Théorie de la démonstration circulaire et application à la vérification

Amina Doumane

Congrès SIF

Université Paris 7– IRIF & ENS Cachan– LSV

1 février 2018

Logique

Crise des fondements en mathématique

Paradox de Russell

Soit $R = \{x \mid x \notin x\}$. On a $R \in R \Leftrightarrow R \notin R$.

Programme de Hilbert

- **Complétude:** est-ce que tout ce qui est "vrai" est "prouvable"?
- **Consistance:** est-ce qu'on peut prouver un énoncé et son contraire?
- **Decidabilité:** peut-on décider si un énoncé est valide ou pas?

Logique

Crise des fondements en mathématique

Paradox de Russell

Soit $R = \{x \mid x \notin x\}$. On a $R \in R \Leftrightarrow R \notin R$.

Programme de Hilbert

- Incomplétude de l'arithmétique du premier ordre [Gödel 31]
- **Consistance:** est-ce qu'on peut prouver un énoncé et son contraire?
- **Decidabilité:** peut-on décider si un énoncé est valide ou pas?

Logique

Crise des fondements en mathématique

Paradox de Russell

Soit $R = \{x \mid x \notin x\}$. On a $R \in R \Leftrightarrow R \notin R$.

Programme de Hilbert

- Incomplétude de l'arithmétique du premier ordre [Gödel 31]
- Les mathématiques ne peuvent pas montrer leur propre consistance [Gödel 31]
- **Decidabilité:** peut-on décider si un énoncé est valide ou pas?

Logique

Crise des fondements en mathématique

Paradox de Russell

Soit $R = \{x \mid x \notin x\}$. On a $R \in R \Leftrightarrow R \notin R$.

Programme de Hilbert

- Incomplétude de l'arithmétique du premier ordre [Gödel 31]
- Les mathématiques ne peuvent pas montrer leur propre consistance [Gödel 31]
- Indécidabilité de l'arithmétique du premier ordre [Tarski 35]

Logique

Crise des fondements en mathématique

Paradox de Russell

Soit $R = \{x \mid x \notin x\}$. On a $R \in R \Leftrightarrow R \notin R$.

Programme de Hilbert

- Incomplétude de l'arithmétique du premier ordre [Gödel 31]
- Les mathématiques ne peuvent pas montrer leur propre consistance [Gödel 31]
- Indécidabilité de l'arithmétique du premier ordre [Tarski 35]

Logique

Crise des fondements en mathématique

Paradox de Russell

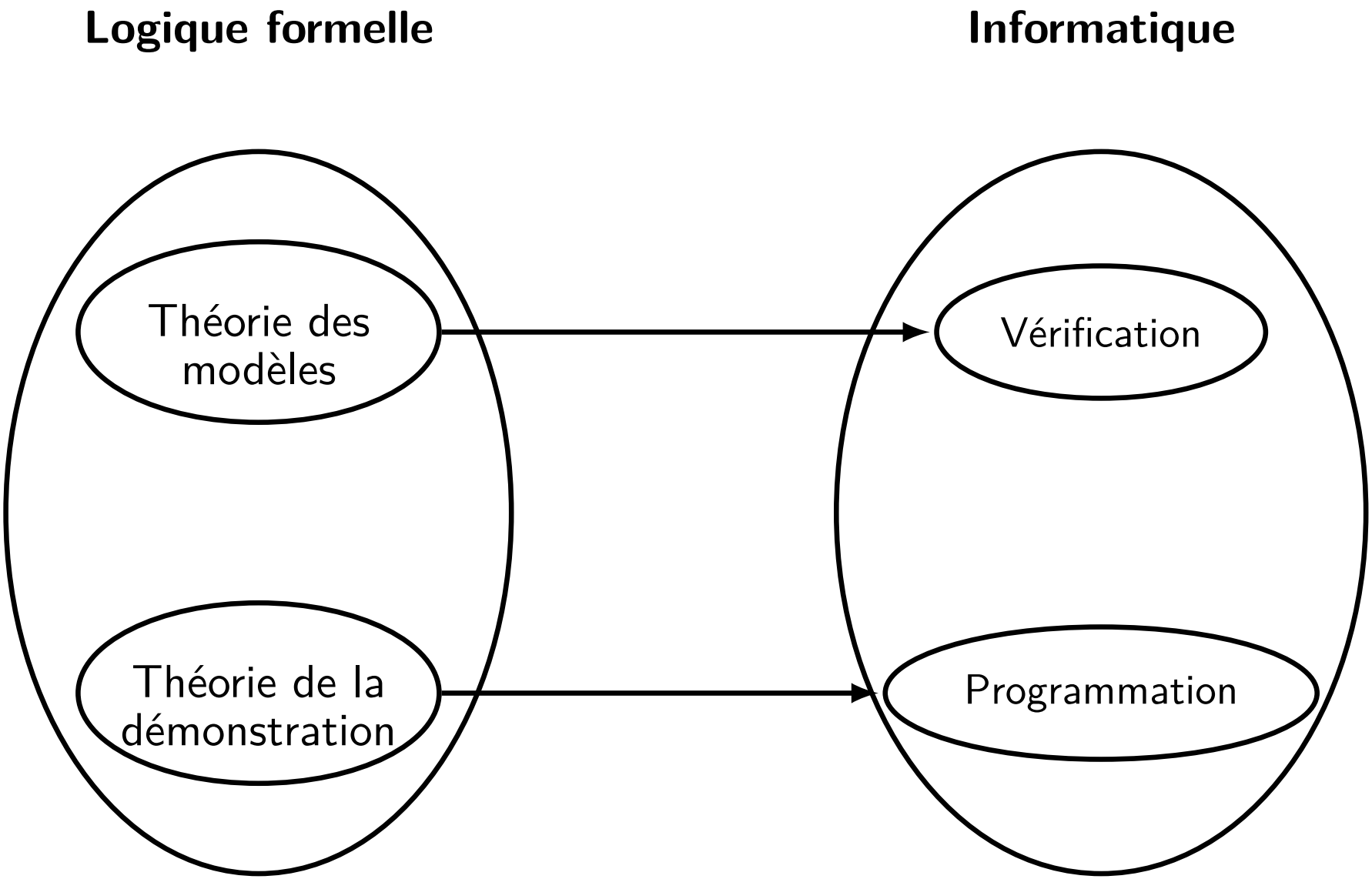
Soit $R = \{x \mid x \notin x\}$. On a $R \in R \Leftrightarrow R \notin R$.

Programme de Hilbert

- Incomplétude de l'arithmétique du premier ordre [Gödel 31]
- Les mathématiques ne peuvent pas montrer leur propre consistance [Gödel 31]
- Indécidabilité de l'arithmétique du premier ordre [Tarski 35]

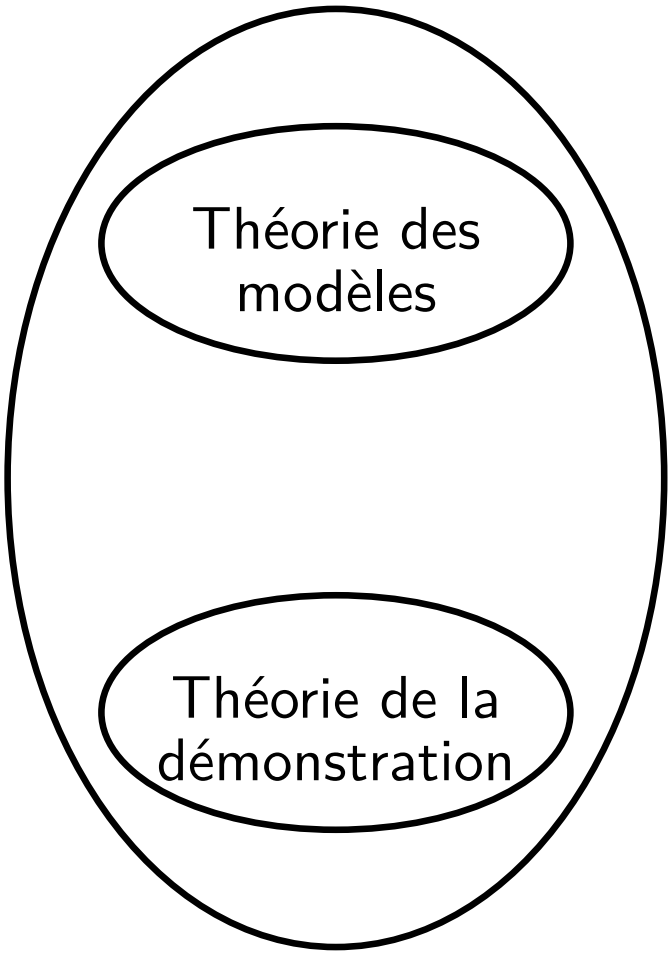
L'histoire aurait pu s'arrêter là...

Logique et informatique



Logique et informatique

Logique formelle



Formule φ

$p \to p \vee q, \qquad p \vee q \to p$

Validité $\models \varphi$

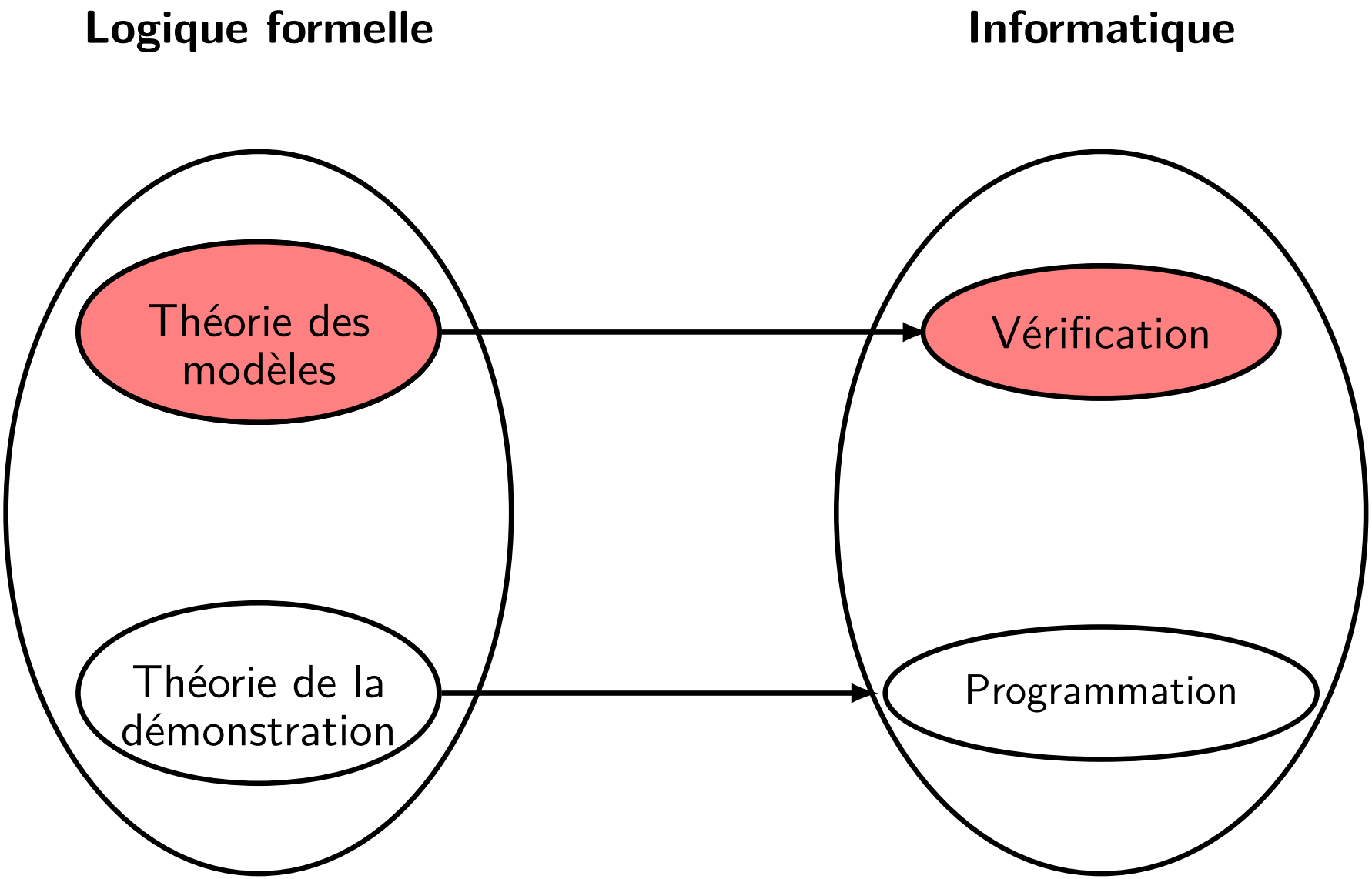
$\not\models p \vee q \to p \qquad (p = \bot, q = \top)$

$\models p \to p \vee q$

Prouvabilité $\vdash \varphi$

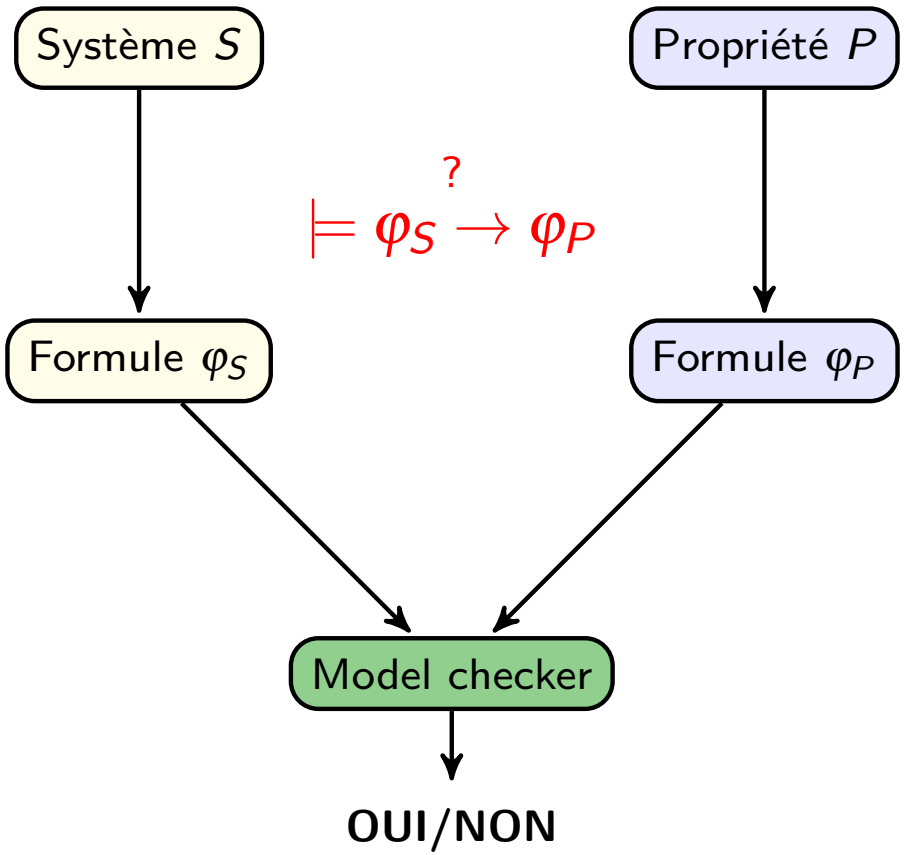
$$\dfrac{\dfrac{\dfrac{}{p \vdash p, q}\,(\mathrm{Ax})}{p \vdash p \vee q}\,(\vee)}{\vdash p \to p \vee q}\,(\to)$$

Logique et informatique

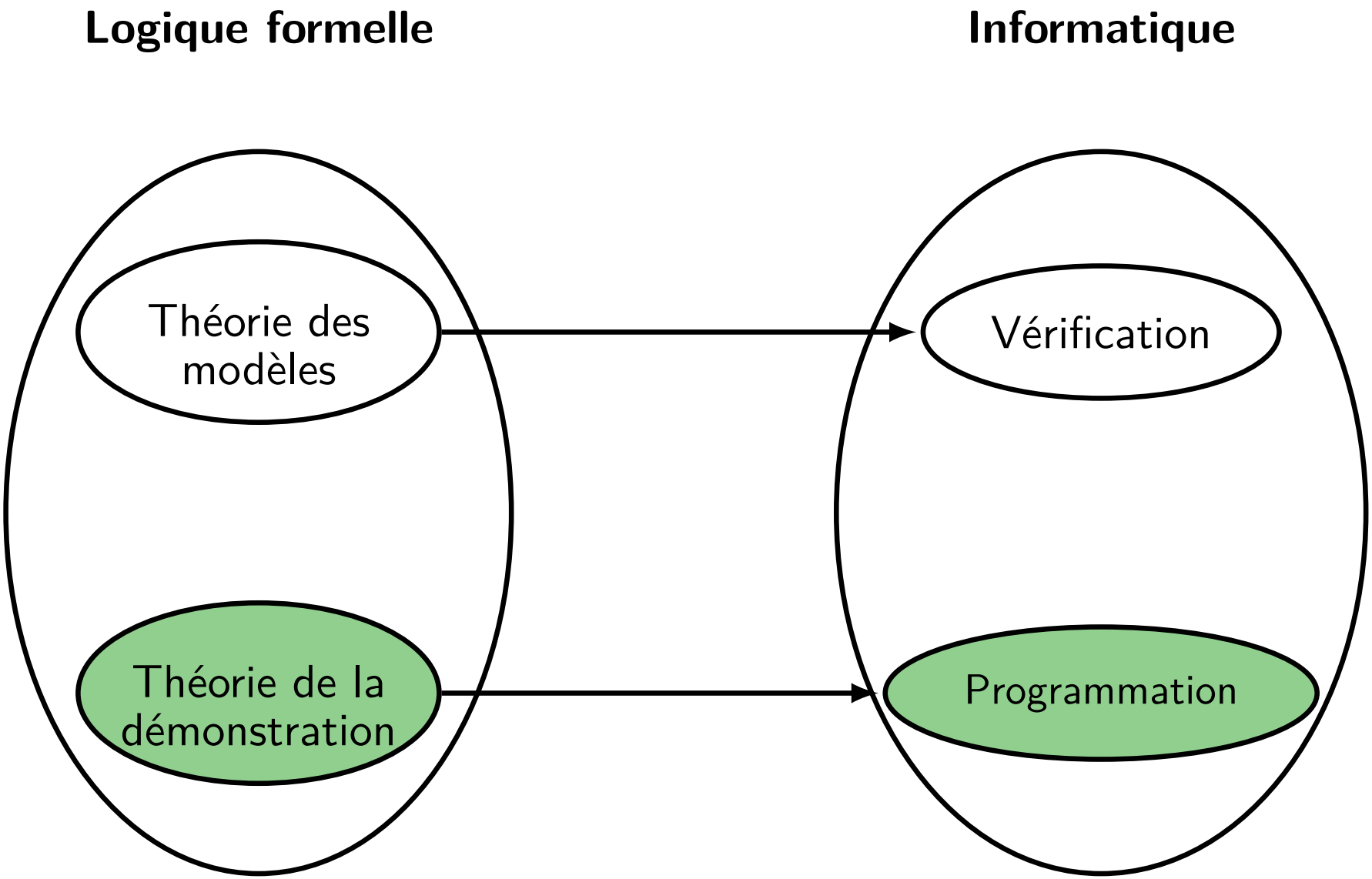


Logique et infomatique

Théorie de modèles et vérification



Logique et informatique



Logique et informatique

Théorie de la démonstration et programmation fonctionnelle

Correspondance de Curry-Howard

Théorie de la démonstration	**Programmation fonctionnelle**
• Preuves	• Programmes
• Formules	• Types
• Elimination des coupures	• Exécution

Théorie de la démonstration et programmation fonctionnelle

Règle de coupure

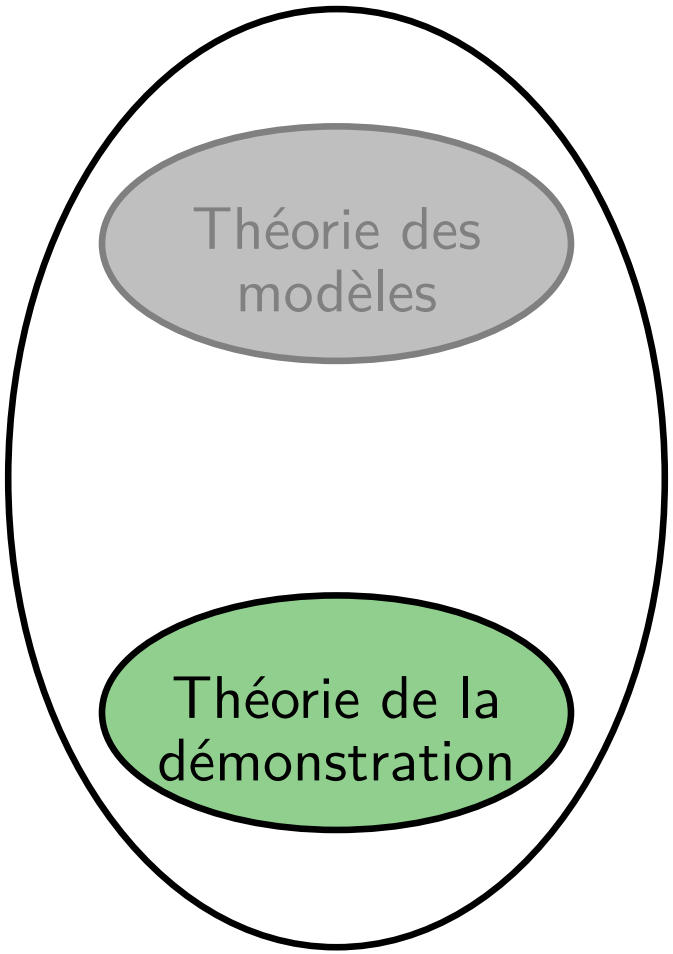
$$\frac{L \qquad L \Rightarrow T}{T}\ \text{(Coupure)}$$

Elimination des coupures (Gentzen 1934)

Toute preuve en logique classique peut être transformée en une preuve sans coupures.

Logique

Logique formelle



Preuves circulaires

Preuves usuelles

Enoncé T

Preuves usuelles

Axiome_1 Axiome_2

Enoncé T

Preuves usuelles

Axiome_1 Axiome_2

E

Enoncé T

Preuves usuelles

$$\dfrac{\dfrac{\text{Axiome}_1 \qquad \text{Axiome}_2}{E} \qquad \text{Axiome}_3}{\vdots}$$

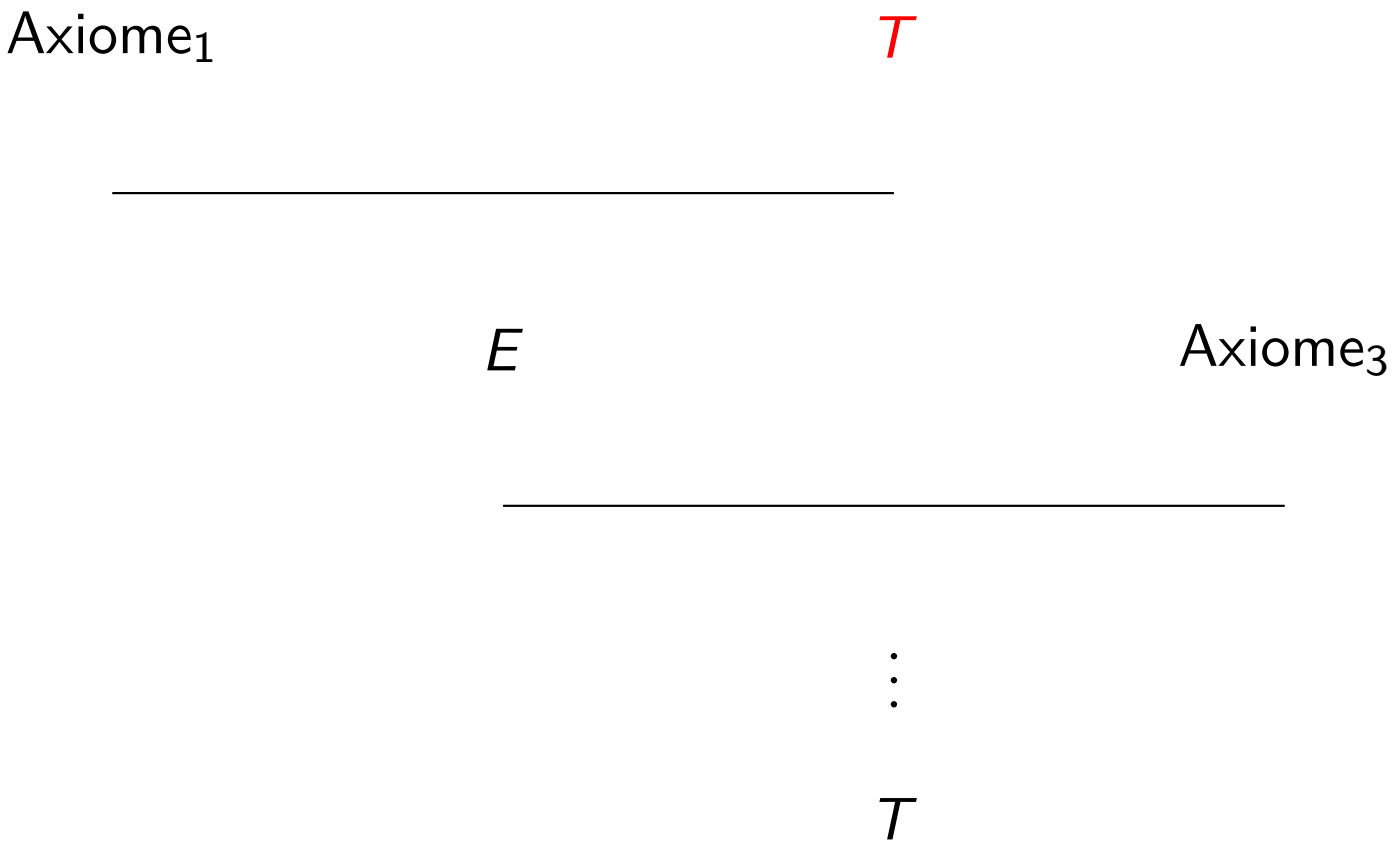
Enoncé T

Preuves circulaires

$$\dfrac{\dfrac{\text{Axiome}_1 \qquad T}{E} \qquad \text{Axiome}_3}{\vdots}$$

$$T$$

Preuves circulaires



Attention aux contradictions!

Preuves circulaires

Ma thèse

Les preuves circulaires ont un réel statut de preuve théorique
elles peuvent être appliquées à
d'autres domaines comme la vérification formelle.

Preuves circulaires

Ma thèse

Les preuves circulaires ont un réel statut de preuve théorique
elles peuvent être appliquées à
d'autres domaines comme la vérification formelle.

Partie I

- Elimination des coupures [Baelde, D., Saurin '16]
- Focalisation [Baelde, D., Saurin '16]
- Sémantique [Baelde, D., Saurin '15]

Preuves circulaires

Ma thèse

Les preuves circulaires ont un réel statut de preuve théorique
elles peuvent être appliquées à
d'autres domaines comme la vérification formelle.

Partie I

- Elimination des coupures [Baelde, D., Saurin '16]
- Focalisation [Baelde, D., Saurin '16]
- Sémantique [Baelde, D., Saurin '15]

Partie II

- Complétude constructive pour le μ-calcul linéaire.

[D., Baelde, Hirschi, Saurin '16] [D. '17]

Preuves circulaires

Ma thèse

Les preuves circulaires ont un réel statut de preuve théorique
elles peuvent être appliquées à
d'autres domaines comme la vérification formelle.

Partie I

- Elimination des coupures [Baelde, D., Saurin '16]
- Focalisation [Baelde, D., Saurin '16]
- Sémantique [Baelde, D., Saurin '15]

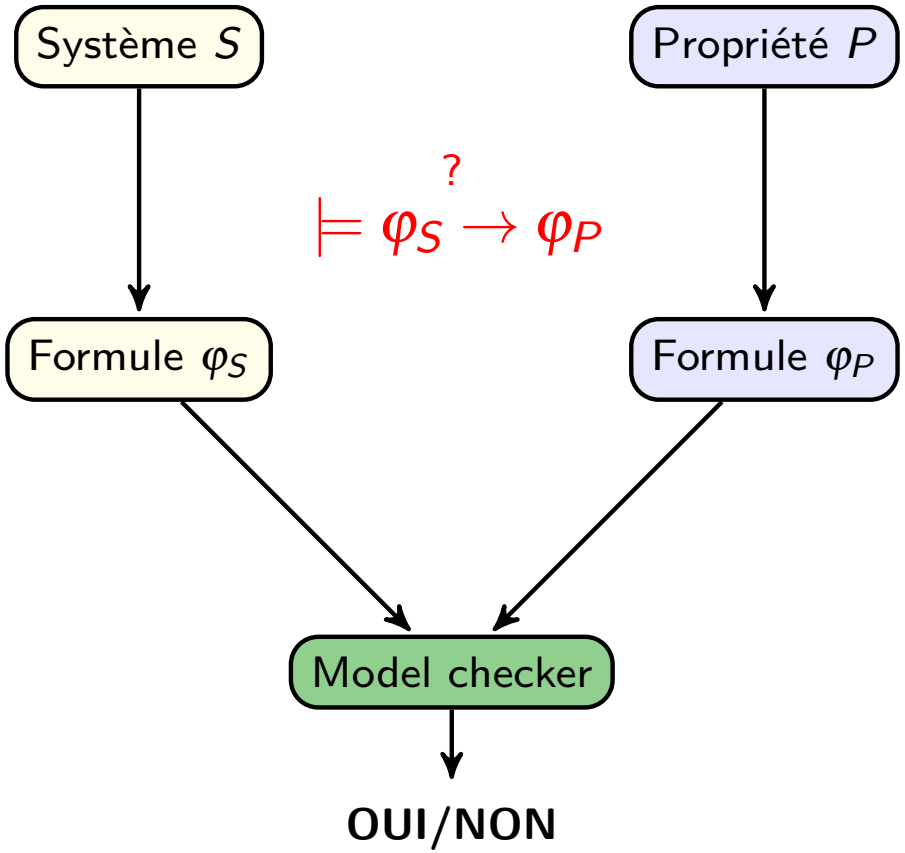
Partie II

- Complétude constructive pour le μ-calcul linéaire.

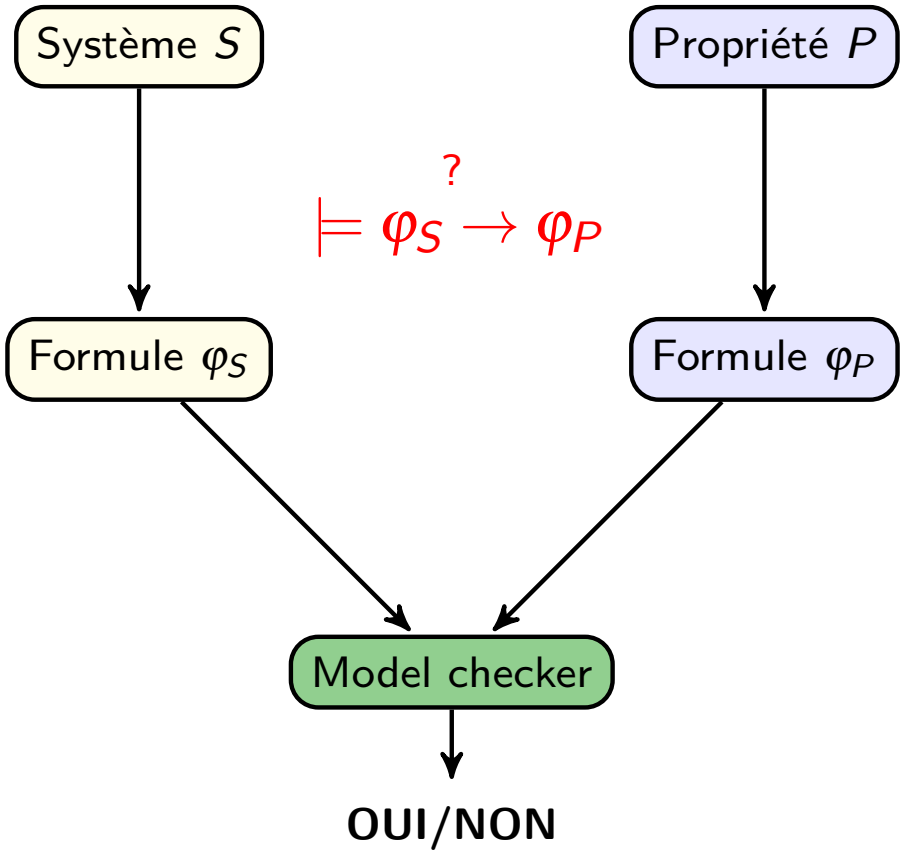
[D., Baelde, Hirschi, Saurin '16] [D. '17]

Complétude constructive pour le μ-calcul linéaire

Paradigme de vérification

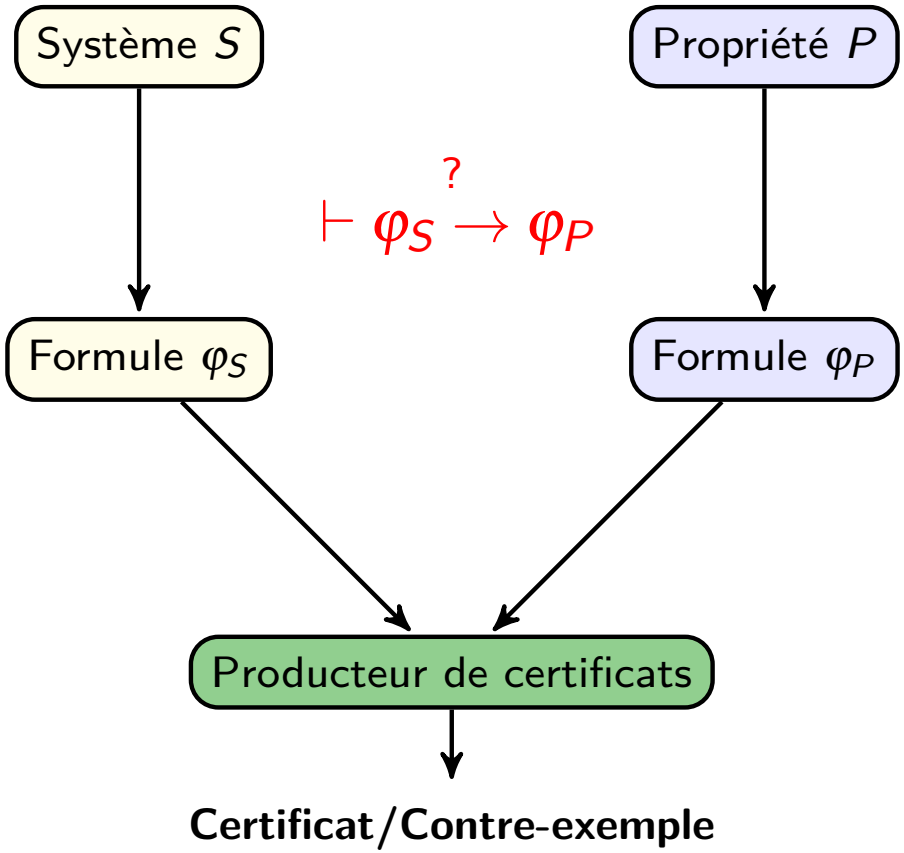


Paradigme de vérification



- Besoin de certificats.
- Les preuves sont des bons candidats.

Paradigme altérnative de vérification



- Besoin de certificats.
- Les preuves sont des bons candidats.

Complétude du μ-calcul

Theorem (Kaivola 1995)

Si une formule du μ-calcul est valide alors elle est prouvable dans le système de Kozen.

Complétude du μ-calcul

Theorem (Kaivola 1995)

Si une formule du μ-calcul est valide alors elle est prouvable dans le système de Kozen.

La preuve de Kaivola n'est pas constructive et ne donne pas de moyen de construire une preuve d'une formule valide.

Complétude du μ-calcul

Theorem (Kaivola 1995)

Si une formule du μ-calcul est valide alors elle est prouvable dans le système de Kozen.

La preuve de Kaivola n'est pas constructive et ne donne pas de moyen de construire une preuve d'une formule valide.

Theorem 12.2, Part II

Si une formule du μ-calcul est valide alors on peut en **construire** une preuve dans le système de Kozen.

Idée de la preuve de complétude

Trouver un sous-ensemble $\mathscr{C} \subseteq \mathscr{F}$ tel que:

1. Toute formule valide de $\mathscr{C}$ est prouvable.
2. Pour toute formule valide φ, il existe une formule valide ψ de $\mathscr{C}$ tel que $\psi \to \varphi$ est prouvable.

$$\dfrac{\dfrac{(1)}{\psi} \qquad \dfrac{(2)}{\psi \Rightarrow \varphi}}{\varphi}\ \text{coupure}$$

Idée de la preuve de complétude

Trouver un sous-ensemble $\mathscr{C} \subseteq \mathscr{F}$ tel que:

1. Toute formule valide de $\mathscr{C}$ est prouvable.
2. Pour toute formule valide φ, il existe une formule valide ψ de $\mathscr{C}$ tel que $\psi \to \varphi$ est prouvable.

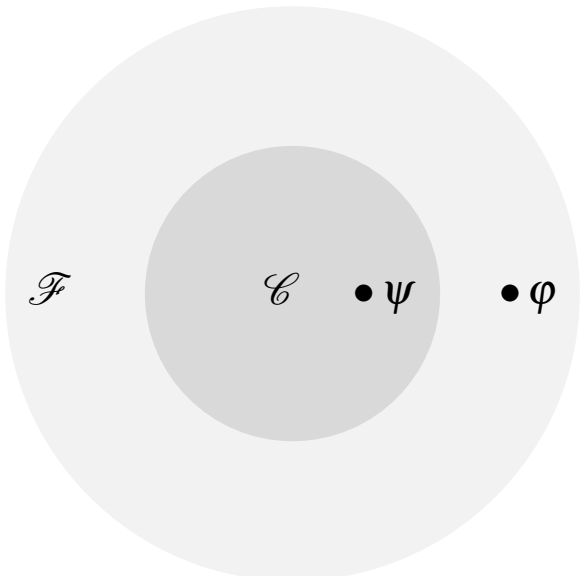
$$\dfrac{\dfrac{(1)}{\psi} \qquad \dfrac{(2)}{\psi \Rightarrow \varphi}}{\varphi}\ \text{coupure}$$

Idée de la preuve de complétude

Trouver un sous-ensemble $\mathscr{C} \subseteq \mathscr{F}$ tel que:

1. Toute formule valide de $\mathscr{C}$ est prouvable.
2. Pour toute formule valide φ, il existe une formule valide ψ de $\mathscr{C}$ tel que $\psi \to \varphi$ est prouvable.

$$\dfrac{\dfrac{(1)}{\psi} \qquad \dfrac{(2)}{\psi \Rightarrow \varphi}}{\varphi}\ \text{coupure}$$

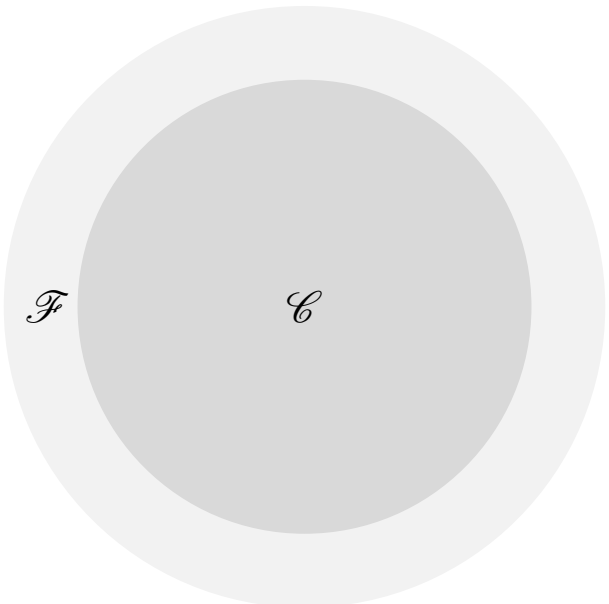


Idée de la preuve de complétude

Trouver un sous-ensemble $\mathscr{C} \subseteq \mathscr{F}$ tel que:

1. Toute formule valide de $\mathscr{C}$ est prouvable.
2. Pour toute formule valide φ, il existe une formule valide ψ de $\mathscr{C}$ tel que $\psi \to \varphi$ est prouvable.

$$\dfrac{\dfrac{(1)}{\psi} \qquad \dfrac{(2)}{\psi \Rightarrow \varphi}}{\varphi}\ \text{coupure}$$



Si $\mathscr{C}$ est trop grand, (1) devient aussi difficile que la complétude.

Idée de la preuve de complétude

Trouver un sous-ensemble $\mathscr{C} \subseteq \mathscr{F}$ tel que:

1. Toute formule valide de $\mathscr{C}$ est prouvable.
2. Pour toute formule valide φ, il existe une formule valide ψ de $\mathscr{C}$ tel que $\psi \to \varphi$ est prouvable.

$$\dfrac{\dfrac{(1)}{\psi} \qquad \dfrac{(2)}{\psi \Rightarrow \varphi}}{\varphi}\ \text{coupure}$$

Si $\mathscr{C}$ est trop petit, le problème (2) devient difficile.

Idée de la preuve de complétude

Trouver un sous-ensemble $\mathscr{C} \subseteq \mathscr{F}$ tel que:

1. Toute formule valide de $\mathscr{C}$ est prouvable.
2. Pour toute formule valide φ, il existe une formule valide ψ de $\mathscr{C}$ tel que $\psi \to \varphi$ est prouvable.

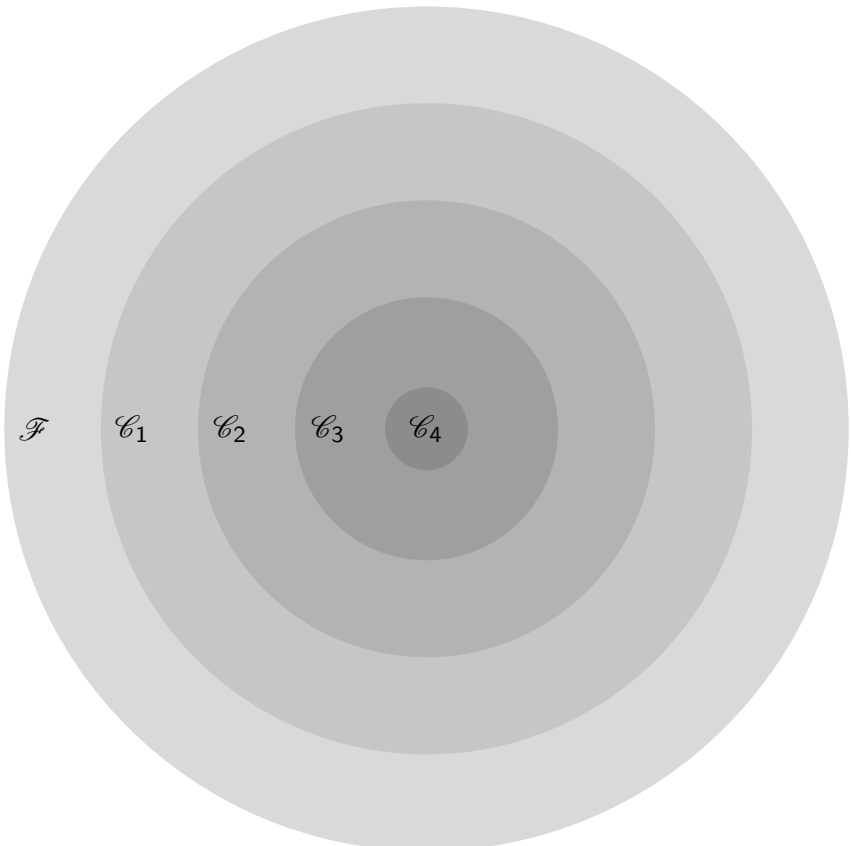
$$\dfrac{\dfrac{(1)}{\psi} \qquad \dfrac{(2)}{\psi \Rightarrow \varphi}}{\varphi}\ \text{coupure}$$

La preuve de Kaivola utilise une classe de ce type.

Notre idée pour la complétude

Pourquoi ne pas introduire plusieurs classes au lieu d'une?

$$\frac{\vdash \psi_4 \qquad \psi_4 \vdash \psi_3 \qquad \psi_3 \vdash \psi_2 \qquad \psi_2 \vdash \psi_1 \qquad \psi_1 \vdash \varphi}{\vdash \varphi}\ \texttt{(cut)}$$



Notre preuve de complétude

Comment trouver ces classes ?

Notre preuve de complétude

Comment trouver ces classes ?

Trois difficultés

Alternance de $\wedge$ et $\vee$

Alternance de μ et ν

Présence de $\vee$

Notre preuve de complétude

Comment trouver ces classes ?

Trois difficultés	**Théorie des automates**
Alternance de $\wedge$ et $\vee$	Alternance
Alternance de μ et ν	Conditions de parité
Présence de $\vee$	Non-déterminisme

Notre preuve de complétude

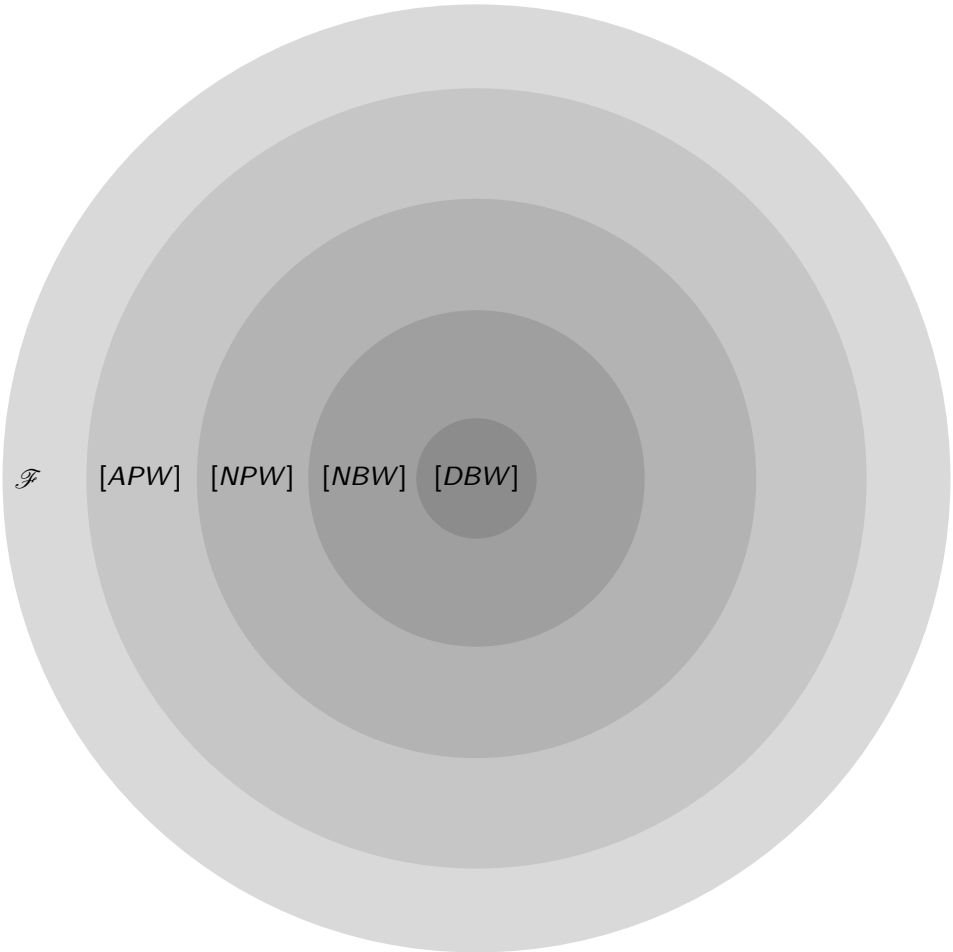
Comment trouver ces classes ?

Trois difficultés	**Théorie des automates**
Alternance de $\wedge$ et $\vee$	Alternance
Alternance de μ et ν	Conditions de parité
Présence de $\vee$	Non-déterminisme

En théorie des automates, on sait résoudre ces difficultés.
$\rightarrow$ Importer ces idées en utilisant les **preuves circulaires**.

Notre preuve de complétude

$$\frac{\vdash [\mathscr{D}] \qquad [\mathscr{D}] \vdash [\mathscr{B}] \qquad [\mathscr{B}] \vdash [\mathscr{P}] \qquad [\mathscr{P}] \vdash [\mathscr{A}] \qquad [\mathscr{A}] \vdash \varphi}{\vdash \varphi}\ (\text{Cut})$$



Et les preuves circulaires dans tout cela?

Utilisée comme un système de preuve intermédiaire:

$$\textbf{Validité} \xrightarrow{(1)} \textbf{Preuves circulaires} \xrightarrow{(2)} \textbf{Preuves de Kozen}$$

(1) Implémenter les algorithmes de transformation d'automates pour la recherche de preuve

(2) Algorithme de transformation de preuves circulaires vers preuves usuelles.

Conclusion

Conclusion

Ma thèse

Les preuves circulaires ont un réel statut de preuve théorique
elles peuvent être appliqués à
d'autres domaines comme la vérification formelle.

Et après?

Faire accepter les preuves circulaires comme mode de preuve standard dans la communauté.

Conclusion

Ma thèse

Les preuves circulaires ont un réel statut de preuve théorique
elles peuvent être appliqués à
d'autres domaines comme la vérification formelle.

Et après?

Faire accepter les preuves circulaires comme mode de preuve standard dans la communauté.

Merci pour votre attention!