Groupe de travail LDP

Le critère de Mogbil-Naurois

Marc Bagnol

4 septembre 2013

Introduction

Depuis l'introduction des réseaux de preuve par J.-Y. Girard [4], plusieurs alternatives au critère de correction originel (*long-trip*) et sa reformulation par V. Danos et L. Regnier [2] ont été étudiées par différents auteurs. Un objectif commun de ces travaux était la reduction de la complexité de l'algorithme décidant si une structure de preuve est un réseau. En effet, une implémentation naïve du critère *long-trip* ou Danos-Regnier (DR) aurait une complexité exponentielle (**coNP**, plus précisément).

Une chronologie partielle :

- Contractibilité [1], en temps quadratique ;
- Parsing [7], implémenté en temps linéaire dans [6] ;
- *Dominator tree* [10], également en temps linéaire ;
- Graphe de dépendance [3], en espace logarithmique (non déterministe : **NL**).

De plus, il est prouvé dans [3] que le problème de correction des structures de preuves de MLL est NL-complet.

Dans cet exposé, on va s'intéresser au critère de Mogbil-Naurois (MN), dont l'idée a été reprise par J.-Y. Girard dans [5] sous le nom de *switchings virtuels*.

On commencera par donner quelques intuitions sur la notion de graphe de dépendance, puis on verra une définition précise du critère de Mogbil-Naurois. On terminera par une preuve de séquentialisation directe pour ce critère, sans passer par l'équivalence avec la contractibilité comme cela est fait dans [3].

Références

[1] Vincent Danos : *Une application de la logique linéaire à l'étude des processus de normalisation (principalement du λ-calcul)*. Ph.D. Thesis, Université Denis Diderot, Paris 7, 1990.

[2] Vincent Danos et Laurent Regnier : The structure of multiplicatives. *Arch. Math. Logic*, 28(3):181–203, 1989.

[3] Paulin Jacobé De Naurois et Virgile Mogbil : Correctness of multiplicative (and exponential) proof structures is NL-complete. *In Proceedings of the 21st international conference, and Proceedings of the 16th annuall conference on Computer Science Logic*, CSL'07/EACSL'07, pages 435–450, Berlin, Heidelberg, 2007. Springer-Verlag.

[4] Jean-Yves Girard : Linear logic. *Theoretical Computer Science*, 50(1):1 – 101, 1987.

[5] Jean-Yves Girard : Geometry of interaction VI : a blueprint for transcendental syntax. preprint.

[6] Stefano Guerrini : A linear algorithm for mll proof net correctness and sequentialization. *Theor. Comput. Sci.*, 412(20):1958–1978, avril 2011.

[7] Yves Lafont : From proof-nets to interaction nets. *In Advances in Linear Logic*, pages 225–247. Cambridge University Press, 1994.

[8] Olivier Laurent : Théorie de la démonstration (notes de cours). http://perso.ens-lyon.fr/olivier.laurent/thdem.pdf.

[9] Virgile Mogbil : Complexité en logique linéaire, et logique linéaire en complexité implicite. *mémoire d'HDR, université Paris 13*, 2012.

[10] A. S. Murawski et C. H. L. Ong : Dominator trees and fast verification of proof nets. *In Proceedings of the 15th Annual IEEE Symposium on Logic in Computer Science*, LICS '00, pages 181–, Washington, DC, USA, 2000. IEEE Computer Society.

1 Le graphe de dépendance

La notion de **graphe de dépendance** est l'outil principal permettant de définir un critère de correction vérifiable en espace logarithmique.

Pour motiver la définition, on va commencer par travailler avec des réseaux séquentialisables et identifier quelques propriétés de leurs liens $\parr$.

Définition 1.1 - sctructure séquentialisable

Si π est une preuve du calcul des séquents de MLL, on note $[\pi]$ sa traduction en structure de preuve.

Une structure de preuve R est **séquentialisable** s'il existe π tel que $R = [\pi]$.

Définition 1.2 - structure DR-correcte

Soit R une structure de preuve MLL. Un **switching** $\mathtt{s}$ de R est un choix pour chaque lien $\parr$ d'une de ses deux prémisses.

On associe à chaque switching $\mathtt{s}$ son **graphe de correction** $\mathtt{s}(R)$ défini comme R auquel on a retiré l'arête de chaque lien $\parr$ non choisie par $\mathtt{s}$.

Une structure de preuve MLL est **DR-correcte** si $\mathtt{s}(R)$ est connexe est acyclique pour tout $\mathtt{s}$.

Notation: *on notera* $\mathtt{g}$ *et* $\mathtt{d}$ *les switchings chosissant respectivement gauche ou droite pour tous les liens* $\parr$ *de R.*

On voit facilement par induction que tout réseau séquentialisable est DR-correct. La réciproque est vraie, mais la preuve est moins évidente. Elle repose sur la notion d'empire (voir par exemple [8]).

Considèrons maintenant une structure de preuve séquentialisable R, un de ses graphes de correction $\mathtt{s}(R)$ et un de ses liens $\parr$. L'unique chemin élémentaire entre ses prémisses va rencontrer un certain nombre d'autres liens, en particulier des liens $\parr$. Comme $R = [\pi]$ est séquentialisable, tous ces liens correspondent à des règles du calcul des séquents qui ont nécessairement été appliquées dans π *au dessus* de la règle $(\parr)$ correspondant au lien $\parr$ qui nous intéresse.

Précisons un peu ces idées :

Définition 1.3 - graphe de dépendance

Soit R un réseau de preuve séquentialisable. Le $\mathtt{s}$-graphe de dépendance de R, que l'on notera $\boldsymbol{D}(\mathtt{s}, R)$, est un graphe orienté défini de la façon suivante :

- les nœuds sont les conclusions des liens $\parr$;
- l'arrête $(A \parr B) \leftarrow (C \parr D)$ est présente si le chemin élémentaire de A à B dans $\mathtt{s}(R)$ passe par $C \parr D$. *Un tel chemin existe et est unique par connexité et acyclicité de* $\mathtt{s}(R)$.

Définition 1.4 - ordre d'introduction

Une preuve de MLL π induit un ordre strict sur les formules principales des règles $\parr$ de π, **l'ordre d'introduction** que l'on notera $<_\pi$, défini par

$$F <_\pi G \text{ si } F \text{ a été introduit au dessus de } G \text{ dans l'arbre } \pi$$

On notera $O(\pi)$ le graphe de la relation $<_\pi$.

On voit par induction que le graphe de dépendance d'une structure séquentialisable $[\pi]$ est inclus dans le graphe de l'ordre d'introduction de π.

Théorème 1.5

Soit π une preuve de MLL. Pour tout switching $\mathtt{s}$ de $[\pi]$, on a $\boldsymbol{D}(\mathtt{s},[\pi]) \subseteq O(\pi)$.

Cela permet de déduire la propriété suivante, que l'on retient pour la suite et qui nous guidera pour définir le critère de correction :

Corollaire 1.6

Si π est une preuve de MLL, pour tout switching $\mathtt{s}$ de $[\pi]$ $\boldsymbol{D}(\mathtt{s},[\pi])$ est acyclique.

2 Critère de correction

Les résultats des la section précédente, en particulier le corollaire 1.6, suggèrent un critère de correction basé sur le graphe de correction.

Le problème est évidemment que les définitions et résultats ne valent que pour les structures de preuve *séquentialisables*. Il s'agit donc d'étendre la définition du graphe de dépendance à n'importe quelle structure de preuve pour en faire un outil pour rejeter les structures incorrectes.

On va aller au plus simple : on fixe un switching arbitraire, par exemple le switching "tout à droite" $\mathtt{r}$ et, si on a bien $\mathtt{r}(R)$ connexe et acyclique, utiliser $\boldsymbol{D}(\mathtt{r},R)$. Plus précisément :

Définition 2.1 - graphe de dépendance

Soit R une structure de preuve telle que $\mathtt{r}(R)$ est connexe et acyclique.

On définit le **graphe de dépendance** $\boldsymbol{D}(R)$ de R comme
- ses nœuds sont les conclusions des liens $\parr$;
- l'arrête $(A \parr B) \leftarrow (C \parr D)$ est présente si le chemin élémentaire de A à B dans $\mathtt{r}(R)$ passe par $C \parr D$. *Un tel chemin existe et est unique par connexité et acyclicité de* $\mathtt{r}(R)$.

On note de plus $\boldsymbol{D}^*(R)$ la clôture transitive de $\boldsymbol{D}(R)$.

On a maintenant un ensemble de conditions nécessaires pour qu'une structure soit séquentialisable, que l'on rassemble en un critère de correction. On montrera ensuite que ces conditions sont suffisantes.

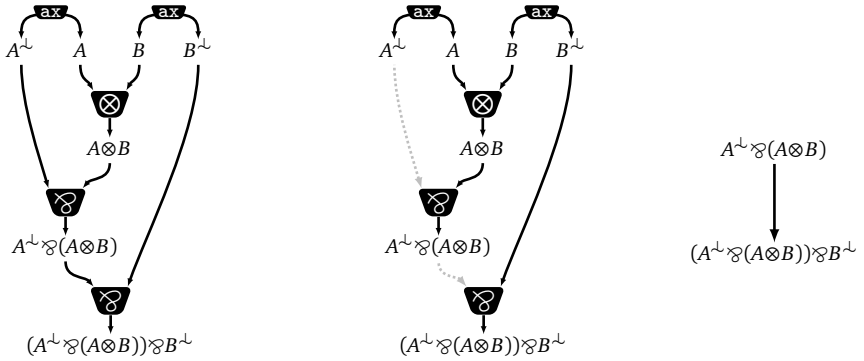

FIGURE 1: UNE STRUCTURE DE PREUVE, SON SWITCHING $\mathtt{r}$ ET LE GRAPHE DE DÉPENDANCE CORRESPONDANT.

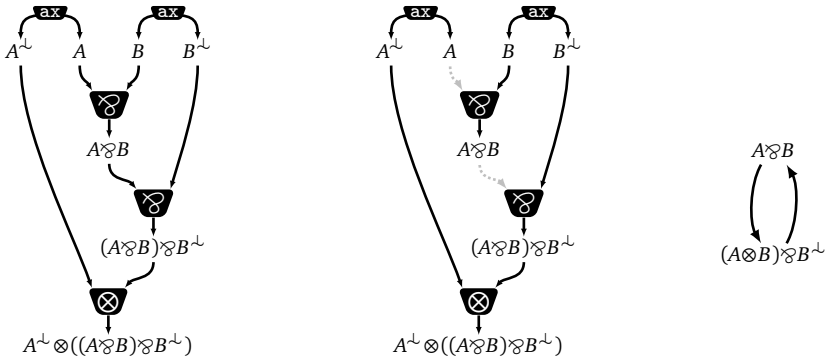

FIGURE 2: UNE STRUCTURE DE PREUVE INCORRECTE. (GRAPHE DE DÉPENDANCE CYCLIQUE)

Définition 2.2 - structure NM-correcte

> Une structure de preuve de MLL est **NM-correcte** si elle satisfait :
>
> 1. $\mathtt{r}(R)$ est connexe et acyclique ;
> 2. $\boldsymbol{D}(R)$ est acyclique.
>
> Dans ce cas, $\boldsymbol{D}^\star(R)$ est le graphe d'une relation d'ordre strict entre les conclusions des liens $\parr$ de R, qu'on notera $<_R$.

Le corollaire 1.6 et la DR-correction des structures séquentialisables impliquent immédiatement :

Proposition 2.3

> Toute structure de preuve séquentialisable est NM-correcte.

On définit les problèmes de décision

NM-CORR : *étant donné une structure de preuve R, est-elle NM-correcte ?*
DR-CORR : *étant donné une structure de preuve R, est-elle DR-correcte ?*

Il est prouvé dans [3] que

Théorème 2.4 - complexité [3]

> NM-CORR est dans **NL**.
> DR-CORR est **NL**-dur.

L'idée est tout d'abord de montrer que le problème SDAG (*étant donné un graphe orienté, est-il acyclique et existe-t-il un nœud* source *tel qu'il y ait un chemin de ce nœud vers tout autre nœud ?*) est **NL**-complet.

La **NL**-dureté de DR-CORR est alors prouvée en y réduisant le problème SDAG.

Le fait que NM-CORR $\in$ **NL** vient du fait que l'on peut générer le switching $\mathtt{r}$ et le graphe de dépendance en espace logarithmique, que le problème TREE (*étant donné un graphe non-orienté, est-ce un arbre ?*) appartient à la classe **L** (espace logarithmique déterministe) et que l'acyclicité du graphe de dépendance est une instance de SDAG [1].

La différence cruciale avec les critères précédemment définis, comme par exemple le parsing, est que ceux-ci nécessitent une modification à la volée de la structure qu'ils manipulent, ce qui ne peut pas être implémenté en espace logarithmique.

1. On a formulé ici le critère de manière un peu différente ce qui fait que l'on n'a pas de nœud *source* pour le graphe de dépendance, mais cela ne change rien à la complexité du problème.

Cependant, bien que l'algorithme présenté dans [3] fonctionne en espace logarithmique non-déterministe sa complexité temporelle est quadratique [9], donc plus importante que pour d'autres critères (par exemple le parsing peut être implémenté en temps linéaire [6]).

Comme les problèmes NM-CORR et DR-CORR s'avèrent finalement être équivalents, on peut les regrouper sous le même problème, MLL-CORR qui est donc **NL**-complet.

3 Séquentialisation

On s'occupe maintenant de montrer la réciproque de la proposition 2.3. Ce que l'on va faire par induction sur le nombre de liens $\parr$ présents dans la structure.

Pour simplifier un peu la preuve, il est commode de généraliser un peu et de rajouter à MLL la règle *daimon*, et d'ajouter aux structures de preuve un lien correspondant :

$$\frac{}{\vdash \Gamma}\ (\maltese) \qquad \overset{\maltese}{\underset{\ldots\ \Gamma\ \ldots}{\cap}}$$

On étend la traduction des preuves de manière évidente. Par rapport au critère de correction le lien $\maltese$ se comporte comme un lien axiome avec un nombre arbitraire de conclusions.

Théorème 3.1 - séquentialisation

> Toute structure de preuve NM-correcte est séquentialisable.

Preuve. On note $|R|$ le nombre de liens $\parr$ de R et on raisonne par induction sur $|R|$.

• **Si** $|R| = 0$ **:** la structure est construite uniquement avec des liens $\otimes$, coupure et axiome. Dans ce cas la NM-correction équivaut à "*R est connexe et acyclique*" et une induction évidente donne une séquentialisation.

• **Si** $|R| > 0$ **:** on choisit $A \parr B$ maximal pour l'ordre strict $<_R$ induit par le graphe de dépendance acyclique. On a alors la situation décrite en FIGURE 3 pour $\mathtt{r}(R)$

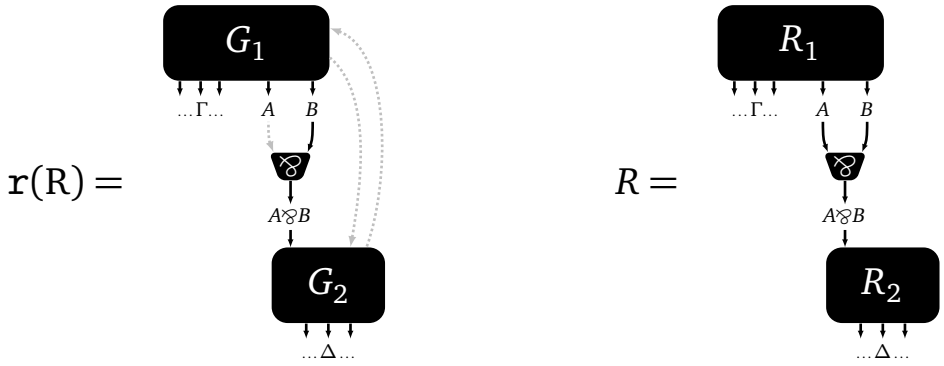

FIGURE 3: DÉCOMPOSITIONS DE $\mathtt{r}(R)$ ET R.

où G_1 et G_2 sont deux parties disjointes, connexes (et acycliques) de $\mathtt{r}(R)$. A est bien connecté à G_1 par la condition **2** du critère : le chemin élémentaire de A à B ne passe pas par $A \parr B$, sinon on aurait $A \parr B <_R A \parr B$ *i.e.* un cycle dans $\boldsymbol{D}(R)$.

Par connexité et acyclicité de $\mathtt{r}(R)$, il est clair que tout lien $\otimes$, axiome ou coupure de R a toutes ses prémisses/conclusions dans le même G_i.

De plus s'il existait un lien $\parr$ avec dont la conclusion $C \parr D$ (et la prémisse D, par connexité et acyclicité) et la prémisse C ne sont pas dans le même G_i, le chemin de D à C passerait par $A \parr B$ et on aurait $A \parr B <_R C \parr D$ ce qui contredirait la maximalité de $A \parr B$.

Les deux points précédents impliquent que G_1 et G_2 sont en fait les graphes de correction $\mathtt{r}(R_1)$ et $\mathtt{r}(R_2)$ de deux sous-structures R_1 et R_2 de R (figure 3).

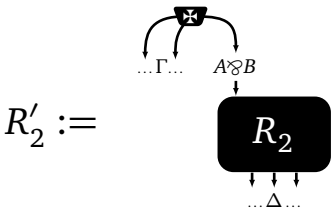

FIGURE 4

Par ailleurs, R_1 et R_2 héritent de la NM-correction de R.

R_1 est séquentialisable par induction, en une preuve π_1 de conclusions Γ, A, B. On pose R_2' (FIGURE 4) qui est également NM-correcte et donc séquentialisable par induction, en une preuve π_2' qui utilise une règle $(\maltese)$ de conclusions $\Gamma, A\otimes B$.

On définit π en remplaçant dans π_2' la règle $(\maltese)$ de conclusions $\Gamma, A\otimes B$ par la preuve π_1 suivie d'une règle $(\otimes)$, de sorte que $R = [\pi]$. ★