK}/β_{KS}
$\frac{1}{3\sqrt{m}}$	0.044 [0.035,0.053]	0.0475 [0.038,0.0056]	1.067
$\frac{2}{3\sqrt{m}}$	0.0545 [0.044,0.064]	0.146 [0.13,0.161]	2.67
$\frac{5}{6\sqrt{m}}$	0.084 [0.071,0.096]	0.343 [0.322,0.364]	4.08
$\frac{1}{\sqrt{m}}$	0.136 [0.121,0.151]	0.629 [0.607,0.65]	4.62
$\frac{4}{3\sqrt{m}}$	0.321 [0.3,0.34]	0.963 [0.955,0.971]	3
$\frac{2}{\sqrt{m}}$	0.946 [0.93,0.95]	1	1.05

Tableau 2: $n = m = 200 F\tilde{}N[0,1]$ et $G\tilde{}N[a_m, 1]$

a_m	β_{KS}	β_{BK}	β_{BK}/β_{KS}
$\frac{1}{2\sqrt{m}}$	0.048 [0.039,0.057]	0.051 [0.041,0.06]	1.05
$\frac{1}{\sqrt{m}}$	0.0725 [0.061,0.083]	0.0605 [0.05,0.07]	0.83
$\frac{3}{2\sqrt{m}}$	0.13 [0.115,0.144]	0.097 [0.08,0.109]	0.74
$\frac{2}{\sqrt{m}}$	0.194 [0.177,0.211]	0.153 [0.137,0.169]	0.78
$\frac{3}{\sqrt{m}}$	0.396 [0.374,0.417]	0.292 [0.272,0.311]	0.73
$\frac{6}{\sqrt{m}}$	0.943 [0.93,0.95]	0.835 [0.81,0.85]	0.88

Tableau 3 : $n = 80$, $m = 200$ $F\tilde{}U[0,1]$ et $G\tilde{}U[a_m, 1 - a_m]$

a_m	β_{KS}	β_{BK}	β_{BK}/β_{KS}
$\frac{1}{2\sqrt{m}}$	0.059 [0.049,0.069]	0.077 [0.065,0.088]	1.3
$\frac{1}{\sqrt{m}}$	0.131 [0.116,0.145]	0.446 [0.424,0.468]	3.4
$\frac{3}{2\sqrt{m}}$	0.489 [0.467,0.51]	0.946 [0.936,0.955]	1.93

Conclusion: Selon les situations de l'alternative, le test de Bahadur Kiefer peut s'averer meilleur que le test de Kolmogorov Smirnov, le rapport des puissances des deux tests peut dépasser 3 dans diverses situations en faveur du test de Bahadur Kiefer, il y'a néanmoins quelques cas où le rapport se montre légèrement inférieur à 1.

Références

[1] J. BEIRLANT, P. DEHEUVELS, *On the approximation of P-P and the Q-Q plot processes by brownian bridges, Statistics and Probability letters,9, 1990, pp 241-251*

[2] M. CSORGO, P REVESZ, *Strong approximation in probability and Statistics, Academic Press, New York., 1981*

[3] P. DEHEUVELS, D-M MASON, *A Bahadur-Kiefer-type two sample statstic with applications to tests of goodness of fit., Coll. Math.. Soc. Janos Bolayai, 57, 1990b, pp 157-172.*

[4] P. DEHEUVELS, D-M MASON ,*Bahadur-Kiefer type processes, Annals of Probability, 18, 1990a, pp 669-697.*

[5] J. HAJECK, Z. SIDAK, *Theory of rank tests, Academic Press, New York.*

Naïma BESSAH
Institut d'informatique BP. 68M
Oued Smar, 16270, Alger, Algérie
n_bessah@yahoo.fr

Introduction à l'arithmétique des ordinateurs

Sylvie Boldo

Introduction

La puissance de nos ordinateurs augmente chaque mois et on peut paralléliser un même programme sur plusieurs ordinateurs. Tout cela permet de faire des calculs de plus en plus compliqués mais on peut s'interroger sur la validité du résultat de tels calculs [2].

De retentissants échecs tels que le bug du Pentium ou l'explosion d'Ariane 5 ont démontré qu'il ne fallait pas croire aveuglément aux résultats d'un calcul sur ordinateur. L'ordinateur ne peut calculer parfaitement et le résultat fourni ne doit pas être pris comme parole d'évangile.

En effet, l'ordinateur n'a qu'une mémoire finie. Il ne peut donc pas manipuler des nombres réels infiniment précis mais ce qu'on appelle des nombres à virgule flottante.

1 Les nombres à virgule flottante

En machine, un nombre à virgule flottante n'est qu'une suite de bits (0 ou 1). Ces bits se répartissent en 3 champs : le signe, la fraction et l'exposant comme montré en figure 1.

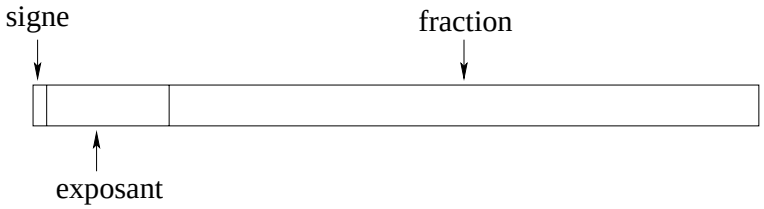


FIG. 1 – *Les champs d'un nombre à virgule flottante*

La plupart des processeurs actuels respectent la norme IEEE-754 [7] qui impose notamment deux formats de nombres à virgule flottante appelés simple et double précision. Un nombre en simple précision est composé de 32 bits : 1 pour le signe, 23 pour la fraction et 8 pour l'exposant. Un nombre en

simple précision est composé de 64 bits : 1 pour le signe, 52 pour la fraction et 11 pour l'exposant.

Notons s le signe, E l'exposant et $f = b_1 b_1 \dots b_p$ la fraction du nombre à virgule flottante avec $b_i = 0$ ou 1. L'exposant est biaisé, ce qui signifie que le vrai exposant e vaut $E + biais$. Sauf cas particuliers, la valeur du nombre à virgule flottante est alors $(-1)^s \times 1.f \times 2^e$ où $1.f = 1 + \sum_{i=1}^{p} b_i 2^{-i}$.

En plus de tels nombres (dits normalisés), on peut représenter des nombres plus petits (dits dénormalisés), $\pm\infty$, ± 0 et NaN. Les deux zéros assurent une cohérence des signes de l'inverse : $\frac{1}{+0} = +\infty$ et $\frac{1}{-0} = -\infty$. NaN, qui signifie *Not A Number*, est le résultat d'opérations telles que $\sqrt{-1}$, $\infty - \infty$, $\frac{\infty}{\infty} \dots$

Comme le résultat exact d'une opération ne peut pas forcément tenir dans le format voulu, la norme IEEE-754 définit quatre modes d'arrondi. L'arrondi vers $-\infty$ ($\bigtriangledown(x)$) est le nombre à virgule flottante le plus grand inférieur ou égal à x ; l'arrondi vers $+\infty$ ($\bigtriangleup(x)$) est le plus petit supérieur ou égal à x ; l'arrondi vers 0 ou troncature ($\mathcal{Z}(x)$) vaut $\bigtriangledown(x)$ si $x \geq 0$ et $\bigtriangleup(x)$ sinon et l'arrondi au plus proche ($\mathcal{N}(x)$) est le plus proche de x. Si deux nombres à virgule flottante sont à égale distance de x, c'est celui dont la mantisse est paire (qui finit par un 0) qui est choisi.

Pour toutes les opérations de base $(+, -, \times, /, \sqrt{})$, la norme impose que le résultat renvoyé soit le même que si l'on avait calculé avec une précision infinie et arrondi ensuite. On ne peut pas avoir un meilleur résultat qui soit représentable dans le format voulu.

Ces propriétés sont très fortes et permettent de faire des preuves sur les calculs flottants comme en [4]. Néanmoins, bien que l'arrondi soit correct, le résultat n'est pas le résultat mathématique exact, ce qui peut créer des résultats absurdes.

2 Quelques exemples de problèmes

L'algorithme Certains algorithmes ont la particularité d'être stables : si l'on change un peu les données initiales, le résultat ne varie que très peu. Il est préférable d'utiliser ces algorithmes car ils donneront presque à coup sûr un bon résultat une fois implanté.

Le programme Le programmeur peut oublier que certains évènements exceptionnels (appelés exceptions) peuvent se produire. Ce sont par exemple les divisions par zéro ou les dépassements de capacité. Ainsi en double précision, pour $x = 2^{60}$ et $y = 1$, le calcul de $\frac{1}{(x+y)-x}$ fait une division par zéro, ce qui est contraire à l'intuition puisque y est non nul !

Le processeur Si l'unité flottante du processeur présente des dysfonctionnements, il est certain que certains calculs ne donneront pas le bon résultat. Ce fut le cas du fameux "bug du Pentium" où certaines divisions n'étaient pas précises du tout.

3 Quelques solutions

Les solutions sont nombreuses [1] et parfois originales comme l'utilisation d'un arrondi aléatoire. Voici quelques autres possibilités.

Certains problèmes sont irréparables : en effet, si l'unité flottante ne donne pas le bon résultat, il n'y a pas grand-chose à faire. Une solution est de prouver de façon certifiée que les opérations du processeur sont correctes comme l'ont fait Harrison (Intel) et Russinoff (AMD).

Une solution à beaucoup de problèmes serait de calculer avec plus de précision [3, 6]. Cela permet de retarder les effets néfastes des dépassements de capacité et des algorithmes instables.

Une solution utilisée mais coûteuse est le calcul par intervalles [5]. Le résultat est alors un intervalle de nombres à virgule flottante qui contient le résultat exact. Cela se fait par exemple en utilisant les propriétés des modes d'arrondi IEEE-754.

Conclusion

Le résultat d'un calcul numérique complexe sur ordinateur est donc tout-à-fait susceptible d'être faux sans que l'utilisateur en soit prévenu. De nombreuses recherches sont menées pour éviter des désagréments et les réponses sont diverses et originales. Il est donc possible en utilisant certaines techniques d'être sûr du résultat de son calcul.

La tendance actuelle est en effet à la garantie du résultat : on veut pouvoir faire confiance aveuglément à la machine et ne pas se poser de questions,

même si le calcul doit prendre plus de temps. Un moyen de donner des garanties à l'utilisateur est de faire des preuves mais ces preuves sont sujettes à l'erreur et ne peuvent donc être totalement rassurantes. On peut alors faire vérifier ces preuves par des assistants de preuves qui vérifieront chaque cas et chaque détail de la preuve avant de l'accepter. On a alors une garantie nettement plus forte du résultat.

Références

[1] *Marc Daumas et Jean-Michel Muller (éditeurs)*, Qualité des calculs sur ordinateur : vers des arithmétiques plus fiables. Masson (1997)

[2] *David Goldberg*, What every computer scientist should know about floating point arithmetic. ACM Computing Surveys (1991)

[3] *Guillaume Hanrot, Vincent Lefèvre, Fabrice Rouillier et Paul Zimmermann*, The MPFR library. `www.mpfr.org`. Version 2001.

[4] *Michèle Pichat*, Contributions à l'etude des erreurs d'arrondi en arithmétique à virgule flottante. Thèse (1976)

[5] *Nathalie Revol et Fabrice Rouillier*, The MPFI library. version 2001, `http://www.ens-lyon.fr/~nrevol`. (2001)

[6] *Jonathan R. Shewchuk*, Adaptive Precision Floating-Point Arithmetic and Fast Robust Geometric Predicates. Discrete and Computational Geometry (1997)

[7] *David Stevenson et al.*, IEEE Standard for Binary Floating-Point Arithmetic. ANSI/IEEE (1985)

Sylvie Boldo
Laboratoire de l'Informatique du Parallélisme
UMR 5668 CNRS-INRIA-ENS Lyon
École Normale Supérieure de Lyon
46, Allée d'Italie
69364 Lyon Cedex 07
France
`Sylvie.Boldo@ens-lyon.fr`
http://www.ens-lyon.fr/~sboldo

Des squelettes dans des images 2D et dans des surfaces discrètes

Jasmine Burguet

1 Introduction

La géométrie discrète, c'est-à-dire l'étude de propriétés géométriques et topologiques d'un ensemble discret, connait de nombreuses applications en informatique notamment. Par exemple, en imagerie, une image 2D binaire est composée de pixels (pour **pic**ture **el**ement), c'est-à-dire d'unités discrètes. De plus, l'utilisation de nombres entiers supprime les problèmes d'approximation des calculs en flottants et le temps nécessaire pour les effectuer est réduit. En pratique, on peut par exemple citer le projet de navigation dans le corps humain Visible Human (http://visible-human.epfl.ch) qui utilise une structure de stockage et des calculs discrets.

Nous allons nous intéresser plus particulièrement à la notion de *squelettisation*, introduite dans [1]. En reconnaissance et analyse de forme, plutôt que de travailler sur un ensemble discret X de grande taille, il est parfois plus pratique de s'intéresser seulement à un sous-ensemble de X qui a les mêmes propriétés topologiques et une forme similaire. On appellera ce sous-ensemble *squelette de X*.

2 Quelques notions de base

Dans la suite, on considère un ensemble X de $\mathbb{Z}^2$ que l'on identifie à un ensemble de *pixels* représenté par des carrés unitaires centrés sur leurs coordonnées entières. On note $\overline{X}$ le complémentaire de X dans $\mathbb{Z}^2$. On définit des adjacences sur les pixels : deux pixels sont dits *4-adjacents* s'ils partagent une arête et *8-adjacents* s'ils partagent une arête ou un sommet. On pose $n \in \{4,8\}$. On en déduit les notions de *n-voisinage* d'un pixel (Figure 2), noté $N_n(x)$ (l'ensemble des pixels qui lui sont n-adjacents), et de *n-chemins* (Figure 3, un 4-chemin en gris foncé et un 8-chemin en gris clair).

Soient x,$y \in X$. On dit que x et y sont n-connectés si il existe un n-chemin dans X joignant x à y. Cette relation est une relation d'équivalence sur les pixels de X dont les composantes n-connexes sont les classes d'équivalence.

FIG. 2 – *Les voisinages d'un pixel noir*

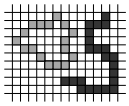


FIG. 3 – *Deux chemins de pixels*

Sur la Figure 4, l'ensemble gris est composé de deux composantes 8-connexes et de trois composantes 4-connexes.

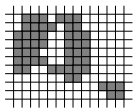


FIG. 4 – *Composantes n-connexes*

Un squelette S de X est un sous-ensemble de X qui en est représentatif. Par là on entend d'abord représentatif de la topologie de E : on doit conserver le nombre de composantes connexes de X et le nombre de "trous" dans X (les composantes connexes de $\overline{X}$). La méthode de squelettisation d'un ensemble repose sur la notion suivante :

Définition 1 : Soient $x \in X$. Le pixel x est dit **n-simple dans** X si sa suppression de X ne modifie pas la topologie de X.

Sur la Figure 5, les pixels p_1 et p_2 sont simples dans l'ensemble gris, ce qui n'est pas le cas de p_3 (suppression d'une composante connexe de $\overline{X}$), de p_4 (création d'une composante connexe de $\overline{X}$) et de p_5 (suppression d'une composante connexe de X).

Définition 2 : Soit $Y \subset X$. On dit que Y est **n-homotope à** X si et seulement si Y peut être obtenu à partir de X par une suppression *séquentielle* de pixels n-simples.

On peut visualiser sur la Figure 6 deux exemples d'ensembles homotopes ou pas.

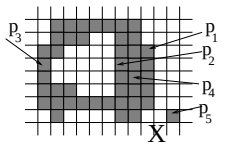


FIG. 5 – *Pixels simples?*

Homotopes Non homotopes

FIG. 6 – *Ensembles homotopes?*

FIG. 7 – *Un squelette décentré*

FIG. 8 – *De meilleurs résultats*

3 Des algorithmes plus ou moins efficaces

Afin de définir un algorithme efficace de squelettisation, il faut pouvoir caractériser *localement* la notion de pixel simple. Tout d'abord, un pixel est dit *n-intérieur* à X s'il n'a pas de n-voisin dans $\overline{X}$. Alors on a :

Proposition 1 : Soit $x \in X$. Alors x est n-simple dans X si et seulement si il n'est pas n-intérieur à X et si le nombre de composantes n-connexes de $X \cap N_8(x)$ qui sont n-adjacentes à x est égal à 1.

Cette caractérisation est locale puisqu'elle n'intervient que sur le voisinage d'un pixel. Nous pouvons alors définir des algorithmes de squelettisation. La première idée est de tester séquentiellement la simplicité des pixels et, le cas échéant, de les supprimer jusqu'à ce qu'il ne reste plus aucun pixel simple. Mais l'ordre de test des pixels influence sensiblement la forme des squelettes obtenus (Figure 7, où on applique un ordre lexicographique). Une première amélioration consiste alors à faire une liste du bord de l'ensemble, de supprimer les pixels simples de la liste, puis de recommencer avec le nouveau bord (Figure 8).

Mais la méthode dont les résultats sont les plus satisfaisants est directionnelle. On définit d'abord les pixels *Nord* (respectivement Sud, Est, Ouest) comme étant les pixels de X dont le 4-voisin au nord est dans $\overline{X}$. On considère alors successivement chaque direction $D \in \{$ Nord, Sud, Est, Ouest$\}$, on supprime séquentiellement les pixels D simples, puis on recommence jusqu'à ce

qu'il n'y ait plus de pixel supprimable (Figure 9).

FIG. 9 – *Composantes n-connexes*

Maintenant, on désire conserver la forme générale de X. Pour ce faire, afin de conserver les branches significatives de X, on impose à certains pixels d'être insupprimables : les pixels de X qui n'ont qu'un seul voisin dans X. On obtient alors des squelettes satisfaisants (Figures 10 et 11).

4 Surfaces discrètes et squelettes

Le calcul de squelettes dans les images binaires 2D est un processus maintenant bien connu. En 3D, il exite un analogue du pixel 2D que l'on appelle *voxel* (pour **vo**lume **el**ement), représenté par un cube unitaire centré sur ses coordonnées dans $\mathbb{Z}^3$. Ainsi, un objet 3D discret O est un ensemble fini de voxels, dont la surface est composée de petits carrés, les *surfels* (pour **surf**ace **el**ement), qui sont les faces des voxels "en contact" avec le complémentaire de O dans $\mathbb{Z}^3$. Des méthodes de squelettisation sur des ensembles inclus dans les surfaces des objets discrets 3D ont été définies (Figures 12). Une application de tel squelettes est présentée dans [2].

FIG. 10 – *Un squelette trop simple.*

FIG. 11 – *Un squelette correct.*

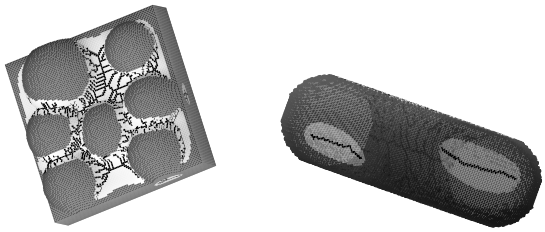


FIG. 12 – *Squelettes dans des surfaces discrètes.*

Références

[1] *J. Blum*, A transformation for extracting new descriptors or shape. W. WATHEN-DUNN ed., Symposium models for the perception of speech and visual form (1967).

[2] *J. Burguet, R. Malgouyres*, Strong Thinning and Polyhedric Approximation of the Surface of a Voxel Object. A paraître dans Discrete Applied Mathmatics.

Jasmine Burguet
LLAIC1
IUT Département Informatique
BP 86
63172 Aubière CEDEX
France
`burguet@llaic.u-clermont1.fr`
http://llaic3.u-clermont1.fr/ burguet

Amélioration de la forme de Horner
pour l'évaluation des polynômes univariés sur les intervalles

Martine Ceberio

1 Introduction

La puissance des ordinateurs rend possibles des calculs toujours plus lourds. Cependant, seul un nombre fini de valeurs reste représentable en machine. Aussi les quantités calculées résultent souvent d'arrondis qui peuvent conduire à des erreurs tragiques. Afin de prendre en compte ces arrondis, Ramon E. Moore [3] a introduit, à la fin des années 60, l'Arithmétique des Intervalles (AI). Celle-ci est définie sur des ensembles de nombres appelés intervalles, modélisant ainsi l'incertitude et gérant les erreurs d'arrondis.

Cependant, l'AI présente des points faibles, dont le problème de dépendance, lié à la décorrélation des variables durant l'évaluation. Cela se traduit par la surestimation de la quantité réelle recherchée, et par le fait que deux expressions équivalentes sur les réels ne le sont pas forcément sur les intervalles. Pour cette raison, nous nous intéressons à rechercher une expression dont l'évaluation s'approche le plus de la quantité réelle recherchée. En particulier, nous rappelons le schéma de factorisation de Horner et nous proposons ensuite une nouvelle forme qui améliore Horner de 27% en moyenne.

2 Notions préliminaires sur les intervalles

Définition 1 : Un **intervalle (réel fermé)** $\boldsymbol{x}$ est un ensemble défini par :

$$\boldsymbol{x} = [\underline{x},\overline{x}] = \{x \in \mathbb{R} \mid \underline{x} \leq x \leq \overline{x}\}, \text{ où } \underline{x} = \inf \boldsymbol{x} \in \mathbb{R},\ \overline{x} = \sup \boldsymbol{x} \in \mathbb{R}$$

Afin de pouvoir représenter tous les intervalles fermés, les infinis $\{^{+}_{-}\infty\}$ sont adjoints à $\mathbb{R}$. Soit $\boldsymbol{x} \in \mathbb{IR}$, la largeur de $\boldsymbol{x}$ est $w(\boldsymbol{x}) = \overline{x} - \underline{x}$. Soit $\rho \subset \mathbb{R}$, le plus petit intervalle contenant ρ est donné par $\mathbf{Hull}(\rho) = [\inf \rho, \sup \rho]$.

Les opérations de l'AI sont des extensions aux ensembles des opérations correspondantes sur les réels. Soient les intervalles $\boldsymbol{x},\boldsymbol{y} \in \mathbb{IR}$ et une opération $\Diamond \in \{+, -, \times, \div\}$, on a : $\boldsymbol{x} \Diamond \boldsymbol{y} = \mathbf{Hull}(\{x \Diamond y \mid (x,y) \in \boldsymbol{x} \times \boldsymbol{y}\})$. Par exemple, l'addition de $\boldsymbol{x} = [a,b]$ et $\boldsymbol{y} = [c,d]$ vaut $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y} = [a + c, b + d]$.

Les lois d'associativité et de commutativité sont préservées sur $\mathbb{R}$, mais l'AI implique aussi des comportements indésirables. Par exemple, l'évaluation de $(\boldsymbol{x} - \boldsymbol{x})$ sur $\boldsymbol{x} = [-1,1]$ vaut $[-2,2]$, alors que $\forall x \in \mathbb{R}$, $(x - x) = 0$. La sous-distributivité remplace la distributivité et on a désormais pour tous $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z} \in \mathbb{R}$, $\boldsymbol{x} \times (\boldsymbol{y} + \boldsymbol{z}) \subseteq \boldsymbol{x} \times \boldsymbol{y} + \boldsymbol{x} \times \boldsymbol{z}$. Par conséquent, sur les intervalles, les expressions factorisées fournissent des évaluations plus fines. Un des principaux objectifs de l'AI est donc de trouver des formes factorisées qui fournissent des évaluations fines sur les intervalles.

Cependant, en pratique, les réels sont remplacés par les nombres flottants. Soit $\mathbb{F}$ l'ensemble de ces nombres, les seuls représentés en machine [2]. Soit un réel a, a^+ (resp. a^-) est le plus petit (resp. grand) flottant supérieur (resp. inférieur) à a. L'ensemble $\mathbb{IF}$ des intervalles flottants est le sous-ensemble de $\mathbb{IR}$ des intervalles à bornes dans $\mathbb{F}$. La différence entre l'arithmétique sur $\mathbb{IF}$ et sur $\mathbb{IR}$ réside dans le fait que les calculs sur $\mathbb{IF}$ nécessitent d'être arrondis. On arrondit les bornes inf. $\underline{x}$ à $\underline{x}^-$, et les bornes sup. $\overline{x}$ à $\overline{x}^+$: on est ainsi assuré de toujours contenir la quantité réelle recherchée.

3 Le schéma de factorisation de Horner

La forme de Horner d'un polynôme $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ est définie par :

$$h_p(x) = (\dots(a_mx + a_{m-1})x + \cdots)\,x + a_0$$

Le schéma de factorisation de Horner [1] fournit un algorithme efficace pour l'évaluation sur les intervalles. Il est en effet constitué d'une séquence de multiplications de polynômes dit intermédiaires

$$\left\{ \begin{array}{lcll} p_m(x) & = & a_m & \\ p_i(x) & = & xp_{i+1}(x) + a_i & i = m-1,m-2,\dots,0 \end{array} \right.$$

Soit O_p le plus petit intervalle contenant 0 et l'ensemble des zéros des polynômes intermédiaires. Lorsque h_p est évaluée en dehors de O_p, Stahl [4] a montré qu'aucune surestimation n'est observée par rapport à la variation exacte de p sur les réels. En effet, l'évaluation des multiplications par l'AI en dehors de O_p s'effectuant sur les bornes des intervalles et en dehors des zéros, les monotonies sont respectées. Cependant, lorsque h_p est évaluée sur un intervalle intersectant O_p, les monotonies n'étant plus nécessairement respectées, la forme de Horner entraîne des surestimations mal contrôlées. Pour cette raison, nous proposons un nouveau schéma de factorisation.

4 Un nouveau schéma de factorisation

Les problèmes de la forme de Horner sont dus à la décomposition aveugle des puissances. En effet, seule la décomposition de puissances paires en puissances paires permet sous certaines conditions l'évaluation sur des intervalles intersectant O_p sans surestimation. Or d'autres décompositions interviennent et impliquent une surestimation. En particulier l'introduction de puissances impaires entraîne systématiquement une surestimation. Nous proposons donc un nouveau schéma de factorisation qui interdit la décomposition en puissances impaires et limite leur nombre, tout en favorisant les puissances paires.

La forme factorisée que nous proposons est basée sur la reconnaissance d'identités remarquables, c'est-à-dire sur le schéma suivant :

$$ax^\alpha + bx^{\alpha+\beta} \rightsquigarrow bx^{\alpha-\beta}\left[\left(x^\beta + \frac{a}{2b}\right)^2 - \left(\frac{a}{2b}\right)^2\right]$$

où $\alpha > \beta \in \mathbb{N}$ sont de même parité. Ainsi, même si β est impair, la forme factorisée ne contient globalement que des puissances paires.

Notons de plus que ce schéma ne concerne que des couples de puissances. Or, dans une expression polynomiale quelconque, il existe donc un nombre combinatoire de possibilités d'application de ce schéma. De nombreuses stratégies sont donc possibles, parmi lesquelles :

- favoriser les schémas tels que α est impair et β minimum,
- favoriser les schémas tels que $\alpha = \beta$.

De plus chaque stratégie peut être combinée avec la forme de Horner afin d'éviter les puissances orphelines, et/ou de gérer les expressions polynomiales ne contenant aucun schéma remarquable.

Quatre stratégies sont retenues pour être testées. Pour déterminer quelle stratégie est la meilleure, des tests comparatifs sont effectués entre les différentes stratégies et la forme de Horner seule sur un échantillon de 500 expressions polynomiales générées aléatoirement. Chaque expression polynomiale est ainsi évaluée sur un intervalle contenant 0, c'est-à-dire intersectant nécessairement O_p. La stratégie qui s'avère être la plus efficace, notée $h \circ s_0$, est celle qui :

- favorise les schémas tels que α est impair et β minimum,
- et est composée avec Horner.

En moyenne, on note une amélioration de 27% par rapport à la largeur de l'évaluation des formes de Horner seules. D'autre part, des tests analogues

sont réalisés avec des évaluations en dehors de O_p, et on constate que $h \circ s_0$ y est équivalente à Horner. Ce résultat est d'autant plus intéressant que de nombreuses techniques numériques utilisent les développements en séries de Taylor, qui sont pour l'essentiel des polynômes.

5 Conclusion

Les points faibles de Horner sont éliminés. Sous les conditions de Stahl, Horner comme notre méthode fournissent la variation exacte. En dehors de ces conditions, notre stratégie améliore Horner.

Tout d'abord, notre méthode se restreint aux polynômes. Or les expressions non-polynomiales peuvent être traitées par les développements de Taylor. On peut imaginer combiner les deux approches. Notre schéma pourrait ensuite être étendu aux fonctions trigonométriques. Enfin, un schéma est également nécessaire pour traiter les expressions multivariées.

Références

[1] *William G. Horner* Philosophical Transactions of the Royal Society of London **109** (1819), 308–33

[2] *IEEE*, IEEE Standard for Binary Floating-Point Arithmetic. Technical Report IEEE Std 754-1985(1985)

[3] *Ramon E. Moore*, Interval Analysis. Prentice-Hall, Englewood Cliffs, NJ(1966)

[4] *Volker Stahl*, Interval Methods for Bounding the Range of Polynomials and Solving Systems of Nonlinear Equations. PhD thesis, University of Linz, Austria (1995)

Martine Ceberio
Institut de Recherche en Informatique de Nantes (IRIN)
Faculté des Sciences de Nantes
2 rue de la Houssinière – BP 92208
44322 Nantes Cedex 3
France
`ceberio@irin.univ-nantes.fr`
http://www.sciences.univ-nantes.fr/info/permanents/ceberio

La maïeutique des destinées
ou comment accoucher de nouveaux problèmes ouverts

Annie Chateau

1 Introduction

Lorsqu'en 1900 Hilbert proposa sa liste de 23 problèmes ouverts, on peut presque dire qu'il faisait avancer la recherche en mathématiques davantage que s'il avait proposé 23 réponses à des problèmes déjà posés. En effet la pratique mathématique ne consiste pas seulement en la résolution de problèmes, vision simpliste suggérée hélas par la pratique scolaire, mais aussi en l'"art de poser les bonnes questions". Nous nous proposons de regarder l'aspect "génératrices de problèmes" des destinées de Francis Nézondet ([4]). Si le cadre choisi reste restreint aux problèmes formalisables en arithmétique, nul doute qu'une généralisation à toute une foule de domaines est possible.

Nous présentons dans un premier temps les destinées, puis quelques exemples de problèmes arithmétiques que leur étude a fait naître, et enfin nous nous interrogeons sur une possible classification des problèmes, induite par une façon de penser "en destinées".

2 Qu'est-ce que les destinées ?

On commence par se donner un langage relationnel fini, et un domaine. Par exemple, nous allons considérer la structure $\mathbb{N}$ (entiers naturels), munie de deux prédicats binaires $\perp$ et $<$, interprétés respectivement par "être premiers entre eux" et l'ordre strict usuel sur les entiers.

Une p-destinée est un arbre dont les branches sont toutes de hauteur p, et dont les nœuds sont des éléments de la structure. L'ensemble des p-destinées de cette structure représente un modèle particulier de l'ensemble des formules du langage choisi satisfaisant aux deux conditions suivantes : elles sont vraies dans le domaine, et elles ont une profondeur de quantification inférieure ou égale à p. La profondeur de quantification d'une formule est définie par induction sur la structure de la formule comme suit :

Définition 1 : La profondeur de quantification d'une formule F, notée $q(F)$, est définie par :

- si F est atomique, alors $q(F) = 0$;
- si $F = \neg G$, alors $q(F) = q(g)$;
- si $F = G \wedge H$ ou $F = G \vee H$, alors $q(F) = \max(q(G),q(H))$;
- si $F = QxG(x)$ où Q est un quantificateur $\forall$ ou $\exists$, alors $q(F) = q(G)+1$.

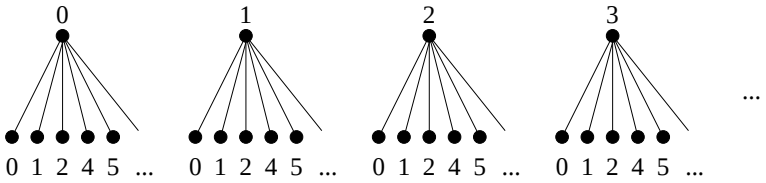
Pour construire les p-destinées d'une structure $\mathcal{X}$ sur le domaine X et le langage relationnel fini $\mathcal{L}$, on procède en trois étapes :

Première étape : Construction d'une forêt exhaustive

On considère la forêt d'arbres construits de la façon suivante :

- Tout élément de $\mathcal{X}$ est racine de l'un de ces arbres;
- Tout nœud soit est une feuille, soit a pour fils tous les éléments de $\mathcal{X}$;
- Toutes les branches sont de hauteur p.

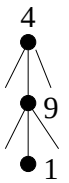
Exemple : Forêt exhaustive de hauteur 2 de la structure $\mathbb{N}$:



Deuxième étape : Constitution des listes de relations

A chaque nœud on associe la liste des relations qu'il vérifie avec ses ancêtres (lui y compris).

Exemple :



$4 \not< 4$

$9 \not< 9$, $9 \perp 4$, $9 > 4$

$1 \perp 1$, $1 \perp 9$, $1 < 9$
$1 \perp 4$, $1 < 4$

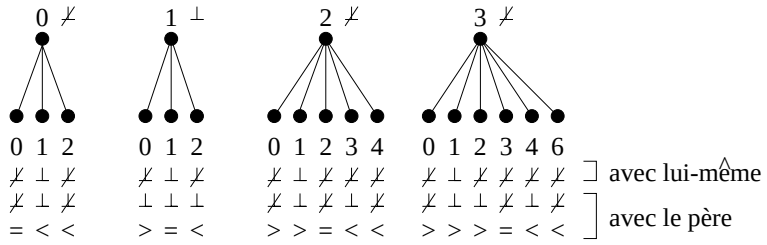
On obtient alors des **destinées exhaustives** portant comme information tous les cas possibles exprimables avec moins de p quantifications. Il reste un problème : l'information est présente à plusieurs reprises (et les arbres sont infinis).

Troisième étape : élimination des redondances

On réalise des simplifications en partant des feuilles : dans chaque sous-arbre de hauteur 2, on ne garde qu'une feuille de chaque classe d'isomorphisme entre les feuilles, puis dans chaque sous-arbre de hauteur 3, on ne

garde qu'un représentant de chaque classe d'isomorphisme entre les sous-arbres de hauteur 2, etc. On obtient alors des **destinées essentielles**. Si on réalise enfin une simplification en ne gardant dans la forêt qu'une seule destinées par classe d'isomorphisme entre les destinées, on obtient une **p-transversale**.

Exemple : Une p-transversale de hauteur 2 de la structure $\langle \mathbb{N}, \perp , < \rangle$:



Une définition plus formelle des destinées peut être trouvée dans [1] ou [2]. Une p-transversale résume l'ensemble des formules de profondeur de quantification inférieure ou égale à p qui sont vraies dans la structure choisie. Construire la p-transversale revient donc à connaître cet ensemble. On peut de plus en déduire un algorithme de vérification pour les formules de profondeur de quantification inférieure ou égale à p (voir [2]).

3 Une usine à problèmes

3.1 L'exemple déclencheur

Les premières destinées qui ont été construites étaient aussi simples que l'exemple présenté ci-dessus avec $\langle \mathbb{N}, \perp , < \rangle$ et une profondeur 2. C'est en cherchant un exemple de destinées moins trivial que Marcel Guillaume, Denis Richard et Ji Lei Yin se sont attaqués à l'étude des 3-destinées de $\mathbb{N}$ muni du successeur et de la coprimarité. Cette étude, détaillée dans [3], commence par l'établissement de "schemas possibles de destinées", en étudiant les propriétés relatives de $\perp$ et S (par exemple un nombre est toujours premier avec son successeur), puis se prolonge par la recherche soit d'exemples satisfaisant à ces schemas, soit de preuves de leur inexistence. On aboutit ainsi à cinq problèmes ouverts correspondant à cinq destinées "possibles" mais dont on ne sait pas si elles existent (et par ailleurs à 51 destinées distinctes dont l'existence est avérée par la présence d'un exemple). Le plus simple de ces problèmes se formule ainsi : "Existe-t-il un entier impair n congru à 2 modulo

3, de la forme $2^a + 1$, dont le nombre de facteurs premiers est 3 ou plus et tel que l'ordre de l'un de ces facteurs modulo un autre est toujours impair ?".

3.2 Autres exemples

Dans certains cas, on sait construire automatiquement les p-transversales pour tout p (par exemple, c'est le cas de $\langle \mathbb{N}, < \rangle$ ou des structures H-bornées), mais dans le cas des "constructions à la main", on fait des rencontres intéressantes. Par exemple avec $\langle \mathbb{N}, P, + \rangle$ (où P est le prédicat "être premier"), on tombe sur une généralisation de la conjecture des premiers jumeaux dès la hauteur 3 : "Quelle est la condition sur n pour qu'il existe $k > n$ tel que k, $k + n$ et $k - n$ soient premiers ?". De même on tombe sur la conjecture de Golbach en construisant cette même 3-transversale. Si l'on arrive à construire cette 3-transversale, on résout du même coup toutes ces conjectures. Ce n'est évidemment pas une chose facile !

4 Vers une classification

Si l'on renverse le point de vue, on peut essayer d'estimer la difficulté d'un problème grâce à la hauteur de la p-transversale qu'il faudrait construire pour le résoudre. Cela revient à classifier les problèmes ouverts selon la profondeur de quantification minimale d'une formule les exprimant. C'est évidemment un peu réducteur, mais il n'est pas impossible de combiner cela avec des mesures intrinsèques aux destinées, par exemple le degré d'une transversale, défini comme étant la plus grande racine de la p-transversale construite en choisissant les plus petits représentants des classes d'isomorphisme. Par exemple, la 3-transversale de $\langle \mathbb{N}, S, \perp \rangle$ est de degré au moins $2^{2^{27}} - 1$, tandis que la 3-transversale de $\langle \mathbb{N}, < \rangle$ est de degré 3.

Références

[1] *Annie Chateau*, Les théories du successeur et de la coprimarité, Mémoire de DEA. Actes du LLAIC, vol. VII, (2000-2001).

[2] *Annie Chateau*, Décision des théories à nombre borné de variables sur les langages relationnels finis : un algorithme utilisant les destinées. Colloque Nationale de la Recherche en IUT, Publications de l'Université de Saint-Etienne, (2001).

[3] *Annie Chateau*, Five keys for a decision. preprint, disponible sur la page web `http://llaic3.u-clermont1.fr/~chateau/` .

[4] *Francis Nézondet*, p-destinées et applications à la théorie du successeur et de la coprimarité sur les entiers, Thèse de doctorat. Université d'Auvergne, (juin 1997),

Annie Chateau
LLAIC1
Département Informatique - IUT des Cézeaux
BP 86 - 63172 Aubière Cedex
France
`chateau@llaic3.u-clermont1.fr`
http://llaic3.u-clermont1.fr/~chateau/

Sur les singularités dans le champs complexe des solutions de certaines équations différentielles singulièrement perturbées.

Sadjia Chettab Aït-Mokhtar

Introduction: Dans cette note, nous nous interessons à la localisation, la nature et au mouvement des singularités des solutions d'une équation différentielle singulièrement perturbée dans le champs complexe du type :

$$\epsilon u' = f(x,u,a,\epsilon) \tag{1}$$

où f désigne une fonction analytique à valeurs dans $\mathbb{C}$ et définie sur un voisinage d'un point $(x_0,u_0,a_0,0)$ de $\mathbb{C}^4$, telle que $f(x_0,u_0,a_0,0) = 0$

Ce problème a été posé par J.L. CALLOT [1] dans une prépublication datant de 1992. En utilisant des outils de l'Analyse Non Standard,il a montré dans le cas d'une équation de RICCATI lente-rapide [1] , l'existence d'une solution maximale $u_a \sim x^{\frac{p}{2}}$ dans $]-\dfrac{3\pi}{p+2},\dfrac{3\pi}{p+2}[$ lorsque $|x| \to \infty$ et admettant des lignes de pôles infiniment proches des lignes de Stokes $\arg(x) = \pm\dfrac{3\pi}{p+2}$. De plus il a observé que pour certaines valeurs du paramètre complexe a, ces lignes se déplaçaient ou disparaissaient. Il conjecturait alors que ces valeurs du paramètre sont les singularités logarithmiques de la fonction multiforme dite *"indicatrice des pôles"* qui à toute valeur du paramètre a fait correspondre les affixes des pôles de la solution u_a. Notre travail apporte des éléments de réponse à cette question : Nous allons montrer en utilisant les résultats d'analyse transasymptotique d'O. COSTIN [2], [3] que dans le cas d'une équation de WEBER la conjecture est vraie. L'idée principale est d'associer à toute solution de l'équation une unique solution transsérie, d'introduire dans la solution transsérie une nouvelle variable pour obtenir un développement à double échelle sous la forme: $\sum_{k=0}^{\infty} F_k(\xi)x^{-k}$. Une correspondance entre les singularités de F_0 et celles de la solution est alors établie.

Equation de WEBER : C'est l'équation linéaire du second ordre:

$$v'' = (t^2 - a)v \tag{2}$$

1. $\epsilon^{\frac{p}{2}}u' = x^p - u^2 + \epsilon$ polynôme en x et en ϵ à coefficients analytiques en a

où a est un paramètre complexe. L'équation de Riccati lente-rapide associée à cette équation est:

$$\epsilon u' = z^2 - \epsilon a - u^2 \tag{3}$$

Pour tout paramètre a, il existe une unique solution $u_a \sim -x$ dans $]\frac{-3\pi}{2}, \frac{3\pi}{2}[$ lorsque $|x| \to \infty$. Mais pour a impair, ces solutions gardent le même comportement asymptotique pour tout $x \in V(\infty)$. On montre alors le résultat suivant :

Théorème : Les entiers impairs positifs sont des singularités logarithmique de la fonction *Indicatrice des pôles* associée à l'équation (3).

Solutions transséries et vraies solutions : Par des changements de variables, l'équation (3) se ramène à la forme :

$$y' \;=\; -y - \frac{a}{2x}y + y^2 + \frac{3 - 4a + a^2}{16x^2} \tag{4}$$

Lemme 1 : L'équation(4) admet une unique solution formelle $\tilde{y}_0 = \sum_{r=2}^{\infty} \tilde{y}_{0,r} x^{-r}$

Définition 1(et proposition) : Une solution formelle à un paramètre de (4) comme combinaison de séries de puissances et d'exponentielles est une série de la forme :

$$\tilde{y}(x,C) \;=\; \sum_{k\geq 0} C^k \, e^{-kx} x^{-k\frac{a}{2}} \, \tilde{s}_k(x) \tag{5}$$

où les $\tilde{s}_k$ sont des séries formelles :

$$\left\{ \begin{array}{lcl} \tilde{s}_k & = & \sum_{r=0}^{\infty} \frac{\tilde{y}_{k,r}}{x^r} \\ \tilde{s}_0 & = & \tilde{y}_0 \end{array} \right. \tag{6}$$

Une telle solution existe et est unique pour tout paramètre C dés que la valeur de $\tilde{y}_{1,0}$ est fixée (par exemple égale à 1).

Définition 2: Etant donnée une direction $d \in \mathbb{C}$, on appelle transsérie sur d toute solution formelle à un paramètre (5) qui est telle que si $C \neq 0$ alors $\Re(x) > 0$ sur d.

Ainsi (5) est une *transsérie* sur toute direction d du secteur ouvert défini par:

$$S_{trans} \;=\; \{\, x \in \mathbb{C} \;:\; \text{si} \;\; C \neq 0 \;\; \text{alors} \;\; \Re(x) \;>\; 0 \,\}$$

Définition 3: On appelle lignes antistokes de (5), les deux directions de $\mathbb{C}$,

données par: $i\,\mathbb{R}_+ \quad et \quad -i\,\mathbb{R}_+$
Dans un contexte beaucoup plus général que (4), une sommation de Borel généralisée est définie dans [cost1]. Cet opérateur de sommation noté $\mathcal{LB}$ opère sur toute solution transsérie (5) de (4) dans toute direction d de S_{trans} et produit une vraie solution $y(x,C) = \mathcal{LB}\tilde{y}(x,C)$. Inversement, toute solution y de (**??**) asymptotique à $\tilde{y}_0$ dans une direction d est représentée par $\mathcal{LB}\tilde{y}$, sur d pour une unique $\tilde{y}$.
Développement à double échelle et formation des singularités Pour $\arg(x) > \frac{\pi}{2}$, la transsérie explose parceque e^{-x} devient grand. La divergence de la transsérie révèle un changement dans le comportement des solutions qui habituellemnet développent des singularités dans cette région.
Lorsque x est proche de $i\,\mathbb{R}_+$, la convergence de (5) dépend de la variable: $\xi(x) = Ce^{-x}\,x^{-\frac{a}{2}}$. Mais quand $|x| \to \infty$, tout terme de la forme $C^k e^{-kx} x^{-k\frac{a}{2}} \tilde{y}_{k,0}$ est plus grand que tous les termes de la forme $C^k e^{-kx} x^{-k\frac{a}{2}} \tilde{y}_{k,0} x^{-r}$.
Le terme dominant dans (5) est:

$$y(x) \sim \sum_{k\geq 0} (Ce^{-x}x^{-\frac{a}{2}})^k \tilde{y}_{k,0} = \sum_{k\geq 0} \xi^k(x)\tilde{y}_{k,0} \equiv F_0(\xi(x)) \tag{7}$$

De plus si on tient compte de tous les termes de $\tilde{s}_k$

$$y(x) \sim \sum_{k\geq 0} (Ce^{-x}x^{-\frac{a}{2}})^k \sum_{j=0}^{\infty} x^{-j}\tilde{y}_{k,j} \equiv \sum_{j\geq 0} x^{-j} F_j(\xi(x)) \tag{8}$$

qu'on appelle *développement à double échelle*
A la différence du développement asymptotique classique (donné par le Lemme 1) qui est valide dans tout secteur strict de $\Re(x) > 0$ [4], le développement (8) est valide dans un domaine qui s'étend dans une surface de Riemann appropriée, à des régions où les solutions développent des singularités. Les singularités dont il est question sont liées aux deux directions antistokes $i\,\mathbb{R}_+$ et $-i\,\mathbb{R}_+$, leur localisation dépend de la constante C.
On note par Ξ l'ensemble (fini) des points singuliers dans le ξ-plan de F_0, par $\mathcal{D}$ un ouvert, relativement compact et connexe du recouvrement universel de $\mathbb{C} \setminus \Xi$ et par $\mathcal{D}_x$ la classe d'équivalence (modulo des homotopies) dans $\{|x| > R, \arg(x) \in [-\frac{\pi}{2}+\delta, \frac{\pi}{2}+\delta]\} \setminus \xi^{-1}(\Xi)$ des chemins qui préservent une certaine régularité. Nous avons alors :
Théorème : Supposons que F_0 admet une singularité isolée $\xi_s \in \Xi$, et que la projection de $\mathcal{D}$ à $\mathbb{C}$ contient un voisinage épointé de ξ_s

Alors, si $C \neq 0$, $y(x)$ est singulière à une distance au plus $o(1)$ de $x_n \in \xi^{-1}(\xi_s) \cap \mathcal{D}_x$, lorsque $x_n \to \infty$
Les x_n sont donnés par:

$$x_n \;=\; 2n\pi\imath - \beta \ln(2n\pi\imath) + \ln(C) - \ln(\xi_s) + o(1) \tag{9}$$

En revenant à la variable initiale, on montre que: 1) la constante C correspondant aux pôles de la solution u_a est à un facteur prés, la constante de *Stokes* associée à l'équation de WEBER, 2) cette constante de *Stokes* est une fonction analytiques de a, 3) les entiers impairs positifs sont les zéros de cette fonction.

Références

[1] *Jean Louis CALLOT*, Sur la piste des canards imaginaires. A. Fruchard et A. Troesch éditions, prépublication IRMA, Strasbourg, pp.191-204, 1995

[2] *Ovidiu Costin*, On Borel summation and Stokes phenomena for rank one nonlinear systems of ODE's. Duke Math. J. 93, 2 (1998), 289-344.

[3] *Ovidiu Costin*, On the formation of singularities of solutions of nonlinear differential systems in antistokes directions. Invent.math (2001)

[4] *Wolfgang Wasow*, Asymptotic expansions for ordinary differential equations. Interscience Publishers, New York, (1968).

Sadjia Chettab Aït-Mokhtar
Laboratoire de Mathematique Calcul Asymptotique
Pôle Science et Technologie
Avenue Michel Crépeau
17042 La Rochelle Cedex 1
France
schettab@univ-lr.fr
http://www.univ-lr.fr

Algorithmes de résolution d'équations différentielles linéaires dans une extension exponentielle

Anne Fredet

Introduction

Au XVII^e siècle, on s'intéressait déjà à l'intégration sous forme finie et aux équations différentielles d'ordre un. Ces problèmes apparaissent dans différents phénomènes physiques, notamment en mécanique. Les travaux de Liouville (1809–1882) servent généralement de point de repère à l'étude d'équations différentielles linéaires de forme générale $L(y) = a_n y^{(n)} + \cdots + a_0 y = b$. Une première étape dans la recherche de ces solutions sous forme close est de considérer les solutions *rationnelles*:

Définition 1 Soient $(k,')$ un corps différentiel et $L(y) = a_n y^{(n)} + \ldots + a_1 y' + a_0 y$ une équation différentielle à coefficients dans k. Une *solution rationnelle* de L est un élément y dans k tel que $L(y) = 0$.

Plusieurs années séparent les résultats théoriques et les résultats algorithmiques. Par exemple, le premier algorithme complet d'intégration sous forme finie a été proposé par Risch en 1960 alors que les résultats théoriques dataient du milieu du XIX^e siècle. De plus, la plupart des algorithmes développés pour calculer les solutions rationnelles traitent des équations différentielles linéaires à coefficients dans $C(x)$ où C désigne un corps des constantes et x est tel que $x' = 1$. Dans cet exposé, on va s'intéresser aux équations différentielles linéaires à coefficients dans des extensions exponentielles et s'intéresser aux récents algorithmes développés pour ce cas. coefficients dans une On verra d'abord la méthode présentée dans [Singer, 1991]. Les améliorations proposées ensuite mettent en évidence l'importance du système de générateurs choisi pour définir l'extension.

Algorithmique

Soient (K,D) un corps différentiel et θ exponentiel sur K (i.e. θ transcendant sur K, $\frac{D\theta}{\theta} \in K$ et on n'étend pas le corps des constantes). Soit $L = D^n + a_{n-1}D^{n-1} + \cdots + a_0$ un opérateur différentiel linéaire unitaire à coefficients dans $K(\theta)$.

Première méthode :
Dans [Singer, 1991], un algorithme de recherche de solutions rationnelles d'équation différentielle linéaire à coefficients dans une extension exponentielle est proposé, qui se décompose en trois étapes :

- *étape 1 : Calculer le dénominateur*
  L'utilisation de développements p-adiques permet de prouver que les polynômes apparaissant aux dénominateurs de solutions rationnelles sont facteurs des dénominateurs des coefficients a_i, et une équation indicielle nous permet de borner l'ordre de ces polynômes. Un changement de variable nous réduit à chercher des solutions polynomiales au sens de Laurent.
- *étape 2 : Borner le degré et la valuation*
  On considère une solution de la forme $Y = y_\gamma\theta^\gamma + \cdots + y_\delta\theta^\delta$ avec les y_i dans K tels que $y_\gamma \neq 0 \neq y_\delta$ où γ et δ sont dans $\mathbb{Z}$, $\gamma \geq \delta$. On cherche une borne supérieure sur γ et inférieure sur δ. On écrit L comme un polynôme en θ : $L = \sum_{i=\mu}^{\nu} \theta^i L_i$ avec les L_i dans $K[D]$ tels que $L_\mu \neq 0 \neq L_\nu$ où μ et ν sont dans $\mathbb{Z}$, $\nu \geq \mu$. On montre que $L(Y) = 0$ implique que $L_\nu(y_\gamma\theta^\gamma) = 0$ et $L_\mu(y_\delta\theta^\delta) = 0$. On cherche alors les solutions *exponentielles* de L_ν et de L_μ (i.e. les solutions de la forme $e^{\int u}$ pour un u dans K). Puis on regarde quelles solutions sont de la forme $f\theta^\alpha$ pour un certain f dans K et α dans $\mathbb{Z}$. Il faut décider si l'équation $y' + uy = 0$ a une solution dans $K(\theta)$. On utilise pour cela des résultats d'intégration (voir [Risch]). Les possibilités pour α nous donneront les bornes cherchées.
- *étape 3 : Calculer les coefficients*
  On écrit la solution sous la forme $y_\gamma\theta^\gamma + \cdots + y_\delta\theta^\delta$ et on l'injecte dans l'équation. On obtient un système différentiel linéaire à coefficients dans K. On utilise l'algèbre linéaire non-commutative (voir [Poo60]) pour diagonaliser ce système, et on calcule ensuite les coefficients.

Améliorations :
Dans [Bronstein, 1992], un autre algorithme permet de calculer la partie *normale* du dénominateur (étape 1), évitant la factorisation des coefficients. Dans [BF99] nous présentons des améliorations des étapes 2 et 3 pour des extensions de la forme $C(x, \exp(\int g(x)dx))$. Je généralise ces améliorations à une classe plus large d'extensions exponentielles dans [Fre01]. Voici ces améliorations esquissées dans le cas d'extensions exponentielles de $C(x)$.
À l'étape 3, on remarque que le système obtenu à une forme particulière :

Si $L(Y) = 0$ alors $M\overrightarrow{Y} = 0$ où $M = \begin{pmatrix} * & 0 & \cdots & \\ \vdots & \ddots & & \\ * & \cdots & * & \\ & \ddots & \vdots & \\ 0 & \cdots & * & \end{pmatrix}$ et $\overrightarrow{Y} = \begin{pmatrix} y_\delta \\ y_{\delta+1} \\ \vdots \\ y_{\gamma-1} \\ y_\gamma \end{pmatrix}$. On utilise un analogue de l'équation aux récurrences permettant de calculer les coefficients de solutions polynomiales d'équations différentielles linéaires à coefficients dans $C(x)$ (voir [ABP95]). Dans le cas des extensions exponentielles, cette relation est différentielle puisque le corps de base n'est plus un corps de constantes, et on a alors des problèmes d'existence de solutions.

À l'étape 2, on évite le calcul des solutions exponentielles de L_μ et L_ν qui ne sont pas de la forme souhaitée. On essaie de calculer directement les solutions sous cette forme (et donc de trouver directement les exposants possibles) afin d'éviter l'utilisation de résultats d'intégration difficile à mettre en place. On utilise pour cela des outils asymptotiques. Cela amène à introduire deux définitions :

Définition 2 Une extension $C(x,\theta_1,\cdots,\theta_l)$ est *une extension exponentielle plate de* $C(x)$ si pour tous c_i dans $\mathbb{Q}$, $\prod \theta_i^{c_i}$ est exponentiel sur $C(x)$

Définition 3 Une extension exponentielle plate $C(x,\theta_1,\cdots,\theta_l)$ est *bien définie* si, pour tout sous-ensemble $\mathcal{N} \subset \{1,\cdots,l\}$,

- soit en notant $\frac{\theta_i'}{\theta_i} = u_i x^{\alpha_i} + \cdots$ on constate que les u_j sont $\mathbb{Q}$-linéairement indépendants pour les $j \in \mathcal{N}$ tels que $\alpha_j = \max_{k\in\mathcal{N}}(\alpha_k)$,
- soit en notant $\frac{\theta_i'}{\theta_i} = \frac{u_i}{p^{\alpha_i}} + \cdots$ et $\alpha = \max_{k\in\mathcal{N}}(\alpha_k)$ on constate que $\alpha > 1$ et les u_j sont $\mathbb{Q}$-linéairement indépendants pour les $j \in \mathcal{N}$ tels que $\alpha_j = \alpha$, ou bien que $\alpha = 1$ et les u_j et p' sont $\mathbb{Q}$-linéairement indépendants pour les $j \in \mathcal{N}$ tels que $\alpha_j = 1$.

J'ai proposé un algorithme qui, étant donnée une extension plate, calcule un système de générateurs tel que l'extension soit bien définie (éventuellement à extension algébrique près). Lorsque l'on s'intéresse aux solutions rationelles d'équations différentielles linéaires à coefficients dans une extension exponentielle bien définie, on se ramène à considérer des équations à coefficients dans $C(x)$, et à chercher des solutions $f\theta_1^{\gamma_1}\cdots\theta_l^{\gamma_l}$ pour f dans $C(x)$ et γ_i dans $\mathbb{Z}$. En utilisant des développements à l'infini ou p-adiques pour un polynôme p bien choisi, on peut calculer directement un ensemble fini de possibilités pour $(\gamma_1,\cdots,\gamma_l)$, sans utiliser de résultats d'intégration difficile à implanter.

Conclusion

On voit ainsi que si deux extensions sont isomorphes, et donc théoriquement semblables, le choix du système de générateurs influe sur l'efficacité de l'algorithme utilisé pour calculer les solutions rationnelles d'équations différentielles linéaires. Cette approche se généralise à certaines extensions exponentielles d'extensions monomiales.

Références

[ABP95] *S. Abramov, M. Bronstein, and M. Petkovšek* On polynomial solutions of linear operator equations. ISSAC'95. ACM Press

[Bronstein] *Manuel Bronstein*
On solutions of linear ordinary differential equations in their coefficient field. Journal of Symbolic Computation,13(4):413–440 - 1992

[BF99] *Manuel Bronstein and Anne Fredet* Solving linear ordinary differential equations over $C(x,e^{\int f(x)dx})$. ISSAC'99. ACM Press.

[Fre01] *Anne Fredet* Résolution sous forme finie d'équations différentielles linéaires et extensions exponentielles Thèse, Laboratoire Gage - École polytechnique, 2001.

[Poo60] *E.G.C Poole* Introduction to the Theory of Linear Differential Equations. Dover Publications Inc., 1960.

[Risch] *R.H. Risch*
The Problem of Integration in Finite Terms. Trans A.M.S. 1969
The Solution of the Problem of Integration in Finite Terms. Bulletin A.M.S. 1970

[Singer] *Michael F. Singer* Liouvillian solutions of linear differential equations with liouvillian coefficients. Journal of Symbolic Computation, 11:251–273. 1991

Anne Fredet
Laboratoire Gage - École polytechnique
91 128 Palaiseau cedex - France
`fredet@gage.polytechnique.fr`
http://www.gage.polytechnique.fr/ fredet

Sur les critères et les formules de résultant pour l'inversion des applications polynômiales

Sihem Hachaïchi-Mesnager

K désigne un corps quelconque, X_1,X_2, Y_1,Y_2 désignent des indéterminées sur K. On note $X = (X_1,X_2)$ et $Y = (Y_1,Y_2)$, $K[X]$ l'anneau des polynômes en X sur K et $K(X)$ le corps des fractions de $K[X]$. Si $f, g \in K[X_1,X_2,Y_1,Y_2]$ et $i \in \{1,2\}$, $j = \{1,2\} \setminus \{i\}$, $\mathrm{Res}_{X_i}(f,g)$ désignera le résultant de f et g par rapport à X_i en tant que polynômes à indéterminée X_i et à coefficients dans $K[X_j,Y_1,Y_2]$. Enfin $\mathrm{Cd}_{X_i}(f)$ et $\deg_{X_i}(f)$ désignent respectivement le coefficient dominant et le degré de f par rapport à X_i. On considère $F = (F_1,F_2) : K^2 \to K^2$ une application polynomiale donnée par ses fonctions coordonnées $F_i \in K[X]$ $(i = 1, 2)$.

Si on s'intéresse aux problèmes d'inversion d'une telle application F en termes de résultants, il est naturel de considérer les questions (1) et (2) suivantes :

(1) Comment peut-on reconnaître par un calcul de résultant si F est inversible d'inverse polynomial, c.a.d $\exists\, G = (G_1,G_2) \in (K[X_1,X_2])^2$ tel que $F \circ G(X) = G \circ F(X) = X$? et dans ce cas, comment obtient-on son inverse G en termes de résultant ?

(2) Comment peut-on reconnaître par un calcul de résultant si F est inversible d'inverse rationnel (ou encore birationnelle), c.a.d $\exists\, G = (G_1,G_2) \in (K((X_1,X_2))^2$ tel que $F \circ G(X) = G \circ F(X) = X$? et dans ce cas, comment obtient-on son inverse G en termes de résultant ?

Ces problèmes d'inversion ont attiré l'attention de plusieurs auteurs, et la première approche du problème (1) est due à McKay et Wang [3], mais leur résultat ne répond que partiellement aux questions (1). En effet, il fournissent seulement une formule explicite de l'inverse de F en fonction de certains coefficients c, d et J, dans le cas particulier où F est supposée inversible et sans termes constants. D'autre part, Adjamagbo et van den Essen [1] ont apporté une réponse complète au problème (1). En effet, ils fournissent non seulement un critère nécessaire et suffisant d'inversibilité de F reposant sur l'existence de coefficients λ_1 et λ_2 dans $K^\star$, mais aussi une expression explicite de l'inverse de F, lorsque F est inversible.

Compte tenu de "l'état de la question" du problème (1), notre premier objectif est d'établir le lien entre les coefficients c,d, J dans le théorème

McKay et Wang et les coefficients λ_1, λ_2 dans le théorème d'Adjamagbo et van den Essen. C'est l'objet du théorème ci-dessous.

Théorème Les coefficients λ_1 et λ_2 du théorème d'Adjamagbo et van den Essen sont telles que :

$$\lambda_1 = (-1)^m Jc \quad \text{et} \quad \lambda_2 = (-1)^{k+1} Jd.$$

avec :

$$\begin{aligned} m &= \deg_{X_2} F_1(0,X_2), \quad k = \deg_{X_1} F_1(X_1,0), \quad J = \left.\frac{\partial(F_1,F_2)}{\partial(X_1,X_2)}\right|_{X_1=0,X_2=0} \\ c &= \mathrm{Res}_{X_2}\left(\frac{F_1(0,X_2)-F_1(0,0)}{X_2}, \frac{F_2(0,X_2)-F_2(0,0)}{X_2}\right), \\ d &= \mathrm{Res}_{X_1}\left(\frac{F_1(X_1,0)-F_1(0,0)}{X_1}, \frac{F_2(X_1,0)-F_2(0,0)}{X_1}\right). \end{aligned}$$

L'intérêt principal de ce dernier résultat, est d'être à la fois un raffinement du théorème d'Adjamagbo et van den Essen et d'avoir comme corollaire le théorème de McKay et Wang. Cet intérêt est renforcé par le fait qu'on prouve que dans la cas où F est linéaire, le critère résultant de ce théorème est équivalent au critère classique de déterminant pour l'inversion des applications linéaires, et que les formules d'inversions du théorème en question sont identiques aux formules classiques de Cramer.

Quant au problème (2) et en supposant que les coefficients de F sont " en position générique " (c'est-à-dire $\forall (i,j) \in \{1,2\}^2, F_i \notin K[X_j]$ et $\forall i \in \{1,2\}$ et $j \in \{1,2\} \setminus \{i\}$, $\mathrm{Cd}_{X_j} F_1(X_1,X_2)$ et $\mathrm{Cd}_{X_j} F_2(X_1,X_2)$ sont premiers entre eux), Abhyankar énonce une réponse complète à ce problème en termes presque identiques à ceux d'Adjamagbo et van den Essen. Son critère d'inversibilité repose sur l'existence de coefficients λ_1,λ_2 éléments de K^* et non de $K[X_1] \setminus \{0\}$ et $K[X_2] \setminus \{0\}$ respectivement, comme on peut s'y attendre à priori. Malheureusement, Abhyankar ne donne pas une démonstration explicite de ce théorème. Sans doute induit en erreur par ce manque de démonstration, Yu dans [4] cite le résultat d'Abhyankar en omettant l'hypothèse cruciale de "position générique"; il énonce ensuite une généralisation à un nombre quelconque d'indéterminées suivie d'une démonstration qui est erronée même dans le cas de deux indéterminées, comme le montre le contre exemple que nous indiquons dans la suite.

La réponse complète suivante au problème (2) a été apportée par Adjamagbo et Boury [2], où ils supposent plus généralement que F est un couple de fractions rationnelles à deux indéterminées:

Théorème (Adjamagbo et Boury) Soient $F = (F_1,F_2) \in (K(X_1,X_2))^2$ et $(P_1,Q_1,P_2,Q_2) \in (K[X_1,X_2])^4$ tels que $Q_1Q_2 \neq 0$, $F_1 = \frac{P_1}{Q_1}$, $F_2 = \frac{P_2}{Q_2}$, P_1 et Q_1 sont premiers entre eux, P_2 et Q_2 sont premiers entre eux. Alors les deux propositions suivantes (i) et (ii) sont équivalentes:

(i) F est birationnelle.

(ii) $\exists (R_1,S_1), (R_2,S_2) \in (K[Y_1,Y_2] \setminus K)^2$ avec R_1 et S_1 premiers entre eux, R_2 et S_2 premiers entre eux, $\exists \lambda_1 \in K[X_1] \setminus \{0\}, \lambda_2 \in K[X_2] \setminus \{0\}$ vérifiant (a) et (b) :

- **(a)** $\forall i \in \{1,2\}$, $F \notin (K(X_i))^2$.
- **(b)** $\forall i \in \{1,2\}$, $j \in \{1,2\} \setminus \{i\}$, $\mathrm{Res}_{X_j}(P_1 - Y_1Q_1, P_2 - Y_2Q_2) = \lambda_i(S_iX_i - R_i)$.

De plus, si F est inversible d'inverse rationnel noté $G = (G_1,G_2)$, alors on a :

$$G_1(Y_1,Y_2) = \frac{R_1(Y_1,Y_2)}{S_1(Y_1,Y_2)}, \quad G_2(Y_1,Y_2) = \frac{R_2(Y_1,Y_2)}{S_2(X_1,Y_2)}.$$

Une des particularités du théorème d'Adjamagbo et Boury sur laquelle nous voudrions insister, est que les coefficients λ_1 et λ_2 sont des éléments respectivement, de $K[X_1] \setminus \{0\}$ et $K[X_2] \setminus \{0\}$ et non de K^* comme dans le théorème d'Abhyankar. La question naturelle qui vient alors à l'esprit est : dans le cas où F est polynomial (et non pas seulement rationnel), ce point de leur résultat peut-il être amélioré en prenant pour λ_1 et λ_2 des constantes dans K^* ?

Compte tenu de "l'état de la question" du problème (2), notre second objectif est de préciser le lien entre les coefficients λ_1,λ_2 du théorème d'Adjamagbo et Boury d'une part, et les coefficients de F d'autre part, de manière à apporter une réponse à la question naturelle précédemment soulevée à propos de ce théorème. C'est l'objet du théorème et du corollaire ci-dessous.

Théorème Avec les notations du théorème d'Adjamagbo et Boury[2], pour tous $i \in \{1,2\}$ et $j \in \{1,2\} \setminus \{i\}$, le plus grand commun diviseur de $\mathrm{Cd}_{X_j}(F_1(X_1,X_2) - Y_1)$ et $\mathrm{Cd}_{X_j}(F_2(X_1,X_2) - Y_2)$ est un élément $\mu_i(X_i) \in K[X_i]$ qui a le même ensemble de racines que $\lambda_i(X_i)$ dans la clôture algébrique $\bar{K}$ de K.

Corollaire Soient $F = (F_1,F_2) \in (K[X_1,X_2])^2$ et $\mu_i(X_i) \in K[X_i]$ le plus grand commun diviseur de $\mathrm{Cd}_{X_j}(F_1(X_1,X_2) - Y_1)$ et de $\mathrm{Cd}_{X_j}(F_2(X_1,X_2) - Y_2)$

avec $i \in \{1,2\}$ et $j \in \{1,2\} \setminus \{i\}$. Les conditions (i) et (ii) suivantes sont équivalentes:

(i) F est inversible d'inverse rationnel tel que $\mu_i \in K^*$ pour $i \in \{1,2\}$.

(ii) il existe deux couples (R_1,S_1) et (R_2,S_2) d'éléments de $K[Y_1,Y_2] \setminus K$ avec R_1 et S_1 premiers entre eux, R_2 et S_2 premiers entre eux, et λ_1,λ_2 éléments de K^* vérifiant :

$$\mathrm{Res}_{X_2}(F_1 - Y_1,F_2 - Y_2) = \lambda_1(S_1X_1 - R_1),$$
$$\mathrm{Res}_{X_1}(F_1 - Y_1,F_2 - Y_2) = \lambda_2(S_2X_2 - R_2).$$

L'intérêt principal de ce dernier théorème, est d'être à la fois un raffinement du théorème d'Adjamagbo et Boury et d'avoir comme corollaire, le théorème d'Abhyankar dont il fournit enfin une démonstration explicite. Quant au corollaire, il permet également d'apporter une réponse négative à la question naturelle précédente, c'est-à-dire d'exhiber un couple de polynôme F élément de $(K[X_1,X_2])^2$ d'inverse rationnel et dont les coefficients λ_1,λ_2 ne sont pas des éléments de K^* en prenant $F_1 = X_1^2X_2$ et $F_2 = X_1X_2$. Ce qui apporte un contre exemple à l'énoncé de Yu [4] et montre que les transformations linéaires génériques sont nécessaires pour garantir la validité du Théorème d'Abhyankar.

Références

[1] *K. Adjamagbo et A. ven den Essen*, A resultant Criterion and formula for the inversion of a polynômial map in two variables. J. of Pure and Appl. Algebra **64** (1990), 1–6.

[2] *K. Adjamagbo et Pierre Boury*, A resultant Criterion and formula for the inversion of a rational map in two variables. J. of Pure and Appl. Algebra **79** (1992), 1–13.

[3] *J.McKay et S. S.S.Wang*, *An inversion formula for two polynômials in two variables.* J. of Pure and Appl. Algebra **40** (1986), 245–257.

[4] *J-T. Yu*, Computing minimal polynomials and the inverse via GCP. communications in algebra, **21** (1993), 2279–2294.

Sihem Hachaïchi-Mesnager
Institut de Mathématiques, Université de Paris VI
4, Place Jussieu, 75252, Paris Cedex 05
hachai@math.jussieu.fr

Régularité des configurations micromagnétiques ayant une énergie de paroi nulle

Myriam Lecumberry

Considérons un échantillon fin d'un matériau ferromagnétique. On suppose que l'échantillon fin est un cylindre de base $\Omega \subset \mathbb{R}^2$ et d'épaisseur ϵ. Une magnétisation spontanée est générée dans le matériau. On la note u, elle est de norme constante, que l'on prendra égale à 1. On supposera qu'il y a invariance par translation, ce qui nous ramène à un problème en dimension 2 sur un domaine Ω de $\mathbb{R}^2$.
Les énergies du problème sont les suivantes:

- L'énergie d'échange (qui pénalise les variations de u): $\int_\Omega |\nabla u|^2$,
- L'énergie démagnétisante: la magnétisation u est compensée par un champ H_u défini sur $\mathbb{R}^2$ par

$$\begin{cases} \operatorname{div}(\bar{u} + H_u) = 0 & \text{dans } \mathbb{R}^2 \\ \operatorname{rot}(H_u) = 0 & \text{dans } \mathbb{R}^2 \end{cases}$$

  où $\bar{u}$ est l'extension de u par 0 hors de Ω. L'énergie qui en résulte est $\int_{\mathbb{R}^2} |H_u|^2$,
- L'énergie d'anisotropie (qui privilégie une direction pour u),
- L'énergie due au champ magnétique extérieur.

On supposera que le matériau est anisotrope et que le champ extérieur est nul. Les deux dernières énergies sont donc nulles. L'énergie totale dépend de l'épaisseur ϵ de la manière suivante:

$$E_\epsilon(u) = \int_\Omega \frac{\epsilon}{2} |\nabla u|^2 + \frac{1}{2\epsilon} \int_{\mathbb{R}^2} H_u^2$$

Un des principaux problèmes est de comprendre le comportement asymptotique d'une famille de configurations u_ϵ, $\epsilon > 0$, dans $H^1(\Omega,S^1)$, ayant une énergie $E_\epsilon(u_\epsilon)$ uniformément bornée quand $\epsilon \to 0$.

Les résultats qui suivent (Théorème 1 et Proposition 1) ont été démontrés dans [4].

Théorème 1 :
Soit $\epsilon_n \to 0$ et $u_n \in H^1(\Omega,S^1)$ tel que u_n admet un relèvement $\phi_n \in H^1(\Omega,\mathbb{R})$

(ie $u_n = e^{i\phi_n}$ p.p.). Supposons que $E_{\epsilon_n}(u_n) \leq C$ et $\|\phi_n\|_{L^\infty} \leq N$. Alors, il existe u et ϕ dans L^p, $\forall\, p < \infty$ tels que, modulo une extraction,
$\phi_n \to \phi$ et $u_n \to u$ dans L^p, fort $\forall\, p < \infty$.
De plus, u et ϕ vérifient

i) $\operatorname{div} \bar{u} = 0$ dans $\mathcal{D}'(\mathbb{R}^2)$,
ii) $u = e^{i\phi}$ p.p. in Ω,
iii) $\operatorname{div}(\phi u + u^\perp)$ est une mesure de Radon sur Ω.

$u^\perp$ désigne la rotation d'angle $\frac{\pi}{2}$ de $u = (u_1,u_2)$, i.e $u^\perp = (-u_2,u_1)$.
On note par $\mathcal{D}'(\mathbb{R}^2)$ l'espace des distributions sur $\mathbb{R}^2$.
Une mesure de Radon sur Ω est une application linéaire sur l'espace des fonctions continues à support compact dans Ω.

$\mathcal{C}_L$ est l'ensemble des couples (u,ϕ) tel que u et ϕ sont limites dans L^1 de suites (u_n) et (ϕ_n) dans $H^1(\Omega)$ vérifiant $u_n = e^{i\phi_n}$ p.p. dans Ω et telles que $E_{\epsilon_n}(u_n)$ et $\|\phi_n\|_{L^\infty}$ soient uniformément bornées.
La mesure $\operatorname{div}(\phi u + u^\perp)$, $\forall (u,\phi) \in \mathcal{C}_L$, est liée aux troncatures $T^a u$ définies par

$$\begin{cases} T^a\phi = \inf(\phi,a) \\ T^a u = e^{iT^a\phi} \end{cases}$$

de la manière suivante:

$$\operatorname{div}(\phi u + u^\perp) = -\int_{\mathbb{R}} \operatorname{div} T^a u \, da \tag{10}$$

Proposition 1 :
Si $(u,\phi) \in \mathcal{C}_L$, alors

$$\int |\operatorname{div}(\phi u + u^\perp)| \leq \iint |\operatorname{div} T^a u| \, da \leq \liminf_{n\to\infty} E_{\epsilon_n}(u_n)$$

quelque soit la suite $u_n = e^{i\phi_n}$, $\phi_n \in H^1(\Omega)$, telle que $E_{\epsilon_n}(u_n)$ et $\|\phi_n\|_{L^\infty}$ soient uniformément bornées, et $\phi_n \to \phi$ dans L^1.

Remarques :

1. Si on suppose que $u_n \in H^1(\Omega)$ vérifie $E_{\epsilon_n}(u_n) \to 0$ et que $u_n \to u$ dans L^1, alors u vérifie $\operatorname{div} T^a u = 0$ dans $\mathcal{M}'(\Omega \times \mathbb{R})$.
2. Si u est régulière (par exemple $u \in H^1(\Omega)$), alors $\operatorname{div} u = 0$ implique que $\operatorname{div} T^a u = 0$.

Essayons maintenant de voir à quel point la mesure div $T^a u$ caractérise le manque de régularité de $(u,\phi) \in \mathcal{C}_L$. Le résultat suivant est démontré dans [3].

Théorème 2 :
Soit $(u,\phi) \in \mathcal{C}_L$. Il y a équivalence entre

1. $\operatorname{div} T^a u = 0$, dans $\mathcal{D}'(\Omega \times \mathbb{R})$.
2. $\phi \in H^{1/2}(\Omega)$.

De plus, si 1. (et 2.) est vrai, then quelque soit $\omega \subset\subset \Omega$, ϕ est Lipschitz dans ω et les ensembles de niveaux de ϕ dans ω sont des lignes droites qui ne se coupent pas dans ω.

Idée de la preuve :
L'équivalence se démontre en utilisant l'interprétation cinétique du problème, donnée dans [4]:

$$\nabla_x \chi(x,a).(e^{ia})^{\perp} = -\partial_a(\operatorname{div} T^a u), \text{ dans } \mathcal{D}'(\Omega \times \mathbb{R}) \tag{11}$$

où χ est défini sur $\Omega \times \mathbb{R}$ par $\chi(x,a) = 1$ si $\phi(x) \leq a$ et $\chi(x,a) = 0$ sinon. Si 1. est vrai, le terme de droite dans l'égalité (2) est nul, la régularité $H^{1/2}$ est obtenue de manière standard grâce à un lemme de moyenne cinétique démontré dans [2].

Supposons maintenant que 1. est vrai, alors d'après (1), $\operatorname{div}(\phi u + u^{\perp}) = 0$. Rappelons que div $u = 0$. Il existe donc deux fonctions Lipschitz g,h telles que

$$\begin{cases} u = \nabla^{\perp} g & \text{dans } \Omega \\ \phi u + u^{\perp} = \nabla^{\perp} h & \text{dans } \Omega \end{cases}$$

où $\nabla^{\perp} = (-\frac{\partial}{\partial y}, \frac{\partial}{\partial x})$.
On définit Ψ sur Ω à valeurs dans $\mathbb{R}^2$ par $\Psi(x,y) = (g,h)$, $\forall (x,y) \in \Omega$. Ψ is Lipschitz et $\operatorname{Jac}(\Psi) = 1$ dès qu'il est défini. On peut alors appliquer à Ψ un théorème d'inversion locale généralisé:
Pour presque tout $(x_0,y_0) \in \Omega$, $\exists V$, voisinage de (x_0,y_0), $\exists W$, voisinage de $\Psi(x_0,y_0)$, tels que $\Psi : V \to W$ est inversible. De plus, Ψ^{-1} est Lipschitz sur W. Pour chaque fonction f définie sur V, on note $\tilde{f} = f \circ \Psi^{-1}$.

Proposition 2 :
$\tilde{\phi}$ est une solution faible de l'équation de Burger sur W, i.e.

$$\forall\, \tilde{v} \,\in\, C_c^\infty(W), \quad \int_W \tilde{\phi}\frac{\partial \tilde{v}}{\partial g} + \frac{\tilde{\phi}^2}{2}\frac{\partial \tilde{v}}{\partial h} = 0$$

De plus, pour toute fonction $S \in C^2(\mathbb{R},\mathbb{R})$,

$$\forall\, \tilde{v} \,\in\, C_c^\infty(W), \quad \int_W S(\tilde{\phi})\frac{\partial \tilde{v}}{\partial g} + F(\tilde{\phi})\frac{\partial \tilde{v}}{\partial h} = 0,$$

où F est défini par $F'(t) = tS'(t), \forall\, t \in \mathbb{R}$.

En particulier, $\tilde{\phi}$ est une solution entropique. Par un argument d'unicité locale pour les solutions entropiques de lois de conservation (cf [1] par exemple), on conclut que $\tilde{\phi} \in BV_{loc}(\Omega)$. Cette régularité est suffisante pour définir les caractéristiques de $\tilde{\phi}$ (courbes sur lesquelles $\tilde{\phi}$ est constante). On montre alors que ce sont des lignes droites qui ne se coupent pas.

Références

[1] *C.M. Dafermos*, Hyperbolic Conservation Laws in Continuum Physics, Springer (1991)

[2] *F. Golse, P.L. Lions, B. Perthame et R. Sentis* , Regularity of the moments of the solution of a transport equation, *J. Funct. Anal.* **76** (1988), no.1, 110-125.

[3] *M.Lecumberry et T. Rivière*, Regularity for Micromagnetic Configurations having Zero Jump Energy, to appear in *Calc. Var. PDE* (2002).

[4] *T. Rivière et S. Serfaty*, Compactness, Kinetic Formulation, and Entropies for a Problem Related to Micromagnetics, submitted.

Myriam Lecumberry
Laboratoire de Mathématiques, UMR 6629
Université de Nantes
2, rue de la Houssinière
44322 Nantes Cedex 03
France
`Myriam.Lecumberry@math.univ-nantes.fr`

Méthode de décomposition de domaine pour des équations au dérivées partielles

Véronique Martin

Introduction

Ces dernières décennies, les mathématiques appliquées ont connu un succès grandissant dans les milieux industriels. En effet, là où des essais effectués en taille réelle étaient coûteux, la simulation numérique offre une grande souplesse dans la résolution du problème étudié.

Dans un premier temps, on choisit les équations qui proviennent de la physique et qui rendent compte du phénomène étudié. Ensuite il s'agit de résoudre ces équations. La plupart n'ayant pas de solution analytique, nous en calculons une approximation de façon numérique à l'aide d'outils informatiques.

Toutefois les problèmes étudiés sont de plus en plus complexes et certaines applications demandent plus de mémoire qu'un seul ordinateur ne peut leur en fournir. Une solution proposée est de décomposer le problème initial en sous-problèmes de plus petite taille qui pourront être gérés chacun par un seul ordinateur. Ensuite un échange d'informations selon un processus itératif permet d'obtenir la solution globale (voir [4], [6]).

1 Méthode de décomposition de domaine

Nous présentons la méthode sur un problème très simple. Sur l'intervalle $I = [0,1]$, on considère l'équation $-C^2u + \dfrac{d^2u}{dx^2} = 0$ avec $C > 0$, et les conditions limites $u(0) = 1$ et $u(1) = e^{1/C}$. On en connait la solution $u = e^{x/C}$.

Nous allons résoudre ce problème par décomposition de domaines i.e. nous introduisons deux sous-domaines I_1 et I_2, avec $I_1 = [0,\frac{1}{2} + L[$, $I_2 =]\frac{1}{2},1]$ et $L < 1/2$ la taille du recouvrement.

Mettre en place une méthode de décomposition de domaines revient à résoudre le problème suivant. Nous possédons deux ordinateurs ; le premier résout l'équation de diffusion sur I_1 avec $u(0) = 1$ et une condition en $x = 1/2 + L$ à définir. Le deuxième résout également l'équation mais sur I_2 avec $u(1) = e^{1/C}$ et une condition à définir en $x = 1/2$. Comment obtenir la solution globale sur I à partir de ces deux machines?

Pour obtenir la solution sur I il est nécessaire que les deux ordinateurs s'échangent des informations au niveau des interfaces artificielles ($x = 1/2 + L$, $x = 1/2$). Historiquement le premier algorithme proposé est le suivant :

$$\left\{\begin{array}{lcl} -C^2\dfrac{d^2u}{dx^2}^{k+1} + u^{k+1} &=& 0 \text{ sur } I_1, \\ u^{k+1}(0) &=& 1, \\ u^{k+1}(1/2+L) &=& v^k(1/2+L), \end{array}\right. \quad \left\{\begin{array}{lcl} -C^2\dfrac{d^2v}{dx^2}^{k+1} + v^{k+1} &=& 0 \text{ sur } I_2, \\ v^{k+1}(1/2) &=& u^{k+1}(1/2), \\ v^{k+1}(1) &=& e^{1/C}. \end{array}\right. \tag{12}$$

La figure (13) montre les différentes étapes de l'algorithme et comment il converge vers la solution du problème global.

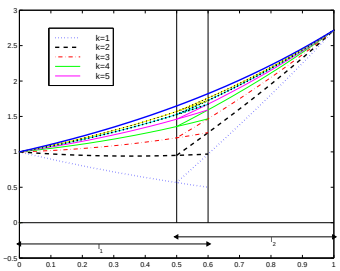


FIG. 13 – *Dirichlet*

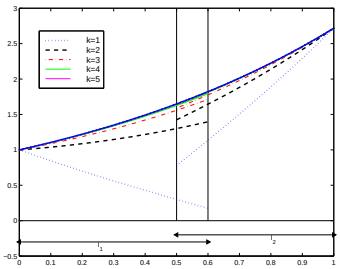


FIG. 14 – *Robin* $\lambda = 10$

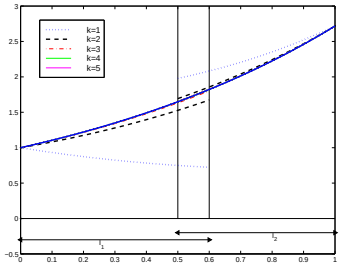


FIG. 15 – *Robin* $\lambda = 1/C$

Ensuite on peut améliorer la vitesse de convergence de cette méthode en changeant les conditions de transmission. On remplace donc dans l'algorithme (12) les conditions en $x = 1/2 + L$ et $x = 1/2$ par les conditions dites de Robin :

$$\begin{array}{lcl} (\dfrac{du}{dx}^{k+1} + \lambda u^{k+1})(1/2+L) &=& (\dfrac{dv}{dx}^{k} + \lambda v^{k})(1/2+L) \\ (\dfrac{dv}{dx}^{k+1} - \lambda v^{k+1})(1/2) &=& (\dfrac{du}{dx}^{k+1} - \lambda u^{k+1})(1/2). \end{array}$$

avec λ à définir. Les figures (14) et (15) montrent le résultat pour deux valeurs de λ. On voit que d'une part il faut moins d'itérations à cette méthode que pour celle de Dirichlet pour converger et que ce nombre d'itérations dépend du choix de λ.
On note que dans ce dernier cas le recouvrement L peut être pris égal à 0.

2 Application à l'équation de convection diffusion

On s'intéresse ici à l'équation de convection diffusion (13) qui régit l'évolution d'un polluant soumis à une force extérieure (par exemple du vent) dans un domaine donné Ω, de frontière $\partial\Omega$.

$$\begin{cases} \mathcal{L}u \equiv \dfrac{\partial u}{\partial t} + a\dfrac{\partial u}{\partial x} + b\dfrac{\partial u}{\partial y} - \nu\triangle u = f \text{ dans } \Omega \\ u(.,0) = u_0 \\ u = g \text{ sur } \partial\Omega \end{cases} \tag{13}$$

On décompose Ω en deux sous-domaines Ω_1 et Ω_2, et on note Γ l'interface commune qui est supposée rectiligne. L'objet de cette étude est d'écrire un algorithme de décomposition de domaine appliqué à cette équation avec pour objectif d'obtenir la convergence la plus rapide possible.

On connait les conditions de transmission (au niveau de l'interface) qui donnent une convergence de l'algorithme en deux itérations ; elles sont données par l'opérateur de Dirichlet-Neumann (voir [3] pour les conditions limites absorbantes). Elles ne sont pas utilisables du point de vue numérique, on est alors amené à les approcher par des opérateurs différentiels en temps et en la variable définie sur l'interface. Ceci conduit à l'algorithme (14), (15) .

$$\begin{cases} \mathcal{L}u^{k+1} &= f \text{ dans } \Omega_1\times]0,T[\\ u^{k+1}(\cdot,0) &= u_0 \text{ dans } \Omega_1 \\ \Big(\dfrac{\partial}{\partial x} + \dfrac{a+p}{2\nu} + q\dfrac{\partial}{\partial t} + bq\dfrac{\partial}{\partial y}\Big)u^{k+1} &= \Big(\dfrac{\partial}{\partial x} + \dfrac{a+p}{2\nu} + q\dfrac{\partial}{\partial t} + bq\dfrac{\partial}{\partial y}\Big)v^{k} \quad \text{sur } \Gamma \end{cases} \tag{14}$$

$$\begin{cases} \mathcal{L}v^{k+1} &= f \text{ dans } \Omega_2\times]0,T[\\ v^{k+1}(\cdot,0) &= u_0 \text{ dans } \Omega_2 \\ \Big(\dfrac{\partial}{x} + \dfrac{a-p}{2\nu}Id - q\dfrac{\partial}{\partial t} - bq\dfrac{\partial}{\partial y}\Big)v^{k+1} &= \Big(\dfrac{\partial}{x} + \dfrac{a-p}{2\nu}Id - q\dfrac{\partial}{\partial t} - bq\dfrac{\partial}{\partial y}\Big)u^{k} \quad \text{sur } \Gamma \end{cases} \tag{15}$$

Le résultat suivant valide cet algorithme. Sa démonstration repose sur des estimations d'energie.

Théorème : L'algorithme (14),(15) definit un problème bien posé dans l'espace de Sobolev *ad hoc* . Et la suite (u^k,v^k) converge vers u.

Pour le choix de p et q i.e. pour l'approximation des conditions exactes, on peut faire un développement de Taylor en basses fréquences du symbole de

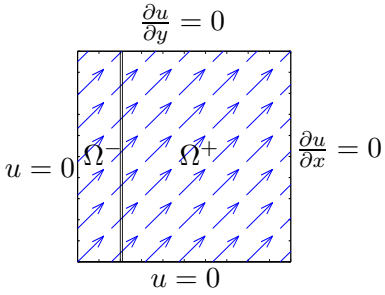


FIG. 16 – *Le problème*

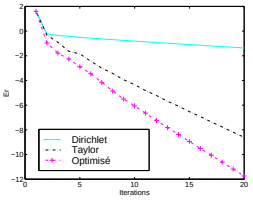


FIG. 17 – *L'erreur*

l'opérateur Dirichlet-Neuman, ou choisir les valeurs de p et q qui minimisent le taux de convergence de l'algorithme (voir [1] pour le cas stationnaire). On étudie le problème aux limites décrit sur la figure (16). La figure (17) montre l'évolution de l'erreur numérique en fonction du nombre d'itérations dans le cas des différents algorithmes proposés. On voit que la convergence de la méthode de Dirichlet est très lente. La méthode de Taylor permet une convergence plus rapide. Mais la méthode la plus rapide est encore la méthode optimisée puisqu'elle prend en compte toutes les fréquences du phénomène.

Références

[1] *Japhet C., Nataf F., Rogier F.*, The optimized order 2 method. Application to convection-diffusion problems. Future Generation Computer Systems FUTURE 2001.

[2] *M.J. Gander, L. Halpern, F. Nataf*, Optimal convergence for overlapping and non-overlapping Schwarz waveform relaxation. Eleventh International Conferences on Domain Decomposition Methods.

[3] *L. Halpern, M. Schatzman*, Artificial boundary conditions for incompressible flows. SIAM Journal on Math. Anal.. 1989, vol 20, 2, 308-353 .

[4] *Lions P.L.*, On the Schwarz alternating method I. First International Symposium on Domain Decomposition Methods for Partial Differential Equations.

[5] *V. Martin*, Domain decomposition method for unsteady convection diffusion equation. En préparation.

[6] *A. Quarteroni et A. Valli*, Domain decomposition methods for partial differential equations Oxford Science Publications, 1999.

Véronique Martin
LAGA,Institut Galilée Université Paris 13
avenue Jean Baptiste Clément, 93 430 Villetaneuse, France
martin@math.univ-paris13.fr

Un langage pour la programmation fonctionnelle

Armelle Merlin

L'un des enjeux principaux de l'informatique est de faire des calculs de grande taille et d'être capable de prévoir le temps que prendront ces calculs. Pour augmenter la rapidité des calculs, de nombreuses pistes sont explorées. L'une d'entre elle consiste à programmer sur des ordinateurs massivement parallèles. Pour assurer une programmation simple et portable, nous avons étendu le langage fonctionnel CAML à l'aide d'opérations de communication entre processus sur le modèle BSP (Valiant [5]). Ce modèle permet d'évaluer les temps de calcul de façon réaliste et portable. Il prend en compte la taille des données, le nombre de processeurs utilisés ainsi que la latence et la bande passante du réseau qui les relie. Pour rendre ce modèle de performance effectif pour le programmeur, notre extension de CAML doit être formellement modélisée à l'aide d'une machine abstraite ou machine à pile qui décrit pécisément les calculs parallèles engendrés par un programme. Nous présenterons ici les différents paradigmes de la programmation parallèle, le modèle BSP, notre extension de CAML appelée BSMLlib, les machines abstraites et les résultats obtenus du point de vue de la prévisibilité des performances.

Les ordinateurs parallèles sont des machines qui comportent une architecture parallèle, constituée de plusieurs processeurs identiques concourant tous au traitement d'une seule application. Le terme de massivement parallèle est couramment utilisé lorsque le système à architecture parallèle comporte de quelques dizaines de processeursà plusieurs dizaines de milliers de processeurs, ou plus encore. Ce systèmes sont souvent scalables, c'est-à-dire que leur puissance est extensible, dans une certaine plage, à peu près proportionnellement au nombre de leurs processeurs. Plusieurs architectures types caractérisent ce domaine :

- Les architectures M.I.M.D. ou encore à mémoire distribuée. Elles concernent les calculateurs où chaque processeur dispose d'une mémoire de données et de programme indépendante (Multiple Instructions Multiple Data), les échanges interprocesseurs s'effectuant par passage de message.
- Les architectures SIMD (Single Instruction Multiple Data). Elles proposent une mémoire de programmation centralisée pour tous les pro-

cesseurs qui exécutent donc de manière synchrone le même programme sur des données différentes.

Les éléments constitutifs d'un système massivement parallèle sont : les processeurs, le réseau qui relie ces processeurs, la mémoire plus ou moins répartie et la partie logiciel (langages et compilateurs pour la réalisation d'algorithmes de traitements en parallèle des tâches, systèmes d'exploitation...). Ces systèmes font intervenir des techniques de communication entre les différents éléments du système, de cohérence mémoire, de parallélisation et d'allocation des tâches, et de systèmes d'exploitation répartis. La machine PRAM (Parallel Random Access Memory) modélise, en le simplifiant, le fonctionnement d'un architecture MIMD à mémoire partagée.

Le modèle *Bulk-Synchronous Parallelism* (BSP) est un modèle de programmation parallèle introduit par Valiant [5] pour offrir un niveau d'abstraction comparable aux modèles PRAM tout en permettant des performances prévisibles et portables sur une large variété d'architectures. Un ordinateur BSP contient un ensemble de paires processeur-mémoire, un réseau de communication permettant l'échange de messages inter-processeur et une unité de synchronisation globale qui exécute des demandes collectives de barrières de synchronisation. Ses performances sont caractérisées par trois paramètres : le nombre p de paires de processeur-mémoire, le temps l nécessaire à une barrière de synchronisation et le temps g nécessaire à une 1-relation (phase de communication où chaque processeur envoie ou reçoit au plus un mot). Pour n'importe quel h le réseau peut réaliser une h-relation, c'est-à-dire une phase de communication où chaque processeur envoie ou reçoit au plus h mots, en temps gh. Un programme BSP est exécuté comme une séquence de *super-étapes*, chacune étant au plus divisée en trois phases successives et logiquement disjointes. Pendant la première phase, chaque processeur utilise ses données locales pour du calcul séquentiel et pour demander des transferts de données vers ou depuis d'autres noeuds. Pendant la seconde phase, le réseau effectue les transferts de données demandées. Pendant la troisème phase, une barrière de synchronisation se produit, rendant disponibles pour la super-étape suivante les données tranférées. Le temps d'exécution d'une super-étape s est ainsi la somme du maximum des temps de calculs locaux, du temps de communication des données et du temps de synchronisation globale :

$$Time(s) = \max_{i:processeur} w_i^{(s)} + \max_{i:processeur} h_i^{(s)} * g + l$$

où $w_i^{(s)}$ = temps de calcul local du processeur i durant la super-étape s et $h_i^{(s)} = \max\{h_{i+}^{(s)}, h_{i-}^{(s)}\}$ où $h_{i+}^{(s)}$ (resp. $h_{i-}^{(s)}$) est le nombre de mots transmis (resp. reçus) par le processeur i durant la super-étape s. Le temps d'exécution $\sum_s Time(s)$ d'un programme BSP composé de S super-étapes est la somme des trois termes : $W + H * g + S * l$ où $W = \sum_s \max_i wi^{(s)}$ et $H = \sum_s \max_i h_i^{(s)}$.

Le langage CAML, proche du λ-calcul, a été étendu [3] à l'aide d'opérations BSP. Cette extension, le BS-λ, présenté succintement ici, est confluent.

Soient $\dot{\mathcal{V}}$ l'ensemble des variables *locales* et $\bar{\mathcal{V}}$ l'ensemble des variables *globales*. Le point $\dot{}$ symbolise un processeur précis du réseau, la barre $\bar{}$ symbolise le réseau tout entier. Les termes *locaux* e sont des λ-termes représentant des valeurs ou des programmes stockés dans la mémoire locale d'un processeur. L'ensemble $\dot{\mathcal{T}}$ des termes locaux est donné par la grammaire suivante :

$$e \quad ::= \quad \dot{x} \mid e\, e \mid \lambda \dot{x}.\, e \mid c$$

où $\dot{x}$ dénote une variable locale arbitraire. Les termes *globaux* représentent des fonctions d'un ensemble fixé de processeurs vers des valeurs. Le terme $\pi\, e$ représente un champ de données dont les valeurs sont données par la fonction e. L'ensemble $\bar{\mathcal{T}}$ des termes globaux est donné par la grammaire suivante :

$$\begin{array}{rcl} E & ::= & \bar{x} \mid E\, E \mid E\, e \mid \lambda \bar{x}.\, E \mid \lambda \dot{x}.\, E \\ & \mid & \pi\, e \mid E \# E \mid E ? E \mid E \xrightarrow{e} E, E \end{array}$$

La dénotation de $\pi\, e$ a, au processeur n_i, la valeur de $e\, n_i$. Les formes $E_1 \# E_2$ et $E_1 ? E_2$ sont appelées application parallèle (*apply-par*) et *get* respectivement. Apply-par représente l'application point à point d'un champ de fonctions à un champ de valeurs (phase de calcul pur d'une super-étape BSP). Get représente la phase de communication d'une super-étape BSP : un échange collectif de données avec une barrière de synchronisation. dernière forme de terme global définit la conditionnelle globale synchrone. La signification de $E_1 \xrightarrow{e} E_2, E_3$ est celle de E_2 (resp. E_3) si le champ de données dénoté par E_1 a la valeur T (resp. F) au processeur de nom dénoté par e.

Dans la sémantique équationnelle l'égalité des termes globaux est définie par des règles basées sur la syntaxe et des règles de contexte qui déterminent l'applicabilité des premières.

Le BSML est un langage purement fonctionnel de données parallèles conçu pour programmer des algorithmes BSP. La BSMLlib est l'implantation du formalisme BSλ.

Une machine abstraite est le lien entre le langage compilé et son exécution. Le langage est d'abord traduit sous forme d'une suite de commandes (c'est-à-dire compilé). La machine exécute les commandes à l'aide de transitions. Pour obtenir un langage dont l'exécution est mieux adaptée au parallélisme, il parrait intéressant d'étendre une machine abstraite spécifique. La SECD, [2], est une machine entièrement documentée. Son extension pour le langage BSλ simplement typé [4] a été implanté et testé. Cela a permis de vérifier que les constantes peuvent être calculées *a priori*. La BSP-CAM, extension de la CAM, [1], permet d'avoir une gestion des environnements plus précise. Dans les deux cas, il existe une machine abstraite en chaque processeur qui exécute ses transitions de manière synchrone uniquement pour les opérations BSP.

Le but du projet est une réalisation complète d'une version BSP du langage Caml. Les différentes étapes réalisées à ce jour ont permis de vérifier la bonne structure du langage et ont mis en évidence les difficultés à surmonter pour une implantation parallèle complète et efficace.

Références

[1] G. Cousineau, P. L. Curien, and M. Mauny. The categorical abstract machine. In J.-P. Jouannaud, editor, *Functional Programming Languages and Computer Architecture*, pages 50–64. Springer-Verlag, Berlin, DE, 1985. Lecture Notes in Computer Science 201Proceedings of. Conference at Nancy.

[2] Peter J. Landin. The mechanical evaluation of expressions. *The Computer Journal*, 6(4):308–320, January 1964.

[3] F. Loulergue. *Conception de langages fonctionnels pour la programmation massivement parallèle.* Thèse de Doctorat d'Université, Université d'Orléans, janvier 2000.

[4] A. Merlin. Bsλ simplement typé: Typage et sémantique naturelle. Rapport de DEA, Université d'Orléans, Septembre 2000.

[5] Leslie G. Valiant. A bridging model for parallel computation. *Communications of the ACM*, 22(8):103–111, August 1990.

Armelle Merlin
Laboratoire d'Informatique Fondamentale d'Orléans
BP 6759
45067 Orléans Cedex 2
France
`merlin@lifo.univ-orleans.fr`

Décidabilité de la théorie universelle de certains semigroupes commutatifs

Céline Moreira Dos Santos

Définition 1 : Un **semigroupe** est la donnée d'un triplet $(S, +, 0)$, où:

- S est un ensemble;
- $+$ est une opération associative, *i.e.*, vérifiant $(x+y)+z = x+(y+z)$, pour tous x, y, $z \in S$;
- 0 est un élément de S neutre pour l'opération $+$, *i.e.*, vérifiant la propriété $x + 0 = 0 + x = x$, pour tout $x \in S$.

Un semigroupe est **commutatif** si son opération vérifie $x + y = y + x$, pour tous x, $y \in S$.

Tous les semigroupes que nous considèrerons seront commutatifs.

Exemple 1 : Les structures usuelles $(\mathbb{N}, +, 0)$ et $(\mathbb{N} \setminus \{0\}, \cdot, 1)$ sont des semigroupes (commutatifs).

Définition 2 : Soient S et T des semigroupes. Un **homomorphisme de semigroupes** $f : S \to T$ est une application de S dans T vérifiant les propriétés suivantes:

1. $f(0_S) = 0_T$;
2. $f(x + y) = f(x) + f(y)$, pour tous x et $y \in S$.

Un plongement $f : S \hookrightarrow T$ est un homomorphisme de semigroupes injectif, *i.e.*, vérifiant $f(x) = f(y) \implies x = y$, pour tous x et $y \in S$.

On s'interesse plus particulièrement à deux types de propriétés sur les semigroupes: la simplifiabilité et le raffinement.

Définition 3 : Un semigroupe S est dit:

- **simplifiable**, si il satisfait: $(x + z = y + z \Rightarrow x = y)$, pour tous x, y et $z \in S$;
- **fortement séparatif**, si il satisfait: $(x + y = 2y \Rightarrow x = y)$, pour tous x et $y \in S$;
- **séparatif**, si il satisfait: $(2x = x + y = 2y \Rightarrow x = y)$, pour tous x et $y \in S$.

On remarque que

$$\text{simplifiabilité} \implies \text{séparativité forte} \implies \text{séparativité}.$$

Définition 4 : Un semigroupe S est un **semigroupe de raffinement** si, pour tous a_0, a_1, b_0, $b_1 \in S$ vérifiant $a_0 + a_1 = b_0 + b_1$, il existe des éléments $c_{ij} \in S$, i, $j \in \{0,1\}$ vérifiant $a_i = c_{i0} + c_{i1}$ et $b_i = c_{0i} + c_{1i}$. Cette information s'exprime avantageusement sous la forme d'une **matrice de raffinement**:

	b_0	b_1
a_0	c_{00}	c_{01}
a_1	c_{10}	c_{11}

Cet énoncé est contraignant, mais beaucoup de semigroupes sont de raffinement, ou se plongent dans un semigroupe de raffinement.

Les liens entre semigroupes simplifiables et semigroupes de raffinement sont activement étudiés actuellement, en théorie des anneaux (cf. [1]) et en théorie des treillis (cf. [8]) tout particulièrement.

Nous donnons maintenant des résultats de décomposition. Il n'en existe actuellement pas de semblables pour les semigroupes de raffinement.

Théorème 1 : (cf.[7]) S séparatif se plonge dans un produit de la forme $\prod_{i\in I} T_i \cup \{\infty\}$, où les T_i sont des semigroupes simplifiables.

Théorème 2 : (cf.[5]) S fortement séparatif se plonge dans un produit de la forme $\prod_{i\in I} T_i \oplus \mathcal{L}_J(\mathbb{R})$, où les T_i sont des semigroupes simplifiables, et $\mathcal{L}_J(\mathbb{R})$ est une sorte de **puissance lexicographique** des réels strictement positifs.

On se donne $\mathcal{S}$ une classe de semigroupes (commutatifs) close par produit direct fini. En particulier, $\mathcal{S}$ pourra être la classe des semigroupes simplifiables (resp. fortement séparatifs, séparatifs).

Définition 5 : On appelle

- *formule atomique*: toute formule de la forme $(\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} b_i x_i)$, où a_i, b_i, $1 \leq i \leq n$ sont des entiers positifs, et x_1, ..., x_n sont des symboles de variables;
- *formule de Horn universelle*: toute formule de la forme

$$\varphi(\vec{\mathbf{x}}) : (\forall \vec{\mathbf{x}})[\psi(\vec{\mathbf{x}}) \Rightarrow \theta(\vec{\mathbf{x}})], \tag{16}$$

où $\psi(\vec{\mathbf{x}}) = \psi_1(\vec{\mathbf{x}}) \wedge \cdots \wedge \psi_l(\vec{\mathbf{x}})$ est une conjonction de formules atomiques et $\theta(\vec{\mathbf{x}})$ est une formule atomique.

Exemple 1 : Les énoncés exprimant la simplifiabilité, la séparativité forte et la séparativité sont des formules de Horn universelles. L'énoncé exprimant le raffinement n'est pas une formule de Horn universelle.

Définition 6 : La **théorie universelle** de $\mathcal{S}$ est l'ensemble des formules de Horn universelles qui sont vraies dans tous les semigroupes de $\mathcal{S}$. On dit que la théorie universelle de $\mathcal{S}$ est **décidable** si il existe un algorithme prenant en entrée une formule de Horn universelle φ et déterminant si φ est vraie dans tous les semigroupes de $\mathcal{S}$.

Exemple 3 : L'énoncé $(\forall x,y)(x+y = 2y \implies x = y)$ appartient aux théories universelles des semigroupes simplifiables et fortement séparatifs, mais pas à la théorie universelle des semigroupes séparatifs.

Propriété 1 : Pour décider tous les problèmes de mot de $\mathcal{S}$, il suffit de pouvoir décider la théorie universelle de $\mathcal{S}$.

Voici deux résultats classiques.

Théorème 3 : La théorie universelle de $(\mathbb{R}, +, 0, \leq)$ est décidable (folklore).

Théorème 4 : La *théorie du premier ordre* de $(\mathbb{N}, +, 0, \leq)$ (arithmétique de Presburger) est décidable (cf.[2]).

Propriété 2 : La théorie universelle des semigroupes simplifiables est décidable.

En effet, pour qu'une formule de Horn universelle φ donnée soit vraie dans tous les semigroupes simplifiables, il faut et il suffit qu'elle soit vraie dans un certain quotient d'une puissance finie de $\mathbb{Z}$; nous pouvons conclure grâce au **Théorème 2**.

Corollaire 1 : (cf.[5, 7]) La théorie universelle des semigroupes séparatifs (resp. fortement séparatifs) est décidable.

Question ouverte : La théorie universelle des semigroupes de raffinement est-elle décidable?

De nouvelles techniques (cf. [6]) semblent assez prometteuses pour répondre à cette question. Nous en donnons un léger aperçu.
Construction d'un semigroupe de raffinement (non simplifiable):

	a_0	c_0
b_0	d_1	b_1
c_0	a_1	c_1

Nous obtenons $c_0 = a_1+c_1 = b_1+c_1$, et nous pouvons réitérer l'opération (une infinité de fois). On obtient un semigroupe de raffinement non simplifiable.

Références

[1] *P. Ara, K. R. Goodearl, K. C. O'Meara et E. Pardo* , Separative cancellation for projective modules over exchange rings.
Israel Journal of Mathematics **105** (1998), 105–137.

[2] *G. S. Boolos et R. C. Jeffrey*, Computability and Logic.
Cambridge University Press éditeur (1989)

[3] *C. C. Chang et H. J. Keisler*, Model Theory.
North Holland éditeur (1973)

[4] *A. H. Clifford et G. B. Preston*, The algebraic theory of semigroups, Vol I.
Mathematical Surveys of the A.M.S **7** (1961)

[5] *Céline Moreira*, Decomposition of strongly separative monoids.
à paraître dans J. Pure Appl. Algebra

[6] *Céline Moreira*, A refinement monoid whose maximal antisymmetric quotient is not a refinement monoid.
à paraître dans Semigroup Forum

[7] *Friedrich Wehrung* , Restricted injectivity, transfer property and decompositions of separative positively ordered monoids.
Communications in Algebra **22-5** (1994), 1747–1781.

[8] *Friedrich Wehrung* , The dimension monoid of a lattice.
Algebra Universalis **40-3** (1998), 247–411.

Céline Moreira Dos Santos
Département de Mathématiques
Université de Caen
BP 5186
14 032 Caen cedex
France
`cmoreira@math.unicaen.fr`
http://www.math.unicaen.fr/ cmoreira/

Les ontologies pour l'optimisation

Mina Ouabiba

1 Introduction

L'optimisation globale est une branche particulièrement active des mathématiques appliquées car elle correspond à un besoin industriel. Plusieurs applications dans plusieurs domaines (automatique, biochimie, systèmes de production, etc) se ramènent à la recherche d'optima globaux. Nous nous intéressons à la résolution de problèmes continus non linéaires avec contraintes en utilisant un système basé sur la coopération de différents solveurs. Depuis quelques années, plusieurs systèmes coopératifs ont été développés. Mais, il n'existe pas d'architectures de coopération génériques [1].

L' ingénierie de connaissance s'est orientée vers la construction de bibliothèques de composants génériques réutilisables afin de minimiser le temps de développement, et de faciliter leur évolutions et leur maintenances. La plupart des méthodologies existantes (CommonKADS, Protégé II,..) décrivent une base de connaissances en utilisant les trois concepts : tâche, PSM (méthodes de résolution de problèmes) et domaine. Une telle séparation entre le traitement à faire, le raisonnement utilisé pour réaliser un traitement donné et les données du domaine d'application nous permet de voir la construction d'une base de connaissances comme un assemblage de ces trois composants préalablement décrits et testés (figure1).

Nous allons modéliser les méthodes coopératives d'optimisation non linéaires basées sur l'analyse d'intervalle [2] et les techniques de satisfaction de contraintes. Ce modèle intègre les trois concepts tâche, méthodes de résolution de problèmes et domaine, ainsi que toutes les relations sémantiques entre ces trois concepts. Ces relations seront décrites comme des entités indépendantes des composants qu'elles lient donc pouvant être elles mêmes réutilisées. la description de ce modèle sera réalisée à l'aide de la notion d'ontologie.

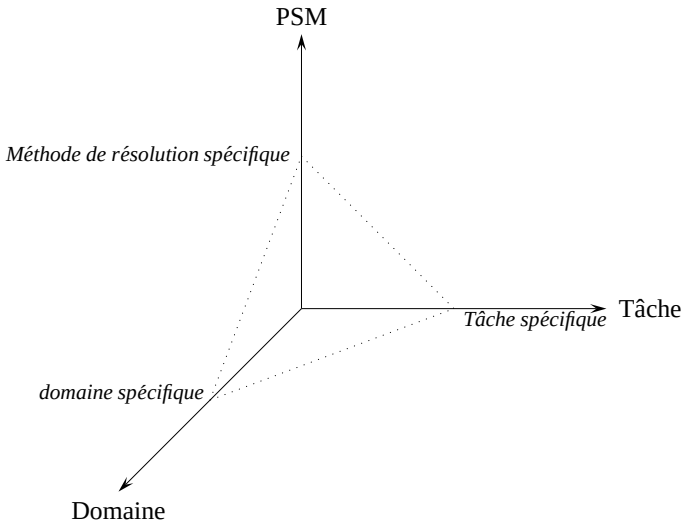


FIG. 18 – *Application (ensemble de composants)*

2 Présentation du problème

Considérons une fonction $f : D \subseteq \Re^n \rightarrow \Re$ appelée critère, ou fonction objectif. On se donne un ensemble de contraintes :

$$C = \{x \in \Re^n / g_i(x) = 0, i \in I, h_j(x) \leq 0, j \in J\}$$

où les fonctions g_i et $h_j : \Re^n \rightarrow \Re$ sont définies sur $\Re^n$. On définit un problème d'optimisation par un triplet (f, C, D) ou par un couple (f, Ω) tel que Ω représente l'ensemble des points admissibles qui est définit par:

$$\Omega = \{x \in D / x \in C\}$$

Définition 1 : On appelle **solution optimale d'un problème d'optimisation** P=(f, C, D) (ou optimum global) une solution qui optimise (maximise ou minimise) f(x) sur l'ensemble de toutes les solutions.

Définition 2 : On dit qu'un vecteur x est un optimum local de $P = (f, C, D)$ si et seulement s' il existe un voisinage V(x)$\subseteq \Omega$ de x tel que x soit un optimum global du problème.

Notre objectif est de construire une bibliothèque de composants génériques. Les approches orientées bibliothèque de composants qui ont été définies que ce soit en ingénierie de connaissances ou en génie logiciel décrivent souvent des composants de même type ou bien spécifiques à une application. Une bibliothèque qui intègre des composants de différents type et les informations permettant de les assembler élargirait le champ de son utilisation et

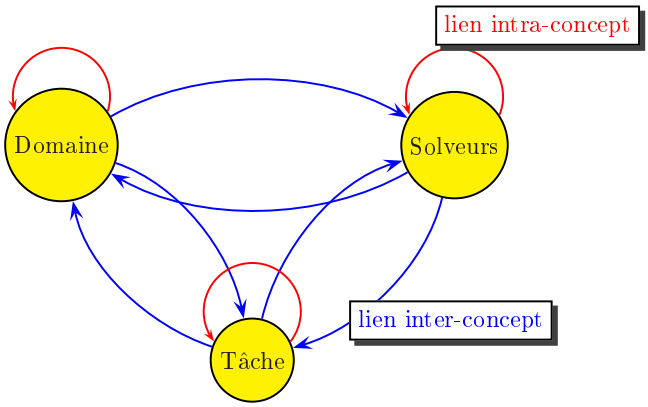


FIG. 19 – *Les concepts et les liens*

réutilisation. Les composants seront décris de manière indépendante les uns des autres en utilisant la notion d'ontologie dans un souci de réutilisation et de partage.

Nous allons tout d'abord définir ce qu'est une ontologie. La définition la plus utilisée est celle de Gruber [3] "une ontologie est la spécification d'une conceptualisation" . Elle définit le vocabulaire et la sémantique associée qui permettent à deux agents de communiquer sur un domaine de connaissances donné. Concrètement, une ontologie est une représentation d'un domaine à l'aide d'une hiérarchie de relations de généralisation et de spécifications de concepts et un ensemble de relations sémantiques entre ces concepts.

3 Description du modèle de coopération

Notre modèle se base sur trois concepts qui sont la tâche, les méthodes de résolution de problèmes et le domaine.

- La tâche : spécifie une action et une méthode pour réaliser l'action qui définit le but poursuivi par la tâche.
- La méthode de résolution de problèmes: représente la méthode qui réalise une tâche. Elle peut être une primitive de résolution ou bien composée de sous tâches.
- Domaine : représente la description des données d'un domaine particulier.

Ces trois concepts sont liés pour construire une application. Afin de pouvoir réutiliser ces trois concepts, par exemple réutiliser une méthode de résolution pour réaliser plusieurs tâches dans différents domaines, des liens sémantiques inter-concepts et intra-concepts ont été définit (figure 2).

Un lien inter-concepts est un lien entre deux concepts différents par exemple la relation entre une tâche qui consiste à chercher un optimum local et une méthode d'exploration locale.

Un lien intra-concepts est un lien entre deux concepts de même type par exemple la relation qui définit la transformation symbolique de la fonction objectif et les fonctions qui définissent les contraintes d'un problème d'optimisation. Cette transformation permet de réduire le nombre d'occurrences des variables afin d'augmenter la précision des calculs d'intervalles.

Au niveau ontologique, une tâche est spécifiée par son nom, les données d'entrée, les données de sortie, son but c'est à dire le problème à résoudre ainsi que les liens qui lui sont attachés. La méthode de résolution de problèmes est spécifié par son nom, son entrée, sa sortie, ses compétences (par exemple, une méthode locale ou globale) à résoudre un problème, toutes les informations sémantiques (par exemple la convergence d'une méthode d'optimisation nécessite la convexité de la fonction objectif) et les liens qui lui sont attachés. La description d'un domaine pour différentes tâches et différentes méthodes de résolution doit être faite suivant plusieurs niveaux de généricité. L'ontologie de domaine est décrite par les concepts d'un domaine tels que les relations sémantiques inter-concepts, les propriétés de ces relations (binaire, transitive, etc), les informations sémantiques (contraintes linéaires, quadratiques, fonction objectif convexe, etc) et les différents liens qui lui sont attachés. Un lien sémantique décrit une relation entre deux concepts qu'elle lient. Elle est doté d'une sémantique et d'un comportement propre permettant aux entités liées de communiquer et de collaborer.

4 Conclusion

Nous avons décrit d'une manière générale notre modèle qui définit une bibliothèque permettant d'intégrer des tâches, des PSM et des domaines. Pour cela, nous nous sommes basés sur les travaux effectués dans le domaine du génie logiciel et de la représentation de connaissances.

Références

[1] *L. Granvilliers, E. Monfroy and F. Benhamou*, Symbolic-Interval Cooperation in Constraint Programming. In Proceedings of ISSAC'2001, 26th International Symposium on Symbolic and Algebraic Computation, 2001

[2] *E. Hansen*, Global optimization using interval analysis, Marcel Dekker, 1992.

[3] *T.R GruberE*, Toward Principles for the Design of Ontologies Used for Knowledge sharing. In Nicola Guarino and Roberto Poli, editors, Formal Ontology in Conceptual Analysis and Knowledge Representation . Kluwer Academic Publishers , 1993.

Mina Ouabiba
Institut de recherche en Informatique de Nantes
Université de Nantes - Faculté des Sciences et Techniques
2, rue de la Houssinière, BP 92208
44322 Nantes Cedex 03
France
ouabiba@irin.univ-nantes.fr

Reconnaissance automatique des parties du discours

Anna Pappa

Abstract

Cet article présente un système informatique, combinant l'intelligence artificielle et la linguistique, capable de reconnaître les parties du discours et de faire émerger des structures du langage très variées sans aucune connaissance préalable. L'algorithme ne comporte pas de dictionnaire et il utilise un minimum de règles grammaticales et syntaxiques.

1 Introduction

Le système développé est basé sur des règles grammaticales [1] qui sont établies sans recours à l'étiquetage traditionnel [2]- même en utilisant des procédures automatiques [3]- ou à d'énormes bases de données d'entrées lexicales. Il procède à la détermination de l'étendue de différents groupes (ou syntagmes) syntaxiques qui composent une phrase : les syntagmes substantifs (SS), les syntagmes verbaux (SV), et les syntagmes prépositionnels (SP), qui se décomposent en une préposition suivie d'un SS ou SV. À la fin de l'analyse, le système crée un dictionnaire séparant les mots en deux catégories : noms et verbes. Le cadre de travail est énonciatif [4], structuraliste [5], fonctionnaliste [6] et prend en compte l'aspect dynamique du langage. Pour notre analyse, nous avons utilisé un corpus (environ 4.000.000 de mots) de textes français de différents auteurs sur des sujets et des styles différents.

2 Méthode suivie

La méthode que nous avons adoptée est basée sur l'étude des catégories grammaticales - syntaxiques sans avoir recours aux connaissances lexicales. Notre méthode fait partie des programmes qui utilisent :

- la division du système des règles en niveaux et,
- la méthode d'analyse morphologique (découpage et interprétation).

Les statistiques effectuées sur le corpus sont basées sur l'analyse distributionnelle [7]. Les régularités relevées forment les règles de notre système.

3 Système réalisé

Les textes sont découpés en phrases. Les mots sont classées dans les colonnes d'un tableau. Le **noyau** de ces phrases est la colonne qui comporte les mots dits grammaticaux (articles, pronoms, etc.), les colonnes qui précèdent le noyau contiennent les mots qui se trouvent juste avant les mots grammaticaux (MG)et constituent le contexte gauche (CG) et les colonnes qui suivent contiennent les mots qui se trouvent après les MG et forment le contexte droit (CD). Le tableau qui suit est un exemple, les phrases sont issues des textes différents :

j'	*ai*	un	*peu*	*de*	*fièvre*	*depuis*	*quelques*	*jours*
et	*voilà*	un	*jeune*	*homme*	*très*	*bien*	*fait*	*et*
les	*peuples*	des	*Nations*	*Unies*	*ont*	*proclamé*	*à*	*instaurer*
et	*qui*	la	*dévorait*	*des*	*yeux*	.	*CHAPITRE*	*HUITIEME*

Le développement de cette démarche a été basé sur les marques grammaticales [8] ou marques de repérage. Les mots sont distinctement séparés en tenant compte des particularités de la langue française, par exemple les mots composés. Le système est un "parseur" basé sur des travaux statistiques [9] avec résolution des cas ambigüs[2], sans avoir étiqueté aucun mot auparavant, et il détermine les groupes syntaxiques sans recours aux grammaires des arbres [10] compactées ou non [11]. Nous citons quelques règles et nous décrivons leur fonctionnement:

N°	*CG2*	*CG1*	Noyau	*CD1*	*CD2*	*CD3*	*CD4*	*CD5*	*CD6*	*Déc*	*Cas*	*Flag*
1	*	*	*	*=Verbal*	*	*	*	*	*	*SV*	*nég ou t.v*	*1*
2	*	*	*	*	*=De*	*	*=Relatif*	*	*	*CD4=m.a*	*Dét*	*4*

La première ligne définit le rôle de chaque colonne. La première colonne indique le n° des règles[3]. Les deuxième et troisième colonnes contiennent le CG du noyau. La quatrième colonne contient les mots grammaticaux, ensuite viennent six colonnes[4] avec le CD du noyau. Les trois dernières colonnes indiquent la **décision**, où il est indiqué la marque d'arrêt (m.a) du syntagme, le **cas** où la décision se justifie, et le **flag** qui nous permettra de constituer notre dictionnaire à la fin du traitement. Nous présentons quelques exemples

2. Par exemple l'ambiguïté entre article défini et pronom personnel : le, la, les, l'.

3. L'étoile signifie n'importe quel mot, le "="renvoit automatiquement à une fonction traitée par le moteur(Parsing). Le moteur appelle la fonction la fonction (=Verbal) ou (=Relatif) et autres mentionnées dans le tableau de règles.

4. Les statistiques ont montré qu'il est vraiment rare de rencontrer un SS -beaucoup moins un SV- qui s'étend au-délà de 7 mots à son contexte droit après le déterminant.

extraits des textes traités :

385	*ruisseaux*	*dont*	aucun	*ne*	*va*	*de*	*droit*	*fil*	,	*SV*	*sub*	*1*
134	*donc*	*comme*	une	*galerie*	*de*	*peintures*	*dont*	*les*	*traits*	*CD4=m.a*	*Relatif*	*4*
171	*roule*	*sur*	des	*choses*	*indifférentes*	.	*Après*	*dîner*	,	*CD3=m.a*	*Prép+SN*	*3*

Notre analyse se termine avec *la création d'un dictionnaire* qui contient les mots qui se trouvent immédiatement à droite des mots grammaticaux : il y a des déterminants qui ne peuvent être suivis que par un nom (soit substantif soit épithète) dans la plupart des cas, par exemple les possessifs (sa maison). Pour ces cas où l'ambiguïté est peu probable (flag 1), nous avons développé une procédure qui enregistre les mots[5] de la colonne **CD1** dans un dictionnaire. Les mots sont étiquetés en deux catégories verbale ou nominale:

N°	**CD1**	**Type**	**Texte d'origine**
282	abstinence	nominal	Paresse
62	armée	nominal	Luc
68	coin	nominal	Pin-Up
254	diable	nominal	Luc
4627	accablait	verbal	Les-Cenc
4523	accompagnai	verbal	domi
11	aller	verbal	Rêveries
161	apprirent	verbal	Luc

4 Conclusion

Le système développé procède à une analyse des marques (mots grammaticaux) sans connaissance préalable sur leur nature et leur fonctionnement. Les taux de réussite sont répartis ainsi : 93% des cas résolus (reconnaissance des SS et SV précédés ou non d'une préposition), dont le taux d'erreur varie entre 0 et 1%, et 7% les cas non résolus. L'algorithme est utilisé également pour résourdre les cas ambigüs (entre article défini et pronom personnel). Cette analyse peut s'effectuer à d'autres langues qui ont la même structure syntaxique que le français (en cours d'étude la langue grecque). La création du dictionnaire à partir du contexte droit des mots grammaticaux peut s'avérer précieuse pour un traitement où le système chercherait des informations supplémentaires dans les entrées lexicales dont le type grammatical est déjà connu.

5. En leur forme fléchie

Références

[1] *G. Sabah*, L'intelligence artificielle et le langage, processus de compréhension, éd. Hermès (1989) vol.2

[2] *J. Vergne, E. Giguet*, Regards théoriques sur le tagging, In proceedings of the fifth annual conference Le Traitement Automatique des Langues Naturelles (TALN 1998), Paris, France, June 10-12.

[3] *E. Brill*, Unsupervised Learning of Disambiguation Rules for Part of Speech Tagging, To appear in Natural Language Processing Using Very Large Corpora. Kluwer Academic Press (1997)

[4] *A. Culioli*, Pour une linguistique de l'énonciation, Opérations et représentations, Orphys (1990) vol. 1

[5] *E. Benveniste*, Saussure après un demi-siècle, in Problèmes de Linguistique Générale, Paris, (1966) chap. III

[6] *J. Vachek*, Dictionnaire de linguistique de l'école de Prague, Anvers, Utrecht (1966)

[7] *Z.S. Harris*, Distributional Structure, Word (1954), p 146-162.

[8] *G. Bernard*, Typologie neuromimétique des substantifs, rapport de recherche 94-06-17-1, laboratoire d'Intelligence Artificielle de l'Université Paris 8 (1994)

[9] *E. Charniak*, Statistical parsing with a context-free grammar and word statistics, in Proceedings of the Fourteenth National Conference on Artificial Intelligence, AAAI Press / MIT Press (1997)

[10] *M. Marcus, et al.*, The Penn Tree-Bank: Annotating predicate argument structure, in Proceedings of ARPA Speech and Natural Language Workshop (1994)

[11] *Y. Wilks, et al.*, Compacting the Penn Treebank Grammar, in Proceedings of the COLING-ACL (17th Int. Conf on Computational Linguistics), Montreal (1998)

Anna Pappa
Groupe CSAR - Laboratoire d'Intelligence Artificielle
Université Paris 8
2, rue de la liberté
93526 Saint Denis Cedex - France
ap@ai.univ-paris8.fr
http://www.ai.univ-paris8.fr/ ap

Structure de treillis et modèle de Chip Firing Games

Ha Duong Phan

Resumé : *Dans ce papier, nous étudions un système dynamique discret classique, le Chip Firing Game, utilisé comme un modèle dans la physique, l'économie et l'informatique [1, 2, 3, 11, 12]. Nous utilisons la théorie des ordres et des treillis pour montrer que l'ensemble des configurations accessibles à partir d'une configuration quelconque est un treillis, qui implique des propriétés fortement structurelles.*

Définition 1 : **Un Chip Firing Game, (CFG)** [2] est défini par la donnée d'un (multi)graphe $G = (V,E)$ orienté (appelé *support* du CFG) et d'une répartition d'un certain nombre de jetons (chips) sur chaque commet (*la configuration initiale* du CFG). La règle d'évolution est alors : si un sommet a au moins autant de jetons que d'arcs sortants, on transfère un jeton le long de chacun de ces arcs.

On peut supposer que les sommets d'un graphe sont indexés par des entiers. Une configuration d'un CFG peut alors être représentée par un vecteur $c = (c_1, \ldots, c_n)$ tel que c_i est le nombre de jetons de i-ème sommet. L'ensemble des configurations accessibles à partir de la configuration initiale est appelé *espace des configuration.* Cet ensemble est muni d'une relation, appelée *relation de successeur* , induite par la règle d'évolution : $a \succ b$ si et seulement si la configuration b peut être obtenue à partir de la configuration a par une application de la règle.

Nous montrons dans ce papier que l'espace des configurations d'un CFG est fortement structurel. Pour cela, nous utilisons la thérie des ordres.

Définition 2 [5]: Un **ordre** est un ensemble muni d'une relation binaire réflexive, transitive et antisymétrique. Considérons deux éléments a et b d'un ordre. Si l'ensemble des éléments plus petits que a et b a un unique élément maximal, on appelle cet élément *l'infimum* de a et b. De façon duale, si l'ensemble des éléments plus grands que a et b a un unique élément minimal, on appelle cet élément *le supremum* de a et b. Sidans un ordre, tout couple d'éléments a un infimum et un supremum, alors cet ordre est un **treillis**.

Le fact que l'espace des confugurations d'un système dynamique a une structure de treillis implique certaines propriétés importantes, comme la convergence. De plus, cette convergence est très forte dans le sens suivant : pour deux configurations de ce système, il existe une unique première configuration obtenue à partir d'elles, et toute configuration qui peut être obtenue à

partir d'elles peut être également obtenue à partir de cette première.

Dans la suite, nous présentons une classe spéciale de CFGs qui joue un rôle central dans notre étude. Les supports de ces CFGs ne contiennent aucune composante fermée.

Définition 3 : **Une composante fermée** d'un multigraphe $G = (V,E)$ est un sous-ensemble S de V non réduit à un élément et tel que :

- S est une composante fortement connexe (c'est-à-dire il existe un chemin de n'importe quel élément de S à n'importe quel élément de S), et

- il n'y a aucun arc d'un sommet de S vers un sommet de $V \backslash S$ (S est fermé)

Nous montrons que dans un CFG sans composantes fermées, la relation de successeur n'a pas de cycles. elle induit donc un ordre sur les configurations accessibles. Nous étendons alors la notion de shot vector (voir par exemple [6]) et nous démontrons que l'espace des configurations est un treillis inférieurement localement distributif.

Lemme 1 *Soit C une composante fortement connexe non fermée. A partir d'une configuration a quelconque, il ne peut pas exister de suite non vide d'application de la règle à des sommets de C telle qu'on obtienne à nouveau a.*

Ce lemme implique que si on n'applique la règele qu'à des sommets qui ne sont pas dans des composantes fermées, on ne peut pas avoir de cycle dans l'espace des configurations, et induit donc un ordre :

Théorème 1 [12] *L'espace des configurations d'un CFG sans composante fermée est ordonné par la clôture réflexive et trasitive de la relation de successeur.*

De plus, on sait [6] que les CFG sont des jeux fortement convergents. En d'autre termes, ou bien un CFG ne s'arrête jamais, ou bien toutes les séquences d'applications de la règle d'une configuration a à une autre b ont la même longueur. Nous allons affiner ce résultat dans le cas des CFG sans composantes fermées. Etant donné une telle séquence p, nous notons $|p|_i$ le nombre d'applications de la règle au sommet i durant la séquence. Commençons par prouver le résultat suivant :

Lemme 2 *Etant donné un CFG sans composantes fermées, si deux séquences s et t d'applications de la règle partent de la même configuration a et amènent à la même configuration b, alors :*

$$|s|_i = |t|_i \text{ pour tout sommet } i.$$

Ce lemme nous permet de définir le *shot vector* $k(a,b)$ de deux configurations a et b si b peut être obtenue à partir de a dans un CFG sans composantes fermées : $k(a,b) = (k_a(a,b), \ldots, k_n(a,b))$ où $k_i(a.b)$ est le nombre d'applications de la règle à i pour obtenir b à partir de a. Nous notons aussi $|k(a.b)|$ la somme $\sum_{i=1}^{i=n} k_i(a,b)$, c'est-à-dire le nombre total d'applications de la règle nécessaires pour obtenir b à partir de a. Si a et b sont deux configurations obtenues à partir de la même configuration O, on définit l'ordre $k(O,a) \leq k(O,b)$ si pour tout i, $k_i(O,a) \leq k_i(O,b)$. De plus, si $a \geq b$, il est clair que $k(O,b) = k(O,a) + k(a,b)$.

Nous pouvons caractériser l'odre entre deux configurations obtenues à partir de la configuration initiale O dans un CFG sans composantes fermées en comparant leurs shot vectors comme suit :

Théorème 2 [12] *Si a et b deux configurations obtenues à partir de la même configuration O d'un CFG sans composantes fermées, alors :*

$$a \geq b \Leftrightarrow k(O,a) \leq k(O,b).$$

Nous pouvons maitement donner le résultat principal de ce papier :

Théorème 3 [12] *L'ensemble de toutes les configurations obtenues à partir de la configuration initiale O d'un CFG sans composantes fermées, ordonné par la clôture réflexive et transitive de la relation de successeur, est un treillis inférieurement localement distributif. De plus, l'infimum de deux éléments a et b est définit comme suit : soit k un vecteur tel que pour tout sommet i, $k_i = max(k_i(O,a),k_i(O,b))$; alors la configuration c telle que $k(O,c) = k$ existe et elle est l'infimum de a et b.*

Nous étudions maintenant la structure de l'esapce des configurations des CFGs quelconques, en particulier ceux dont le support a des composantes fermées. On peut remarquer que dans un tel cas on n'obient pas un treillis, ni même un ordre. Par conséquence, nous proposons une extension naturelle des notions présentées dans les parties précédentes, qui nous amènera à considerer des espaces de configurations structurées en treillis infinis.

Une *configuration étendue* d'un CFG est un couple (i,c) où c est une configuration, et i est le nombre total d'applications de la règle nécessaires pour obtenir c à partir de la configuration initiale. On étend naturellement la notion de la ralation successeur en disant que $(i,a) \succ (j,b)$ si et seulement si $j = i + 1$ et b peut être obtenue à partir de a par une application de la règle. Il est alors évident que l'espace des configurations étendues de n'importe quel CFG ne contient pas de cycle. De plus, il possède une structure de treillis :

Théorème 4 [12] *L'ensemble des configurations étendues obtenues à partir de la configuration étendue initiale* $(0,O)$ *d'un CFG, ordonné par la clôture réflexive et transitive de la relation de successeur, est un treillis inférieurement localement distributif. De plus, l'infimum de deux éléments a et b est définit comme suit : soit k un vecteur tel que pour tout sommet i,* $k_i = max(k_i(O,a),k_i(O,b))$*; alors la configuration* (m,c) *telle que* $k((0,O),(m,c)) = k$ *et* $m = \sum_{i\geq 1} k_i$ *existe etelle est l'infimum de a et b.*

Le modèle CFG est un modle très général, beaucoup de modèles connus peuvent être codés comme des CFGs spéciaux, à savoir les modèles suivants : Modèle de Piles de Sable (SPM) [3, 4, 7, 10], modèle $L(n,\theta)$, modèle $CFG(n,m)$ [10], le Jeux de cartes [8]. Grace à ces codages, on peut voir comment des résultats de ces modèles peuvent être déduits à partir des résulatts du modèle CFG.

Références

[1] *N. Biggs*, Chip Firing and the critical groupe of a graph. Journal of Algebraic Combinatoirics **9** (1999), 25–45.

[2] *A. Bjorner, L. Lovász et W. Shor* , Chip-firing games on graphs. E. J. Combinatorics **12** (1991), 283–291.

[3] *P. Bak, C. Tang et K. Wiessenfeld* , Physics Review Letters . **59** (1987), 381.

[4] *R. Cori et D. Rossin*, On the sand pile group of a graph . LIX Technical Report (1998),

[5] *B. A. Davey et H. A. Prietley*, Introduction to Lattiec and Orders . Cambridge University Press (1990),

[6] *K. Eriksson*, Strongly convergent Games and Coxeter Groups . PhD thesis, Kungl Tekniska Hogskolan, Sweden (1993),

[7] *E. Goles et M. A. Kiwi*, Games on line graphs and sand piles. TCS, **115** (1993), 321-349

[8] *E. Goles, M. Morvan et H. D. Phan*, Lattice structure and convergence of a game of cards . à paraître dans Annals of Combinatorics **12**

[9] *E. Goles, M. Morvan et H. D. Phan*, Sand piles and order structure of integer partitions . a paraître dans Discrete Applied Mathematics

[10] *E. Goles, M. Morvan et H. D. Phan*, The structure of Chip Firing games and related modles . a paraître dans TCS.

[11] *Jan van den Heuvel*, Algorithmic aspect of a chip firing game . London School of Economics, CDAM Reseach Reports (1999),

[12] *M. Latapy et H. D. Phan*, The Lattice structure of Chip Firing Games Physica D (2001),

Ha Duong Phan
LIAFA, Université Paris 7
175, rue Chevaleret, 75013 Paris, France
`phan@liafa.jussieu.fr`
http://www.liafa.jussieu.fr/ phan

Symbole de Kronecker Torique

Herimampita Ratsimbazafy

La théorie des résidus analytiques peut être rapidement résumée de la façon suivante (cf. [3]) :

Etant données $n+2$ fonctions g et f_i, $i \in \{0,\ldots,n\}$, à $n+1$ variables x_i, holomorphes dans un voisinage de $0 \in \mathbb{C}^{n+1}$, telles que les f_i ne s'annulent simultanément qu'en 0, on définit, sous forme intégrale complexe, le résidu local en 0, $res_0(\omega_g)$, de la forme différentielle $\omega_g = \dfrac{g dx_0 \wedge ... \wedge dx_n}{f_0 \cdots f_n}$.

Dans le cas où les f_i sont des polynômes homogènes de degré d et g un polynôme homogène de degré $\rho = (n+1)(d-1)$, l'application associant g à $res_0(\omega_g)$, induit un isomorphisme entre le $\mathbb{C}$-espace vectoriel,
$\mathbb{C}[X_0,...,X_n]_\rho/\langle f_0,\ldots,f_n\rangle_\rho$, des classes, modulo l'idéal $\langle f_0,\ldots,f_n\rangle$, des polynômes homogènes de degré ρ, et $\mathbb{C}$.

D. Cox généralise cette approche analytique sur une variété torique projective et complète sur $\mathbb{C}$. D'autres l'ont poursuivi en étudiant quelques propriétés de ce **résidu torique** (loi de transformation, ...) (cf. [1]).

Dans le cadre algébrique, si $(f) = (f_1,...,f_n)$ est une suite de n polynômes de $\mathbb{C}[X_1,...,X_n]$, vérifiant certaines conditions, on considère le $\mathbb{C}$-espace vectoriel quotient $A = \mathbb{C}[X_1,...,X_n]/\langle f_1,...,f_n\rangle$. On définit le bezoutien généralisé $B(f)$ associé à (f). On peut écrire :

$$B(f) = \sum_i a_i \otimes b_i \in A \otimes A, \text{ où } \{a_i\},\{b_i\} \text{ sont deux bases de } A.$$

Le résidu (affine), appelé aussi Symbole de Kronecker affine, se définit alors comme l'application linéaire de A vers $\mathbb{C}$ telle que :

$$\sum_i \ell(a_i) b_i = 1.$$

Dans [2], une première généralisation de cette approche, au cas torique est amorcée. Elle permet de traiter le cas du Symbole de Kronecker dans le tore associé à une suite de polynômes de Laurent.

Nous poursuivons cette généralisation, en définissant, le Symbole de Kronecker torique pour le cas d'une variété torique complète et simpliciale.

Soit $\mathcal{X}$ une telle variété, de dimension n, associée à un polytope convexe rationnel et fermé P, de $\mathbb{R}^n$. On désigne par $\mathcal{T}$ son tore maximal, et par $\eta_1, \ldots, \eta_s$ les vecteurs primitifs normaux rentrant à P. On note $S = \mathbb{C}[X_1,...,X_s]$ l'anneau de coordonnées multihomogènes de $\mathcal{X}$, et $\deg(X_j)$ le multidegré de X_j.

On considère $n+1$ polynômes multihomogènes, $F_0,...,F_n \in S$, vérifiant certaines conditions.
On appelle multidegré critique pour les F_i, le multidegré $\rho = \sum_{i=0}^{n} \deg(F_i) - \sum_{j=1}^{s} \deg(X_j)$.

On note par $(F_0,...,\widehat{F_i},...,F_n)$ la suite $(F_0,...,F_{i-1},F_{i+1},...,F_n)$.

Une partie I, à n éléments, de $\{1, \ldots, s\}$ est dit ensemble simplicial si les n faces de P, perpendiculaires aux vecteurs $\eta_i, i \in I$, se rencontrent exactement en un sommet de P et si $\det(\eta_I) = \det(\eta_i, i \in I) > 0$. A chaque ensemble simplicial I, on associe l'ouvert :

$$U_I = \{(x_1 : ... : x_s) \in \mathcal{X} \ / \ x_i = 1 \ \forall \ i \notin I\}.$$

C'est une variété affine d'anneau de coordonnées : $\mathbb{C}[X_I] = \mathbb{C}[X_i, i \in I]$. Ces ouverts forment un recouvrement (affine) de $\mathcal{X}$ lorsque I varie.

Comme l'anneau de coordonnées de U_I est un anneau de polynômes à n variables, on a besoin de n polynômes pour définir le symbole de Kronecker sur U_I. On obtient le symbole de Kronecker (affine) relatif à un polynôme F_i : $\ell^I_{F_i}$. C'est une forme $\mathbb{C}$-linéaire sur $\mathbb{C}[X_I]/\langle F_{0I}, \ldots, \widehat{F_{iI}}, \ldots, F_{nI} \rangle$ (où $F_{jI}(X_k, k \in I) = F_j(X_1, \ldots, X_s)$ avec $X_l = 1$ pour $l \notin I$).

Grâce à des résultats de compatibilité entre ces symboles de Kronecker (affines), on obtient, par recollement, la restriction, $\ell^{I_1 \cap ... \cap I_m}_{F_i}$, sur l'intersection de m ouverts U_{I_1}, ..., U_{I_m}, du symbole de Kronecker sur $\mathcal{X}$.

On définit ensuite le symbole de Kronecker sur $\mathcal{X}$, relatif à chaque F_i :

Définition 1 :
Si on désigne par p le nombre d'ensembles simpliciaux, on appelle **Symbole de Kronecker relatif à** F_i, l'application $\mathbb{C}$-linéaire, $\ell^{\mathcal{X}}_{F_i}$ de $S_\rho / \langle F_0,...,F_n \rangle_\rho$ vers $\mathbb{C}$ définie par :

$$\ell^{\mathcal{X}}_{F_i} = \sum_{j=1}^{p} (-1)^{j+1} \sum_{1 \le i_1 < ... < i_j \le p} \ell^{I_{i_1} \cap ... \cap I_{i_j}}_{F_i}.$$

Afin de pouvoir définir le *Symbole de Kronecker torique associé à* $(F_0,F_1,...,F_n)$, on a le résultat suivant, qui donne une relation entre deux Symboles de Kronecker relatifs $\ell^{\mathcal{X}}_{F_i}$ et $\ell^{\mathcal{X}}_{F_j}$ pour $i,j \in \{0,...,n\}$.

Théorème (théorème d'échange) :
Pour tout $i,j \in \{0,...,n\}$, on a : $\ell^{\mathcal{X}}_{F_i}(H) = (-1)^{i+j}\ell^{\mathcal{X}}_{F_j}(H)$.

Définition 2 :
On appelle **Symbole de Kronecker torique** sur $\mathcal{X}$, l'application $\mathbb{C}$-linéaire, $\ell^{\mathcal{X}}$ de $S_\rho/\langle F_0,...,F_n\rangle_\rho$ vers $\mathbb{C}$ définie par :

$$\ell^{\mathcal{X}}(H) = (-1)^i \ell^{\mathcal{X}}_{F_i}(H), \text{ pour } i \in \{0,...,n\}.$$

Notons que $\ell^{\mathcal{X}}(H)$ dépend de l'ordre des variables $[X_1,\ldots,X_s]$.

Propriétés :
Loi de transformation
Soient $F = (F_0,...,F_n)$ et $G = (G_0,...,G_n)$ deux suites de polynômes telles que, pour tout $i \in \{0,...,n\}$, on a : $G_i = \sum_{j=0}^{n} A^i_j F_j$. On note D le déterminant de la matrice de transformation $((A^i_j)_{\ 0\le i,j\le n})$, alors, pour tout polynôme multihomogène H de multidegré critique ρ, on a : $\ell^{\mathcal{X}}(H;F) = \ell^{\mathcal{X}}(DH;G)$.

Valeur au Jacobien torique
Le Jacobien torique de $F = (F_0,\ldots,F_n)$ est, par définition, le déterminant :

$$J(F) = \frac{1}{\det(\eta_I)\prod_{j\notin I} x_j} \begin{vmatrix} F_0 & ... & F_n \\ \partial F_0/\partial x_{i_1} & ... & \partial F_n/\partial x_{i_1} \\ & ... & \\ \partial F_0/\partial x_{i_n} & ... & \partial F_n/\partial x_{i_n} \end{vmatrix}.$$

Il ne dépend pas de l'ensemble simplicial choisi $I = \{i_1,\ldots,i_n\}$.

La valeur du Symbole de Kronecker torique au Jacobien torique est égale au volume normalisé du polytope P, c'est-à-dire :

$$\ell^{\mathcal{X}}(J(F);F) = n!\ Vol(P).$$

Références

[1] *E. Cattani, D. Cox, A. Dickenstein*, Residues in Toric Varieties.
Compositio Mathematica, Vol. 108, pages 35 - 76 (1997)

[2] *M.F. Coste Roy, A. Szpirglas*, Symboles de Kronecker affine, projectif et dans le tore.
Prépublication IRMAR (1998)

[3] *P. Griffiths, J. Harris*, Principles of Algebraic Geometry.
Wiley, New York (1978)

Herimampita Ratsimbazafy
Département de Maths - U.F.R. Sciences
6, Avenue Le Gorgeu
29 285 Brest Cedex
France
ratsimba@univ-brest.fr

Autour des fractals de Rauzy

Anne Siegel

Étant donné un système dynamique, une méthode classique pour étudier la structure locale des orbites est de considérer l'application de premier retour sur un ouvert bien choisi autour d'un point. Pour certains systèmes (automorphismes hyperboliques du tore, difféomorphismes pseudo-Anosov des surfaces entre autres), l'application de premier retour est conjuguée au système de départ. On dit alors que le système original est *autosimilaire*. C'est le cas de l'addition du nombre d'or sur le tore de dimension 1.

A partir du moment où un phénomène d'autosimilarité se produit, une substitution est sous-jacente au système : après avoir découpé l'espace en suffisamment de morceaux, la trajectoire des points de l'ouvert avant qu'ils y reviennent définit une substitution. Le système dynamique symbolique associé à la substitution est l'ensemble des codages, dans la partition, des trajectoires des points du système dynamique. On s'intéresse au chemin inverse : quelles actions sont codées par une substitution donnée ? Ceci revient à caractériser les substitutions qui engendrent un pavage périodique autosimilaire.

Systèmes substitutifs Une *substitution* ou *morphisme itéré* remplace les lettres d'un alphabet fini $\mathcal{A}$ par des mots finis non vides, par exemple $1 \mapsto 12$, $2 \mapsto 1$ sur l'alphabet {1,2}. On étend canoniquement sa définition à l'ensemble $\mathcal{A}^{\mathbb{Z}}$ des mots bi-infinis. Un *point périodique* est un mot bi-infini stable par une itération finie de la substitution. Si la substitution mélange suffisamment les lettres (condition de primitivité), les points périodiques d'une substitution ont même ensemble de facteurs. Les mots bi-infinis ayant cet ensemble de facteurs forment un compact stable par le décalage sur $\mathcal{A}^{\mathbb{Z}}$. Ce système dynamique symbolique, appelé *système substitutif*, est minimal et uniquement ergodique [3]. Il présente des propriétés d'autosimilarité puisqu'engendré par un point périodique pour la substitution.

Substitution de Tribonacci et fractal de Rauzy La substitution de Tribonacci σ est définie par $1 \mapsto 12$, $2 \mapsto 13$, $3 \mapsto 1$. Sa matrice d'incidence, obtenue par linéarisation, a pour polynôme caractéristique $x^3 - x^2 - x - 1$. Ses valeurs propres non dominante sont deux complexes α et $\overline{\alpha}$ tous deux appelés *nombre de Tribonacci*. En particulier, la matrice d'incidence admet dans $\mathbb{R}^3$ une droite dilatante et un plan contractant. On représente le point fixe de σ en une ligne brisée de $\mathbb{R}^3$ en remplaçant chaque lettres du point fixe par le vecteur de base de $\mathbb{R}^3$ correspondant. Cette ligne s'enroule autour de la direction dilatante. Les sommets de la ligne brisée se projettent sur le plan contractant parallèlement

à la droite dilatante sur un ensemble borné dont l'adhérence $\mathcal{R}$ est un compact appelé *fractal de Rauzy*.

Cylindres du fractal de Rauzy et autosimilarité Trois sous-ensembles du fractal de Rauzy se distinguent : les *cylindres* correspondent aux projections des points de la ligne Ces cylindres constituent un recouvrement de $\mathcal{R}$, et Rauzy montrent dans [4] que leurs intersections sont de mesure nulles. Ainsi, les cylindres pavent le fractal de Rauzy. L'autosimilarité du système substitutif se transmet graphiquement sur l'ensemble $\mathcal{R}$ par le fait que chaque cylindre de $\mathcal{R}$ n'est rien d'autre que la copie de $\mathcal{R}$ multipliée par un des complexes α, α^2 ou α^3. Ceci prouve que le fractal de Rauzy est autosimilaire.

Un travail plus approfondi sur la combinatoire de la substitution, montre que le fractal de Rauzy est l'ensemble des sommes de séries en α ayant pour coefficients les suites de 0,1 qui ne contiennent pas trois 1 consécutifs : $\mathcal{R} = \{\sum_{i\geq 0} \varepsilon_i\, \alpha^i;\ \varepsilon_i = 0,1;\ \varepsilon_i\varepsilon_{i+1}\varepsilon_{i+2} = 0\} \subset \mathbb{C}$.

Dynamique du fractal de Rauzy Sur la ligne brisée, on se déplace de sommet en sommet en utilisant les trois vecteurs canoniques. En particulier, on peut translater chaque cylindre par le projeté du vecteur canonique correspondant, tout en restant dans $\mathcal{R}$. Ceci définit un échange de morceaux représenté à la Figure 20. Il est naturel de coder, dans la partition définie par les cylindres, l'action de cet échange de morceaux sur $\mathcal{R}$. Rauzy montre que l'application de codage est injective en mesure, surjective dans le système substitutif associé à la substitution de Tribonacci. Ainsi, *il existe un isomorphisme mesurable entre l'échange de morceaux de $\mathcal{R}$ et le décalage sur le système substitutif.*

Pavage périodique Le quotient de $\mathbb{C}$ par un réseau donné projette l'échange de morceaux sur $\mathcal{R}$ sur une translation torique. Selon [4], ce passage au quotient est neutre (injectif en mesure) : les décalés de $\mathcal{R}$ selon un réseau donné ne s'intersectent pas. Puisqu'ils recouvrent $\mathbb{C}$ par le théorème de Kronecker, on construit ainsi un pavage régulier (voir figure 20).

L'utilisation couplée de la dynamique, des propriétés d'autosimilarité et de la théorie des nombres impliquent ainsi les énoncés équivalents suivants :

- *géométriquement* : le fractal de de Rauzy engendre un pavage périodique et autosimilaire de $\mathbb{C}$,
- *dynamiquement* : le système dynamique engendré par la substitution de Tribonacci est mesurablement isomorphe à une rotation sur un tore,
- *spectralement* : ce système dynamique est à spectre purement discret.

Plus généralement, quelles sont les substitutions qui engendrent un pavage périodique autosimilaire ? D'un point de vue spectral, de telles substitutions engendrent un système dynamique qui est à spectre purement discret.

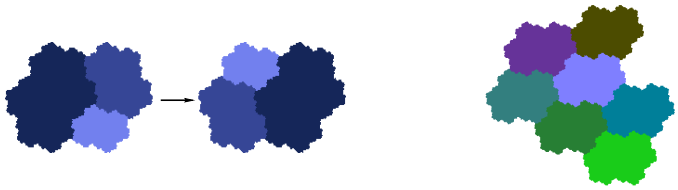


FIG. 20 – *fractal de Rauzy : translation par morceaux et pavage périodique.*

Fractals de Rauzy pour les substitutions de type Pisot On peut construire un fractal de Rauzy pour toute substitution dont la matrice a un espace dilatant de dimension 1 et telle que la ligne brisée correspondant à un de ses points fixes reste à distance bornée de cette droite dilatante. La valeur propre dominante de la matrice est alors un *nombre de Pisot*, et une telle substitution est dite *de type Pisot*. Notons que si la matrice d'incidence n'est pas de déterminant ± 1, le fractal de Rauzy a des composantes p-adiques.

Comme pour la substitution de Tribonacci, le fractal de Rauzy a une structure autosimilaire et est recouvert par d cylindres correspondant aux lettres de l'alphabet, mais rien ne permet d'affirmer que les cylindres s'intersectent sur un ensemble de mesure nulle. Une condition suffisante a été mise en évidence : cette condition purement combinatoire, dite de *coïncidences*, signifie que les points périodiques de la substitution ont suffisamment de parties communes. Sous cette condition, *les cylindres du fractal de Rauzy s'intersectent sur un ensemble de mesure nulle* [1]. On peut alors définir un échange de morceaux sur le fractal de Rauzy de la substitution. *Cet échange de morceaux est isomorphe en mesure au système substitutif de départ.*

Notons qu'on ne connaît aucun exemple de substitution de type Pisot sans coïncidences. Récemment il a été prouvé que les substitutions de type Pisot sur deux lettres sont toutes à coïncidences. *On conjecture que toutes les substitutions de type Pisot vérifient la condition de coïncidences* (voir le survol [2], Chap. 7).

Condition de pavage Comme pour la substitution de Tribonacci, on peut quotienter le fractal de Rauzy d'une substitution de type Pisot avec coïncidences, par un réseau tel que les vecteurs de l'échange de morceaux sont égaux après

passage au quotient. Le système substitutif est alors représenté par une rotation sur un groupe compact qui est le facteur équicontinu maximal du système substitutif sous certaines hypothèses.

Autrement dit, les décalés du fractal de Rauzy d'une substitution par un réseau donné recouvrent l'espace, mais il reste à prouver que ces décalés s'intersectent sur un ensemble de mesure nulle. Ceci est démontré pour les substitutions sur deux lettres. Aucun contre-exemple n'est connu. Un critère algorithmique existe, qui permet de vérifier au cas par cas qu'il y a bien pavage (voir [2], Chap. 7). *On conjecture que la substitution de coïncidences est suffisante pour qu'il y ait pavage/spectre discret.*

Références

[1] *P. Arnoux and S. Ito*, Pisot substitutions and Rauzy fractals, Bull. Belg. Math. Soc. Simon Stevin **8-2** (2001), 181–207.

[2] *P. Fogg*, Substitutions in Dynamics, Arithmetics and Combinatorics. Lecture Notes in Mathematics. Springer-Verlag (to appear). Edited by V. Berthé, S. Ferenczi, C. Mauduit, and A. Siegel.

[3] *M. Queffelec*, Substitution dynamical systems—spectral analysis. Lecture Notes in Mathematics, 1294. Springer-Verlag (1987).

[4] *G. Rauzy*, Nombres algébriques et substitutions, Bull. Soc. Math. France **110-2** (1982), 147–178.

Anne SIEGEL
IRISA
Campus de Beaulieu
35042 Rennes Cedex - FRANCE
asiegel@irisa.fr

Vérification de réseaux paramétrés par analyse d'accessibilité

Tayssir Touili

Les systèmes informatiques sont de plus en plus présents dans le contrôle de tâches critiques et très complexes. Une erreur dans la conception de ces systèmes peut avoir des conséquences graves et irréversibles. C'est pourquoi il est crucial de disposer de méthodes rigoureuses pour les concevoir et de techniques automatiques pour les vérifier.

Le problème de la vérification consiste à s'assurer qu'un système satisfait bien ses spécifications. Ces dernières années, des méthodes de vérification automatiques ont été développées et sont largement utilisées. Seulement, ces méthodes concernent essentiellement les systèmes finis (à nombre fini d'états).

Nous considérons ici le problème de la vérification des réseaux paramétrés de processus, c'est-à-dire, des réseaux comprenant un nombre arbitraire de processus identiques. Il s'agit de vérifier un système quelque soit le nombre de ses composantes. Des exemples de réseaux paramétrés sont les algorithmes d'exclusion mutuelle, les protocoles de communication entre un nombre arbitraire de processus,...etc. La vérification de tels systèmes est hors de portée des techniques usuelles de vérification pour les systèmes finis.

Nous réduisons le problème de la vérification des systèmes paramétrés au calcul de l'ensemble des configurations accessibles. Cet ensemble étant infini (dû à la paramétrisation), nous adoptons une approche symbolique basée sur la représentation d'un ensemble infini de configurations par un langage de mots (resp. d'arbres) si la topologie du réseau est linéaire (resp. arborescente). Par exemple, dans le cas des réseaux linéaires, nous représentons l'état global d'un système ayant n processus par un mot de longueur n, en concaténant les états locaux des différents processus. Un ensemble de configurations peut donc être représenté par un langage de mots. Par exemple, l'ensemble des configurations d'un système qui vérifie la propriété d'exclusion mutuelle peut être représenté par n^*cn^* où c (resp. n) exprime que le processus est (resp. n'est pas) dans la section critique.

Une action du programme peut être alors modélisée par une règle de réécriture de mots (ou d'arbres). Ainsi, la règle $a \rightarrow b$ exprime qu'une composante du système passe de l'état a à l'état b.

Par exemple, si nous considérons le cas du "token passing protocol" où un système est formé par un vecteur de processus, l'action qui consiste à faire passer le jeton de la gauche vers la droite peut être modélisée par la règle (ou semi-commutation) $t\perp \rightarrow \perp t$ où t (resp. $\perp$) exprime que le processus a (resp. n'a pas) le jeton. Initialement, c'est le processus le plus à gauche qui a le jeton, l'ensemble des configurations initiales est donc représenté par $t\perp^*$.

Nous réduisons alors le problème de la vérification au calcul de la fermeture d'un langage régulier par un système de réécriture, c'est à dire au calcul de $R^*(L)$, où L est un langage régulier d'arbres ou de mots, et R est un système de réécriture. Ce problème étant indécidable, notre but est de:

- Proposer des sous-classes $\mathcal{L}$ de langages réguliers et $\mathcal{R}$ de systèmes de réécriture pour lesquelles le calcul de la fermeture de tout langage de la classe $\mathcal{L}$ par un système de réécriture de la classe $\mathcal{R}$ est effectif.
- Définir une approche symbolique générale (semi-algorithmique) pour le calcul de l'ensemble des accessibles.

Dans cet exposé, nous nous restreignons au cas des réseaux linéaires, c'est à dire aux langages réguliers de mots sur un alphabet fini Σ. Nous présentons dans ce qui suit deux résultats principaux:

1. Fermeture des APCs par semi-commutations

Dans un premier temps, nous considérons les semi-commutations, i.e., les règles de la forme $ab \rightarrow ba$. Ces règles apparaissent de manière naturelle dans la modélisation d'un grand nombre de protocoles, tel que le "token passing protocol" considéré précédemment. Notre but est alors de calculer $R^*(L)$ pour un langage régulier L et un ensemble de semi-commutations R. Seulement, ce type de règles ne préserve pas la régularité. En effet, pour $R = ab \leftrightarrow ba$, le langage $R^*((ab)^*)$ n'est pas régulier puisque c'est l'ensemble de tous les mots de $(a + b)^*$ qui contiennent le même nombre de "a" et de "b". Nous voulons alors une sous-classe des réguliers qui soit effectivement fermée par semi-commutations. Nous avons identifié la classe des *Alphabetic Pattern Constraints* (APC):

Définition 1 : Un langage **APC** est une union finie de langages de la forme $\Sigma_0^* a_1 \Sigma_1^* \cdots a_n \Sigma_n^*$, où les Σ_i sont des ensembles finis de lettres, et les a_i sont des lettres.

Cette classe de langages apparaît naturellement dans la modélisation des ensembles de configurations des réseaux paramétrés. Par exemple, le langage $\Sigma^* c \Sigma^* c \Sigma^*$ représente l'ensemble des configurations qui ne satisfont pas l'exclusion mutuelle.

Nous avons montré que cette classe est effectivement fermée par semi-commutations :

Théorème 1 [3] : Soit R un ensemble de semi-commutations, et L un langage APC, alors $R^*(L)$ est un langage APC et peut être effectivement calculé.

2. Calcul des accessibles par "*regular widening*"

De manière plus générale, nous adoptons une méthode semi-algorithmique basée sur l'accélération de la terminaison du calcul, qui permet de calculer une

sur-approximation de l'ensemble des accessibles. En effet, ceci s'avère suffisant pour vérifier certains systèmes.

Le principe de cette méthode nommée *regular widening* [2, 5] consiste à *deviner automatiquement* l'effet de l'itération de R un nombre arbitraire de fois sur un ensemble régulier L donné: si une telle situation

$$L = L_1.L_2 \text{ et } R(L) = L_1.\Delta.L_2$$

est détectée, nous devinons qu'à chaque fois l'effet de R est d'introduire un "Δ" au milieu, nous rajoutons donc $L_1.\Delta^*.L_2$ à l'ensemble des accessibles. Un principe plus général qui tient compte du cas où R introduit plusieurs croissances est défini dans [5]. De manière plus générale, si nous représentons R par un langage de $\Sigma \times \Sigma$, ce même mécanisme permet de deviner l'effet de R^*, la fermeture reflexive-transitive de R.

Ce principe peut être utilisé pour calculer l'ensemble d'accessibilité exact si nous avons un *test* qui permet de décider si l'ensemble deviné est *exactement égal à* $R^*(L)$. Pour définir ce test, nous introduisons quelques définitions:

Définition 2 : Un système de réécriture R est nœthérien s'il n'existe pas une séquence infinie de mots w_0,w_1,... tels que pour chaque $i \geq 0$, $w_{i+1} \in R(w_i)$.

Définition 3 : Si R est un système de réécriture qui comprend les règles $\{l_i \rightarrow r_i\}$, R^{-1} est le système de réécriture qui comprend les règles $\{r_i \rightarrow l_i\}$.

Nous avons alors le résultat suivant dont une partie est due à [4]:

Proposition 1 : Si R ou R^{-1} est nœthérien alors $L' = R^*(L)$ ssi $L' = R(L') \cup L$.

Ainsi, si R ou R^{-1} est nœthérien, nous pouvons utiliser notre *regular widening* pour deviner l'ensemble des accessibles, et appliquer le test précédent pour nous assurer que notre calcul est exact.

Notre méthode s'avère être assez puissante pour simuler plusieurs constructions existantes. En effet, elle peut simuler le résultat du Théorème 1:

Théorème 2 [5] : Soit R un ensemble de semi-commutations, et L un langage APC, alors $R^*(L)$ peut être effectivement calculé par *regular widening*.

Dans [1], Abdulla et al. ont défini la classe des "*règles de réécriture contextuelles*" et ont donné une construction de R^* pour toute règle R dans cette classe. Notre technique est capable de calculer cette fermeture:

Théorème 3 [5] : Soit R une *règle de réécriture contextuelle*, alors R^* peut être effectivement calculé par *regular widening*.

Références

[1] P. A. Abdulla, A. Bouajjani, B. Jonsson, and M. Nilsson. Handling global conditions in parametrized system verification. *Lecture Notes in Computer Science*, 1633:134–150, 1999.

[2] A. Bouajjani, B. Jonsson, M. Nilsson, and T. Touili. Regular model checking. In *12th Intern. Conf. on Computer Aided Verification (CAV'00)*. LNCS, Springer-Verlag, 2000.

[3] A. Bouajjani, A. Muscholl, and T. Touili. Permutation Rewriting and Algorithmic Verification. In *Proc. 17th Symp. on Logic in Computer Science (LICS'01)*. IEEE, 2001.

[4] L. Fribourg and H. Olsen. Reachability sets of parametrized rings as regular languages. In *Infinity'97*. volume 9 of Electronical Notes in Theoretical Computer Science. Elsevier Science, 1997.

[5] T. Touili. Widening Techniques for Regular Model Checking. In *1st vepas workshop*. Volume 50 of Electronic Notes in Theoretical Computer Science, 2001.

Tayssir Touili
Laboratoire LIAFA
Université Paris VII
2, place Jussieu, case 7014
F-75251 Paris Cedex 05
France
`touili@liafa.jussieu.fr`
http://verif.liafa.jussieu.fr/∼touili

Conception d'un chiffrement symétrique par blocs

Marion Videau

1 Introduction

La cryptographie se définit comme un ensemble de procédés visant à protéger une information contre toute forme d'utilisation malveillante par des tiers. Elle recouvre donc plusieurs fonctionnalités dont les principales sont le chiffrement et la signature. Cette présentation concerne la définition et les principaux critères de conception d'un algorithme de chiffrement symétrique.

Un algorithme de chiffrement transforme, grâce à une donnée secrète appelée *clé*, un message dit *texte clair* en un *texte chiffré* destiné à n'être lisible que du destinataire légitime. Pour ce faire, on dispose de deux grandes familles d'algorithmes, les algorithmes à clé secrète, dits aussi symétriques, et les algorithmes à clé publique, ou asymétriques. Les systèmes à clé secrète, les plus anciens, nécessitent le partage du secret entre les interlocuteurs. Les systèmes à clé publique datant de 1976 apportent une solution au partage de la clé. Le destinataire possède une clé dite *privée* connue de lui seul, lui permettant de lire tout message chiffré grâce à sa clé *publique*, connue de tous. Cependant, le problème de la gestion des clés se pose alors en d'autres termes et ces systèmes n'apportent pas une solution définitive dans la mesure où leur lenteur les rend inaptes au chiffrement en ligne. C'est pourquoi la plupart des applications utilisent des systèmes hybrides comprenant un chiffrement asymétrique pour l'échange de la clé secrète et un système symétrique pour le chiffrement des données.

2 Étude d'un algorithme de chiffrement

Hormis les contraintes de vitesse ou de mémoire qui pèsent sur un algorithme de chiffrement, le problème essentiel qui se pose est de pouvoir assurer un niveau de sécurité suffisant au système. Afin d'en évaluer la sécurité, on est amené à faire des hypothèses sur les conditions d'une éventuelle attaque visant à retrouver soit le message d'origine soit la clé de chiffrement. On doit en outre qualifier, voire quantifier, le contexte de l'attaque. On considère tout d'abord qu'on doit faire reposer la confidentialité d'un échange sur le seul secret de la clé. L'expérience prouve en effet qu'il est illusoire de compter sur le secret d'un algorithme qui se trouvera toujours être éventé à plus ou moins longue échéance. On pose donc comme principe qu'un attaquant a à sa disposition toutes les spécifications du système.

On définit en outre divers contextes d'attaques dont principalement celles à chiffré seul, à clair connu et à clair choisi, pour lesquelles l'attaquant dispose respectivement de quelques chiffrés ou de certains couples clairs-chiffrés, soit quelconques, soit correspondant à des clairs de son choix. Enfin, l'attaquant peut aussi tenter de retrouver la clé par *recherche exhaustive*, c'est-à-dire par énumération de l'ensemble des clés possibles pour le système. Si la clé est choisie aléatoirement parmi les mots de k bits, l'attaque nécessite en moyenne 2^{k-1} déchiffrements. Compte tenu de l'état actuel de la technologie, on recommande une taille de clé supérieure à 80 bits. En général, on quantifie la faisabilité d'une attaque par le nombre d'opérations de déchiffrement à effectuer. On considère que pour être sûr, un système ne doit pas permettre des attaques donc le coût est significativement inférieur à celui de la recherche exhaustive.

3 Le chiffrement itératif par blocs

On peut considérer un système de chiffrement *par blocs* comme une permutation d'un mot de n bits en un autre mot de n bits, la permutation étant indexée par une clé de k bits.

Il s'agit d'un système qui divise le texte clair en blocs de taille fixe (en général 64 ou 128 bits) puis les chiffre successivement avec la même clé. Le chiffré est ensuite obtenu par application d'un mode opératoire paliant la faiblesse d'une simple concaténation de blocs.

L'idée générale d'un chiffrement *itératif* est de réaliser un algorithme à partir d'unités élémentaires de chiffrement qui répétées un nombre suffisant de fois produiront un chiffrement cryptographiquement plus résistant qu'une unité isolée. Cette technique a été formalisée au début des années 70 par Horst Feistel. Les notions fondamentales utilisées sont tirées de l'article fondateur de Claude Shannon, *The communication theory of secrecy systems* [1], où sont traitées les bases mathématiques d'un système de communication chiffrée, à partir de la théorie de l'information. Ont été dégagées en particulier les notions de diffusion et de confusion.

La confusion permet de rendre inextricables les liens entre le message clair, la clé et le message chiffré. La diffusion assure la propagation de l'information contenue dans le texte clair et la clé dans tous les bits du texte chiffré.

Les itérations d'une unité élémentaire de chiffrement, ou fonction interne paramétrée par une sous-clé dérivée de la *clé maître*, permettent de répartir les permutations de manière satisfaisante parmi l'ensemble des permutations des mots de n bits afin que les liens entre le clair, le chiffré et la clé soient suffisamment inextricables.

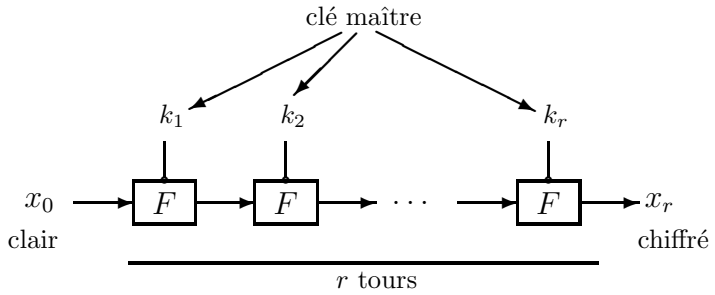


FIG. 21 – *Chiffrement itératif par blocs*

4 Détails de la fonction itérée

Les algorithmes itératifs par blocs se répartissent essentiellement en deux grandes familles suivant la structure de la fonction interne F : la structure de Feistel et la structure substitution-permutation. Elles s'illustrent dans les deux standards successifs de chiffrement à clé secrète : le DES choisi en 1977 et l'AES en 2000.

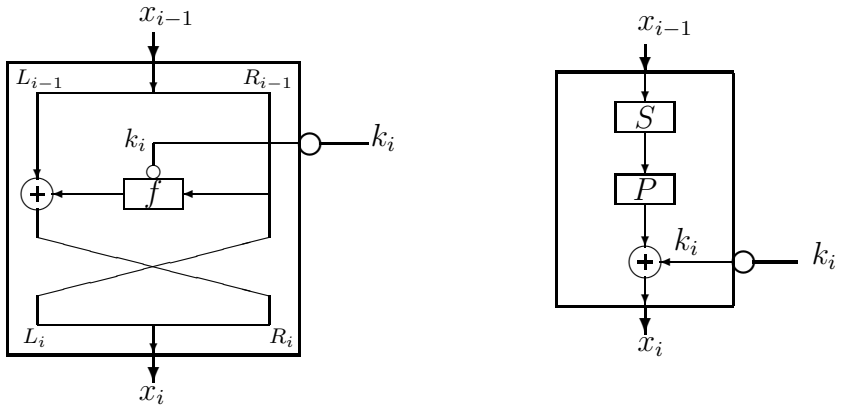


FIG. 22 – *Fonction itérée : à gauche d'un schéma de Feistel, à droite d'un réseau substitution-permutation*

Les chiffrements itératifs par blocs ne possèdent pas de théories mathématiques complètes permettant de se prononcer définitivement quant à leur sécurité. La fiabilité de tels systèmes se mesure d'abord en terme de résistance contre des cryptanalyses connues. L'effort essentiel de formalisation a porté sur les propriétés des fonctions F assurant la meilleure résistance aux deux principales attaques génériques : la cryptanalyse différentielle présentée par Biham et Shamir en 1991 [2] et la cryptanalyse linéaire due à Matsui en 1993 [3]. Les caractéristiques relevées ont conduit au concept de *sécurité démontrable* [4]. Les fonctions présentant des propriétés de résistance optimale contre ces deux types de cryptanalyses sont les fonctions *presque parfaitement non-linéaires* et les fonctions *presque-courbes*.

Ces fonctions sont alors dotées de structures algébriques fortes, exploitables dans d'autres attaques. Il est donc important de pouvoir énoncer de nouveaux critères de sécurité concernant les fonctions utilisées dans des chiffrements itératifs par blocs.

Références

[1] *Shannon (C.E.)* , Communication theory of secrecy systems. Bell System Technical Journal, **28** (1949), pp. 656-715.

[2] *Biham (E.) et Shamir (A.)*, Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, vol.4, **1** (1991), pp. 3-72.

[3] *Matsui (M.)*, Linear cryptanalysis method for DES cipher. Advances in Cryptology - EUROCRYPT'93, LNCS, **765**, pp. 386-397. Springer-Verlag, 1994.

[4] *Nyberg (K.) et Knudsen (L.R.)*, Provable security against differential cryptanalysis. Advances in Cryptology - CRYPTO'92, LNCS, **740**, pp. 566-574. Springer-Verlag, 1993.

Marion Videau
INRIA Projet CODES
Domaine de Voluceau, BP 105
78153 LE CHESNAY Cedex, FRANCE
`Marion.Videau@inria.fr`
http://www-rocq.inria.fr/codes/Marion.Videau/

Existence et unicité de solution pour le problème aux limites associé à certains systèmes hyperboliques de lois de conservation

Nawel ZAIDI

Résumé: Les systèmes de TEMPLE sont des systèmes hyperboliques de lois de conservation dont les ondes de choc et de raréfaction coincident, ils ont été introduits par B. TEMPLE (1983).
Dans ce travail, on montre d'abord l'existence de solutions faibles entropiques pour le problème aux limites associé à ces systèmes dans le cas d'une bande $(a,b)\times\mathbb{R}^+$,et ce par l'approximation parabolique.
On considère ensuite le cas particulier du système d'électrophorèse, X.GENG et C.M. DAFERMOS ont montré l'unicité de la solution pour le problème de Cauchy qui lui est associé par la méthode des caractéristiques généralisées. La positivité de ses valeurs propres nous permet d'adapter cette méthode dans le cas d'un demi plan $(-\infty,b)\times\mathbb{R}^+$ avec une donnée au bord constante; par la suite on utilise ces derniers résultats pour montrer l'unicite de la solution dans le cas d'une bande$(a,b)\times\mathbb{R}^+$, pour ce faire on introduit un prolongement et on montre que le prolongement est unique.

1.Introduction: Soit le système non linéaire de deux équations aux dérivées partielles

$$(S) \qquad \partial_t U + \partial_x F(U) = 0$$

où F est un champ de vecteurs de $\mathbb{R}^2$ dans $\mathbb{R}^2$, U est une fonction vectorielle inconnue de $(a,b)\times\mathbb{R}^+$ dans $\mathbb{R}^2$
(S) est dit hyperbolique si la matrice $\nabla F(U)$ admet deux valeurs propres distinctes, il sera dit de TEMPLE si ses ondes de choc et de raréfaction coincident.
Définition:*On dira que la k-onde de choc coincide avec la k-onde de raréfaction dans un ensemble U,si l'ensemble d'Hugoniot de tout point de U contient U*
Ces systèmes apparaissent dans l'étude de simulation des réservoirs d'hydrocarbures, en élasticité et en chromatographie à multicomposants. En voici certains exemples :

$$(S_1)\begin{cases} \partial_t u + \partial_x(u\Phi(u,v)) = 0 \\ \partial_t v + \partial_x(v\Phi(u,v)) = 0 \end{cases}$$

$$(S_2)\begin{cases} \partial_t u + \partial_x(\dfrac{1}{1+u+v}) = 0 \\ \partial_t v + \partial_x(\dfrac{kv}{1+u+v}) = 0 \end{cases}$$

$$(S_3)\ \partial_t U_i + \partial_x\left(\frac{a_i U_i}{U_1+...+U_n}\right) \quad i = 1,...,n$$

(S_1)apparait dans le problème de simulation des réservoirs d'hydrocarbures et en théorie de l'élasticité, (S_2) apparait dans l'étude de deux composants chromatographiques. (S_3) est le système d'electrophorèse, il modélise la séparation de n composants ioniques.
D. Serre (1987) a étudié l'existence de solutions pour le problème de Riemann et de Cauchy associés à ce genre de systèmes avec donnée initiale à variations bornées, il a montré que la solution est à variations totales décroissantes (résultat remarquable car habituellement propre aux équations).
C.M. Dafermos et X. Geng (1991) ont étudié le problème de Cauchy associé au système d'électrophorèse; par la suite en s'inspirant de leur travail A. Heibig (1994) a généralisé le résultat de l'unicité de la solution pour le problème de Cauchy associé à un système quelconque de la classe de Temple.

2. Existence de solutions faibles pour le problème aux limites associé à un système de Temple : On considère dans unebande $(a,b) \times \mathbb{R}^+$ le problème aux limites suivant:

$$\begin{cases} \partial_t U + \partial_x F(U) = 0, & (x,t)\,]a,b[\times \mathbb{R}^+ \quad (1.1) \\ U(x,0) = U_0(x) & x \in]a,b[\quad (1.2) \\ U \text{vérifie une certaine condition au bord sur } \{a,b\} \times \mathbb{R}^+ & \quad (1.3) \end{cases}$$

où
$\cdot F$ est un champ de vecteurs de $\mathbb{R}^2$ dans $\mathbb{R}^2$
$\cdot U_0$ est une fonction vectorielle définie de (a,b) dans $\mathbb{R}^2$
$\cdot U$ est une fonction vectorielle de $(a,b) \times \mathbb{R}^+$ dans $\mathbb{R}^2$
Le système de deux lois de conservation est supposé hyperbolique et appartenant à la classe de Temple.

On montre le résultat suivant :

Théorème: *Sous les conditions :*
$\cdot F$ *est de classe* C^2 *et* $\|DF\|$ *borné*
$\cdot U_0 \in (BV(a,b))^2 \bigcap (L^\infty(a,b))^2$
Le problème (1.1),(1.2) *admet dans l'espace* $(BV((a,b) \times \mathbb{R}^+))^2$ *une solution faible entropique* U
la condition au bord est formulée comme suit:

$$\begin{cases} \Psi(U(a,t)) - \Psi(U_1) - \nabla\Phi(U_1)(F(U(a,t) - F(U_1) \leq 0 \\ \Psi(U(b,t)) - \Psi(U_2) - \nabla\Phi(U_2)(F(U(b,t) - F(U_2) \leq 0 \end{cases} \quad (1.4)$$

pour tout couple (Φ,Ψ) *entropie- flux d'entropie.*

3. Unicité de la solution pour le problème aux limites associé à l'électrophorèse dans $(-\infty,b) \times \mathbb{R}^+$:On considère le système d'electrophorèse, un

système particulier de la classe de Temple, dans $(-\infty,b) \times\mathbb{R}^+$ sous la forme: $\begin{cases} \partial_t u - \partial_x \left(\frac{v}{u}\right) = 0 \\ \partial_t v - \partial_t \left(\frac{1}{u}\right) = 0 \end{cases}$

On montre le résultat suivant:

Théorème: *Sous les conditions :*

i)(u_0,v_0) *est une fonction à variations bornées et à petites oscillations*
i) l'invariant de Riemann induit satisfait une condition unilatérale de Lipschitz:
$\frac{z_0(y) - z_0(x)}{y - x} \geq -\alpha \quad pourx < y < b$
alors le problème (S) défini par :

$$\begin{cases} \partial_t u - \partial_x \left(\frac{v}{u}\right) = 0 & (x,t) \in (-\infty,b) \times \mathbb{R}^*_+ \\ \partial_t v - \partial_t \left(\frac{1}{u}\right) = 0 & (x,t) \in (-\infty,b) \times \mathbb{R}^*_+ \\ (u,v)\,(x,0) = (u_0,v_0)(x,0) & x \in (-\infty,b) \end{cases}$$

admet une unique solution entropique à variations bornées.

4. Unicité de la solution pour le problème aux limites associé à l'électrophorèse dans $(a,b) \times \mathbb{R}^+$

Soit (E) le problème aux limites associé à l'électrophorèse dans $(a,b) \times \mathbb{R}^+$

$$(E) \begin{cases} \partial_t u - \partial_x \left(\frac{v}{u}\right) = 0 & (x,t) \in (a,b) \times \mathbb{R}^*_+ \\ \partial_t v - \partial_t \left(\frac{1}{u}\right) = 0 & (x,t) \in (a,b) \times \mathbb{R}^*_+ \\ (u,v)\,(x,0) = (u_0,v_0)(x) & x \in (a,b) \\ (u,v)\,(a,t) = (u_1,v_1)(t) & t \in \mathbb{R}^+ \end{cases}$$

On montre le théorème suivant :

Théorème : *Sous les hypothèses*
i)(u_0,v_0) *est une fonction à variations bornées à petites oscillations, et l'invariant de Riemann induit vérifie:*

$$\frac{z_0(y) - z_0(x)}{y - x} \geq -\alpha$$

ii)(u_1,v_1) *est un vecteur constant*
le problème (E)*admet une unique solution à variations bornées.*

Références

[1] *C. BARDOS, A-Y. LEROUX, J-C. NEDELC*, First order quasilinear equations with boundary conditions, comm. in. P.D.E, 4(9), 1017-1034, 1979

[2] *C-M. DAFERMOS, X. GENG*, Generalized characteristics uniqueness and regularity of solutions in a hyperbolic system of conservation laws, Ann. Inst. Henri Poincaré, Vol. 8, n° 3-4, 1991, pp 231 -269

[3] *F. DUBOIS, P. LE FLOCH*, Boundary conditions for non linear hyperbolic systems of conservation laws, J. Diff. Eqts, Vol. 70, 1987, pp 111-131

[4] *A. HEIBIG*, Existence and uniqueness of solutions for some hyperbolic systems of conservation laws, Arch. Rational Mechanics and analysis, 1994, pp 79-101.

[5] *D. SERRE*, Solutions à variations bornées pour certains systèmes hyperboliques de lois de conservation, J. Diff. Eqts. Vol. 68, 1987, pp 137-169.

[6] *B. TEMPLE*, Systems of conservation laws with invariant submanifolds, transaction of the A.M.S, vol.280, 1983, pp781-795.

Nawel ZAIDI
INI-Institut d'informatique
BP. 68M
Oued Smarr-16270-Alger
Algérie
n_zaidi@ini.dz