Deduction Modulo: une introduction

Olivier HERMANT

9 Juillet 2007

Déduction et Calcul

- Le calcul est la base des mathématiques.

Déduction et Calcul

- Le calcul est la base des mathématiques.
- Il a été oublié par la formalisation.

Déduction et Calcul

- Le calcul est la base des mathématiques.
- Il a été oublié par la formalisation.
- retrouvé par les règles de réécriture.
- besoin d'un équilibre : la Déduction Modulo.

Systèmes de déduction : la logique

- logique du premier ordre: symboles de fonction, de prédicats et des connecteurs logiques: $\wedge, \vee, \Rightarrow, \neg$, ainsi que les quantificateurs $\forall, \exists$.

$$
\begin{gathered}
Pair(0) \\
\forall n (Pair(n) \Rightarrow Impair(n+1)) \\
\forall n (Impair(n) \Rightarrow Pair(n+1))
\end{gathered}
$$

Systèmes de déduction : la logique

- logique du premier ordre: symboles de fonction, de prédicats et des connecteurs logiques: $\wedge, \vee, \Rightarrow, \neg$, ainsi que les quantificateurs $\forall, \exists$.

$$\begin{array}{c} Pair(0) \\ \forall n (Pair(n) \Rightarrow Impair(n+1)) \\ \forall n (Impair(n) \Rightarrow Pair(n+1)) \end{array}$$

- un séquent :

$$\overbrace{\Gamma}^{\text{hyp.}} \vdash \overbrace{A}^{\text{conc.}}$$

- et des règles pour les dériver: le calcul des séquents (déduction naturelle)
- cadre ici présenté: logique intuitionniste (classique, linéaire, contraintes, ordre sup ...)

Système de Déduction : le calcul des séquents (LJ)

- Une règle de déduction:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

- règles à gauche/à droite

$$\frac{}{\Gamma, A \vdash A}\text{axiome} \qquad\qquad \frac{\Gamma, A \vdash B \quad \Gamma \vdash A}{\Gamma \vdash B}\text{coupure}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-d} \qquad\qquad \frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge\text{-g}$$

$$\frac{\Gamma, \forall x A[x], A[t] \vdash B}{\Gamma, \forall x A[x] \vdash B}\forall\text{-g, } t \text{ quelconque} \qquad\qquad \frac{\Gamma \vdash A[x]}{\Gamma \vdash \forall x A[x]}\forall\text{-d, } x \text{ libre}$$

Exemple: 1

$$\forall x P(x) \vdash P(0) \wedge P(1)$$

Exemple: 1

$$\frac{\forall x P(x) \vdash P(0) \qquad \forall x P(x) \vdash P(1)}{\forall x P(x) \vdash P(0) \wedge P(1)} \wedge\text{-d}$$

Exemple: 1

$$\dfrac{\forall\text{-g}\ \dfrac{\forall x P(x), P(0) \vdash P(0)}{\forall x P(x) \vdash P(0)} \qquad \dfrac{faxP(x), P(1) \vdash P(0)}{\forall x P(x) \vdash P(1)}\ \forall\text{-g}}{\forall x P(x) \vdash P(0) \wedge P(1)}\ \wedge\text{-d}$$

Exemple: 1

$$
\dfrac{
\forall\text{-g}\;\dfrac{\dfrac{}{\forall x P(x), P(0) \vdash P(0)}\;\text{axiome}}{\forall x P(x) \vdash P(0)}
\qquad
\dfrac{\dfrac{}{faxP(x), P(1) \vdash P(0)}\;\text{axiome}}{\forall x P(x) \vdash P(1)}\;\forall\text{-g}
}{\forall x P(x) \vdash P(0) \wedge P(1)}\;\wedge\text{-d}
$$

Exemple: 2

$$\forall x P(x) \vdash P(0) \land P(1)$$

Exemple: 2

$$\dfrac{\dfrac{\forall x P(x), P(1), P(0) \vdash P(0) \wedge P(1)}{\forall x P(x), P(0) \vdash P(0) \wedge P(1)}\ \forall\text{-g}}{\forall x P(x) \vdash P(0) \wedge P(1)}\ \forall\text{-g}$$

Exemple: 2

$$\cfrac{\cfrac{\cfrac{\text{axiome}\ \cfrac{}{\forall xP(x), P(1), P(0) \vdash P(0)} \qquad \cfrac{}{\forall xP(x), P(1), P(0) \vdash P(1)}\ \text{axiome}}{\forall xP(x), P(1), P(0) \vdash P(0) \land P(1)}\ \land\text{-d}}{\forall xP(x), P(0) \vdash P(0) \land P(1)}\ \forall\text{-g}}{\forall xP(x) \vdash P(0) \land P(1)}\ \forall\text{-g}$$

Exemple: 2

$$\dfrac{\dfrac{\dfrac{\text{axiome}\;\overline{\forall x P(x), P(1), P(0) \vdash P(0)} \qquad \overline{\forall x P(x), P(1), P(0) \vdash P(1)}\;\text{axiome}}{\forall x P(x), P(1), P(0) \vdash P(0) \wedge P(1)}\,\wedge\text{-d}}{\forall x P(x), P(0) \vdash P(0) \wedge P(1)}\,\forall\text{-g}}{\forall x P(x) \vdash P(0) \wedge P(1)}\,\forall\text{-g}$$

- la première règle n'est pas forcément anodine: liberté des variables.

Axiomes vs. réécriture

Axiomes	Réécriture
$x + S(y) = S(x + y)$ $x + 0 = x$ $x * 0 = 0$ $x * S(y) = x + x * y$ $(x * y = 0) \Leftrightarrow (x = 0 \vee y = 0)$	$x + S(y) \rightarrow S(x + y)$ $x + 0 \rightarrow x$ $x * 0 \rightarrow 0$ $x * S(y) \rightarrow x + x * y$ $(x * y = 0) \rightarrow (x = 0 \vee y = 0)$
$\dfrac{\dfrac{\vdots}{\mathcal{T} \vdash 2 * 2 = 4}}{\mathcal{T} \vdash \exists x (2 * x = 4)}$	$\dfrac{\dfrac{}{\vdash 4 = 4}}{\vdash \exists x (2 * x = 4)}$

Déduction modulo : les règles de réécriture

- Forme générale :

$$l \to r$$

Déduction modulo : les règles de réécriture

- Forme générale :

$$l \rightarrow r$$

- utilisation : Si $t = l_\sigma$ alors on le remplace par r_σ (+ unification)

Déduction modulo : les règles de réécriture

- Forme générale :

$$l \to r$$

- utilisation : Si $t = l_\sigma$ alors on le remplace par r_σ (+ unification)
- règles de réécriture sur des termes :

$$x + S(y) \to S(x + y)$$

Déduction modulo : les règles de réécriture

- Forme générale :

$$l \to r$$

- utilisation : Si $t = l_\sigma$ alors on le remplace par r_σ (+ unification)
- règles de réécriture sur des termes :

$$x + S(y) \to S(x + y)$$

- et sur des **propositions** :

$$x * y = 0 \to x = 0 \vee y = 0$$

- avantages : puissance, souplesse

Déduction modulo : les règles de réécriture

- Forme générale :
$$l \to r$$
- utilisation : Si $t = l_\sigma$ alors on le remplace par r_σ (+ unification)
- règles de réécriture sur des termes :
$$x + S(y) \to S(x + y)$$
- et sur des **propositions** :
$$x * y = 0 \to x = 0 \vee y = 0$$
- avantages : puissance, souplesse
- on obtient une congruence modulo $\mathcal{R}$ (ensemble de règles, choisi): $\equiv$

Déduction modulo : les règles de réécriture

- Forme générale :

$$l \to r$$

- utilisation : Si $t = l_\sigma$ alors on le remplace par r_σ (+ unification)
- règles de réécriture sur des termes :

$$x + S(y) \to S(x + y)$$

- et sur des **propositions** :

$$x * y = 0 \to x = 0 \vee y = 0$$

- avantages : puissance, souplesse
- on obtient une congruence modulo $\mathcal{R}$ (ensemble de règles, choisi): $\equiv$
- les règles se transforment

$$\text{axiome}\,\frac{}{\Gamma, A \vdash A} \quad \text{devient} \quad \frac{}{\Gamma, A \vdash B}\,\text{axiome}, A \equiv B$$

Déduction modulo : le calcul des séquents modulo

$$\frac{}{\Gamma, A \vdash B}\text{axiome } A \equiv B \qquad \frac{\Gamma, A \vdash C \quad \Gamma \vdash B}{\Gamma \vdash C}\text{coupure } A \equiv B$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash C} \wedge\text{-d } A \wedge B \equiv C \qquad \frac{\Gamma, A, B \vdash C}{\Gamma, D \vdash C} \wedge\text{-g } A \wedge B \equiv D$$

$$\frac{\Gamma, B, A[t] \vdash C}{\Gamma, B \vdash C}\forall\text{-g } \forall x A[x] \equiv B \qquad \frac{\Gamma \vdash A[x]}{\Gamma \vdash B}\forall\text{-d}^{*} \ \forall x A[x] \equiv B$$

Exemple: 3

- considérons le système $\mathcal{R}$:

$$\begin{aligned} P(0) &\rightarrow A \\ P(1) &\rightarrow B \end{aligned}$$

$$\forall x P(x) \vdash A \wedge B$$

Exemple: 3

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\frac{\forall x P(x) \vdash A \qquad \forall x P(x) \vdash B}{\forall x P(x) \vdash A \wedge B} \wedge\text{-r}$$

Exemple: 3

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\dfrac{\forall\text{-d}\,\dfrac{\forall x P(x), P(0) \vdash B}{\forall x P(x) \vdash A} \qquad \dfrac{\forall x P(x), P(1) \vdash B}{\forall x P(x) \vdash B}\,\forall\text{-d}}{\forall x P(x) \vdash A \wedge B}\,\wedge\text{-r}$$

Exemple: 3

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\dfrac{\dfrac{\dfrac{}{\forall x P(x), P(0) \vdash B}\text{ axiome}}{\forall x P(x) \vdash A}\ \forall\text{-d} \qquad \dfrac{\dfrac{}{\forall x P(x), P(1) \vdash B}\text{ axiome}}{\forall x P(x) \vdash B}\ \forall\text{-d}}{\forall x P(x) \vdash A \wedge B}\ \wedge\text{-r}$$

La règle de coupure : le détour

$$\frac{\Gamma, A \vdash B \quad \Gamma \vdash C}{\Gamma \vdash B}\text{coupure}, A \equiv C$$

- on prouve $\Gamma \vdash A$
- on prouve $\Gamma, A \vdash B$
- on a prouvé $\Gamma \vdash B$
- correspond à l'application d'un lemme.

Exemple: 4

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\forall x P(x) \vdash A \wedge B$$

Exemple: 4

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\dfrac{\forall x P(x), A \vdash A \wedge B \qquad \forall x P(x) \vdash A}{\forall x P(x) \vdash A \wedge B}\text{ coupure}$$

Exemple: 4

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\dfrac{\forall x P(x), A \vdash A \wedge B \qquad \dfrac{\dfrac{AX.}{\forall x P(x), P(0) \vdash A}}{\forall x P(x) \vdash A}\ \forall\text{-d}}{\forall x P(x) \vdash A \wedge B}\ \text{coupure}$$

Exemple: 4

- considérons le système $\mathcal{R}$:

$$
\begin{array}{rcl}
P(0) & \rightarrow & A \\
P(1) & \rightarrow & B
\end{array}
$$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{AX.}
\UnaryInfC{$\forall x P(x), A \vdash A$}
\AxiomC{}
\RightLabel{AX.}
\UnaryInfC{$\forall x P(x), P(1), A \vdash B$}
\RightLabel{$\forall$-d}
\UnaryInfC{$\forall x P(x), A \vdash B$}
\LeftLabel{$\wedge$-d}
\BinaryInfC{$\forall x P(x), A \vdash A \wedge B$}
\AxiomC{}
\RightLabel{AX.}
\UnaryInfC{$\forall x P(x), P(0) \vdash A$}
\RightLabel{$\forall$-d}
\UnaryInfC{$\forall x P(x) \vdash A$}
\RightLabel{coupure}
\BinaryInfC{$\forall x P(x) \vdash A \wedge B$}
\end{prooftree}
$$

Exemple: 4

- considérons le système $\mathcal{R}$:

$$\begin{array}{rcl} P(0) & \rightarrow & A \\ P(1) & \rightarrow & B \end{array}$$

$$\dfrac{\dfrac{\text{AX.}}{\forall x P(x), A \vdash A} \quad \dfrac{\dfrac{\text{AX.}}{\forall x P(x), P(1), A \vdash B}}{\forall x P(x), A \vdash B}\ \forall\text{-d}}{\forall x P(x), A \vdash A \wedge B}\ \wedge\text{-d} \quad \dfrac{\dfrac{\text{AX.}}{\forall x P(x), P(0) \vdash A}}{\forall x P(x) \vdash A}\ \forall\text{-d}$$
$$\overline{\qquad\qquad \forall x P(x) \vdash A \wedge B \qquad\qquad}\ \text{coupure}$$

- un détour “inutile”
- coupure sur n’importe quelle proposition!

La règle de coupure : le détour

$$\frac{\Gamma, A \vdash B \quad \Gamma \vdash C}{\Gamma \vdash B}\ \text{coupure} A \equiv C$$

- on prouve $\Gamma, A \vdash B$ et $\Gamma \vdash A$
- on a prouvé $\Gamma \vdash B$.
- lemme : adapté pour un être humain.
- en pratique: pas adaptée à la démonstration automatique.

La règle de coupure : le détour

$$\frac{\Gamma, A \vdash B \quad \Gamma \vdash C}{\Gamma \vdash B} \text{coupure} A \equiv C$$

- on prouve $\Gamma, A \vdash B$ et $\Gamma \vdash A$
- on a prouvé $\Gamma \vdash B$.
- lemme : adapté pour un être humain.
- en pratique: pas adaptée à la démonstration automatique.
- en théorie: cohérence, normalisation de fonctions (Curry-Howard) dépendent de son élimination.

La règle de coupure : le détour

$$\frac{\Gamma, A \vdash B \quad \Gamma \vdash C}{\Gamma \vdash B} \text{ coupure} A \equiv C$$

- on prouve $\Gamma, A \vdash B$ et $\Gamma \vdash A$
- on a prouvé $\Gamma \vdash B$.
- lemme : adapté pour un être humain.
- en pratique: pas adaptée à la démonstration automatique.
- en théorie: cohérence, normalisation de fonctions (Curry-Howard) dépendent de son élimination.
- éliminer les coupures: un résultat central.

$$\Gamma \vdash A \quad \triangleright \quad \Gamma \vdash_{cf} A$$

- deux méthodes principales de démonstration :
  - normalisation.
  - méthodes sémantiques.

La règle de coupure : le détour

$$\frac{\Gamma, A \vdash B \quad \Gamma \vdash C}{\Gamma \vdash B} \text{ coupure} A \equiv C$$

- on prouve $\Gamma, A \vdash B$ et $\Gamma \vdash A$
- on a prouvé $\Gamma \vdash B$.
- lemme : adapté pour un être humain.
- en pratique: pas adaptée à la démonstration automatique.
- en théorie: cohérence, normalisation de fonctions (Curry-Howard) dépendent de son élimination.
- éliminer les coupures: un résultat central.

$$\Gamma \vdash A \quad \rhd \quad \Gamma \vdash_{cf} A$$

- deux méthodes principales de démonstration :
  - normalisation.
  - méthodes sémantiques.
- en déduction modulo: indécidable, besoin de critères généraux (sur $\mathcal{R}$)

La méthode de normalisation

- Curry-Howard: preuves = programmes
- propositions = types
- dérivation d'une preuve = arbre de typage
- coeur des assistants de preuve (PVS, Coq, Isabelle, ...)
- quand un programme calcule, il élimine les coupures

La méthode de normalisation

- Curry-Howard: preuves = programmes
- propositions = types
- dérivation d'une preuve = arbre de typage
- coeur des assistants de preuve (PVS, Coq, Isabelle, ...)
- quand un programme calcule, il élimine les coupures
- montrer que toutes les fonctions terminent leurs calculs.

La méthode sémantique

- on définit un espace sémantique (vérité). Ex: Alg. de Boole.
- on doit avoir correction/complétude

La méthode sémantique

$$
\begin{tikzcd}
\Gamma \vdash A \arrow[rr, shift left, "\text{correction}"] \arrow[d, swap, "\begin{array}{c}\text{Gentzen}\\ \text{Tait-Girard}\\ \text{Dowek-Werner}\\ \ldots\end{array}"] & & \Gamma \models A \arrow[ll, shift left, "\text{complétude}"] \\
\Gamma \vdash_{cf} A & &
\end{tikzcd}
$$

La méthode sémantique

$$
\begin{tikzcd}
\Gamma \vdash A \arrow[rr, shift left, "\text{correction}"] \arrow[d, swap, "\begin{array}{c}\text{Gentzen}\\ \text{Tait-Girard}\\ \text{Dowek-Werner}\\ \text{...}\end{array}"] & & \Gamma \models A \arrow[ll, shift left, "\text{complétude}"] \arrow[dll, "\text{complétude forte}"] \\
\Gamma \vdash_{cf} A & &
\end{tikzcd}
$$

La méthode sémantique

$$\begin{tikzcd}
\Gamma \vdash A \arrow[rr, "\text{correction}"] \arrow[d, "\begin{array}{c}\text{Gentzen}\\ \text{Tait-Girard}\\ \text{Dowek-Werner}\\ \ldots\end{array}"'] & & \Gamma \models A \arrow[dll, "\text{complétude forte}"] \\
\Gamma \vdash_{cf} A & &
\end{tikzcd}$$

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

- algèbres de Heyting [Lipton,Okada]

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

- algèbres de Heyting [Lipton,Okada]
- structures de Kripke

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

- structures de Kripke

Une structure de Kripke (KS) est un quadruplet $\langle K, \leq, D, \Vdash \rangle$:

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

- structures de Kripke

Une structure de Kripke (KS) est un quadruplet $\langle K, \leq, D, \Vdash \rangle$:

- K l'ensemble des mondes, ordonné partiellement par $\leq$ (passé, présent, futurs possibles: information partielle)

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

- structures de Kripke

Une structure de Kripke (KS) est un quadruplet $\langle K, \leq, D, \Vdash \rangle$:

- K l'ensemble des mondes, ordonné partiellement par $\leq$ (passé, présent, futurs possibles: information partielle)
- $D : \alpha \to \mathcal{S}et$ une fonction monotone (domaine d'interprétation).

Une sémantique pour la déduction modulo

Deux sémantiques possibles:

- structures de Kripke

Une structure de Kripke (KS) est un quadruplet $\langle K, \leq, D, \Vdash \rangle$:

- K l'ensemble des mondes, ordonné partiellement par $\leq$ (passé, présent, futurs possibles: information partielle)
- $D : \alpha \rightarrow \mathcal{S}et$ une fonction monotone (domaine d'interprétation).
- $\Vdash$ est une relation entre mondes et propositions, qui vérifie entre autres:

Une sémantique pour la déduction modulo

- P atomique: si $\alpha \leq \beta$ et $\alpha \Vdash P$, alors $\beta \Vdash P$.
- $\alpha \Vdash A \Rightarrow B$ ssi pour tout $\beta \geq \alpha$ si $\beta \Vdash A$ alors $\beta \Vdash B$.
- $\alpha \Vdash A \vee B$ ssi $\alpha \Vdash A$ ou $\alpha \Vdash B$.

Une sémantique pour la déduction modulo

- P atomique: si $\alpha \leq \beta$ et $\alpha \Vdash P$, alors $\beta \Vdash P$.
- $\alpha \Vdash A \Rightarrow B$ ssi pour tout $\beta \geq \alpha$ si $\beta \Vdash A$ alors $\beta \Vdash B$.
- $\alpha \Vdash A \vee B$ ssi $\alpha \Vdash A$ ou $\alpha \Vdash B$.
- Contrainte supplémentaire en déduction modulo:

$$A \equiv B \quad \text{implique} \quad \alpha \Vdash A \Leftrightarrow \alpha \Vdash B$$

$$
\begin{tikzcd}
\Gamma \vdash A \arrow[r, "\text{correction}"] \arrow[d, "\begin{array}{c}\text{Gentzen}\\ \text{Tait-Girard}\\ \text{Dowek-Werner}\\ \ldots\end{array}"'] & \Gamma \models A \arrow[dl, "\text{complétude forte}"] \\
\Gamma \vdash_{cf} A &
\end{tikzcd}
$$

$$
\begin{tikzcd}
\Gamma \vdash A \arrow[r, "\text{correction}"] & \Gamma \models A \arrow[dl, "\text{complétude forte}"'] \arrow[d, shift left, "\text{complétude tableaux}"] \\
\Gamma \vdash_{cf} A & \text{Tab } (T\emptyset \Vdash \Gamma, F\emptyset \Vdash \Delta) \hookrightarrow \odot \arrow[u, shift left, "\text{correction}"]
\end{tikzcd}
$$

$$\begin{tikzcd}
\Gamma \vdash \Delta \arrow[r, "\text{correction}"] & \Gamma \models \Delta \arrow[dl, "\text{complétude forte}"'] \arrow[d, "\text{complétude tableaux}"] \\
\Gamma \vdash_{cf} \Delta & \mathrm{Tab}\,(T\emptyset \Vdash \Gamma,\ F\emptyset \Vdash \Delta) \hookrightarrow \odot \arrow[l, "\text{correction tableaux}"]
\end{tikzcd}$$

La méthode des tableaux

- Recherche de contre-modèle

La méthode des tableaux

- Recherche de contre-modèle
- algorithme de recherche exhaustive

La méthode des tableaux

- Recherche de contre-modèle
- algorithme de recherche exhaustive
- quelques règles:

$$\begin{array}{c} Tp \Vdash A \vee B \\ \hline Tp \Vdash A \quad Tp \Vdash B \end{array} \qquad \begin{array}{c} Fp \Vdash A \vee B \\ | \\ Fp \Vdash A \\ | \\ Fp \Vdash B \end{array}$$

$$\begin{array}{c} Tp \Vdash A \Rightarrow B \\ \hline Tq \Vdash B \quad Fq \Vdash A \end{array} \qquad \begin{array}{c} Fp \Vdash A \Rightarrow B \\ | \\ Tq \Vdash A \\ | \\ Fq \Vdash B \end{array}$$

avec certaines conditions sur q.

Tableau: exemple 1

On choisit en général les séquences d'entiers pour les mondes.

On veut prouver "$A \vee B \vdash C \Rightarrow A$"

$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$

Tableau: exemple 1

On choisit en général les séquences d'entiers pour les mondes.

$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$

Tableau: exemple 1

On choisit en général les séquences d'entiers pour les mondes.

$$
\begin{array}{c}
T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A \\
| \\
T1 \Vdash C \\
| \\
F1 \Vdash A
\end{array}
$$

Tableau: exemple 1

On choisit en général les séquences d'entiers pour les mondes.

$$
\begin{array}{c}
T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A \\
| \\
T1 \Vdash C \\
| \\
F1 \Vdash A
\end{array}
$$

Tableau: exemple 1

On choisit en général les séquences d'entiers pour les mondes.

$$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$$

$$T1 \Vdash C$$

$$F1 \Vdash A$$

$$T\emptyset \Vdash A \qquad T\emptyset \Vdash B$$

Tableau: exemple 1

On choisit en général les séquences d'entiers pour les mondes.

$$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$$

$$T1 \Vdash C$$

$$F1 \Vdash A$$

$$T\emptyset \Vdash A \qquad T\emptyset \Vdash B$$

$$\odot$$

Tableau: exemple 2

On veut prouver "$\vdash (A \Rightarrow B) \Rightarrow (A \Rightarrow B)$"

$F_{\emptyset} \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$

Tableau: exemple 2

$$F_\emptyset \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$

$$|$$

$$T_1 \Vdash (A \Rightarrow B)$$

$$|$$

$$F_1 \Vdash A \Rightarrow B$$

Tableau: exemple 2

$$F_{\emptyset} \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$

$$T_1 \Vdash (A \Rightarrow B)$$

$$F_1 \Vdash A \Rightarrow B$$

$$F_1 \Vdash A \qquad T_1 \Vdash B$$

Tableau: exemple 2

$$\begin{tikzcd}[column sep=small]
 & F_\varnothing \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B \arrow[d, dash] & \\
 & T_1 \Vdash (A \Rightarrow B) \arrow[d, dash] & \\
 & F_1 \Vdash A \Rightarrow B \arrow[dl, dash] \arrow[dr, dash] & \\
F_1 \Vdash A \arrow[d, dash] & & T_1 \Vdash B \\
T_1 \Vdash (A \Rightarrow B) & &
\end{tikzcd}$$

Tableau: exemple 2

$$F_{\emptyset} \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$

$$T_1 \Vdash (A \Rightarrow B)$$

$$F_1 \Vdash A \Rightarrow B$$

$$F_1 \Vdash A \qquad\qquad T_1 \Vdash B$$

$$T_1 \Vdash (A \Rightarrow B)$$

$$T_{11} \Vdash A$$

$$F_{11} \Vdash B$$

Tableau: exemple 2

$$F_\varnothing \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$

$$T_1 \Vdash (A \Rightarrow B)$$

$$F_1 \Vdash A \Rightarrow B$$

$$\begin{array}{cc} F_1 \Vdash A & T_1 \Vdash B \\ T_1 \Vdash (A \Rightarrow B) & \\ T_{11} \Vdash A & \\ F_{11} \Vdash B & \end{array}$$

$$\begin{array}{cc} F_{11} \Vdash A & T_{11} \Vdash B \end{array}$$

Tableau: exemple 2

$$F_{\emptyset} \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$

$$T_1 \Vdash (A \Rightarrow B)$$

$$F_1 \Vdash A \Rightarrow B$$

$$F_1 \Vdash A \qquad\qquad T_1 \Vdash B$$

$$T_1 \Vdash (A \Rightarrow B)$$

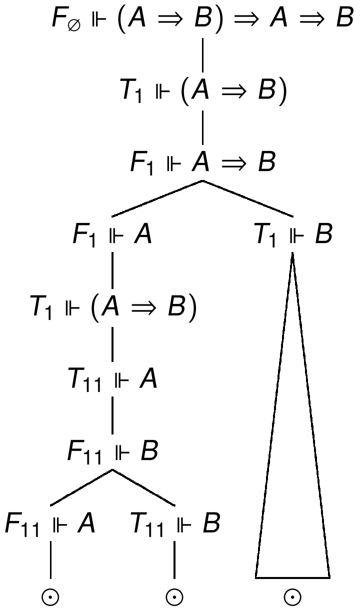
$$T_{11} \Vdash A$$

$$F_{11} \Vdash B$$

$$F_{11} \Vdash A \qquad T_{11} \Vdash B$$

$$\odot \qquad\qquad \odot$$

Tableau: exemple 2



Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): génère-t-elle un contre-modèle ?
- bien connu dans le calcul des séquents classique.

Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): génère-t-elle un contre-modèle ?
- bien connu dans le calcul des séquents classique.
  - définir un modèle à partir d'une branche infinie: celle-ci vérifie certaines propriétés.

Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): génère-t-elle un contre-modèle ?
- bien connu dans le calcul des séquents classique.
  - définir un modèle à partir d'une branche infinie: celle-ci vérifie certaines propriétés.
  - prouver que le modèle est en accord avec la branche:

$$Tp \Vdash P \quad \text{ssi} \quad p \Vdash P$$

Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): génère-t-elle un contre-modèle ?
- bien connu dans le calcul des séquents classique.
  - définir un modèle à partir d'une branche infinie: celle-ci vérifie certaines propriétés.
  - prouver que le modèle est en accord avec la branche:

$$Tp \Vdash P \quad \text{ssi} \quad p \Vdash P$$

  - en déduction modulo: prouver que le modèle est un modèle des règles de réécriture.

Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): génère-t-elle un contre-modèle ?
- bien connu dans le calcul des séquents classique.
  - définir un modèle à partir d'une branche infinie: celle-ci vérifie certaines propriétés.
  - prouver que le modèle est en accord avec la branche:

$$Tp \Vdash P \quad \text{ssi} \quad p \Vdash P$$

  - en déduction modulo: prouver que le modèle est un modèle des règles de réécriture.
- point de vue constructif: s'il n'y a pas de contre-modèle, la méthode termine-t-elle ? (définition modifiée)

Pour $A \vee B \vdash C \Rightarrow A$:

$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$

$T1 \Vdash C$

$F1 \Vdash A$

$T\emptyset \Vdash A \qquad T\emptyset \Vdash B$

$\odot$

génère un contre-modèle. Nerf de la guerre: les propositions *atomiques* (ext. par induction)

Conditions sur les règles de réécriture

Sous l'hypothèse de confluence et pour:

- Une condition d'ordre: $\succ$ est bien-fondé, possède la propriété de la sous-formule, et si $P \rightarrow^{*} Q$ alors $P \succ Q$.

la méthode de tableaux est complète.

Conditions sur les règles de réécriture

Sous l'hypothèse de confluence et pour:

- Une condition d'ordre: $\succ$ est bien-fondé, possède la propriété de la sous-formule, et si $P \rightarrow^* Q$ alors $P \succ Q$.
- Une condition de positivité: si $A \rightarrow P$ alors P a des occurrences d'atomes uniquement positives.

la méthode de tableaux est complète.

Conditions sur les règles de réécriture

Sous l'hypothèse de confluence et pour:

- Une condition d'ordre: $\succ$ est bien-fondé, possède la propriété de la sous-formule, et si $P \rightarrow^* Q$ alors $P \succ Q$.
- Une condition de positivité: si $A \rightarrow P$ alors P a des occurrences d'atomes uniquement positives.
- Les deux conditions ensemble: $\mathcal{R}_{\succ} \cup \mathcal{R}_{+}$. À condition que ces deux derniers soient compatibles.

la méthode de tableaux est complète.

Conditions sur les règles de réécriture

Sous l'hypothèse de confluence et pour:

- Une condition d'ordre: $\succ$ est bien-fondé, possède la propriété de la sous-formule, et si $P \rightarrow^* Q$ alors $P \succ Q$.
- Une condition de positivité: si $A \rightarrow P$ alors P a des occurrences d'atomes uniquement positives.
- Les deux conditions ensemble: $\mathcal{R}_{\succ} \cup \mathcal{R}_{+}$. À condition que ces deux derniers soient compatibles.
- La règle:

$$R \in R \rightarrow \forall y \; (\forall x (y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

la méthode de tableaux est complète.

$$
\begin{tikzcd}
\Gamma \vdash \Delta \arrow[r, "\text{correction}"] & \Gamma \models \Delta \arrow[d, "\begin{array}{c}\text{complétude}\\ \text{tableaux}\end{array}"] \\
\Gamma \vdash_{cf} \Delta & \begin{array}{l}\text{Tab } (T\emptyset \Vdash \Gamma, \\ \quad F\emptyset \Vdash \Delta) \hookrightarrow \odot\end{array}
\end{tikzcd}
$$

Correction des tableaux

On prouve le théorème suivant:

Theorem

Si le tableau de $T\emptyset \Vdash \Gamma, F\emptyset \Vdash P$ est fermé, alors on peut en tirer une preuve de $\Gamma \vdash_{cf} P$.

- cela pose une difficulté: dans un tableau, on peut avoir plusieurs formules "fausses":

$$\begin{array}{c} F\emptyset \Vdash P \vee Q \\ | \\ F\emptyset \Vdash P \\ | \\ F\emptyset \Vdash Q \end{array}$$

Correction des tableaux

On prouve le théorème suivant:

Theorem

Si le tableau de $T\emptyset \Vdash \Gamma, F\emptyset \Vdash P$ est fermé, alors on peut en tirer une preuve de $\Gamma \vdash_{cf} P$.

- cela pose une difficulté: dans un tableau, on peut avoir plusieurs formules “fausses”:

$$\begin{array}{c} F\emptyset \Vdash P \vee Q \\ | \\ F\emptyset \Vdash P \\ | \\ F\emptyset \Vdash Q \end{array}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash_{cf} A \vee B \quad \Gamma \vdash_{cf} A \vee C}{\Gamma \vdash_{cf} A \vee (B \wedge C)}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash_{cf} A \vee B \quad \Gamma \vdash_{cf} A \vee C}{\Gamma \vdash_{cf} A \vee (B \wedge C)}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash_{cf} A \vee B \quad \Gamma \vdash_{cf} A \vee C}{\Gamma \vdash_{cf} A \vee (B \wedge C)}$$

- facile avec la coupure:

$$\dfrac{\dfrac{\Gamma, A \vee B, A \vee C \vdash A \vee (B \wedge C) \quad \Gamma, A \vee B \vdash A \vee C}{\Gamma, A \vee B \vdash A \vee (B \wedge C)} \quad \Gamma \vdash A \vee B}{\Gamma \vdash A \vee (B \wedge C)}\ \text{coupure}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash_{cf} A \vee B \quad \Gamma \vdash_{cf} A \vee C}{\Gamma \vdash_{cf} A \vee (B \wedge C)}$$

- facile avec la coupure:

$$\dfrac{\dfrac{\Gamma, A\vee B, A\vee C \vdash A\vee(B\wedge C) \quad \Gamma, A\vee B \vdash A\vee C}{\Gamma, A\vee B \vdash A\vee(B\wedge C)} \quad \Gamma \vdash A \vee B}{\Gamma \vdash A \vee (B \wedge C)}\ \text{coupure}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash_{cf} A \vee B \quad \Gamma \vdash_{cf} A \vee C}{\Gamma \vdash_{cf} A \vee (B \wedge C)}$$

- facile avec la coupure:

$$\frac{\dfrac{\Gamma, A \vee B, A \vee C \vdash A \vee (B \wedge C) \quad \Gamma, A \vee B \vdash A \vee C}{\Gamma, A \vee B \vdash A \vee (B \wedge C)} \quad \Gamma \vdash A \vee B}{\Gamma \vdash A \vee (B \wedge C)} \text{ coupure}$$

- Sans coupure, montrer le lemme:

$$\begin{array}{rl} \Gamma_1 \vdash_{cf} A \vee B & \Gamma_2 \vdash_{cf} A \vee C \\ \text{alors} & \Gamma_1, \Gamma_2 \vdash_{cf} A \vee (B \wedge C) \end{array}$$

Contenu calculatoire: quel algorithmes ?

Revenons sur la règle:

$$R \in R \to \forall y\ (\forall x(y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

- ce ne peut pas être un algorithme de normalisation.

Contenu calculatoire: quel algorithmes ?

Revenons sur la règle:

$$R \in R \to \forall y\ (\forall x (y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

- ce ne peut pas être un algorithme de normalisation.
- c'est grosso-modo la méthode des tableaux décrite.

$$\begin{tikzcd}[column sep=huge, row sep=large]
\Gamma \vdash A \arrow[r, "\text{correction}"] \arrow[d, swap, "\begin{array}{c}\text{Gentzen}\\ \text{Tait-Girard}\\ \text{Dowek-Werner}\\ \ldots\end{array}"] & \Gamma \models A \arrow[d, "\begin{array}{c}\text{complétude}\\ \text{tableaux}\end{array}"] \\
\Gamma \vdash_{cf} A & {} \arrow[l, swap, "\textit{correctiontableaux}"]
\end{tikzcd}$$

- Ce diagramme ne commute pas.

$$
\begin{tikzcd}[column sep=huge, row sep=large]
\Gamma \vdash A \arrow[rr, "\text{correction}"] \arrow[d, swap, "\begin{array}{c}\text{Gentzen}\\ \text{Tait-Girard}\\ \text{Dowek-Werner}\\ \ldots\end{array}"] & & \Gamma \models A \arrow[d, "\begin{array}{c}\text{complétude}\\ \text{tableaux}\end{array}"] \\
\Gamma \vdash_{cf} A & \arrow[l, "\textit{correctiontableaux}"'] & {}
\end{tikzcd}
$$

- Ce diagramme ne commute pas.
- Cependant tout n’est pas perdu: les méthodes de normalisation “génèrent” certaines méthodes sémantiques [Dowek - Hermant]