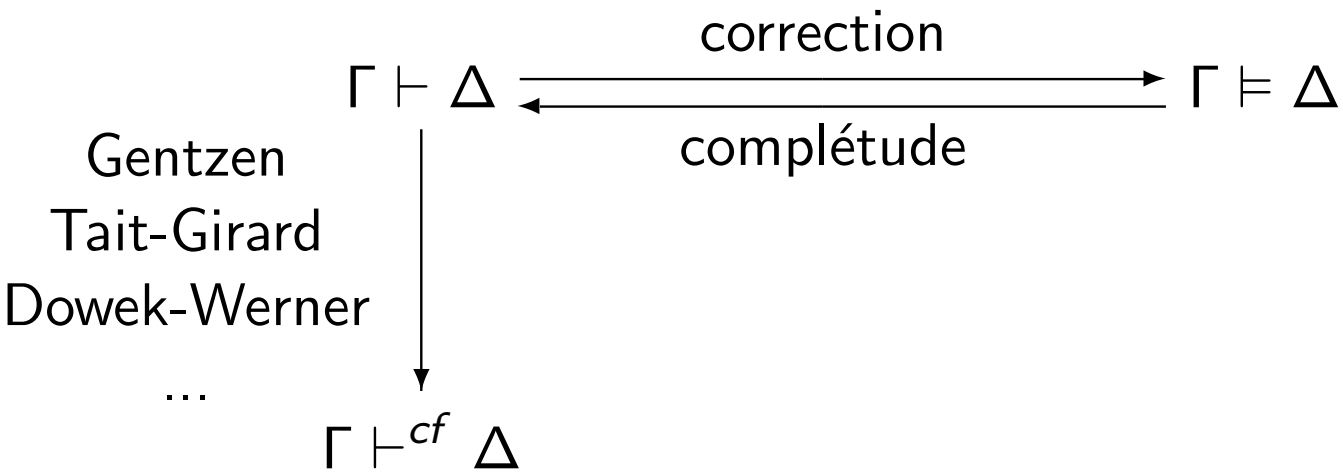
Constructive semantic cut elimination

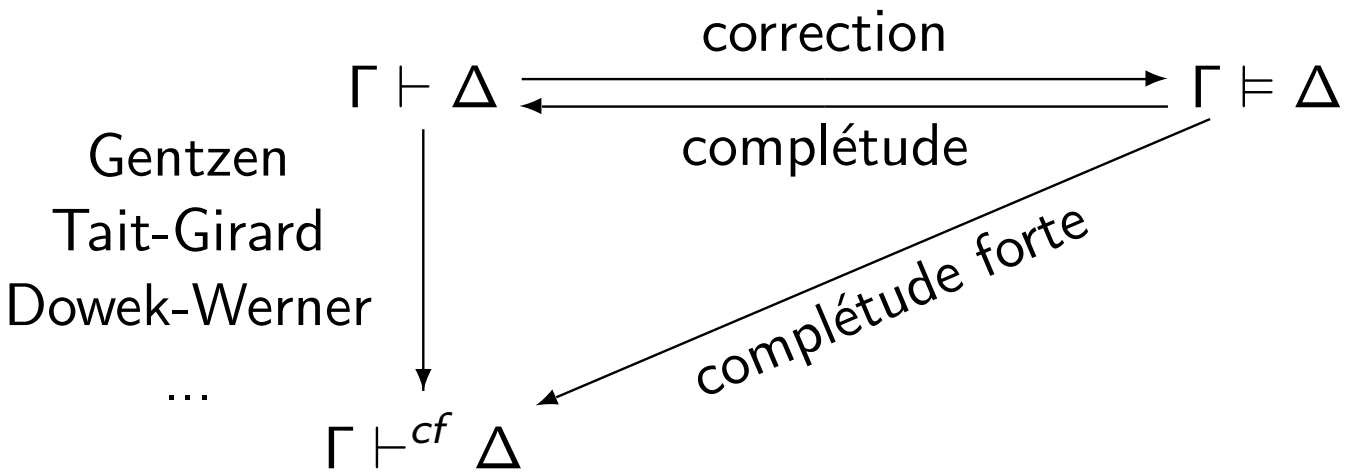
Olivier Hermant

November 5, 2006

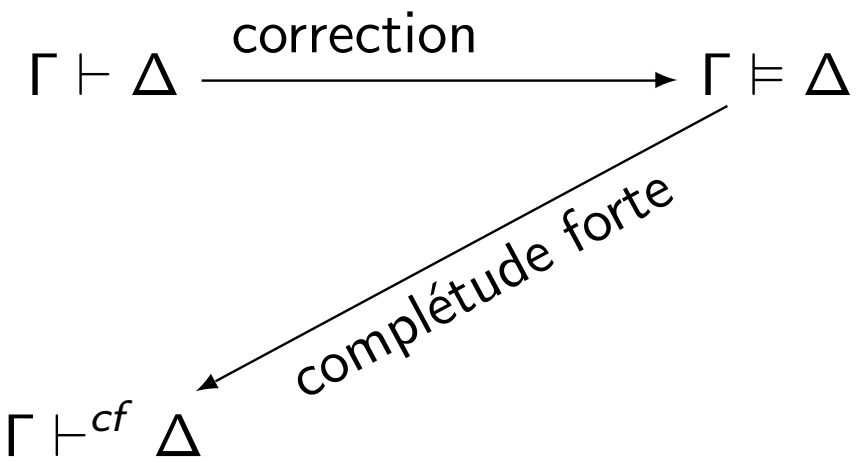
Élimination des coupures sémantique



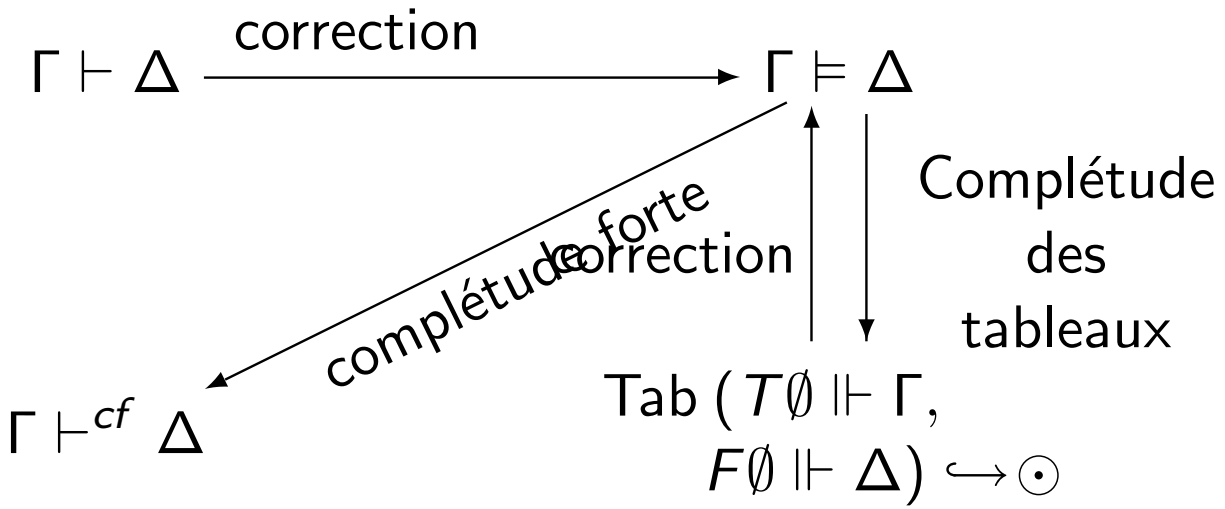
Élimination des coupures sémantique



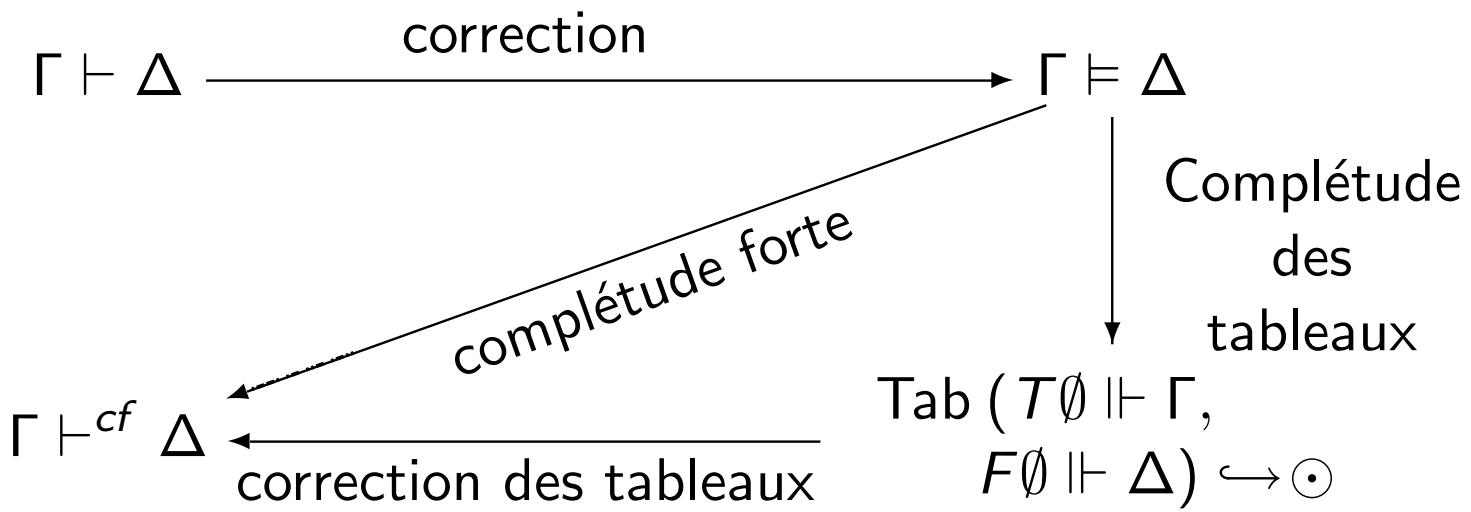
Élimination des coupures sémantique



Élimination des coupures sémantique



Élimination des coupures sémantique



Déduction Modulo

Logique + Règles de Réécriture

- Le calcul des séquents intuitionniste

Déduction Modulo

Logique + Règles de Réécriture

- Le calcul des séquents intuitionniste
- réécriture sur des termes:

$$\begin{aligned} x + 0 &\rightarrow x \\ x * 0 &\rightarrow 0 \end{aligned}$$

Déduction Modulo

Logique + Règles de Réécriture

- Le calcul des séquents intuitionniste
- réécriture sur des termes:

$$\begin{aligned} x + 0 &\rightarrow x \\ x * 0 &\rightarrow 0 \end{aligned}$$

- réécriture sur des propositions:

$$\begin{aligned} x * y = 0 &\rightarrow x = 0 \vee y = 0 \\ P(0) &\rightarrow \forall x P(x) \end{aligned}$$

Déduction Modulo

Logique + Règles de Réécriture

- Le calcul des séquents intuitionniste
- réécriture sur des termes:

$$\begin{aligned} x + 0 &\rightarrow x \\ x * 0 &\rightarrow 0 \end{aligned}$$

- réécriture sur des propositions:

$$\begin{aligned} x * y = 0 &\rightarrow x = 0 \vee y = 0 \\ P(0) &\rightarrow \forall x P(x) \end{aligned}$$

- Puissance expressive: on peut transformer des axiomes en règles de réécriture.

Le calcul des séquents intuitionniste

$$\frac{}{\Gamma, P \vdash P}\text{axiom} \qquad \frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut}$$

$$\frac{\Gamma, P, P \vdash Q}{\Gamma, P \vdash Q}\text{contr-l} \qquad \frac{}{\Gamma, \bot \vdash Q}\bot\text{-l}$$

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R} \vee\text{-l} \qquad \frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q} \vee\text{-r} \qquad \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q} \vee\text{-r}$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \Rightarrow Q \vdash R} \Rightarrow\text{-l} \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash P \Rightarrow Q} \Rightarrow\text{-r}$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, \exists x P \vdash Q}\exists\text{-l, } c \text{ fresh constant} \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash \exists x P}\exists\text{-r}$$

Le calcul des séquents intuitionniste

$$\frac{}{\Gamma, P \vdash P}\text{axiom} \qquad \frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut}$$

$$\frac{\Gamma, P, P \vdash Q}{\Gamma, P \vdash Q}\text{contr-l} \qquad \frac{}{\Gamma, \bot \vdash Q}\bot\text{-l}$$

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R} \vee\text{-l} \qquad \frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q} \vee\text{-r} \qquad \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q} \vee\text{-r}$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \Rightarrow Q \vdash R} \Rightarrow\text{-l} \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash P \Rightarrow Q} \Rightarrow\text{-r}$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, \exists x P \vdash Q}\exists\text{-l, } c \text{ fresh constant} \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash \exists x P}\exists\text{-r}$$

Le calcul des séquents intuitionniste modulo

On remplace:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \vee\text{-g (LJ)}$$

par:

$$\frac{\Gamma \vdash_{\mathcal{R}} A \qquad \Gamma \vdash_{\mathcal{R}} B}{\Gamma \vdash_{\mathcal{R}} C} \vee\text{-g (LJmod)} C \equiv_{\mathcal{R}} A \wedge B$$

Le calcul des séquents intuitionniste modulo

On remplace:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \vee\text{-g (LJ)}$$

par:

$$\frac{\Gamma \vdash_{\mathcal{R}} A \qquad \Gamma \vdash_{\mathcal{R}} B}{\Gamma \vdash_{\mathcal{R}} C} \vee\text{-g (LJmod)} C \equiv_{\mathcal{R}} A \wedge B$$

La condition $C \equiv_{\mathcal{R}} A \wedge B$ est un degré de liberté.

The Intuitionnistic Sequent Calculus Modulo

$$\frac{}{\Gamma, P \vdash Q}\text{axiom } P \equiv_{\mathcal{R}} Q \qquad \frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, P, Q \vdash R}{\Gamma, P \vdash R}\text{contr-l } P \equiv_{\mathcal{R}} Q \qquad \frac{}{\Gamma, P \vdash Q}\bot\text{-l } P \equiv_{\mathcal{R}} \bot$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, S \vdash R} \Rightarrow\text{-l } P \Rightarrow Q \equiv S \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash S} \Rightarrow\text{-r } P \Rightarrow Q \equiv_{\mathcal{R}} S$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, R \vdash Q}\exists\text{-l}^{*}\ \exists x P \equiv_{\mathcal{R}} R \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash R}\exists\text{-r}\ \exists x P \equiv_{\mathcal{R}} R$$

The Intuitionnistic Sequent Calculus Modulo

$$\frac{}{\Gamma, P \vdash Q}\text{axiom } P \equiv_{\mathcal{R}} Q \qquad \frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\text{cut } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, P, Q \vdash R}{\Gamma, P \vdash R}\text{contr-l } P \equiv_{\mathcal{R}} Q \qquad \frac{}{\Gamma, P \vdash Q}\bot\text{-l } P \equiv_{\mathcal{R}} \bot$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, S \vdash R} \Rightarrow\text{-l } P \Rightarrow Q \equiv S \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash S} \Rightarrow\text{-r } P \Rightarrow Q \equiv_{\mathcal{R}} S$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, R \vdash Q}\exists\text{-l}^{*}\ \exists x P \equiv_{\mathcal{R}} R \qquad \frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash R}\exists\text{-r } \exists x P \equiv_{\mathcal{R}} R$$

Sémantique

Sémantiques intuitionnistes:

Sémantique

Sémantiques intuitionnistes:

- algèbres de Heyting [Lipton,Okada]

Sémantique

Sémantiques intuitionnistes:

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

Sémantique

Sémantiques intuitionnistes:

- structures de Kripke

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

Sémantique

Sémantiques intuitionnistes:

- 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 $\leq$

Sémantique

Sémantiques intuitionnistes:

- 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 $\leq$
- $D : \alpha \longrightarrow \mathcal{S}et$ une fonction monotone (interprète les termes).

Sémantique

Sémantiques intuitionnistes:

- 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 $\leq$
- $D : \alpha \longrightarrow \mathcal{S}et$ une fonction monotone (interprète les termes).
- $\Vdash$ est une relation entre les mondes, qui vérifie entre autres:

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

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

$$P \equiv_{\mathcal{R}} Q \quad \text{implique} \quad \alpha \Vdash P \Leftrightarrow \alpha \Vdash Q$$

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:

$$\frac{T p \Vdash A \vee B}{T p \Vdash A \quad T p \Vdash B}$$

$$\begin{array}{c} F p \Vdash A \vee B \\ | \\ F p \Vdash A \\ | \\ F p \Vdash B \end{array}$$

$$\frac{T p \Vdash A \Rightarrow B}{T q \Vdash B \quad F q \Vdash A}$$

$$\begin{array}{c} F p \Vdash A \Rightarrow B \\ | \\ T q \Vdash A \\ | \\ F q \Vdash B \end{array}$$

avec certaines conditions sur q.

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.

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

Tableau: exemple 1

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

$$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$$
$$\Big|$$
$$T1 \Vdash C$$
$$\Big|$$
$$F1 \Vdash A$$

Tableau: exemple 1

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

$$T\emptyset \Vdash A \vee B, F\emptyset \Vdash C \Rightarrow A$$
$$\Big|$$
$$T1 \Vdash C$$
$$\Big|$$
$$F1 \Vdash A$$

Tableau: exemple 1

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

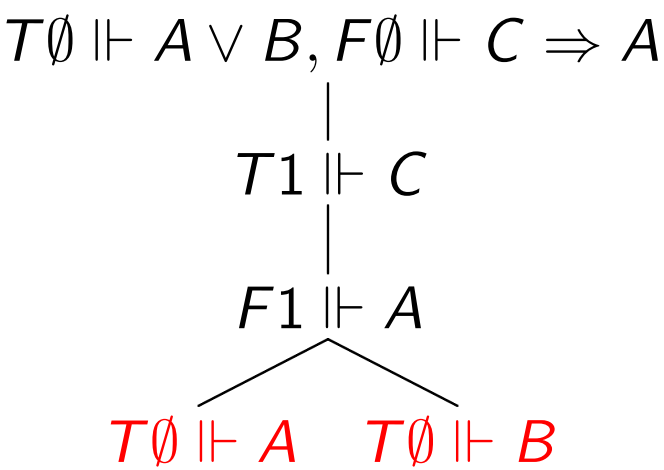


Tableau: exemple 1

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

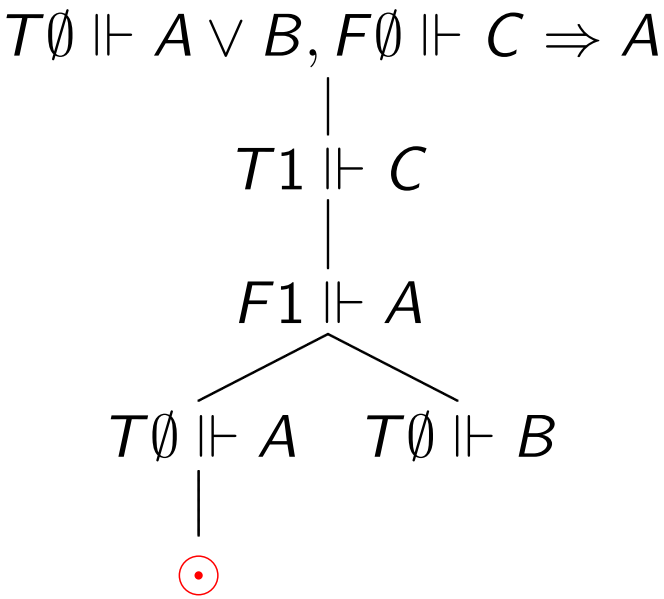


Tableau: exemple 2

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

Tableau: exemple 2

$$F_\varnothing \Vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$
$$\vert$$
$$T_1 \Vdash (A \Rightarrow B)$$
$$\vert$$
$$F_1 \Vdash A \Rightarrow B$$

Tableau: exemple 2

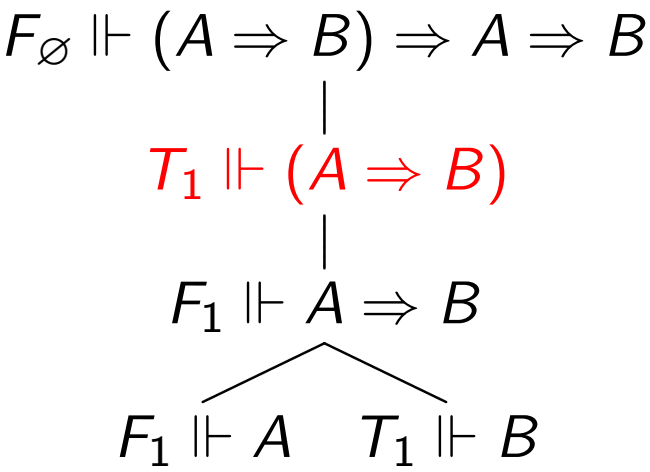


Tableau: exemple 2

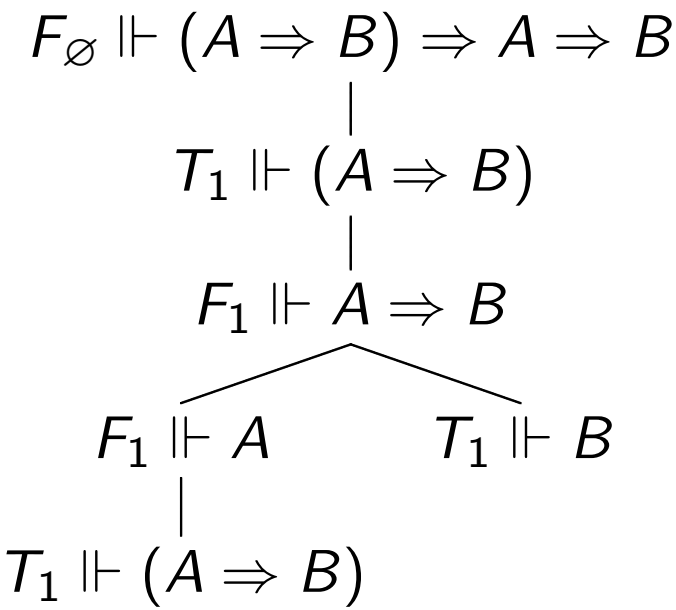


Tableau: exemple 2

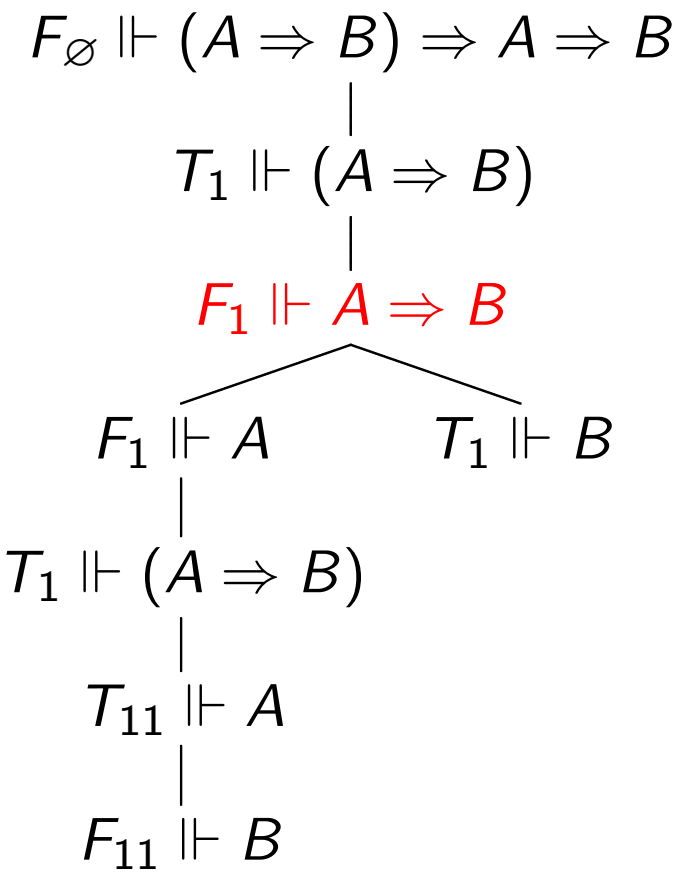


Tableau: exemple 2

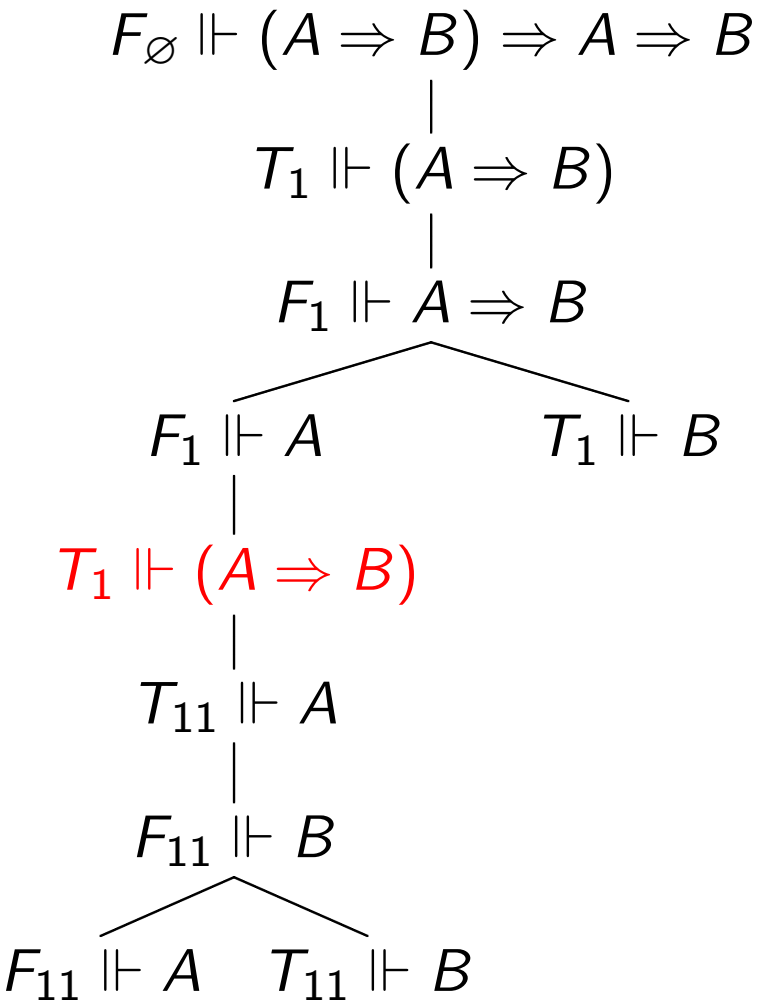


Tableau: exemple 2

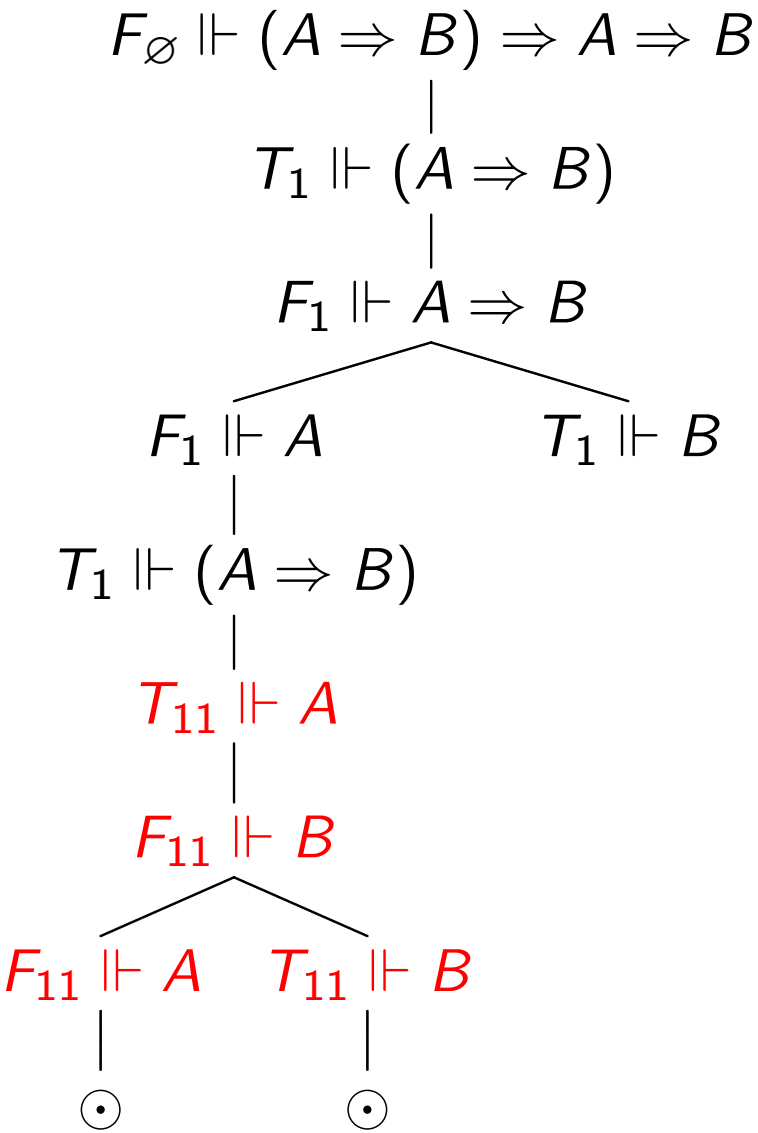
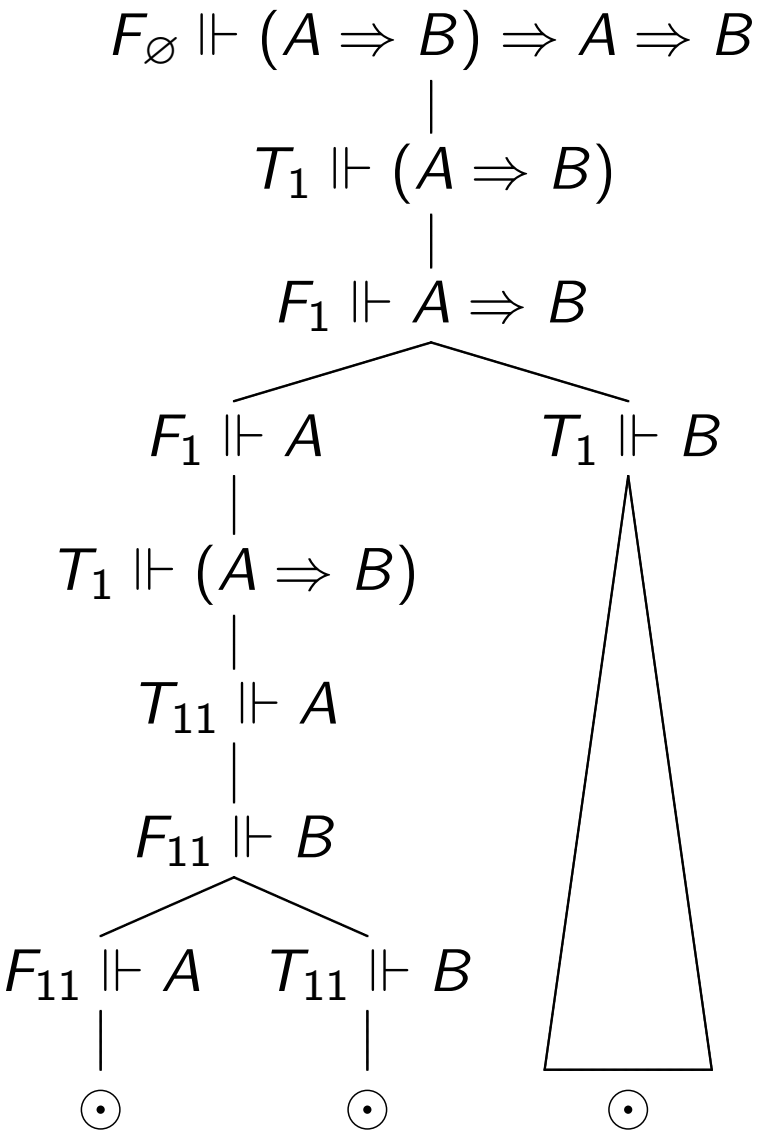


Tableau: exemple 2



Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): a-t-on un contre-modèle ?

Complétude des tableaux

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

Complétude des tableaux

- Si la méthode de génération systématique échoue (ne termine pas): a-t-on 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): a-t-on 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): a-t-on 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.

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 $P \to^* Q$ alors $P \succ Q$.
- Une condition de positivité: si $A \to P$ 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 $P \to^* Q$ alors $P \succ Q$.
- Une condition de positivité: si $A \to P$ 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:

$$R \in R \rightarrow_{\mathcal{R}} \forall y\ (\forall x(y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

la méthode de tableaux est complète.

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* $\Gamma \vdash^{cf}_{\mathcal{R}} P$.

- 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* $\Gamma \vdash^{cf}_{\mathcal{R}} P$.

- 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:

$$\frac{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee B \quad \Gamma \vdash^{cf}_{\mathcal{R}} A \vee C}{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee (B \wedge C)}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee B \quad \Gamma \vdash^{cf}_{\mathcal{R}} A \vee C}{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee (B \wedge C)}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee B \quad \Gamma \vdash^{cf}_{\mathcal{R}} A \vee C}{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee (B \wedge C)}$$

- facile avec la coupure:

$$\frac{\dfrac{\Gamma, A \vee B, A \vee C \vdash_{\mathcal{R}} A \vee (B \wedge C) \quad \Gamma, A \vee B \vdash_{\mathcal{R}} A \vee C}{\Gamma, A \vee B \vdash_{\mathcal{R}} A \vee (B \wedge C)} \qquad \Gamma \vdash_{\mathcal{R}} A \vee B}{\Gamma \vdash_{\mathcal{R}} A \vee (B \wedge C)}\ \text{coupure}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee B \quad \Gamma \vdash^{cf}_{\mathcal{R}} A \vee C}{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee (B \wedge C)}$$

- facile avec la coupure:

$$\frac{\dfrac{\Gamma, A \vee B, A \vee C \vdash_{\mathcal{R}} A \vee (B \wedge C) \quad \Gamma, A \vee B \vdash_{\mathcal{R}} A \vee C}{\Gamma, A \vee B \vdash_{\mathcal{R}} A \vee (B \wedge C)} \qquad \Gamma \vdash_{\mathcal{R}} A \vee B}{\Gamma \vdash_{\mathcal{R}} A \vee (B \wedge C)}\ \text{coupure}$$

- on doit pouvoir dériver la règle suivante:

$$\frac{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee B \quad \Gamma \vdash^{cf}_{\mathcal{R}} A \vee C}{\Gamma \vdash^{cf}_{\mathcal{R}} A \vee (B \wedge C)}$$

- facile avec la coupure:

$$\frac{\dfrac{\Gamma, A \vee B, A \vee C \vdash_{\mathcal{R}} A \vee (B \wedge C) \quad \Gamma, A \vee B \vdash_{\mathcal{R}} A \vee C}{\Gamma, A \vee B \vdash_{\mathcal{R}} A \vee (B \wedge C)} \qquad \Gamma \vdash_{\mathcal{R}} A \vee B}{\Gamma \vdash_{\mathcal{R}} A \vee (B \wedge C)}\ \text{coupure}$$

- Sans coupure, montrer le lemme:

$$\Gamma_1 \vdash^{cf}_{\mathcal{R}} A \vee B \qquad \Gamma_2 \vdash^{cf}_{\mathcal{R}} A \vee C$$
$$\text{alors} \qquad \Gamma_1, \Gamma_2 \vdash^{cf}_{\mathcal{R}} A \vee (B \wedge C)$$

Contenu calculatoire

Revenons sur la règle:

$$R \in R \rightarrow_{\mathcal{R}} \forall y\ (\forall x(y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

- ce ne peut pas être un algorithme de normalisation.

Contenu calculatoire

Revenons sur la règle:

$$R \in R \rightarrow_{\mathcal{R}} \forall y\ (\forall x(y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

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