

Candidats de réductibilité quantitatifs et logique linéaire élémentaire modulo

Aloïs BRUNEL*

sous la direction d'Olivier Hermant[†] et de Gilles Dowek[‡]

Mars - Juillet 2010

Introduction

La complexité algorithmique a été intensivement étudiée ces dernières décennies. Cependant, aucun résultat significatif de séparation concernant les classes de complexité (comme P, NP ou PH) n'a été établi. Certains pensent que ce manque de résultat provient du fait que les définitions et les caractérisations mathématiques de ces classes de complexité sont toujours insatisfaisantes. Le domaine de la complexité implicite cherche à fournir des caractérisations intrinsèques (qui ne font référence à aucun modèle de calcul spécifique) de ces classes de complexité.

Logiques allégées

En 1995, Jean-Yves Girard introduit la *logique linéaire allégée* ou LLL ainsi que ELL (pour Elementary Linear Logic) dans [18]. Ces logiques, vue au travers de la correspondance de Curry-Howard et notamment via la normalisation des preuves, constituent des langages de programmation capturant respectivement les classes de complexité en temps P et ELEMENTARY. Depuis, un certain nombre d'autres logiques, génériquement appelées *logiques allégées* telles que SLL (pour Soft Linear Logic [23]) ou LAL (pour Light Affine Logic [1]) ont été introduites pour caractériser d'autres classes de complexité.

Orthogonalité et réalisabilité

La réalisabilité est une technique permettant habituellement d'établir des propriétés calculatoires de langages de programmation typés et de fournir des modèles de différents systèmes logiques. De récents travaux basés sur la réalisabilité ont par exemple permis de fournir un cadre uniforme d'étude des logiques allégées, en particulier la réalisabilité de Dal Lago et Hofmann [5] et [6]. La technique des candidats de réductibilité est une autre forme de réalisabilité introduite par Girard [16] pour prouver la normalisation forte du système F , et a été utilisée par la suite dans de nombreuses preuves de normalisation forte, faible ou encore de confluence forte [13] de nombreux systèmes.

Le concept de l'orthogonalité en informatique théorique est basé sur l'observation des interactions entre un programme et des environnements d'exécution. La réalisabilité à la Krivine, basée sur ce concept, a notamment permis de généraliser le forcing de Cohen [3] et de montrer l'indécidabilité de nombreux énoncés en théorie des ensembles [21] et [22].

*<http://perso.ens-lyon.fr/alois.brunel> - alois.brunel@ens-lyon.fr

[†]ISEP - <http://perso.isep.fr/ohermant/>

[‡]équipe TYPICAL, LIX - <http://www.lix.polytechnique.fr/dowek/>

D'autres travaux basés sur la réalisabilité à la Krivine permettent de prouver la correction de compilateurs de langages fonctionnels [19].

L'utilisation de l'orthogonalité de concert avec la technique des candidats de réductibilité (voir par exemple [25] et [29]) permet de construire des preuves de normalisation modulaires et avec un haut niveau d'abstraction. Les candidats de réductibilité pour la logique linéaire en sont un exemple [17]. Une version généralisée de ces candidats linéaires, basée sur la sémantique des phases et proche de la réalisabilité à la Krivine, a été introduite par Okada [27]. C'est cette présentation des candidats de réductibilité linéaires qui constitue le point de départ de notre travail.

Déduction modulo

La déduction modulo, introduite par Dowek et Werner dans [11], est une extension de la logique des prédicats du premier ordre où les axiomes sont remplacés par une congruence et dans laquelle on peut exprimer de nombreuses théories comme la théorie des types simples, l'arithmétique [9] ou encore certaines variantes de la théorie des ensembles [10]. La déduction modulo a l'avantage de fournir un cadre où l'on peut exprimer une notion de réduction des preuves indépendante de la théorie ambiante et de fournir un critère algébrique de normalisation forte d'une théorie appelé *superconsistance* [9].

Candidats de réductibilité quantitatifs

L'objet de ce rapport est l'introduction des *candidats de réductibilité quantitatifs*. Basée à la fois sur les candidats de réductibilité pour la logique linéaire d'Okada, sur la réalisabilité de Dal Lago et Hofmann et des idées issues de la réalisabilité à la Krivine, cette construction permet d'obtenir de manière modulaire et uniforme des bornes de complexité sur la normalisation des réseaux de preuve. Nous appliquons en particulier dans ce rapport la technique à **ELL** et montrons un théorème de normalisation en temps élémentaire de ses réseaux de preuve.

En utilisant les techniques héritées de la déduction modulo, nous montrons également comment obtenir un critère algébrique de normalisation en temps élémentaire d'une théorie (pour **ELL**) donnée appelé *superconsistance*. Nous donnons un exemple concret d'une théorie non triviale satisfaisant ce critère. Nous espérons que ce critère permettra d'étendre plus facilement les langages fonctionnels basés sur les logiques allégées sans perdre leurs propriétés de complexité.

Plan du rapport

Nous rappelons dans la section 1 une version simplifiée de la construction des candidats de réductibilité d'Okada pour le fragment multiplicatif exponentiel de la logique linéaire **MELL**. Dans la section 2, nous introduisons les candidats de réductibilité quantitatifs pour le fragment multiplicatif de la logique linéaire **MLL** qui fournit le cadre général pour l'étude des différentes logiques allégées, puis nous appliquons la technique mise en place à l'étude de la normalisation faible en temps élémentaire de **ELL** dans la section 3. La déduction modulo et le critère algébrique de normalisation en temps borné sont introduits en section 4. Enfin, nous concluons ce travail dans la section 5.

1 Candidats de réductibilité pour la logique linéaire

Dans cette partie, nous introduisons une version simplifiée de la construction d'Okada dans le cas d'une preuve de normalisation faible du fragment multiplicatif exponentiel de la logique

linéaire (MELL). La simplification vient du fait que nous ne cherchons pas à prouver la normalisation forte et nous utilisons uniquement des candidats de réductibilité non typés. Les techniques décrites dans cette partie servent de cadre de base aux autres constructions présentées dans ce rapport.

Il s'agit de définir une relation de *réalisabilité* notée \Vdash entre un programme (ici une structure de preuve) et une formule de *MELL*. $t \Vdash A$ signifie informellement que le programme t se comporte suivant la spécification décrite par la formule A . Nous allons voir comment montrer ainsi des propriétés de normalisation faible. Les notations et les définitions ont été choisies dans le but de clarifier la présentation et de la rapprocher des techniques de réalisabilité à la Krivine.

1.1 Structures et réseaux de preuve de MELL

Nous définissons brièvement le fragment multiplicatif et exponentiel de la logique linéaire (noté *MELL*) ainsi que le langage choisi pour définir la relation de réalisabilité, celui des réseaux de preuve de *MELL* non typés, autrement appelés structures de preuves de *MELL*. Les structures de preuve ont l'avantage d'être munis d'une relation de réduction locale (au contraire du λ -calcul) et possèdent de nombreuses symétries. On définit les structures et réseaux de preuve uniquement de manière informelle, car en faire une présentation rigoureuse serait long et fastidieux. On trouvera dans [15] une introduction plus complète aux réseaux de preuve de la logique linéaire.

Structures de preuve

On introduit d'abord le fragment multiplicatif des structures de preuve ainsi que la relation de réduction associée à ce fragment. On considère des graphes formés à partir des composants (appelés *liens*) de la figure 1. Les noeuds (représentés par des symboles \circ) situés au dessus d'un lien sont appelés *prémisses* et les noeuds situés en dessous d'un lien sont appelés *conclusions*. Les noeuds conclusions qui ne sont prémisses d'aucun lien sont appelés *noeuds pendants*.

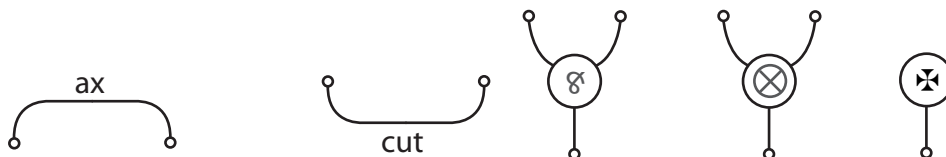


Figure 1: Liens multiplicatifs: axiome, coupure, par, tenseur et daimon

Une *structure de preuve multiplicative* est un tel graphe où chaque noeud est prémisses d'au plus un lien et conclusion d'exactly un lien. Les structures de preuve de *MELL* sont construits de la même manière, en utilisant les liens multiplicatifs ainsi que les liens contraction, affaiblissement et déréluction ((*C*), (*W*) et (*D*)) de la figure 2. De plus si t est une structure de preuve de *MELL*, le graphe obtenu en plaçant t dans une $!$ -boîte est aussi une structure de preuve de *MELL* (voir figure 2).

Le noeud à droite du port $!$ de la boîte est appelé *noeud principal* de la boîte.

Définition 1 (Profondeur). Si t est une structure de preuve, on appelle *profondeur* de t et on note $\partial(t)$ le nombre maximum de boîtes $!$ encapsulées. La profondeur d'une coupure est le nombre de boîtes $!$ encapsulant ce lien coupure.

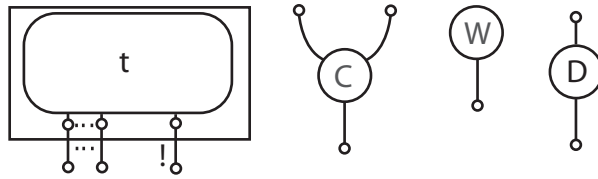


Figure 2: !-boîte et liens exponentiels: contraction, affaiblissement et dérélaction

Réduction

Le langage des structures de preuve multiplicatives est muni d'une relation de réduction $>_{MLL}$: on dit que t se réduit sur u et on note $t >_{MLL} u$ si u est obtenu à partir de t en appliquant une des trois règles de la figure 3. La relation de réduction de **MELL**, notée $>$ contient la relation $>_{MLL}$ ainsi que les réductions décrites dans les figures 4 et 5. On note $t >_0 u$ si t se réduit sur u en éliminant une coupure à profondeur 0 en utilisant n'importe quelle règle autre que (ax/\boxtimes) .

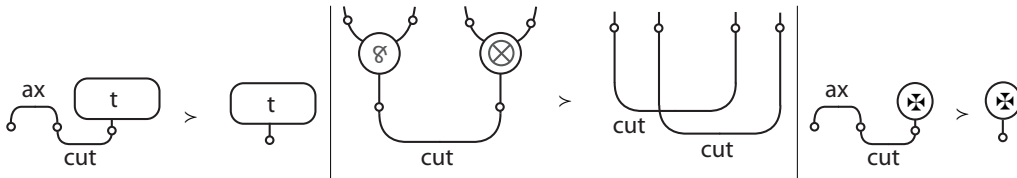


Figure 3: Réduction (ax/cut) , (\otimes/\otimes) et (ax/\boxtimes)

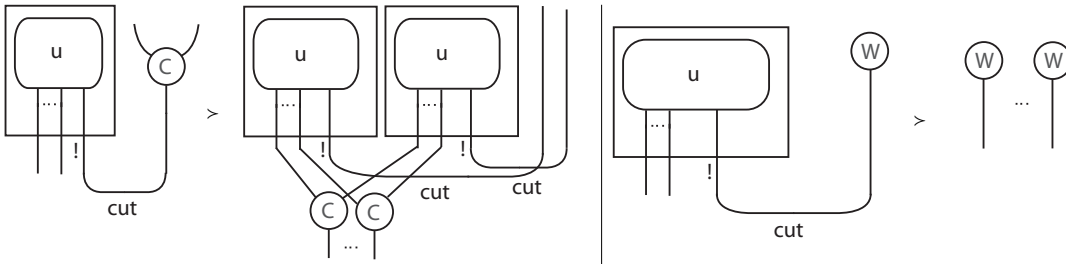


Figure 4: Réduction $(!/C)$ et $(!/W)$

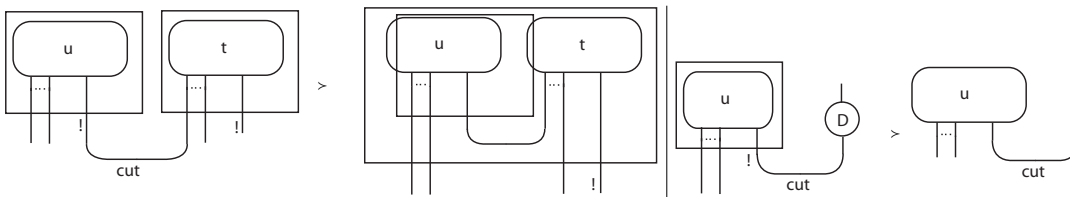


Figure 5: Réduction $(!/!)$ et $(!/d)$

Définition 2 (Mesure de temps). Si t est une structure de preuve, et que R est une suite de réductions $t > t_1 > \dots > t_n$ telle que t_n est en forme normale (on ne peut plus lui appliquer de règle de réduction), alors on note $\#R$ le nombre de règles autre que (ax/\boxtimes) utilisées dans

cette suite de réductions. Si t normalise faiblement, on note

$$Time(t) = \min\{ \#R \mid R \text{ est une réduction partant de } t \text{ et menant à une forme normale pour } > \}$$

Réseaux de preuve

On suppose disposer d'un langage de termes du premier ordre \mathcal{T} (notés s, t , etc.) et pour chaque entier n , d'une infinité de variables du second ordre (notés X, Y , etc.) d'arité n . Le langage des formules de MELL est défini par la grammaire suivante:

$$A, B ::= X(t_1, \dots, t_n) \mid X(t_1, \dots, t_n)^\perp \mid A \otimes B \mid A \wp B \mid !A \mid ?A$$

Les *formules atomiques* sont les formules de la forme $X(t_1, \dots, t_n)$. La négation A^\perp d'une formule A , uniquement définie sur les atomes, peut être étendue inductivement:

- $(A \otimes B)^\perp = A^\perp \wp B^\perp$ et $(A \wp B)^\perp = A^\perp \otimes B^\perp$.
- $(!A)^\perp = ?(A^\perp)$ et $(?A)^\perp = !(A^\perp)$.

Définition 3 (Réseaux de preuve). Une structure de preuve t dont les noeuds sont étiquetés par des formules est un *réseau de preuve* de MLL (resp. de MELL) si il a été construit inductivement en utilisant les règles (Ax) , (Cut) , (\otimes) , (\wp) (resp. toutes les règles) suivantes:

$$\begin{array}{cccc} \frac{}{\vdash A, A^\perp} (Ax) & \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} (Cut) & \frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} (\otimes) & \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \wp B} (\wp) \\ \frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A} (Prom) & \frac{\vdash \Gamma}{\vdash \Gamma, ?A} (W) & \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A} (C) & \frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} (D) \end{array}$$

Les prémisses de chaque règle de construction correspondent à un réseau de preuve déjà construit et les formules étiquettant chacun des noeuds pendants du réseau. On obtient le réseau conclusion en appliquant le lien correspondant à la règle aux formules modifiées. Par exemple: la règle (C) permet d'obtenir un réseau de preuve en reliant par un lien (C) deux noeuds pendants d'un réseau de preuve étiquetés par $?A$.

On notera que le daimon \bowtie n'apparaît dans aucun réseau de preuve.

1.2 Définitions de base

Nous définissons un certain nombre de notions utilisées tout au long de ce rapport.

Définition 4 (Structures pointées). On dit que une structure de preuve est *pointée* si exactement un des noeuds pendants est distingué. S'il existe, cet unique noeud est appelé *noeud distingué* et les autres noeuds pendants sont appelés *noeuds d'environnement*. On note Λ° (resp. Λ) l'ensemble des structures pointées (resp. non pointées).

On notera \bowtie la structure pointée constituée d'un unique lien (\bowtie) et dont l'unique noeud pendant est distingué.

Définition 5 (Interaction). On peut définir une opération $\star : \Lambda^\circ \times \Lambda^\circ \longrightarrow \Lambda$ dite *opération d'interaction*. Si $t, u \in \Lambda^\circ$, alors on définit $t \star u$ comme la structure de preuve obtenue en reliant les deux noeuds distingués de t et u par un lien coupure.

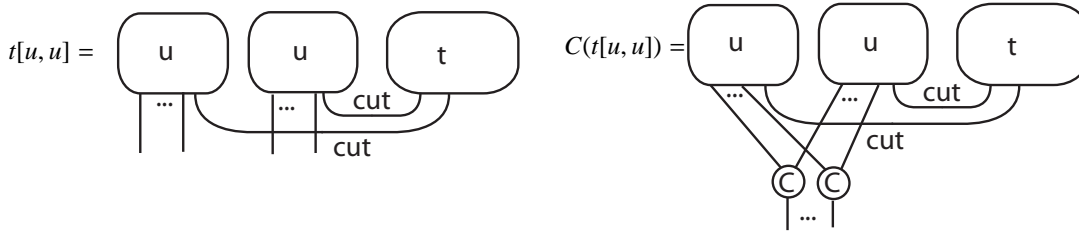
Remarque. Il est à noter que pour tout t , $Time(t \star \bowtie) = Time(t)$.

Si $t \in \Lambda^\circ$ alors on note $[t]!$ la structure pointée obtenue en plaçant t dans une !-boîte, telle que le noeud principal de la boîte soit le noeud distingué de t (qui reste distingué dans $[t]!$). Si $X \subseteq \Lambda^\circ$, on note $[X]! = \{ [t]! \mid t \in X \}$.

Si $t, u \in \Lambda^\circ$, on note $t \otimes u$ l'élément de Λ° obtenu en reliant les deux noeuds distingués de t et u par un lien (\otimes). Le noeud résultant est distingué.

Si t est une structure pointée avec au moins n noeuds d'environnements notés x_1, \dots, x_n , et si u_1, \dots, u_n sont des éléments de Λ° , on note $t[x_1 := u_1, \dots, x_n := u_n]$ (ou simplement $t[u_1, \dots, u_n]$) la structure pointée obtenue en connectant les noeuds x_i aux noeuds distingués des u_i en utilisant un lien coupure.

Si t est une structure de preuve avec au moins deux noeuds d'environnements et $u \in \Lambda^\circ$, $C(t[u, u])$ est la structure obtenue en connectant dans $t[u, u]$ chaque noeud d'environnement x du premier u au noeud d'environnement x dans la seconde copie de u , via un lien contraction.



1.3 Comportements et réalisabilité

Nous décrivons la notion de *modèle de phase calculatoire*, puis nous donnons un exemple pratique de tel modèle: le modèle des candidats de réductibilité. Ces modèles sont basés sur la notion de réalisabilité et d'orthogonalité.

On suppose qu'un ensemble $\perp \subseteq \Lambda$ appelé *pôle* (parfois appelé *observable*) est fixé. Cet ensemble induit une notion d'orthogonalité entre deux structures pointées:

$$t \perp u \text{ ssi } t \star u \in \perp$$

On peut voir \perp comme l'ensemble des structures de preuve "correctes", et $t \perp u$ signifie que t et u interagissent de manière satisfaisante: ils sont *orthogonaux*. Si $X \subseteq \Lambda^\circ$, alors on note X^\perp et on appelle l'*orthogonal de X* l'ensemble

$$X^\perp \equiv \{ u \in \Lambda^\circ \mid \forall t \in X, t \perp u \}$$

On dispose de plusieurs propriétés usuelles liées à l'orthogonalité:

Lemme 1.

Si $X, Y \subseteq \Lambda^\circ$ alors:

1. $X \subseteq Y$ implies $Y^\perp \subseteq X^\perp$
2. $X \subseteq X^{\perp\perp}$
3. $X^{\perp\perp\perp} = X^\perp$

Si X est un ensemble de structures pointées, on peut voir $X^{\perp\perp}$ comme l'ensemble des structures qui se comportent de la même manière que les structures de X (puisque les éléments de X et $X^{\perp\perp}$ sont orthogonaux aux mêmes éléments). Ainsi un ensemble égal à son biorthogonal est un ensemble contenant toutes les structures partageant un même comportement. C'est pourquoi un ensemble $X \subseteq \Lambda^\circ$ tel que $X = X^{\perp\perp}$ est appelé *comportement*.

Exemple. Tout ensemble de la forme X^\perp est un comportement (par la propriété 3 du lemme 1).

Lemme 2.

Si X et Y sont des comportements, $X \cap Y$ aussi.

preuve. Soit $t \in (X \cap Y)^{\perp\perp}$. Si $u \in X^\perp \subseteq (X \cap Y)^\perp$, $t \star u \in \perp$, et donc $t \in X^{\perp\perp} = X$. De même $t \in Y^{\perp\perp} = Y$.
D'où $t \in X \cap Y$. De plus $X \cap Y \subseteq (X \cap Y)^{\perp\perp}$ par le lemme 1. \triangleleft

Si X et Y sont deux ensembles de structures pointées, on définit deux comportements $X \otimes Y$ et $!X$ qui vont servir à interpréter les formules de MELL :

- $X \otimes Y = \{ t \otimes u \mid t \in X \wedge u \in Y \}^{\perp\perp}$
- $!X = ([X], \cdot)^{\perp\perp}$

Les *modèles de phase calculatoires*, qui sont une version simplifiée des *modèles de phase pour les preuves* d'Okada [27], sont essentiellement la donnée d'un pôle \perp et d'un ensemble de comportements D . Ils nous fournissent une classe de modèles de MELL.

Définition 6 (Modèle de phase calculatoire). On dit que la structure $(\perp, D, |\cdot|)$ est un *modèle de phase calculatoire* si:

- (**>₀-saturation**) Si $u \in \perp$ et $t >_0 u$, alors $t \in \perp$.
- (**Affaiblissement**) Si $t \in \perp$, alors toute structure de preuve t' obtenue en plaçant côte à côte t et un lien affaiblissement est dans \perp également.
- (**Stabilité**) D est un ensemble de comportements clos par \otimes , $(\cdot)^\perp$ et $!$.
- $|\cdot|$ est une valuation des formules atomiques de MELL vers D .

Exemple. Posons $\perp = \{ t \in \Lambda \mid t \text{ possède une suite de réductions infinie} \}$ et D l'ensemble de tous les comportements. Alors la structure $(\perp, D, |\cdot| : A \mapsto \{\mathfrak{X}\}^\perp)$ est un modèle de phase calculatoire.

Etant donné une telle structure, on peut associer à chaque formule A de MELL un comportement noté $|A|$, appelé *valeur de vérité de A* ou *interprétation de A* . Pour chaque $t \in \Lambda^\circ$, on dit que t *réalise* A et on note $t \Vdash A$, si $t \in |A|$. On définit $|A|$ par induction sur le langage des formules (pour simplifier, jusqu'à la section 4 on ne considèrera pas la présence de termes du premier ordre, et tous les prédicats atomiques sont d'arité 0):

- $|A|$ si A est atomique.
- $|A^\perp| = |A|^\perp$ si A est atomique.
- $|A \otimes B| = |A| \otimes |B|$.
- $|A \wp B| = |A| \wp |B| = (|A|^\perp \otimes |B|^\perp)^\perp$.
- $!|A| = !|A|$.
- $|?A| = ?|A| = (!(|A|^\perp))^\perp$.

Remarque. • On vérifie que $|A^\perp| = |A|^\perp$ pour toute formule A . Ainsi $t \Vdash A \Leftrightarrow \forall u \Vdash A^\perp, t \star u \in \perp$.

• La stabilité de D par toutes les opérations utilisées ci-dessus assure que $|A|$ est toujours un élément de D .

La relation de réalisabilité vérifie un théorème dit d'adéquation au typage dans MELL. Cela signifie que toute structure de preuve (pointée) qui est un réseau de preuve typé par une formule A est également un réalisateur de cette formule et donc se comporte suivant la spécification donnée par la formule A . Cela implique que les modèles de phase calculatoires sont des modèles de MELL.

Théorème 1 (Adéquation MELL).

Soit $(\perp, D, |\cdot|)$ un espace de phase calculatoire et \Vdash la relation de réalisabilité associée. Si t est un réseau de preuve MELL de conclusion $\vdash A_1, \dots, A_n, B$, alors pour tous $u_1 \Vdash A_1^\perp, \dots, u_n \Vdash A_n^\perp$, on a $t[u_1, \dots, u_n] \Vdash B$ (où le noeud de type B est distingué).

1.4 Modèle des candidats de réductibilité

On décrit maintenant un modèle de phase calculatoire particulier, le modèle des candidats de réductibilité. Le théorème d'adéquation, une fois appliqué à ce modèle, nous fournit une preuve de normalisation faible pour les réseaux de preuve de MELL.

Le pôle choisit est $\perp \equiv \{ t \in \Lambda \mid t \text{ normalise faiblement} \}$ et on notera dans le reste de ce rapport \perp° l'ensemble des structures pointées $t \in \Lambda^\circ$ telles que la structure non pointée sous-jacente appartient à \perp . Une propriété remarquable est que $\perp^\circ = \{\boxtimes\}^\perp$. Et donc en particulier, \perp° est comportement.

Définition 7 (Candidats de réductibilité). On définit D comme l'ensemble des comportements X vérifiant $\boxtimes \in X \subseteq \perp^\circ$. Les éléments de D sont appelés *candidats de réductibilité*.

Exemple. \perp° est le plus grand candidat de réductibilité.

On peut obtenir le théorème suivant:

Théorème 2 (Modèle de réductibilité).

Pour toute valuation $|\cdot|$ des formules atomiques vers D , la structure $(D, \perp, |\cdot|)$ est un modèle de phase calculatoire.

Associé au théorème d'adéquation, ce théorème permet d'obtenir le théorème de normalisation faible suivant. Le même paradigme sera appliqué par la suite aux logiques allégées pour obtenir des théorèmes de normalisation en temps borné.

Théorème 3 (Normalisation faible).

Si t est un réseau de preuve de MELL ayant A_1, \dots, A_n et B comme conclusions, alors t normalise faiblement.

preuve. Le théorème d'adéquation appliqué à un modèle de réductibilité (par exemple avec la valuation $|A| = \perp^\circ$) nous donne $t[\boxtimes, \dots, \boxtimes] \Vdash B$ (car pour tout i , $|A_i^\perp| \in D$ et donc $\boxtimes \Vdash A_i^\perp$). Or $|B| \subseteq \perp^\circ$, donc $t[\boxtimes, \dots, \boxtimes]$ normalise faiblement. D'où l'on déduit aisément que t lui-même normalise faiblement (sinon $t[\boxtimes, \dots, \boxtimes]$ ne normaliserait pas faiblement). ◀

2 Candidats de réductibilité quantitatifs: le fragment multiplicatif

Dans cette partie et la suivante, nous développons une version plus élaborée des candidats de réductibilité présentés à la section 1, appelés *candidats de réductibilité quantitatifs*, dont le rôle est non seulement de prouver la normalisation faible des réseaux de preuve mais également de fournir des bornes sur le nombre d'étapes de réduction nécessaires à leur normalisation. Nous commençons par introduire une structure inspirée des monoïdes de ressource de Dal Lago et Hofmann [5], le *monoïde quantitatif*, dont les éléments (appelés *majorants*) vont nous permettre d'exprimer ces bornes. Les éléments p d'une telle structure ont la particularité de

pouvoir être "mesurés" via une fonction $\|\cdot\|$. La relation de réalisabilité qui était auparavant de la forme:

$$t \Vdash A$$

devient dans notre nouveau cadre une relation entre un couple réalisateur/majorant et une formule:

$$(t, p) \Vdash A$$

et signifie informellement " t est une structure de preuve se comportant suivant la spécification A et utilise au plus $\|p\|$ ressources pour normaliser". Nous donnerons plus tard un sens au terme "ressource" utilisé ici.

Dans cette section nous introduisons les candidats de réductibilité quantitatifs pour **MLL**, que nous étendrons dans la section suivante au cas d'une logique allégée plus complexe: **ELL**.

2.1 Monoïdes quantitatifs

Nous allons définir plusieurs notions dérivées de celle de monoïde, qui serviront à la fois à quantifier les ressources (comme le nombre de pas de réduction nécessaire à une structure de preuve pour normaliser), et à modéliser les règles de **MLL**.

On s'attachera dans la suite de ce rapport à différencier les structures nécessaires pour obtenir l'adéquation au typage et celles nécessaires à la construction du modèle des candidats. Dans le cas du fragment multiplicatif, la structure nécessaire pour obtenir l'adéquation est celle de monoïde pointé.

Définition 8 (Monoïde pointé). On dit que $\mathcal{M} = (M, +, 0, g)$ est un *monoïde pointé* si $(M, +, 0)$ est un monoïde commutatif et $g \in M$.

Pour construire le modèle des candidats, nous aurons besoin d'une structure plus riche: le monoïde quantitatif. Pour obtenir des bornes concrètes en utilisant un élément x du monoïde, il est nécessaire de savoir quelle quantité cet élément représente. Dans un monoïde quantitatif, c'est l'existence d'une mesure $\|x\|$ de cet élément qui nous fournit cette information.

Définition 9 (Monoïde quantitatif). Un *monoïde quantitatif* est un quintuplet $\mathcal{M} = (M, +, 0, \leq_M, \|\cdot\|_M)$ tel que:

- $(M, +, 0)$ est un monoïde commutatif.
- \leq_M est un préordre sur M compatible avec $+$.
- $\|\cdot\|_M : M \rightarrow \mathbb{N}$ est une fonction telle que:

- + $\|a\|_M + \|b\|_M \leq \|a + b\|_M$
- + Si $p \leq_M q$, alors $\|p\|_M \leq \|q\|_M$.
- + Pour chaque $n \in \mathbb{N}$, il y a un $a \in M$ tel que $n \leq \|a\|_M$.

On dit de plus qu'un élément $\mathbf{1} \in M$ est une *unité* si pour tout $p \in M$, $\|p + \mathbf{1}\| = \|p\| + 1$ (on considérera implicitement un monoïde quantitatif avec unité comme un monoïde pointé).

Exemple. La structure $(\mathbb{N}, +, 0, \leq, \|\cdot\|_{\mathbb{N}})$, avec $\|n\|_{\mathbb{N}} = n$ est un monoïde quantitatif.

On peut expliquer les différents points de cette définition en pensant à la mesure d'un élément d'un monoïde quantitatif comme à un temps de calcul d'un programme informatique (comme un λ -terme ou une structure de preuve):

- L'opération $+$ du monoïde correspond à la composition de programmes. Ainsi, si x et y bornent le temps de deux programmes, $x + y$ borne leur composition.

- L'inégalité anti-triangulaire peut alors s'expliquer par le fait que le temps de calcul de la composition de deux programmes est en général plus grande que la somme des temps de calcul des deux programmes (par exemple: la composition dans le λ -calcul $(t)u$ ou la coupure $t \star u$ de deux structures de preuve).
- Un programme pouvant avoir un temps de calcul arbitraire, on doit disposer d'éléments du monoïde dont la mesure est elle-même arbitrairement grande.

Les monoïdes quantitatifs diffèrent des monoïdes de ressource de Dal Lago et Hofmann car ces derniers supposent l'existence d'une "anti"-distance (vérifiant une inégalité anti-triangulaire) sur $\mathcal{M} \times \mathcal{M}$ alors que nous n'avons ici besoin que d'une mesure. Tout monoïde de ressource est en particulier un monoïde quantitatif. Cette différence permet de simplifier en partie les arguments développés par la suite.

2.2 Orthogonalité et réalisabilité

Dans ce qui suit, on considère un langage de structures de preuve contenant au moins le fragment multiplicatif (i.e. les liens axiome, coupure, \otimes , \wp et \bowtie) muni d'une relation de réduction contenant $>_{MLL}$. On suppose avoir fixé un monoïde commutatif pointé $\mathcal{M} = (\mathcal{M}, +, 0, \mathbf{1})$. Désormais, une formule va être réalisée par un couple (t, p) formée d'une structure pointée (appelée *réalisateur*) et d'un élément du monoïde \mathcal{M} (appelé *majorant*). Nous étendons l'opération d'interaction \star aux éléments de $\Lambda^\circ \times \mathcal{M}$:

$$(t, p) \star (u, q) = (t \star u, p + q)$$

Fixons maintenant un pôle \perp dorénavant sous-ensemble de $\Lambda \times \mathcal{M}$. Celui-ci induit naturellement une notion d'orthogonalité pour un ensemble $X \subseteq \Lambda^\circ \times \mathcal{M}$:

$$X^\perp = \{ (t, p) \in \Lambda^\circ \times \mathcal{M} \mid \forall (u, q) \in X, (t, p) \star (u, q) \in \perp \}$$

Comme dans la section 1, X est un *comportement* si $X^{\perp\perp} = X$.

Si $X, Y \subseteq \Lambda^\circ \times \mathcal{M}$, nous définissons les opérations suivantes:

- $X.Y = \{ (t \otimes s, p + q) \mid (t, p) \in X \text{ et } (s, q) \in Y \}$
- $X \otimes Y = (X.Y)^{\perp\perp}$
- $X \wp Y = (X^\perp.Y^\perp)^\perp$

Nous allons à présent définir une classe de modèles basés sur les structures pointées et les monoïdes pointés, à partir de laquelle on peut, comme dans la section 1.3, définir une relation de réalisabilité qui vérifie un théorème d'adéquation au typage (dans MLL).

Définition 10 (Modèle de phase quantitatif multiplicatif). On dit que le quadruplet $(\mathcal{M}, \perp, D, |\cdot|)$ est un *modèle de phase quantitatif multiplicatif* si:

- $\mathcal{M} = (M, +, 0, \mathbf{1})$ est un monoïde pointé.
- (**$>_0$ -saturation**) Si $(t, p) \in \perp$ et $u >_0 t$ alors $(u, p + \mathbf{1}) \in \perp$.
- (**Stabilité**) D est un ensemble de comportement clos par \otimes et $(\cdot)^\perp$.
- $|\cdot|$ est une valuation des formules atomiques vers D .

Remarque. La clôture de D par \otimes et $(\cdot)^\perp$ implique la clôture par \wp .

Les comportements héritent des propriétés calculatoires du pôle \perp . En effet,

Lemme 3.

Si X est un comportement, alors X est $>_0$ -saturé.

Définition 11 (Relation de réalisabilité). Etant donné un espace de phase multiplicatif quantitatif, on peut associer à chaque formule A de **MLL** un comportement noté $|A|$, appelé *valeur de vérité de A* ou *interprétation de A* . Pour chaque $(t, p) \in \Lambda^\circ \times \mathcal{M}$, on dit que (t, p) *réalise* A et on note $(t, p) \Vdash A$, si $(t, p) \in |A|$. On définit $|A|$ par induction sur le langage des formules de **MLL**:

- L'interprétation de A est $|A|$ (la valuation) si A est atomique.
- $|A^\perp| = |A|^\perp$ si A est atomique.
- $|A \otimes B| = |A| \otimes |B|$.
- $|A \wp B| = |A| \wp |B|$.

Cette notion de réalisabilité vérifie un théorème d'adéquation similaire au théorème 1. Désormais un réseau de preuve t typé par une formule A nous fournit non seulement un réalisateur de cette formule, mais également un majorant $p \in \mathcal{M}$ qui représente les ressources utilisées par t au cours de sa normalisation.

Théorème 4 (Adéquation).

Soit $(D, \mathcal{M}, \perp, |\cdot|)$ un modèle de phase quantitatif multiplicatif. Si $\vdash_{\text{MLL}} x_1 : A_1, \dots, x_n : A_n, t : B$ alors il existe $p \in \mathcal{M}$ tel qu'on ait pour tous $(u_i, q_i) \Vdash A_i$, $(t[x_1 := u_1, \dots, x_n := u_n], p + (q_1 + \dots + q_n)) \Vdash B$. De plus, $p = (\#(t)_{ax} + \#(t)_{\wp})\mathbf{1}$, où $\#(t)_{ax}$ (resp. $\#(t)_{\wp}$) est le nombre de liens axiome (resp. liens \wp) de t .

2.3 Candidats de réductibilité quantitatifs

On introduit ici les candidats de réductibilité quantitatifs. $\mathcal{M} = (\mathcal{M}, +, \mathbf{0}, \|\cdot\|, \mathbf{1})$ est un monoïde quantitatif avec unité fixé. La définition du pôle diffère de celles de la section 1.4 par le fait qu'il contient maintenant des éléments de $\Lambda^\circ \times \mathcal{M}$ et qu'en plus de normaliser faiblement, le temps de normalisation du réalisateur est borné par la mesure du majorant associé:

$$\perp = \{ (t, p) \in \Lambda \times \mathcal{M} \mid \text{Time}(t) \leq \|p\| \}$$

Remarque. *On suppose implicitement que $\text{Time}(t) \leq \|p\|$ implique que $\text{Time}(t)$ est défini et donc que t normalise faiblement.*

Lemme 4.

On a toujours $\perp^\circ = \{\star\}^\perp$ et \perp° est donc en particulier un comportement.

Remarque. *Cette définition du pôle est similaire à la notion de σ -saturation introduite dans [2]. Il semble que la possibilité de définir simplement le pôle (ou la σ -saturation) vienne du choix d'utiliser des réalisateurs en forme non-nécessairement normale, à l'inverse de ce qui est fait dans [5] et qui nécessite la présence d'une anti-distance.*

L'ensemble des *candidats de réductibilité quantitatifs* (ou plus simplement des candidats) noté D est l'ensemble des $X \subseteq \Lambda^\circ$ tels que:

$$X^{\perp\perp} = X \text{ et } (\star, \mathbf{0}) \in X \subseteq \perp^\circ$$

Théorème 5 (Modèle de réductibilité de MLL).

Pour toute valuation $|\cdot|$, et tout monoïde quantitatif avec unité \mathcal{M} , la structure $(\mathcal{M}, \perp, D, |\cdot|)$ est un modèle de phase quantitatif multiplicatif. En particulier, on note C_{MLL} et on appelle modèle de réductibilité pour MLL le modèle obtenu en choisissant le monoïde des entiers naturels $(\mathbb{N}, +, 0, n \mapsto n, 1)$ et la valuation $A \mapsto |A| = \perp^\circ$.

Nous ne développons pas de preuve de ce théorème par manque de place. Néanmoins, notons que le seul point difficile de la preuve est la stabilité de D par $(\cdot)^\perp$ et \otimes . L'existence de l'unité du monoïde est quant à elle nécessaire pour montrer la $>_0$ -saturation de \perp .

En appliquant le théorème d'adéquation au modèle C_{MLL} , nous pouvons prouver un théorème de normalisation en temps linéaire.

Théorème 6 (Normalisation faible en nombre de pas linéaire).

Si $\vdash_{MLL} A_1, \dots, A_n, t : B$, alors t normalise en n pas, avec $n \leq |t|$.

preuve. Tout d'abord, notons que pour tout $i \in \llbracket 1; n \rrbracket$, $(\mathfrak{X}, \mathbf{0}) \Vdash A_i$. En appliquant le théorème d'adéquation au modèle C_{MLL} , on obtient l'existence d'un entier $k \in \mathbb{N}$ tel que :

1. $(t[\mathfrak{X}, \dots, \mathfrak{X}], k + n\mathbf{0}) \Vdash B$
2. $k \leq |t|$

En utilisant 1, puisque $|B| \in D$, on obtient $Time(t[\mathfrak{X}, \dots, \mathfrak{X}]) \leq \|k + n\mathbf{0}\| = k$. Mais cela signifie alors que $Time(t) \leq k$. En utilisant 2, on obtient $Time(t) \leq |t|$. Enfin, on conclut en notant que t ne contenant pas de \mathfrak{X} (car il est bien typé), $Time(t)$ est exactement le nombre de pas de réduction nécessaire à t pour normaliser. ◀

On aurait tout aussi bien pu construire un modèle prouvant la normalisation forte en temps linéaire. Cependant, pour plus de simplicité et parce que la méthode ne s'étend pas simplement en présence d'exponentielles, nous ne traitons pas cette question ici.

3 Candidats de réductibilité quantitatifs: ELL

Nous allons maintenant étendre le cadre des candidats de réductibilité quantitatifs à une logique plus élaborée: ELL (pour Elementary Linear Logic). Cette logique, introduite dans [18] est une version de la logique linéaire où la modalité $!$ est affaiblie. En particulier les règles de promotion et de déréliction sont abandonnées au profit d'une promotion fonctorielle. Le résultat de cette restriction est le théorème de normalisation des réseaux de preuve ELL en temps élémentaire.

Définition 12 (Fonctions élémentaires). L'ensemble des *fonctions élémentaires* (au sens de Kalmar) est l'ensemble la clôture par composition et projection de l'ensemble des fonctions suivantes:

- $(n, m) \mapsto n + m$.
- $(n, m) \mapsto \max(n - m, 0)$.
- $(n, m) \mapsto [n/m]$ où $[.]$ est la partie entière inférieure.
- $n \mapsto 2^n$.

Théorème (Normalisation en temps élémentaire).

Il existe une famille de fonctions élémentaires $(e_i)_{i \in \mathbb{N}}$ telle que dès que si t est un réseau de preuve de ELL, alors t normalise en un nombre d'étapes borné par $e_{\partial(t)}(|t|)$.

Les candidats de réductibilité quantitatifs nous permettent d'obtenir une borne similaire en utilisant une méthode sémantique, modulaire et extensible.

3.1 ELL et ses réseaux de preuve

ELL est un fragment de MELL, qu'on va décrire par ses réseaux de preuve. Il est possible de caractériser les réseaux de preuve de ELL comme les réseaux de preuve de MELL vérifiant une certaine propriété dite de *stratification* (voir [8]). Cependant, on choisit ici d'introduire des règles de typage spécifiques à ELL.

Le langage des structures de preuves de ELL est le même que celui de MELL. Les règles de typage des réseaux de preuve de ELL sont celles de MELL, à la seule différence que les règles

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} \text{ (Dereliction)} \quad \frac{\vdash ?\Gamma, B}{\vdash ?\Gamma, !B} \text{ (Promotion)}$$

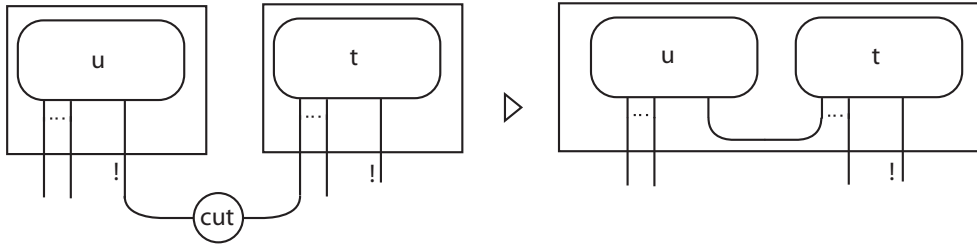
ont été remplacées par la règle de *promotion fonctorielle*:

$$\frac{\vdash \Gamma, B}{\vdash ?\Gamma, !B} \text{ (Promotion)}$$

C'est-à-dire que si t est un réseau de preuve dont les noeuds pendants sont étiquetés par A_1, \dots, A_n, B , la structure de preuve obtenue en étiquetant les noeuds pendants de $[t]$ par $?A_1, \dots, ?A_n, !B$ est un réseau de preuve.

Remarque. En particulier, la règle de *digging* $!A \multimap !!A$ n'est plus prouvable dans ELL.

Quant à la réduction des structures de preuve, elle diffère par la règle (!/!) qui devient:



3.2 Monoïde élémentaire

Comme dans la section précédente, nous présentons ici la structure nécessaire à l'obtention d'un théorème d'adéquation pour ELL. Cette structure est celle de monoïde avec exponentielles élémentaires.

Définition 13 (Monoïde avec exponentielles élémentaires). Une structure $\mathcal{M} = (M, +, 0, \leq, !, r_{contr})$ est un *monoïde avec exponentielles élémentaires* si:

- $(M, +, 0, \leq)$ est un monoïde commutatif préordonné.
- $! : M \rightarrow M$ est une opération unaire telle que:
 1. **(Fonctorialité)** Pour tous $p, q \in M$, on a $!(p + q) \leq !p + !q$.
 2. **(Contraction)** Pour tout $p \in M$, $!p + !p \leq !p + r_{contr}$.

Les conditions de fonctorialité et de contraction sont respectivement utilisées pour modéliser les règles de promotion fonctorielle et de contraction.

Exemple. $(\mathbb{N}, \max(\cdot, \cdot), 0, \leq, n \mapsto n, 0)$ (où $\max(n, m)$ est le maximum de n et m et \leq l'ordre usuel sur \mathbb{N}) est un *monoïde avec exponentielles élémentaires*.

Pour construire le modèle des candidats quantitatifs, nous aurons besoin d'un monoïde avec exponentielles élémentaires particulier, que nous appellerons le monoïde élémentaire.

Définition 14 (Le monoïde élémentaire). Le *monoïde élémentaire* est le monoïde quantitatif \mathcal{M}_e suivant:

- Les éléments de $\mathcal{M}_e = \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}^{\mathbb{N}}$ sont les quadruplets (a, n, m, f) tels que $f : \mathbb{N} \rightarrow \mathbb{N}$ est une fonction élémentaire croissante.
- L'addition est définie par: $(a, n, m, f) + (b, l, k, g) = (a + b, n + l, m + k, \max(f, g))$. Avec $\max(f, g)$ la fonction qui à x associe $\max(f(x), g(x))$.
- On dit que $(a, n, m, f) \leq (b, l, k, g)$ quand:
 - + $a \leq b$
 - + $n \leq l$
 - + $2^n m \leq 2^l k$
 - + Pour tout $x \in \mathbb{N}$, $f(x) \leq g(x)$
- La mesure est $\|(a, n, m, f)\| = nf(n + 2^n m) + a$
- L'opération exponentielle est $!(a, n, m, f) = (0, 1, n+m+a, f^+)$ où $f^+(x) = \max(xf(x2^x), x)$ si $(a, n, m, f) \neq (0, 0, 0, x \mapsto 0)$ et $!(0, 0, 0, x \mapsto 0) = (0, 0, 0, x \mapsto 0)$.

Ce monoïde est directement adapté du monoïde utilisé par Dal Lago et Hofmann dans [5] pour prouver la correction de **ELL** vis-à-vis de la classe **ELEMENTARY**. Notre monoïde diffère essentiellement en trois points:

- Il possède un élément unité **1** tel que $\|p + \mathbf{1}\| = \|p\| + 1$, ce qui permet de borner plus finement le nombre d'étapes de réduction d'une structure de preuve. C'est une condition nécessaire à la construction des candidats de réductibilité.
- Il possède la propriété

$$(P1) \quad !(0, 0, 0, \mapsto 0) = (0, 0, 0, \mapsto 0)$$

- La fonction f^+ est la fonction $x \mapsto \max(xf(x2^x), x)$, quand le monoïde introduit dans [5] utilise $f^+(x) = xf(x2^x)$. Cette différence minimale permet pourtant d'obtenir la propriété

$$(P2) \quad \forall p \in \mathcal{M}_e, \|p\| \leq \|!p\|$$

La première propriété était nécessaire pour construire le modèle C_{MLL} (en fait, pour montrer la $>_0$ -saturation de \perp , voir section 2.3), la deuxième (P1) et la troisième (P2) permettent de construire le modèle des candidats de réductibilité dans le cas de **ELL**. Il est possible de prouver que \mathcal{M}_e est un monoïde quantitatif avec exponentielles élémentaires et avec unité.

3.3 Comportements et réalisabilité

Dans ce qui suit, on suppose fixé un monoïde avec exponentielles élémentaires \mathcal{M} et un pôle $\perp \subseteq \Lambda \times \mathcal{M}$. Toutes les définitions et constructions développées dans le cas de **MLL** sont toujours valides. Ce qui suit constitue une extension de la section 2. Grâce à l'opération $!$ du monoïde, on peut ajouter une construction modélisant $!$ et $?$:

- $!X = \{ ([t]!, !p) \mid (t, p) \in X \}^{\perp\perp}$
- $?X = (!X^{\perp})^{\perp}$

Définition 15 (Espace de phase quantitatif élémentaire). On dit que la structure $(\mathcal{M}, \perp, D, |\cdot|)$ est un *espace de phase quantitatif élémentaire* ssi:

- $\mathcal{M} = (M, +, \mathbf{0}, \leq, !, r_{contr}, \mathbf{1})$ est un monoïde pointé avec exponentielles élémentaires.
- (**$>_0$ -saturation**) Si $(t, p) \in \perp$ et $u >_0 t$ alors $(u, p + \mathbf{1}) \in \perp$.
- (**\leq -saturation**) Si $(t, p) \in \perp$ et $p \leq q$ alors $(t, q) \in \perp$.
- (**Affaiblissement**) Si $(t, p) \in \perp$, alors pour toute structure de preuve t' formée de t et de l'ajout d'un lien affaiblissement, $(t', p) \in \perp$.
- (**Contraction**) Si $(t[u, u], p) \in \perp$ alors $(C(t[u, u]), p) \in \perp$.
- (**Stabilité**) D est un ensemble de comportements clos par $\otimes, \wp, !, ?$ et $(\cdot)^\perp$.
- $|\cdot|$ est une valuation des formules atomiques vers D .

Bien entendu, comme tout monoïde pointé avec exponentielles élémentaires est aussi un monoïde pointé, tout espace de phase quantitatif élémentaire est également un espace de phase quantitatif multiplicatif.

Définition 16 (Réalisation étendue). On peut étendre l'interprétation définie dans la section précédente à toutes les formules de **ELL** de la manière suivante:

- $|A|$ si A est atomique.
- $|A^\perp| = |A|^\perp$ si A est atomique.
- $|A \otimes B| = |A| \otimes |B|$.
- $|A \wp B| = |A| \wp |B|$.
- $!|A| = !|A|$.
- $?|A| = ?|A|$.

Cette notion de réalisation induit un théorème d'adéquation pour **ELL**.

Théorème 7 (Adéquation à ELL).

Soit $(\mathcal{M}, \perp, D, |\cdot|)$ un espace de phase quantitatif élémentaire. Si $\vdash_{ELL} x_1 : A_1, \dots, x_n : A_n, t : B$ alors il existe $p \in \mathcal{M}$ tel que pour chaque $(u_1, q_1) \Vdash A_1, \dots, (u_n, q_n) \Vdash A_n$, on ait $(t[x_1 := u_1, \dots, x_n := u_n], p + (q_1 + \dots + q_n)) \Vdash B$.

Par manque de place nous ne donnons pas la preuve de ce théorème, mais on peut cependant trouver dans le tableau suivant le récapitulatif des bornes données par le théorème d'adéquation. Il donne les majorants utilisés en fonction de la dernière règle utilisée dans le réseau de preuve (sur laquelle est effectuée l'induction).

3.4 Candidats de réductibilité quantitatifs pour ELL

La construction des candidats de réductibilité quantitatifs pour **ELL** ne diffère que très peu de celle pour **MLL** introduite à la section 2.3. En effet, la seule différence est le monoïde utilisé: on a besoin ici d'un monoïde quantitatif (pointé avec exponentielles élémentaires) qui dispose d'une unité et vérifie à la fois les conditions **(P1)** et **(P2)**. On pourra ainsi choisir le monoïde élémentaire (voir définition 14) en lieu et place du monoïde des entiers \mathbb{N} . Le fait que $\|p + \mathbf{1}\| = \|p\| + 1$ assure que les preuves de saturation de \perp et de stabilité de D par $(\cdot)^\perp$ et \otimes sont toujours valides. Il reste uniquement à traiter les modalités, ce qui donne lieu au théorème de stabilité, qui constitue la seule difficulté de la construction et qui repose sur la preuve du cas multiplicatif et les conditions **(P1)** et **(P2)**.

Figure 6: Majorants obtenus par adéquation

$$\begin{array}{c}
\frac{}{\mathbf{1} : (\vdash A^\perp, A)} \text{ (Axiom)} \qquad \frac{p_1 : (\vdash A, \Gamma) \quad p_2 : (\vdash A^\perp, \Delta)}{p_1 + p_2 : (\vdash \Gamma, \Delta)} \text{ (Cut)} \\
\\
\frac{p_1 : (\vdash A, \Gamma) \quad p_2 : (\vdash B, \Delta)}{p_1 + p_2 : (\vdash A \otimes B, \Gamma, \Delta)} \text{ (\otimes)} \qquad \frac{p : (\vdash A, B, \Gamma)}{p + \mathbf{1} : (\vdash A \wp B, \Gamma)} \text{ (\wp)} \\
\\
\frac{p : (\vdash C_1, \dots, C_n, A)}{!p + \mathbf{1} : (\vdash ?C_1, \dots, ?C_n, !A)} \text{ (Prom)} \qquad \frac{p : (\vdash \Gamma, ?A, ?A)}{p + \mathbf{1} + r_{\text{contr}} : (\vdash \Gamma, ?A)} \text{ (Contr)} \\
\\
\frac{p : (\vdash \Gamma)}{p : (\vdash \Gamma, ?A)} \text{ (weak)}
\end{array}$$

Théoreme 8 (Stabilité de D).

D est clos par $(\cdot)^\perp$, \otimes et $!$.

Grâce à ce théorème, on montre que la structure $C_{ELL} = (D, \mathcal{M}_e, \perp, |\cdot|)$ est un modèle de phase quantitatif élémentaire (\mathcal{M}_e est le monoïde élémentaire, et si A est atomique, $|A| = \perp^\circ$). On peut alors obtenir le théorème de normalisation en temps élémentaire.

Théoreme 9 (Normalisation en temps élémentaire).

Il existe une famille de fonctions élémentaires $(e_i)_{i \in \mathbb{N}}$ telle que dès que $\vdash_{ELL} A_1, \dots, A_n, t : B$, t normalise faiblement en k étapes avec $k \leq e_{\partial(t)}(|t|)$.

La preuve de ce théorème, utilisant le théorème d'adéquation appliqué au modèle C_{ELL} , repose sur une analyse fine du monoïde élémentaire \mathcal{M}_e et sur les bornes fournies par le théorème d'adéquation (résumées dans le tableau 3.3).

4 Déduction Modulo et logiques linéaires

La déduction modulo [11] permet de définir de manière uniforme une notion de réduction des preuves paramétrée par une théorie du premier ordre. Nous allons ici adapter ce concept à ELL, dans le but d'obtenir un critère algébrique impliquant la normalisation faible en temps élémentaire de ELL enrichie d'une théorie donnée.

4.1 Logiques linéaires modulo

Les logiques linéaires modulo sont obtenues en quotientant le langage des formules par une congruence sur les formules \equiv . C'est-à-dire qu'on ajoute la règle de typage des réseaux de preuve dite de conversion:

$$\frac{\vdash \Gamma, A \quad A \equiv B}{\vdash \Gamma, B} (\equiv)$$

Si t est un réseau de preuve et A étiquette un des noeuds de t , alors si $A \equiv B$, la structure obtenue en remplaçant A par B est également un réseau de preuve. Cela permet d'exprimer dans un même cadre la normalisation d'un grand nombre de théories "non-calculatoires" (par exemple l'arithmétique), c'est-à-dire qui ne nécessitent pas l'extension du langage des structures de preuve ni de la relation de réduction. On obtient ainsi plusieurs systèmes que l'on notera MLL_{\equiv} , ELL_{\equiv} et $MELL_{\equiv}$.

Si l'on dispose d'un modèle de phase quantitatif (élémentaire ou multiplicatif) $\mathcal{P} = (\mathcal{M}, \perp, D, |\cdot|)$ tel que: $A \equiv B$ implique $|A| = |B|$, alors la relation de réalisabilité qui en découle vérifie le théorème d'adéquation au typage étendu à la règle de conversion (car si $A \equiv B$, les réalisateurs de A sont également des réalisateurs de B). On dit alors que la valuation $|\cdot|$ est *adaptée* à \equiv .

4.2 La superconsistance

Les algèbres de valeur de vérité (ou *TVA* pour "Truth Value Algebra") sont une extension des algèbres de Heyting, définies par Dowek dans [9] pour étudier la normalisation de théories exprimées en déduction modulo. On introduit une version simplifiée des algèbres de valeur de vérité adaptée à la logique linéaire.

Définition 17 (Algèbre de valeur de vérité linéaire). Une *algèbre de valeur de vérité linéaire* (ou *LTVA*) est une structure $(\mathcal{B}, \otimes, !, (\cdot)^\perp)$ telle que \mathcal{B} est un ensemble (appelé *domaine*), \otimes est une fonction $\mathcal{B} \times \mathcal{B} \rightarrow \mathcal{B}$, $!$ et $(\cdot)^\perp$ sont des applications de $\mathcal{B} \rightarrow \mathcal{B}$.

On notera \mathcal{B} pour parler du domaine aussi bien que de l'algèbre.

Remarque. Cette notion est une simplification de la notion habituelle de *TVA*, car elle ne fait pas référence à un ensemble de valeurs dites positives, clos par les règles de la logique dans laquelle on travaille (logique intuitionniste pour les *TVA* et les préalgèbres de Heyting, logique linéaire pour les *LTVA*). Cette simplification se retrouve également dans le travail de Cousineau [4].

Définition 18 (Algèbre ordonnée). On dit qu'une *LTVA*, $(\mathcal{B}, \otimes, !, (\cdot)^\perp)$ est *ordonnée* si il existe un ordre \leq sur \mathcal{B} tel que \otimes et $!$ sont des fonctions croissantes pour \leq et $(\cdot)^\perp$ est décroissante pour \leq . On dit de plus que \mathcal{B} est *complète* si \leq est complet (tout sous-ensemble de \mathcal{B} possède une borne inférieure et une borne supérieure).

Théorème 10 (Algèbre des candidats).

La structure $(D, \otimes, !, (\cdot)^\perp)$ des candidats de réductibilité quantitatifs élémentaires est une *LTVA ordonnée et complète pour l'inclusion*.

preuve. On rappelle que D est l'ensemble des candidats de réductibilité quantitatifs et est stable par \otimes , $!$ et $(\cdot)^\perp$ (voir 3.4) donc $(D, \otimes, !, (\cdot)^\perp)$ est une *LTVA*. De plus cette algèbre est ordonnée pour l'inclusion entre ensembles \subseteq . En effet, par les propriétés d'orthogonalité $(\cdot)^\perp$ est décroissante pour \subseteq et \otimes et $!$ sont trivialement croissantes.

De plus cet ordre est complet. Soit $S \subseteq D$, alors:

- La borne inférieure est l'intersection. $\bigcap_{X \in S} X$ est un comportement, et de plus il est clair que $(\mathfrak{X}, \mathbf{0}) \in \bigcap_{X \in S} X \subseteq \perp^\circ$, donc $\bigcap_{X \in S} X \in D$.
- La borne supérieure est $(\bigcup_{X \in S} X)^{\perp\perp}$. Il est aisé de voir que c'est le plus petit comportement contenant $\bigcup_{X \in S} X$. Il suffit donc de vérifier que $(\bigcup_{X \in S} X)^{\perp\perp} \in D$, ce qui est immédiat. ◀

Remarque. On pourrait vérifier de la même manière que les candidats de réductibilité pour **MELL** définis à la section 1 forment également une *LTVA ordonnée et complète*.

On peut maintenant énoncer la définition de la superconsistance d'une congruence \equiv et montrer qu'elle implique la normalisation en temps borné de **ELL_≡**.

Définition 19 (Superconsistance). Une théorie \equiv est *superconsistante* si pour toute *LTVA* \mathcal{A} ordonnée et complète, il existe un modèle \mathcal{A} -valué adapté à \equiv .

La superconsistance était connue pour être un critère de normalisation forte d'une théorie en déduction modulo. On montre ici qu'elle est un critère de normalisation faible en temps élémentaire en logique linéaire élémentaire modulo.

Théorème 11 (Superconsistance implique normalisation).

Si \equiv est une théorie superconsistante, alors le théorème 9 est toujours valable pour ELL_{\equiv} .

preuve. La preuve repose essentiellement sur le fait que le théorème 9 a besoin:

- du théorème d'adéquation, qui est toujours vrai si la valuation $|\cdot|$ est adaptée à \equiv , ainsi qu'on l'a dit précédemment.
- de la construction d'un modèle des candidats de réductibilité quantitatifs, construction qui est toujours possible si l'on peut construire une valuation adaptée à \equiv . Or étant donné le théorème 10, la superconsistance implique l'existence d'une telle valuation. \triangleleft

Remarque. • *Nous n'avons pas montré que la superconsistance impliquait la normalisation forte dans MELL . Cependant cette propriété est certainement vraie. Pour la prouver, il faudrait reprendre la preuve de normalisation forte commencée par Okada dans [27]. Cette preuve traite de manière incomplète les additifs et la modalité $!$, mais si l'on se restreint à MELL , il est possible de la compléter (voir [28] pour plus d'explications). Il est à noter que si \equiv est superconsistante, alors MELL_{\equiv} normaliserait fortement et ELL_{\equiv} normaliserait faiblement en temps élémentaire. Existe-t-il alors une théorie normalisant fortement dans MELL mais pas en temps élémentaire dans ELL ?*

- *Il existe des théories exprimables sous la forme d'une congruence \equiv , telles que ELL_{\equiv} normalise en temps élémentaire, mais \equiv n'est pas superconsistante. On sait depuis les travaux de Girard [18] et Terui [31] que l'on peut rajouter un schéma de compréhension naïf à ELL sans casser la normalisation en temps élémentaire. Or cette théorie implique qu'il existe une formule A telle que $A \equiv !(A^+)$. Si l'on prend la LTVA $\mathcal{B} = (\{0, 1\}, +, x \mapsto x, x \mapsto (1-x))$ ($+$ est le "OU" booléen), trivialement complète et ordonnée, alors $!|A^+| = 1 - |A| \neq |A|$ et donc il est impossible d'obtenir un modèle de \equiv pour cette algèbre.*

4.3 Des théories superconsistantes

Plusieurs théories intéressantes sont superconsistantes et donc ne cassent pas la normalisation en temps élémentaire. Dans la tradition de la déduction modulo, quelques théories sont bien connues pour être superconsistantes. Parmi celles-ci, notons:

- La logique d'ordre supérieur (cf [9]).
- L'arithmétique de Péano (cf [9]).

Pour exprimer ces théories, il nous faudrait disposer de la quantification du premier ordre \forall . Néanmoins, par manque de place, nous ne l'avons pas traitée dans ce rapport. Nous nous intéressons donc à une théorie intéressante qui n'en a pas besoin. Cette théorie introduit un type point-fixe, et correspond à l'équivalence linéaire suivante, valable pour toute formule A telle que la variable du second-ordre X n'apparaît qu'en occurrence positive dans A (c'est-à-dire qu'on ne traverse qu'un nombre pair de $(\cdot)^{\perp}$ pour atteindre X):

$$\mu X.A \circ\text{-}\circ A[\mu X.A/X]$$

Cette théorie permet notamment de définir différentes structures de données linéaires comme les entiers ou les mots de Scott [26]. On introduit ici cette théorie sous la forme d'une congruence \equiv et on montre que \equiv est superconsistante, et donc que ELL_{\equiv} normalise en temps élémentaire. On rappelle qu'une théorie du premier ordre porte sur un langage du premier ordre, lui-même constitué d'un ensemble de sortes, de symboles de prédicats et de termes du premier ordre. On pourra se reporter à [9] pour une présentation plus formelle des théories du premier ordre avec congruence. Décrivons la théorie considérée, en commençant par le langage du premier ordre:

- Il existe une seule sorte o .
- Le langage introduit un unique symbole de prédicat unaire ϵ d'arité (o).
- Les termes sont construits inductivement à partir des constantes $\bar{\otimes} : o \rightarrow o \rightarrow o$, $\bar{\wp} : o \rightarrow o \rightarrow o$, $\bar{\neg} : o \rightarrow o$, $\bar{\dagger} : o \rightarrow o$, $\bar{\ddagger} : o \rightarrow o$, $\bar{\mu} : (o \rightarrow o) \rightarrow o$ et des variables \bar{X} pour chaque variable X du second ordre. $\bar{\mu}$ représente l'opérateur de point fixe.

On peut étendre la notation $\bar{\cdot}$ en une traduction des formules de ELL vers le langage des termes (ici \odot est une notation pour \otimes et \wp , et \diamond signifie ! ou ?):

$$\begin{aligned}\overline{A \odot B} &= \overline{A} \odot \overline{B} \\ \overline{\diamond A} &= \diamond \overline{A} \\ \overline{A^\perp} &= \overline{\neg A}\end{aligned}$$

On définit la relation \equiv comme la plus petite congruence \equiv telle que:

$$\begin{aligned}\epsilon(\overline{A}) &\equiv A \\ \epsilon(x \overline{\odot} y) &\equiv \epsilon(x) \odot \epsilon(y) \\ \epsilon(\overline{\diamond} x) &\equiv \diamond \epsilon(x) \\ \epsilon(\overline{\neg} x) &\equiv \epsilon(x)^\perp\end{aligned}$$

Et telle que pour chaque formule F où la variable du second ordre X n'apparaît qu'en occurrence positive $\bar{\mu}(\lambda \bar{X}. \overline{F}) \equiv \overline{F}[(\bar{\mu}(\lambda \bar{X}. \overline{F}))/\bar{X}]$

Remarque. Pour toute formule F , $\epsilon(\overline{F}) \equiv F$. On peut alors considérer de manière équivalente une formule de ELL comme un terme et ainsi lui appliquer le point fixe.

Exemple. On a par exemple $\epsilon(\bar{\mu}(\lambda \bar{X}. \overline{Y^\perp \otimes X})) \equiv Y^\perp \otimes \epsilon(\bar{\mu}(\lambda \bar{X}. \overline{Y^\perp \otimes X}))$.

Théoreme 12 (Superconsistance).

La théorie \equiv est superconsistante.

preuve. On pose $M_o = C$ et $D_{a \rightarrow b} = D_b^{D_a}$. On interprète $\bar{\odot}$ (resp. $\bar{\diamond}$, $\bar{\neg}$) par \odot (resp. \diamond , \neg) les opérations sur les comportements définies dans les sections précédentes. On choisit n'importe quel candidat pour interpréter les \bar{A} . ϵ est alors l'identité.

$$\mu : f \in D_{o \rightarrow o} \mapsto \begin{cases} \text{Un point fixe de } f \text{ si } f \text{ est croissante sur } (C, \subseteq) \\ \perp^\circ \text{ sinon} \end{cases}$$

Pour vérifier qu'on a bien un modèle de \equiv , il suffit de voir que si A est une formule où la variable X n'apparaît qu'en occurrence positive, alors $x \mapsto \overline{A}$ est croissante sur (C, \subseteq) (on le montre aisément par induction sur le langage des formules). ◀

5 Conclusion

Nous avons introduit dans ce rapport les candidats de réductibilité quantitatifs, un cadre d'étude de la normalisation des réseaux de preuve en temps borné à la fois proche des idées de la réalisabilité à la Krivine [20], des espaces de phase calculatoires d'Okada [27] et de la réalisabilité de Hofmann et Dal Lago [5]. Cette technique permet de donner une preuve sémantique hautement modulaire du théorème de normalisation faible en temps élémentaire des réseaux de preuve de ELL. Nous avons également exprimé un critère algébrique de normalisation faible en temps élémentaire de théories du premier ordre pour ELL. Ce critère permet d'étendre l'ensemble des structures de preuve typables dans ELL sans perdre la propriété de normalisation en temps élémentaire. Il reste un certain nombre de questions ouvertes et de pistes à explorer. En voici une liste non exhaustive.

- Peut-on complètement reformuler le cadre décrit ici pour le λ -calcul et ainsi simplifier à l'aide de la biorthogonalité la réalisabilité de Dal Lago et Hofmann?
- Krivine a introduit récemment le concept d'algèbre de réalisabilité [21]. Est-il possible de faire rentrer les espaces de phase quantitatifs dans ce cadre?
- Une piste semblant prometteuse concerne le domaine de la compilation. Dans [19], les auteurs utilisent une variante de la réalisabilité classique de Krivine pour montrer la correction de la compilation d'un langage fonctionnel. Leur cadre de travail étant proche du notre (notamment par son utilisation centrale de la biorthogonalité), il pourrait être possible de montrer qu'un compilateur bien choisi préserve les propriétés de complexité de λ -termes typables dans une logique allégée comme **ELL** ou **LAL**.
- Les travaux de Shirahata [30], de Girard [18] et de Terui [31] ont montré qu'on pouvait étendre certains fragments de la logique linéaire comme **MLL**, **LAL** ou **ELL** avec un schéma de compréhension naïf sans perdre la cohérence ni la propriété de normalisation en temps borné. Est-il possible de définir des modèles de réalisabilité d'une de ces théories naïves des ensembles par des méthodes similaires à celles présentées dans ce rapport? Prouver l'existence d'un modèle valué du schéma de compréhension naïf valué dans les candidats de réductibilité permettrait par exemple de prouver la normalisation de la théorie associée.
- Nous avons ici uniquement parler de normalisation faible. Il pourrait être intéressant de se pencher sur la question de la normalisation forte en temps borné, en commençant par celle de **ELL**.
- Si nos candidats de réductibilité quantitatifs ne s'intéressent ici qu'à borner le temps de normalisation, il pourrait être intéressant de s'intéresser à la complexité en espace.
- Enfin, il est nécessaire de continuer à explorer le champs des théories superconsistantes, ce qui permettrait d'étendre l'expressivité des logiques allégées.

Remerciements

Je tiens à adresser mes plus sincères remerciements à Olivier Hermant pour son accueil, sa gentillesse et sa disponibilité. Je remercie également Gilles Dowek pour son accueil chaleureux au sein du LIX et de l'équipe TYPICAL et les discussions, toujours enrichissantes, que nous avons eues au cours de ces 5 mois. Enfin, je remercie l'ensemble des personnes avec qui j'ai pu interagir au sein du LIX et de l'ISEP.

References

- [1] A. Asperti. Light affine logic. In *Thirteenth Annual IEEE Symposium on Logic in Computer Science, 1998. Proceedings*, pages 300–308, 1998.
- [2] A. Brunel and K. Terui. Church \Rightarrow Scott = Ptime: an application of resource sensitive realizability. *Electronic Proceedings in Theoretical Computer Science*, 23, 2010.
- [3] P.J. Cohen. The independence of the continuum hypothesis. *Proceedings of the National Academy of Sciences of the United States of America*, 50(6):1143, 1963.
- [4] D. Cousineau. Complete reducibility candidates. *proceedings of PSTT09*, 2009.

- [5] U. Dal Lago and M. Hofmann. Quantitative models and implicit complexity. *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science*, pages 189–200, 2005.
- [6] U. Dal Lago and M. Hofmann. A Semantic Proof of Polytime Soundness of Light Affine Logic. *Theory of Computing Systems*, 46(4):673–689, 2010.
- [7] U. Dal Lago and S. Martini. Phase semantics and decidability of elementary affine logic. *Theoretical Computer Science*, 318(3):409–433, 2004.
- [8] V. Danos and J.B. Joinet. Linear logic and elementary time. *Information and Computation*, 183(1):123–137, 2003.
- [9] G. Dowek. Truth values algebras and proof normalization. *Types for Proofs and Programs*, pages 110–124, 2007.
- [10] G. Dowek and A. Miquel. Cut elimination for Zermelo set theory. *manuscript*, 2007.
- [11] G. Dowek and B. Werner. Proof normalization modulo. *Types for proofs and programs*, pages 62–77, 1999.
- [12] M. Gaboardi, J.Y. Marion, and S.R. Della Rocca. A logical account of PSPACE. In *Proceedings of the 35th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 121–131. ACM, 2008.
- [13] J.H. GALLIER. On Girard's" Candidats de Reductibility. In *Logic and computer science*, page 123. Academic Pr, 1990.
- [14] Olivier Hermant Gilles Dowek. A Simple Proof That Super-Consistency Implies Cut Elimination. In *Term rewriting and applications: 18th international conference, RTA 2007, Paris, France, June 26-28, 2007: proceedings*, page 93. Springer-Verlag New York Inc, 2007.
- [15] S. Gimenez. Programmer, Calculer et Reasonner avec les Réseaux de la Logique Linéaire. *PHD Thesis*.
- [16] J.Y. Girard. Interpr etation fonctionnelle et elimination des coupures de l'arithm etique d'ordre superieur. *Th ese d'etat, Universit e Paris VII*, 1972.
- [17] J.Y. Girard. Linear logic* 1. *Theoretical computer science*, 50(1):1–101, 1987.
- [18] J.Y. Girard. Light linear logic. In *Logic and Computational Complexity*, pages 145–176. Springer, 1995.
- [19] G. Jaber and N. Tabareau. Krivine realizability for compiler correctness. *LOLA 2010*, 2010.
- [20] JL Krivine. Realizability in classical logic. Course notes of a series of lectures given in the University of Marseille, may 2004 (last revision: july 2005). *Panoramas et synthèses, Société Mathématique de France*, 2005.
- [21] J.L. Krivine. Realizability algebras: a program to well order R. *manuscript*, 2010.
- [22] J.L. Krivine. Realizability algebras II: new models of ZF+ DC. *Arxiv preprint arXiv:1007.0825*, 2010.
- [23] Y. Lafont. Soft linear logic and polynomial time. *Theoretical Computer Science*, 318(1-2):163–180, 2004.

- [24] D. Leivant and J.Y. Marion. Lambda calculus characterizations of poly-time. In *Typed Lambda Calculi and Applications: International Conference on Typed Lambda Calculi and Applications, TLCA'93, March 16-18, 1993, Utrecht, the Netherlands: Proceedings*, page 274. Springer, 1993.
- [25] S. Lengrand and A. Miquel. Classical F [omega], orthogonality and symmetric candidates. *Annals of Pure and Applied Logic*, 153(1-3):3–20, 2008.
- [26] M. n Abadi, L. Cardelli, and G. Plotkin. Types for the Scott numerals. *manuscript*, 1993.
- [27] M. Okada. Phase semantic cut-elimination and normalization proofs of first-and higher-order linear logic. *Theoretical Computer Science*, 227(1-2):333–396, 1999.
- [28] M. Pagani and L. Tortora de Falco. Strong normalization property for second order linear logic. *Theoretical Computer Science*, 411(2):410–444, 2010.
- [29] C. Riba and I.S. Antipolis-Méditerranée. Toward a General Rewriting-Based Framework for Reducibility. *manuscript*, 2008.
- [30] M. Shirahata. Linear set theory. *PHD Thesis*, 1994.
- [31] K. Terui. Light affine set theory: a naive set theory of polynomial time. *Studia Logica*, 77(1):9–40, 2004.

A Preuves des théorèmes: MLL

A.1 Théorème d'adéquation à MLL

On donne ici la preuve du théorème 4 d'adéquation des modèles de phase quantitatifs multiplicatifs à MLL énoncé dans la section 2. On rappelle l'énoncé:

Théorème (Adéquation à MLL).

Soit $(D, \mathcal{M}, \perp, |\cdot|)$ un modèle de phase quantitatif multiplicatif. Si $\vdash_{MLL} x_1 : A_1, \dots, x_n : A_n, t : B$ alors il existe $p \in \mathcal{M}$ tel qu'on ait pour tous $(u_i, q_i) \Vdash A_i$,

$$(t[x_1 := u_1, \dots, x_n := u_n], p + (q_1 + \dots + q_n)) \Vdash B$$

de plus, $p = (\#(t)_{ax} + \#(t)_{\mathfrak{X}})\mathbf{1}$, où $\#(t)_{ax}$ (resp. $\#(t)_{\mathfrak{X}}$) est le nombre de liens axiome (resp. liens \mathfrak{X}) de t .

Proof. Le théorème est prouvé par induction sur la construction du réseau de preuve t :

- Si t est un axiome:

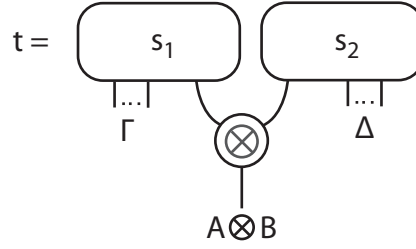
$$t = \begin{array}{c} ax \\ \text{---} \\ A^\perp \quad A \end{array}$$

Alors, étant donné un couple $(u, q) \Vdash A$ on a

$$t[u] = \begin{array}{c} \text{---} \\ \boxed{u} \\ \text{---} \\ \text{cut} \end{array} \begin{array}{c} ax \\ \text{---} \\ \text{---} \\ \circ \end{array} \triangleright \begin{array}{c} \text{---} \\ \boxed{u} \\ \text{---} \\ \circ \end{array}$$

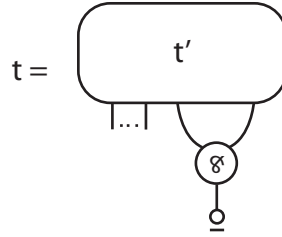
Enfin, comme $|A|$ est $>_0$ -saturé (car c'est un comportement), nous pouvons conclure que $(t[u], q + \mathbf{1}) \Vdash A$: le majorant est $p = \mathbf{1}$.

- Si t se termine par un tenseur:

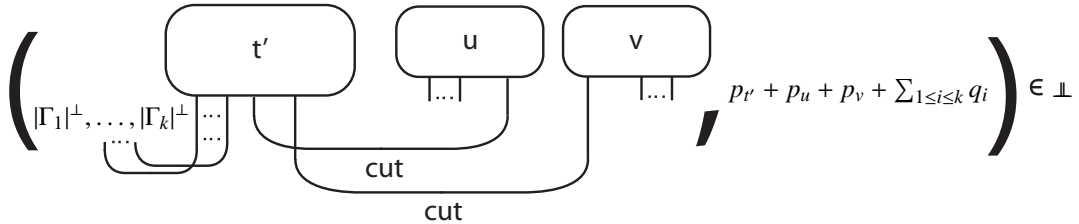


On sait par induction qu'il existe deux majorants p_1 et p_2 tels que pour tous $(g_1, q_1) \Vdash \Gamma_1^\perp, \dots, (g_n, q_n) \Vdash \Gamma_n^\perp$, et tous $(d_1, r_1) \Vdash \Delta_1^\perp, \dots, (d_k, r_k) \Vdash \Delta_k^\perp$, on ait $(s_1[g_1, \dots, g_n], p_1 + (q_1 + \dots + q_n)) \in |A|$ et $(s_2[d_1, \dots, d_n], p_2 + (r_1 + \dots + r_k)) \in |B|$. Ainsi, on a de manière évidente $(s_1[g_1, \dots, g_n] \otimes s_2[d_1, \dots, d_n], (p_1 + p_2) + (q_1 + \dots + q_n) + (r_1 + \dots + r_k)) \in |A|. |B| \subseteq |A \otimes B|$. Enfin, comme $s_1[g_1, \dots, g_n] \otimes s_2[d_1, \dots, d_n] = (s_1 \otimes s_2)[g_1, \dots, g_n, d_1, \dots, d_n]$, on peut conclure si l'on choisit le majorant $p = p_1 + p_2$.

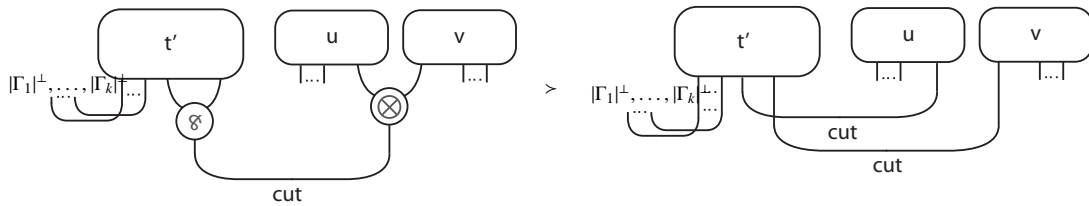
- Si t se termine par un lien \wp :



Il existe par hypothèse d'induction un majorant $p_{t'}$ tel que pour tout $(u, p_u) \Vdash A^\perp$ et pour tout $(v, p_v) \Vdash B^\perp$,

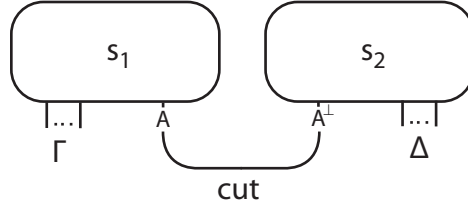


Par $>_0$ -saturation, et comme nous avons



on peut conclure que $(t[|\Gamma_1|^\perp, \dots, |\Gamma_k|^\perp] \star (u \otimes v), p_t + (p_u + p_v + \mathbf{1}) + \sum_{1 \leq i \leq k} q_i + \mathbf{1}) \in \perp$. Mais cela signifie que $(t[|\Gamma_1|^\perp, \dots, |\Gamma_k|^\perp], p_t + \sum_{1 \leq i \leq k} q_i + \mathbf{1}) \in (|A|^\perp. |B|^\perp)^\perp$. C'est exactement le résultat voulu (si l'on prend le majorant $p = p_t + \mathbf{1}$) car $|A \wp B| = (|A|^\perp. |B|^\perp)^\perp$.

- Enfin si t se termine par un lien coupeure:



Alors nous savons qu'il y a deux majorants p_1 et p_2 tels que pour tous $(g_1, q_1) \Vdash \Gamma_1^\perp, \dots, (g_n, q_n) \Vdash \Gamma_n^\perp$, et pour tous $(d_1, r_1) \Vdash \Delta_1^\perp, \dots, (d_k, r_k) \Vdash \Delta_k^\perp$, nous avons $(s_1[g_1, \dots, g_n], p_1 + (q_1 + \dots + q_n)) \Vdash A$ et $(s_2[d_1, \dots, d_n], p_2 + (r_1 + \dots + r_k)) \Vdash A^\perp$. Ainsi, $(s_1[g_1, \dots, g_n] \star s_2[d_1, \dots, d_k], (p_1 + p_2) + (q_1 + \dots + q_n + r_1 + \dots + r_k)) \in \perp$. Puis comme $s_1[g_1, \dots, g_n] \star s_2[d_1, \dots, d_k] = (s_1 \star s_2)[g_1, \dots, g_n, d_1, \dots, d_k]$, on peut conclure (le majorant est $p = p_1 + p_2$).

□

A.2 Modèle des candidats quantitatifs pour MLL

Nous prouvons ici les propriétés nécessaires pour montrer le théorème 5 exposé dans la section 2.3, qui exprime le fait que la structure des candidats de réductibilité quantitatifs pour MLL est bien un modèle de phase. On suppose qu'un monoïde quantitatif avec unité $\mathcal{M} = (\mathcal{M}, \mathbf{0}, +, \|\cdot\|, \mathbf{1})$ est fixé. Nous rappelons la définition du pôle:

$$\perp = \{ (t, p) \in \Lambda \times \mathcal{M} \mid \text{Time}(t) \leq \|p\| \}$$

On commence par montrer que le pôle est $>_0$ -saturé. C'est ici qu'on a besoin du fait que $\mathbf{1}$ est une unité de \mathcal{M} .

Lemme 5.

\perp est $>_0$ -saturé.

preuve. Si $(t, p) \in \perp$ et $u >_0 t$, alors $\text{Time}(u) = \text{Time}(t) + 1 \leq \|p\| + 1 = \|p + \mathbf{1}\|$ (car $\mathbf{1}$ est une unité de \mathcal{M}). Donc $(u, p + \mathbf{1}) \in \perp$.

◀

On continue en prouvant que \perp° est un comportement.

Lemme 6.

$\perp^\circ = \{ (\star, \mathbf{0}) \}^\perp$ et est en particulier un comportement.

preuve. Cette propriété repose sur le fait que $\text{Time}(t \star \star) = \text{Time}(t)$.

- Si $(t, p) \in \perp^\circ$ alors $\text{Time}(t) \leq \|p\|$. Or $\text{Time}(t \star \star) = \text{Time}(t)$ et $\|p + \mathbf{0}\| = \|p\|$. Donc $\text{Time}(t \star \star) \leq \|p + \mathbf{0}\|$ et ainsi $(t, p) \star (\star, \mathbf{0}) \in \perp : (t, p) \in \{ (\star, \mathbf{0}) \}^\perp$.
- Si $(t, p) \in \{ (\star, \mathbf{0}) \}^\perp$, cela signifie que $\text{Time}(t) = \text{Time}(t \star \star) \leq \|p + \mathbf{0}\| = \|p\|$. Donc $(t, p) \in \perp^\circ$.

◀

Enfin on montre la stabilité de D (l'ensemble des candidats de réductibilité quantitatifs) par $(\cdot)^\perp$ puis par \otimes .

Lemme 7.

Si $X \in D$, alors $X^\perp \in D$.

preuve.

- On veut montrer $(\star, \mathbf{0}) \in X^\perp$. Il suffit de prendre $(t, p) \in X^{\perp\perp} = X$ et montrer $(\star, \mathbf{0}) \star (t, p) \in \perp$. Comme $X \subseteq \perp^\circ$, $\text{Time}(t \star \star) = \text{Time}(t) \leq \|p\| = \|p + \mathbf{0}\|$, et donc $(\star, \mathbf{0}) \star (t, p) \in \perp$.
- Montrons que $X^\perp \subseteq \perp^\circ$. Soit $(t, p) \in X^\perp$. Alors comme $(\star, \mathbf{0}) \in X$, $(t \star \star, p + \mathbf{0}) \in \perp$. Cela signifie que $\text{Time}(t) = \text{Time}(t \star \star) \leq \|p + \mathbf{0}\| = \|p\|$.

◀

Lemme 8.

Si $X, Y \in D$, alors $X \otimes Y \in D$.

- preuve.**
- Pour montrer que $(\mathbf{0}, \mathbf{0}) \in X \otimes Y$, il suffit de prendre $(t, p) \in (X \otimes Y)^\perp = (X.Y)^\perp$ et de prouver $(\mathbf{0}, \mathbf{0}) \star (t, p) \in \perp$, ce qui est équivalent à $(t, p) \in \perp^\circ$. Or, $Time(t) \leq Time(t \star (\mathbf{0} \otimes \mathbf{0})) \leq \|p + (\mathbf{0} + \mathbf{0})\| = \|p\|$ (car comme $X, Y \in D$ on a $(\mathbf{0} \otimes \mathbf{0}, \mathbf{0} + \mathbf{0}) \in X.Y$).
 - Si $(t, p) \in X$ et $(u, q) \in Y$, alors par hypothèse, $Time(t) \leq \|p\|$ et $Time(u) \leq \|q\|$. Or, il est aisé de voir que $Time(t \otimes u) = Time(t) + Time(u) \leq \|p\| + \|q\| \leq \|p + q\|$ (car \mathcal{M} est un monoïde quantitatif). Donc on obtient $X.Y \subseteq \perp^\circ$. Or \perp° étant un comportement, $X \otimes Y = (X.Y)^{\perp\perp} \subseteq \perp^{\circ\perp\perp} = \perp^\circ$.

◁

Tous ces lemmes suffisent à montrer le théorème 5.

B Preuves pour ELL

B.1 Théorème d'adéquation à ELL

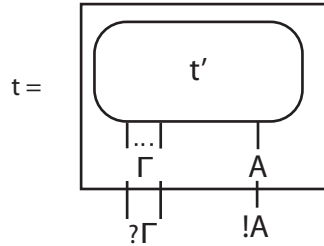
On donne ici la preuve du théorème 7 d'adéquation des modèles de phase quantitatifs élémentaires à ELL énoncé dans la section 3. On rappelle l'énoncé:

Théorème (Adéquation à ELL).

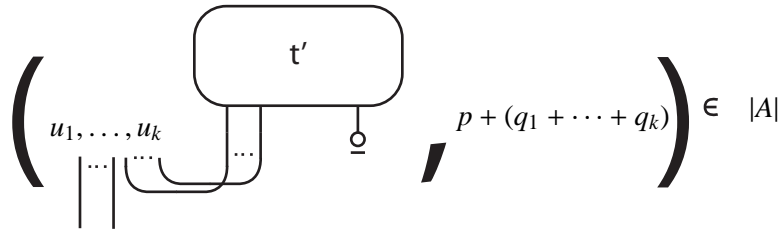
Soit $(\mathcal{M}, \perp, D, |\cdot|)$ un espace de phase quantitatif élémentaire. Si $\vdash_{ELL} x_1 : A_1, \dots, x_n : A_n, t : B$ alors il existe $p \in \mathcal{M}$ tel que pour chaque $(u_1, q_1) \Vdash A_1, \dots, (u_n, q_n) \Vdash A_n$, on ait $(t[x_1 := u_1, \dots, x_n := u_n], p + (q_1 + \dots + q_n)) \Vdash B$.

Proof. La preuve est effectuée par induction sur la construction de t . Les cas multiplicatifs sont les mêmes que dans le théorème 4

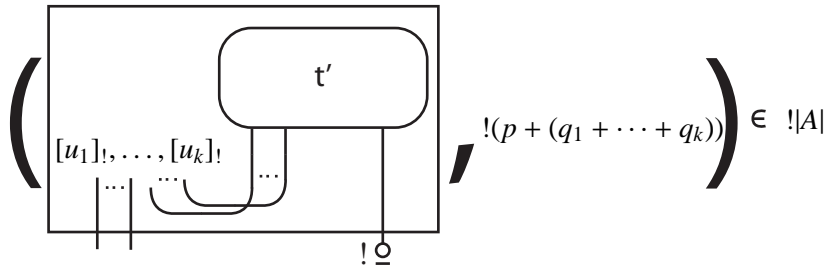
- Si t est une promotion fonctorielle:



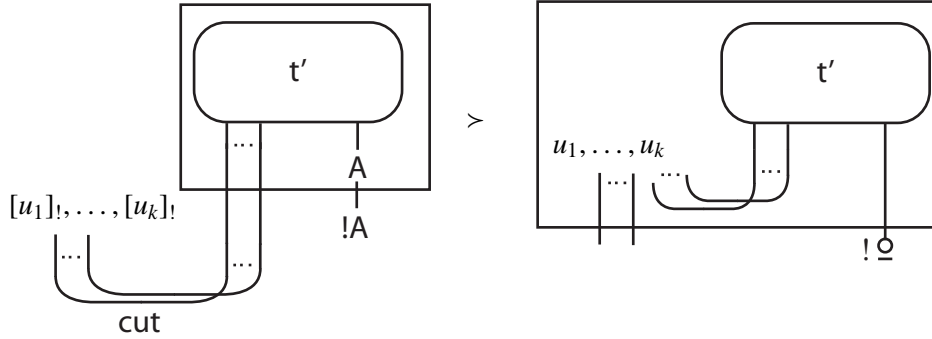
Avec $\Gamma = C_1, \dots, C_n$. On connaît par hypothèse d'induction l'existence d'un majorant p tel que pour tous $(u_1, q_1) \Vdash C_1^\perp, \dots, (u_n, q_n) \Vdash C_n^\perp$.



En appliquant la !-boîte et l'opération ! du monoïde au majorant, on obtient:

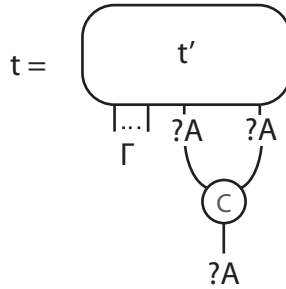


Mais, en utilisant la règle de réduction (!/!), on sait que:

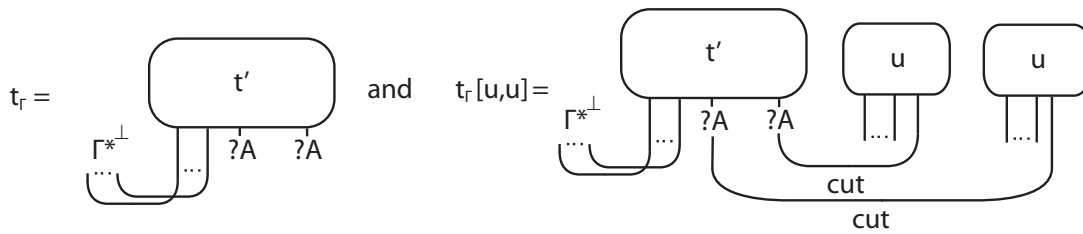


ce qui signifie par $>_0$ -saturation de $!|A|$ que $(t[[u_1]!, \dots, [u_n]!], !(p + \sum q_i) + \mathbf{1}) \Vdash !A$. Mais $!(p + \sum_i q_i) \leq !p + \sum_i (!q_i)$ (car le monoïde vérifie la propriété de functorialité de la définition 13) donc si on note $\alpha_i = \{ ([u]!, !q) \mid (u, q) \Vdash C_i \}$, alors par \leq -saturation de \perp , on obtient $(t, !p + \mathbf{1})[\alpha_1, \dots, \alpha_n] \subseteq !|A|$. Comme $!|C_i| = \alpha_i^{\perp\perp}$, nous avons $(t, !p + \mathbf{1})[!|C_1|, \dots, !|C_n|] \subseteq !|A|$, ce qui permet de conclure en choisissant le majorant $!p + \mathbf{1}$.

- Si la dernière règle utilisée est une contraction:

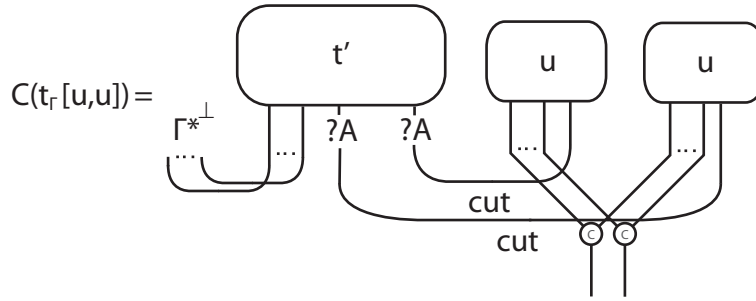


Alors si on prend $(u, !p_u) \in \Phi(|A|^\perp) \subseteq !|A|^\perp$ et si on pose

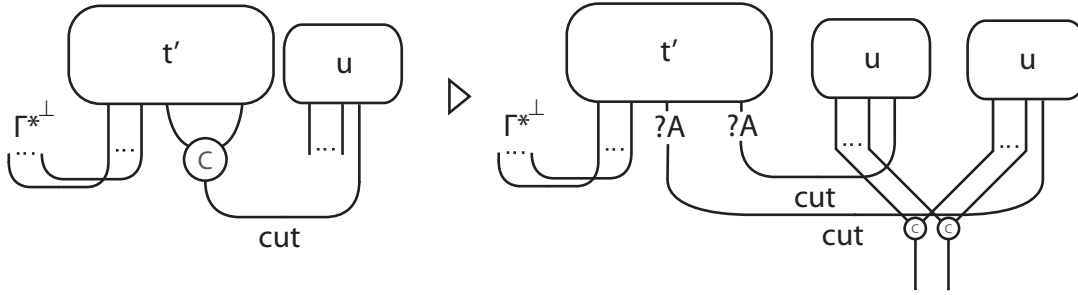


Comme t' est bien typé, on obtient par induction l'existence d'un $p_{t'}$ tel que $(t_\Gamma[u, u], p_{t'} + \sum_\Gamma q_i + !p_u + !p_u) \in \perp$.

Mais par la condition de contraction vérifiée par \perp , on sait que $C(t_\Gamma[u, u], p_{t'} + \sum_\Gamma q_i + !p_u + !p_u) \in \perp$ aussi, avec



Enfin comme le pas de réduction suivant s'applique:



On peut conclure par $>_0$ -saturation de \perp que $(t[\Gamma^*] \star u, p_r + \sum_{\Gamma} q_i + 2!p_u + \mathbf{1}) \in \perp$. Mais comme le monoïde vérifie la condition de contraction de la définition 13, $!p_u + !p_u \leq !p_u + r_{contr}$ et par \leq -saturation de \perp , $(t[\Gamma^*] \star u, p_r + \sum_{\Gamma} q_i + !p_u + \mathbf{1} + r_{contr}) \in \perp$. Ainsi, en prenant $p = p_r + \mathbf{1} + r_{contr}$, nous pouvons conclure.

- Si la dernière règle utilisée est un affaiblissement:



La propriété d'affaiblissement de \perp implique directement que le majorant recherché est p où est le majorant donné par hypothèse d'induction appliquée à t .

□

B.2 Le monoïde élémentaire

On montre les propriétés importantes du monoïde élémentaire \mathcal{M}_e (voir définition 14). En particulier, on montre que c'est un monoïde quantitatif et qu'il vérifie la propriété (P2).

Lemme 9.

$\mathcal{M}_e = (\mathcal{M}_e, +, 0, \leq, \|\cdot\|, !, (0, 2, 0, x \mapsto 0))$ vérifie les propriétés suivantes:

1. \leq est compatible avec $+$
2. $!(p + q) \leq !p + !q$
3. Pour tout $p \in \mathcal{M}_e$, $!p + !p \leq (0, 2, 0, x \mapsto 0) + !p$
4. Pour tous $p, q \in \mathcal{M}_e$, $\|p\| + \|q\| \leq \|p + q\|$
5. Si $p \leq q$ alors $\|p\| \leq \|q\|$

6. Pour chaque $p \in \mathcal{M}_e$, $\|p\| \leq \|!p\|$

preuve. Les preuves de ces propriétés utilisant l'opération $!$ sont triviales dès lors qu'un des majorants est $(0, 0, 0, x \mapsto 0)$ on suppose donc toujours que chaque majorant est non nul (ce qui évite de faire plusieurs cas).

$$\begin{aligned} !(a, n, m, f) + (b, l, k, g) &= !(a + b, n + l, m + k, f|g) \\ &= (1, n + l + m + k + a + b, (f|g)^+) \\ &= (1, n + l + m + k + a + b, (f^+|g^+)) \\ &\leq (2, n + l + m + k + a + b, (f^+|g^+)) \\ &= !(a, n, m, f) + !(b, l, k, g) \end{aligned}$$

$$\begin{aligned} !(a, n, m, f) + !(a, n, m, f) &= (0, 2, 2(n + m + a), f^+) \\ &\leq (0, 3, n + m + a, f^+) \\ &= (0, 2, 0, x \mapsto 0) + (0, 1, n + m + a, f^+) \\ &= (0, 2, 0, x \mapsto 0) + !(a, n, m, f) \end{aligned}$$

$$\begin{aligned} \|(a, n, m, f)\| + \|(b, l, k, g)\| &= nf(n + 2^n m) + a + lg(l + 2^l k) + b \\ &\leq nf(n + l + 2^{n+l}(m + k)) + lg(n + l + 2^{n+l}(m + k)) + a + b \\ &\leq n(f|g)(n + l + 2^{n+l}(m + k)) + l(f|g)(n + l + 2^{n+l}(m + k)) + a + b \\ &= (n + l)(f|g)(n + l + 2^{n+l}(m + k)) + a + b \\ &= \|(a + b, n + l, m + k, f|g)\| \\ &= \|((a, n, m, f) + (b, l, k, g))\| \end{aligned}$$

si $(a, n, m, f) \leq (b, l, k, g)$ alors

$$\begin{aligned} a + nf(n + 2^n m) &\leq a + lf(n + 2^n m) \\ &\leq b + lf(n + 2^n m) \\ &\leq b + lf(l + 2^l m) \\ &\leq b + lf(l + 2^l k) \\ &\leq b + lg(l + 2^l k) \\ &= \|(b, l, k, g)\| \end{aligned}$$

◀

B.3 Modèle des candidats de réductibilité quantitatifs élémentaires

Pour justifier la construction du modèle des candidats de réductibilité quantitatifs élémentaires évoquée dans la section 3.4, il suffit de prouver les propriétés suivantes:

- \perp est $>_0$ -saturé.
- \perp° est un comportement.
- D est stable par $(\cdot)^\perp$, \otimes et $!$.

Les deux premières propriétés ont été prouvées dans le cas multiplicatif. Il suffit d'étendre le théorème de stabilité pour les candidats multiplicatifs au cas de l'exponentielle élémentaire:

Lemme 10.

Si $X \in D$, alors $!X \in D$.

- preuve.**
- Montrons $(\star, \mathbf{0}) \in !X = (!X)^{\perp\perp}$. Soit $(u, q) \in (!X)^\perp$ et montrons $Time(u) \leq \|q\|$ (ce qui est équivalent à montrer $(\star, \mathbf{0}) \star (u, q) \in \perp$). Comme $X \in D$, on a $(\star, \mathbf{0}) \in X$ et donc $([\star]_!, \mathbf{0}) \in !X$. On conclut donc $Time(u) \leq Time(u \star [\star]_!) \leq \|q + \mathbf{0}\| = \|q\|$ (par la propriété **(P1)**).
 - Soit $(t, p) \in X$. On montre alors que $([t]_!, !p) \in \perp^\circ$. Comme $X \subseteq \perp^\circ$, on a $Time(t) \leq \|p\|$. Mais par la condition **(P2)**, on sait également que $\|p\| \leq \|!p\|$. De plus $Time([t]_!) = Time(t)$. On peut donc conclure $Time([t]_!) \leq \|!p\|$. On vient de montrer que $\{([t]_!, !p) \mid (t, p) \in X\} \subseteq \perp^\circ$. Or comme \perp° est un comportement on obtient:

$$!X = \{([t]_!, !p) \mid (t, p) \in X\}^{\perp\perp} \subseteq \perp^{\circ\perp\perp} = \perp^\circ$$

B.4 Preuve du théorème de normalisation en temps élémentaire

On donne la preuve du théorème 9 de normalisation en temps élémentaire. Elle utilise les deux propriétés suivantes, spécifiques au monoïde élémentaire \mathcal{M}_e . On rappelle que $r_{contr} = (0, 2, 0, x \mapsto 0)$.

Lemme 11.

Si $p = (x, y, z, f) \in \mathcal{M}_e$ et $a, b \in \mathbb{N}$, alors on a :

$$!(!(p) + ar_{contr} + b\mathbf{1}) = !(!(p + ar_{contr} + b\mathbf{1}))$$

Lemme 12.

Si $p, q \in \mathcal{M}_e$ et que $!p \leq !q$, alors $!!p \leq !!q$.

Théorème (Normalisation en temps élémentaire).

Il existe une famille de fonctions élémentaires $(e_i)_{i \in \mathbb{N}}$ telle que $\vdash_{ELL} A_1, \dots, A_n, t : B$ implique que t normalise en k étapes avec $k \leq e_{\partial(t)}(x)$.

preuve. Tout d'abord, remarquons que pour tout i , $|A_i| \in D$ et donc $(\mathfrak{X}, \mathbf{0}) \Vdash A_i$ quand $i \in \llbracket 1; n \rrbracket$. Ainsi, en appliquant le théorème d'adéquation 7 au modèle C_{ELL} , on obtient un majorant $p \in \mathcal{M}$ tel que $(t[\mathfrak{X}, \dots, \mathfrak{X}], p + n\mathbf{0}) \in |B| \subseteq \perp^\circ$. Donc, $Time(t[\mathfrak{X}, \dots, \mathfrak{X}]) \leq \|p + n\mathbf{0}\| = \|p\|$. Mais cela implique que $Time(t) \leq \|p\|$.

Maintenant, regardons plus en détail le majorant p . Si on inspecte le tableau 3.3, on voit que si $d = \partial(t)$:

$$p = !(!(\dots(!(q_d) + q_{d-1}) \dots) + q_2) + q_1) + q_0$$

où pour chaque $i \in \llbracket 0; n \rrbracket$, $q_i = a_i r_{contr} + b_i \mathbf{1}$ et

$$q_0 + \dots + q_d = (a_0 + \dots + a_d)r_{contr} + (b_0 + \dots + b_d)\mathbf{1} \leq |t|r_{contr} + |t|\mathbf{1} = (|t|)(r_{contr} + \mathbf{1})$$

Mais en itérant le lemme 11 on obtient que

$$p = !^d \left(\sum_{0 \leq i \leq d} q_i \right)$$

Parce que $q_0 + \dots + q_d \leq |t|(r_{contr} + \mathbf{1}) = (|t|, 2|t|, 0, 0)$, il est facile de voir que $!(\sum_i q_i) \leq !(|t|, 2|t|, 0, 0) = (0, 1, 3|t|, x \mapsto x)$. Et maintenant, en utilisant de manière itérée la propriété 12, on obtient $p = !^d (\sum_{0 \leq i \leq d} q_i) \leq !^d (|t|, 2|t|, 0, 0) = (0, 1, 3|t| + (d-1), \underbrace{((x \mapsto x)^+ \dots)^+}_{d \text{ fois}})$. Et

finalemtent:

$$\begin{aligned} Time(t) &\leq (x \mapsto x)^{++\dots+} (1 + 2(3|t| + (d-1))) \\ &\leq (x \mapsto x)^{++\dots+} (6|t| + 3d) \end{aligned}$$

Mais on voit que $e_d : x \mapsto (id)^{\overbrace{+ \dots +}^{d \text{ fois}}} (6x + 3d)$ est une fonction élémentaire en x .

C Modèles de phase quantitatifs généralisés

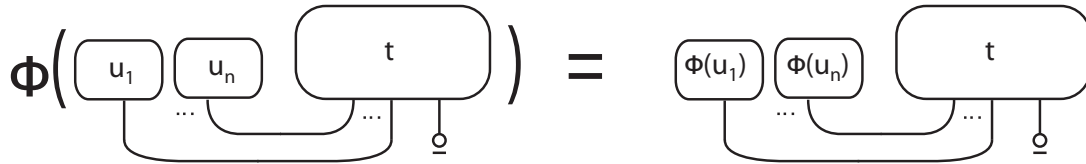
Il est possible de généraliser la notion de modèles quantitatifs en modifiant légèrement le langage des structures pointées, comme le fait Okada [27]. Cela permet de construire le modèle des candidats de réductibilité quantitatifs typés et d'obtenir une projection vers les espaces de phase élémentaires [7].

Définition 20 (Structures de preuve étiquetées). Soit L un ensemble quelconque. On note $L^\circ = L \cup \{\circ\}$ l'ensemble dont les éléments sont appelés *étiquettes*. Une L° -structure est une

structure de preuve dont les noeuds pendants sont étiquetés par des éléments de L° et telle qu'au plus un noeud pendent est étiqueté par \circ . L'ensemble des L° -structures dont un noeud est *distingué*, c'est-à-dire étiqueté par \circ est noté Λ° et l'ensemble des L° -structures sans noeud distingué est noté Λ .

Remarque. La notion de L° -structure généralise celle de structure pointée (il suffit de prendre L un singleton quelconque différent de $\{\circ\}$).

L'interprétation de l'exponentielle est généralisée elle aussi. On suppose fixée une fonction $\Phi : L \rightarrow L$. On définit alors l'action de Φ sur une L° -structure t comme la L° -structure $\Phi(t)$ obtenue en remplaçant dans t les étiquettes l par leur image $\Phi(l)$. On peut voir Φ comme un morphisme, en effet:



L'opération $!$ devient alors:

$$!X = \{ ([\Phi(t)]!, !p) \mid (t, p) \in X \}$$

On modifie en conséquence la définition de modèle de phase quantitatif.

Définition 21 (Espace de phase quantitatif élémentaire généralisé). On dit que la structure $(\mathcal{M}, L, \perp, \Phi, D, |\cdot|)$ est un *espace de phase quantitatif élémentaire généralisé* si $(\mathcal{M}, \perp, D, |\cdot|)$ vérifie les conditions des espaces de phase quantitatifs élémentaires (où l'opération $!$ originale est remplacée par celle que l'on vient de définir) exceptée la condition **(Contraction)** qui est remplacée par la condition **(Contraction')** suivante:

$$\text{(Contraction')} \text{ Si } (t[\Phi(u), \Phi(u)], p) \in \perp \text{ alors } (C(t[\Phi(u), \Phi(u)]), p) \in \perp.$$

C.1 Candidats de réductibilité quantitatifs typés

On dit qu'une L° -structure non distinguée $t \in \Lambda$ est L° -typable si il existe un étiquettage des noeuds internes de t par des formules de ELL tel que le résultat de cet étiquettage soit un réseau de preuve de ELL . On dit qu'un élément $t \in \Lambda^\circ$ possédant un noeud distingué est L° -typable par A si la structure non distinguée obtenue en remplaçant l'étiquette \circ par A est L° -typable. De plus \mathfrak{X} est toujours L° -typable par A , quelque soit la formule A .

Le pôle est désormais

$$\perp = \{ (t, p) \in \Lambda \times \mathcal{M} \mid \text{Time}(t) \leq \|p\| \text{ et } t \text{ est } L^\circ\text{-typable} \}$$

On définit l'observable de type A :

$$[[A]] = \{ (t, p) \in \Lambda^\circ \times \mathcal{M} \mid \text{Time}(t) \leq \|p\| \text{ et } t \text{ est } L^\circ\text{-typable par } A \}$$

Chaque observable est un comportement (on peut prouver que $[[A]] = \{(ax_{A^+}, \mathbf{1})\}^\perp$). Un *candidat de réductibilité quantitatif de type A* est un comportement X tel que:

$$(\mathfrak{X}, \mathbf{0}) \in X \subseteq [[A]]$$

Le domaine D choisi est encore une fois l'ensemble de tous les candidats de réductibilité quantitatifs typés. Enfin le morphisme Φ est défini comme $\Phi(A) = ?A$. Il est ainsi aisé de voir

que la propriété (**Contraction'**) est vérifiée, puisque une contraction ne sera bien typée que si elle relie deux formules de la forme $?A$. Enfin, pour montrer la stabilité de D par \otimes , $(.)^\perp$ et $!$, il faut reprendre la preuve des candidats non typés et l'étendre pour prendre en compte le typage.

On obtient ainsi un modèle des candidats de réductibilité quantitatifs typés, qui permettent d'obtenir une forme de complétude de la classe des modèles de phases quantitatifs élémentaires généralisés par rapport à ELL.

Illustrons la différence avec le modèle des candidats non typés. On peut en utilisant ce modèle, justifier la théorie $A \equiv A^\perp$. Il suffit de quotienter l'ensemble des formules par la plus petite congruence vérifiant $A \equiv A^\perp$ dans la définition de L° -typabilité. Les définitions des ensembles $\llbracket A \rrbracket$ et \perp sont alors modifiées en conséquence: comme $\llbracket A \rrbracket$ sera alors égal à $\llbracket A^\perp \rrbracket$, il suffit d'utiliser une valuation $|\cdot|$ telle que $|A| = \llbracket A \rrbracket$ ($|A^\perp|$ sera alors égale à $\llbracket A \rrbracket^\perp = \llbracket A^\perp \rrbracket = \llbracket A \rrbracket$) pour construire un modèle de candidats de réductibilité validant cet axiome.

C.2 Espaces de phase élémentaires

En utilisant les modèles de phases généralisés, on peut obtenir une notion de projection vers les modèles de phases élémentaires (pour la prouvabilité). On rappelle la définition de modèle de phase élémentaire, qui est une version légèrement modifiée de celle donnée dans [7].

Définition 22 (Modèle de phase élémentaire). Une structure $(P, \cdot, 1, \perp, \Phi, D, |\cdot|)$ est un *modèle de phase élémentaire* si:

- $(P, \cdot, 1)$ est un monoïde commutatif.
- $\perp \subseteq P$ est le pôle (qui définit une relation d'orthogonalité).
- $\Phi : P \rightarrow P$ est un morphisme de monoïde tel que si $\Phi(x) \in \{\Phi(x).\Phi(x)\}^{\perp\perp}$. De manière équivalente, si $y.(\Phi(x).\Phi(x)) \in \perp$ alors $y.\Phi(x) \in \perp$.
- D est un ensemble de *faits*, c'est-à-dire d'ensembles $X \subseteq P$ tels que $X = X^{\perp\perp}$.
- $|\cdot|$ est une valuation des formules atomiques vers D

Avec un tel modèle de phase élémentaire on interprète les formules de ELL par:

- $|A|$ si A est atomique
- $|A^\perp| = |A|^\perp$ si A est atomique
- $|A \otimes B| = (|A|.|B|)^{\perp\perp}$
- $|A \wp B| = (|A|^\perp.|B|^\perp)^\perp$
- $!|A| = (\Phi(|A|))^{\perp\perp}$
- $|?A| = (\Phi(|A|^\perp))^\perp$

Etant donné un modèle de phase élémentaire, on dit qu'une formule A est valide dans ce modèle si $1 \in |A|$. La classe des modèles de phase élémentaire est *correcte* et *complète* pour ELL [7], c'est-à-dire que si une formule est prouvable dans ELL, elle est valide dans tous les modèles, et inversement si une formule est valide dans tous les modèles, elle est prouvable.

On peut maintenant définir une *projection* des modèles de phase quantitatifs élémentaires généralisés vers les modèles de phase élémentaires.

Définition 23 (Projection). Soit $\mathcal{P} = (\mathcal{M}, L, \perp, \Phi, D, |\cdot|)$ un modèle de phase quantitatif élémentaire généralisé. On note \bar{L} le monoïde libre commutatif engendré par L . Si t est une L° -structure on note \bar{t} le mot formé des étiquettes étiquetant les noeuds d'environnement de t . Ce mot est un élément de \bar{L} . Si $X \subseteq \Lambda^\circ \times \mathcal{M}$ ou $X \subseteq \Lambda \times \mathcal{M}$, on note $\bar{X} = \{ \bar{t} \mid (t, p) \in X \}$.

On définit la *projection de \mathcal{P}* et on note $\bar{\mathcal{P}} = (\bar{L}, \perp, \bar{\Phi}, \bar{D}, |\cdot|)$ le modèle de phase élémentaire tel que:

- $\bar{\Phi}$ est le morphisme de monoïde obtenu par extension de Φ au monoïde \bar{L} .
- \bar{D} est l'ensemble des faits \bar{X} tels que X soit un élément de D .
- $|\cdot| : A \mapsto |\bar{A}|$.

Les conditions de la définition 22 sont aisées à vérifier.

On pourrait prouver le théorème suivant très simplement:

Théorème 13 (Représentation).

Si $P = (P, \cdot, 1, \Phi, D, |\cdot|)$ est un modèle de phase élémentaire et $(P, \cdot, 1)$ est isomorphe à un monoïde libre commutatif, alors il existe un modèle de phase quantitatif élémentaire généralisé \mathcal{P} tel que $P = \bar{\mathcal{P}}$.

Okada [27] montre également les deux points suivants (pour les modèles de phase de **MELL**, mais adapter les preuves à **ELL** est immédiat):

1. Le théorème de correction des modèles de phase élémentaire (dont le monoïde est libre) est une conséquence du théorème d'adéquation pour les modèles quantitatifs.
2. La construction du modèle des candidats quantitatifs pour **ELL** implique le théorème de complétude pour les modèles de phase élémentaire.