

Table des matières

1	Logique intuitionniste propositionnelle : approche par le calcul de séquents	
	LJ	2
1.1	Définition du calcul LJ	2
1.2	Prouvabilité d'un séquent	3
1.3	Une définition de la prouvabilité en logique intuitionniste	3
1.4	Comparaison avec la logique classique (calcul LK)	3
2	Propriétés favorisant l'application d'un calcul de séquents à la recherche automatisée de preuve et exemples de calculs	4
2.1	Algorithme de recherche de preuve	4
2.2	Propriétés intéressantes des calculs de séquents	5
	Absence de contraction. Propriété de la sous-formule. Inversibilité de certaines règles ou prémisses. Localité des règles.	
2.3	Deux exemples de calculs de séquents pour la logique intuitionniste	6
3	Le calcul de séquents utilisé pour l'implémentation : LSJ, légèrement modifié en LSJℓ	7
3.1	Séquents et règles de LSJ	7
3.2	Séquents et règles de LSJℓ	8
3.3	Équivalence entre LSJℓ et LSJ	9
4	Implémentation	11
4.1	Indexation	11
4.2	Structure de données pour le séquent	11
5	Perspective de certification	11
5.1	Un langage simple pour faciliter la certification	11
5.2	Compilation d'un programme spécifique à une formule donnée	11
5.3	Comparaison de différentes implémentations	11
5.4	Propriété de la sous-formule et indexation	12
6	Implémentation	13
6.1	Indexation	13
6.2	Structure de données pour le séquent	13

1 Logique intuitionniste propositionnelle : approche par le calcul de séquents LJ

Il existe de nombreuses approches de la logique intuitionniste : on choisit ici celle par le calcul de séquents **LJ** introduit par Gentzen. Elle fournit une définition de la prouvabilité d'une formule en logique intuitionniste qui n'est pas la plus courante ni la plus rapide à exposer ; mais elle permet de présenter un premier calcul de séquents avec de nombreuses définitions qui seront utiles par la suite.

On s'intéresse à la partie propositionnelle de la logique intuitionniste : les formules sont construites à partir de la constante \perp , de variables propositionnelles et des connecteurs binaires \wedge , \vee , \rightarrow . Une formule est *atomique* si elle est réduite à une variable propositionnelle ou \perp . La notation $\neg A$ signifie $A \rightarrow \perp$.

1.1 Définition du calcul LJ

Les éléments qui caractérisent généralement un calcul de séquents sont une définition de ses *séquents* et un ensemble de *règles*. Présentons ceux du calcul **LJ**.

Multiensembles et notations. On s'intéresse à des *multiensembles*, c'est-à-dire des collections où le nombre d'occurrences est pris en compte, mais non l'ordre des éléments. Cela permettra de ne pas avoir besoin de règles explicites d'échange. On utilise des lettres romaines (typiquement A, B, D, G) pour désigner les formules et des lettres grecques (Γ, Δ) pour les multiensembles de formules. La notation " A, Γ " représente le multiensemble obtenu à partir de Γ en ajoutant une occurrence de A .

Définition 1. Un **séquent** de **LJ** consiste en un multiensemble de formules Γ (les "*hypothèses*") et une formule D (la "*conclusion*") ; on écrit $\Gamma \Rightarrow D$.

Les **règles** du calcul **LJ** sont données dans la figure 1. Pour une règle $\frac{prem_1 \quad \dots \quad prem_p}{concl}(\mathcal{R})$, \mathcal{R} est le nom de la règle, $prem_1, \dots, prem_p$ sont les **prémisses**, et $concl$ la **conclusion**. $prem_k$ sera appelée la *k-ième prémiss*e ou *prémiss*e numéro *k*. Les prémisses et la conclusion sont des séquents où A, B, D sont des formules quelconques et Γ un multiensemble de formules quelconques. Les **axiomes** sont les règles sans prémisses. On distingue deux grandes familles de règles. Les *règles logiques* remplacent une formule de la conclusion par une ou des formules plus simples. La formule remplacée, appelée *formule principale*, doit avoir une forme donnée en fonction de la règle. Les *règles structurelles* manipulent la structure du séquent en enlevant, dupliquant, déplaçant des formules dont on n'a pas besoin de connaître la forme. Elles dépendent du choix de structure du séquent : si on avait représenté Γ par une liste et non un multiensemble, on aurait eu besoin d'ajouter une règle d'échange $\frac{\Gamma_1, A, B, \Gamma_2 \Rightarrow D}{\Gamma_1, B, A, \Gamma_2 \Rightarrow D} (permut. L)$.

Cette présentation est à peu près celle donnée par Dyckhoff dans [1]. Elle diffère de celle de Gentzen, mais elle en est suffisamment proche pour qu'on puisse quand même l'appeler le calcul **LJ**. On peut d'ailleurs facilement passer d'une définition à l'autre à l'aide des règles structurelles.

Identité	$\frac{}{A, \Gamma \Rightarrow A} (\text{Id})$	Coupure
$\frac{}{\perp, \Gamma \Rightarrow D} (\perp L)$	Règles logiques	$\frac{\Gamma_1 \Rightarrow A \quad \Gamma_2, A \Rightarrow D}{\Gamma_1, \Gamma_2 \Rightarrow D} (\text{cut})$
$\frac{A, B, \Gamma \Rightarrow D}{A \wedge B, \Gamma \Rightarrow D} (\wedge L)$	$\frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} (\wedge R)$	Règles structurales
$\frac{A, \Gamma \Rightarrow D \quad B, \Gamma \Rightarrow D}{A \vee B, \Gamma \Rightarrow D} (\vee L)$	$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} (\vee R_1)$ $\frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B} (\vee R_2)$	$\frac{\Gamma \Rightarrow D}{\Gamma, A \Rightarrow D} (\text{weakening } L)$
$\frac{\Gamma \Rightarrow A \quad B, \Gamma \Rightarrow D}{A \rightarrow B, \Gamma \Rightarrow D} (\rightarrow L)$	$\frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B} (\rightarrow R)$	$\frac{\Gamma, A, A \Rightarrow D}{\Gamma, A \Rightarrow D} (\text{contraction } L)$

FIGURE 1 – Règles du calcul **LJ**

1.2 Prouvabilité d'un séquent

Les définitions suivantes s'appliquent aux calculs de séquents en général, pas seulement **LJ**. Une **instance** d'une règle \mathcal{R} a la même forme que la règle : $\frac{\sigma_1 \quad \dots \quad \sigma_p}{\sigma} (\mathcal{R})$, mais ici les σ_i et σ sont des séquents connus explicitement ; bien entendu il faut qu'il s'agisse de séquents qui correspondent à la forme donnée par la définition de la règle. Une **preuve** (ou **arbre de preuve**) est un arbre dont les nœuds sont étiquetés par un séquent et une règle et ont la même arité que le nombre de prémisses de la règle, et tel que : pour tout nœud de séquent σ et de règle \mathcal{R} , si $\sigma_1, \dots, \sigma_p$ sont les séquents associés à chacun de ses fils respectivement, alors $\frac{\sigma_1 \quad \dots \quad \sigma_p}{\sigma} (\mathcal{R})$ est une instance de \mathcal{R} . Les feuilles d'un tel arbre sont les nœuds auxquels est associé un axiome.

Définition 2. Un séquent σ est **prouvable** dans un calcul de séquents s'il existe un arbre de preuve tel que le séquent associé à la racine est σ . De manière équivalente, on peut définir l'ensemble des séquents prouvables comme le plus petit ensemble vérifiant : pour toute instance $\frac{\sigma_1 \quad \dots \quad \sigma_p}{\sigma} (\mathcal{R})$ d'une règle, si pour tout i , σ_i est prouvable, alors σ est prouvable (en particulier pour toute instance $\frac{}{\sigma} (\mathcal{A})$ d'un axiome \mathcal{A} , σ est prouvable).

1.3 Une définition de la prouvabilité en logique intuitionniste

On peut maintenant donner une définition de la prouvabilité d'une formule en logique intuitionniste. L'idée est qu'un séquent $\Gamma \Rightarrow D$ représente la formule $(\bigwedge_{G \in \Gamma} G) \rightarrow D$.

Définition 3. Une formule A est **prouvable en logique intuitionniste** si le séquent $\Rightarrow A$ est prouvable par le calcul **LJ** (on écrit $\Rightarrow A$ pour $\emptyset \Rightarrow A$).

Il existe de nombreuses autres manières d'aborder la logique intuitionniste. Celle-ci n'est pas la plus courante, mais a permis d'introduire des définitions sur les calculs de séquents qui seront utiles par la suite.

1.4 Comparaison avec la logique classique (calcul LK)

La logique classique peut être définie à l'aide d'un calcul de séquents appelé **LK**, dont **LJ** a été dérivé pour la logique intuitionniste. Un séquent de **LK** comporte un autre multien-semble Δ de "conclusions" au lieu d'une unique conclusion D : on écrit $\Gamma \Rightarrow \Delta$. Un tel séquent

a également une interprétation logique : il représente la formule $(\bigwedge_{G \in \Gamma} G) \rightarrow (\bigvee_{D \in \Delta} D)$ en logique classique. Les règles diffèrent en conséquence : par exemple $\frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta} (\wedge R)$ remplace $\frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} (\wedge R)$. Bien entendu, on ajoute aussi des règles structurelles agissant sur Δ . Mais surtout, on n'a plus qu'une règle pour le \vee à droite : $\frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta} (\vee R)$. (Dans d'autres définitions, on conserve deux règles distinctes, mais la règle que nous donnons ici peut être déduite de ces deux règles et de règles structurelles.)

C'est la possibilité d'avoir plusieurs formules dans la partie droite du séquent qui permet de prouver davantage de séquents dans **LK** que dans **LJ**. On comprend ainsi la différence entre le "ou" classique et le "ou" intuitionniste. En logique classique, prouver $A \vee B$, c'est prouver le séquent $\Rightarrow A, B$: les deux formules sont encore présentes. Un bon exemple est la preuve du principe du tiers exclu $A \vee \neg A$ (figure 2 ; on rappelle que $\neg A$ est une notation pour $A \rightarrow \perp$) : si on peut appliquer l'axiome Id à la formule A (ce qui nécessite deux occurrences distinctes de la formule, une de chaque côté), c'est bien parce qu'on a conservé les deux parties de la formule initiale. Tandis qu'en logique intuitionniste, pour prouver $A \vee B$ c'est-à-dire $\Rightarrow A \vee B$, les seules règles applicables sont $\vee R_1$ et $\vee R_2$: il faut donc prouver $\Rightarrow A$ ou prouver $\Rightarrow B$; une fois qu'on a choisi lequel on va prouver, on n'a plus accès à l'autre. Ainsi, on ne peut pas prouver $A \vee \neg A$, car ni $\Rightarrow A$ ni $\Rightarrow \neg A$ n'est prouvable.

$$\frac{\frac{}{A \Rightarrow A, \perp} \text{Id}}{\Rightarrow A, (A \rightarrow \perp)} \rightarrow R \quad \frac{}{\Rightarrow A \vee (A \rightarrow \perp)} \vee R$$

FIGURE 2 – Preuve de $A \vee \neg A$ dans **LK**

2 Propriétés favorisant l'application d'un calcul de séquents à la recherche automatisée de preuve et exemples de calculs

Il existe plusieurs calculs de séquents pour la logique intuitionniste, sans parler des nombreuses autres logiques existantes. Un tel calcul comporte ses propres définition d'un séquent, règles, et construction pour chaque formule d'un séquent qui est prouvable par le calcul si et seulement si la formule est prouvable en logique intuitionniste. En dériver l'algorithme de recherche de preuve ci-après est assez naturel. Sa correction est immédiate par construction. En revanche, la terminaison pose problème. Elle n'est pas toujours assurée, et même quand elle l'est, souvent difficile à prouver. Nous présentons quelques propriétés sur les calculs de séquents qui sont intéressantes pour assurer la terminaison et améliorer la complexité de l'algorithme qui leur est associé. Enfin, nous donnons deux exemples de calculs de séquents existants pour la logique intuitionniste, antérieurs au calcul que nous utilisons pour l'implémentation.

2.1 Algorithme de recherche de preuve

On considère un calcul de séquents. Pour déterminer si un séquent est prouvable, on choisit une règle dont il peut être la conclusion et on applique récursivement la recherche de preuve aux prémisses correspondantes. Si elles sont toutes prouvables (en particulier, s'il n'y en a pas : si le séquent est la conclusion d'un axiome), alors par définition le séquent initial est aussi prouvable ; de plus, si on a calculé un arbre de preuve pour chaque prémisses, on en obtient un pour le séquent initial. Sinon, on essaie une autre règle (sauf dans certains cas où on peut conclure grâce à la notion de règle ou prémisses inversibles que nous verrons plus loin). Si on a essayé toutes les règles applicables au séquent sans succès, c'est-à-dire que pour chacune, au

moins une prémisses est non prouvable (en particulier, s'il n'y a aucune règle applicable : si le séquent n'est la conclusion d'aucune instance), on conclut que le séquent initial n'est pas prouvable.

Cet algorithme est correct par construction et d'après la définition de la prouvabilité d'un séquent. En revanche, il y a des causes possibles de non terminaison, qui se regroupent en deux catégories : "largeur" infinie, "profondeur" infinie. Pour éviter une "largeur" infinie, il faut que pour un séquent donné, le nombre d'instances dont il est conclusion soit fini. En ce qui concerne le problème de "profondeur" dû à la récursivité, on peut souvent munir les séquents d'un ordre bien fondé, de sorte que pour toute instance de règle, les prémisses sont toutes strictement inférieures à la conclusion.

Remarque : la règle de coupure. La règle de coupure, par exemple pour **LJ** :

$$\frac{\Gamma_1 \Rightarrow A \quad \Gamma_2, A \Rightarrow D}{\Gamma_1, \Gamma_2 \Rightarrow D} \text{ (cut)},$$

rend l'algorithme proposé inutilisable parce qu'il ne termine jamais. En effet, on explore indéfiniment en "largeur", car le nombre d'instances dont un séquent donné est conclusion est infini, A pouvant être n'importe quelle formule. Heureusement, cette règle est souvent non nécessaire. De nombreux calculs la formulent car c'est une bonne chose que l'implication représentée par un séquent soit transitive, mais s'en passent ensuite grâce à un *théorème d'élimination de la coupure* (souvent difficile à établir). Quoi qu'il en soit, on ne s'intéresse désormais qu'à des calculs dans lesquels cette règle n'est pas énoncée.

2.2 Propriétés intéressantes des calculs de séquents

Un calcul de séquents peut présenter certaines des propriétés suivantes, qui contribuent à assurer la terminaison ou à améliorer la complexité de l'algorithme précédent.

Absence de contraction. Certaines règles, comme la contraction à gauche de **LJ** :

$$\frac{\Gamma, A, A \Rightarrow D}{\Gamma, A \Rightarrow D} \text{ (contraction } L),$$

sont problématiques pour la terminaison de l'algorithme. En effet, pour essayer de prouver $\Gamma, A \Rightarrow D$, on peut être amené à essayer de prouver $\Gamma, A, A \Rightarrow D$, puis en appliquant encore la même règle à essayer de prouver $\Gamma, A, A, A \Rightarrow D$, et ainsi de suite, sans fin. Il est parfois possible d'adapter l'algorithme à une possibilité de contraction en prenant certaines précautions, comme on le verra pour le calcul **LJ**.

Propriété de la sous-formule. La formule B est une *sous-formule* de la formule A si B est égale à A ou si A est de la forme $A_1 \diamond A_2$ où \diamond est un connecteur et $[B$ est une sous-formule de A_1 ou B est une sous-formule de $A_2]$. Un calcul de séquents vérifie la *propriété de la sous-formule* si tout séquent prouvable σ admet une preuve telle que toute formule apparaissant dans (un séquent de) cette preuve est une sous-formule d'une formule de σ . La propriété de la sous-formule est très utile pour un calcul de séquents. Souvent, elle fait partie des arguments qui permettent de montrer la terminaison. Elle fournit en effet un ordre bien fondé sur les formules, qu'il reste à étendre de façon bien choisie aux séquents. Elle est également utile lors de l'implémentation : si on veut appliquer la recherche de preuve à un séquent donné, on peut connaître à l'avance la liste exhaustive de toutes les formules susceptibles d'apparaître. On peut donc effectuer une indexation préliminaire, puis représenter les formules par des objets de taille constante, par exemple des entiers, au lieu d'arbres qui peuvent être coûteux en mémoire. Voir la sous-section ? pour un exemple détaillé d'une telle indexation.

Inversibilité de certaines règles ou prémisses. Dans l'algorithme proposé, il peut être assez long de montrer qu'un séquent n'est pas prouvable, puisqu'on essaie toutes les instances dont il est la conclusion. La notion d'inversibilité permet de terminer beaucoup plus rapidement dans certains cas. Une prémisses $prem_i$ d'une règle $\frac{prem_1 \dots prem_p}{concl}(\mathcal{R})$ (auss appelé *i-ème prémisses de \mathcal{R}*) est **inversible** si on a : si $prem_i$ est non prouvable, alors $concl$ est non prouvable. Une règle est **inversible** si toutes ses prémisses sont inversibles. Ainsi, si au cours de la recherche de preuve, on obtient qu'une prémisses inversible est non prouvable, on peut directement conclure que la conclusion ne l'est pas non plus, sans avoir besoin d'essayer d'autre règle.

Localité des règles. L'algorithme nécessite de savoir déterminer, pour un séquent donné, toutes les instances dont il est conclusion, et en particulier calculer les prémisses de ces instances. Pour une instance, la *formule principale* est la formule de la conclusion qui est remplacée dans les prémisses par d'autres formules (règles logiques), ou dupliquée ou supprimée (règles structurelles). Dans le cas des règles logiques, la formule principale doit avoir une forme particulière, par exemple présenter un connecteur donné. Souvent, pour une conclusion et une règle données et un choix de formule principale autorisé par la règle, il existe une unique instance correspondante, dont on peut facilement calculer toutes les prémisses. Parfois, on a aussi le sens inverse : à partir de la k -ième prémisses, si on connaît la règle et le numéro k et la formule principale, on peut construire la conclusion. On dit qu'une règle est **locale** si on a cette dernière propriété pour toutes les prémisses de toutes ses instances. Si toutes les règles sont locales (et si on cherche juste à décider si un séquent est prouvable sans demander d'arbre de preuve le cas échéant), alors on peut ne garder qu'un seul séquent en mémoire à tout moment, plus des informations (numéro de prémisses, formule principale) qui sont moins coûteuses. Lorsqu'on s'intéresse à une instance dont le séquent retenu est conclusion, on transforme ce séquent en une prémisses, sur laquelle on relance l'algorithme. Et inversement, on a parfois besoin de revenir à la conclusion à partir d'une prémisses et des informations supplémentaires retenues : par exemple pour ensuite calculer une autre prémisses de l'instance, ou encore pour essayer d'appliquer une autre règle à la conclusion si on a trouvé une prémisses non prouvable et non inversible. Ainsi, si toutes les règles du calcul sont locales, on peut améliorer la complexité spatiale de l'algorithme.

2.3 Deux exemples de calculs de séquents pour la logique intuitionniste

LJ. Pour appliquer le calcul **LJ** présenté dans la première partie à la recherche automatique de preuves, il faut quelques ajustements sur le calcul lui-même et sur l'algorithme proposé. Il faut notamment enlever la règle de coupure (figure 1, *cut*), ce qui est possible car le calcul reste évidemment correct, mais surtout complet. Pour la même raison, on peut aussi enlever la règle *weakening*. En revanche, on ne peut pas supprimer purement et simplement la règle $\frac{\Gamma, A, A \Rightarrow D}{\Gamma, A \Rightarrow D}(\text{contraction } L)$. On ne pourrait par exemple plus prouver la formule $\neg\neg(A \vee \neg A)$. Mais comme on l'a vu, cette règle pose un problème de terminaison de l'algorithme. Une solution consiste à remplacer les deux règles *contraction L* et $\frac{\Gamma \Rightarrow A \quad B, \Gamma \Rightarrow D}{A \rightarrow B, \Gamma \Rightarrow D}(\rightarrow L)$ par une seule règle $\frac{A \rightarrow B, \Gamma \Rightarrow A \quad B, \Gamma \Rightarrow D}{A \rightarrow B, \Gamma \Rightarrow D} \rightarrow L$. On n'a alors plus d'appels récursifs sur des séquents strictement croissants $\Gamma, A \Rightarrow D$ puis $\Gamma, A, A \Rightarrow D$ puis $\Gamma, A, A, A \Rightarrow D$ etc. En revanche, on peut avoir un appel récursif sur un

séquent déjà rencontré, par exemple si $D = A$, une prémisse est identique à la conclusion dans $\frac{A \rightarrow B, \Gamma \Rightarrow A \quad B, \Gamma \Rightarrow A}{A \rightarrow B, \Gamma \Rightarrow A} \rightarrow L$. On ajoute alors un système de détection de cycles en retenant tous les séquents rencontrés. L'algorithme obtenu est correct et termine. On a la propriété de la sous-formule. Les règles sont toutes inversibles et locales sauf $\rightarrow L$, dont seule la deuxième prémisse est inversible. Mais la détection de cycles est très coûteuse.

LJT. Le calcul **LJT** est introduit par R. Dyckhoff dans [1] pour pallier le problème de cycles de **LJ**. Il n'y a pas de règle de contraction, et la règle $\rightarrow L$ est remplacée par quatre règles selon la structure de A dans la formule principale $A \rightarrow B$: par exemple $\frac{B, A, \Gamma \Rightarrow D}{A \rightarrow B, A, \Gamma \Rightarrow D} (\rightarrow L_1)$ où A doit être réduite à une variable, ou encore $\frac{A_1 \rightarrow (A_2 \rightarrow B), \Gamma \Rightarrow D}{(A_1 \wedge A_2) \rightarrow B, \Gamma \Rightarrow D} (\rightarrow L_2)$. On n'a pas la propriété de la sous-formule, mais on peut quand même déterminer toutes les formules susceptibles d'apparaître lorsqu'on essaie de prouver un séquent donné. Dyckhoff montre que l'algorithme termine en choisissant bien un bon ordre sur les formules puis sur les séquents. Toutes les règles sont inversibles et locales sauf une des règles qui remplacent $\rightarrow L$, qui comporte deux prémisses dont seule la deuxième est inversible.

3 Le calcul de séquents utilisé pour l'implémentation : **LSJ**, légèrement modifié en **LSJℓ**

Le calcul de séquents utilisé pour l'implémentation est **LSJℓ**, une variante de **LSJ**. Le calcul **LSJ** est présenté par M. Ferrari, C. Fiorentini et G. Fiorino dans [2]. Il présente des propriétés très intéressantes pour l'application à la recherche de preuve. **LSJℓ** est fondamentalement le même calcul, avec une représentation des séquents un peu plus riche en informations. Il a été proposé par mon maître de stage D. Larchey-Wendling. **LSJℓ** hérite de toutes les bonnes propriétés de **LSJ**, en ajoutant la localité des règles.

3.1 Séquents et règles de **LSJ**

Définition 4. Un séquent de **LSJ** est la donnée de trois multiensembles Θ , Γ et Δ de formules ; on écrit $\Theta ; \Gamma \Rightarrow \Delta$.

On a vu que dans les calculs **LK** et **LJ**, le séquent $\Gamma \Rightarrow \Delta$ représente la formule $(\bigwedge_{G \in \Gamma} G) \rightarrow (\bigvee_{D \in \Delta} D)$, respectivement en logique classique et en logique intuitionniste, avec Δ contenant exactement une formule pour **LJ**. C'est une interprétation courante en calcul de séquents. Pour **LSJ**, on ne sait pas représenter un séquent $\Theta ; \Gamma \Rightarrow \Delta$ par une seule formule. On a cependant le résultat suivant : un séquent $\emptyset ; \Gamma \Rightarrow \Delta$ est prouvable dans **LSJ** si et seulement si la formule $(\bigwedge_{G \in \Gamma} G) \rightarrow (\bigvee_{D \in \Delta} D)$ est prouvable en logique intuitionniste. Γ et Δ ont donc une signification ordinaire. En revanche, Θ est propre à **LSJ**, et difficile à interpréter. On peut dire que Θ contient des formules gardées en réserve, non accessibles directement (une formule de Θ ne peut pas être *formule principale*), mais qui peuvent être transférées dans Γ et ainsi devenir accessibles. On verra que les seules règles qui agissent sur Θ sont celles qui concernent le connecteur \rightarrow . L'article [2] propose bien une interprétation du séquent $\Theta ; \Gamma \Rightarrow \Delta$ pour Θ quelconque, en utilisant des modèles de Kripke. Nous ne la détaillons pas, car ce qui nous intéresse surtout est la propriété suivante qui découle du résultat énoncé sur un séquent avec Θ vide.

Proposition 5. *Soit A une formule, elle est valide en logique intuitionniste si et seulement si le séquent $\emptyset; \emptyset \Rightarrow A$ est prouvable dans **LSJ**.*

Les **règles** du calcul **LSJ** sont données dans la figure 3. Toutes les règles sont des *axiomes* ou des *règles logiques*. Il n’y a pas de *règle structurelle* ni de règle de *coupure*.

$$\begin{array}{c}
\frac{}{\Theta; \perp, \Gamma \Rightarrow \Delta} \perp L \qquad \frac{}{i : A, \Gamma \Rightarrow_n n : A, \Delta} \text{Id}' \\
\frac{\Theta; A, B, \Gamma \Rightarrow \Delta}{\Theta; A \wedge B, \Gamma \Rightarrow \Delta} \wedge L \qquad \frac{\Theta; \Gamma \Rightarrow A, \Delta \quad \Theta; \Gamma \Rightarrow B, \Delta}{\Theta; \Gamma \Rightarrow A \wedge B, \Delta} \wedge R \\
\frac{\Theta; A, \Gamma \Rightarrow \Delta \quad \Theta; B, \Gamma \Rightarrow \Delta}{\Theta; A \vee B, \Gamma \Rightarrow \Delta} \vee L \qquad \frac{\Theta; \Gamma \Rightarrow A, B, \Delta}{\Theta; \Gamma \Rightarrow A \vee B, \Delta} \vee R \\
\frac{\Theta; B, \Gamma \Rightarrow \Delta \quad B, \Theta; \Gamma \Rightarrow A, \Delta \quad B; \Theta, \Gamma \Rightarrow A}{\Theta; A \rightarrow B, \Gamma \Rightarrow \Delta} \rightarrow L \\
\frac{\Theta; A, \Gamma \Rightarrow B, \Delta \quad \emptyset; A, \Theta, \Gamma \Rightarrow B}{\Theta; \Gamma \Rightarrow A \rightarrow B, \Delta} \rightarrow R
\end{array}$$

FIGURE 3 – Les règles du calcul **LSJ**

Propriétés de LSJ. (Pour les démonstrations, voir [2].) Le calcul **LSJ** est sans contraction et vérifie la propriété de la sous-formule. L’algorithme décrit dans la deuxième partie termine pour **LSJ**. Les règles $\wedge L$, $\wedge R$, $\vee L$ et $\vee R$ sont inversibles; les deux premières prémisses de $\rightarrow L$ et la première prémisses de $\rightarrow R$ sont inversibles; la troisième prémisses de $\rightarrow L$ et la deuxième prémisses de $\rightarrow R$ ne sont pas inversibles.

Non localité de certaines règles. Les règles $\rightarrow L$ et $\rightarrow R$ ne sont pas locales : pour chacune, les formules représentées par Δ dans la conclusion n’apparaissent nulle part dans la dernière prémisses, il n’est donc pas possible de retrouver la conclusion en connaissant uniquement cette prémisses, la formule principale et le numéro de la prémisses, puisqu’il n’y a aucun moyen d’en déduire ce qui se trouve dans Δ . C’est pour cette raison qu’on introduit le calcul **LSJl**, dans lequel toutes les règles sont locales.

3.2 Séquents et règles de LSJl

Le calcul **LSJl** est très proche du calcul **LSJ** : chaque règle de **LSJl** est l’adaptation directe d’une règle de **LSJ** à une autre structure des séquents. Contrairement à **LSJ**, les règles de **LSJl** sont toutes locales. Pour cela, les séquents de **LSJl** représentent chacun un séquent de **LSJ**, avec un peu plus d’informations : celles qui sont parfois nécessaires pour retrouver la conclusion à partir d’une prémisses. Cette représentation est exhaustive et correcte. On définit en effet une surjection Φ de l’ensemble des séquents de **LSJl** dans l’ensemble des séquents de **LSJ**, et on montre dans la sous-section suivante qu’un séquent de **LSJl** est prouvable dans **LSJl** si, et seulement si, son image par Φ est prouvable dans **LSJ**.

Définition 6. *Un séquent de LSJl est la donnée de deux multiensembles Γ et Δ de couples “entier : formule”, et d’un entier naturel n , tels que tous les entiers présents dans Γ sont $\leq n + 1$ et tous ceux présents dans Δ sont $\leq n$; on écrit $\Gamma \Rightarrow_n \Delta$.*

Lien avec les séquents de LSJ : l’application Φ . Soit M un multiensemble de couples “entier : formule”, l’entier d’un couple étant appelé son indice. On note M_k le multiensemble obtenu à partir de M en ne gardant que les couples d’indice k , et $M_{\leq k}$ celui obtenu en ne gardant que les couples d’indice inférieur à k . On note $\text{forget}(M)$ le multiensemble de formules obtenu en oubliant l’indice et ne gardant que la formule de chaque couple de M . On définit l’application Φ de l’ensemble des séquents de **LSJl** dans l’ensemble des séquents de **LSJ**,

qui à $\Gamma' \Rightarrow_n \Delta'$ associe $\Theta; \Gamma \Rightarrow \Delta$ où : $\begin{cases} \Theta = \text{forget}(\Gamma'_{n+1}) \\ \Gamma = \text{forget}(\Gamma'_{\leq n}) \\ \Delta = \text{forget}(\Delta'_n) \end{cases}$. C'est une **surjection** : en

effet tout séquent $\Theta; \Gamma \Rightarrow \Delta$ de **LSJ** a au moins pour antécédent le séquent $\Gamma' \Rightarrow_0 \Delta'$, avec $\Gamma' = 0 : \Gamma \cup 1 : \Theta$ et $\Delta' = 0 : \Delta$, où par exemple $0 : \Gamma$ est le multiensemble de couples obtenu à partir de Γ en remplaçant chaque occurrence d'une formule A par une occurrence du couple $0 : A$.

Les **règles** du calcul **LSJℓ** sont données dans la figure 4. Chacune correspond à une règle de **LSJ**.

LSJℓ présente les mêmes propriétés que **LSJ**, auxquelles s'ajoute la localité de toutes les règles.

$$\begin{array}{c}
n \text{ et parfois } i \text{ désignent toujours des entiers naturels, avec } i \leq n \\
\\
\frac{}{i : \perp, \Gamma \Rightarrow_n \Delta} \perp L' \qquad \frac{}{i : A, \Gamma \Rightarrow_n n : A, \Delta} \text{Id}' \\
\\
\frac{i : A, i : B, \Gamma \Rightarrow_n \Delta}{i : A \wedge B, \Gamma \Rightarrow_n \Delta} \wedge L' \qquad \frac{\Gamma \Rightarrow_n n : A, \Delta \quad \Gamma \Rightarrow_n n : B, \Delta}{\Gamma \Rightarrow_n n : A \wedge B, \Delta} \wedge R' \\
\\
\frac{i : A, \Gamma \Rightarrow_n \Delta \quad i : B, \Gamma \Rightarrow_n \Delta}{i : A \vee B, \Gamma \Rightarrow_n \Delta} \vee L' \qquad \frac{\Gamma \Rightarrow_n n : A, n : B, \Delta}{\Gamma \Rightarrow_n n : A \vee B, \Delta} \vee R' \\
\\
\frac{i : B, \Gamma \Rightarrow_n \Delta \quad n+1 : B, \Gamma \Rightarrow_n n : A, \Delta \quad n+2 : B, \Gamma \Rightarrow_{n+1} n+1 : A, \Delta}{i : A \rightarrow B, \Gamma \Rightarrow_n \Delta} \rightarrow L' \\
\\
\frac{0 : A, \Gamma \Rightarrow_n n : B, \Delta \quad 0 : A, \Gamma \Rightarrow_{n+1} n+1 : B, \Delta}{\Gamma \Rightarrow_n n : A \rightarrow B, \Delta} \rightarrow R'
\end{array}$$

FIGURE 4 – Les règles du calcul **LSJℓ**

3.3 Équivalence entre **LSJℓ** et **LSJ**

On note \mathfrak{S} l'ensemble des séquents de **LSJ**, et \mathfrak{S}' l'ensemble des séquents de **LSJℓ**. Soit $\sigma \in \mathfrak{S}$, on note $\vdash \sigma$ si σ est prouvable dans **LSJ**; soit $\sigma' \in \mathfrak{S}'$, on note $\vdash' \sigma'$ si σ' est prouvable dans **LSJℓ**. Montrons que pour tous $\sigma \in \mathfrak{S}$ et $\sigma' \in \mathfrak{S}'$ tels que $\sigma = \Phi(\sigma')$, on a $\vdash \sigma$ si et seulement si $\vdash' \sigma'$, où Φ est la surjection de \mathfrak{S}' sur \mathfrak{S} définie précédemment.

Soit \mathcal{R} une règle de **LSJ**. On note \mathcal{R}' la règle de **LSJℓ** qui lui correspond. On écrit $\frac{\sigma_1 \quad \dots \quad \sigma_p}{\sigma}(\mathcal{R})$ et $\frac{\sigma'_1 \quad \dots \quad \sigma'_p}{\sigma'}(\mathcal{R}')$ des instances de ces règles.

Lemme 7. Soit $\sigma \in \mathfrak{S}$ et $\sigma' \in \mathfrak{S}'$ tels que $\sigma = \Phi(\sigma')$ et soit \mathcal{R} une règle de **LSJ**.

1) Si $\frac{\sigma_1 \quad \dots \quad \sigma_p}{\sigma}(\mathcal{R})$ alors il existe $\sigma'_1, \dots, \sigma'_p$ tels que pour tout k , $\sigma_k = \Phi(\sigma'_k)$, et $\frac{\sigma'_1 \quad \dots \quad \sigma'_p}{\sigma'}(\mathcal{R}')$.

2) Si $\frac{\sigma'_1 \quad \dots \quad \sigma'_p}{\sigma'}(\mathcal{R}')$, posons pour tout k , $\sigma_k = \Phi(\sigma'_k)$, alors $\frac{\sigma_1 \quad \dots \quad \sigma_p}{\sigma}(\mathcal{R})$.
Pour un axiome \bar{A} , cela signifie simplement : $\frac{}{\sigma}(\bar{A})$ si et seulement si $\frac{}{\sigma'}(\bar{A}')$.

Démonstration. On le montre pour chaque règle; c'est une conséquence assez directe de la définition de Φ . Faisons-le par exemple pour **Id** et $\rightarrow L$. À chaque fois, on se donne $\sigma = \Theta; \Gamma \Rightarrow \Delta$ et $\sigma' = \Gamma' \Rightarrow_n \Delta' \in \mathfrak{S}'$ tels que $\sigma = \Phi(\sigma')$.

Id : On a $\frac{}{\sigma}(\text{Id})$ si et seulement s'il existe une formule A appartenant à la fois à Γ et Δ , ce qui équivaut, par définition de Φ , à : il existe A et $i \leq n$ tels que $n : A \in \Delta'$ et $i : A \in \Gamma'$, c'est-à-dire $\frac{}{\sigma'}(\text{Id}')$.

$\rightarrow L :$ 1) Si $\frac{\sigma_1 \quad \sigma'_2 \quad \sigma_3}{\sigma}(\rightarrow L)$ alors il existe A, B et $\tilde{\Gamma}$ tels que $\Gamma = A \rightarrow B, \tilde{\Gamma}$ et $\sigma_1 = \Theta; B, \tilde{\Gamma} \Rightarrow \Delta$ et $\sigma_2 = B, \Theta; \tilde{\Gamma} \Rightarrow A, \Delta$ et $\sigma_3 = B; \Theta, \tilde{\Gamma} \Rightarrow A$; et il existe $i \leq n$

tel que $i : A \rightarrow B \in \Gamma'$. On pose $\tilde{\Gamma}' = \Gamma' - i : A \rightarrow B$ (on retire une seule occurrence de $i : A \rightarrow B$ de Γ') et $\sigma'_1 = i : B, \tilde{\Gamma}' \Rightarrow_n \Delta'$ et $\sigma'_2 = n + 1 : B, \tilde{\Gamma}' \Rightarrow_n n : A, \Delta'$ et $\sigma'_3 = n + 2 : B, \tilde{\Gamma}' \Rightarrow_{n+1} n + 1 : A, \Delta'$ et on vérifie qu'on a bien $\sigma_1 = \Phi(\sigma'_1)$ et $\sigma_2 = \Phi(\sigma'_2)$ et $\sigma_3 = \Phi(\sigma'_3)$ (en remarquant que $\tilde{\Gamma} = \text{forget}(\tilde{\Gamma}'_{\leq n})$), et aussi $\frac{\sigma'_1 \ \sigma'_2 \ \sigma'_3}{\sigma'} (\rightarrow L')$.

2) Si $\frac{\sigma'_1 \ \sigma'_2 \ \sigma'_3}{\sigma'} (\rightarrow L')$ alors il existe i, A, B et $\tilde{\Gamma}'$ tels que $\Gamma' = i : A \rightarrow B, \tilde{\Gamma}'$ et σ'_1, σ'_2 et σ'_3 ont la forme donnée ci-dessus; on pose $\tilde{\Gamma} = \Gamma - A \rightarrow B$ (on retire une seule occurrence de $A \rightarrow B$ de Γ), alors les images σ_1, σ_2 et σ_3 par Φ de σ'_1, σ'_2 et σ'_3 respectivement s'écrivent comme ci-dessus et donc $\frac{\sigma_1 \ \sigma_2 \ \sigma_3}{\sigma} (\rightarrow L)$. \square

Théorème 8. Soit $\sigma \in \mathfrak{S}$ et $\sigma' \in \mathfrak{S}'$ tels que $\sigma = \Phi(\sigma')$, alors $\vdash \sigma$ si et seulement si $\vdash' \sigma'$.

Démonstration. Par récurrence sur la *taille* de $\sigma \in \mathfrak{S}$, c'est-à-dire la somme des tailles des formules des trois multienssembles apparaissant dans σ .

On initialise pour tout $\sigma = \Theta; \Gamma \Rightarrow \Delta$ tel que toutes les formules dans Γ et dans Δ sont atomiques : soit $\sigma' = \Gamma' \Rightarrow_n \Delta' \in \mathfrak{S}'$ tel que $\sigma = \Phi(\sigma')$. Alors toutes les formules associées à un $i \leq n$ dans Γ' et toutes les formules associées à n dans Δ' sont aussi atomiques. En étudiant la forme des conclusions des règles non axiomatiques de **LSJ** comme de **LSJℓ**, on remarque que si σ (resp. σ') est la conclusion d'une règle de **LSJ** (resp. **LSJℓ**), alors la règle est un axiome. L'initialisation est donc un cas particulier de ce qui suit avec $p = 0$ (ce qui entraîne qu'on n'utilise en fait pas l'hypothèse de récurrence).

Soit $\sigma = \Theta; \Gamma \Rightarrow \Delta \in \mathfrak{S}$. Soit $\sigma' = \Gamma' \Rightarrow_n \Delta' \in \mathfrak{S}'$ tel que $\sigma = \Phi(\sigma')$.

On suppose $\vdash \sigma$. Alors il existe une règle \mathcal{R} de **LSJ** et $\sigma_1, \dots, \sigma_p \in \mathfrak{S}$ (avec éventuellement p nul) tels que $\vdash \sigma_k$ pour tout k et $\frac{\sigma_1 \ \dots \ \sigma_p}{\sigma} (\mathcal{R})$. D'après le lemme, il existe $\sigma'_1, \dots, \sigma'_p \in \mathfrak{S}'$ tels que $\sigma_k = \Phi(\sigma'_k)$ pour tout k et $\frac{\sigma'_1 \ \dots \ \sigma'_p}{\sigma'} (\mathcal{R}')$. Pour tout k , on applique l'hypothèse de récurrence à σ_k qui a une *taille* strictement inférieure à celle de σ , et on obtient $\vdash' \sigma'_k$. On en déduit $\vdash' \sigma'$.

On suppose $\vdash' \sigma'$. Alors il existe une règle \mathcal{R}' de **LSJℓ** et $\sigma'_1, \dots, \sigma'_p \in \mathfrak{S}'$ tels que $\vdash' \sigma'_k$ pour tout k et $\frac{\sigma'_1 \ \dots \ \sigma'_p}{\sigma'} (\mathcal{R}')$. On pose $\sigma_k = \Phi(\sigma'_k)$ pour tout k . D'après le lemme on a $\frac{\sigma_1 \ \dots \ \sigma_p}{\sigma} (\mathcal{R})$, en particulier on peut appliquer l'hypothèse de récurrence aux σ_k donc $\vdash \sigma_k$ pour tout k , d'où $\vdash \sigma$. \square

4 Implémentation

4.1 Indexation

4.2 Structure de données pour le séquent

5 Perspective de certification

5.1 Un langage simple pour faciliter la certification

5.2 Compilation d'un programme spécifique à une formule donnée

5.3 Comparaison de différentes implémentations

Références

- [1] R. Dyckhoff, “Contraction-free sequent calculi for intuitionistic logic,” *J. Symb. Log.*, vol. 57, no. 3, pp. 795–807, 1992.
- [2] M. Ferrari, C. Fiorentini, and G. Fiorino, “Contraction-Free Linear Depth Sequent Calculi for Intuitionistic Propositional Logic with the Subformula Property and Minimal Depth Counter-Models,” *Journal of Automated Reasoning*, vol. 51, no. 2, pp. 129–149, 2013.

Efficacité de LSJ

L'étude qui suit porte sur le calcul **LSJ**. En effet, **LSJℓ** hérite de toutes les propriétés intéressantes de **LSJ**, en apportant une localité des règles qui facilite une implémentation économe en mémoire.

5.4 Propriété de la sous-formule et indexation

B est une **sous-formule** de A si $B = A$ ou si A est de la forme A_1 'connecteur' A_2 et (B est une sous-formule de A_1 ou B est une sous-formules de A_2). Un calcul de séquents vérifie la **propriété de la sous-formule** si tout séquent prouvable σ admet une preuve telle que toute formule apparaissant dans (un séquent de) la preuve est une sous-formule d'une formule de σ . En particulier, le séquent $\Rightarrow A$ a une preuve dans laquelle toute formule est une sous-formule de A .

Le calcul **LSJ** vérifie la propriété de la sous-formule : on le constate aisément en observant chaque règle.

La propriété de la sous-formule est très recherchée en calcul des séquents. D'une part, elle donne une borne sur les formules qu'il faudra manipuler au cours d'une recherche de preuve, qui sont évidemment toutes plus petites que la formule qu'on essaie de prouver. Mais surtout, elle permet de connaître à l'avance la liste exhaustive des formules qu'on pourra rencontrer. On peut donc à l'avance les numéroter : ainsi, les formules d'un séquents sont simplement représentées par un entier. Il faut quelques informations sur ces numéros : par exemple pour une formule $A \wedge B$, il faut savoir qu'il s'agit d'un "et", et pouvoir déterminer A et B . Il faut aussi pouvoir reconnaître quand l'axiome Id (une même formule apparaît des deux côtés du séquent) s'applique : pour cela on associe à chaque formule une classe, qui correspond à une classe d'équivalence de la relation d'égalité structurelle. La taille de toutes ces informations réunies est linéaire en la taille de la formule de départ (c'est-à-dire le nombre de nœuds de l'arbre qui la représente, qui est aussi le nombre de sous-formules avec multiplicité). Un exemple est donné par la figure 5.

La propriété de la sous-formule est encore plus intéressante dans le cadre de la recherche de preuve compilée : connaître à l'avance les formules qui apparaîtront permet d'écrire pour chacune des fonctions agissant sur le séquent, au lieu de les calculer au cours de la recherche de preuve (voir ??).

```
((a & b) & (non (c) | (a & b)))
```

sf	classe	description
1	1	Var a
2	2	Var b
3	3	1 & 2
4	4	Var c
5	0	Faux
6	5	4 \rightarrow 5
7	1	Var a
8	2	Var b
9	3	7 & 8
10	6	6 9
11	7	3 & 10

FIGURE 5 – Indexation de la formule $(a \wedge b) \wedge (\neg c \vee (a \wedge b))$

6 Implémentation

6.1 Indexation

cf “Propriété de la sous-formule et indexation” + explication sur les classes (et priorités) et les champs axiomes du séquent

6.2 Structure de données pour le séquent

Comme toutes les règles de **LSJℓ** sont locales, on peut n’avoir à tout moment qu’un seul séquent en mémoire. Un séquent de **LSJℓ** consiste en deux multiensembles Γ et Δ de couples “*indice : formule*” et un *indice* du séquent n . Les indices sont des entiers, et grâce à l’indexation, les formules sont aussi des entiers. La question qui se pose est le choix de structure de données pour Γ et Δ .

Considérons une des règles les plus simples : $\frac{i : A, i : B, \Gamma \Rightarrow_n \Delta}{i : A \wedge B, \Gamma \Rightarrow_n \Delta} \wedge L'$. Au cours de l’algorithme de recherche de preuve, on peut être amené à vouloir transformer notre séquent courant, alors égal à la conclusion, en la prémisse. On veut pour cela retirer $i : A \wedge B$ de Γ et y ajouter $i : A$ et $i : B$. On peut aussi avoir besoin de faire la transformations inverse, c’est-à-dire retirer les deux derniers couples et rajouter le premier. Un des objectifs est donc que ces opérations soient rapides.

On définit la complexité d’une étape comme la somme des complexités dans le pire cas de l’ajout d’un couple, du retrait d’un couple, et du choix d’un couple principal. De simples listes entraînent bien sûr une complexité de l’ordre du cardinal des multiensembles. On peut obtenir un choix de couple principal en temps constant avec des listes triées, et

Au cours de l’algorithme, on manipule un “séquent”, censé représenter un séquent du calcul **LSJℓ**, contenant les informations suivantes :

- des informations de taille constante : l’indice n du séquent, et des booléens *id* et *fauxL*, indiquant si les axiomes de même nom sont applicables au séquent ;
- les couples *indice : formule* contenus dans les champs Γ et Δ du séquent.

Comme nous l’avons expliqué en introduisant le calcul **LSJℓ**, le but de celui-ci est de pouvoir effectuer la recherche de preuve en ne gardant à chaque instant qu’un seul séquent en mémoire.

Intéressons-nous maintenant à la complexité temporelle.

Celle-ci dépend du nombre de règles qu’on essaie d’appliquer, c’est-à-dire le nombre d’appels récursifs à la fonction *prouvable* (?) dont le pseudo-code est donné en figure? page?. Ce nombre dépend de la taille de la formule et des connecteurs présents dedans (et selon l’ordre dans lequel on choisit les formules principales cela peut beaucoup varier pour une même formule, mais on s’intéresse à la complexité dans le pire cas). Mais il ne dépend pas de notre choix d’implémentation (sauf pour l’ordre des “implique”, mais encore une fois pas si on regarde le pire cas).

Références

- [1] R. Dyckhoff, “Contraction-free sequent calculi for intuitionistic logic,” *J. Symb. Log.*, vol. 57, no. 3, pp. 795–807, 1992.

- [2] M. Ferrari, C. Fiorentini, and G. Fiorino, “Contraction-Free Linear Depth Sequent Calculi for Intuitionistic Propositional Logic with the Subformula Property and Minimal Depth Counter-Models,” *Journal of Automated Reasoning*, vol. 51, no. 2, pp. 129–149, 2013.