

Recherche automatique de preuves

(une introduction)

Fête de la science 2018

Aurore Alcolei
ENS Lyon, LIP

Recherche automatique de preuves

1 Qu'est-ce qu'une preuve ?

2 Dédution automatique

À l'école

Données

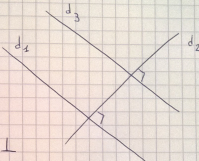
$$d_1 \perp d_2$$

$$d_2 \perp d_3$$

Propriété

Si deux droites sont \perp
à une même droite alors elles
sont \parallel entre elles

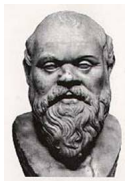
Conclusion

$$d_1 \parallel d_3$$


$$\frac{A \vdots A \implies C}{C}$$

Sagesse grecque

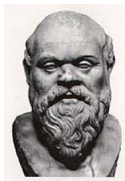
Tous les hommes sont mortels,
Socrate est un homme,
donc Socrate est mortel.



$$\begin{array}{c} A \\ \vdots \\ \hline A \quad A \implies C \\ C \end{array}$$

Sagesse grecque

Tous les hommes sont mortels,
Socrate est un homme,
donc Socrate est mortel.

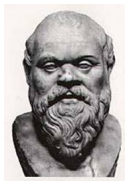


$$\begin{array}{c} A \\ \vdots \\ A \end{array} \quad A \implies C$$

$$C$$

Sagesse grecque

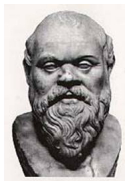
Tous les hommes sont mortels,
Socrate est un homme,
donc Socrate est mortel.



$$\begin{array}{c} A \\ \vdots \\ A \end{array} \quad A \implies C \quad \frac{\quad}{C}$$

Sagesse grecque

Tous les hommes sont mortels,
Socrate est un homme,
donc Socrate est mortel.

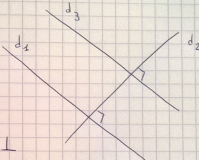


$$\begin{array}{c} A \\ \vdots \\ \hline A \implies C \\ C \end{array}$$

(Retour) À l'école

Données

$$d_1 \perp d_2$$

$$d_2 \perp d_3$$


Propriété

Si deux droites sont \perp
à une même droite alors elles
sont \parallel entre elles

Conclusion

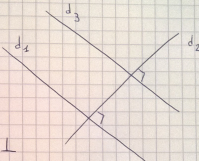
$$d_1 \parallel d_3$$

$$\frac{A}{\begin{array}{c} \vdots \\ \bar{A} \end{array}} \quad \frac{A \implies C}{C}$$

(Retour) À l'école

Données

$$d_1 \perp d_2$$

$$d_2 \perp d_3$$


Propriété

Si deux droites sont \perp
à une même droite alors elles
sont \parallel entre elles

Conclusion

$$d_1 \parallel d_3$$

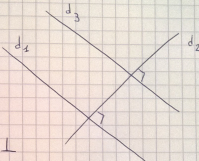
$$\frac{\begin{matrix} A \\ \vdots \\ \bar{A} \end{matrix} \quad A \implies C}{C}$$

H
 \vdots
 H

(Retour) À l'école

Données

$$d_1 \perp d_2$$

$$d_2 \perp d_3$$


Propriété

Si deux droites sont \perp
à une même droite alors elles
sont \parallel entre elles

Conclusion

$$d_1 \parallel d_3$$

$$\begin{array}{c} A \\ \vdots \\ \frac{A \quad A \Rightarrow C}{C} \end{array}$$

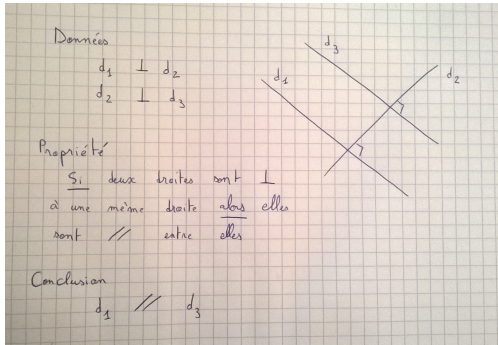
H

⋮

H

$$\frac{A \quad A \Rightarrow C}{C}$$

(Retour) À l'école



$$\begin{array}{c}
 A \quad B \\
 \vdots \\
 \hline
 A \& B \quad A \& B \Rightarrow C \\
 C
 \end{array}$$

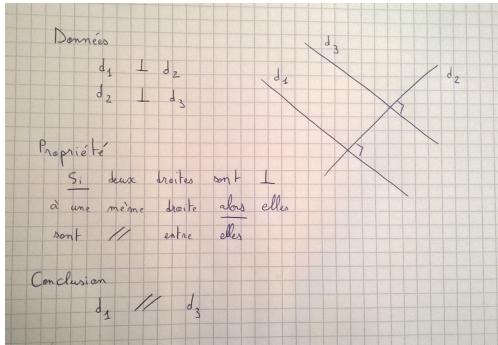
H

:

H

$$\begin{array}{c}
 A \quad A \Rightarrow C \\
 \hline
 C
 \end{array}$$

(Retour) À l'école



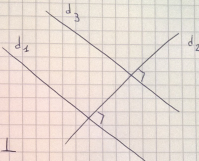
$$\frac{A \quad B \quad \vdots \quad A \& B}{A \& B \Rightarrow C} \quad C$$

$$\frac{H \quad A \quad B \quad \vdots \quad H \quad A \& B}{A \Rightarrow C} \quad C$$

(Retour) À l'école

Données

$$d_1 \perp d_2$$

$$d_2 \perp d_3$$


Propriété

Si deux droites sont \perp
à une même droite alors elles
sont \parallel entre elles

Conclusion

$$d_1 \parallel d_3$$

$$\begin{array}{c} A \quad B \\ \vdots \quad \vdots \\ \hline A \quad B \\ \hline A \& B \quad A \& B \implies C \\ \hline C \end{array}$$

H

:

H

$$\begin{array}{c} A \quad B \\ \hline A \& B \quad A \quad A \implies C \\ \hline C \end{array}$$

L'enquête Corse

- Tous mes amis aiment soit les comédies, soit les policiers
- L'enquête Corse est une comédie
- L'enquête Corse est un policier
- Je peux donc aller voir ce film avec tous mes amis.



$$\begin{array}{cc}
 [A] & [B] \\
 & \vdots \quad \vdots \\
 A \text{ ou } B & \begin{array}{c} \underline{C} \quad \underline{C} \\ C \end{array}
 \end{array}$$

L'enquête Corse

- Tous mes amis aiment **soit** les comédies, **soit** les policiers
- L'enquête Corse est une comédie
- L'enquête Corse est un policier
- Je peux donc aller voir ce film avec tous mes amis.



$$\begin{array}{cc}
 [A] & [B] \\
 & \vdots \quad \vdots \\
 A \text{ ou } B & \begin{array}{c} \underline{C} \quad \underline{C} \\ C \end{array}
 \end{array}$$

L'enquête Corse

- Tous mes amis aiment **soit** les comédies, **soit** les policiers
- L'enquête Corse est une comédie
- L'enquête Corse est un policier
- Je peux donc aller voir ce film avec tous mes amis.



$H_1, H_2 \dots H_n$

$$\begin{array}{cc}
 [A] & [B] \\
 & \vdots \quad \vdots \\
 A \text{ ou } B & \begin{array}{c} \underline{C} \quad \underline{C} \\ C \end{array}
 \end{array}$$

Plus de preuves

$$\begin{array}{c}
 A \\
 \vdots \\
 A
 \end{array}$$

$$\frac{A \quad A \implies C}{C}$$

$$\frac{A \quad B}{A \& B}$$

$$\frac{A \text{ ou } B \quad \begin{array}{c} [A] \\ \vdots \\ C \end{array} \quad \begin{array}{c} [B] \\ \vdots \\ C \end{array}}{C}$$

Plus de preuves

$$\begin{array}{c} A \\ \vdots \\ A \end{array} \qquad \frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \Rightarrow B} \qquad \frac{A \quad A \Rightarrow C}{C}$$

$$\frac{A \quad B}{A \& B}$$

$$\frac{A \text{ ou } B \quad \begin{array}{c} [A] \quad [B] \\ \vdots \\ C \end{array} \quad \begin{array}{c} \vdots \\ C \end{array}}{C}$$

Plus de preuves

$$\begin{array}{c} A \\ \vdots \\ A \end{array} \qquad \frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \implies B} \qquad \frac{A \quad A \implies C}{C}$$

$$\frac{A \quad B}{A \& B}$$

$$\frac{A \& B}{A}$$

$$\frac{A \& B}{B}$$

$$\frac{A \text{ ou } B \quad \begin{array}{c} [A] \quad [B] \\ \vdots \\ C \end{array} \quad \begin{array}{c} \vdots \\ C \end{array}}{C}$$

Plus de preuves

$$\begin{array}{c} A \\ \vdots \\ A \end{array} \qquad \frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \Rightarrow B} \qquad \frac{A \quad A \Rightarrow C}{C}$$

$$\frac{A \quad B}{A \& B}$$

$$\frac{A \& B}{A}$$

$$\frac{A \& B}{B}$$

$$\frac{A}{A \text{ ou } B}$$

$$\frac{B}{A \text{ ou } B}$$

$$\frac{A \text{ ou } B \quad \begin{array}{c} [A] \quad [B] \\ \vdots \\ C \end{array} \quad \begin{array}{c} \vdots \\ C \end{array}}{C}$$

Plus de preuves : Dédution Naturelle

$$\begin{array}{c} A \\ \vdots \\ A \end{array} \qquad \frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \Rightarrow B} \qquad \frac{A \quad A \Rightarrow C}{C}$$

$$\frac{A \quad B}{A \& B}$$

$$\frac{A \& B}{A}$$

$$\frac{A \& B}{B}$$

$$\frac{A}{A \text{ ou } B}$$

$$\frac{B}{A \text{ ou } B}$$

$$\frac{A \text{ ou } B \quad \begin{array}{c} [A] \quad [B] \\ \vdots \\ C \end{array} \quad \begin{array}{c} \vdots \\ C \end{array}}{C}$$

Automatisation

- Vérification :

Question 1 : Ma preuve est-elle **correcte** ?

- Dédution automatique :

Question 2 : En supposant H_1, \dots, H_k , **puis-je** déduire A ?

Automatisation

- Vérification :

Question 1 : Ma preuve est-elle **correcte** ?

✓ Facile !

- Dédution automatique :

Question 2 : En supposant H_1, \dots, H_k , **puis-je** déduire A ?

Algorithme de déduction

$$\frac{A \quad B}{A \& B}$$

Hypothèses : H_1, \dots, H_n

But : $A \& B$

Algorithme :

- 1 Rechercher une preuve pour A avec H_1, \dots, H_n
- 2 Rechercher une preuve pour B avec H_1, \dots, H_n
- 3 Dire oui si on a réussi dans les deux cas (et non sinon !)

Algorithme de déduction

$$\frac{A}{A \text{ ou } B}$$

$$\frac{B}{A \text{ ou } B}$$

Hypothèses : H_1, \dots, H_n

But : $A \text{ ou } B$

Algorithme :

- 1 Rechercher une preuve pour A avec H_1, \dots, H_n
- 2 Rechercher une preuve pour B avec H_1, \dots, H_n
- 3 Dire oui si on a réussi dans un des deux cas (et non sinon)

Algorithme de déduction

$$\frac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A \implies B}$$

Hypothèses : H_1, \dots, H_n

But : $A \implies B$

Algorithme :

- 1 Rechercher une preuve pour B avec H_1, \dots, H_n, A
- 2 Dire oui si on a réussi (et non sinon)

Algorithme de déduction

A
 \vdots
 A

Hypothèses : H_1, \dots, H_n

But : C

Algorithme :

- 1 Rechercher C dans H_1, \dots, H_n
- 2 Dire oui si on l'a trouvé, sinon ...

Algorithme de déduction

$$\frac{A \& B}{A}$$

$$\frac{A \& B}{B}$$

Hypothèses : $A \& B, H_1, \dots, H_n$

But : C

Algorithme :

- 1 Rechercher une preuve de C dans A, B, H_1, \dots, H_n
- 2 Dire oui si on a réussi, sinon ...

Algorithme de déduction

$$\frac{A \text{ ou } B \quad \begin{array}{c} [A] \\ \vdots \\ C \end{array} \quad \begin{array}{c} [B] \\ \vdots \\ C \end{array}}{C}$$

Hypothèses : $A \text{ ou } B, H_1, \dots, H_n$

But : C

Algorithme :

- ① Rechercher une preuve de C dans A, H_1, \dots, H_n
- ② Rechercher une preuve de C dans B, H_1, \dots, H_n
- ③ Dire oui si on a réussi dans les deux cas, sinon ...

Algorithme de déduction

$$\frac{A \quad A \implies C}{C}$$

Hypothèses : H_1, \dots, H_n

But : C

Algorithme :

- 1 Rechercher une preuve de A dans H_1, \dots, H_n
- 2 Dire oui si on a réussi... et non sinon !

Algorithme de déduction

Théorème 1 : L'algorithme **termine**.

Théorème 2 : L'algorithme est **correcte**.

Algorithme de déduction

Théorème 1 : L'algorithme **termine**.

Lemme : Si il existe une preuve de A avec les hypothèses H_1, \dots, H_k , alors il existe une preuve **sans détour** de A sous les mêmes hypothèses.

Théorème 2 : L'algorithme est **correcte**.

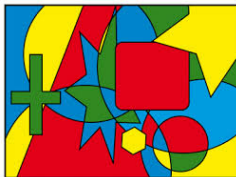
Pour aller plus loin


- ✓ Vérification.
- ✓ Dédution automatique.

Mais...

- Très grande complexité
- Impossible sur des logiques plus complexes

Le meilleurs des deux mondes ? Assistants de preuves.



→ Preuve du théorème des quatre couleurs (2005) utilisant COQ .

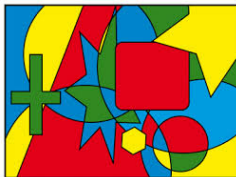
Pour aller plus loin

- ✓ Vérification.
- ✓ Dédution automatique.

Mais...

- Très grande complexité
- Impossible sur des logiques plus complexes

Le meilleurs des deux mondes ? Assistants de preuves.



→ Preuve du théorème des quatre couleurs (2005) utilisant COQ 🧑🏫.

Merci !

Sagesse grecque ?

Toutes les vaches sont mortelles,
Socrate est mortel,
donc Socrate est une vache.

$$\frac{A \quad C \implies A}{C}$$

Sagesse grecque ?

Toutes les vaches sont mortelles,
Socrate est mortel,
donc Socrate est une vache.

$$\frac{A \quad C \implies A}{C}$$

Ce système n'est pas **cohérent**.