Introduction

Plan du chapitre 1

Objectifs

Savoir faire

- Raisonner clairement, se faire comprendre
- Démontrer proprement, (se) convaincre

Outils fondamentaux

- *Logique* : formules, déduction naturelle, récurrence(s)
- *Langage des ensembles* : fonctions, relations, structures, ordres

Motivations

Les objets informatiques sont complexes

- *Structures de données :* organisation d'informations
- *Programmes :* calculs d'informations
- *Il faut constamment raisonner*, expérimenter ne suffit pas
- Vous allez devoir prouver la correction de vos programmes

L'informatique est une science

- *Étude* du *sens mathématique* des programmes
- *Quantification* des ressources nécessaires à leur exécution

Repères historiques : à retenir

Quelques résultats surprenants

Certaines tâches sont irréalisables par des programmes

Outils fondamentaux de l'informatique

Nés au moins 10 ans avant le premier ordinateur

Développements poussés de la logique formelle

Bien plus importants pour l'informaticien que pour le mathématicien

- en mathématiques, il suffit de savoir qu'*en principe* un raisonnement pourrait être rédigé complètement comme une suite de formules ; en pratique on fait confiance aux confrères ;
- en informatique :
  - clarification de notions essentielles pour exprimer calculs et structures de données
  - raisonnements compliqués, nécessité de *vérifier* (voire produire) *automatiquement* ceux qui sont critiques
    $\Rightarrow$ ils doivent être *formels*

La route (1)

Premier raisonnement

- *Une route verglassée est glissante.*
- *Une route glissante est dangereuse.*
- *Donc une route verglassée est dangereuse.*

La route (2)

Second raisonnement

On ajoute une hypothèse.

- *Une route verglassée est glissante.*
- *Une route glissante est dangereuse.*
- *Une route enneigée est glissante.*
- *Donc une route verglassée ou enneigée est dangereuse.*
  En effet, si elle est verglassée, elle est glissante ; si elle est enneigée elle est glissante ; elle est donc glissante dans les deux cas, et donc dangereuse.

La route (3)

Troisième raisonnement

Mêmes hypothèses et même conclusion que pour le second.

- *Une route verglassée est glissante.*
- *Une route glissante est dangereuse.*
- *Une route enneigée est glissante.*
- *Donc une route verglassée ou enneigée est dangereuse.*
  En effet, si elle est verglassée, elle est glissante, donc dangereuse ; si elle est enneigée elle est glissante, donc dangereuse ;
  elle est donc dangereuse dans les deux cas, ce qui signifie qu'une route verglassée ou enneigée est dangereuse.

La route (4)

Quatrième raisonnement

Mêmes hypothèses mais conclusion différente.

- *Une route verglassée est glissante.*
- *Une route glissante est dangereuse.*
- *Une route enneigée est glissante.*
- *Donc une route verglassée et enneigée est dangereuse.*
  En effet, si elle est verglassée et enneigée, elle est verglassée, donc glissante, donc dangereuse.
  Variante (autre raisonnement)
  si elle est verglassée et enneigée, elle est enneigée, donc glissante, donc dangereuse.

Ingrédients

On a des *énoncés*.

Certains énoncés sont admis : *hypothèses*.

Certains énoncés sont déduits des autres :
inférence = règle « de prémisses vers conclusion »

Les déductions s'emboîtent les unes dans les autres :
les conclusions de certaines étapes de déduction
servent de prémisse aux étapes suivantes.
déduction = emboîtement d'inférences

Comment présenter des déductions ?

Présentation usuelle : texte informel

Exemples : voir planches précédentes

Avantage : facile à lire (aucun apprentissage)

Inconvénients :

- pas toujours facile à écrire
- ellipses (parties implicites), risques d'omissions

Présentation formelle, et précise : fractions

Inférence simple

$$\frac{\text{prémisse}_1 \qquad \text{prémisse}_2}{\text{conclusion}}$$

Déduction = emboîtement d'inférences = arbre de preuve

$$\frac{\dfrac{\text{prémisse}_1 \qquad \text{prémisse}_2}{\text{conclusion}_1} \qquad \dfrac{\text{prémisse}_3 \qquad \text{prémisse}_4}{\text{conclusion}_2}}{\text{conclusion}_3}$$

Intermède : arbres

Intuitivement

- une *feuille* est un arbre
  un *nœud* relié à des arbres déjà construits est un nouvel arbre
  il n'y a pas d'autre moyen de former des arbres
- chaque nœud ou feuille est muni d'une *étiquette*
  étiquette = nom, formule logique, ou autre

En informatique : objets couramment manipulés

- Représentables en machine (ex. pointeurs ou tableaux)
- cf. fin INF 121

Mathématiquement

- Définition précise possible à l'aide de fonctions

Exemple d'inférence formelle

$$\frac{\textit{une route verglassée est glissante} \qquad \textit{une route glissante est dangereuse}}{\textit{une route verglassée est dangereuse}}$$

C'est bien une inférence, mais ce n'est pas une inférence logique : comment justifier le passage des prémisses à la conclusion ?

Il faut analyser la *structure logique* des énoncés tels que *une route verglassée est glissante*

Décomposition logique des énoncés

Simplification provisoire : il n'y a qu'une route, *la route*

Énoncés élémentaires (atomiques)

- *la route est verglassée*
- *la route est enneigée*
- *la route est glissante*
- *la route est dangereuse*

Exemple

une route verglassée est glissante
la route est verglassée $\Rightarrow$ *la route est glissante*

$\Rightarrow$ est un *connecteur logique* qui se lit : *implique*

Exercice

$$\frac{\textit{une route verglassée est glissante} \qquad \textit{une route glissante est dangereuse}}{\textit{une route verglassée est dangereuse}}$$

Reformuler cet arbre en posant :

rv = *la route est verglassée* re = *la route est enneigée*
rg = *la route est glissante* rd = *la route est dangereuse*

Justifier

- TRI : transitivité de l'implication

La route (2)

Si la route est verglassée, elle est glissante ; si elle est enneigée elle est glissante ; elle est donc glissante dans les deux cas, et donc dangereuse ; il s'ensuit qu'une route verglassée ou enneigée est dangereuse

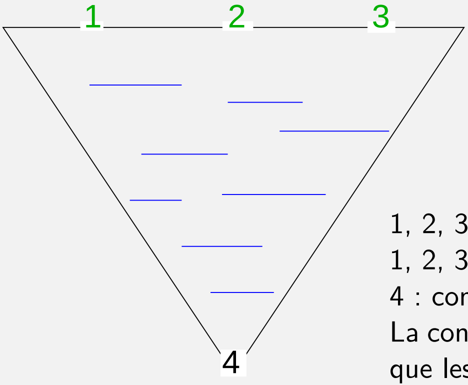
Nouveau *connecteur logique :* $\vee$ qui se lit *ou*

$$\dfrac{\dfrac{\mathsf{rv} \Rightarrow \mathsf{rg} \qquad \mathsf{re} \Rightarrow \mathsf{rg}}{(\mathsf{rv} \vee \mathsf{re}) \Rightarrow \mathsf{rg}}\,\mathrm{OGI} \qquad \mathsf{rg} \Rightarrow \mathsf{rd}}{(\mathsf{rv} \vee \mathsf{re}) \Rightarrow \mathsf{rd}}\,\mathrm{TRI}$$

Justification

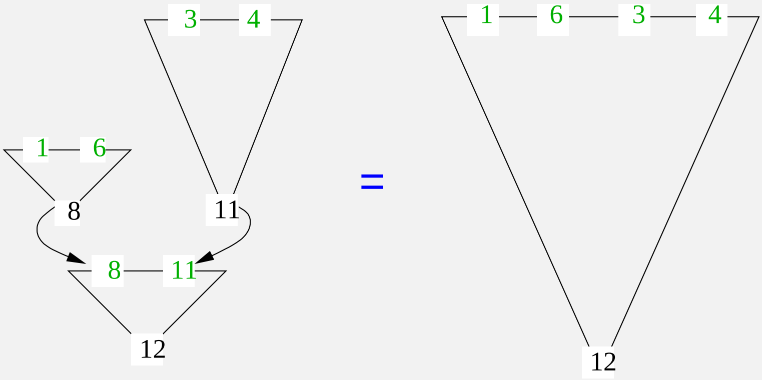
- OGI : Ou à Gauche d'une Implication
- TRI : transitivité de l'implication

Forme générale d'un arbre de preuve

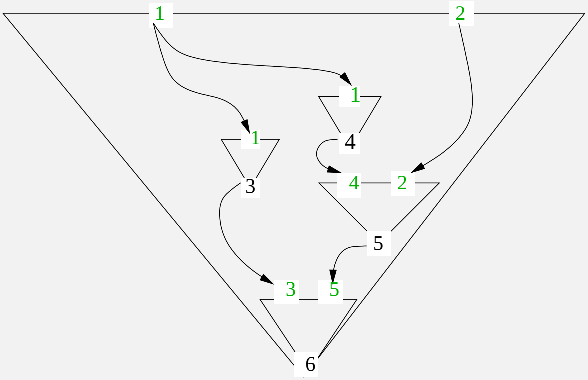


1, 2, 3, 4 : énoncés
1, 2, 3 : hypothèses
4 : conclusion
La conclusion est bonne pourvu que les hypothèses le soient

Assemblage d'arbres de preuve



Imbrication d'arbres de preuve



La route (3)

Si la route est verglassée, elle est glissante, donc dangereuse ;
si elle est enneigée elle est glissante, donc dangereuse ;
elle est donc dangereuse dans les deux cas, ce qui signifie qu'une route verglassée ou enneigée est dangereuse.

Justification

- OGI : Ou à Gauche d'une Implication
- TRI : transitivité de l'implication

La route (4)

Si la route est verglassée et enneigée, elle est verglassée, donc glissante, donc dangereuse.

Nouveau *connecteur logique :* $\wedge$ qui se lit *et*

$$\dfrac{\dfrac{\dfrac{}{(\mathsf{rv} \wedge \mathsf{re}) \Rightarrow \mathsf{rv}}\,\mathrm{EGI}_1 \qquad \mathsf{rv} \Rightarrow \mathsf{rg}}{(\mathsf{rv} \wedge \mathsf{re}) \Rightarrow \mathsf{rg}}\,\mathrm{TRI} \qquad \mathsf{rg} \Rightarrow \mathsf{rd}}{(\mathsf{rv} \wedge \mathsf{re}) \Rightarrow \mathsf{rd}}\,\mathrm{TRI}$$

Justification

- EGI : Et à Gauche d'une Implication
- TRI : transitivité de l'implication

La route (4), variantes

Si la route est verglassée et enneigée, elle est enneigée, donc glissante, donc dangereuse.

Terrain de la logique : bien délimité

Connecteurs logiques

- conjonction $\wedge$
- disjonction $\vee$
- implication $\Rightarrow$
- autres connecteurs dérivés, par ex. l'équivalence $\Leftrightarrow$

Décomposition fonctionnelle et prédicative des énoncés

langage permettant de construire systématiquement des énoncés (en nombre arbitrairement grand) : *plus tard*

Quantification

énoncés portant sur tous les individus ou sur un individu
ex. la route / une route / toute route : *plus tard*

Hors logique

L'interprétation des énoncés (ou de leurs constituants élémentaires) dans la réalité.
Lois de la physique, de la chimie, de la biologie, du gruyère, de l'économie...

À retenir

Arbres de preuve (ou de démonstration)

Une démonstration est essentiellement un arbre

- formé à partir de règles d'inférence et d'hypothèses
- chaque nœud est une règle d'inférence
- chaque feuille est une hypothèse
- la racine est le théorème démontré

Sélection d'un jeu de règles d'inférence

TRI, OGI, EGI, correctes mais ad-hoc
$\rightarrow$ abandonnées dans la suite au profit d'un système bien étudié, la

$\boxed{\text{déduction naturelle}}$

Déduction naturelle

Plan du chapitre 2

Plan du chapitre 2 (cont.)

Plan du chapitre 2 (cont.)

Égalité et raisonnement équationnel

- Règles
- Propriétés de l'égalité
- Exemples
- Présentation de preuves équationnelles

Récurrence sur les entiers

Énoncés logiques, formules

On se donne des énoncés élémentaires (ou atomiques) p, q, r, etc.
On construit d'autres énoncés en reliant par un connecteur $\Rightarrow$, $\wedge$, $\vee$

- des *énoncés élémentaires* :
  - $p \Rightarrow q$,
  - $p \wedge q$,
  - $p \vee q$,
  - etc.
- des énoncés *déjà construits* :
  - $(p \wedge q) \wedge p$, $(p \wedge q) \Rightarrow p$,
  - $(p \wedge q) \Rightarrow (p \vee r)$,
  - etc.

Règles d'inférence en déduction naturelle

Chaque règle d'inférence porte sur un seul connecteur
Pour chaque connecteur $*$, on donne

- les règles canoniques qui permettent d'inférer une nouvelle formule $A * B$ à partir des sous-formules A et B : *règles d'introduction*
- les règles canoniques qui permettent d'utiliser une formule $A * B$ à partir des sous-formules A et B : *règles d'élimination*

Connecteur le plus simple : la conjonction $\wedge$

$$\frac{A \qquad B}{A \wedge B}\ \wedge\mathrm{I} \qquad \frac{A \wedge B}{A}\ \wedge\mathrm{E}_1 \qquad \frac{A \wedge B}{B}\ \wedge\mathrm{E}_2$$

Remarque : A et B représentent des énoncés quelconques (en prenant des exemplaires particuliers, on obtient une déclinaison possible de chaque règle)

Exemple : commutativité de ∧

But : démontrer $B \wedge A$ à partir de $A \wedge B$

Démonstration

$$\dfrac{\dfrac{A \wedge B}{B}\,\wedge E_2 \qquad \dfrac{A \wedge B}{A}\,\wedge E_1}{B \wedge A}\,\wedge I$$

NB.

- l'ordre des prémisses est important
- la même hypothèse peut être utilisée un nombre quelconque de fois (y compris 0)

Commutativité de $\wedge$, textuellement

Démonstration textuelle

- supposons $A \wedge B$ .... (1)
- de (1), on infère B
- de (1), on infère A
- des deux conclusions précédentes, on infère $B \wedge A$

Démonstration formelle

$$\dfrac{\dfrac{\overbrace{A \wedge B}^{1}}{B}\,\wedge E_2 \qquad \dfrac{\overbrace{A \wedge B}^{1}}{A}\,\wedge E_1}{B \wedge A}\,\wedge I$$

Démarche

La déduction naturelle se prête à une démarche systématique pour la recherche d'une démonstration, en partant du bas (racine) :

- prendre comme *but* la conclusion désirée
- on a *fini* si le but est déjà parmi les *hypothèses*
- sinon, examiner la *forme* du but : essayer les règles qui aboutissent à une conclusion de cette forme, en privilégiant les règles d'introduction (décomposition du but)
- *recommencer* en prenant successivement comme nouveau but chacune des prémisses ; ces nouveaux buts sont des sous-formules du but précédent, donc plus simples
- lorsqu'un but est plus simple que les hypothèses disponibles, procéder par décomposition d'une hypothèse appropriée en utilisant une règle d'élimination

Rédaction a posteriori

La déduction naturelle permet de structurer la rédaction d'une démonstration, en partant du haut (feuilles) :

- il suffit de suivre les règles appliquées
- La rédaction textuelle a tendance à être peu précise
  $\longrightarrow$ connaître l'arbre de preuve aide à l'améliorer.

Commutativité de $\wedge$, démarche systématique

Raisonnement textuel pour la recherche

- on se donne l'hypothèse $A \wedge B$
- on se donne comme but $B \wedge A$
- décomposition de $B \wedge A$
- éliminer $A \wedge B$ pour obtenir B
- éliminer $A \wedge B$ pour obtenir A

Démonstration formelle en construction

$$\dfrac{\dfrac{A \wedge B}{B}\,\wedge E_2 \qquad \dfrac{A \wedge B}{A}\,\wedge E_1}{B \wedge A}\,\wedge I$$

Implication

Élimination : comment utiliser $A \Rightarrow B$?

- si on a $A \Rightarrow B$
- et si on a A
- on infère B

$$\boxed{\dfrac{A \Rightarrow B \qquad A}{B} \Rightarrow\mathrm{E}}$$

Introduction : comment inférer (conclure) $A \Rightarrow B$?

En démontrant B à partir de A

- supposons A
- on démontre B
- on infère $A \Rightarrow B$

$$\dfrac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A \Rightarrow B} \Rightarrow\mathrm{I}$$

A n'est plus une hypothèse de l'arbre de preuve pour $A \Rightarrow B$.

Exemple : transitivité de $\Rightarrow$

Il faut démontrer $A \Rightarrow C$ à partir de $A \Rightarrow B$ et de $B \Rightarrow C$

- supposons $A \Rightarrow B$ ....(1)
- supposons $B \Rightarrow C$ ....(2)
- *(pour démontrer* $A \Rightarrow C$*, on va démontrer* C *à partir de l'hypothèse supplémentaire* A*)*
- supposons A ....(3)
  - de (3), en utilisant l'hypothèse (1), on infère B
  - puis en utilisant l'hypothèse (2), on infère C
- ayant déduit C à partir de A, on infère $A \Rightarrow C$

$$\dfrac{\dfrac{\overbrace{B \Rightarrow C}^{2} \qquad \dfrac{\overbrace{A \Rightarrow B}^{1} \qquad \overbrace{A}^{3}}{B}\Rightarrow\mathrm{E}}{C}\Rightarrow\mathrm{E}}{A \Rightarrow C}\Rightarrow\mathrm{I}$$

Statut des feuilles

Dans nos premiers exemples, toutes les feuilles sont des hypothèses servant à démontrer la conclusion

$$\frac{rv \Rightarrow rg \qquad rg \Rightarrow rd}{rv \Rightarrow rd}\,\mathrm{TRI} \qquad\qquad \frac{\dfrac{A \wedge B}{B}\wedge E_2 \qquad \dfrac{A \wedge B}{A}\wedge E_1}{B \wedge A}\wedge I$$

Dans l'exemple précédent : encore vrai à l'étape aboutissant à C mais faux à l'étape finale où l'on conclut $A \Rightarrow C$ à partir des seules hypothèses $A \Rightarrow B$ et $B \Rightarrow C$: l'hypothèse A est « *levée* » (i.e. enlevée) au dernier stade.

Gestion des hypothèses

À un stade donné, certaines hypothèses sont *disponibles*, les autres sont dites *levées* (ou *enlevées*).
On appelle *environnement* l'ensemble des hypothèses disponibles.

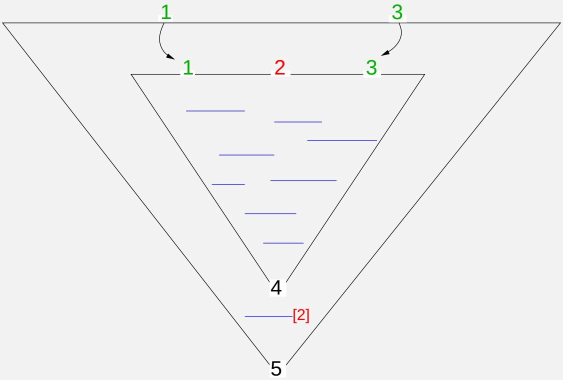
Dans la construction d'un arbre de preuve, le stade où une hypothèse est levée doit être reflété :

- numérotation des hypothèses, convention disponible / [levée]
- report du numéro sur l'inférence qui la lève

$$\dfrac{\dfrac{\overbrace{B \Rightarrow C}^{2} \qquad \dfrac{\overbrace{A \Rightarrow B}^{1} \qquad \overbrace{A}^{[3]}}{B}\,{\Rightarrow}\mathrm{E}}{C}\,{\Rightarrow}\mathrm{E}}{A \Rightarrow C}\,{\Rightarrow}\mathrm{I}[3]$$

Un arbre de preuve formalise le raisonnement

- aboutissant à la *conclusion* (formule placée à sa racine),
- sous les *hypothèses disponibles* (feuilles « encore actives »).



Formulation définitive de $\Rightarrow \mathrm{I}$

Ayant déduit B à partir de A

$$\begin{array}{c} \overbrace{A}^{n} \\ \vdots \\ B \end{array}$$

on infère $A \Rightarrow B$

$$\boxed{\dfrac{\begin{array}{c} \overbrace{A}^{[n]} \\ \vdots \\ B \end{array}}{A \Rightarrow B} \Rightarrow \mathrm{I}[n]}$$

Exemple (TRI) :

$$\dfrac{\dfrac{\overbrace{B \Rightarrow C}^{2} \qquad \dfrac{\overbrace{A \Rightarrow B}^{1} \qquad \overbrace{A}^{[3]}}{B} \Rightarrow \mathrm{E}}{C} \Rightarrow \mathrm{E}}{A \Rightarrow C} \Rightarrow \mathrm{I}[3]$$

Utilisation multiple d'hypothèses

Une même formule peut éventuellement être placée sur différentes feuilles, tout en étant levée dans une seule inférence

$$\dfrac{\dfrac{\dfrac{\overbrace{A \wedge B}^{[1]}}{B}\,\wedge E_2 \qquad \dfrac{\overbrace{A \wedge B}^{[1]}}{A}\,\wedge E_1}{B \wedge A}\,\wedge I}{(A \wedge B) \Rightarrow (B \wedge A)}\,\Rightarrow I[1]$$

En général, on peut en avoir un nombre quelconque d'occurrences, y compris 0

Notion de théorème

Définition : *un théorème est un énoncé pouvant être démontré dans l'environnement vide ; autrement dit, c'est la conclusion d'un arbre de preuve sans hypothèse (c-à-d. où toutes les feuilles correspondent à des hypothèses levées).*

Exemple : $(A \wedge B) \Rightarrow (B \wedge A)$ est un théorème (mais pas $B \wedge A$)

$$\dfrac{\dfrac{\dfrac{\overbrace{A \wedge B}^{[1]}}{B}\,\wedge\mathrm{E}_2 \qquad \dfrac{\overbrace{A \wedge B}^{[1]}}{A}\,\wedge\mathrm{E}_1}{B \wedge A}\,\wedge\mathrm{I}}{(A \wedge B) \Rightarrow (B \wedge A)}\,\Rightarrow\mathrm{I}[1]$$

Quelques théorèmes élémentaires

$A \Rightarrow A$

$$\dfrac{\overbrace{A}^{[1]}}{A \Rightarrow A}\Rightarrow\mathrm{I}[1] \qquad \overbrace{A}^{1} = \text{arbre de prv d'hypothèse } A \text{ et de conclusion } A$$

$A \Rightarrow B \Rightarrow A$

$$\overbrace{B}^{[1]} \qquad \dfrac{\dfrac{\overbrace{A}^{[2]}}{B \Rightarrow A}\Rightarrow\mathrm{I}[1]}{A \Rightarrow (B \Rightarrow A)}\Rightarrow\mathrm{I}[2]$$

La disjonction

Règles d'introduction (conclusion))

2 possibilités :

$$\frac{A}{A \vee B}\vee I_1 \qquad \frac{B}{A \vee B}\vee I_2$$

Règle d'élimination (utilisation)

Raisonnement par cas sur les 2 façons canoniques d'inférer $A \vee B$

- on a $A \vee B$
  - supposant A ....(n)
    on démontre C
  - supposant B ...(m)
    on démontre C
- on infère alors C
  en levant (n) et (m)

$$\frac{A \vee B \qquad \begin{matrix}\overbrace{A}^{[n]}\\ \vdots \\ C\end{matrix} \qquad \begin{matrix}\overbrace{B}^{[m]}\\ \vdots \\ C\end{matrix}}{C}\vee E[n,m]$$

Exemple : route (2)

Si la route est verglassée, elle est glissante ; si elle est enneigée elle est glissante ; elle est donc glissante dans les deux cas, et donc dangereuse ; il s'ensuit qu'une route verglassée ou enneigée est dangereuse

$$\dfrac{\dfrac{\overbrace{\mathrm{rg} \Rightarrow \mathrm{rd}}^{3} \qquad \dfrac{\overbrace{\mathrm{rv} \vee \mathrm{re}}^{[4]} \qquad \dfrac{\overbrace{\mathrm{rv} \Rightarrow \mathrm{rg}}^{1} \quad \overbrace{\mathrm{rv}}^{[5]}}{\mathrm{rg}}\Rightarrow\mathrm{E} \qquad \dfrac{\overbrace{\mathrm{re} \Rightarrow \mathrm{rg}}^{2} \quad \overbrace{\mathrm{re}}^{[6]}}{\mathrm{rg}}\Rightarrow\mathrm{E}}{\mathrm{rg}}\vee\mathrm{E}[5,6]}{\mathrm{rd}}\Rightarrow\mathrm{E}}{(\mathrm{rv} \vee \mathrm{re}) \Rightarrow \mathrm{rd}}\Rightarrow\mathrm{I}[4]$$

Exemple : route (3)

Si la route est verglassée, elle est glissante, donc dangereuse ;
si elle est enneigée elle est glissante, donc dangereuse ;
elle est donc dangereuse dans les deux cas, ce qui signifie qu'une route verglassée ou enneigée est dangereuse.

$$\dfrac{\dfrac{\overbrace{\mathrm{rv} \vee \mathrm{re}}^{[4]} \quad \dfrac{\overbrace{\mathrm{rg} \Rightarrow \mathrm{rd}}^{3} \quad \dfrac{\overbrace{\mathrm{rv} \Rightarrow \mathrm{rg}}^{1} \quad \overbrace{\mathrm{rv}}^{[5]}}{\mathrm{rg}} \Rightarrow\mathrm{E}}{\mathrm{rd}} \Rightarrow\mathrm{E} \quad \dfrac{\overbrace{\mathrm{rg} \Rightarrow \mathrm{rd}}^{3} \quad \dfrac{\overbrace{\mathrm{re} \Rightarrow \mathrm{rg}}^{2} \quad \overbrace{\mathrm{re}}^{[6]}}{\mathrm{rg}} \Rightarrow\mathrm{E}}{\mathrm{rd}} \Rightarrow\mathrm{E}}{\mathrm{rd}} \vee\mathrm{E}[5,6]}{(\mathrm{rv} \vee \mathrm{re}) \Rightarrow \mathrm{rd}} \Rightarrow\mathrm{I}[4]$$

Exemple : route (4)

Si la route est verglassée et enneigée, elle est verglassée, donc glissante, donc dangereuse.

$$\dfrac{\dfrac{\overbrace{\mathsf{rg} \Rightarrow \mathsf{rd}}^{3} \qquad \dfrac{\overbrace{\mathsf{rv} \Rightarrow \mathsf{rg}}^{1} \qquad \dfrac{\overbrace{\mathsf{rv} \land \mathsf{re}}^{[4]}}{\mathsf{rv}}\,\land\mathrm{E}_1}{\mathsf{rg}}\,\Rightarrow\mathrm{E}}{\mathsf{rd}}\,\Rightarrow\mathrm{E}}{(\mathsf{rv} \land \mathsf{re}) \Rightarrow \mathsf{rd}}\,\Rightarrow\mathrm{I}[4]$$

Commutativité de $\vee$: $(A \vee B) \Rightarrow (B \vee A)$

On démontre $B \vee A$ sous l'hypothèse $A \vee B$.

Pour démontrer $B \vee A$
essayons une
règle d'introduction

$$\overbrace{A \vee B}^{[1]} \qquad \dfrac{\dfrac{\dfrac{?}{A}}{B \vee A}\,\vee\mathrm{I}_2}{(A \vee B) \Rightarrow (B \vee A)}\Rightarrow\mathrm{I}[1]$$

Échec

Il faut commencer
par éliminer
l'hypothèse $A \vee B$

$$\dfrac{\dfrac{\overbrace{A \vee B}^{[1]} \qquad \dfrac{\overbrace{A}^{[2]}}{B \vee A}\,\vee\mathrm{I}_2 \qquad \dfrac{\overbrace{B}^{[3]}}{B \vee A}\,\vee\mathrm{I}_1}{B \vee A}\,\vee\mathrm{E}[2,3]}{(A \vee B) \Rightarrow (B \vee A)}\Rightarrow\mathrm{I}[1]$$

Commutativité de $\vee$ (suite)

On démontre $B \vee A$ sous l'hypothèse $A \vee B$.
Supposons $A \vee B$ ....(1)
On analyse les 2 cas possibles

- supposons A ....(2)
  on a alors $B \vee A$
- supposons B ....(3)
  on a alors $B \vee A$

Dans chaque cas on a $B \vee A$, ce qui nous a permis de déduire $B \vee A$ de la seule hypothèse $A \vee B$. Il en résulte que $A \vee B$ implique $B \vee A$.

$$\dfrac{\overbrace{A \vee B}^{1} \qquad \dfrac{\overbrace{A}^{[2]}}{B \vee A}\,\vee\mathrm{I}_2 \qquad \dfrac{\overbrace{B}^{[3]}}{B \vee A}\,\vee\mathrm{I}_1}{B \vee A}\,\vee\mathrm{E}[2,3]$$

$$\dfrac{\dfrac{\overbrace{A \vee B}^{[1]} \qquad \dfrac{\overbrace{A}^{[2]}}{B \vee A}\,\vee\mathrm{I}_2 \qquad \dfrac{\overbrace{B}^{[3]}}{B \vee A}\,\vee\mathrm{I}_1}{B \vee A}\,\vee\mathrm{E}[2,3]}{(A \vee B) \Rightarrow (B \vee A)}\,\Rightarrow\mathrm{I}[1]$$

Énoncés paramétrés

Problème

Beaucoup d'énoncés tels que D35v : « la D35 est verglassée »

Objectif : en fabriquer à volonté

Moyen : prédicats et constantes

- En langage courant : *être verglassé* est un *prédicat* portant sur des *individus* (en l'occurrence des routes)
- Formellement :
  - *symboles d'individus* (= de *constantes*) c, d, D35... ;
  - *symboles de prédicats* P, Q, ... ;
  - étant donné un symbole de prédicat P,
    on obtient un énoncé pour chaque symbole de constante c :
    P(c)

Prédicats, relations

Exemple

- constantes : D35, D44, N7, N20, etc.
- prédicats : V (être verglassée), E (être enneigée), G (être glissante)
- D35v représenté par V(D35)

Généralisation

Symboles de prédicat (ou de *relation*) binaires, ternaires . . . n-aires

- va-de-à(N90, Bernin, Crolles) : la N90 va de Bernin à Crolles

Exemple : route (4)

Si la D35 est verglassée et enneigée, elle est verglassée, donc glissante, donc dangereuse.

- $V(D35)$ = la D35 est verglassée
- $E(D35)$ = la D35 est enneigée
- $G(D35)$ = la D35 est glissante
- $D(D35)$ = la D35 est dangereuse

$$\dfrac{\dfrac{\overbrace{G(D35) \Rightarrow D(D35)}^{3} \qquad \dfrac{\overbrace{V(D35) \Rightarrow G(D35)}^{1} \qquad \dfrac{\overbrace{V(D35) \wedge E(D35)}^{[4]}}{V(D35)}\wedge\mathrm{E}_1}{G(D35)}\Rightarrow\mathrm{E}}{D(D35)}\Rightarrow\mathrm{E}}{V(D35) \wedge E(D35) \Rightarrow D(D35)}\Rightarrow\mathrm{I}[4]$$

Variable

Le raisonnement précédent peut être reproduit à l'identique en remplaçant D35 par n'importe quelle autre constante.

Variable = symbole représentant une constante non figée

Notation : x, y, z, ...

$$\dfrac{\dfrac{\overbrace{G(x) \Rightarrow D(x)}^{3} \qquad \dfrac{\overbrace{V(x) \Rightarrow G(x)}^{1} \qquad \dfrac{\overbrace{V(x) \wedge E(x)}^{[4]}}{V(x)}\,\wedge E_1}{G(x)}\,\Rightarrow E}{D(x)}\,\Rightarrow E}{V(x) \wedge E(x) \Rightarrow D(x)}\,\Rightarrow I[4]$$

On pourra *substituer* une constante à une variable dans certaines circonstances

Énoncé, formule paramétrée

Énoncé

- G(D35) : la D35 est glissante
- G(N90) : la N90 est glissante

Formule paramétrée

- G(x) : la route x est glissante

Formule universelle

Définitions

L'énoncé	se lit indifféremment
$\forall x G(x)$	– *quel que soit* x, x est glissante – *pour tout* G(x), G(x) est glissant(e) – toutes les routes sont glissantes

$\forall$ est le *quantificateur universel*

Dans $\forall x G(x)$, la variable x est *quantifiée universellement*

Portée du quantificateur : le plus à droite possible

$\forall x\ G(x) \Rightarrow D(x)$	$\forall x\ [G(x) \Rightarrow D(x)]$
$(\forall x G(x)) \Rightarrow D(x)$	$[\forall x G(x)] \Rightarrow D(x)$
$\forall x G(x) \Rightarrow \forall x D(x)$	$\forall x [G(x) \Rightarrow [\forall x D(x)]]$

Élimination (utilisation) d'une formule universelle

De $\forall x\ G(x)$ on peut déduire $G(D35)$, $G(N90)$, $G(N7)$, ...
en substituant à x les constantes D35, N90, N7, ...

$$\frac{\forall x\ P(x)}{P(t)}\ \forall_E(\tfrac{x}{t})$$

t représente une constante ou une variable

$G(t)$ représente la formule $G(x)$ dans laquelle on a substitué t à toutes les occurrences libres de x

« libre » : voir plus loin

Anonymat

Le nom d'une variable quantifiée n'est pas significatif

- $\forall x G(x)$ = *toutes* les routes sont glissantes
- $\forall y G(y)$ = *toutes* les routes sont glissantes

$\rightarrow$ $\forall x G(x)$ et $\forall y G(y)$ ont même interprétation

- De $\forall x G(x)$ on peut déduire G(D35), G(N90), G(N7), ...
  en substituant à x les constantes D35, N90, N7, ...
- De $\forall y G(y)$ on peut déduire G(D35), G(N90), G(N7), ...
  en substituant à y les constantes D35, N90, N7, ...

$\rightarrow$ On déduit les mêmes énoncés de $\forall x G(x)$ que de $\forall y G(y)$

Introduction du quantificateur universel

Objectif :

démontrer que pour tout x, $P(x)$

Méthode :

- soit x quelconque
- on démontre $P(x)$
  attention : x doit rester quelconque, en particulier les hypothèses éventuellement faites sur x doivent être levées
- on infère $\forall x\ P(x)$

Situation fréquente

Pour tout x tel que $P(x)$, on a $Q(x)$

- soit x quelconque
  - supposons $P(x)$
  - on démontre $Q(x)$
- on infère $P(x) \Rightarrow Q(x)$
- on infère $\forall x\ [P(x) \Rightarrow Q(x)]$
  notation : $\forall x\ P(x) \Rightarrow Q(x)$

Gestion des variables

- $\forall x\ G(x)$ identique à $\forall y\ G(y)$:
  dans ces formules x et y sont des variables **liées**
- $G(x)$ non identique à $G(y)$
  par exemple on a $G(x) \Rightarrow D(x)$ mais pas $G(y) \Rightarrow D(x)$
  (x est dangereuse si x est glissante,
  pas nécessairement si y est glissante) ;
  dans ces formules x et y sont des variables **libres**
- mais $[\forall x\ G(x)] \Rightarrow D(x)$ reste identique à $[\forall y\ G(y)] \Rightarrow D(x)$:
  ces deux formules signifient
  « » ;
  ces deux formules *dépendent de* x
  ces deux formules *sont paramétrées par* x
  x est *libre* dans ces deux formules ;
  plus précisément son *occurrence* dans $D(x)$ est libre
  (son occurrence dans $\forall x\ G(x)$ est liée)

Variable fraîche

Il arrive que l'on doive démontrer $\forall x\ P(x)$ sous des hypothèses comportant déjà des occurrences libres de x.

$$\dfrac{\begin{array}{c}\overbrace{H_1(x)}^{h_1}\ldots\overbrace{H_n(y)}^{h_n}\\ \vdots \\ P(\,?\,)\end{array}}{\forall x\ P(x)}\ \forall_I$$

Pour évacuer ce problème potentiel, on effectue systématiquement un renommage de x en choisissant une variable x_0 dite *fraîche* (c-à-d. non encore utilisée) :

- « soit x_0 un individu sur lequel on n'a aucune hypothèse, démontrons $P(x_0)$. »

Introduction et élimination de $\forall$

$$\dfrac{\begin{array}{c}\overbrace{\mathrm{H}_1(\_)}^{h_1}\ldots\overbrace{\mathrm{H}_n(\_)}^{h_n}\\ \vdots \\ \mathrm{P}(x_0)\end{array}}{\forall x\ \mathrm{P}(x)}\ \forall_{\mathrm{I}}$$

$$\dfrac{\forall x\ \mathrm{P}(x)}{\mathrm{P}(t)}\ \forall_{\mathrm{E}}(\tfrac{x}{t})$$

Condition d'application de $\forall_{\mathrm{I}}$: x_0 ne doit être libre dans aucune des hypothèses disponibles $h_1 \ldots h_n$

Dans $\forall_{\mathrm{E}}$
t représente une constante ou une variable
(dans le cas général : un terme ; *vu plus tard*)
$\mathrm{P}(t)$ représente la formule $\mathrm{P}(x)$ dans laquelle on a substitué t à toutes les occurrences libres de x.

Retour sur la route (4) : généralisation

Une (= toute) route verglassée est glissante

Une (= toute) route glissante est dangereuse

Si une route quelconque est verglassée et enneigée,
elle est verglassée, donc glissante, donc dangereuse.

Soit r_0 une route quelconque.

- Supposons r_0 verglassée et enneigée

  On en déduit que r_0 est dangereuse

Donc : r_0 est verglassée et enneigée implique que r_0 est dangereuse.
Il en résulte que toute route verglassée et enneigée est dangereuse.

Exemple : route (4)

$$
\dfrac{
  \dfrac{
    \dfrac{\overbrace{\forall x \;\; G(x) \Rightarrow D(x)}^{3}}{G(r_0) \;\Rightarrow D(r_0)}\;\forall_{\mathrm{E}}\left(\tfrac{x}{r_0}\right)
    \qquad
    \dfrac{
      \dfrac{\overbrace{\forall x \;\; V(x) \Rightarrow G(x)}^{1}}{V(r_0) \;\Rightarrow G(r_0)}\;\forall_{\mathrm{E}}\left(\tfrac{x}{r_0}\right)
      \qquad
      \dfrac{\overbrace{V(r_0) \;\wedge\; E(r_0)}^{[4]}}{V(r_0)}
    }{G(r_0)}\;\Rightarrow\mathrm{E}
  }{
    \dfrac{D(r_0)}{V(r_0) \wedge E(r_0) \;\Rightarrow D(r_0)}\;\Rightarrow\mathrm{I}[4]
  }\;\Rightarrow\mathrm{E}
}{\forall r \;\; V(r) \wedge E(r) \;\Rightarrow D(r)}\;\forall_{\mathrm{I}}
$$

Formule existentielle

Définitions

L'énoncé	se lit indifféremment
$\exists x G(x)$	– *il existe* x, x est glissante – il existe une route glissante

$\exists$ est le *quantificateur existentiel*

Dans $\exists x G(x)$, la variable x est *quantifiée existentiellement*

Portée du quantificateur : le plus à droite possible

$\exists x\ G(x) \Rightarrow D(x)$	$\exists x\ [G(x) \Rightarrow D(x)]$
$(\exists x G(x)) \Rightarrow D(x)$	$[\exists x G(x)] \Rightarrow D(x)$
$\exists x G(x) \Rightarrow \exists x D(x)$	$\exists x[G(x) \Rightarrow [\exists x D(x)]]$

Introduction d'une formule existentielle

Exemple

Nous sommes le 1er février à minuit : la N90 est verglassée.
On en déduit que la N90 est glissante, et donc que (dans l'univers du 1er février à minuit), il existe une route glissante.

$$\dfrac{\begin{array}{c}\vdots\\ G(N90)\end{array}}{\exists x\ G(x)}$$

Pour démontrer $\exists x\ P(x)$

- proposer un individu t, appelé un *témoin*
- démontrer $P(t)$
- inférer $\exists x\ P(x)$

Anonymat

Le nom d'une variable quantifiée n'est pas significatif

- $\exists x G(x)$ = *une* route est glissante
- $\exists y G(y)$ = *une* route est glissante

→ $\exists x G(x)$ et $\exists y G(y)$ ont même interprétation

- De $G(D35)$, $G(N90)$, $G(N7)$, ... on peut conclure $\exists x G(x)$ en prenant comme témoin pour x D35, N90, N7, ...
- De $G(D35)$, $G(N90)$, $G(N7)$, ... on peut conclure $\exists y G(y)$ en prenant comme témoin pour y D35, N90, N7, ...

→ On peut conclure à $\exists x G(x)$
chaque fois que l'on peut conclure à $\exists y G(y)$ et vice-versa

Élimination (utilisation) d'une formule existentielle

Informellement : pour utiliser l'information contenue dans $\exists x\ P(x)$, on se donne un tel individu – on le nomme y par exemple – et on travaille avec.

Plus formellement : que sait-on lorsque l'on a démontré $\exists x\ P(x)$?

- qu'il existe un individu vérifiant le prédicat P
- mais on ne sait pas lequel

Un peu comme pour $A \vee B$:

- on sait que l'un (au moins) parmi A et B est vérifié,
- mais on ne sait pas lequel

De même on considère tous les cas aboutissant à $\exists x\ P(x)$

- on suppose $P(x_0)$ pour un x_0 arbitraire
- sous cette hypothèse on démontre C

On peut alors inférer C à partir de $\exists x\ P(x)$

Introduction et élimination de $\exists$

$$\frac{P(t)}{\exists x\ P(x)}\ \exists_{\mathrm{I}}$$

$$\frac{\exists x\ P(x) \qquad \begin{array}{c} \overbrace{P(x_0)}^{[h]} \\ \vdots \\ C \end{array}}{C}\ \exists_{\mathrm{E}}[h]$$

Conditions d'application de $\exists_{\mathrm{E}}$

- Dans la preuve de C à partir de $P(x_0)$, x_0 ne doit être libre dans aucune hypothèse disponible exceptée h.
- C ne doit pas dépendre de x_0 (c-à-d. ne doit pas comporter d'occurrence libre de x_0)

Exemple

S'il existe une route verglassée, alors il existe une route glissante.

- soit r_0 une route quelconque
- supposons que r_0 est verglassée
- comme toute route verglassée est glissante, r_0 est glissante
- donc il existe une route glissante

Donc, sous l'hypothèse qu'il existe une route verglassée, il existe une route glissante.

$$\dfrac{\overbrace{\exists r\ V(r)}^{5} \qquad \dfrac{\dfrac{\dfrac{\overbrace{\forall x\ V(x) \Rightarrow G(x)}^{1}}{V(r_0) \Rightarrow G(r_0)}\ \forall_E\left(\frac{x}{r_0}\right) \qquad \overbrace{V(r_0)}^{[6]}}{G(r_0)}\ \Rightarrow_E}{\exists r\ G(r)}\ \exists_I}{\exists r\ G(r)}\ \exists_E[6]$$

L'absurde

On se donne une proposition « fausse » appelée l'*absurde*, notée $\perp$

Introduction

On ne veut pas que l'absurde soit démontrable !

$$\boxed{\text{Pas de règle d'introduction de } \perp}$$

Élimination

De l'absurde on infère n'importe quoi

$$\boxed{\frac{\perp}{C}\ \perp\mathrm{E}}$$

Peut-on démontrer l'absurde ?

Tentatives

$$\dfrac{\dfrac{\vdots\,?}{A \wedge \bot}}{\bot}\,\wedge E_2 \qquad\qquad \dfrac{\dfrac{\vdots\,?}{A \Rightarrow \bot} \quad \dfrac{\vdots\,?}{A}}{\bot}\,\Rightarrow E$$

De telles tentatives peuvent aboutir dans un environnement comportant simultanémént, par exemple, des hypothèses comme B, $C \Rightarrow \bot$, $B \Rightarrow A \Rightarrow C$, $B \Rightarrow A$, ou tout simplement l'hypothèse $\bot$.

*Théorème de la théorie de la démonstration

L'absurde est indémontrable dans l'environnement vide

Exercices

Exercice 1

Démontrer $\bot$ sous les hypothèses B, $C \Rightarrow \bot$, $B \Rightarrow A \Rightarrow C$, $B \Rightarrow A$.

Exercice 2

Que faut-il ajouter à l'environnement décrivant les lois du gruyère pour aboutir à l'absurde ?

- $pg \Rightarrow pt$
- $pt \Rightarrow mg$

La réponse doit comporter des énoncés intuitivement valides et formés seulement à partir de pg, mg et $\bot$.

La négation

La négation de A (notation $\neg A$) est la proposition qui, en présence de A, conduit à l'absurde.

Définition

$$\boxed{\neg A \quad \stackrel{\text{déf}}{=\!=} \quad A \Rightarrow \bot}$$

Remarques

- la définition précédente indique que la négation de $\neg A$ est $\neg A \Rightarrow \bot$, c-à-d. $(A \Rightarrow \bot) \Rightarrow \bot$
- en présence d'une proposition de la forme $A \Rightarrow \bot$, A aussi conduit à l'absurde

La double négation

A-t-on l'équivalence entre A et $\neg\neg A$?

- $A \Rightarrow \neg\neg A$ (pas difficile)
- mais la réciproque $\neg\neg A \Rightarrow A$ ne peut se démontrer avec les règles précédentes (cf. théorème fondamental d'élimination des coupures)

D'où :

Règle supplémentaire : élimination de $\neg\neg$

$$\boxed{\dfrac{\neg\neg A}{A}\ \neg\neg\mathrm{E}}$$

Utilisation de définitions et arbres de preuve

$\neg A$ étant $A \Rightarrow \bot$ par définition,
(où A est une proposition quelconque) on peut remplacer à volonté $\neg A$ par $A \Rightarrow \bot$ et réciproquement

Convention

On utilise une barre de fraction en pointillé

$$\boxed{\dfrac{A \Rightarrow \bot}{\neg A}\ \neg\,\text{déf}} \qquad \boxed{\dfrac{\neg A}{A \Rightarrow \bot}\ \neg\,\text{déf}}$$

Exemples

Exemple 1

$$\dfrac{(A \wedge B) \Rightarrow \bot}{\neg (A \wedge B)}\ \neg\,\text{déf}$$

Exemple 2

$$\dfrac{A \wedge (B \Rightarrow \bot)}{A \wedge \neg B}\ \neg\,\text{déf}$$

Exemple 3

$$\dfrac{A \vee \neg\neg B}{A \vee (\neg B \Rightarrow \bot)}\ \neg\,\text{déf}$$

Raisonnement par l'absurde

La règle d'élimination de la double négation permet de démontrer une proposition A de manière indirecte, en *raisonnant par l'absurde :*

- supposer $\neg A$
- en déduire l'absurde $\perp$
- par $\Rightarrow_{\mathrm{I}}$, inférer $(\neg A) \Rightarrow \perp$, c-à-d. $\neg\neg A$
- par $\neg\neg\mathrm{E}$ inférer A

$$\cfrac{\cfrac{\cfrac{\begin{array}{c}\overbrace{\neg A}^{[1]}\\ \vdots \\ \perp\end{array}}{\neg A \Rightarrow \perp}\ {\Rightarrow}\mathrm{I}[1]}{\neg\neg A}\ \neg\,\text{déf}}{A}\ \neg\neg\mathrm{E}$$

Utilisation du raisonnement par l'absurde

Exemples d'utilisation indispensable de $\neg\neg\mathrm{E}$

- $\neg\neg A \Rightarrow A$ (évidemment !)
- $\neg(A \wedge B) \Rightarrow \neg A \vee \neg B$
- $\neg(\forall x\ P(x)) \Rightarrow \exists x\ \neg P(x)$

Tiers exclu et raisonnement par l'absurde

Autre forme usuelle de raisonnement :

- pour n'importe quelle proposition A,
  on a soit A soit sa négation $\neg$A.

Pas de troisième possibilité, d'où le nom de *principe du tiers exclu*.

$$\boxed{\dfrac{}{A \vee \neg A}\ \tfrac{1}{3}ex}$$

Le tiers exclu ne peut être démontré à partir des règles précédentes à moins d'utiliser $\neg\neg\mathrm{E}$ *(théorème fondamental de réduction)*.

Réciproquement, le tiers exclu permet d'éliminer les doubles négations.

Quelques arbres de preuve avec négation (1)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\neg A}^{[2]}}{A \Rightarrow \bot}\,\neg\,\text{déf} \qquad \overbrace{A}^{[1]}}{\bot}\,\Rightarrow\text{E}}{\neg A \Rightarrow \bot}\,\Rightarrow\text{I}[2]}{\neg\neg A}\,\neg\,\text{déf}}{A \Rightarrow \neg\neg A}\,\Rightarrow\text{I}[1]$$

$$\dfrac{\dfrac{\dfrac{}{A \vee \neg A}\,\tfrac{1}{3}ex \qquad \overbrace{A}^{[2]} \qquad \dfrac{\dfrac{\dfrac{\overbrace{\neg\neg A}^{[1]}}{\neg A \Rightarrow \bot}\,\neg\,\text{déf} \qquad \overbrace{\neg A}^{[3]}}{\bot}\,\Rightarrow\text{E}}{A}\,\bot\text{E}}{A}\,\vee\text{E}[2,3]}{\neg\neg A \Rightarrow A}\,\Rightarrow\text{I}[1]$$

Quelques arbres de preuve avec négation (2)

Dérivation du tiers exclu utilisant $\neg\neg\mathrm{E}$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{(A \lor \neg A) \Rightarrow \bot}^{[1]} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overbrace{(A \lor \neg A) \Rightarrow \bot}^{[1]} \qquad \dfrac{\overbrace{A}^{[2]}}{A \lor \neg A}\,\lor\mathrm{I}_1}{\bot}\,\Rightarrow\mathrm{E}}{A \Rightarrow \bot}\,\Rightarrow\mathrm{I}[2]}{\neg A}\,\neg\,\text{déf}}{A \lor \neg A}\,\lor\mathrm{I}_2}{\bot}\,\Rightarrow\mathrm{E}}{((A \lor \neg A) \Rightarrow \bot) \Rightarrow \bot}\,\Rightarrow\mathrm{I}[1]}{\neg\neg(A \lor \neg A)}\,\neg\,\text{déf}}{A \lor \neg A}\,\neg\neg\mathrm{E}
$$

Logique constructive (ou non)

L'axiome du tiers exclu ne dit pas lequel parmi A ou ¬A est vérifié
Dans une démonstration par l'absurde, ou utilisant le tiers exclu, de $\exists x\, P(x)$ on n'a pas le témoin de l'existence de x

- démonstrations plus faciles avec $\frac{1}{3}ex$ ou $\neg\neg\mathrm{E}$
- mais moins informatives

Définition

- la *logique classique* est le système de déduction naturelle comprenant toutes les règles précédentes, avec $\frac{1}{3}ex$ (ou $\neg\neg\mathrm{E}$)
- la *logique intuitionniste* est le système de déduction naturelle comprenant toutes les règles précédentes, sans $\frac{1}{3}ex$ (ni $\neg\neg\mathrm{E}$)

Conséquence : la logique intuitionniste n'accepte que des démonstrations *constructives*, contrairement à la logique classique.

L'équivalence

Définition : $\boxed{A \Leftrightarrow B \quad \stackrel{\text{déf}}{=\!=} \quad A \Rightarrow B \ \wedge \ B \Rightarrow A}$

On peut donc utiliser, dans un arbre de preuve :

$$\frac{A \Rightarrow B \ \wedge \ B \Rightarrow A}{A \Leftrightarrow B}\Leftrightarrow \text{déf} \qquad \frac{A \Leftrightarrow B}{A \Rightarrow B \ \wedge \ B \Rightarrow A}\Leftrightarrow \text{déf}$$

En général, on les utilise en combinaison avec $\wedge\mathrm{I}$, $\wedge\mathrm{E}_1$ et $\wedge\mathrm{E}_2$:

$$\dfrac{\dfrac{A \Rightarrow B \qquad B \Rightarrow A}{A \Rightarrow B \ \wedge \ B \Rightarrow A}\wedge\mathrm{I}}{A \Leftrightarrow B}\Leftrightarrow \text{déf} \qquad \dfrac{\dfrac{A \Leftrightarrow B}{A \Rightarrow B \ \wedge \ B \Rightarrow A}\Leftrightarrow \text{déf}}{A \Rightarrow B}\wedge\mathrm{E}_1$$

et similairement pour $B \Rightarrow A$ en utilisant $\wedge\mathrm{E}_2$.

En raccourci *(la double barre de fraction symbolise plusieurs étapes)* :

$$\frac{A \Rightarrow B \qquad B \Rightarrow A}{A \Leftrightarrow B}\wedge\mathrm{I} \qquad \frac{A \Leftrightarrow B}{A \Rightarrow B}\wedge\mathrm{E}_1 \qquad \frac{A \Leftrightarrow B}{B \Rightarrow A}\wedge\mathrm{E}_2$$

Raisonnement équationnel

Introduction : un individu t quelconque est égal à lui-même

$$\boxed{\dfrac{}{t = t}\ {=}\mathrm{I}}$$

où t représente une constante ou une variable quelconque
(plus généralement : un terme, vu plus tard)

Élimination : principe de substitution de Leibniz
Si $a = b$, toute propriété de a est transmise à b
(on peut remplacer à volonté a par b).

$$\boxed{\dfrac{a = b \qquad \mathsf{P}(a)}{\mathsf{P}(b)}\ {=}\mathrm{E}}$$

Propriétés de l'égalité

L'égalité est une relation réflexive

- $\forall x \;\; x = x$

L'égalité est une relation symétrique

- $\forall xy \;\; x = y \;\Rightarrow\; y = x$

L'égalité est une relation transitive

- $\forall xyz \;\; x = y \Rightarrow y = z \;\Rightarrow\; x = z$

Ces propriétés sont en fait des conséquences des principes d'introduction et d'élimination de l'égalité.

Exemple de raisonnement équationnel

Remarque

Si $a = b$, et si on a une propriété de a dans l'énoncé de laquelle a apparaît plusieurs fois, le principe de Leibniz permet d'inférer la propriété obtenue en remplaçant des occurrences de a par b, mais pas nécessairement toutes

Exemple

Sachant $5=2+3$, de $5 - 5 < 1$ on peut inférer $5 - (2+3) < 1$

Application : symétrie de l'égalité

Soient x et y arbitraires

- supposons $x = y$ ....(1)
- on sait que $x = x$ (par $=_{\mathrm{I}}$) ....(2)
- grâce à (1) on remplace dans (2) la première occurrence de x par y :
  $y = x$ ....(3)

En levant (1), on infère $x = y \Rightarrow y = x$ ....(4)
et comme il ne subsiste aucune hypothèse où x et y sont libres, on a
$\forall xy\ \ x = y\ \Rightarrow\ y = x$

Présentation de preuves équationnelles

$$
\mathcal{D}_i \left\{
\begin{array}{lll}
 & U & \\
= & & \{\text{indication justifiant } U = V\} \\
 & V & \\
= & & \{\text{indication justifiant } V = W\} \\
 & W & \\
\vdots & & \\
 & Y & \\
= & & \{\text{indication justifiant } Y = Z\} \\
 & Z &
\end{array}
\right.
$$

Utilisation

$$
\frac{}{U = Z}\,\mathcal{D}_i
$$

Preuve équationnelle sous hypothèses

$$
\mathcal{D}_i \begin{cases}
\quad U \\
= \quad \{\text{justification de } U = V \text{ sous les hypothèses } h_1 \ldots h_2\} \\
\quad V \\
\vdots \\
\quad Y \\
= \quad \{\text{justification de } Y = Z \text{ sous les hypothèses } h_3 \ldots h_4\} \\
\quad Z
\end{cases}
$$

Utilisation

$$
\frac{\overbrace{}^{h_1} \;\ldots\; \overbrace{}^{h_2} \;\ldots\; \overbrace{}^{h_3} \;\ldots\; \overbrace{}^{h_4}}{U = Z}\ \mathcal{D}_i
$$

Entiers et récurrence

Tous les individus considérés ici sont des entiers naturels

S est la fonction qui envoie tout entier n vers son *successeur* $n+1$

Définition des entiers naturels

- 0 est un entier naturel
- si n est un entier naturel, $\mathsf{S}(n)$ est un entier naturel
- tous les entiers sont engendrés par application des règles précédentes (en nombre fini)

Récurrence

$$\boxed{\dfrac{\mathsf{P}(0) \qquad \forall n \;\; \mathsf{P}(n) \Rightarrow \mathsf{P}(\mathsf{S}(n))}{\forall n \;\; \mathsf{P}(n)} \;\text{nat-rec}}$$

Arithmétique et récurrence

Plan du chapitre 3

Récurrence forte

Récurrence forte sur les entiers

Toutes les variables m, n … considérées sont des entiers naturels

Rappel : récurrence simple

$$\frac{\mathsf{P}(0) \qquad \forall n\ \mathsf{P}(n) \Rightarrow \mathsf{P}(\mathsf{S}(n))}{\forall n\, \mathsf{P}(n)}\ \text{nat-rec}$$

Récurrence forte (ou : induction complète)

$$\frac{\forall n\ [\forall m\ ,\ m < n\ \Rightarrow \mathsf{P}(m)]\ \Rightarrow \mathsf{P}(n)}{\forall n\, \mathsf{P}(n)}\ \text{nat-recG}$$

Il s'agit d'un principe plus fort = démontrer la prémisse est plus facile :

- par exemple pour déduire $\mathsf{P}(n)$ avec $n = 3$,
  on peut utiliser non seulement $\mathsf{P}(2)$, mais aussi $\mathsf{P}(1)$ et $\mathsf{P}(0)$
- le travail est le même pour $n = 0$: $m < 0$ est absurde

Théorème des plaquettes de chocolat

Énoncé

Prenons une plaquette de n carrés
et découpons la en suivant les rainures

En combien de coups a-t-on réduit la plaquette en carrés ?

Réponse

n - 1
Cela ne dépend pas des choix successifs de rainures !

Démonstration

Par récurrence forte

Raisonnement par cas sur les entiers

Raisonnement par cas

$$\boxed{\dfrac{\mathsf{P}(0) \qquad \forall n\ \mathsf{P}(\mathsf{S}(n))}{\forall n\, \mathsf{P}(n)}\ \text{nat-cas}}$$

Conséquence de la récurrence simple

$$\dfrac{\mathsf{P}(0) \qquad \forall n\ \mathsf{P}(n) \Rightarrow \mathsf{P}(\mathsf{S}(n))}{\forall n\, \mathsf{P}(n)}\ \text{nat-rec}$$

Mais s'admet indépendamment
(il n'est pas nécessaire de répéter son application)

Exemple : $\forall n,\ n = 0\ \vee\ \exists x,\ n = \mathsf{S}(x)$

- $0 = 0\ \vee\ \exists x,\ 0 = \mathsf{S}(x)$
- $\mathsf{S}(n) = 0\ \vee\ \exists x,\ \mathsf{S}(n) = \mathsf{S}(x)$

Récurrence forte $\Rightarrow$ récurrence simple

Soit P un prédicat vérifiant :

$P(0)$ .... (1)

$\forall n,\ P(n) \Rightarrow P(S(n))$ .... (2)

Posons $Q(n) \stackrel{\text{déf}}{\equiv} \forall m,\ m < n \Rightarrow P(m)$,

et montrons $\forall n\ Q(n) \Rightarrow P(n)$ .... (3)

Raisonnement par cas :

- $Q(0) \Rightarrow P(0)$ en utilisant (1) et en oubliant $Q(0)$
- soit n quelconque et supposons $Q(S(n))$ .... (4)
  par définition de Q et sachant que $n < S(n)$, on obtient $P(n)$;
  avec (2), on obtient $P(S(n))$;
  on a donc $\forall n\ , Q(S(n)) \Rightarrow P(S(n))$

En conséquence (3) est démontré, et par récurrence forte cela donne $\forall n\ P(n)$ QED

Récurrence simple $\Rightarrow$ récurrence forte

Soit P un prédicat vérifiant :
$\forall n\ [\forall m,\ m < n \Rightarrow \mathsf{P}(m)] \Rightarrow \mathsf{P}(n)$ . . . . (1)
On pose $\mathsf{Q}(n) \stackrel{\text{déf}}{=\!=} \forall m,\ m < n \Rightarrow \mathsf{P}(m)$; (1) se réécrit :
$\forall n\ \mathsf{Q}(n) \Rightarrow \mathsf{P}(n)$ . . . . (1')

Démontrons par récurrence simple : $\forall n\ \mathsf{Q}(n)$

- soit m un entier naturel tel que $m < 0$, cela est absurde, ce qui donne en particulier $\mathsf{P}(m)$; donc $\forall m,\ m < 0 \Rightarrow \mathsf{P}(m)$, c-à-d. $\mathsf{Q}(0)$
- soit n tel que $\mathsf{Q}(n)$ . . . . (2)
  c-à-d. $\forall x,\ x < n \Rightarrow \mathsf{P}(x)$ . . . . (2')
  soit m un entier naturel tel que $m < \mathsf{S}(n)$ . . . . (3)
  (3) entraîne $m < n \vee m = n$ . . . . (4)

  - si $m < n$, on a grâce à (2') : $\mathsf{P}(m)$
  - si $m = n$: (1') et (2) donnent $\mathsf{P}(n)$, donc $\mathsf{P}(m)$

  on a $\mathsf{P}(m)$ dans chaque cas de (4), donc (3) $\Rightarrow \mathsf{P}(m)$ c-à-d. $\mathsf{Q}(\mathsf{S}(n))$

On a donc par récurrence $\mathsf{Q}(n)$ pour tout n, et donc $\mathsf{P}(n)$ par (1')

Les structures mathématiques

Plan du chapitre 4

Plan du chapitre 4 (cont.)

Rôle de la théorie des ensembles

Pour les mathématiques : outil universel, fondement des différentes branches

- Georg Cantor (1845-1918) à l'origine des travaux sur la théorie des ensembles
- Zermelo (1871-1953), Fraenkel (1891-1965) et von Neumann (1903-1957) développent une théorie *axiomatique* des ensembles. Principalement en réaction au paradoxe de Russell :

$$\mathrm{Ru} = \{X \mid X \notin X\}$$

Pour l'informatique : fournit un vocabulaire précis et des notions utilisées constamment pour décrire des données, des opérations, etc.

Théorie naïve des ensembles

Un *ensemble* est une collection d'objets

- *distinguables* les unes des autres
- telle qu'il existe un critère pour savoir si un objet *appartient* à cette collection ou pas

Notation

$x \in E$ se lit : x appartient à l'ensemble E, ou x est un *élément* de E.

Description extensionnelle

Un ensemble peut être défini de manière *extensionnelle*, par une *enumération* de ses *éléments* entre accolades.

Exemples

- $\{0\}$
- $\{3, 1, 17\}$

Remarques

- Il existe un unique ensemble à 0 élément, nommé *l'ensemble vide* et noté $\emptyset$
- L'ordre dans lequel on écrit les éléments d'un ensemble n'est pas significatif, pas plus que la répétition d'un élément
  Exemple : $\{1, 2, 4\} = \{2, 4, 1\} = \{1, 2, 1, 4, 4, 4\}$
- Les ensembles peuvent avoir des contenus hétérogènes
  Exemple : $\{1, 3, 'A', \mathbb{N}, 1,542\}$.
- Les ensembles peuvent être des éléments d'autres ensembles
  Exemple : $\{1, \{1, 2, 4\}, \emptyset, \{\{1\}, 7\}, 3, 'A', \mathbb{N}, 1,542\}$.

Et si l'ensemble est infini ?

On peut *évoquer* le résultat attendu, par exemple :

- $\{0, 2, 4, \ldots, 2k, \ldots\}$

Mais ce n'est pas rigoureux !

Description intensionnelle

Un ensemble peut aussi être défini de manière *intensionnelle*, par une *propriété* vérifiée par tous les éléments de l'ensemble (et seulement par ceux là) : $\{x \mid P(x)\}$, où P est un prédicat

Exemple

$\{n \mid n \in \mathbb{N} \ \wedge \ \text{est\_pair}(n)\}$

Notation

On écrit aussi $\{x \in A \mid R(x)\}$ au lieu de $\{x \mid x \in A \ \wedge \ R(x)\}$

Exemple

$\{n \in \mathbb{N} \mid n \geq 3\}$ est equivalent à $\{n \mid n \in \mathbb{N} \wedge n \geq 3\}$.

Paradoxe de Russell

Remarque préliminaire

Étant donné une proposition quelconque A, on a $\neg(A \Leftrightarrow \neg A)$

- on démontre $(A \Leftrightarrow (A \Rightarrow B)) \Rightarrow B$ et on prend $\perp$ pour B
- ou on procède par cas sur le tiers exclu appliqué à A

Conséquence

Une propriété ne suffit pas à définir un ensemble !

Considérons $\mathrm{Ru} = \{X \mid X \notin X\}$
L'ensemble Ru existe-t-il vraiment ?

- par définition de Ru on a : $\forall X\, , X \in \mathrm{Ru} \Leftrightarrow \neg(X \in X)$;
- donc, en particulier : $\mathrm{Ru} \in \mathrm{Ru} \Leftrightarrow \neg(\mathrm{Ru} \in \mathrm{Ru})$;
- on applique la remarque ci-dessus en prenant pour A : $\mathrm{Ru} \in \mathrm{Ru}$

Parade

Une définition intensionnelle n'est possible qu'à l'intérieur d'un ensemble déjà construit.

Axiome de séparation

Si E est un ensemble déjà construit et P est un prédicat, alors $\{x \in E \mid P(x)\}$ est un nouvel ensemble.

Conséquence

L'ensemble de tous les ensembles n'existe pas.

- Si un tel ensemble T pouvait être formé, on retrouverait le paradoxe de Russell en considérant $\{x \in \mathrm{T} \mid x \notin x\}$.

Théorie axiomatique des ensembles

La véritable théorie des ensembles, sur laquelle reposent les mathématiques actuelles, énonce un certain nombre d'*axiomes* indiquant les constructions autorisées pour former des ensembles de plus en plus complexes.

Exemple : l'axiome de séparation.

Pour comprendre ces axiomes, il est nécessaire de maîtriser les notions de la théorie « naïve » des ensembles.

Pour simplifier, on utilise donc ici la version « naïve » en se munissant de précautions.

Théorie naïve prudente des ensembles

Nous supposons un univers U préalablement construit et cohérent.

La notation $\{x \mid P(x)\}$ représente désormais, implicitement :

$$\{x \in \mathrm{U} \mid P(x)\}$$

Autrement dit : on se limite à considérer des objets (éléments, ensembles) qui sont tous des éléments de U.
En pratique U contient les entiers, les réels, etc.

Remarque

En particulier, si on écrit $\{x \in E \mid P(x)\}$, on a implicitement :

- E appartient à U : $E \in \mathrm{U}$
- tout élément de E appartient à U : $\forall x\ x \in E \Rightarrow x \in \mathrm{U}$

Égalité

Deux ensembles E et F sont *égaux*, noté $E{=}F$ si tout élément de E appartient à F et tout élément de F appartient à E :

$$E = F \Leftrightarrow \forall x \; x \in E \Leftrightarrow x \in F$$

Exemple

$$\{0, 2, 4\} = \{n \mid n \in \mathbb{N} \wedge n \leq 5 \wedge \text{est\_pair}(n)\}$$

Inclusion

Un ensemble E est *inclus* dans un ensemble F, noté $E \subseteq F$ si tout élément de E appartient à F

$$E \subseteq F \overset{\text{déf}}{\equiv} \forall x \; x \in E \Rightarrow x \in F$$

Exemple :

$$\{0, 2, 4\} \subseteq \{n \mid n \in \mathbb{N} \land n \leq 5\}$$

Un ensemble E est *strictement inclus* dans un ensemble F, noté $E \subset F$ si E est inclus dans F et s'il existe un élément de F qui n'appartient pas à E

$$E \subset F \overset{\text{déf}}{\equiv} E \subseteq F \land \exists x \; x \in F \land x \notin E$$

Exemple :

$$\{0, 2, 4\} \subset \{n \mid n \in \mathbb{N} \land n \leq 5\}$$

Union et intersection

L'*union* (ou *réunion*) de A et de B, notée $A \cup B$, est l'ensemble des éléments appartenant à A ou à B :

$$A \cup B \overset{\text{déf}}{=\!=} \{x \mid x \in A \vee x \in B\}$$

Exemple : $\{0, 2\} \cup \{2, 4\} = \{0, 2, 4\}$

L'*intersection* de A et de B, notée $A \cap B$, est l'ensemble des éléments appartenant à la fois à A et à B :

$$A \cap B \overset{\text{déf}}{=\!=} \{x \mid x \in A \wedge x \in B\}$$

Exemple : $\{0, 2\} \cap \{4\} = \varnothing$

Différence et complémentaire

La *différence A moins B*, notée $A \setminus B$, est l'ensemble des éléments appartenant à A mais pas à B :

$$A \setminus B \overset{\text{déf}}{=\!=} \{x \mid x \in A \wedge x \notin B\}$$

Exemple : $\{n \mid n \in \mathbb{N} \wedge n \leq 5 \wedge \mathsf{est\_pair}(n)\} \setminus \{4\} = \{0, 2\}$

Le *complémentaire de A*, notée A^c (ou $\overline{A}$), est l'ensemble des éléments de U qui n'appartiennent pas à A :

$$A^c \overset{\text{déf}}{=\!=} \mathrm{U} \setminus A$$

Exemple : $\mathrm{U}^c = \varnothing$

Définitions ensemblistes

Langage : on se donne le prédicat binaire $\in$, notation infixe $x \in A$

Axiome d'extensionalité : $A = B \Leftrightarrow (\forall x,\ x \in A \Leftrightarrow x \in B)$

Inclusion : $A \subseteq B \ \stackrel{\text{déf}}{=\!=} \ (\forall x,\ x \in A \Rightarrow x \in B)$

Intersection : $x \in A \cap B \ \stackrel{\text{déf}}{=\!=} \ x \in A \wedge x \in B$

Union : $x \in A \cup B \ \stackrel{\text{déf}}{=\!=} \ x \in A \vee x \in B$

Définition par extension :
$x \in \{a\} \ \stackrel{\text{déf}}{=\!=} \ x = a$ (singleton)
$x \in \{a_1, \ldots a_n\} \ \stackrel{\text{déf}}{=\!=} \ x = a_1 \vee \ldots \vee x = a_n$

Ensemble vide : $x \in \varnothing \ \stackrel{\text{déf}}{=\!=} \ \bot$

Complément : $x \in A \backslash B \ \stackrel{\text{déf}}{=\!=} \ x \in A \wedge \neg(x \in B)$

Ensemble des parties : $A \in \mathcal{P}(B) \ \stackrel{\text{déf}}{=\!=} \ A \subseteq B$

Inclusion (introduction)

Version longue

$$
\cfrac{\cfrac{\cfrac{\begin{array}{c}\overbrace{x_0 \in A}^{[n]}\\ \vdots \\ x_0 \in B\end{array}}{x_0 \in A \Rightarrow x_0 \in B}\ \Rightarrow\mathrm{I}[n]}{\forall x,\ x \in A \Rightarrow x \in B}\ \forall_{\mathrm{I}}}{A \subseteq B}\ \subseteq \text{déf}
$$

Version abrégée

$$
\cfrac{\begin{array}{c}\overbrace{x_0 \in A}^{[n]}\\ \vdots \\ x_0 \in B\end{array}}{A \subseteq B}\ \subseteq\mathrm{I}\,[n]
$$

Inclusion (élimination)

$$
\dfrac{\dfrac{\dfrac{A \subseteq B}{\forall x,\ x \in A \Rightarrow x \in B}\ \subseteq\text{déf}}{x_0 \in A \Rightarrow x_0 \in B}\ \forall_{\mathrm{E}}(\,) \qquad x_0 \in A}{x_0 \in B}\ \Rightarrow\mathrm{E}
$$

Abrégé

$$
\dfrac{A \subseteq B \qquad x_0 \in A}{x_0 \in B}\ \subseteq\mathrm{E}
$$

Égalité extensionnelle

$$
\dfrac{\dfrac{\dfrac{\begin{array}{c}\overbrace{x_0 \in A}^{[n]} \\ \vdots \\ x_0 \in B\end{array}}{x_0 \in A \Rightarrow x_0 \in B}\,{\Rightarrow}\mathrm{I}[n] \qquad \dfrac{\begin{array}{c}\overbrace{x_0 \in B}^{[m]} \\ \vdots \\ x_0 \in A\end{array}}{x_0 \in B \Rightarrow x_0 \in A}\,{\Rightarrow}\mathrm{I}[m]}{x_0 \in A \Leftrightarrow x_0 \in B}\,{\wedge}\mathrm{I}}{\dfrac{\forall x\ x \in A \Leftrightarrow x \in B}{A = B}\,\mathrm{ext}}\,\forall_{\mathrm{I}}
$$

Abrégé

$$
\begin{array}{c}
\begin{array}{c}\overbrace{x_0 \in A}^{[n]} \\ \vdots \\ x_0 \in B\end{array} \qquad \begin{array}{c}\overbrace{x_0 \in B}^{[m]} \\ \vdots \\ x_0 \in A\end{array} \\ \hline\hline A = B
\end{array}\ \mathrm{ext}[n,m]
$$

Intersection

Version longue

$$\dfrac{\dfrac{x \in A \qquad x \in B}{x \in A \ \wedge\ x \in B}\ \wedge\mathrm{I}}{x \in A \cap B}\ \cap\,\text{déf}$$

$$\dfrac{\dfrac{x \in A \cap B}{x \in A \ \wedge\ x \in B}\ \cap\,\text{déf}}{x \in A}\ \wedge\mathrm{E}_1$$

$$\dfrac{\dfrac{x \in A \cap B}{x \in A \ \wedge\ x \in B}\ \cap\,\text{déf}}{x \in B}\ \wedge\mathrm{E}_2$$

Version abrégée

$$\dfrac{x \in A \qquad x \in B}{x \in A \cap B}\ \wedge\mathrm{I}\cap$$

$$\dfrac{x \in A \cap B}{x \in A}\ \cap\wedge\mathrm{E}_1$$

$$\dfrac{x \in A \cap B}{x \in B}\ \cap\wedge\mathrm{E}_2$$

Union (introduction)

Version longue

$$\cfrac{\cfrac{x \in A}{x \in A \ \vee\ x \in B}\ \vee\mathrm{I}_1}{x \in A \cup B}\ \cup\,\text{déf}$$

$$\cfrac{\cfrac{x \in B}{x \in A \ \vee\ x \in B}\ \vee\mathrm{I}_2}{x \in A \cup B}\ \cup\,\text{déf}$$

Version abrégée

$$\cfrac{x \in A}{x \in A \cup B}\ \vee\mathrm{I}_1\cup$$

$$\cfrac{x \in B}{x \in A \cup B}\ \vee\mathrm{I}_2\cup$$

Union (élimination)

$$\dfrac{\dfrac{x \in A \cup B}{x \in A \;\vee\; x \in B}\,\cup\text{déf} \qquad \begin{array}{c}\overbrace{x \in A}^{[n]}\\ \vdots \\ P\end{array} \qquad \begin{array}{c}\overbrace{x \in B}^{[m]}\\ \vdots \\ P\end{array}}{P}\,\vee\mathrm{E}[n,m]$$

Version abrégée

$$\dfrac{x \in A \cup B \qquad \begin{array}{c}\overbrace{x \in A}^{[n]}\\ \vdots \\ P\end{array} \qquad \begin{array}{c}\overbrace{x \in B}^{[m]}\\ \vdots \\ P\end{array}}{P}\,\cup\vee\mathrm{E}[n,m]$$

Union et intersection

1. Monotonie de $\cup$: si $A \subseteq B$ et $C \subseteq D$ alors $A \cup C \subseteq B \cup D$.
2. Monotonie de $\cap$: si $A \subseteq B$ et $C \subseteq D$ alors $A \cap C \subseteq B \cap D$.
3. Associativité de $\cup$: $(A \cup B) \cup C = A \cup (B \cup C)$.
4. Associativité de $\cap$: $(A \cap B) \cap C = A \cap (B \cap C)$.
5. Commutativité de $\cup$: $A \cup B = B \cup A$.
6. Commutativité de $\cap$: $A \cap B = B \cap A$.
7. Distributivité de $\cup$ par rapport à $\cap$:
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
8. Distributivité de $\cap$ par rapport à $\cup$:
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Démonstration de la monotonie de $\cup$

Soient A, B, C et D des ensembles tels que :

$$A \subseteq B \wedge C \subseteq D.$$

On montre $A \cup C \subseteq B \cup D$. C'est-à-dire :

$$\forall x \; x \in A \cup C \;\Rightarrow\; x \in B \cup D.$$

Soit x tel que $x \in A \cup C$. On distingue deux cas :

1. $x \in A$. De l'hypothèse $A \subseteq B$, nous déduisons $x \in B$. Donc $x \in B \cup D$.
2. $x \in C$. De l'hypothèse $C \subseteq D$, nous déduisons $x \in D$. Donc $x \in B \cup D$.

q.e.d.

Différence et complémentaire

1. Si $A \cap B = \varnothing$ alors $A \setminus B = A$. En particulier, $A \setminus \varnothing = A$.
2. Si $A \subseteq B$ alors $A \setminus B = \varnothing$. En particulier, $A \setminus A = \varnothing$.
3. Monotonie de $\setminus$ dans le premier argument :
   si $A \subseteq B$ alors $A \setminus C \subseteq B \setminus C$.
4. Anti-monotonie de $\setminus$ dans le deuxième argument :
   si $A \subseteq B$ alors $C \setminus B \subseteq C \setminus A$.
5. Lois de Morgan
   - $\overline{A \cup B} = \overline{A} \cap \overline{B}$
   - $\overline{A \cap B} = \overline{A} \cup \overline{B}$
6. Anti-monotonie du complémentaire : si $A \subseteq B$ alors $\overline{B} \subseteq \overline{A}$

Eléments neutres et absorbants

1. $\emptyset$ est un élément neutre de $\cup$: $\forall A\ A \cup \emptyset = \emptyset \cup A = A$.
2. $\emptyset$ est l'unique élément neutre de $\cup$:

$$\forall X\ (\forall A\ X \cup A = A \cup X = A) \Rightarrow\ X = \emptyset.$$

3. $\emptyset$ est un élément absorbant de $\cap$: $\forall A\ A \cap \emptyset = \emptyset \cap A = \emptyset$.
4. $\emptyset$ est l'unique élément absorbant de $\cap$:

$$\forall X\ (\forall A\ X \cap A = A \cap X = X) \Rightarrow\ X = \emptyset.$$

Unicité de l'élément neutre de $\cup$

On veut montrer que l'ensemble vide est l'unique élément neutre de $\cup$. C'est-à-dire :

$$\forall X\ (\forall A\ X \cup A = A \cup X = A) \Rightarrow\ X = \emptyset.$$

Soit X un ensemble tel que $\forall A\ X \cup A = A \cup X = A$. $\qquad (\dagger)$

On doit montrer $X = \emptyset$.

- De $(\dagger)$, nous obtenons $X \cup \emptyset = \emptyset$.
- Mais comme $\emptyset$ est un élément neutre de $\cup$, nous avons aussi $X \cup \emptyset = X$.
- Donc, $X \cup \emptyset = \emptyset = X$. q.e.d.

Parties d'un ensembles

On appelle *partie* de A tout ensemble X inclus dans A : $X \subseteq A$.
L'ensemble des parties de A est défini par

$$\mathcal{P}(A) \stackrel{\text{déf}}{=} \{X \mid X \subseteq A\}.$$

Exemples

1. $\mathcal{P}(\{0\}) = \{\varnothing, \{0\}\}$.
2. $\mathcal{P}(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$.
3. $\mathcal{P}(\mathbb{N}) = \{ \quad \begin{array}{l} \varnothing, \\ \{0\}, \{0,1\}, \{0,2\}, \cdots \\ \{1\}, \{1,2\}, \{1,3\}, \{1,4\}, \cdots \\ \ldots \\ \textit{trop d'éléments pour les énumérer} \quad \} \end{array}$

Quelques propriétés de $\mathcal{P}(\cdot)$

1. $\mathcal{P}(A) \neq \varnothing$.
2. $A \in \mathcal{P}(A)$ et $\varnothing \in \mathcal{P}(A)$.
3. $X \in \mathcal{P}(A) \iff X \subseteq A$.
4. $\{x\} \in \mathcal{P}(A) \iff x \in A$.
5. $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$.
6. $\mathcal{P}(A \cup B) = \{X \cup Y \mid X \in \mathcal{P}(A) \wedge Y \in \mathcal{P}(B)\}$.
7. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
8. En général, $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ est faux.
9. Si A contient $n \in \mathbb{N}$ éléments distincts alors $\mathcal{P}(A)$ contient 2^n éléments.

Produit cartésien

Couple

$$(a, b) \overset{\text{déf}}{=\!=} \{\{a\}, \{a, b\}\}$$

On peut montrer

$$(x, y) = (x', y') \Leftrightarrow x = x' \wedge y = y'.$$

Produit cartésien

$$A \times B \overset{\text{déf}}{=\!=} \{(a, b) \mid a \in A \wedge b \in B\}.$$

Exemples :

1. $\{0, 1\} \times \{\mathrm{a}, \mathrm{b}\} = \{(0, \mathrm{a}), (0, \mathrm{b}), (1, \mathrm{a}), (1, \mathrm{b})\}$.
2. $\{0, 1\} \times \{0, 2\} = \{(0, 0), (0, 2), (1, 0), (1, 2)\}$.

Propriétés du produit cartésien

1. Monotonie du produit cartésien :
   si $A \subseteq C$ et $B \subseteq D$ alors $A \times B \subseteq C \times D$.
2. $\cup$-Distributivité : $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
3. $\cap$-Distributivité : $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
4. $\setminus$-Distributivité : $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.
5. $\emptyset \times A = A \times \emptyset = \emptyset$.

En général, les propriétés suivantes sont fausses :

- $A \times B = B \times A$
- $(A \times B) \times C = A \times (B \times C)$
- $(A \times B) \cup C = (A \cup C) \times (B \cup C)$
- $(A \times B) \cap C = (A \cap C) \times (B \cap C)$.

Somme (union disjointe)

L'*union disjointe* (ou *somme*) de A et B, notée $A \uplus B$ est définie par

$$A \uplus B \stackrel{\text{déf}}{=\!=} (0, a) \mid a \in A\} \cup \{(1, b) \mid b \in B\}.$$

Exemples

1. $\{\mathrm{a}, \mathrm{b}\} \uplus \{\mathrm{a}, \mathrm{c}\} = \{(0, \mathrm{a}), (0, \mathrm{b}), (1, \mathrm{a}), (1, \mathrm{c})\}.$
2. $\{0, 1\} \uplus \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$

Propriétés de l'union disjointe

1. Monotonie : Si $A \subseteq C$ et $B \subseteq D$ alors $A \uplus B \subseteq C \uplus D$.
2. $\cup$-Distributivité : $(A \cup B) \uplus C = (A \uplus C) \cup (B \uplus C)$ et $C \uplus (A \cup B) = (C \uplus A) \cup (C \uplus B)$.
3. $\cap$-Distributivité : $(A \cap B) \uplus C = (A \uplus C) \cap (B \uplus C)$ et $C \uplus (A \cap B) = (C \uplus A) \cap (C \uplus B)$.
4. $\setminus$-Distributivité : $(A \setminus B) \uplus C = (A \uplus C) \setminus (B \uplus C)$ et $C \uplus (A \setminus B) = (C \uplus A) \setminus (C \uplus B)$.
5. $A \uplus B = \{0\} \times A \cup \{1\} \times B$.

En général, les propriétés suivantes sont fausses :

- $\emptyset \uplus A = A \uplus \emptyset = A$, $A \uplus B = B \uplus A$
- $(A \uplus B) \uplus C = A \uplus (B \uplus C)$
- $(A \uplus B) \times C = (A \times C) \uplus (B \times C)$

Partition d'un ensemble

On appelle *partition* de E tout ensemble $\mathcal{Y}$ inclus dans $\mathcal{P}(E)$ qui satisfait les propriétés suivantes :

1. $\forall A\ A \in \mathcal{Y} \Rightarrow\ A \neq \varnothing$
2. $\forall x\ x \in E \Rightarrow\ \exists A\ A \in \mathcal{Y} \wedge x \in A$
3. $\forall A\ A \in \mathcal{Y} \Rightarrow\ \forall B\ B \in \mathcal{Y} \Rightarrow\ (A \neq B \Leftrightarrow A \cap B = \varnothing)$

Exemples

- Si l'ensemble E est non vide, alors $\{E\}$ et $\{\{x\} \mid x \in E\}$ sont des partitions de E.
- Si $E = \{1, 2, 3\}$ alors les partitions de E sont $\{\{1, 2, 3\}\}$, $\{\{1\}, \{2\}, \{3\}\}$, $\{\{1, 3\}, \{2\}\}$, $\{\{1, 2\}, \{3\}\}$, $\{\{2, 3\}, \{1\}\}$.

Relations

- Une *relation* R entre A et B est un sous-ensemble de $A \times B$.
  Exemple :
  $$R_0 \subseteq \{1, 2, 3\} \times \{1, \mathrm{a}, \mathrm{b}\}, \; R_0 \stackrel{\text{déf}}{=\!=} \{(1, 1), (1, \mathrm{a}), (2, \mathrm{a})\}.$$
- $(\mathrm{a}, \mathrm{b}) \in R$ est aussi noté $\mathrm{a}R\mathrm{b}$, ou $R(\mathrm{a}, \mathrm{b})$.
  Exemple : $(1, \mathrm{a}) \in R_0$, $(1, 1) \in R_0$, $(2, 1) \notin R_0$.

Relations (II)

- Le *domaine de R* :

$$\mathcal{D}(R) = \{x \in A \mid \exists y \in B \cdot (x, y) \in R\}$$

  Exemple : $\mathcal{D}(R_0) = \{1, 2\}$.

- Le *co-domaine de R* (ou son image) :

$$\mathcal{IM}(R) = \{y \in B \mid \exists x \in A \cdot (x, y) \in R\}$$

  Exemple $\mathcal{IM}(R_0) = \{1, a\}$.

Réflexivité, transitivité

Pour toutes les relations dans les examples on suppose :
$R_i \subseteq \{1,2,3\} \times \{1,2,3\}$

- $R \subseteq A \times A$ est *réflexive*, si $\forall x \in A \cdot (x,x) \in R$.

  Exemples

  - $R_1 \stackrel{\text{déf}}{=\!=} \{(1,1),(1,2),(2,2),(3,3)\}$ réflexive
  - $R_2 \stackrel{\text{déf}}{=\!=} \{(1,1),(2,1),(3,3)\}$ pas réflexive

- $R \subseteq A \times A$ est *transitive*, si
  $\forall x, y, z \in A \cdot (x,y) \in R \wedge (y,z) \in R \implies (x,z) \in R$

  Exemples

  - $R_3 \stackrel{\text{déf}}{=\!=} \{(1,2),(2,1),(1,1),(2,2),(3,1),(3,2)\}$ transitive
  - $R_4 \stackrel{\text{déf}}{=\!=} \{(1,2),(2,3),(2,2)\}$ pas transitive

Symétrie

- $R \subseteq A \times A$ est *symétrique*, si
  $\forall x\ , y \in A \cdot (x, y) \in R \implies (y, x) \in R$

  Exemples

  - $R_5 \stackrel{\text{déf}}{=} \{(1,2),(2,1),(1,1),(2,2),(3,1),(1,3)\}$ symétrique
  - $R_3 \stackrel{\text{déf}}{=} \{(1,2),(2,1),(1,1),(2,2),(3,1),(3,2)\}$ pas symétrique

- $R \subseteq A \times A$ est *anti-symétrique*, si
  $\forall x\ , y \in A \cdot (x, y) \in R \wedge (y, x) \in R \implies y = x$

  Exemples

  - $R_7 \stackrel{\text{déf}}{=} \{(1,2),(2,1),(1,1),(3,3),(3,1),(1,3)\}$ anti-symétrique
  - $R_5 \stackrel{\text{déf}}{=} \{(1,2),(2,1),(1,1),(2,2),(3,1),(1,3)\}$ pas anti-symétrique

Autres propriétés

- $R \subseteq A \times A$ est *asymétrique*, si $\forall x , y \in A \cdot (x, y) \in R \Rightarrow \neg(y, x) \in R$.

  Exemples

  - $R_8 \stackrel{\text{déf}}{=\!=} \{(1, 2), (2, 3)\}$ asymétrique
  - $R_9 \stackrel{\text{déf}}{=\!=} \{(1, 2), (2, 3), (3, 2)\}$ pas asymétrique

- $R \subseteq A \times A$ est *irréflexive*, si $\forall x \in A \cdot \neg(x, x) \in R$

  Exemples

  - $R_8 \stackrel{\text{déf}}{=\!=} \{(1, 2), (2, 3)\}$ irréflexive
  - $R_5 \stackrel{\text{déf}}{=\!=} \{(1, 2), (2, 1), (1, 1), (2, 2), (3, 1), (1, 3)\}$ pas irréflexive

Remarque : Une relation irréflexive et transitive est forcément asymétrique.

Relations remarquables

- $R \subseteq A \times B$ est *totale*, si $\mathcal{D}(R) = A$
- $R \subseteq A \times A$ est une *relation d'équivalence*, si R est transitive, symétrique et réflexive.
- $R \subseteq A \times A$ est un *ordre*, si R est transitive, réflexive et anti-symétrique.

Classes d'équivalence et ensemble quotient

- Soit $R \subseteq A \times A$ une relation d'équivalence sur A. Pour chaque $x \in A$, on appelle *classe d'équivalence* de x (modulo R) le sous-ensemble de A défini par :

$$\mathcal{C}(x) \overset{\text{déf}}{=\!=} \{y \in A | (x, y) \in R\}$$

- Tout élément de $\mathcal{C}(x)$ est appelé *un représentant* de la classe $\mathcal{C}(x)$.
- L'ensemble des classes d'équivalence modulo R se nomme *ensemble quotient* de E par R et se note E/R.

Exemples :

- Le relation d'égalité dans un ensemble E quelconque est une relation d'équivalence, d'ensemble quotient $\{\{x\} \mid x \in E\}$
- Pour tout entier $n > 0$, la congruence modulo n sur les entiers est une relation d'équivalence, d'ensemble quotient $\mathbb{Z}/n\mathbb{Z} = \{\mathcal{C}(0), \mathcal{C}(1), \ldots, \mathcal{C}(n-1)\}$.

Théorème

Théorème

A toute relation R d'équivalence sur M correspond une partition de M en classes d'équivalence, et réciproquement, toute partition de M définit une relation d'équivalence dont les classes coincident avec les éléments de la partition donnée.

Démonstration.

On va prouver d'abord "$\Rightarrow$". Soit $\mathcal{Y}_R = \{\mathcal{C}(x) \mid x \in M\}$. On montre que $\mathcal{Y}_R$ est une partition de M.

- Par la réflexivité de R, on a $\forall x \in M$, $x \in \mathcal{C}(x)$, et donc $\forall A \in \mathcal{Y}_R$, $A \neq \varnothing$.
- Par la réflexivité de R, on a $\forall x \in M$, $x \in \mathcal{C}(x)$, et donc $\forall x \in M$, $\exists A \in \mathcal{Y}_R$ tel que $x \in A$.

Théorème - continuation(I)

Démonstration.

Rappel : $\mathcal{Y}_R = \{\mathcal{C}(x) \mid x \in M\}$.

- On prouve $\forall(A, B) \in \mathcal{Y}_R \times \mathcal{Y}_R,\ A \cap B \neq \emptyset \Rightarrow A = B$. Soit $(A, B) \in \mathcal{Y}_R \times \mathcal{Y}_R$ quelconque.
  Par definition, $\exists(x, y) \in M \times M$, tel que $A = \mathcal{C}(x)$ et $B = \mathcal{C}(Y)$
  On prouve $\mathcal{C}(x) \cap \mathcal{C}(y) \neq \emptyset \Rightarrow \mathcal{C}(x) = \mathcal{C}(y)$.
  Soit $(x, y) \in M \times M$ et supposons $\mathcal{C}(x) \cap \mathcal{C}(y) \neq \emptyset$. Donc $\exists z \in \mathcal{C}(x) \cap \mathcal{C}(y)$, et on obtient xRz et yRz.
  Par la symétrie de R, zRx et ensuite par transitivité, yRx.
  Maintenant soit $t \in \mathcal{C}(x)$ quelconque. Donc xRt, et comme yRx, par transitivité on obtient yRt, donc $t \in \mathcal{C}(y)$ et on conclu $\mathcal{C}(x) \subseteq \mathcal{C}(y)$. De facon similaire on montre $\mathcal{C}(y) \subseteq \mathcal{C}(x)$, et donc $\mathcal{C}(x) = \mathcal{C}(y)$

Théorème - continuation(II)

Démonstration.

On prouve "$\Leftarrow$". Soit $\mathcal{Y} \subseteq \mathcal{P}(M)$ une partition et soit $R_{\mathcal{Y}} = \{(x, y) \mid \exists P \in \mathcal{Y}, (x \in P \text{ et } y \in P)\}$. On prouve d'abord que $R_{\mathcal{Y}}$ est une relation d'équivalence.

- Par définition, $\forall x \in M$, $\exists P \in \mathcal{Y}$ tel que $x \in P$, d'où $(x, x) \in R_{\mathcal{Y}}$, et donc $R_{\mathcal{Y}}$ est réflexive.
- Pour tout $(x, y) \in M \times M$, on a $(x, y) \in R_{\mathcal{Y}} \iff (\exists P \in \mathcal{Y}, (x \in P \text{ et } y \in P)) \iff (\exists P \in \mathcal{Y}, (y \in P \text{ et } x \in P)) \iff (y, x) \in R_{\mathcal{Y}}$
  et donc $R_{\mathcal{Y}}$ est symétrique.
- Soit $((x, y), z) \in (M \times M) \times M$ tels que $(x, y) \in R_{\mathcal{Y}}$ et $(y, z) \in R_{\mathcal{Y}}$. Il existe $P \in \mathcal{Y}$ et $Q \in \mathcal{Y}$ tels que $(x \in P \text{ et } y \in P)$ et $(y \in Q \text{ et } z \in Q)$. Comme $P \cap Q \neq \varnothing$ et $\mathcal{Y}$ est une partition, on a $P = Q$, donc $(x \in P \text{ et } z \in P)$, et donc $(x, z) \in R_{\mathcal{Y}}$ et on conclu que $R_{\mathcal{Y}}$ est transitive.

Composition de relations

Soient $R \subseteq A \times B$ et $R' \subseteq B \times C$ deux relations. La *composition* de R et R' notée $R \circ R'$ est définie par
$R' \circ R \stackrel{\text{déf}}{=} \{(a, c) \in A \times C \mid \exists b \in B \cdot (a, b) \in R \wedge (b, c) \in R'\}$.

Propriétés :

1. La composition des relations est associative.
2. Elle est monotone.
3. $\cup$-distributive : $(R_1 \cup R_2) \circ R = (R_1 \circ R) \cup (R_2 \circ R)$.
4. $(R_1 \cap R_2) \circ R \subseteq (R_1 \circ R) \cap (R_2 \circ R)$.

L'inverse d'une relation R est la relation
$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$.
Propriété : $(R^{-1})^{-1} = R$.

Relations n-aires

$R \subseteq A \times B$ est une relation binaire.
On peut étendre cette notion aux relations n-aires :
$R \subseteq A_1 \times \cdots \times A_n$ où $n \in \mathbb{N}$.

- Pour $n = 0$, la relation R est soit la constante vrai soit la constante faux.
- Pour $n = 1$, la relation R est un sous-ensemble A_1 de A. Elle induit un *prédicat* $\mathcal{P}_{A_1}$, tel que $\mathcal{P}_{A_1}(x)$ est vrai ssi $x \in A_1$.

Relations et fonctions

- $f \subseteq A \times B$ est une *fonction*, si pour tout $x \in A$ il existe au plus un $y \in B$ tel que xRy.

  Exemples : Pour toutes les fonctions dans les examples on suppose : $f_i \subseteq \{1, 2, 3\} \times \{a, b, c\}$.

  - $f_1 \stackrel{\text{déf}}{=\!=} \{(1, a), (2, b)\}$ fonction
  - $f_2 \stackrel{\text{déf}}{=\!=} \{(1, a), (2, c), (1, b)\}$ pas fonction

- On écrit $f : A \to B$ au lieu de $f \subseteq A \times B$ et $f(x) = y$ au lieu de $(x, y) \in f$.
  Example : $f_1 : \{1, 2, 3\} \to \{a, b, c\}$ défini par $f_1(1) = a$, $f_1(2) = b$

Relations et fonctions (II)

- Une fonction f est une *application*, si pour tout $x \in A$ il existe un $y \in B$ unique tel que $f(x) = y$ (i.e. f est fonction et $\mathcal{D}(f) = A$).

  Exemples :

  - $f_3 \stackrel{\text{déf}}{=\!=} \{(1, \text{a}), (2, \text{b}), (3, \text{a})\}$ application
  - $f_1 \stackrel{\text{déf}}{=\!=} \{(1, \text{a}), (2, \text{b})\}$ fonction, mais pas application
  - $f_2 \stackrel{\text{déf}}{=\!=} \{(1, \text{a}), (2, \text{c}), (1, \text{b})\}$ ni fonction, ni application

Propriétés des fonctions

- Une fonction f est *injective* (on dit aussi qu'elle est une injection), si $\forall\, x, y \in A,\ f(x) = f(y) \implies x = y$
- Une fonction f est *surjective* (on dit aussi qu'elle est une surjection), si $\forall y \ \in B \exists x \in A$ tel que $f(x) = y$ (i.e. $\mathcal{IM}(f) = B$)
- Une fonction f est *bijective* (on dit aussi qu'elle est une bijection), si elle est injective et surjective.

Théorèmes

Théorème

Soit $f : A \to B$ *et* $g : B \to C$ *deux fonctions.*

- *Si* f *et* g *sont injectives, alors* $g \circ f$ *est injective.*
- *Si* f *et* g *sont surjectives, alors* $g \circ f$ *est surjective.*
- *Si* f *et* g *sont bijectives, alors* $g \circ f$ *est bijective.*
- *Si* $g \circ f$ *est injective, alors* f *est injective.*
- *Si* $g \circ f$ *est surjective, alors* g *est surjective.*

Théorèmes (2)

Notation : id_A denote l'identité sur A, c'est-à-dire $\{(x, x) \mid x \in A\}$.

Théorème

Soit $f : A \to B$ une application. Il existe une application injective $g : B \to A$ telle que $g \circ f = id_A$ ssi f est bijective.

Démonstration.

On va prouver d'abord " $\Rightarrow$ ".
Soit $g : B \to A$ une application injective telle que $g \circ f = id_A$.
Alors $f(x_1) = f(x_2)$ implique
$x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2$, donc f est injective.
Soit $y \in B$ quelconque. Alors $\exists x \in A$ tel que $x = g(y)$. Donc $(g \circ f)(x) = g(f(x)) = x = g(y)$, et par l'injectivité de g, on obtient $f(x) = y$. Donc f est surjective.

Théorèmes (3)

Théorème

Soit $f : A \to B$ une application. Il existe une application injective $g : B \to A$ telle que $g \circ f = id_A$ ssi f est bijective.

Démonstration.

On prouve "$\Leftarrow$".
Soit $g \subseteq B \times A$, définie par $g = f^{-1}$.
L'injectivité de f implique que g est une fonction : $(y, x_1) \in g$ et $(y, x_2) \in g$ impliquent $f(x_1) = y = f(x_2)$, et donc $x_1 = x_2$.
La surjectivité de f implique que g est une application : pour tout $y \in B$, il existe $x \in A$, tel que $f(x) = y$, et donc $g(y) = x$.
g est injective : si $g(y_1) = x = g(y_2)$, alors $y_1 = f(x) = y_2$ et donc $y_1 = y_2$ (f est une fonction).
En plus, pour tout $x \in A$, on a $(x, f(x)) \in f$, d'où $(f(x), x) \in g$ et on obtient $(g \circ f)(x) = g(f(x)) = x$.

Théorèmes (4)

Corollaire

Soit $f : A \to B$ *une application bijective. Alors* f^{-1} *est une application bijective telle que* $f^{-1} \circ f = id_A$ *et* $f \circ f^{-1} = id_B$*.*

Démonstration.

On a prouvé que f^{-1} est une application injective et que $f^{-1} \circ f = id_A$.

f^{-1} est surjective : comme f est une application, ,pour tout $x \in A$, il existe $y \in B$ tel que $(x, y) \in f$, et donc $(y, x) \in f^{-1}$.

En plus, pour tout $y \in B$, on a $(y, f^{-1}(y)) \in f^{-1}$, d'où $(f^{-1}(y), y) \in f$ et on obtient $(f \circ f^{-1})(y) = f(f^{-1}(y)) = y$.

$\square$

Ordres partiels

Soit R une relation sur A. R est *un ordre (partiel)* sur A ssi

1. R est reflexive : $\forall a \in A \cdot aRa$.
2. R est anti-symétrique : $\forall a, b \in A \cdot aRb \wedge bRa \Rightarrow a = b$.
3. R est transitive : $\forall a, b, c \in A \cdot aRb \wedge bRc \Rightarrow aRc$.

Soit S une relation sur A. S est *un ordre strict* sur A ssi

1. S est asymétrique : $\forall a, b \in A \cdot aSb \Rightarrow \neg bSa$.
2. S est transitive : $\forall a, b, c \in A \cdot aSb \wedge bSc \Rightarrow aSc$.

A tout ordre strict S on peut associer l'ordre (non strict) $R = S \cup \{(a, a) | a \in A\}$.
Reciproquement, a tout ordre non strict R on peut associer l'ordre strict $S = R \setminus \{(a, a) | a \in A\}$.
On va utiliser souvent $\prec$ et $\preceq$ pour noter un ordre strict et son ordre non strict associé.

Ordre total

Un ordre R est *total* (ou linéaire), si on a aRb ou bRa, pour tout $a, b \in A$.
On va utiliser souvant $\sqsubset$ et $\sqsubseteq$ pour noter un ordre total strict et son ordre total non strict associé.
Un ordre total $\sqsubset$ (resp. $\sqsubseteq$) est un *ordonnancement topologique* d'un ordre partiel $\prec$ (resp. $\preceq$) si $a \prec b \Rightarrow a \sqsubset b$ (resp. $a \preceq b \Rightarrow a \sqsubseteq b$).

Théorème

Pour tout ordre partiel $\prec$ (resp. $\preceq$) on peut construire un ordonnancement topologique $\sqsubset$ (resp. $\sqsubseteq$).

Application : ordonnancement des taches.

Isomorphisme des relations

Soit R une relation sur A et S une relation sur B. Alors R et S sont *isomorphes* si et seulement si il existe une fonction bijective $f : A \mapsto B$ telle que $a \; R \; b$ si et seulement si $f(a) \; S \; f(b)$.

Théorème

Pour tout ordre $\prec$ (resp. $\preceq$) sur un ensemble A, on peut construire un ordre isomorphe $\subset$ (resp. $\subseteq$) sur l'ensemble $\mathcal{P}(A)$.

Démonstration.

On construit la bijection $f : A \mapsto \mathcal{P}(A)$ donnée par
$f(a) \stackrel{def}{=} \{x \in A | x \prec a\}$. $\square$

Exemples

- $(\mathbb{N}, \leq)$ est un ordre total non strict.
- $(\mathbb{N}, <)$ est un ordre total strict.
- $(\mathcal{P}(\{1, 2, 3\}), \subset)$ est un ordre partiel qui n'est pas total.
- $\mathbb{N}^*$ doté de l'ordre lexigrographique est un ordre total.
- $\mathbb{N}^*$ doté de l'ordre prefixe est un ordre partiel qui n'est pas total.
- $(\mathbb{Z}, \leq)$ est un ordre total.

Ordres bien-fondés et exemples

Soit $\preceq$ un ordre sur A. Une partie de A totalement ordonnée s'appelle *une chaîne* de A.
Un ordre $\leq$ est dit *bien-fondé* s'il n'y pas de chaîne décroissante infinie $a_0 > a_1 > a_2 \cdots$.

- $(\mathbb{N}, \leq)$ est un ordre bien-fondé.
- $\mathbb{N}^*$ doté de l'ordre lexigrographique n'est pas un ordre bien-fondé.
- $(\mathcal{P}(\mathbb{N}), \subseteq)$ n'est pas un ordre bien-fondé.
- $(\mathbb{Z}, \leq)$ n'est pas un ordre bien-fondé.
- $(\mathbb{R}, \leq)$ n'est pas un ordre bien-fondé.

Théorèmes (5)

Théorème (Cantor-Bernstein)

Soit $f : A \to B$ et $g : B \to A$ deux applications injectives. Alors il existe une application bijective $h : A \to B$.

Théorème (Cantor)

Soit A un ensemble. Alors il n'existe pas de surjection (et donc, pas de bijection) de A vers $\mathcal{P}(A)$.

Preuve

- Supposons qu'il y ait une fonction f surjective de A vers $\mathcal{P}(A)$.
- Soit $X = \{x \in A \mid x \notin f(x)\}$. Donc $X \subseteq A$ et $X \in \mathcal{P}(A)$.
- A cause de la surjectivité de f, il existe x_0 tel que $f(x_0) = X$.
- On obtient : $x_0 \in f(x_0) \iff x_0 \in X \iff x_0 \notin f(x_0)$ contradiction.

Equipotence

- Soient A et B deux ensembles. A et B sont *equipotents* ssi il existe une bijection de A vers B.
- On note : $A \approx B$.
- $\approx$ est une relation d'equivalence

On peut prouver :

- $A \times B \approx B \times A$
- $(A \times B) \times C \approx A \times (B \times C)$
- $A \uplus \emptyset \approx A$
- $A \uplus B \approx B \uplus A$
- $(A \uplus B) \uplus C \approx A \uplus (B \uplus C)$
- $(A \uplus B) \times C \approx (A \times C) \uplus (B \times C)$

Ensemble infinis, dénombrables

- Un ensemble A est *infini* ssi il est équipotent à une de ses parties propres. Sinon, il est *fini*.
- L'ensemble A est appelé *dénombrable* ssi $\mathbb{N} \approx A$ ou A est fini.

Théorème

- *$\mathbb{N}^2$ est dénombrable.*
- *tout produit cartésien fini d'ensembles dénombrables est dénombrable.*
- *Toute union dénombrable d'ensembles dénombrables est dénombrable.*
- *l'ensemble des rationnels $\mathbb{Q}$ est dénombrable.*
- *A et $\mathcal{P}(A)$ ne sont pas équipotents.*
- *$\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.*

$\mathbb{R}$ n'est pas dénombrable

-

	d_1	d_2	d_3	$\cdots$	d_n	$\cdots$
r_1	3	1	1	$\cdots$	7	$\cdots$
r_2	0	1	2	$\cdots$	5	$\cdots$
r_3	4	9	0	$\cdots$	0	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
r_n	0	1	0	$\cdots$	0	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

- supposons que les r_i forment la liste des réels de $(0, 1)$.
- soit r le réel tel que $r = 0, e_1 e_2 \cdots e_n \cdots$ où $e_i = d_i + 1$ si $d_i \neq 9$ et $e_i = 0$ si $d_i = 9$
- donc r n'est pas parmi les r_i ...
- donc l'ensemble des réels de $(0, 1)$ est non-dénombrable, et donc $\mathbb{R}$ n'est pas dénombrable

Cardinaux

- Soit A un ensemble ; le cardinal de A (noté $|A|$) est la classe d'équivalence des ensembles équipotents à A.
- $|A| + |B| \stackrel{\text{déf}}{=\!=} |A \uplus B|$
- $|A| \cdot |B| \stackrel{\text{déf}}{=\!=} |A \times B|$
- $|A|^{|B|} \stackrel{\text{déf}}{=\!=} |A^B|$ ou A^B est l'ensemble des fonctions de A vers B.
- on note $|A| \leq_e |B|$ ssi il existe une injection de A dans B

On peut prouver :

- si $A \subseteq B$ alors $|A| \leq_e |B|$
- $|A| <_e |\mathcal{P}(A)|$ (conséquence du Th. de Cantor)
- $\leq_e$ est une rélation d'ordre (conséquence du Th. de Cantor-Bernstein)

Ensembles inductifs

Plan du chapitre 5

Définitions inductives

La définition inductive d'une partie X d'un ensemble U consiste :

1. en la donnée explicite de certains éléments de X (la base) ;
2. en la donnée de moyens de construire de nouveaux éléments de X à partir d'éléments déjà connus (construits), ce sont les étapes inductives ;

Définitions inductives

Soit U un ensemble. Une définition inductive d'une partie X de U est donnée :

1. d'un sous ensemble B de U ;
2. d'un ensemble K de fonctions (partielles) $f : U^{a(f)} \mapsto U$, où $a(f)$ est l'arité de f (le nombre d'arguments).

L'ensemble X est défini comme étant **le plus petit** ensemble vérifiant les assertions (B) et (I) suivantes :

(B) $B \subseteq X$;

(I) $\forall f \in K, \forall x_1, \ldots, x_{a(f)} \in X \cdot f(x_1, \ldots, x_{a(f)}) \in X$.

Définitions inductives

L'ensemble ainsi défini existe. On a $X = \bigcap_{Y \in \mathcal{Y}} Y$, où $\mathcal{Y} = \{Y \in U | B \subseteq Y \text{ et } Y \text{ vérifie } (I)\}$.

1. Par définition $\bigcap_{Y \in \mathcal{Y}} Y$ est plus petit que tout ensemble qui vérifie (B) et (I).
2. On s'assure que $\bigcap_{Y \in \mathcal{Y}} Y$ vérifie (B) et (I).

(B) : $\forall Y \in \mathcal{Y} \cdot B \subseteq Y$. Donc $B \subseteq \bigcap_{Y \in \mathcal{Y}} Y$.

(I) : Soient $f \in K$ et $x_1, \ldots, x_{a(f)} \in \bigcap_{Y \in \mathcal{Y}} Y$. Alors pour tout $Y \in \mathcal{Y}$ on a $x_1, \ldots, x_{a(f)} \in Y$ et comme tout $Y \in \mathcal{Y}$ vérifie (I), on obtient $f(x_1, \ldots, x_{a(f)}) \in Y$, et donc $f(x_1, \ldots, x_{a(f)}) \in \bigcap_{Y \in \mathcal{Y}} Y$.

Définition explicite

Théorème

Si X est défini inductivement par (B, K) alors $X = \bigcup_{i \in \mathbb{N}} X_i$ où

1. $X_0 = B$
2. $X_{i+1} = X_i \cup \{f(x_1, \ldots, x_{a(f)}) \mid f \in K, x_1, \ldots, x_{a(f)} \in X_i\}$

Démonstration.

1. Pour montrer $\bigcup_{i \in \mathbb{N}} X_i \subseteq X$, on montre, par récurrence sur i, $\forall i \in \mathbb{N}, X_i \subseteq X$.
2. Pour montrer $X \subseteq \bigcup_{i \in \mathbb{N}} X_i$ on montre que $\bigcup_{i \in \mathbb{N}} X_i$ vérifie (B) et (I).

□

Principe de preuve par induction

Théorème

Soit $X \subseteq U$ *un ensemble défini inductivement par* (B, K)*. Pour montrer* $\forall x \in X \cdot P(x)$ *il sufit de montrer :*

1. *Cas de base : pour tout* $b \in B$*, on a* $P(b)$ *vraie.*
2. *Pas d'induction : pour tout* $f \in K$*, pour tous* $x_1, \ldots, x_{a(f)} \in U$*, si* $P(x_1), \ldots, P(x_{a(f)})$ *sont vraies, alors* $P(x_1, \ldots, x_{a(f)})$ *est vraie.*

Démonstration.

Soit $\mathcal{P} \stackrel{def}{=} \{x \in U \mid P(x)\}$. Alors, il suffit de montrer que $\mathcal{P}$ vérifie (B) et (I) et exploiter la minimalite de X.
On obtient $X \subseteq \mathcal{P}$, et donc tous les éléments de X satisfont P. $\square$

Définition non-ambigue

Théorème

Une définition (B, K) *est* *non-ambigue* *si*

1. *pour tout* $f \in K$, *et* $x_1, \ldots, x_{a(f)} \in X$, $f(x_1, \ldots, x_{a(f)}) \notin B$;
2. *pour tout* $f, f' \in K$, *et* $x_1, \ldots, x_{a(f)}, x'_1, \ldots, x'_{a(f')} \in X$, $f(x_1, \ldots, x_{a(f)}) = f'(x'_1, \ldots, x'_{a(f')})$ *implique* $f = f'$ *et* $x_1 = x'_1, \ldots, x_{a(f)} = x'_{a(f')}$.

Fonctions définies inductivement

Théorème

Soit $X \subseteq U$ un ensemble défini inductivement par (B, K) tel que (B, K) soit non-ambigue. Soit G un ensemble quelconque, soit $g_B : B \mapsto G$ une fonction et une famille de fonctions $g_f : U^{2 \times a(f)} \mapsto G$, pour tout $f \in K$. Il existe une unique fonction $g : X \mapsto G$ telle que

1. *pour tout $x \in B$, $g(x) = g_B(x)$;*
2. *pour tout $f \in K$, et $x_1, \ldots, x_{a(f)} \in X$,*
   $g(f(x_1, \ldots, x_{a(f)})) = g_f(x_1, \ldots, x_{a(f)}, g(x_1), \ldots, g(x_{a(f)}))$.

Ensembles inductifs

1. L'ensemble des entier $\mathbb{N}$ est donné par

   (B) $0 \in \mathbb{N}$;
   (I) si $n \in \mathbb{N}$, alors $S(n) \in \mathbb{N}$.

   Remarque : d'habitude on note $n + 1 = S(n)$, et on utilise par exemple 3 à la place de $S(S(S(0)))$.

2. L'ensemble des listes $li(\{0, 1\})$ avec des 0 et 1 est donné par

   (B) $[] \in li(\{0, 1\})$;
   (I) si $l \in li(\{0, 1\})$, alors $0 :: l, 1 :: l \in li(\{0, 1\})$.

3. L'ensemble des arbres binaires $arb(\{0, 1\})$ avec des 0 et 1 dans les noeuds est donné par

   (B) $F \in arb(\{0, 1\})$;
   (I) si $g, d \in arb(\{0, 1\})$, alors $N(g, 0, d), N(g, 1, d) \in arb(\{0, 1\})$.

Generalisation à un ensemble fini *Elements* à la place de $\{0, 1\}$.

Raisonnements par récurrence structurelle

Récurrence sur les listes

P est un prédicat arbitraire sur les listes

$$\boxed{\frac{\mathrm{P}([\,]) \qquad \forall x\ \forall l\ \ \mathrm{P}(l) \Rightarrow \mathrm{P}(\mathrm{x} :: \mathrm{l})}{\forall l\ \ \mathrm{P}(l)}}$$

Récurrence sur les arbres binaires

P est un prédicat arbitraire sur les arbres binaires

$$\boxed{\frac{\mathrm{P}(\mathrm{F}) \qquad \forall g\ \forall x\ \forall d\ \ \mathrm{P}(g) \Rightarrow \mathrm{P}(d) \Rightarrow \mathrm{P}(\mathrm{N}(g,x,d))}{\forall a\ \ \mathrm{P}(a)}}$$

Rappel : $P \Rightarrow Q \Rightarrow R$ se lit $P \Rightarrow (Q \Rightarrow R)$

Ceci se généralise à tous les types inductifs

Exemple : bégaiement et longueur

```
let rec begaie = function
  | [] → []
  | x :: l → x :: x :: begaie l
```

Conjecture : le bégaiement double la longueur

$\forall l$ longueur (begaie$l$) = 2 × longueur$l$

```
let rec longueur = function
  | [] → 0
  | x :: l → 1 + longueur l
```

On pose $P(l) \stackrel{\text{déf}}{=}$ longueur (begaie$l$) = 2 × longueur$l$

Montrons $\forall l$ $P(l)$ par récurrence structurelle sur l

Cas de base

$$
\mathcal{D}_0 \left\{
\begin{array}{ll}
 & \mathsf{longueur}\,(\mathsf{begaie}\,[\,]) \\
= & \quad \{\text{définition de } \mathsf{begaie}\,\} \\
 & \mathsf{longueur}\,([\,]) \\
= & \quad \{\text{définition de } \mathsf{longueur}\,\} \\
 & 0 \\
= & \quad \{\text{arithmétique}\} \\
 & 2 \times 0 \\
= & \quad \{\text{définition de } \mathsf{longueur}\,\} \\
 & 2 \times \mathsf{longueur}\,[\,]
\end{array}
\right.
$$

Pas de récurrence

Soient l_0 et x_0 quelconques vérifiant l'hypothèse de récurrence $\overbrace{\text{hrec}}^{1}$
avec hrec $\stackrel{\text{déf}}{=\!=}$ longueur (begaie l_0) $=$ $2 \times$ longueur l_0

$$\mathcal{D}_1 \left\{ \begin{array}{ll} & \text{longueur (begaie } (x_0 :: l_0)) \\ = & \quad \{\text{définition de begaie}\} \\ & \text{longueur}(x_0 :: x_0 :: \text{begaie } l_0) \\ = & \quad \{\text{définition de longueur}\} \\ & 1 + \text{longueur } (x_0 :: \text{begaie } l_0) \\ = & \quad \{\text{définition de longueur}\} \\ & 1 + 1 + \text{longueur (begaie } l_0) \\ = & \quad \{\text{hypothèse de récurrence } 1\} \\ & 1 + 1 + 2 \times \text{longueur } l_0 \\ = & \quad \{\text{arithmétique}\} \\ & 2 \times (1 + \text{longueur } l_0) \\ = & \quad \{\text{définition de longueur}\} \\ & 2 \times (\text{longueur } (x_0 :: l_0)) \end{array} \right.$$

Assemblage (préparation)

Case de base

$$\dfrac{\dfrac{}{\text{longueur (begaie } [\,]) = 2 \times (\text{longueur } [\,])}\ \mathcal{D}_0}{\mathsf{P}\ ([\,])}$$

Pas de récurrence

$$\dfrac{\dfrac{\dfrac{\overbrace{\mathsf{P}(l_0)}^{1}}{\text{hrec}}}{\text{longueur (begaie } (x_0 :: l_0)) = 2 \times \text{longueur } (x_0 :: l_0)}\ \mathcal{D}_1}{\mathsf{P}\ (x_0 :: l_0)}$$

Assemblage final

$$\dfrac{\dfrac{}{\mathrm{P}\ ([])}\ \mathcal{D}_0 \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\mathrm{P}(l_0)}^{[1]}}{\mathrm{P}\ (x_0 :: l_0)}\ \mathcal{D}_1}{\mathrm{P}\ (l_0) \Rightarrow \mathrm{P}\ (x_0 :: l_0))}\ \Rightarrow\mathrm{I}[1]}{\forall l\ \ \mathrm{P}\ (l) \Rightarrow \mathrm{P}\ (x_0 :: l)}\ \forall_{\mathrm{I}}}{\forall x\ \ \forall l\ \ \mathrm{P}\ (l) \Rightarrow \mathrm{P}\ (x :: l)}\ \forall_{\mathrm{I}}}{\forall l\ \ \mathrm{P}(l)}$$

Exemple : nombre de feuilles et de clés

```
let rec nbf = function
    | F → 1
    | N(g, x, d) → nbf g + nbf d

let rec nbc = function
    | F → 0
    | N(g, x, d) → nbc g + 1 + nbc d
```

Conjecture : $\forall a \;\; \text{nbf } a = \text{nbc } a + 1$

On pose $\text{P}(a) \stackrel{\text{déf}}{=\!=} \text{nbf } a = \text{nbc } a + 1$

Montrons $\forall a \;\; \text{P}(a)$ par récurrence structurelle sur a

- $\text{nbf F} = 1 = 0 + 1 = \text{nbc F} + 1$
- Soient g_0, x_0 et d_0 quelconques vérifiant les hypothèses de récurrence :

$$\text{nbf } g_0 = \text{nbc } g_0 + 1 \quad \text{et} \quad \text{nbf } d_0 = \text{nbc } g_0 + 1$$

$$\begin{aligned} \text{nbf N}(g_0, x_0, d_0) &= \text{nbf } g_0 + \text{nbf } d_0 \\ &= (\text{nbc } g_0 + 1) + (\text{nbc } d_0 + 1) \qquad \textit{(hyps r} \\ &= (\text{nbc } g_0 + 1 + \text{nbc } d_0) + 1 \\ &= (\text{nbc N}(g_0, x_0, d_0)) + 1 \end{aligned}$$

Fermeture réflexive

Fermer une relation par une propriété revient à compléter la relation pour qu'elle vérifie cette propriété.
Soit $R \subseteq A \times A$ une relation.
La *fermeture réflexive* de R, notée R^{re} est la plus petite relation $Q \subseteq A \times A$ qui contient R et qui est reflexive :

$$(\forall x\ , y \in A \cdot xRy \implies xQy) \wedge (\forall x\ \in A \cdot xQx)$$

Définition constructive de R^{re} :

$$R^{re} = R \cup \{(a, a) \mid a \in A\}.$$

Fermeture transitive

La *fermeture transitive* de R, notée R^+ est la plus petite relation $Q \subseteq A \times A$ qui contient R et qui est transitive :

$$(\forall x\ , y \in A \cdot xRy \implies xQy) \wedge (\forall x\ , y, z \in A \cdot xQy \wedge yQz \implies xQz)$$

Une definition inductive de R^+ :

(B) $R \subseteq R^+$;

(I) si $(a, b), (b, c) \in R^+$, alors $(a, c) \in R^+$.

Définition constructive de R^+ : $R^+ = \bigcup_{i \in \mathbb{N}} R_i$ où

1. $R_0 = R$;
2. $R_{i+1} = R_i \ \cup \ \{(a, c) \mid (a, b), (b, c) \in R_i\}$

Fermeture réflexive-transitive

La *fermeture réflexive-transitive* de R, notée R^* est la plus petite relation $Q \subseteq A \times A$ qui contient R et qui est reflexive et transitive :

$$(\forall x\ , y \in A \cdot x R y \implies x Q y) \wedge (\forall x\ , y, z \in A \cdot x Q y \wedge y Q z \implies x Q z)$$

$$\wedge (\forall x\ \in A \cdot x Q x)$$

Une definition inductive de R^* :

(B) $R \cup \{(a, a) \mid a \in A\} \subseteq R^*$;

(I) si $(a, b), (b, c) \in R^*$, alors $(a, c) \in R^*$.

Définition constructive de R^* : $R^* = \bigcup_{i \in \mathbb{N}} R_i$ où

1. $R_0 = R \cup \{(a, a) \mid a \in A\}$;
2. $R_{i+1} = R_i\ \cup\ \{(a, c) \mid (a, b), (b, c) \in R_i\}$