Des Tableaux pour la Déduction Modulo

Richard Bonichon

LIP6
Université Pierre et Marie Curie Paris VI

Journées LAC, Chambéry
9 février 2007

Ceci n'est pas un tableau

Qu'est-ce qu'un tableau ?

- Un tableau a une structure d'arbre.
- Méthode de réfutation sans coupure :

$$\text{Prouver } P\ (T\ P) \text{ devient réfuter } \neg P\ (F\ P)$$

- Deux lectures :
  - Syntaxique : décomposer la structure des formules
  - Sémantique : construire un modèle

Exemple

$T\ \forall x P(x) \wedge (\neg P(c) \vee \neg Q(a))$

Règle

Priorité :$\alpha > \beta > \delta > \gamma$

Exemple

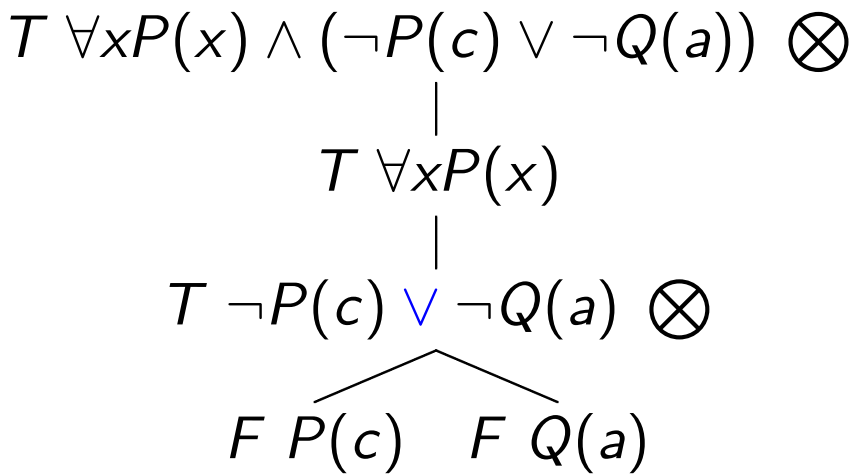
$$T\ \forall x P(x) \wedge (\neg P(c) \vee \neg Q(a))\ \otimes$$
$$\Big|$$
$$T\ \forall x P(x)$$
$$\Big|$$
$$T\ \neg P(c) \vee \neg Q(a)$$

Règle

Priorité : $\alpha > \beta > \delta > \gamma$

$$\frac{\alpha(A, B)}{A, B}$$

Exemple

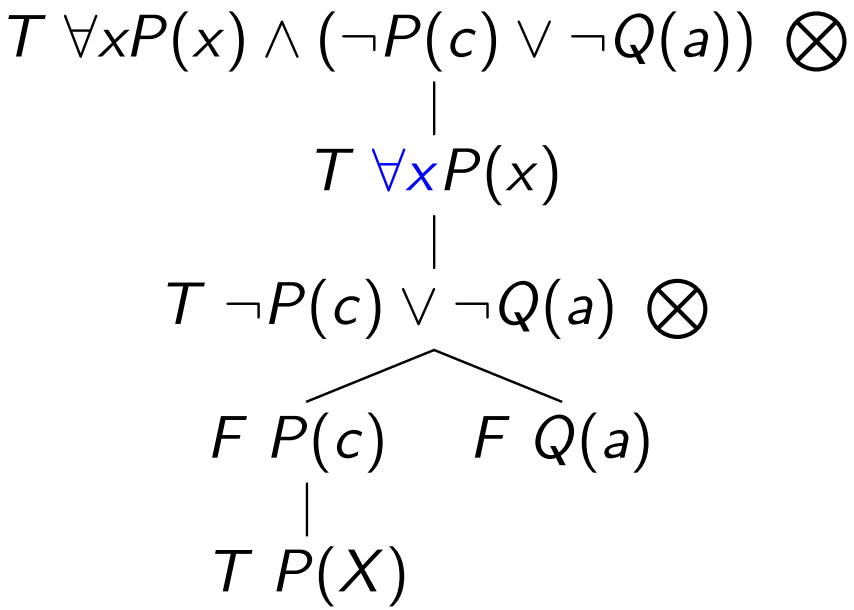


Règle

Priorité : $\alpha > \beta > \delta > \gamma$

$$\frac{\beta(A, B)}{A \mid B}$$

Exemple

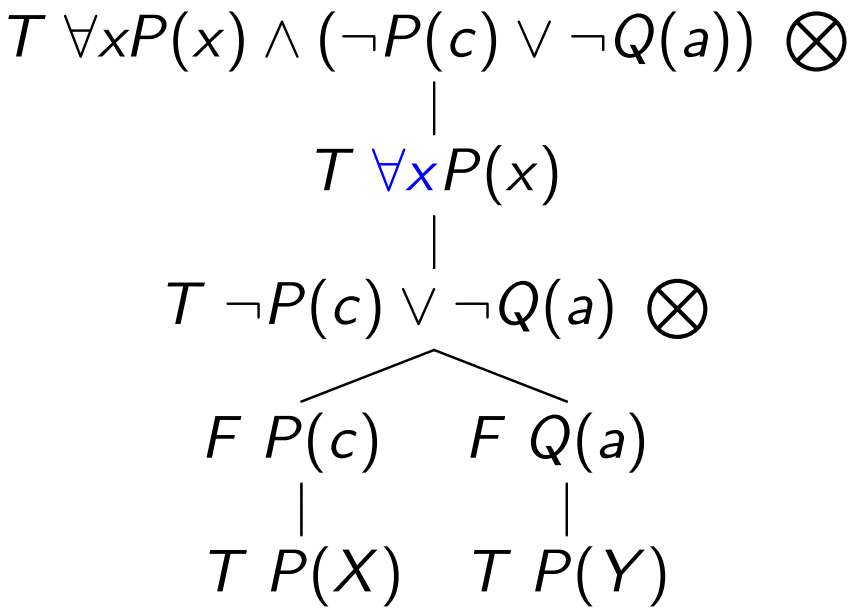


Règle

Priorité : $\alpha > \beta > \delta > \gamma$

$$\frac{\gamma(x, A)}{A[x := X]}$$

Exemple

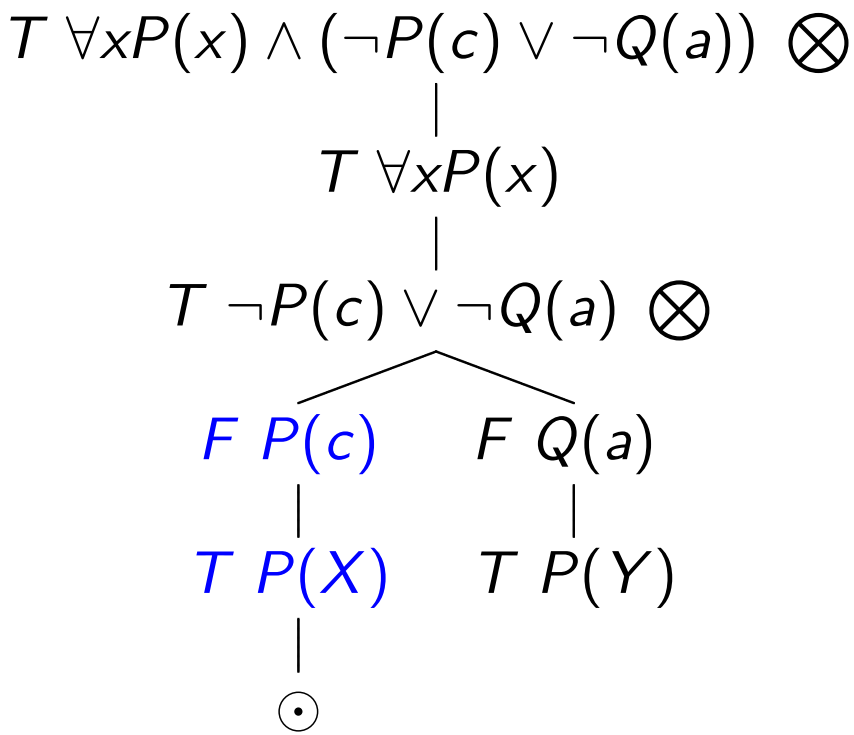


Règle

Priorité : $\alpha > \beta > \delta > \gamma$

$$\frac{\gamma(x, A)}{A[x := X]}$$

Exemple

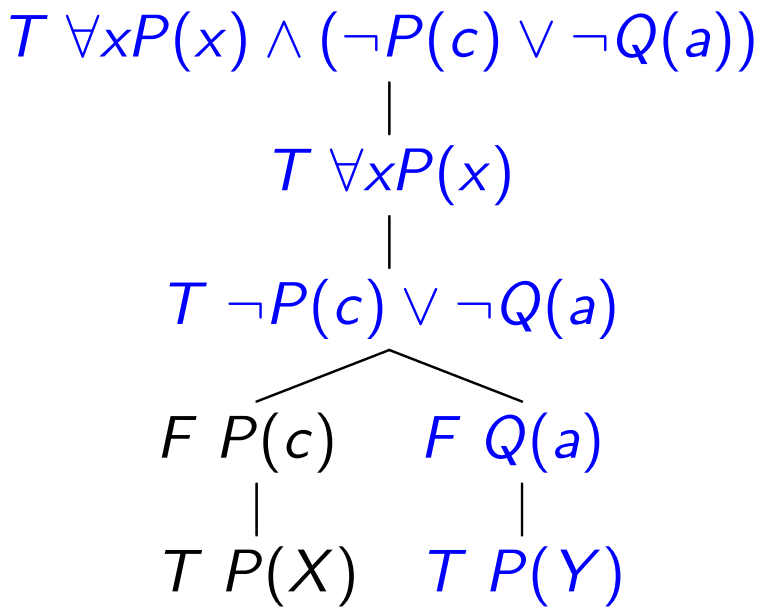


Règle

Priorité : $\alpha > \beta > \delta > \gamma$

$$\frac{TA, FB}{\odot}\ \odot,\ \sigma = \{X := c\}$$

Exemple



Extraction d'un modèle

$$\begin{aligned} Q(a) &= \text{faux} \\ P(t) &= \text{vrai pour tout } t \end{aligned}$$

Règles de tableaux avec métavariables

$$\frac{\alpha(A, B)}{A, B}$$

Type de formule

$\alpha(A, B)$:

$$T\ A \wedge B$$
$$F\ A \vee B$$
$$F\ (A \Rightarrow B)$$

Inférence correspondante (séquents)

$$\frac{\Gamma, A, B \vdash}{\Gamma, A \wedge B \vdash} \text{ et}$$

Règles de tableaux avec métavariables

$$\frac{\alpha(A, B)}{A, B} \qquad \frac{\beta(A, B)}{A \mid B}$$

Type de formule

$\beta(A, B)$:

$$T\ A \vee B$$
$$F\ (A \wedge B)$$
$$T\ A \Rightarrow B$$

Inférence correspondante (séquents)

$$\frac{\Gamma, A \vdash \qquad \Gamma, B \vdash}{\Gamma, A \vee B \vdash} \text{ ou}$$

Règles de tableaux avec métavariables

$$\frac{\alpha(A, B)}{A, B} \qquad \frac{\beta(A, B)}{A \mid B}$$

$$\frac{\gamma(x, A)}{A[x := X]}$$

Type de formule

$\gamma(x, A)$:

$$T\ \forall x A$$
$$F\ (\exists x A)$$

Inférence correspondante (séquents)

$$\frac{\Gamma, \forall x\ A, A[x := t] \vdash}{\Gamma, \forall x\ A \vdash}\ \text{qqs}$$

Règles de tableaux avec métavariables

$$\frac{\alpha(A, B)}{A, B} \qquad \frac{\beta(A, B)}{A \mid B}$$

$$\frac{\gamma(x, A)}{A[x := X]} \qquad \frac{\delta(x, A)}{A[x := f_{\text{sko}}(\text{args})]}$$

Type de formule

$\delta(x, A)$:

$$T\ \exists x A$$
$$F\ (\forall x A)$$

Inférence correspondante (séquents)

$$\frac{\Gamma, A[x := c] \vdash}{\Gamma, \exists x\ A \vdash}\ \text{ex}$$

Règles de tableaux : fermeture et conversion

$$\frac{TA, FB}{\odot}\ \odot,\ \sigma = mgu(A, B)$$

Il faut propager σ dans le reste du tableau.

$$\frac{T\ \neg A}{F\ A}\ \text{conversion}$$

Déduction modulo

- Déduction : séquents, déduction naturelle
- *Modulo* calcul :
  - Réécriture sur les *propositions* ($\mathcal{R}$)

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

  - Axiomes équationnels ($\mathcal{E}$)

$$x + y = y + x$$

  - Réécriture sur les termes ($\mathcal{E}$)

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

Extension des règles d'inférences

$\mathcal{R}$ ensemble de règles de réécriture propositionnelles

$\mathcal{E}$ ensemble de règles de réécriture sur les termes et d'axiomes équationnels

$\equiv_{\mathcal{RE}}$ congruence définie par $\mathcal{R} \cup \mathcal{E}$.

Une inférence modulo

$$\frac{\Gamma, A \vdash_{\mathcal{RE}} \qquad \Gamma, B \vdash_{\mathcal{RE}}}{\Gamma, P \vdash_{\mathcal{RE}}} \text{ ou}$$

si $P \equiv_{\mathcal{RE}} A \vee B$.

Séquents modulo : connecteurs

$$\frac{}{\Gamma, A, P \vdash_{\mathcal{RE}}} \text{ axiome}$$

$$\frac{\Gamma, A, B \vdash_{\mathcal{RE}}}{\Gamma, P \vdash_{\mathcal{RE}}}$$

si $P \equiv_{\mathcal{RE}} \neg A$

si $P \equiv_{\mathcal{RE}} A \wedge B$

$$\frac{\Gamma, A \vdash_{\mathcal{RE}} \qquad \Gamma, B \vdash_{\mathcal{RE}}}{\Gamma, P \vdash_{\mathcal{RE}}}$$

$$\frac{\Gamma, \neg A \vdash_{\mathcal{RE}} \qquad \Gamma, B \vdash_{\mathcal{RE}}}{\Gamma, P \vdash_{\mathcal{RE}}}$$

si $P \equiv_{\mathcal{RE}} A \vee B$

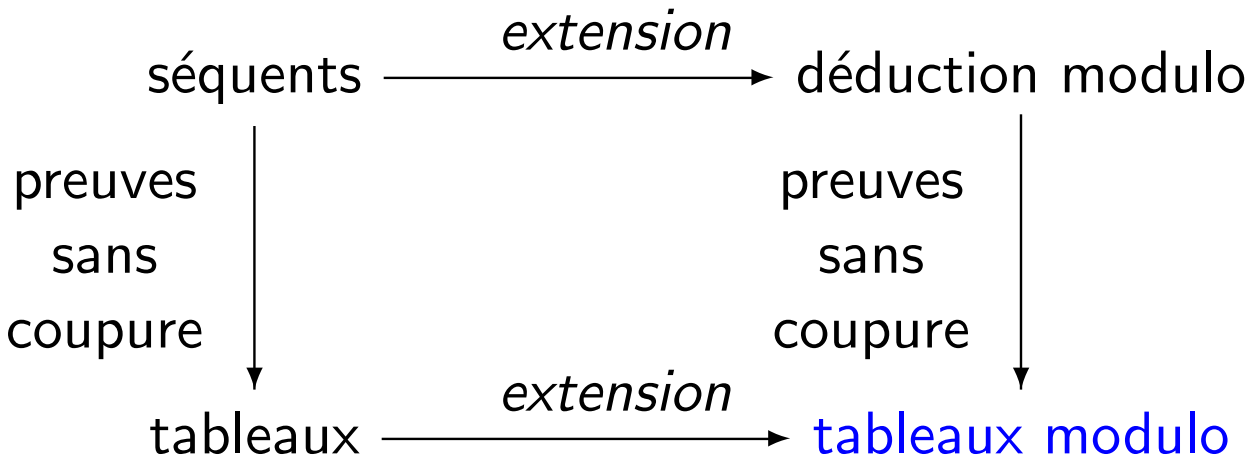
si $P \equiv_{\mathcal{RE}} A \Rightarrow B$

...

Remarques

- Preuves plus courtes et plus lisibles.
- Expression sans axiome de :
  - HOL (Dowek,Hardin,C.Kirchner) ;
  - Arithmétique (Dowek,Werner ; F.Kirchner) ;
  - Théorie des ensembles de Zermelo (Dowek,Miquel).
- Perte de la normalisation (élimination syntaxique de coupure) même dans le cas de (certains) systèmes convergents.

Tableaux modulo



Questions

- Comment étendre les tableaux ?
  - Ajouter de la réécriture
  - Impact sur la procédure
- Que deviennent les propriétés sémantiques ?
- Quid de l'élimination des coupures ?

Ajouter de la réécriture : une idée

$\mathcal{R}$: règles de réécriture sur les termes et les propositions

$$\frac{P[\zeta]_\omega}{P[d]_\omega}\ \mathrm{rw}$$

si

- $g \to d \in \mathcal{R}$;
- $\{\zeta \stackrel{?}{=} g\}$;

Contraintes

- Contraintes :
  - sur les formules (réécriture)

$$P(X) \text{ et } g \longrightarrow d$$

  - sur les tableaux (fermeture)

$$P(X) \text{ et } P(c)$$

TaMeD

Connecteurs

$$\frac{\Gamma_1, \beta(P,Q)^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}{\Gamma_1, \beta(P,Q)^I_c, P^I_c \mid \Gamma_1, \beta(P,Q)^I_c, Q^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}\ \beta$$

$$\frac{\Gamma_1, \alpha(P,Q)^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}{\Gamma_1, \alpha(P,Q)^I_c, P^I_c, Q^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}\ \alpha$$

TaMeD

Quantificateurs

$$\frac{\Gamma_1, \gamma(x,P)^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}{\Gamma_1, P(x := X)^{I\cup\{X\}}_c, \gamma(x,P)^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}\ \gamma$$

$$\frac{\Gamma_1, \delta(x,P)^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}{\Gamma_1, P^I_c[\mathrm{x} := \mathtt{sko}(I)], \delta(x,P)^I_c \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}\ \delta$$

TaMeD

Réécriture

$$\frac{\Gamma_1, P_c[\zeta]_\omega \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}{\Gamma_1, P_c[\zeta]_\omega, P_{c'}[d]_\omega \mid \ldots \mid \Gamma_n \cdot \mathcal{C}}\ \text{rw}$$

si $g \to d \in \mathcal{R}$
et $c' = c \cup \{\zeta \stackrel{?}{=} g\}$

Fermeture

$$\frac{\Gamma_1, P_{c_1}, \neg P'_{c_2} \mid \ldots \mid \Gamma_n \cdot C}{(\Gamma_2 \mid \ldots \mid \Gamma_n) \cdot \mathcal{C} \cup c_1 \cup c_2 \cup \{P \stackrel{?}{=} P'\}}\ \texttt{closure}\ (\odot)$$

Premiers résultats (syntaxiques)

En *supposant* l'élimination des coupures possible, on démontre par transformation syntaxique :

Théorème (Correction)

$$\begin{aligned} \textit{Si} \quad & \textit{Tab}(\Gamma, \neg\Delta) \hookrightarrow \odot \\ \textit{alors} \quad & \Gamma \vdash_{\mathcal{RE}} \Delta \end{aligned}$$

Théorème (Complétude)

$$\begin{aligned} \textit{Si} \quad & \Gamma \vdash_{\mathcal{RE}} \Delta \quad (\textit{i.e.}\ \Gamma \vdash^{cf}_{\mathcal{RE}} \Delta) \\ \textit{alors} \quad & \textit{Tab}(\Gamma, \neg\Delta) \hookrightarrow \odot \end{aligned}$$

En bref

Difficultés

1. Les tableaux ont des *métavariables*, les séquents sont *clos*.
2. Les étapes de réécriture et de skolemisation (dynamique) sont entremêlées.

Solutions

- Pour 1, il suffit à priori de raisonner modulo un unificateur Θ des contraintes de tableaux.
- Pour 2, il faut utiliser des labels (choix d'une skolemisation externe).
- Pour 1 et 2, il faut démontrer, un certain de nombre de lemmes de commutation entre règles de tableau, l'unificateur, et des transformations des symboles de Skolem.

Développement systématique et complétude sémantique

$$\forall x P(x) \wedge (\neg P(c) \vee \neg Q(a))$$

$$\mathcal{R} = P(a) \rightarrow Q(a)$$

Priorité : $\alpha > \beta > \delta > (\gamma|\mathsf{rw})$

Règle :

$$\mathcal{C} = \emptyset$$

Développement systématique et complétude sémantique

$$\forall x P(x) \wedge (\neg P(c) \vee \neg Q(a)) \otimes$$
$$|$$
$$\forall x P(x)$$
$$|$$
$$\neg P(c) \vee \neg Q(a)$$

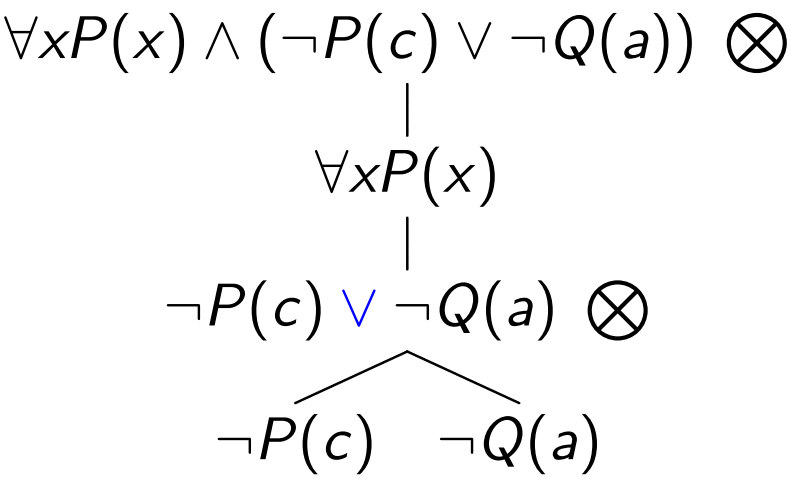
$\mathcal{R} = P(a) \rightarrow Q(a)$

Priorité : $\alpha > \beta > \delta > (\gamma|\mathsf{rw})$

Règle : $\dfrac{\alpha(A, B)}{A, B}$

$\mathcal{C} = \emptyset$

Développement systématique et complétude sémantique



$\mathcal{R} = P(a) \rightarrow Q(a)$

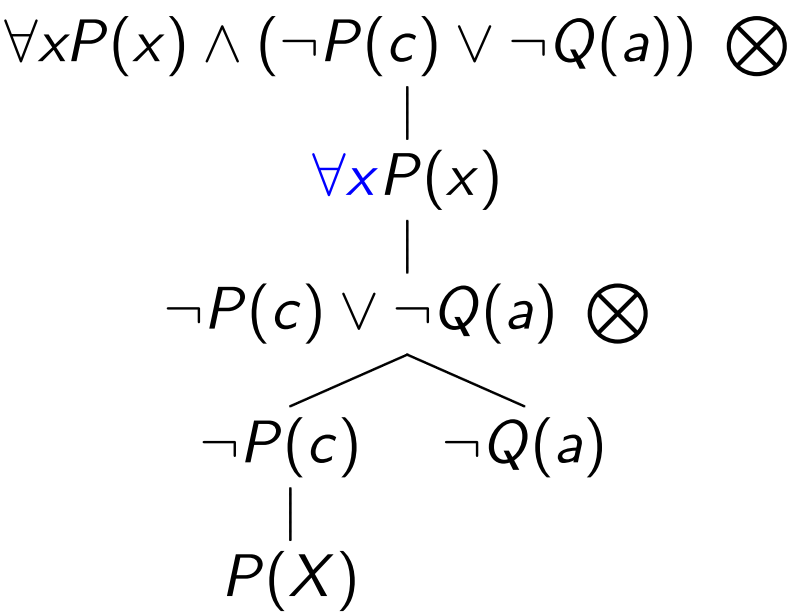
Priorité : $\alpha > \beta > \delta > (\gamma|\text{rw})$

Règle : $\dfrac{\beta(A, B)}{A \mid B}$

$\mathcal{C} = \emptyset$

	l	r
long	4	4
$\gamma >$ rw	t	t

Développement systématique et complétude sémantique



$\mathcal{R} = P(a) \rightarrow Q(a)$

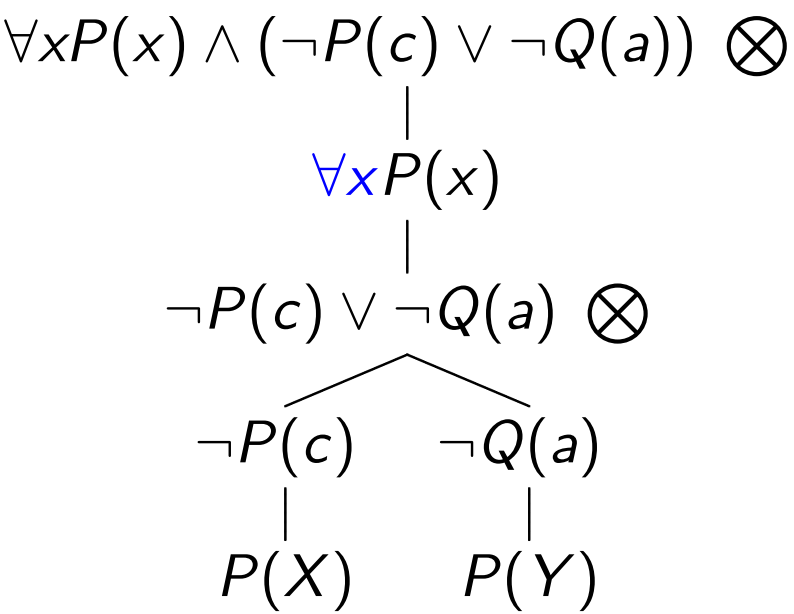
Priorité : $\alpha > \beta > \delta > (\gamma|\text{rw})$

Règle : $\dfrac{\gamma(x, A)}{A[x := X]}$

$\mathcal{C} = \emptyset$

	l	r
long	5	4
$\gamma >$ rw	f	t

Développement systématique et complétude sémantique



$\mathcal{R} = P(a) \rightarrow Q(a)$

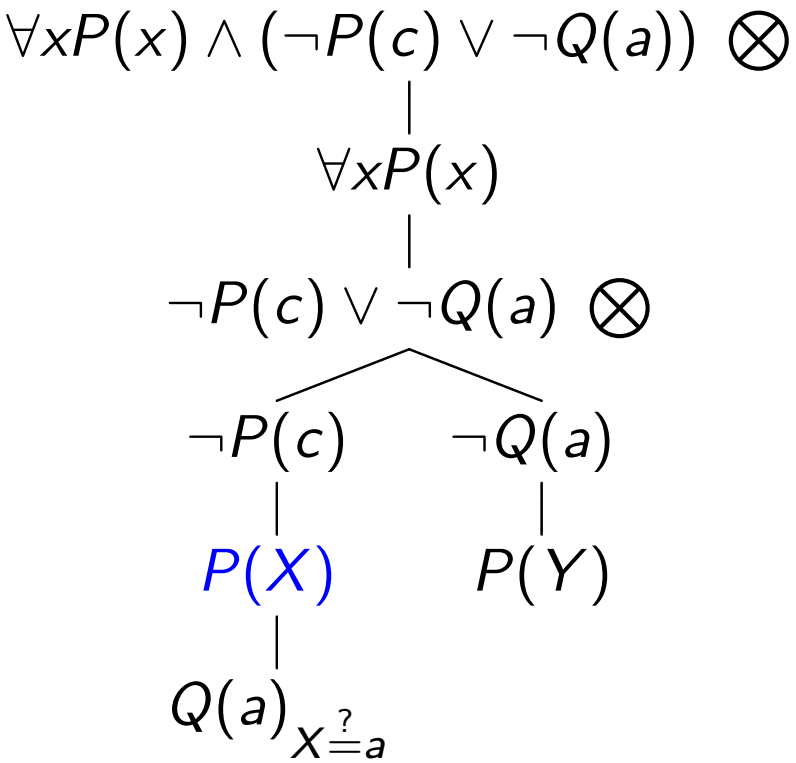
Priorité : $\alpha > \beta > \delta > (\gamma|\text{rw})$

Règle : $\dfrac{\gamma(x, A)}{A[x := X]}$

$\mathcal{C} = \emptyset$

	l	r
long	5	5
$\gamma >$ rw	f	f

Développement systématique et complétude sémantique



$\mathcal{R} = P(a) \rightarrow Q(a)$

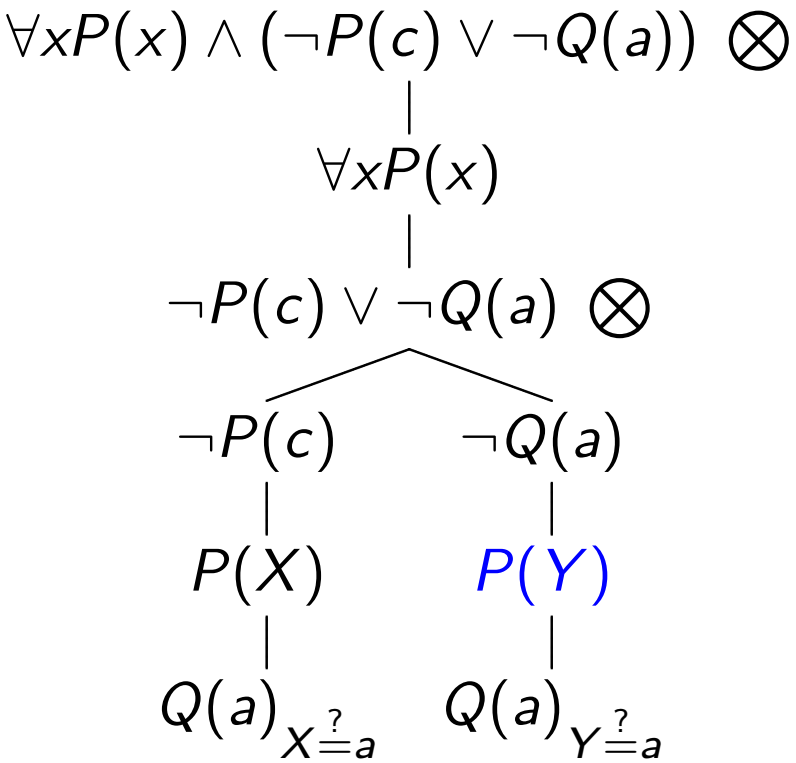
Priorité : $\alpha > \beta > \delta > (\gamma | \mathsf{rw})$

Règle : $\dfrac{P(\zeta)}{P(d)}$

$\mathcal{C} = \emptyset$

	l	r
long	6	5
$\gamma >$ rw	t	f

Développement systématique et complétude sémantique



$\mathcal{R} = P(a) \rightarrow Q(a)$

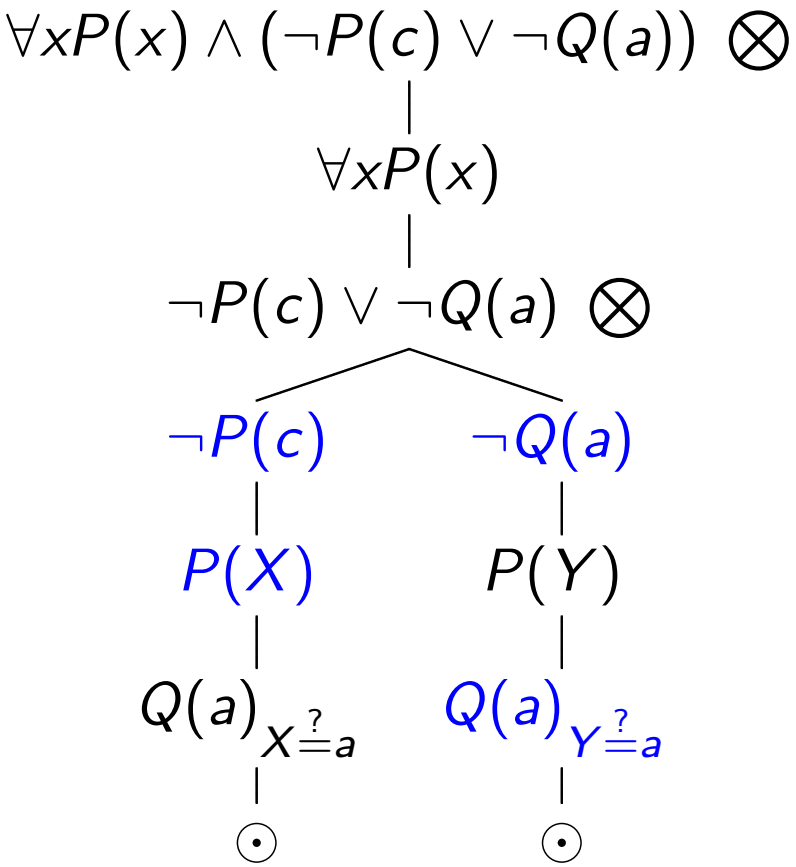
Priorité : $\alpha > \beta > \delta > (\gamma | \text{rw})$

Règle : $\dfrac{P(\zeta)}{P(d)}$

$\mathcal{C} = \emptyset$

	l	r
long	6	6
$\gamma >$ rw	t	t

Développement systématique et complétude sémantique



$\mathcal{R} = P(a) \rightarrow Q(a)$

Priorité : $\alpha > \beta > \delta > (\gamma | \text{rw})$

Règle : fermeture

$\mathcal{C} = \{X \stackrel{?}{=} c, Y \stackrel{?}{=} a\}$

	l	r
long	6	6
$\gamma >$ rw	t	t

Complétude sémantique

Théorème

Soit $\mathcal{R}$ un système de réécriture confluent et soit Γ un ensemble de propositions. Si le tableau systématique pour Γ n'est pas fermée, alors Γ a un modèle.

Valuations (Schütte)

Définition (Semi-valuation (valuation partielle))

Une interprétation est une fonction $V : \mathcal{P} \mapsto \{0, 1\}$ *dont le domaine est l'ensemble des propositions du langage. Elle est appelée* semi-*valuation (resp. valuation partielle) lorsque :*

- *si* $V(\neg P) = 0$ *alors (resp. ssi)* $V(P) = 1$
- *si* $V(\neg P) = 1$ *alors (resp. ssi)* $V(P) = 0$
- *si* $V(P \vee Q) = 0$ *alors (resp. ssi)* $V(P) = V(Q) = 0$
- *si* $V(P \vee Q) = 1$ *alors (resp. ssi)* $V(P) = 1$ *ou* $V(Q) = 1$
- *si* $V(P \wedge Q) = 0$ *alors (resp. ssi)* $V(P) = 0$ *ou* $V(Q) = 0$
- *...*

$\mathcal{R}$-valuations

Définition ($\mathcal{R}$-valuations)

Une semi-valuation (resp. valuation partielle) V est dite compatible avec un système de réécriture $\mathcal{R}$ si :

$$\begin{array}{ll} \textit{quand } P \equiv_{\mathcal{R}} Q & \textit{et } V(P) \textit{ est définie} \\ \textit{alors (resp. ssi)} & V(Q) = V(P). \end{array}$$

Modèles en déduction modulo : $\mathcal{R}$-modèles

Les $\mathcal{R}$-modèles sont des extensions des modèles booléens telles que pour tout couple de propositions :

$$\begin{array}{ll} \text{Si} & P \equiv_{\mathcal{R}} Q \\ \text{alors} & |P| = |Q|. \end{array}$$

Obtenir un modèle pose des probèmes

On commence par définir une semi-valuation V à partir d'une branche ouverte...

$\mathcal{R}$-semi-valuation ($\mathcal{V}$)

Si $P \to Q$ (par $g \to d$), $V(P)$ doit être définie quand $V(Q)$ l'est.

$\mathcal{R}$-valuation partielle($\tilde{V}$)

On veut avoir $\mathcal{V}(\forall x(A(x) \wedge B(x))) = 1$ si pour tout terme t on a $\mathcal{V}(A(t)) = 1$ et $\mathcal{V}(B(t)) = 1$.

Convergence de $\mathcal{R}$

Ne suffit pas pour la complétude (Dowek-Werner, Hermant) !

Classe de systèmes complets

Condition d'ordre

On considère des systèmes de réécriture confluents sur lesquels on peut définir un ordre bien fondé $\prec$ comme suit :

- si $P \rightarrow_{\mathcal{R}} Q$ alors $P \prec Q$,
- si P est une sous-formule de Q, alors $P \prec Q$.

Définition (Modèle pour une condition d'ordre)

$|.|_{\mathcal{R}}$ *est définie inductivement en suivant* $\prec$ *:*

- *si* P *est une proposition atomique normale,* $|P|_{\mathcal{R}} = \tilde{V}(P)$ *si* $\tilde{V}(P)$ *est définie et* $|P|_{\mathcal{R}} = 1$ *sinon.*
- *si* P *est un atome non normal, alors* $|P|_{\mathcal{R}} = |P \downarrow|_{\mathcal{R}}$.
- *si* P *est une proposition composée alors* $|P|_{\mathcal{R}}$ *est définie en fonction de ses sous-formules.*

Classe de systèmes complets

Condition de positivité

Une condition de positivité : si $g \longrightarrow d$ alors d a des occurrences d'atomes uniquement positives.

Définition (Modèle pour une condition de postitivté)

Soit $\mathcal{R}$ un système de réécriture positif. L'interprétation des formules est définie comme suit :

- *Si P est une proposition atomique,*
  - *si $\tilde{V}(P)$ est définie, alors $|P|_{\mathcal{R}} = \tilde{V}(P)$,*
  - *sinon $|P|_{\mathcal{R}} = 1$.*
- *Si P est une proposition composée, $|P|_{\mathcal{R}}$ est définie inductivement en fonction de l'interprétation de ses sous-formules.*

Classe de systèmes complets

Mixte

Les deux conditions ensemble : $\mathcal{R} = \mathcal{R}_{\succ} \cup \mathcal{R}_{+}$ et $\mathcal{R}_{+}$ est normal à droite pour $\mathcal{R}_{>}$.

Définition (Normalité droite)

Soit deux systèmes de réécriture R' et R. R' est normal à droite pour $\mathcal{R}$ si pour toute règle de réécriture propositionnelle $g \rightarrow d \ \in \mathcal{R}'$, toutes les instances des atomes de d par des substitutions $\mathcal{R}$-normales σ sont en forme normale pour $\mathcal{R}$.

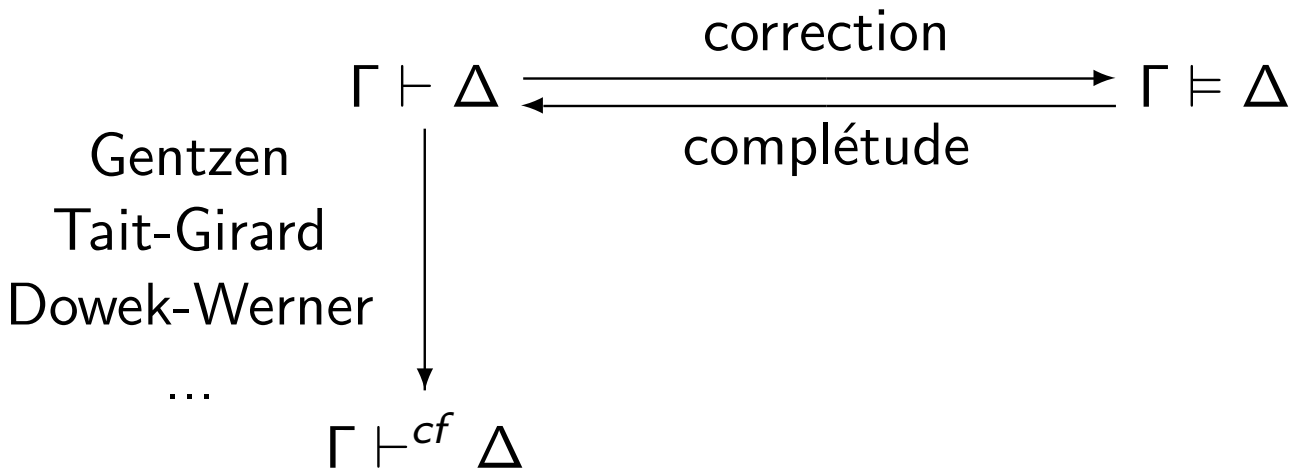
Élimination des coupures modulo

- La normalisation est parfois impossible (paradoxe de Russell modifié) :

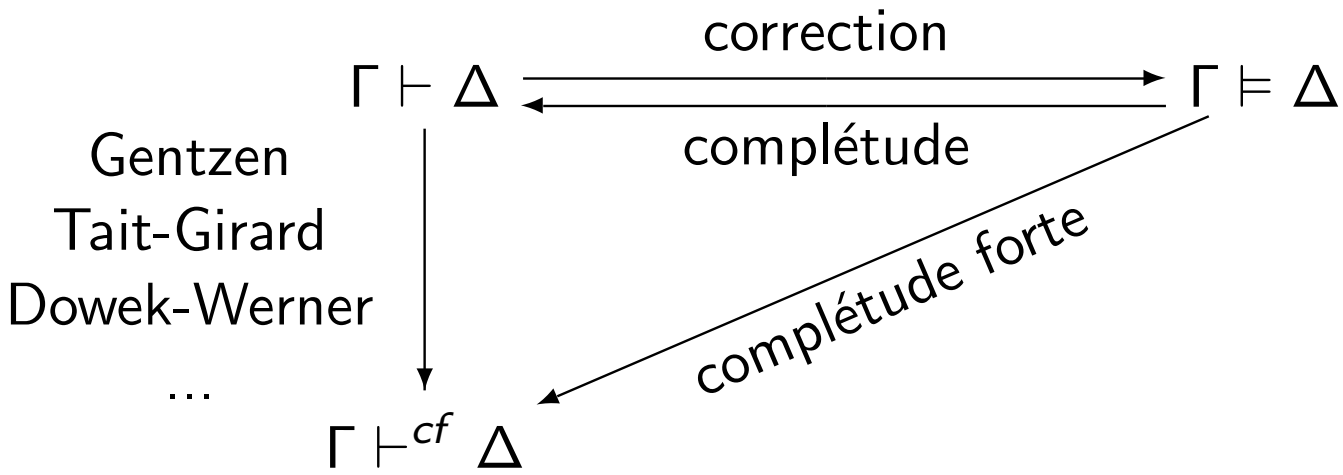
$$R \in R \longrightarrow \forall y\ (\forall x(y \in x \Rightarrow R \in x) \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

- On peut cependant prouver l'*admissibilité* de la règle de coupure par des moyens sémantiques.

Élimination(s) des coupures

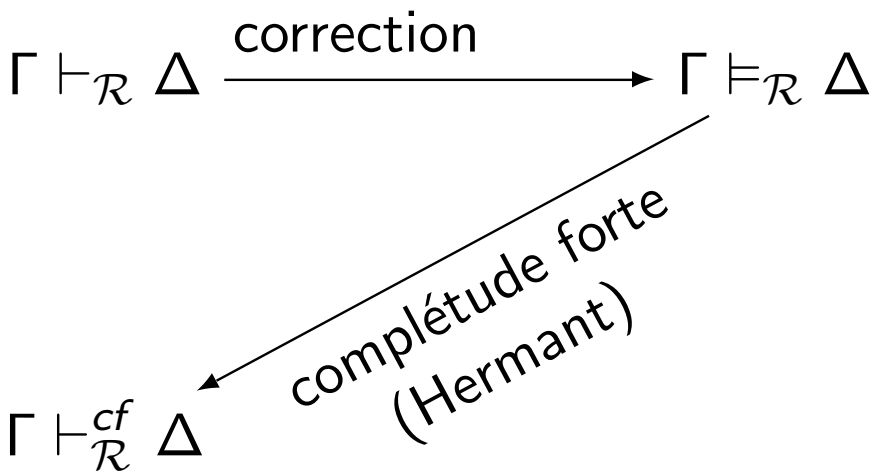


Élimination(s) des coupures

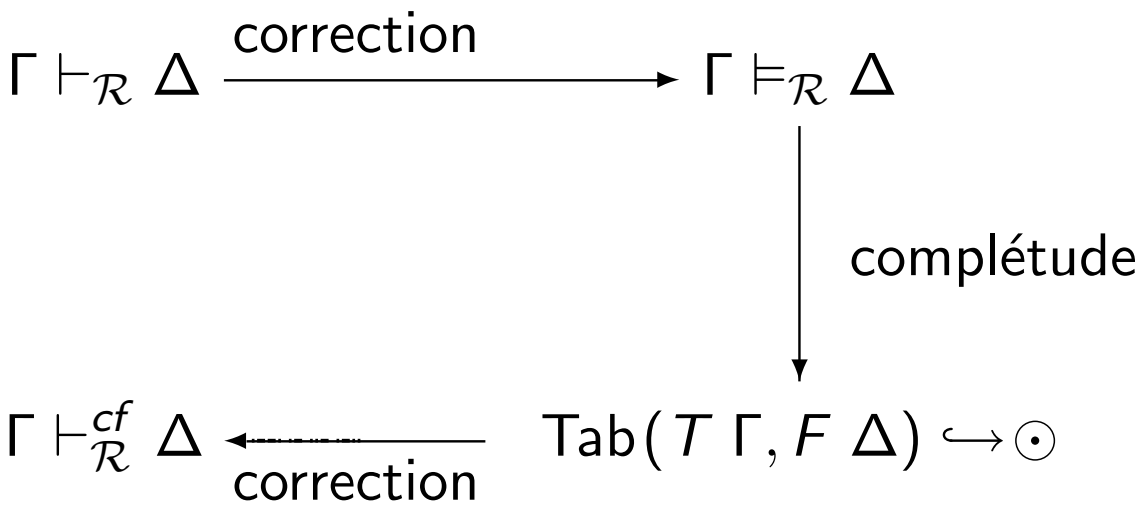


Élimination(s) des coupures

Cas le plus général en déduction modulo :



Élimination(s) des coupures



Contenu calculatoire de l'élimination des coupures

Revenons sur la règle "de Russell" :

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

- La méthode des tableaux modulo est complète pour ce système.
- Mais l'élimination des coupures ne peut pas être un algorithme de normalisation.
- C'est dans ce cas *grosso modo* la méthode des tableaux décrite.

Conclusion

Méthodes de preuves automatiques

Tableaux modulo pour :

- la logique classique
- la logique intuitionniste

Élimination des coupures

Extraction d'un contenu calculatoire (dans le cas intuitionniste) grâce aux tableaux modulo (travail en cours pour la logique classique)

Gain par les méthodes sémantiques

Identification de classes de systèmes de réécriture

Travaux en cours

- Implantantation dans Zenon (démonstrateur automatique fondé sur les tableaux, D. Doligez)
  - Extension vers plus de déduction modulo ;
  - Illustration par des exemples ;
  - Utilisation d'outils comme CiMe pour la partie réécriture (complétion, terminaison,...).
- Tableaux HOL modulo en utilisant :
  - $\text{HOL}_{\lambda\sigma}$;
  - TaMeD.
- ...

Merci de votre attention.