École polytechnique — X2010 — INF423 Fondements de l'informatique

Systèmes de preuves : logique intuitionniste propositionnelle

Sujet proposé par David Monniaux

En *logique classique*, on a l'axiome du tiers-exclu : quelle que soit la proposition X, on a $X \vee \neg X$. Ceci correspond à la notion usuelle de vérité logique, mais pose toutefois certains problèmes. Par exemple, il est possible de définir en logique classique la fonction qui à un code source de programme x associe 1 s'il termine ou 0 s'il ne termine pas : il suffit d'utiliser le fait que pour tout x, $\mathit{termine}(x) \vee \neg \mathit{termine}(x)$. Or, nous verrons dans un cours prochain que cette fonction n'est pas *calculable* (nous donnerons alors une définition précise de ce que ce mot veut dire). On peut préférer des logiques où toutes les fonctions que l'on peut définir sont calculables. Le problème du tiers exclu est qu'il nous « parachute » le fait que $\mathit{termine}(x) \vee \neg \mathit{termine}(x)$ est vrai sans nous dire si c'est $\mathit{termine}(x)$ ou $\neg \mathit{termine}(x)$ qui l'est : nous allons donc supprimer le tiers-exclu. Nous obtiendrons ainsi une *logique intuitionniste*.

Les modèles en logique propositionnelle classique sont simples : il suffit d'associer à chaque variable libre un booléen $\{0, 1\}$. Les modèles intuitionnistes sont plus complexes [2] et nous n'en parlerons donc pas. Nous ne nous intéresserons donc qu'à l'aspect *syntaxique* des preuves : application du système de règles. Notamment, nous n'aurons pas recours à l'approche « calculer tous les cas dans la table de vérité ».

Bien qu'il soit naturel pour un mathématicien de raisonner en logique classique, un très grand nombre de théorèmes classiques peuvent être prouvés en logique intuitionniste (si un théorème est prouvable en logique intuitionniste, alors il l'est en logique classique). Cette direction a été explorée par l'école mathématique de l'*intuitionnisme* et des *mathématiques constructives*, menée par Brouwer (1881–1966) et Heyting (1898–1980). L'outil Coq [1] est basé sur une logique intuitionniste.

Les formules de la logique intuitionniste sont de la forme A (atome), $\neg F$, $F_1 \Rightarrow F_2$, $F_1 \wedge F_2$, $F_1 \vee F_2$ où F, F_1, F_2 sont des formules. Attention, $F_1 \Rightarrow F_2$, en logique intuitionniste, n'est plus considéré comme une notation pour $\neg F_1 \vee F_2$, de même que $\neg\neg F$ n'est plus équivalent à F. [2]

Les règles de déduction travaillent sur des *séquents*. Certaines présentations de la déduction en logique classiques donnent des règles de déduction sur des séquents de la forme $\Gamma \vdash \Delta$, où Γ et Δ sont deux ensembles de formules. Un tel séquent a le sens de « de la conjonction des formules de Γ on peut déduire la disjonction des formules de Δ ». Dans le cas de la logique intuitionniste, on restreint Δ à une seule formule au plus. Un séquent intuitionniste est donc de la forme $\Gamma \vdash \Delta$ où Δ est une unique formule (*conclusion*) ou rien du tout et Γ est un ensemble de formules (hypothèses). $\Gamma \vdash \Delta$ veut donc dire, en termes intuitifs, « de la conjonction des formules de Γ on peut déduire Δ », et $\Gamma \vdash$ veut dire « de Γ on peut déduire n'importe quoi », autrement dit « Γ est contradictoire ».

1. Développé à l'INRIA, à l'École polytechnique et à l'Université Paris-Sud, et antérieurement au CNRS et à l'École normale supérieure de Lyon. `http://coq.inria.fr/`

2. Dans certaines présentations, on introduit $\neg F$ comme une notation pour $F \Rightarrow \bot$ où $\bot$ dénote l'absurde, et on a un schéma d'axiomes disant que de l'absurde on peut déduire n'importe quoi :

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash F}$$

On travaillera sur des arbres de preuve formés par application de règles

$$\frac{\Gamma_1 \vdash \Delta_1 \quad \dots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta} \tag{1}$$

Une telle règle veut dire que si l'on a réussit à déduire les séquents $\Gamma_1 \vdash \Delta_1, \dots, \Gamma_n \vdash \Delta_n$ (bref, qu'on les obtient à la racine d'arbres de preuves bien formés), alors on peut déduire $\Gamma \vdash \Delta$.

Le calcul des séquents LJ comprend les règles [3] :

– Identités

$$\frac{}{A \vdash A}\ \text{Ax} \qquad \frac{\Gamma_1 \vdash A \quad \Gamma_2, A \vdash \Delta}{\Gamma_1, \Gamma_2 \vdash \Delta}\ \text{coupure}$$

– Affaiblissement

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ LW \qquad \frac{\Gamma \vdash}{\Gamma \vdash A}\ RW$$

– Contraction et échange

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ LC \qquad \frac{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}\ LEx$$

Par souci de lisibilité, nous omettrons souvent l'application de ces règles dans les preuves.

– Règles logiques

$$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash}\ L\neg \qquad \frac{\Gamma, A \vdash}{\Gamma \vdash \neg A}\ R\neg$$

$$\frac{\Gamma_1 \vdash A \quad \Gamma_2, B \vdash \Delta}{\Gamma_1, \Gamma_2, A \Rightarrow B \vdash \Delta}\ L\Rightarrow \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ R\Rightarrow$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ L\wedge 1 \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ L\wedge 2 \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ R\wedge$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ L\vee \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ R\vee 1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ R\vee 2$$

Vous remarquerez que, pour le moment, nous n'avons pas supposé que les symboles $\vee$ et $\wedge$ étaient associatifs ou commutatifs.

On se limite dans ce sujet à la logique intuitionniste *propositionnelle*. On pourrait rajouter des règles pour les quantificateurs $\forall$ et $\exists$, mais cela nous entraînerait dans le *calcul des prédicats* intuitionniste ou dans la *théorie des types*, trop loin pour traiter les choses dans le cadre d'une PC. Les plus curieux pourront rechercher ailleurs des informations sur le Système F [2], le Calcul des Constructions, etc. Nous n'en dirons rien, si ce n'est que dans un système de preuves constructives, donner une preuve de $\forall x \exists y\ F(x, y)$ revient à donner un algorithme de calcul de y tel que $F(x, y)$ en fonction de x, alors qu'en logique classique, cela ne fonctionne pas. Le lien entre les preuves intuitionnistes et le calcul est plus profond encore : on peut voir une preuve de $A \Rightarrow B$ comme un programme qui transforme une preuve de A en une preuve de B, donc de type $A \to B$. Ceci donne une théorie de la preuve mêlant calcul et déduction, via les isomorphismes de Curry-Howard. Là encore, pour plus de détails, reportez-vous à des ouvrages spécialisés.

Notez que la logique propositionnelle intuitionniste reste décidable, c'est-à-dire qu'il existe des algorithmes qui, étant donné Γ et Δ, disent s'il existe une dérivation de $\Gamma \vdash \Delta$ et, si oui, la fournissent. La tactique `tauto` de Coq implémente ainsi un algorithme dû à Dyckhoff [1] qui passe par des règles de déduction modifiées, mais équivalentes.

1 Exemples de preuves non intuitionnistes

Question 1.1. *Montrez, en arithmétique classique, qu'il existe un couple (a, b) de réels irrationnels tel que a^b est rationnel. Indice : considérez $\sqrt{2}^{\sqrt{2}}$ et utilisez le tiers-exclu.*

3. Je reprends ici une présentation d'Alexis Saurin, que je remercie donc.

La preuve «simple» en logique classique donne deux couples possibles, et on ne sait pas lequel est le bon. Ce genre de preuves n'est pas accepté en logique intuitionniste.

(En fait, sur cet exemple, on peut prouver que $\sqrt{2}^{\sqrt{2}}$ est transcendant, c'est-à-dire racine d'aucun polynôme à coefficients entiers, donc irrationnel, mais c'est une preuve beaucoup plus compliquée que la solution en deux lignes plus haut...)

Un autre exemple de preuve non intuitionniste est la preuve de l'existence de nombres transcendants pour raisons de cardinalité (un réel est dit transcendant s'il n'est pas algébrique, et algébrique s'il est racine d'un polynôme à coefficients entiers). Il y a une infinité dénombrable de réels algébriques, et une infinité non dénombrable de réels, donc une infinité non dénombrable de transcendants. Bref, il y en a «beaucoup» mais nous n'en avons pas exhibé un seul !

2 Quelques preuves

On peut démontrer, ce que nous ne ferons pas ici, que l'on peut se passer de la règle de coupure. À titre d'exercice, nous vous demanderons donc de ne pas introduire de coupures dans vos preuves.

Question 2.1. *Donnez une dérivation de* $A \Rightarrow (B \Rightarrow C) \vdash (A \wedge B \Rightarrow C)$.

Question 2.2. *Donnez une dérivation de* $A \wedge B \Rightarrow C \vdash A \Rightarrow (B \Rightarrow C)$.

Ainsi, en logique intuitionniste (et par conséquent en logique classique), $A \wedge B \Rightarrow C$ et $A \Rightarrow (B \Rightarrow C)$ sont équivalents.

3 Élimination de la règle d'affaiblissement

Là encore, nous vous demanderons donc de ne pas introduire de coupures dans vos preuves.
On propose une nouvelle règle

$$\frac{}{\Gamma, A \vdash A}\ AxW \tag{2}$$

Question 3.1. *Prouvez que l'on peut remplacer les règles Ax et LW par la règle AxW, c'est à dire que si le séquent* $\Gamma \vdash \Delta$ *admet une dérivation dans le système LJ original, il admet une dérivation dans le nouveau système (que l'on nommera LJ'), et réciproquement.*

4 Propriétés usuelles

Là encore, nous vous demanderons donc de ne pas introduire de coupures dans vos preuves.

Question 4.1. *Prouvez que s'il existe une dérivation de* $\Gamma \vdash A \vee B$, *alors il en existe une de* $\Gamma \vdash B \vee A$.

Question 4.2. *Prouvez que s'il existe une dérivation de* $\Gamma, A \vee B \vdash \Delta$, *alors il en existe une de* $\Gamma, B \vee A \vdash \Delta$.

Nous n'en donnerons pas une démonstration lourde, mais on voit bien que pour toute dérivation de preuve $\Gamma \vdash \Delta$, si on remplace $A \vee B$ par $B \vee A$ dans Γ et/ou Δ, on pourra réécrire la dérivation π pour l'adapter. On pourra donc supposer que le symbole $\vee$ est commutatif, et remplacer les règles $R \vee 1$ et $R \vee 2$ par une unique règle.

$$\vdots\ \pi$$

On pourrait faire de même pour $A \wedge B$. Plus généralement, on pourrait prouver que si l'on a des preuves de $\vdash A \Rightarrow B$ et $\vdash B \Rightarrow A$ (cf §2), et de $\Gamma \vdash \Delta$, alors on peut remplacer A par B dans Γ et Δ et reconstruire une preuve.

5 Rapport avec la logique classique

Question 5.1. *Donnez une dérivation de* $A \vdash \neg\neg A$.

Question 5.2. *Donnez une dérivation de* $\neg\neg\neg A \vdash \neg A$.

Un *schéma d'axiomes* est une représentation compacte d'un ensemble infini d'axiomes tous construits « sur le même modèle ». Ainsi, $\overline{\neg\neg X \vdash X}$ représente l'infinité (dénombrable) d'axiomes obtenus en remplaçant X par n'importe quelle proposition, par exemple, $\overline{\neg\neg(A \vee B) \vdash (A \vee B)}$.

Question 5.3. *On suppose un schéma d'axiomes* $\overline{\neg\neg X \vdash X}^{\ Peirce}$ *(axiome de Peirce). Donnez une dérivation de* $\vdash A \vee \neg A$.

Question 5.4. *On suppose un schéma d'axiomes* $\overline{\vdash X \vee \neg X}^{\ tiers\ exclu}$. *Donnez une dérivation de* $\neg\neg A \vdash A$. *Vous avez droit aux coupures.*

Résumé de la situation : en logique intuitionniste, A implique $\neg\neg A$, mais la direction opposée est équivalente à l'axiome du tiers exclu (logique classique). En revanche, $\neg\neg\neg A$ et $\neg A$ sont équivalents. Plus généralement, le théorème de Glivenko dit que si l'on peut prouver $\vdash A \Rightarrow B$ en logique classique, alors on peut prouver $\vdash (\neg\neg A) \Rightarrow (\neg\neg B)$ en logique intuitionniste ; cette approche se généralise en *traductions négatives* (Gödel – Gentzen etc.) [3].

Ceci nous donne une technique de preuve pratique en logique intuitionniste, très utilisée par exemple par Georges Gonthier (auteur avec Benjamin Werner d'une preuve en Coq du théorème de coloriage de graphes planaires en 4 couleurs) : quand on a une preuve classique d'un lemme $A \Rightarrow B$, on a facilement une preuve intuitionniste de $\neg\neg A \Rightarrow \neg\neg B$; bref on peut tout faire en rajoutant deux négations. Si le théorème final est $\forall x\ T(x)$, on se retrouve donc à avoir prouvé $\forall x\ \neg\neg T(x)$. Si de plus on peut prouver $\forall x\ T \vee \neg\neg T(x)$ (ce qui est le cas, grosso modo, si $T(x)$ se réfère à une propriété décidable par un algorithme), on peut conclure $\forall x\ T(x)$ en logique intuitionniste !

Références

[1] Roy Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *Journal of Symbolic Logic*, 57(3) :795–807, September 1992.

[2] Jean-Yves Girard. *Proofs and types*, volume 7 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1990. Traduit et avec annexes par Paul Taylor et Yves Lafont.

[3] Joan Moschovakis. Intuitionistic logic. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, summer 2010 edition, 2010.