INF551 :ÉCRITURE D'UNE PREUVE DANS LE CALCUL DES SÉQUENTS DE DIKHOFF

GETTE, G. AND LAURENS, J.

Abstract. Ce rapport synthétise les rsultats de notre travail de première période visant modifier la mthode de preuve d'un SAT-solver intuitionniste dtaill dans **??**. Il s'agit de faire en sorte de transformer l'algorithme pour produire une preuve d'une formule intuitionniste crite dans le calcul des squents de Dikhoff tel que présenté dans **??**. Le prsent rapport détaille dans une première partie le contenu des deux articles sus-cités avant de présenter les mcanismes de notre algorithme modifié et les détails de l'implémentation en OCaml.

Contents

1. Ĺogique intuitionniste et méthode de résolution

1.1. Détail d'un SAT-solver en logique intuitionniste. Syntaxiquement, une formule intuitionniste est definie rcursivement, comme il suit :

On remarque que cette définition diffère de la logique classique par l'absence de symbole de négation. Cette absence est lié à l'absence de l'axiome du tiers exclu, à savoir : $A \vee \neg A = T$

1.2. Calcul des squents intuitionniste. Une construction importante en logique et en théorie de la preuve est le calcul des séquents qui permet l'écriture et la construction formelle de preuve. L'idée principale est de manier un certain nombre de règles en jouant sur la formes des formules considérées, pour récrire ce que l'on veut démontrer et remonter ainsi successivement à des formes de plus en plus simple et par suite de plus en plus facile à manipuler. Il est naturel de vouloir étendre ce système à la logique intuitionniste. Un séquent intuitionniste s'écrit sous la forme :

$$A_1, A_2, A_3, ..., A_n \vdash B$$

et doit se comprendre comme la formule : $(A_1 \rightarrow (A_2 \rightarrow ... \rightarrow (A_n \rightarrow B)))$. Pour mémoire, l'èquivalent en logique classique, se lit différemment savoir que $A_1, A_2, ..., A_n \vdash B_1, ..., B_m$ se comprend comme $(A_1 \wedge A_2 ... \wedge A_n) \rightarrow (B_1 \vee ... \vee B_m)$.

Les règles du calcul de Dikhoff sont les suivantes :

$$\text{Axiom} \; \frac{}{\Gamma, A \vdash A}$$

$$\wedge \text{ Left} \; \frac{A, B, \Gamma \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}$$

$$\vee \text{ Left} \; \frac{A, \Gamma \vdash \Delta \qquad B, \Gamma \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}$$

$$\wedge \text{ Right} \; \frac{A, \Gamma \vdash A \qquad B, \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

$$\rightarrow \text{Right} \; \frac{\Gamma, A \vdash B}{\Gamma \vdash (A \rightarrow B)}$$

$$\rightarrow \text{LeftAtom} \; \frac{B, a, \Gamma \vdash \Delta}{a \rightarrow B, a, \Gamma \vdash \Delta}$$

$$\rightarrow \text{LeftAnd} \; \frac{C \rightarrow (A \rightarrow B), \Gamma \vdash \Delta}{(C \wedge A) \rightarrow B \vdash \Delta}$$

$$\rightarrow \text{LeftOr} \; \frac{(C \rightarrow A), (C \rightarrow B), \Gamma \vdash \Delta}{(C \wedge A) \rightarrow B \vdash \Delta}$$

$$\rightarrow \text{LeftImplies} \; \frac{C \rightarrow A, \Gamma \vdash C \rightarrow A \qquad B, \Gamma \vdash \Delta}{(C \wedge A) \rightarrow B \vdash \Delta}$$

Pour démontrer une formule automatiquement en utilisant ces règles, il suffit de les appliquer "de bas en haut", et d'essayer de remonter à une forme simple et facilement vérifiable, comme un sequent ne comprenant qu'un ensemble d'atomes. On s'assure de la terminaison d'un tel algorithme utilisant ces règles, en utilisant un poids w et en montrant qu'il s'agit d'une fonction décroissante "en remontant" dans un arbre de preuve; c'est-à-dire que le poids de l'ensemble des formules au dessus de la barre de déduction est strictement infrieur celui placé au dessous de la barre. La fonction w est définie récursivement comme il suit :

$w(a) = 1$ quand a est un atome
$w(A \wedge B) = w(A) + w(B) + 2$
$w(A \rightarrow B) = w(A \vee B) = w(A) + w(B) + 1$
$w(A \vee B) = w(A) + w(B) + 1$

On peut constater que ces règles sont très similaire à celle utilisèe dans le calcul des séquents classique, avec une subtilitè suplémentaire apportée par Dykhoff, la règle "$\rightarrow$ Left" est décomposée en 4 nouvelles règlesselon la forme de la formule servant de prémisse l'implication laquelle la règles est appliquée. Cette modification de Dykhoff permet d'éviter la création de copies de formules, et ainsi d'assurer la terminaison (grâce à l'argument du poids décroissant.)

Le but de ce projet est de comprendre les liens qui unissent l'article **??** et le calcul d'une preuve dans ce calcul. Pour ce faire nous modifions l'algorithme original et tentons de formaliser les différentes etapes du calcul pour les récrire dans les règles explicitées ci-dessus. Ce calcul permet trois choses :

- Fournir une méthode efficace de preuve en logique intuitionniste, car l'algorithme décrit dans **??** est de loin l'un des plus efficace de l'état de lárt
- Comprendre ce qui fait précisément l'efficacité de cette algorithme en le formalisant

EME RAISON

2. Construction d'une preuve en logique intuitionniste

2.1. Modification de l'algorithme.

2.2. Récriture d'une preuve classique en intuitionniste.

3. Implémentation et résultat

3.1. Structure du projet.

3.2. Résultats.