Spécification et Modélisation Informatiques

(CNAM - 6 crédits ECTS)

Alexandre S. Saidi-Glandus

ECL - LIRIS (UMR 5205 CNRS)

(Alexandre.Saidi@ec-lyon.fr)
(alexandre.saidi@liris.cnrs.fr)

2008-2009

Les outils de formalisation en Informatique

- Matière habituellement désignée (en grande partie) par :
  - *Mathématiques pour l'Informatique* ou
  - *Mathématiques Discrètes*

- Traite des (liste non exhaustive) :
  - Logique Propositionnelle, Calculs des Prédicats, Preuves
  - Théorie des ensembles , Relations, Fonctions,...
  - AEF (et MEF) : Automates (et Machines) d'Etats Finis
  - Spécification et TDA (Types de Données Abstraits)
  - Théorie des Graphes et Algorithmes, ...
  - Notions sur les BDs, l'Algèbre Relationnelle et de Boole, Combinatoire, Complexité, Recherche Op., ...

Idée reçue (à éviter) : $\boxed{\textit{Informatique} = \textit{programmation !}}$

Motivations (suite)

- **A ne pas négliger :**
  - La phase de spécification
  - Les outils et formalismes de spécification (voire de *validation*)
  - Outils employés en modélisation et spécification des Systèmes Informatiques :
    - Génie Logiciels
    - Réseaux Informatiques et de Communication
    - Conception et modélisation des BDs
    - Systèmes d'Information (au sens large)
    - Systèmes transactionnels
    - ...
  - ➥ Une matière de base.

Organisation du cours

Un total de 15 séances

- env. 20h de cours
- env. 20h de TD
- Des études de cas
- Un à deux devoirs
- Un examen final

• A priori, pas de pré requis.
➥ Mais toutes notions Mathématiques et Informatique seront bienvenues.

• Pour rappel : l'UE précédent $\rightarrow$ BAC+2
Mais ici, on a plus de séances.

• Et enfin, l'organisation des séances (1 pause)

Plan Général du cours

Deux grands chapitres :

1. Chapitre 1
   - Logique (propositionnelle, prédicats)
   - Méthodes de Preuve
   - Induction Mathématique
2. Chapitre 2
   - Machines et Automates d'états finis
   - Autre formalismes (UML, RdP)
   - OCL : expression des contraintes
3. Plusieurs exemples traités tout le long.

La logique : Introduction

• **La logique** = la signification des expressions, raisonnements et preuves Mathématiques :

- *Il existe un entier qui n'est pas la somme de deux carrés*
- $\forall n > 0, \Sigma_{k=1}^{n} = \frac{n(n+1)}{2}$

• Est appliquée dans la conception des machines (et ordinateurs), spécification de systèmes, IA, Programmation (construction, vérification), Langages de Programmation, Raisonnement, etc.

• Dans ces domaines, on manipule des *objets*, structurés en **ensembles** ;

➙ *Combinaisons* : ensembles non ordonnés de collections d'objets

➙ *Relations* : ensembles ordonnés de tuples ;

➙ *Graphes* : ensembles de noeuds et d'arêtes (d'arcs) ;

➥ des *Machines d'états finis* pour modéliser les ordinateurs

Définition

- **Proposition =** une phrase déclarative qui est vraie ou fausse

1. Paris est la capitale de France.
2. $1 + 1 = 2$
3. $2 + 2 = 3$

Mais que penser de :

1. Quelle heure est-il ?
2. Lisez cette page.
3. $x + 2 = 5$
4. $10 > x > y > 0, x^2 + y^2 = 25$

➤ **Logique Propositionnelle, Calcul Propositionnel**

Definition (négation)

Si p est une proposition, alors $\neg p$ est une proposition

Exemple

La négation de *"aujourd'hui, on est jeudi"* :

- ➥ On peut écrire : $jeudi(ajourdhui)$ et $\neg jeudi(ajourdhui)$
- ➥ Ou $jour(ajourdhui, jeudi)$ et $\neg jour(ajourdhui, jeudi)$

- **La table de vérité :**

p	$\neg p$
Vrai	*Faux*
Faux	*Vrai*

Tab.: La table de vérité de la négation.

Definition (conjonction, disjonction)

Si p, q sont des propositions, alors $p \wedge q$ et $p \vee q$ sont des propositions

Exemple

Conjonction : "aujourd'hui, on est jeudi" et "il pleut aujourd'hui" ?
Disjonction : "aujourd'hui, on est jeudi" ou "il pleut aujourd'hui" ?

- **La table de vérité :** (V=Vrai, F=Faux)

p	q	$p \wedge q$	$p \vee q$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F

Tab.: La table de vérité de la conjonction et de la disjonction.

Dans la langue parlée, on emploie souvent un ou exclusif (*ou bien*)

Definition (OuX)

Si p, q sont des propositions, alors $p \bigoplus q$ est une proposition.

Exemple

"Ce chien ne sait parler" ou "je suis la reine d'Angleterre"?

➥ On veut dire : seule une des propositions est vraie.

N.B. : que dire de "Il est dedans" ou (bien) "il est dehors"!

- **La table de vérité :**

p	q	$p \bigoplus q$
V	V	F
V	F	V
F	V	V
F	F	F

Tab.: La table de vérité de OuX.

Definition (Implication)

Si p, q sont des propositions, alors $p \longrightarrow q$ est une proposition.
On a : $p \longrightarrow q \quad \equiv \quad \neg p \vee q$

Exemple

Sachant que *Tout homme est mortel* et *Socrates est un homme* :

$$homme(socrates) \longrightarrow mortel(socrates)\,?$$

Remarque (quelques paraphrases sur l'implication, comme *Si-Alors*)

- *Si p alors q* (ou *Si p, q*)
- *q si p* (ou *q quand p*)
- *p implique (cause) q.*
- *p est suffisant pour q*
- *une condition suffisante pour q est p.*
- *q découle de p.*

Comprendre l'Implication

p	q	$p \longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Tab.: La table de vérité de l'implication

➥ $p \longrightarrow q$ est fausse SSI p est vraie mais q ne l'est pas.

Comprendre l'Implication comme une obligation/contrat

Un politicien : **"Si je suis élu, on rasera gratis."**

➤ S'il est élu, une chance pour que l'on rase gratuitement ;

➤ S'il n'est pas élu, on ne s'y attend pas (même si la personne peut influer sur cette réforme !)

C'est uniquement s'il est élu mais que l'on ne rase pas gratis que les électeurs diront qu'il n'a pas respecté sa promesse.

➥ Correspond au seul cas où l'implication est fausse.

Comprendre l'Implication (suite)

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Exemple (un autre)

Le prof dit :

"Si vous avez 20 à l'examen, vous aurez les félicitations."

➤ *Si vous obtenez 20 au test, vous pouvez vous attendre aux félicitations*

➤ *Mais si vous n'avez pas 20, vous pouvez éventuellement avoir les félicitations (selon d'autres facteurs) : la 3e ligne de la table.*

➤ *Mais si vous avez obtenu 20 mais pas les félicitations, vous aurez l'impression d'être grugé (fausse).*

Contraposée, Converse et Inverse

- A partir de $p \longrightarrow q$, on obtient :
  - **Contraposée** de $p \longrightarrow q$: $\neg q \longrightarrow \neg p$ (appelée aussi *Contrapositif*)

    La contraposée a la même table de vérité que $p \longrightarrow q$
    ➥ sont **équivalents** et on note : $p \longrightarrow q \quad \equiv \quad \neg q \longrightarrow \neg p$
    On utilise la contraposée en *raisonnement pas l'absurde*.
  - **La Converse** de $p \longrightarrow q$: $\quad q \longrightarrow p$
  - **L'Inverse** de $p \longrightarrow q$: $\quad \neg p \longrightarrow \neg q$

    Converse et *Inverse* sont **équivalentes** entre elles.
    Par contre, elles n'ont pas la même table que $p \longrightarrow q$

Exemple

Quels sont la contraposée, la converse et l'inverse de la proposition :
S'il pleut, je prendrai mon parapluie *?*

Terminologies (bis)

- **Rappel** :
  La *Contraposée* (ou *Contrapositif*) de $p \longrightarrow q$: $\neg q \longrightarrow \neg p$

Remarque (paraphrases sur la Contraposée (et donc sur $p \longrightarrow q$))

- *Une condition nécessaire pour p est q* *(si $\neg q$ alors $\neg p$)*
- *p seulement si q.*
- *q est nécessaire pour p.*

➤ *Attention : "q seulement si p" $\neq$ "$p \longrightarrow q$" mais plutôt $q \longrightarrow p$*

Aperçu du raisonnement par l'absurde

- La contraposée utilisée en raisonnement par **l'absurde**.

Exemple (exercice)

Aristote l'a utilisé pour démontrer que *la racine carrée de 2 ne peut pas être un nombre rationnel.*

L'équivalenve logique

1 • Correspond à une double implication et se note $\Leftrightarrow$ (ou $\equiv$).

2 • $p \Leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

3 • $p \Leftrightarrow q$ se dit aussi :

- p si et seulement si q (p SSI q)
- p est nécessaire et suffisant pour q
- Si p alors q et inversement
- p si q et q si p

4 • $p \Leftrightarrow q$ **est vraie si** p **et** q **ont la même valeur de vérité.**

Exercice

Vérifier (4) ci-dessus par la table de vérité de l'équivalence.

Précédence relative des opérateurs

- De gauche à droite :

$$\neg \quad < \quad \wedge \quad < \quad \vee \quad < \quad \rightarrow \quad < \quad \leftrightarrow$$

N.B. : La priorité est l'inverse de la précédence :

➙ C'est la négation qui est la plus prioritaire ici.

➙ Donc $\neg p \rightarrow q \quad = \quad (\neg p) \rightarrow q$,

Exemple

- $\neg p \wedge q = (\neg p) \wedge q \neq \neg(p \wedge q)$
- $p \wedge q \vee r = (p \wedge q) \vee r$

Expression en logique

• La traduction de phrases en langue naturelle vers des expressions logiques est une part essentielle de la spécification de systèmes (matériels ou logiciels).
• Les cahiers des charges sont en général exprimés en français.

Exemples (traduction des phrases en expression logique)

- "vous pouvez accéder à l'intranet seulement si vous êtes inscrit ou vous n'êtes pas mineur"! $(p \longrightarrow q \ : \ p \ seulement \ si \ q)$
  ➥ $acces \longrightarrow (inscrit \vee \neg mineur)$
- "vous ne pouvez pas faire du skate si vous mesurez moins d'1 mètre sauf si vous avez 16 ans (ou plus)"!
  ➥ $(moins1m \wedge \neg plus16ans) \longrightarrow \neg skate$
- "La réponse automatique ne peut pas être envoyée lorsque le disque est plein. "
  ➥ $disque \ plein \longrightarrow \neg envoi$

Exercice

Vérifier si les 3 expressions suivantes sont consistantes (ensemble) :

1. *Le message de diagnostic est stocké dans un tampon ou il est retransmis.* ($tempon \vee retransmis$)
2. *Le message de diagnostic n'est pas stocké dans un tampon.* ($\neg tempon$)
3. *Si le message de diagnostic est stocké dans un tampon, alors il est retransmis.* ($tempon \rightarrow retransmis$)

Passer

Que dire si l'on ajoute :
Le message de diagnostic n'est pas transmis. ? ($\neg retransmis$)

Puzzles logiques

• Puzzles logiques : une bonne façon de manipuler les connecteurs et le raisonnement logiques.

Exemple

- Dans une île, il y a 2 sortes (catégories) de gens : ceux qui mentent toujours (*menteurs*) et ceux qui disent toujours la vérité (*honnêtes*).
- On y rencontre 2 personnes A et B.
  - ➤ A dit : `B est honnête` ;
  - ➤ B dit : `Nous deux sommes de catégories opposées`.
- De quels camp sont ils ?

Autres utilisations des opérateurs logiques

- On utilise les connecteurs logique dans les recherches sur le WEB.
  - ➥ Recherche par ET, OU, NON, ...
- On utilise les connecteurs logique dans les opérations sur les chaînes de bits.
  - ➥ Exemple : avec les deux chaînes suivantes

    01 1011 0110
    11 0001 1101

---

11 1011 1111	OU (bitwise OR)
01 0001 0100	ET (bitwise AND)
10 1010 1011	OuX (bitwise XOR)

N.B. : Il y a aussi *NAND* (=no AND) et *NOR* (= no OR)

Exercices de construction de tables de vérités

1. Construire la table de vérité de :
   1. $p \rightarrow (\neg q \vee r)$
   2. $\neg p \rightarrow (q \rightarrow r)$
   3. $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$
   4. Vérifier : $p \rightarrow (q \wedge r) \equiv (p \rightarrow q) \wedge (p \rightarrow r)$.
   5. Montrer que : $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$

   Indication : pour le dernier, créer la table de verité de $X = [(p \rightarrow q) \wedge (q \rightarrow r)]$, et celle de $Y = (p \rightarrow r)$. Ensuite, la démonstration est faite en montrant que $X \rightarrow Y$ ne contient que Vrai. On peut aussi directement constater que $X \rightarrow Y$ correspond bien à la table de l'implication.

2. Est-ce que l'affirmation Cette affirmations est fausse. est une proposition ?

Détente

• Un anthropologue étudie les habitants d'une Île où vivent deux tribus : l'une dont les membres mentent toujours, et l'autre dont les membres disent toujours la vérité.

• Un jour, l'anthropologue, qui veut se rendre au village, arrive à l'embranchement d'une route qui se subdivise en deux.

• Ne sachant quelle direction prendre, il attend. Vient à passer un habitant de l'île. Comme il ne sait pas à quelle tribu appartient ce passant, quelle question doit-il lui poser pour savoir quelle route conduit au village ?

Equivalence Propositionnelle

• Si l'on peut remplacer une expression logique par une autre, on dira que les deux sont équivalentes.
• Par exemple, $p \longrightarrow q$ et $\neg p \vee q$ sont équivalentes.

Définition (Tautologie)

• *Une proposition composée est une tautologie si elle est* **vraie** *quelque soit la valeur de vérité des propositions qui la composent.*
• *Une proposition composée est une contradiction si elle est* **fausse** *quelque soit la valeur de vérité des propositions qui la composent.*
• *Une proposition composée qui est ni une tautologie ni une contradiction est une contingence.*
• *Les propositions p et q sont dites équivalentes si* $p \leftrightarrow q$ *est une tautologie.*
On note l'équivalence de p et de q par $p \equiv q$.

Définitions (suite)

Exemples

- $p \vee \neg p$ est une tautologie.
- $p \wedge \neg p$ est une contradiction.

• Si l'on peut remplacer une expression par une autre, on dira que les deux sont équivalentes.

Remarque

Le symbole $\equiv$ n'est pas un connecteur logique et $p \equiv q$ n'est pas une proposition composée mais plutôt pour dire que $p \leftrightarrow q$ est une tautologie.

• Une façon de vérifier une équivalence est d'utiliser la table de vérité.

Exercices

Exercice

A l'aide des tables de vérité,

- *Montrer que* $p \vee \neg p$ *et une tautologie et que* $p \wedge \neg p$ *est une contradiction.*
- *La loi de Morgan : Montrer que* $\neg(p \vee q)$ *et* $\neg p \wedge \neg q$ *sont équivalentes.*
- *Montrer l'équivalence de* $p \longrightarrow q$ *et* $\neg p \vee q$.
- *Distribution de OU sur ET : Montrer l'équivalence de* $p \vee (q \wedge r)$ *et* $(p \vee q) \wedge (p \vee r)$.

- L'associativité de la disjonction montre que $p \vee q \vee r$ est bien formée (l'ordre n'a pas d'importance).
- Idem pour $p \wedge q \wedge r$
- La loi de De Morgan peut être étendue à n temes :
  - $\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n$
  - $\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n$

Quelques équivalences (1/2)

Equivalence	*Nom (Loi)*
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identité
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotence
$\neg\neg p \equiv p$	Double Nég.
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Négation

Tab.: la table des équivalences

Quelques équivalences (2/2)

Equivalence	*Nom (Loi)*
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorbtion

Quelques équivalences avec Implication

1. $p \rightarrow q \equiv \neg p \vee q$
2. $p \rightarrow q \equiv \neg q \rightarrow \neg p$
3. $p \vee q \equiv \neg p \rightarrow q$
4. $p \wedge q \equiv \neg(p \rightarrow \neg q)$
5. $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$ (Dist. de $\rightarrow$ sur $\wedge$)
6. $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$ (Dist. de $\rightarrow$ sur $\vee$)
7. $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$ (Factorisation) *développer*
8. $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$ (Factorisation) $'\rightarrow'$

9. $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
10. $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
11. $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ *évident, cf. table de vérité*
12. $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$ *développer puis utiliser (11)*

Exercice de démonstration

1. Montrer que $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$
   Indication : entrer la négation puis distribuer ET sur OU.
2. Montrer que $(p \wedge q) \rightarrow (p \vee q)$ est une tautologie.
   Indication : utiliser l'équivalent disjonctif de l'implication.

Remarque (Pourquoi utiliser les lois et les équivalences ?)

Une proposition (par exemple une tautologie à démontrer) peut contenir 20 variables.

- ➤ *Dans ce cas, la table de vérité aura* $2^{20} = 1,048,576$ *lignes !*
- ➤ *On pourrait utiliser un ordinateur pour établir cette table ;*
- ➤ *Mais que faire si l'on a 1000 variables ?*
  - ➥ 2^{1000} *est un nombre avec plus de 300 chiffres.*
  - ➥ *Mêmes un ordinateur ne pourra plus décider si l'on a une tautologie (des millards d'années de calculs ! !).*

Exercices

1. Utiliser les lois pour montrer que les propositions suivantes sont des tautologies (N.B. : faire apparaître les T) :
   - $(p \wedge q) \rightarrow p$
   - $p \rightarrow (p \vee q)$
   - $\neg p \rightarrow (p \rightarrow q)$
   - $(p \wedge q) \rightarrow (p \rightarrow q)$
   - $\neg(p \rightarrow q) \rightarrow p$
   - $\neg(p \rightarrow q) \rightarrow \neg q$

2. Démontrer les mêmes tautologies **en utilisant** les tables de vérité (T par tout !).

Rappel : l'expression telle que $P \wedge \neg P$ qui apparaît dans vos démonstrations est une contradiction et vaut Faux.
Par contre, $P \vee \neg P$ est toujours vraie.

Exercice (énigme)

- Soit les expressions suivantes :
  - La servante dit qu'elle a vu le sommelier dans le salon.
  - Le salon est à côté de la cuisine.
  - Le coup de feu a été tiré dans la cuisine et pouvait être entendu dans toutes les pièces.
  - Le semmelier, qui a une bonne ouïe, dit qu'il n'a pas entendu le coup de feu.

➙ Montrer que si la servante a dit vrai, le sommelier a menti.

Indications : poser des propositions pour chaque affirmation (par exemple, $P =$ *"la servante a dit vrai"* ou $Q =$ *"le sommelier était dans le salon"*) puis établir les expressions logiques (par exemple, $P \rightarrow Q$).

On obtient ainsi un ensemble de propositions dont il faut vérifier la validité (montrer que c'est une tautologie).

Exercice

Réaliser un additionneur **1 bit + 1 bit** (avec retenue possible) à l'aide des expressions logiques.

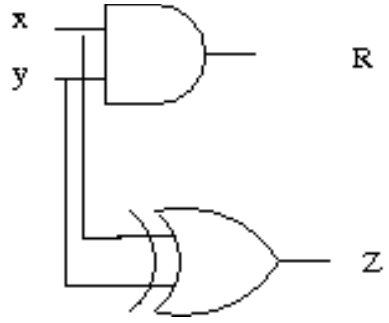
Rappel : considérer les tables de vérité de NON, ET, OU et OuX .

L'addition de 2 bits contenant chacun 0 ou 1 :

➔ On note le résultat de X+Y=Z/R (R = retenue).

➔ 0+0=0/0, 0+1=1/0, 1+0=1/0, 1+1=0/1

Solution :



Exercice (suite)

On peut utiliser ce circuit pour réaliser un additionneur 2 bits, puis . . .8 bits.

Nota Bene : dans la conception des circuits électroniques, on utilise (largement) les portes **NAND**=la négation de ET et **NOR**=la négation de OU.
Le symbole $|$ désigne NAND.

➔ On a $1 \mid 1 = 0$, $1 \mid 0 = 0 \mid 1 = 0 \mid 0 = 1$

La porte NOR est noté par $\downarrow$.

➔ On a : $1 \downarrow 1 = 1 \downarrow 0 = 0 \downarrow 1 = 0$ et $0 \downarrow 0 = 1$.

La plupart des autres portes peuvent s'exprimer à l'aide de NAND et NOR. Par exemple :

$\neg X = X \mid X$

$X \wedge Y = (X \mid Y) \mid (X \mid Y)$

Solution

Pour faciliter la suite, on présente l'additionneur 2 bits par un schéma abstrait (une boîte), puis on l'utilise pour réaliser un additionneur 3 bits.

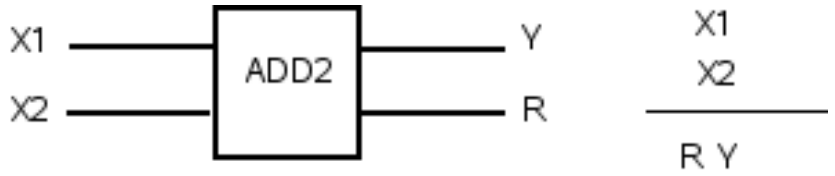
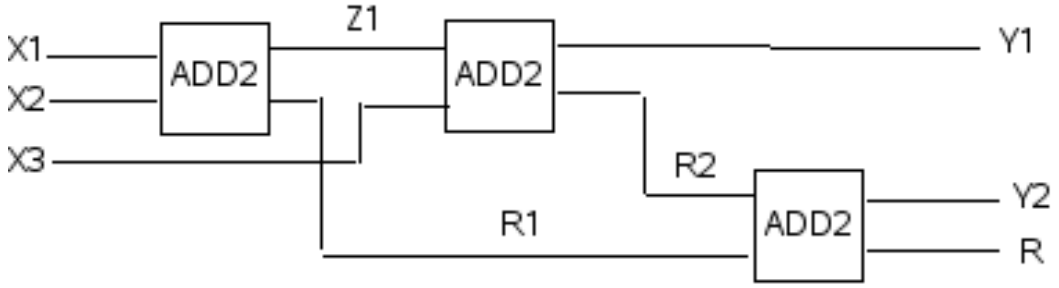


Schéma abstrait d'additionneur 2 bits

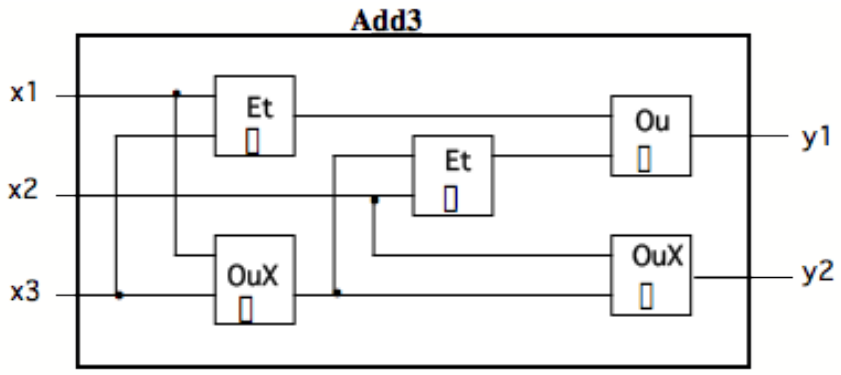
Additionneur 3 bits à l'aide de 3 ADD2 (la sortie toujours R=0)



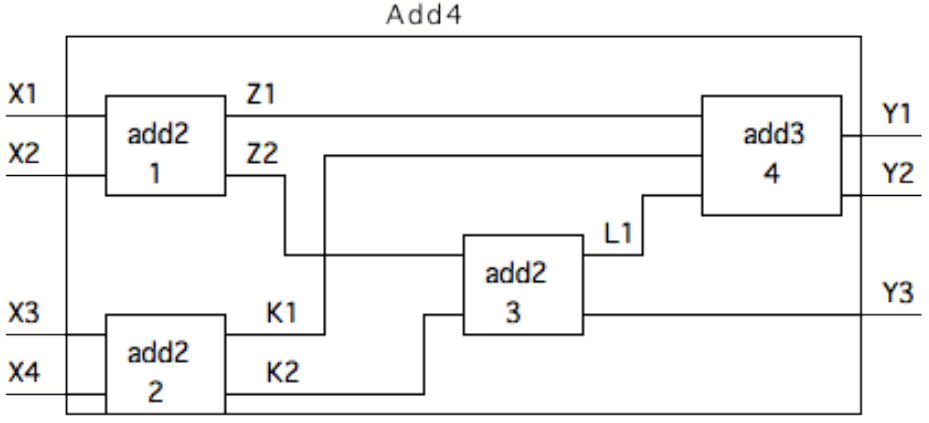
Additionneur 3 bits : X1+X2+X3 = Y2 Y1 (R)

Solution (suite)

A titre d'indication, un additionneur 3 bits peut également être réalisé directement à l'aide des portes de base (ET, OU, NON, OUX, ...).



Un additionneur 4 bits réalisé à l'aide de ADD2 et ADD3 :



Additionneurs (suite)

Application :

Pour réaliser par exemple, l'addition de deux octets (8 bits chacun) :

Notons le premier octet $X = x_8\ x_7\ x_6\ x_5\ x_4\ x_3\ x_2\ x_1$

Et le second par $Y = y_8\ y_7\ y_6\ y_5\ y_4\ y_3\ y_2\ y_1$

Pour additionner $x_1 + y_1 = z_1/R_1$, on peut utiliser un additionneur 2 bits.

➔ La retenue R_1 est ensuite utilisée pour additionner x_2 et y_2.

➔ $x_2 + y_2 + R_1 = z_2/R_2$,

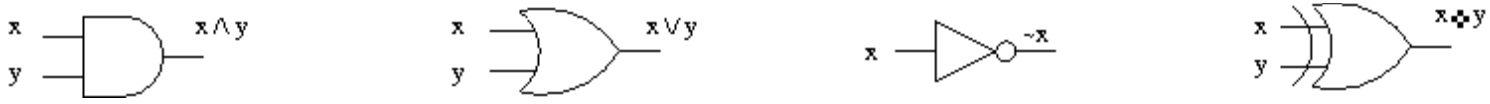
➔ Ayant 3 bits à additionner, on utilise un additionneur 3 bits,

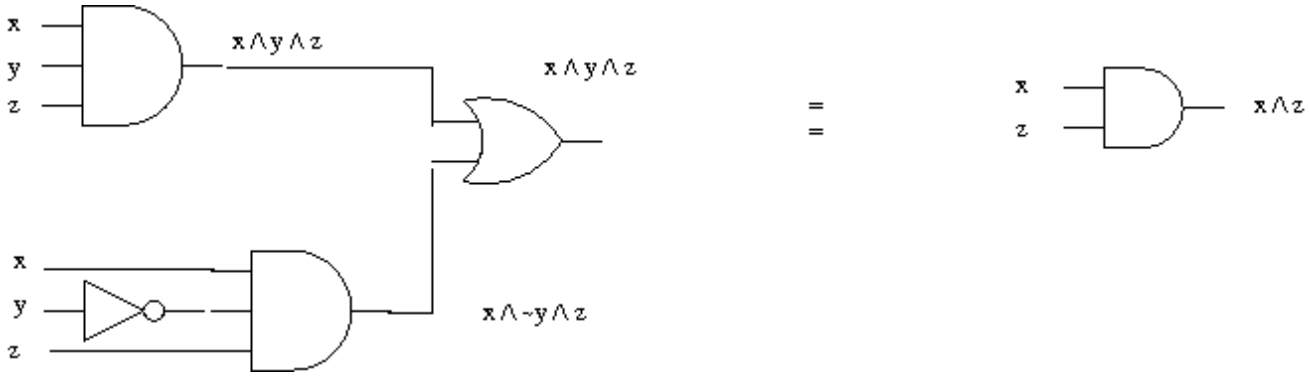
...

ET finalement, l'addition de $x_8 + y_8 + R_7 = z_8/R_8$

Exercice (circuits)

Montrer par simplification que les deux circuits suivants sont équivalents (le premier schéma rappelle les portes de base) :
➔ Montrer que $(x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z)$ (figure dessus) est équivalente à $(x \wedge z)$





Logique des Prédicats : Introduction

- Les expressions suivantes comportent des variables :
  - ➤ $x > 3$ $\quad x = y + 3$ $\quad x + y = z$
  - ➤ Elles ne peuvent pas être évaluées (être =T/F) si les variables sont sans valeur.
- L'expression $x > 3$ a deux parties : **x** la variable et $' > \mathbf{3}'$ le prédicat.
  - ➤ Ce prédicat précise ici une propriété de x (ou une contrainte).
  - ➤ On pourra noter $x > 3$ par $P(x)$ où P désigne le prédicat $' > 3'$ et x la variable.
  - ➤ On dira aussi que $P(x)$ représente la valeur de la *fonction propositionnelle P sur x*.
  - ➤ Une fois que x aura une valeur, $P(x)$ devient une proposition avec une valeur de vérité. Par exemple :
    - ➥ pour $x = 2$, $P(x)$ sera fausse ;
    - ➥ pour $x = 4$, elle sera vraie.

Introduction (suite)

- On peut avoir plus d'une variable dans une expression :
  - ➤ On peut représenter $x = y + 3$ par $Q(x, y)$.
  - ➤ La valeur de vérité de $Q(x, y) =$

$$\begin{cases} \text{fausse si } \mathrm{x}{=}1,\ \mathrm{y}{=}2 \\ \text{vraie si } \quad \mathrm{x}{=}3,\ \mathrm{y}{=}0 \end{cases}$$

- D'une manière générale, un prédicat est noté par $P(x_1, x_2, \ldots, x_n)$
  - ➤ $P(x_1, x_2, \ldots, x_n)$ représente la valeur de la *fonction propositionnelle* P sur le *n-uplet (tuple)* $(x_1, x_2, \ldots, x_n)$

  - ➤ Terminologie : le nom générique de P est **prédicat**
  - ➤ On précise aussi $P(\ldots)$ par :
    - ➥ si $n = 0$, P est une **proposition**,
    - ➥ si $n = 1$, $P(x_1)$ est aussi une **propriété** de x_1,
    - ➥ pour $n > 1$, $P(x_1, x_2, \ldots, x_n)$ est une **relation**.
  - ➤ Le symbole P seul est aussi appelé *symbole de prédicat*.
  - ➤ La notation P/n est un raccourci pour $P(x_1, x_2, \ldots, x_n)$.

Suite

• Les prédicats apparaissent dans les programmes informatiques.

➤ Par exemple, pour **if x $>$ 0 then x := x+1**

➥ la valeur de x permet d'évaluer P(x) qui est $x > 0$ et d'effectuer (ou pas) l'opération d'incrémentation de x.

• On utilise également les prédicats à la sortie des boucles, fonctions, etc. pour représenter un état de calcul.

• La preuve de justesse d'un calcul peut aussi être exprimée à l'aide des prédicats (par exemple, la fonction *factorielle* ou le calcul de la *longueur d'une chaine*, etc., à l'aide de l'induction).

• D'autres exemples d'utilisation sont : TDA (axiomes et propriétés), calcul de la complexité, etc.

Spécification TDA Ensemble (Set) I

TDA set (de *data*)

Utilise : *nat, bool, data*

Opérations :

egal : set x set $\longrightarrow$ bool

ajout : set x data $\longrightarrow$ set

supprime : set x data $\longrightarrow$ set

membre : set x data $\longrightarrow$ bool

vide : set $\longrightarrow$ bool

card : set $\longrightarrow$ nat

...

Equations (axiomes) : d $\in$ data, s, s1 $\in$ set

egal(vide, vide) = True

egal(vide, $\neg$ vide) = False

egal(ajout(d,s), ajout(d,s1)) = egal(s,s1)

supprime(d,vide) = vide

supprime(d,ajout(d,s)) = s

membre(d,vide) = false

Spécification TDA Ensemble (Set) II

membre(d, ajout(d,s)) = true
vide(ajout(d,s))=false
card(vide)=0
card(ajout(d,s))= card(s) si membre(d,s) ; 1+card(s) sinon.
....

• Habituellement, pour constituer la section Axiomes, on croise les opérations 2 (celles qui ne renvoient pas *set*) avec les **internes** (celles qui renvoient 1).
On appelle cela la complétude suffisante (ou minimale). La complétude maximale est de croiser toutes les opérations, deux à deux.
• On peut imposer (et ajouter dans la définition) des préconditions aux opérations. Par exemple, exiger que l'indice d'un tableau soit dans un intervalle défini (les bornes du tableau).

• Exercice : définir le TDA bool.

Utilisation dans les algorithmes I

• Soit un algorithme de recherche d'un élément x dans un tableau T(1..N).

• La spécification du cahier des charges :
La Procédure doit renvoyer -1 si $x \notin T[1..N]$, son indice sinon.
Plus exactement : si la réponse est -1 : $\nexists i \in 1..n | T[i] = x$
sinon $\exists i \in 1..n | T[i] = x$

Procédure **recherche**(x : élément, T : tableau[1..N] d'éléments,
indice ind) : indice

```
si (T=vide) OU (ind > N)
alors renvoie -1
sinon si (T[ind] = x)
        alors renvoie ind
        sinon
        renvoie recherche(x,T,ind+1)
```

• La version commentée :

Utilisation dans les algorithmes II

Procédure **recherche**(x : élément, T : tableau[1..N] d'éléments,
indice ind) : indice

- renvoie -1 si ...
  si (T=vide) OU (ind $>$ N)
  alors renvoie -1
  - $(T \neq vide) \wedge (ind <= N)$

  sinon si (T[ind] $=$ x)
  alors renvoie ind
  sinon
  - $T \neq vide \wedge ind <= N \wedge T[ind] \neq x$

  renvoie recherche(x,T,ind+1)

• Un autre exemple (le même algorithme en itératif)

Procédure **recherche**(x : élément, T : tableau[1..N] d'éléments,
indice ind) : indice

i : indice $= 1$
tantque $(i <= N \wedge T[i] \neq x)$
i $=$ i+1

Utilisation dans les algorithmes III

➤ Quel est l'état du calcul, que faut-il renvoyer ?

➥ Construire la table (de ET) avec les mêmes conditions que pour le TantQue.

➥ Décider... *Si* $i \leq N$ *renvoyer i ; renvoyer -1 ;*

N.B. : la table de OU (la négation des conditions) donne les mêmes résultats.

Les Quantifieurs

• Lorsque toutes les variables d'une expression sont instanciées, l'expression devient une proposition avec une certaine valeur de vérité.

➥ De fait, un prédicat génère (potentiellement) une **infinité** de propositions, sans les énumérer.

• On peut créer, par quantification, des propositions à partir d'une fonction propositionnelle P/n.

• Deux quantifieurs : Universel et Existentiel :

⇨ calcul des prédicats.

Quantifieur Universel

Définition

La quantification universelle de $P(x)$ est la proposition

$P(x)$ est vrai pour toutes x (de l'univers du discours $\approx$ Dom_x).

Notation : $\forall x, P(x)$

Exemple (1)

Si $P(x) = \mathrm{x}+1 > \mathrm{x}$ et que l'univers du discours = les nombres réels

➤ $\forall x, P(x)$ est vraie.

- Similaire à la notation mathématique $\forall x \in \mathbb{R}, P(x)$

Exemple (2)

Si $Q(x) = \mathrm{x} > 2$ et que l'univers du discours = les nombres réels

➤ $\forall x, Q(x)$ n'est pas vraie (par exemple, $x = 1$)

- Lorsque $\forall x, R(x)$ est vraie pour $x_1, x_2, \ldots, x_n$, elle résume

$$\bigwedge_{R(x_i)} = R(x_1) \wedge R(x_2) \wedge \cdots \wedge R(x_n)$$

Quelques exemples

Exemple (avec l'implication (la règle))

- *toute personne a deux parents*
  - ➥ $\forall x, \mathit{personne}(x) \rightarrow \mathit{a\_2\_parents}(x)$.

  A ne pas confondre avec $\forall x, \mathit{personne}(x) \wedge \mathit{a\_2\_parents}(x)$

- Que dire de $\forall x, x^2 \geq x$ pour $x \in \mathbb{R}$?
  - ➥ il faut $x \leq 0$ ou $x \geq 1$
  - ➥ $\forall x, \mathit{reel}(x) \wedge (x \leq 0 \vee x \geq 1) \rightarrow x^2 \geq x$.

- Même chose mais avec l'univers du discours = les entiers ?
  - ➥ toujours vrai car pas d'entier x tel que $0 < x < 1$
  - ➥ $\forall x, \mathit{entier}(x) \rightarrow x^2 \geq x$.

.../ ...

Exemples (suite)

Attention :
Le prédicat $\forall x, P(x)$ sera faux s'il existe une seule valeur (au moins) pour x dans l'univers du dicsours pour laquelle $P(x) = \mathit{faux}$.

➥ Une telle valeur est appelée un contre-exemple pour $\forall x, P(x)$.

Exemple (univers des nombres réels)

Si P(x) est $\forall x, x^2 > 0$, on peut trouver le contre-exemple $x = 0$.

La recherche de contre exemples est une activité importante dans la spécification et le développement de tout système automatisé.

Quantifieur existentiel

- Affirmer s'il existe une valeur avec telles propriétés.

Définition

La quantification existentielle de $P(x)$ est la proposition :
il existe un élément x dans l'univers du discours tel que $P(x) = vrai$
➙ *Notation :* $\exists x, P(x)$

Exemples

1. Si $P(x) : x > 3$ pour les entiers, x=4 permet d'affirmer $\exists x, P(x)$
2. Si $Q(x) : x = x + 1$ pour les entiers, aucune valeur pour x permet d'affirmer $\exists x, Q(x)$

Quantifieurs (suite)

• Lorsque $\exists x, R(x)$ est vraie pour au moins l'une des valeurs $x_1, x_2, \ldots, x_n$, elle résume

$$\bigvee_{R(x_i)} = R(x_1) \vee R(x_2) \vee \cdots \vee R(x_n)$$

Remarque

Lorsque $\exists x, P(x) = \textit{faux}$, *on en déduit* $(\forall x, \neg P(x)) = \textit{vrai}$.
Lorsque $\forall x, P(x) = \textit{faux}$, *on en déduit* $(\exists x, \neg P(x)) = \textit{vrai}$.

Etat des variables

En logique, une variable est soit **libre**, soit **instanciée** :

Définition (libre, liée, instanciée)

- *Variable* **liées** *: une variable quatifiée (avec $\forall$ ou $\exists$) ou lorsqu'elle a reçu une valeur ;*

  ➥ *En cas de présence d'une valeur précise, on précisera que la variable est* **instanciée**.

- *Variable* **libre** *: une variable non quatifiée ou sans aucune valeur ;*

  ➥ *Dans la pratique (cf. codage), une valeur particulière (comme NULL, NIL, FREE, etc.) peut initialiser une variable libre (pour pouvoir estimer son état libre ou non) ;*

Variables (suite)

Définition (portée (champ) d'une variable)

- *Pour qu'une fonction propositionnelle devienne une proposition, les variables qui y apparaissent doivent être instanciées.*

- *Dans une expression logique, la* **portée** *(scope=champ) d'une variable est la partie de l'expression à laquelle le quantifieur s'applique ;*

  ➥ *Une variable sera libre lorsqu'elle est hors tout quantifieur.*

Variables (suite)

Exemples

- Dans $\exists \mathbf{x}, \mathbf{Q}(\mathbf{x}, \mathbf{y}), \mathbf{x}$ est liée (quantifiée) et $\mathbf{y}$ est libre.
- Dans $\exists \mathbf{x}, (\mathbf{P}(\mathbf{x}) \wedge \mathbf{Q}(\mathbf{x})) \vee \forall \mathbf{x}, \mathbf{R}(\mathbf{x})$, toutes les variables (les deux x) sont liées.

  ➙ Les deux x sont différentes et on peut remplacer le second x en y sans changer de signification.

Négation

- Soit l'expression
  "tous les élèves de cette classe suivent le cours communication"
  Dans l'univers des élèves de cette classe, on a $\forall x, P(x)$.

- La négation de cette expression : *il n'est pas vrai que .....*
  ➥ $\neg(\forall x, P(x)) \quad \equiv \quad \exists x, \neg P(x)$

- De même :
  ➥ $\neg(\exists x, P(x)) \quad \equiv \quad \forall x, \neg P(x)$

  ➥ Par exemple, *P(x) : mesurer plus de 2m87*!

négation (suite)

Remarque (la négation des quantifieurs)

- *Soit l'univers du discours contenant n éléments.*
  Appliquons la négation aux quantifieurs :
  - $\forall x, P(x) \;=\; P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$
    $\rightarrow \neg\forall x, P(x) \quad = \quad \neg(P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n))$

    La loi De Morgan s'applique :
    $\rightarrow \neg P(x_1) \vee \neg P(x_2) \vee \cdots \vee \neg P(x_n) \quad \equiv \quad \exists x, \neg P(x)$
  - *De même :* $\exists x, Q(x) \;=\; Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n)$
    $\rightarrow \neg\exists x, Q(x) \quad = \quad \neg(Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n))$
    $\rightarrow \neg Q(x_1) \wedge \neg Q(x_2) \wedge \cdots \wedge \neg Q(x_n) \quad \equiv \quad \forall x, \neg Q(x)$

$$\boxed{\neg\forall x, P(x) \equiv \exists x, \neg P(x)}$$

$$\boxed{\neg\exists x, P(x) \equiv \forall x, \neg P(x)}$$

Exercices

Exercice

Quelle est la **négation** *des expressions suivantes :*

1. *il y a des politiciens honnêtes.*
2. *tous (les bèlges) aiment les frites.*
3. $\forall x, (x^2 > x)$ *(pour x : entier)*
4. $\exists x, (x^2 = 2)$ *(pour x : réel)*

Quantifieurs et implication

Dans les expressions suivantes, les deux premières sont les **prémices** (prémisses) et la 3e la **conclusion** :

1. *tous les lions sont féroces*
2. *certains lions ne boivent pas de café*
3. ➙ *certaines (créatures) féroces ne boivent pas de café*

Exprimées en logique :

1. $\forall x, (lion(x) \longrightarrow feroce(x))$
2. $\exists x, (lion(x) \wedge \neg boit\_cafe(x))$
3. ➙ $\exists x, (feroce(x) \wedge \neg boit\_cafe(x))$

NB : la 2e et la 3e ne peuvent pas être écrites sous forme d'implication (pourquoi ?)

Vers Prolog

ProLog : langage utilisant (une forme simplifiée) des prédicats.

Exemple (faits et règles Prolog)

```
enseignant(jean, info1A).     % enseignant(nom, matière).
enseignant(pierre, maths2A). ...
assiste(helene, info1A).        % assist(élève, matière).
assiste(paul, maths2A). ...
```

On peut ajouter le prédicat *enseigne(P,E)* si prof P enseigne une matière M suivie par l'élève E :

```
enseigne(P,E) ← enseignant(P, M) , assiste(E, M).
```

- L'implication en Prolog.

  ➙ Poser des questions au système... *qui enseigne à qui ?*

Exercices : Traduire en logique

1. *personne n'est parfait.*
2. *non tout le monde est parfait.*
3. *tous vos amis sont parfaits*
4. *un de vos amis est parfait*
5. *tout le monde est votre ami et parfait.* à comparer avec (3)

• Montrer que $P \rightarrow Q$ et $P \wedge \neg Q \rightarrow \ Faux$ sont équivalents.

➙ On a pour toute expression P : $P \equiv P \vee Faux$.

On pose :

➙ $P \rightarrow Q \equiv (P \rightarrow Q) \vee F \equiv (\neg P \vee Q) \vee F \equiv \neg(P \wedge \neg Q) \vee F$

➙ Considérons $A = \neg(P \wedge \neg Q)$, on a $\neg A \vee F \equiv A \rightarrow F$

➙ Donc, on obtient $\equiv P \wedge \neg Q \rightarrow F$ **CQFD**.

➥ Correspond au seul cas Faux de la table de vérité de $\rightarrow$

➔ Notation : $P \rightarrow Q \quad \vdash \quad P \wedge \neg Q \rightarrow \ Faux$

Quantifieurs imbriqués

• Quantifieur dans la portée d'autres quantifieurs.

Exemples

$\forall x \exists y\ (x + y = 0)$
$\forall x \forall y \forall z\ (x + (y + z) = (x + y) + z)$
$\forall x \forall y\ ((x > 0) \wedge (y < 0) \rightarrow (xy < 0))$

• **Exercices** : exprimer en logique les expressions (étudiants d'une école)

1- tout étudiant a un ordinateur ou a un ami qui a un ordinateur.
➙ $\forall x(possede\_ordi(x) \vee \exists y(possede\_ordi(y) \wedge ami(x, y)))$

2- il y a un étudiant dont 2 (des) amis ne sont pas amis entre eux.
➙ $\exists x \forall y \forall z((ami(x, y) \wedge ami(x, z) \wedge (y \neq z)) \rightarrow \neg ami(y, z))$

Exercice

• Exprimer en logique :

1- **si une personne est une femme et est un parent alors elle est la mère de quelqu'un.**

2- **toute personne a exactement un meilleur ami.**

NB : la notation $\exists!$ veut dire *il existe exactement un* (quantifieur existentiel unique) ;

➙ On peut écrire alors : $\forall x \; \exists! y \; (meilleur\_amis(x, y))$

Négation des quantifieurs imbriqués

- **But** : arriver à une forme normale.

➤ On utilise l'affirmation

pour tout réel x différent de zéro, il existe un réel y inverse de x.

Exemple

Exprimer la **négation** de l'expression $\forall x \exists y(xy = 1)$ **sans** faire figurer la négation avant les quantifieurs :

➤ On a d'abord $\neg \forall x \exists y(xy = 1)$

On applique (étape par étape) les règles de la négation des quantifieurs vues plus haut (les '()' pour clarifier) :

➤ $\neg(\forall x \exists y(xy = 1)) \equiv \exists x(\neg \exists y(xy = 1)) = \exists x \forall y(\neg(xy = 1))$.

➤ En notant $\neg(xy = 1) \equiv xy \neq 1$, on obtient :

➤ $\exists x \forall y(xy \neq 1)$.

Suite exercices

• Exprimer : *il n'existe pas de* **F***emme qui ait voyagé sur un* **V***ol (affrété par) toutes les* **C***ompagnies aériennes du monde !*

Indication : utiliser le fait que cette phrase est la négation de :
Il y a une Femme qui a voyagé sur un Vol de toutes les Compagies aériennes du monde.

- $\neg\ \exists F \forall C \exists V (a\_pris(F, V) \wedge affrete(V, C))$
- $\forall F \neg \forall C \exists V (a\_pris(F, V) \wedge affrete(V, C))$
- $\forall F \exists C \neg \exists V (a\_pris(F, V) \wedge affrete(V, C))$
- $\forall F \exists C \forall V \neg (a\_pris(F, V) \wedge affrete(V, C))$
- $\forall F \exists C \forall V (\neg a\_pris(F, V) \vee \neg affrete(V, C))$

Ordre des quantifieurs

• L'ordre des quantifieurs est **important** sauf s'ils sont tous universels ou tous existentiels.

Exemple (importance de l'ordre)

Comparer la valeur de vérité de

(1) $\exists y \forall x\ somme(x, y, 0)$ et (2) $\forall x \exists y\ somme(x, y, 0)$

1. $\exists y \forall x\ somme(x, y, 0)$ veut dire

   il existe un réel y tel que pour tout réel $x, x + y = 0$

   ➙ Or, peu importe la valeur de y, on sait qu'il existe un seul réel x tel que $x + y = 0$

   ➙ Donc, il n'est pas vrai qu'en choisissant un réel y, tous les réels x sont tels que $x + y = 0$!

   ➥ L'expression $\exists y \forall x\ somme(x, y, 0)$ est donc fausse.

2. Par contre, la seconde affirmation est vraie.

   pour tout réel x, il existe un réel y tel que $x + y = 0$

Ordre des quantifieurs (suite)

Exemple (ordre avec 3 quantifications)

Comparer la valeur de vérité de

(1) $\forall x \forall y \exists z$ *somme*(x, y, z) et (2) $\exists z \forall x \forall y$ *somme*(x, y, z)

1. $\forall x \forall y \exists z$ *somme*(x, y, z) veut dire
   pour 2 réels x et y, il existe un réel z tel que $x + y = z$
   ➙ Cette affirmation est vraie.

2. Par contre, la seconde affirmation est fausse.
   ➙ Il n'y a pas un réel z tel que la somme de n'importe quel couple de réels x, y soit z !

Exercices

Exprimer les expressions suivantes à l'aide des opérateurs logiques. L'univers du discours est le nombres entiers.

- La somme de deux entiers négatifs est un négatif.
- La différence de deux entiers positifs n'est pas forcément positif.
- La somme des carrés de deux entiers est plus petite ou égale au carré de leur somme.
- La valeur absolue du produit de 2 entiers est le produit de leur valeur absolue.
- Tout entier positif est la somme des carrés de 4 entiers.

Exercices (suite)

Exprimer $\exists!\ P(x)$ en utilisant les quantifieurs et des connecteurs logiques.

Récapitulatif

- La tableau récapitulatif d'ordre pour deux variables :

Expression	**cas vrai (V)**	**cas faux (F)**
$\forall x \forall y, P(x,y)$ $\forall y \forall x, P(x,y)$	pour tout couple x,y P(x,y)=V	il y a une paire x,y pour lequel P(x,y)=F
$\forall x \exists y, P(x,y)$	pour tout x, il y a un y tq P(x,y)=V	il y a un x tq P(x,y) =F pour tout y
$\exists x \forall y, P(x,y)$	il y a un x pour lequel P(x,y)=V pour tout y	pour tout x, il y a un y tq P(x,y)=F
$\exists x \exists y, P(x,y)$ $\exists y \exists x, P(x,y)$	il y a un couple x,y pour lequel P(x,y)=V	pour tout couple x,y P(x,y)=F

Remarque (importante)

- Si $\exists y \forall x, P(x,y) = T$ alors $\forall x \exists y, P(x,y)$ doit être vraie.
- Par contre, si $\forall x \exists y, P(x,y) = T$, il n'est pas toujours le cas d'avoir $\exists y \forall x, P(x,y) = T$. (vu ci-dessus).

Forme Normale Prenex

• La forme **Prenex** : $Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \quad P(x_1, \ldots, x_n)$ où
  ➔ Q_i est une quantifieur
  ➔ P/n une expression (sans quantifieur, négation possible)
  ➙ Exemple : $\forall x \exists y (P(x, y) \wedge \neg Q(y))$ est sous forme Prenex.
  ➙ Par contre : $\forall x (P(x, y) \vee \exists y Q(y))$ ne l'est pas (à cause de la quantification de y).
  ➙ Dans une forme Prenex, tous les quantifieurs sont à gauche.

➔ **On peut démontrer** : toute expression formée de variables propositionnelles, prédicats, les constates V et F, des connecteurs logiques et des quantifieurs est équivalente à une forme Prenex.
➔ **Plus exactement** : si la forme Prenex d'une expression est satisfiable, sa forme originale l'est aussi.

✓ En rentrant la négation dans les expressions (exercices), nous avons commencé la à mettre des expressions sous forme Prenex.

Prenex (suite)

- Dans les exmples ci-dessous :
  ➔ deux quantifieurs ne quantifient pas la même variable ;
  ➔ une même variable n'est pas à la fois liée et libre.

$\neg\forall x P$	devient	$\exists x \neg P$	P contient x
$\neg\exists x P$	devient	$\forall x \neg P$	
$(\forall x, P) \wedge Q$	devient	$\forall x (P \wedge Q)$	
$(\exists x, P) \wedge Q$	devient	$\exists x (P \wedge Q)$	
$(\forall x, P) \vee Q$	devient	$\forall x (P \vee Q)$	
$(\exists x, P) \vee Q$	devient	$\exists x (P \vee Q)$	

➔ Pour éviter les erreurs, transformer d'abord " $\leftrightarrow$ " et " $\rightarrow$ " pour n'utiliser que $\wedge, \vee$ et $\neg$.

➔ On utilisera cette forme dans la normalisation des expressions logiques (voir plus loin)

Exemple (forme Prenex)

• Soit l'expression (inductive) :

S'il y a un train en retard, alors tous les trains sont en retard.

➔ Soit T(x) : x est un train

➔ R(x) : x est en retard , l'univers de discours = les objets.

➔ On note : $\exists x, (T(x) \wedge R(x)) \rightarrow \forall x, (T(x) \rightarrow R(x))$

• On met sous la forme *Prenex* :

$\neg(\exists x(T(x) \wedge R(x))) \vee \forall x(\neg T(x) \vee R(x))$ " $\rightarrow$ " en " $\vee$ "

On renomme les variables x qui n'ont rien de commun :

$\neg(\exists x\ (T(x) \wedge R(x))) \vee \forall y\ (\neg T(y) \vee R(y))$

$(\forall x\ (\neg T(x) \vee \neg R(x))) \vee \forall y(\neg T(y) \vee R(y))$ on rentre $\neg$

• Le résultat final = la forme Prenex de l'expression :

$$\forall x\ \forall y\ (\neg T(x) \vee \neg R(x)) \vee (T(y) \rightarrow R(y)))$$

Exercice I

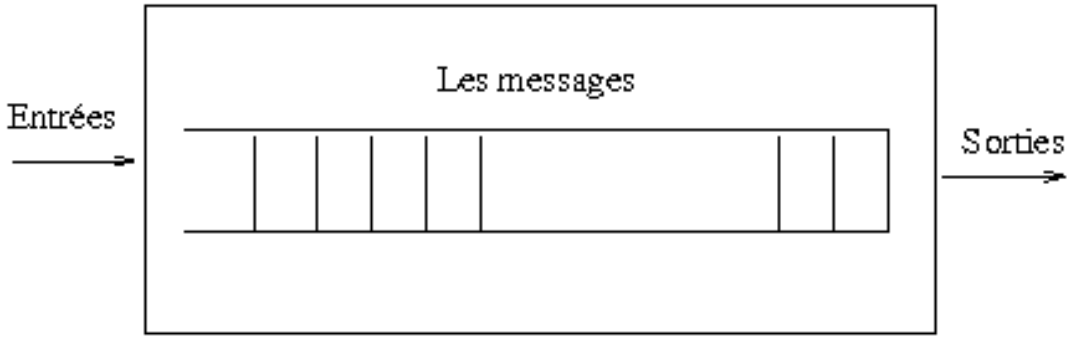
• A l'aide des expressions logiques, modéliser le fonctionnement d'un ascenseur sur 2 étages.

• Les prédicats dont on dispose sont (liste non restrictive) :
asc_a_etage(Etage), *aller_a(Etage)*,
appel({*exterieur*, *interieur*}, *Etage*),
fermer_portes, *ouvrir_portes*, *vérouiller_portes*,
porte_fermée, *porte_ouverte*, *porte_vérouillée*,
attendre(Temps), *opérateurs* ($=$, $\neq$, ...),
etc.

• Vous pouvez introduire d'autres prédicats.
• On notera que pour une spécification exécutable, il faudra imposer un **ordre** dans les évaluation (par ex. l'abandon de la cummutativité de la conjonction)
• Voir plus loin pour les méthodes de vérification, déduction, simulation, exploitation (comme un système de règles de production), etc.

Exercice : spécfication et modélisation d'une file de messages I

• A l'aide des expressions logiques, modéliser le fonctionnement d'une file de messages.



File des messages F

Exercice : spécfication et modélisation d'une file de messages II

• Dans une spécification à l'aide de la logique, les prédicats dont on dispose sont (liste non restrictive) :

initialisation(File), est_vide(File)
enfiler(File, Elément), défiler(File, Elément)
tete(File, Elément), dernier(File, Elément)
taille(File),
etc.

Nota Bene : la *File* est présente dans tous les prédicats. On pourra faire l'hypothèse (comme pour l'exemple de l'ascenseur) que l'univers de ce problème (le domaine) est celui d'une file. Dans ce cas, on pourra abandonner le paramètre *File* dans ces prédicats.

• Au besoin Vous pouvez introduire d'autres prédicats.
• N.B. : voir avec l'enseignant la spécification algébrique.

Un exemple de spécification I

Un exemple de spécification :

• La commission EU a établi un protocole de sécurité d'accès aux données par les utilisateurs. Dans sa recommandation, la commission précise (*TOE : target of evaluation* = le système évalué) :

"le TOE doit être capable de distinguer et administrer les droits d'accès entre un utilisateur (user) et les objets (données) de cette administration. Ceci est fait sur la base d'un utilisateur individuel ou sur celle d'appartenance à un groupe (group) d'utilisateurs ; ou les deux. Il devra être possible de complètement interdire l'accès à certains objets (données) à un utilisateur ainsi qu'à un groupe d'utilisateurs."

• Une spécification (signature et axiomes) de ces recommandations :

user autorisé d'accès à : user x object
user interdit d'accès à : user x object
group autorisé d'accès à : group x object
group inerdit d'accès à : group x object
user associé à : user x group
autoriser accès à : user x object

Un exemple de spécification II

Axiomes (prédicats) u : user, g : group, o : object

uc : user **u** autorisé d'accès à **o**
$\wedge$ user **u** interdit d'accès à **o** = Faux ;

gc : group **g** autorisé d'accès à **o**
$\wedge$ group **g** interdit d'accès à **o** = Faux ;

ga : autoriser **u** d'accès à **o** $\rightarrow$
((user **u** autorisé d'accès à **o**
$\vee$ ($\exists g_1 \in$ *group* $\wedge$ (u associé à $g_1 \wedge g_1$ autorisé d'accès à o)))
$\wedge$ user u interdit d'accès à o = Faux
$\wedge$ ($\exists g_2 \in$ *group* $\wedge$ (u associé à $g_2 \wedge g_2$ interdit d'accès à o)) = Faux)

• Cet exemple montre la possibilité d'utiliser la spécification algébrique avec la spécification logique. On a vu un exemple de ces spécifications (TDA) plus haut.

Méthodes de preuve : introduction

- Quand une argumentation mathématique est-ell correcte ?
- Quelles sont les méthodes pour les construire (e.g. déduction vs abduction) ?

Définition

✓ *Une proposition est une expression qui est vraie ou fausse.*
✓ *Un théorème est une proposition conclusion d'une démonstration valide à l'aide d'axiomes et de définitions.*
✓ *Un lemme est un théorème simple intermédiare de la preuve d'un théorème.*
✓ *Les lemmes et propositions peuvent être utilisés pour simplifier la démonstration d'un théorème complexe.*

✓ *La démonstration d'un théorème est appelée une preuve.*
✓ *Une preuve est construite à partir des axiomes, postulats, hypothèses, propriétés ou théories déjà démontrés.*
✓ *La démonstration d'un théorème suit des règles d'inférence valides.*

Suite

✓ Une démonstration utilisant des règles invalides est dite fallacieuse (e.g. caviar cher, cheval cher → caviar=cheval !) .../...

✓ Un corrolaire est une proposition établie à partir d'un théorème prouvé.

✓ Une conjecture est une expression que l'on ne peut pas prouver mais qui est démontrable par expérience (eg. *Syracus*)

➙ Lorsqu'elle est prouvée, une conjecture devient un théorème.

✓ Les méthodes de preuve sont utilisées dans l'informatique :

➥ Par exemple, dans la preuve d'un programme (*applications critiques, TR*).

➥ On démontre par exemple qu'un système informatique est sécurisé.

N.B. : Une règle (d'inférence ou de preuve) est également appelée une *forme argumentaire*.

Règles d'inférence en propositionnelle

✓ La tautologie $(p \wedge (p \rightarrow q)) \rightarrow q$ est la base d'une règle d'inférence appelée modus ponens ou la règle de détachement.

➙ La règle modus ponens est une méthode d'affirmation.

➙ On note cette règle sous la forme $\frac{p \ , \ p \rightarrow q}{q}$

N.B. : une autre notation formelle de modus ponens est

$$\begin{array}{r} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Exemples

Sachant l'implication **s'il neige, je vais skier** et l'hypothèse **il neige**, on déduit *je vais skier*.

A partir de l'implication si $n > 3$ alors $n^2 > 9$, on peut déduire, pour $n = 4$ que $n^2 > 9$.

Inférence (suite)

- La règle d'addition $\dfrac{p}{p \vee q}$ est une autre règle d'inférence.

Exemple

S'il gèle alors il gèle ou il pleut.

- La règle simplification $\dfrac{p \wedge q}{p}$ est une autre règle d'inférence.

Exemple

S'il gèle et il pleut alors il pleut !

- Le syllogisme hypothétique $\dfrac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}$ est une autre règle d'inférence.

Exemple

S'il pleut alors pas de barbecue, Si pas de barbecue (maintenant) alors barbecue demain et il pleut ; alors on en déduit *barbecue demain*.

Régles d'Inférence (suite)

Définition

La règle modus tollens est une des règles importantes.

➙ *Elle est également appelée la* **méthode de déni**.

On a :

$$\frac{p \longrightarrow q \quad \neg q}{\neg p}$$

- ➙ Lien modus tollens et la contra-posée.
- ➙ modus tollens est également employée dans la résolution.
- ➙ modus tollens et la contraposée.

Exercices

Montrer la preuve des définitions suivantes :

Définition

Le Dilemme par cas : $\dfrac{p \vee q \quad p \rightarrow r \quad q \rightarrow r}{r}$

Définition

Le Dilemme Destructif : $\dfrac{\neg q \vee \neg s \quad p \rightarrow q \quad r \rightarrow s}{\neg p \vee \neg r}$

Définition

Preuve Conditionnelle : $\dfrac{p \quad (p \wedge q) \rightarrow r}{q \rightarrow r}$

Table des règles d'inférence

Regle	**Nom**
$p \rightarrow (p \vee q)$	*Adition*
$(p \wedge q) \rightarrow p$	*Simplification*
$((p) \wedge (q)) \rightarrow (p \wedge q)$	*Conjonction*
$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus Ponsens
$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus Tollens
$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Syllogisme hypothétique
$[(p \vee q) \wedge \neg p] \rightarrow q$	Syllogisme disjonctif
$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Résolution

Tab.: Les principales règles d'inférence

• **Notation :** une règle d'inférence telle que $[p \wedge (p \rightarrow q)] \rightarrow q$ se note également : $p \wedge (p \rightarrow q) \vdash q$.

$p \wedge (p \rightarrow q) \models q$: même chose mais calculatoire.

➔ Un objectif : $\boxed{\vdash \equiv \models}$

Formes valides

• Montrer que q découle logiquement d'un ensemble d'hypothèses $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ revient à démonter que $p_1 \wedge p_2 \wedge \cdots \wedge p_n \longrightarrow q$.

• Pour ce faire, **il faut que** :
  ✓ chacune des hypothèses p_i utilisées soit valide et vraie
  ✓ la règle d'inférence utilisée soit valide.

➙ Rappel : on peut réécrire $P \longrightarrow Q$ en $P \wedge \neg Q \longrightarrow F$.

Car $$P \longrightarrow Q = \neg P \vee Q = (\neg P \vee Q) \vee F$$
$$= \neg(P \wedge \neg Q) \vee F = (P \wedge \neg Q) \longrightarrow F$$

➙ Même chose dans la table de vérité de l'implication.

C-à-d., pour démontrer Q, on déduit une **contradiction** de ce que l'on sait (P) et la négation de ce qu'il faut démontrer.

➥ Certains systèmes utilisent ce mode de démonstration (appelé *réfutation*). Voir plus loin.

Exemple

- Inférer (déduire) *retour_le_soir* du système suivant :

Exemple (d'inférence)

1. $\neg ensoleille \wedge plus\_froid\_que\_hier$. (pas de soleil cette après midi et il fait plus froid qu'hier)
2. $plage \rightarrow ensoleille$. (plage seulement si le temps est ensoleillé)
3. $\neg plage \rightarrow canoe$ (si pas à la plage alors on fait du canoë)
4. $canoe \rightarrow retour\_le\_soir$ (Si canoë alors retour avant le soir)

1. $\neg ensoleille \wedge plus\_froid\_que\_hier$ donne $\neg ensoleille$ (simplification)
2. $\neg ensoleille$ et $plage \rightarrow ensoleille$ donnent $\neg plage$ (modus Tollens)
3. $\neg plage$ et $\neg plage \rightarrow canoe$ donnent $canoe$ (modus Ponens)
4. $canoe$ et $canoe \rightarrow retour\_le\_soir$ donnent $retour\_le\_soir$ (modus Ponens)

Exemple (suite)

- Inférer (déduire) $\neg finir\_programmer \rightarrow me\_leve\_tout\_frais$

Exemple (d'inférence)

1. $mail \rightarrow finir\_programmer$ (si vous m'envoyez un mail, je finirais le programme)
2. $\neg mail \rightarrow irais\_dormir\_tot$ (si vous ne m'envoyez pas de mail, j'irais me coucher tôt)
3. $irais\_dormir\_tot \rightarrow me\_leve\_tout\_frais$ (si je me couche tôt, je me léverais tout frais)

La Résolution

- Il y a des programmes informatiques (compilateurs, interpréteurs) développés pour utiliser le raisonnement et la preuve.
  - ➥ On les appelle *Démonstrateurs automatiques de théorèmes.*
- La plupart utilise la règle d'inférence appelée **résolution** basée sur la tautologie $\boxed{((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r).}$
  - ➥ Notée également : $(p \vee q) \wedge (p \rightarrow r) \vdash (q \vee r).$
    (poser $(p \rightarrow r) \equiv (\neg r \rightarrow \neg p) \wedge (\neg p \rightarrow q) \vdash (\neg r \rightarrow q)$)

- La disjonction obtenue $(q \vee r)$ est appelée **résolvant**.
- En posant $r = q$, on obtient $((p \vee q) \wedge (\neg p \vee q)) \rightarrow q$
- Si l'on pose $r = F$, on obtient $((p \vee q) \wedge (\neg p)) \rightarrow q$ $(q \vee F \equiv q)$
  - ➥ Ce dernier est la tautologie de base du syllogisme disjonctif.

N.B. : le circuit de l'exemple **??** (page **??**) précédent se simplifie par la résolution. De même pour l'ascenseur.

Résolution Propositionnelle

Exemple

Appliquer la **résolution** aux expressions :

$$\textit{pierre\_mange} \vee \neg \textit{il\_pleut} \text{ et } \textit{il\_pleut} \vee \textit{marie\_nage}.$$

$$\begin{array}{lcl} \textit{pierre\_mange} & \vee & \neg \textit{il\_pleut} \\ \textit{il\_pleut} & \vee & \textit{marie\_nage} \\ \hline \therefore \textit{pierre\_mange} & \vee & \textit{marie\_nage} \end{array}$$

Résolution(suite)

• La résolution joue un rôle important en Programmation (Logique).
• Dans le cas du langage Prolog, la résolution est appliquée aux expressions quantifiées.
• Pour utiliser la résolution en logique propositionnelle, on utilise la forme appelée **clause** (de la forme $p \leftarrow q_1 \wedge q_2 \wedge \cdots \wedge q_n.$)

Exemple

Montrer que $(p \wedge q) \vee r$ et $r \rightarrow s$ impliquent $p \vee s$.
➙ Solution :
On ré écrit $(p \wedge q) \vee r$ en

$$p \vee r \quad (1)$$

et

$$q \vee r \quad (2)$$

On remplace également $r \rightarrow s$ par

$$\neg r \vee s \quad (3)$$

➙ On a une conjonction de ces 3 expressions.

$$\_\_\_\_\_$$

➥ En utilisant seulement (1) et (3), on déduit

$$p \vee s.$$

• On appelle ces transformations (ici simplifiées) la mise sous la **forme normale**.

Règles d'inférence fallacieuses I

Règles d'inférence fallacieuses :

- Ces règles ressemblent aux règles valides (c'est le danger !)
- Une des plus connues est $[(p \rightarrow q) \wedge q] \rightarrow p$ (abduction)
- Elle est résumée par le dicton *"il n'y a pas de fumée sans feu"*

➙ Elle est également appelée *fausse affirmation de la conclusion*.

Exemple (un exemple connu)

- **Les bèlges aiment les frites**
- **Napoléon aime(ait) les frites**

➙ On en déduirait (faussement) : **Napoléon est bélge !**

.

- Une autre règle non valide d'inférence :

$$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$$

➙ Elle est également appelée *faux déni de l'hypothèse*.

Règles d'inférence fallacieuses II

➙ Pour le même exemple ci-dessus :

➤ ne pas être bèlge ne veut pas dire qu'on n'aime pas les frites.

Néanmoins, ces règles ont des applications (ex. détection des pannes)

où l'implication ($\rightarrow$) est considéré comme une équivalence ($\leftrightarrow$)../..

A propos de la détection (simplifiée) de pannes :

• On considère une relation de **causalité** entre l'état (panne ou pas) d'un port élémentaire et sa fonction.

• **Exemple** :

Dans le cas de l'hypothèse de panne unique, pour un port élémentaire **P** avec la fonction logique ET (X et Y en entrée, Z en sortie), on pose $\neg P \rightarrow (Z \leftrightarrow X \wedge Y)$.

➥ C'est à dire :

Soit P est en panne (sa valeur = Vrai)

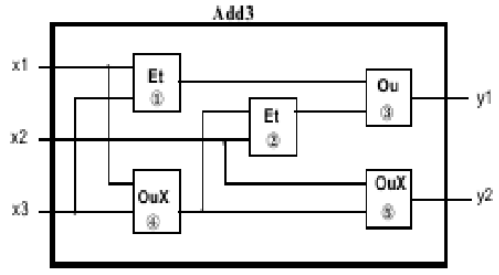
soit il n'est pas en panne (P vaut Fausse) et le circuit se réalise comme une équivalence des entrées et de la sortie.

Règles d'inférence fallacieuses III

La totalité d'un circuit est décrite de cette manière.

On mesure ensuite les entrées et les sorties de ce circuit. Si la fonction n'est pas réalisée, on conlue sur une panne unique. ../..

- **Exemple** : additionneur 3 bits avec des ports élémentaires



- Entrées : [X1,X2,X3], sorties : [Y1,Y2], ports : [P1,P2,P3,P4,P5]).
- On décrit le circuit :

$$\begin{aligned}
&\neg P1 \rightarrow (U1 \leftrightarrow X1 \wedge X3) \quad \wedge \\
&\neg P2 \rightarrow (U2 \leftrightarrow X2 \wedge U3) \quad \wedge \\
&\neg P3 \rightarrow (Y1 \leftrightarrow U1 \vee U2) \quad \wedge \\
&\neg P4 \rightarrow (U3 \leftrightarrow \neg(X1 \leftrightarrow X3)) \quad \wedge
\end{aligned}$$

Règles d'inférence fallacieuses IV

$$\neg P5 \rightarrow (Y2 \leftrightarrow \neg(X2 \leftrightarrow U3)).$$

• On pose ensuite :

Exemple 1 : Entrées = [1,1,0], Sorties = [0,1] panne de P4

Exemple 2 : Entrées = [1,0,1], Sorties = [0,0] panne unique de P3 ou bien de P1.

Inférence avec quantifieurs

- **Instanciation universelle (déduction)** : permet, à partir de $\forall x, P(x)$, de conlure sur $P(c)$ avec c dans l'univers du discours.
  ➤ Par exemple, pour les individus dont *jean* fait partie, si on a $\forall x, mortel(x)$, on déduit $mortel(jean)$
  $\forall x, P(x) \quad \rightarrow \quad P(c)$
- **généralisation universelle (induction)** : permet, à partir de $P(c)$ avec c un élément arbitraire de l'univers du discours, de conlure sur $\forall x, P(x)$ pour x dans l'univers du discours.
  ➤ Par exemple, pour les individus, si on a :
  $mortel(jean), mortel(marie), \ldots$ (arbitrairement choisis),
  on déduit $\forall x, mortel(x)$
  $P(c)$ (c arbitraire) $\quad \rightarrow \quad \forall x, P(x)$
- **instanciation existentielle** : permet, à partir de $\exists x, P(x)$ de conlure sur $P(c)$ avec c un élément particulier (non arbitraire) de l'univers du discours pour lequel $P(c) = True$.
  ➤ En général, on ne connaît pas c mais simplement qu'il existe.
  $\exists x, P(x) \quad \rightarrow \quad P(c)$, c un élément particulier
- **généralisation existentielle** : permet, à partir de $P(c)$ avec c un élément connu de l'univers du discours, de conlure sur $\exists x, P(x)$ pour x dans l'univers du discours.

Règles Inférence (récapitulatif)

Règle d'inférence	**Nom**
$\forall x P(x)$ ——— $\therefore \forall x P(x)$	Instanciation Universelle
P(c) pour un c arbitraire ——— $\therefore \forall x P(x)$	Généralisation Universelle
$\exists x P(x)$ ——— $\therefore$ P(c) pour un c particulier	Instanciation Existentielle
P(c) pour un c particulier ——— $\therefore \exists x P(x)$	Généralisation Existentielle

Inférence (suite)

Remarque

• *Avec* $\forall x, (P(x) \rightarrow Q(x))$ *, si* $P(c) = T$ *pour un* c *donné, alors* $Q(c) = T$*.*

• *N.B. : les règles du tableau ci-dessus sont utilisées en Mathématiques, souvent sans préciser les quantifieurs.*

➤ *Par exemple, si* $x > y$ *alors* $x^2 > y^2 \quad x, y \in \mathbb{R}^+$ *veut dire : pour tous réels positifs, si* $x > y$ *alors . . ..*

• *De même, la démonstration de ces théorèmes procède à la généralisation (sans mention explicite).*

➤ *Par exemple, la méthode de preuve par récurrence utilise ces généralisations.*

Méthodes de preuve de théorèmes

Méthode de preuve Directe :

- On utilise des implications :
  ➙ les méthodes de preuve des implications sont importantes.
- **Rappel** : $p \rightarrow q$ est vrai sauf si $p \wedge \neg q$ (cf. la table de vérité).

- Important : lorsque $p \rightarrow q$ est prouvée, il est seulement besoin de montrer que $q = vrai$ si $p = vrai$.
  ➥ Rappel : $(p \rightarrow q) \equiv \neg p \vee (p \wedge q)$

  ➙ Il n'est généralement pas nécessaire (ni habituel) de prouver $q = vrai$ (suivant la forme disjonctive $\neg p \vee \mathbf{q}$). ../..

Exercice (Résolution)

Dilleme constructif :

Exemple

Montrer que $p \vee r$, $p \rightarrow q$ et $r \rightarrow s$, impliquent $q \vee s$.

Preuves Directes

Preuves Directes :

• L'implication $p \longrightarrow q$ est prouvée en montrant que si $p = vrai$ alors q doit également être vrai.

➔ Ce qui montre que la combinaison $p = vrai, q = faux$ n'arrive jamais (cf. l'unique cas faux de la table de vérité de '$\longrightarrow$').

➥ **Rappel** : $p \longrightarrow q$ est vrai sauf si $p \wedge \neg q$

• On appelle cette méthode la **preuve directe**.

• Pour ce faire, on pose $p = vrai$ et on utilise les règles d'inférence et théorèmes existants pour montrer que $q = vrai$.

Exemple de preuve directe

Avant de voir un exemple, on a besoin d'une définition accessoire :

Définition

Un entier n est pair s'il existe un entier k tel que $n = 2k$.
Un entier n est impair s'il existe un entier k tel que $n = 2k + 1$.

Exemple

Démontrer par la méthode de preuve directe que **si n est impair, alors n^2 est impair**.

Preuve :

Si n est impair, alors $n = 2k + 1$

➥ $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Sachant que $2(2k^2 + 2k)$ est forcément pair (ou nul),

➥ $n^2 = 2(2k^2 + 2k) + 1$ est impair. ∎

Preuves Indirectes

Preuves Indirectes :

Rappel : L'implication $p \longrightarrow q$ est équivalente à la contraposée $\neg q \longrightarrow \neg p$.

Dans la méthode de **preuve indirecte**, *on démontre la contraposée et on en déduit que l'implication du départ est vraie.*

• Habituellement, la preuve de la contraposée est apportée de manière directe mais n'importe quelle autre méthode peut bien s'appliquer.

• Cette méthode ressemble à la méthode de preuve par l'absurde.

Exemple

Exemple (preuve indirecte)

Donner la preuve indirecte du théorème suivant :

si $3n+2$ *est impair alors* n *est impair.*

Démonstration.

Supposons que n est pair (i.e. $\neg q$) : $n = 2K$,

➥ $3n+2 = 6k+2 = 2(3k+1)$

➥ $3n+2$ est pair (multiple de 2) et donc il n'est pas impair.

➥ Ainsi, la négation de q (q est la conclusion de $p \longrightarrow q$) donne la négation de p

➥ On a $\neg q \longrightarrow \neg p$, donc $p \longrightarrow q$.

➥ n est donc impair. ∎

• **Remarque** : dans cette preuve indicrecte, la peuve de la contraposée a été apportée par une méthode directe.

Preuves Triviales

- Une preuve **triviale** est une preuve immédiate et évidente.
- Supposons que l'hypothèse (p) de l'implication $p \longrightarrow q$ est fausse.
  Dans ce cas, $p \longrightarrow q$ est vraie car l'expression aura la forme :
  $$Faux \longrightarrow Vrai \quad \text{ou} \quad Faux \longrightarrow Faux$$

➥ donc : $p \longrightarrow q$ est vraie, quelque soit la valeur de q ($\neg p \vee q$).

Exemple

Montrez que la proposition $P(0)$ est vraie où $P(n)$ est :
Si n > 1 alors $n^2 > n$

Démonstration.

La proposition $P(0)$ est l'implication : Si $0 > 1$ alors $0^2 > 0$
Mais puisque l'hypothèse $0 > 1$ est fausse, la proposition $P(0)$ est automatiquement vraie !
N.B. : le fait que la conclusion $0^2 > 0$ soit fausse ne change rien à la valeur de vérité de la proposition car une implication avec une hypothèse fausse est toujours vraie. ∎

Preuve Triviale (suite)

• De même, si la conclusion de l'implication $p \longrightarrow q$ est vraie alors $p \longrightarrow q$ est vraie dans tous les cas car on aura une des formes :
$Vrai \longrightarrow Vrai$ ou $Faux \longrightarrow Vrai$ (qui sont vraies, cf. Tab. Ver.).

• La preuve triviale est souvent utilisée dans le cas spécial des théorèmes énoncés sur, par exemple, tous les entiers positifs.
Ce type de preuve est utilisé lorsque des cas spéciaux de thérèmes sont démontrés.

Exemple

Montrez que $P(0)$ est vraie avec $P(n) =$
Si a et b sont des entiers positifs avec $a \geq b, alors\ a^n \geq b^n$.

Démonstration.

$P(0)$: Si a et b sont des entiers positifs avec $a \geq b, alors\ a^0 \geq b^0$.
Puisque $a^0 = b^0 = 1$, la conclusion de $P(0)$ est vraie.
N.B. : notons que l'hypothèse $a \geq b$ n'est pas utilisée. ∎

Stratégie de preuve

Remarque

- *Que choisir : preuve directe ou indirecte ?*

➙ *Essayer d'abord la preuve directe :*
Commencer par développer les hypothèses et utiliser les axiomes disponibles.

➙ *Si une preuve directe ne donne rien, essayer la preuve indirecte.*
Rappelons que dans ce cas, on suppose que la conclusion de l'implication (q) est fausse mais on utilise ensuite la preuve directe pour montrer que cette hypothèse mène à une hypothèse (p) fausse de l'implication.

- *Parfois, la preuve directe n'est pas évidente mais la méthode indirecte fonctionne bien.*
  ➙ *Voir les exemples* *.../ ...*

Preuves (exemple)

- Avant de voir un exemple, une définition est nécessaire :

Définition

Un nombre réel r est **rationnel** *s'il existe les entiers p, q avec $q \neq 0$ tels que $r = p/q$.*
N.B. : une fraction peut être irréductible (ou pas). On peut exiger d'une fraction à être irréductible.

Exemple (méthode directe)

Prouver que la somme de 2 rationnels est un rationnel.

Démonstration.

- Essayons la preuve directe :
  Supposons que r, s sont des rationnels :
  ➙ $r = p/q$ et $s = t/u$ avec $q \neq 0, u \neq 0$.

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} \text{ où } q.u \neq 0$$

  ➙ On constate donc que $r + s$ se ré écrit sous forme d'une fraction. ∎

Preuves (suite)

Un autre exemple :

Exemple (méthode indirecte)

Prouver : si n est un entier et n^2 est impair, alors n est impair.

Démonstration.

On essaie d'abord la méthode directe :

- ➙ n^2 est impaire ➙ $n^2 = 2k + 1$
- ➙ Donc $n = \pm\sqrt{2k+1}$ mais on ne peut aller plus loin !

On essaie la méthode indirecte : poser $\neg q$

Hypothèse : n n'est pas impair ➙ $n = 2k$

- ➙ On a alors besoin de démontrer que n^2 n'est pas impair.
- ➙ $n = 2k$ ➙ $n^2 = 4k^2 = 2(2k^2)$
- ➙ On constate que n^2 est pair.

• De la même manière, montrer que si n^2 est pair, alors n est pair. ∎

Preuve par contradiction

Aux côtés des méthodes **directe** et **indirecte**, on a d'autres méthodes de preuve.
➔ La méthode de **preuve par contradiction** (par réfutation) nie la proposition p et montre que $\neg p$ mène à une contradiction.

➤ On en déduit que p devait être vraie.

Plus précisément :

Définition (preuve par contradiction)

• *Supposons qu'une contradiction (q de la forme $r \wedge \neg r$) puisse être trouvée telle que $\neg p \rightarrow q$ soit vraie,*

(on a nié p et cela a conduit à une contradiction appelée ici q),

➥ *Donc $\neg p \rightarrow Faux$ est vrai,*

Ce qui correspond au cas $Faux \rightarrow Faux$ de la table de vérité de l'implication (le cas $(? \rightarrow F) = V$ est lorsque $? = F$).

➤ *Donc, la proposition $\neg p$ doit être fausse, donc p doit être vraie.*

Preuves (suite)

Exemples

Montrer qu'au moins 4 parmi 22 jours consécutifs du calendrier correspondent au même jour de la semaine.

Démonstration.

Soit p la proposition : *au moins 4 parmi 22 jours correspondent au même jour de la semaine*.
Supposons que $\neg p = \textit{vraie}$ ($p = \textit{fausse}$).
Donc (on sait que) au plus 3 de ces 22 jours consécutifs correspondent au même jour de la semaine ($22/3 \simeq 7$),
Mais si au plus 3 jours consécutifs correspondent

- ➙ On a forcément choisi 21 jours (pas 22)
- ➙ C'est donc une contradiction qui permet d'affirmer p . ∎

Nota Bene : une chose et son contraire !

Une contradiction veut dire que l'on arrive à une forme $r \wedge \neg r$.

Preuves (suite)

Exemple

Montrer par une preuve par contradiction que $\sqrt{2}$ est irrationnel.

Démonstration.

Soit p la proposition : $\sqrt{2}$ *est irrationnel*.
Supposons que $\neg p =$ *vraie* ($p =$ *fausse*).
Donc $\sqrt{2}$ est rationnel
- ➙ $\exists a, b$ des entiers avec $b \neq 0$ où $\sqrt{2} = \frac{a}{b}$ irréductible,

On lève au carré : $2 = \frac{a^2}{b^2}$ ➙ $a^2 = 2b^2$ ➙ a^2 est pair ➙ a est pair
- ➙ $a = 2k$ ➙ $a^2 = 2b^2 = 4k^2$ ➙ $b^2 = 2k^2$
- ➙ Si a et b sont pairs, alors $\frac{a}{b}$ est réductible
- ➙ Contradiction de l'hypothèse : $\neg p \longrightarrow$ *Faux* devient vraie.
- ➙ Donc, forcément $\neg p$ *est fausse* ➙ $p =$ *vraie* (cf. la table). ∎

N.B. : Ici, $\neg p$ a conduit à $(r \wedge \neg r)$ où r = a/b est irréductible.
L'irréductibilité de a/b a été posée par hypothèse.

Preuves indirecte et contradiction

• La preuve indirecte d'une implication peut être ré écrite comme une preuve par contradiction.

• Dans une preuve indirecte, on montre que $p \longrightarrow q$ est vraie en utilisant une preuve directe pour montrer que $\neg q \longrightarrow \neg p$ est vrai.

➙ c-à-d. : dans une preuve indirecte de $p \longrightarrow q$, on suppose que $\neg q$ est vraie et on montre que $\neg p$ doit aussi être vraie.

• **Pour ré écrire une preuve indirecte** de $p \longrightarrow q$ comme une preuve par contradiction, on suppose que p et $\neg q$ sont tous les deux vraies.

➙ Puis, on utilise les étapes de la preuve directe de $\neg q \longrightarrow \neg p$ pour montrer que $\neg p$ doit aussi être vraie.

➙ Ce qui mène à la contradiction $p \wedge \neg p$ (on a supposé p mais on a démontré $\neg p$).

➔ Résumons : pour montrer $p \longrightarrow q$ à l'aide de $\neg q \longrightarrow \neg p$

➔ Poser p et $\neg q$ mais démonter $\neg p$ à l'aide de $\neg q \longrightarrow \neg p$

➔ C'est à dire : $p \wedge \neg q \vdash F$; donc $\neg p \vee q \vdash V$

➔ En déduire $p \longrightarrow q$ ../..

Preuve (suite)

Exemple

Donner une preuve par contradiction du théorème

si $3n+2$ *est impair, alors* n *est impair*.

Preuve : Supposons que $3n+2$ est bien impair mais n est pair.

En suivant les même étapes de preuve indirecte du même théorème (vue plus haut), on peut montrer que

si n est pair alors $3n+2$ est pair,

➔ Ce qui contredit l'hypothèse $3n+2$ est impair. ∎

N.B. : la réfutation s'applique bien à une hypothèse.
Ici, on l'applique à une implication. Aussi, selon la table de vérité, le cas où $p \longrightarrow q$ est faux est $p = \mathit{vrai},\ q = \mathit{faux}$.
Donc, on pose $\neg q$ et on démontre $\neg p$, ce qui contredit la table.

Preuve par cas

Preuve par cas :

• Pour prouver une implication de la forme

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q \text{ (tout } p_i \text{ doit pouvoir impliquer } q)$$

On peut utiliser, comme règle d'inférence, la tautologie

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

• Ainsi, si $p \rightarrow q$ et $p \equiv (p_1 \vee p_2 \vee \cdots \vee p_n)$ alors, à la place de p, on utilise cette règle en prouvant que $\bigwedge_i (p_i \rightarrow q)$.

Cette méthode est appelée **Preuve par cas** ou par énumération.

Preuve par cas : exercice

Exemple

Montrer $|xy| = |x||y|$ où x, y sont des réels et $|x|$ dénote la valeur absolue de x.

Démonstration.

- Soit $p =$ "x *et* y sont des réels" et $q = (|xy| = |x||y|)$.
- Posons $p = p_1 \vee p_2 \vee p_3 \vee p_4$ avec :
  $p_1 = x \geq 0 \wedge y \geq 0$, $p_2 = x \geq 0 \wedge y < 0$ ....
- On montre ensuite que $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \ldots$

➙ La preuve pour chaque cas est évidente. ∎

Exercice : Preuve par cas (suite)

Exemple

Montrer que pour tout entier impair n, $n^2 - 1$ est divisible par 8.

Preuve de l'équivalence

• Pour prouver un théorème qui est bidirectionnel, c-à-d. $p \leftrightarrow q$, on utilise la tautologie $(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$

Rappel : $p \leftrightarrow q$ se lit p si et seulement si q (SSI = IFF)

La preuve de cette équivalence est apportée par la preuve de $p \rightarrow q$ (*si p alors q*) et de $q \rightarrow p$ (*si q alors p*).

Exemple

Prouver que l'entier n est impair SSI n^2 est impair

➙ On a déjà traité les deux exemples :
n impair $\rightarrow$ n^2 impair et
n^2 impair $\rightarrow$ n impair

➙ Donc n impair $\leftrightarrow$ n^2 impair

Chaîne de Preuves

- Parfois, un théorème propose l'équivalence de plusieurs propositions. C'est à dire : $p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n$.
  - ➙ Toutes ces propositions ont la même valeur de vérité.
- Une manière de prouver cette équivalence est d'utiliser la tautologie :

$$[p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n]$$

$$\leftrightarrow$$

$$[(p_1 \rightarrow p2) \wedge (p_2 \rightarrow p_3) \wedge (p_n \rightarrow p_1)]$$

➙ Bien plus efficace que de prouver pour toute paire $p_i \rightarrow p_j$.
N.B. : On peut utiliser n'importe quelle **chaîne (en boucle) d'implication**.
➔ Exemple, pour prouver que $p_1 \leftrightarrow p_2 \leftrightarrow p_3$
On peut démontrer $p_1 \rightarrow p_3$, $p_3 \rightarrow p_2$ et $p_2 \rightarrow p_1$.

Preuves (suite)

Exercice

Montrer que les propositions suivantes sont équivalentes :

p_1 : *n est un entier pair*

p_2 : $n-1$ *est un entier impair*

p_3 : n^2 *est un entier pair*

Théorèmes avec Quantifieurs

• Plusieurs méthodes existent pour prouver des thérèmes qui font figurer des quantifieurs.

Définition (Preuve d'existence)

Lorsque l'on affirme que tel objet de type particulier existe : $\exists x P(x)$, *la preuve de ce théorème est une* **preuve d'existence**

• La preuve d'existence peut être apportée de plusieurs manières :

➔ preuve constructive : on trouve un a tel que $P(a)$.

➔ preuve non constructive : on ne trouve pas un a particulier mais par exemple, on utilise la preuve par contradiction pour montrer que la négation de la quantification existentiel conduit à une contradiction.

Preuve (suite)

Exemple (Une preuve constructive d'exisance)

• Montrer qu'il existe un entier positif qui peut être écrit comme la somme des cubes d'entiers positifs et de deux manières différentes.

Démonstration.

Si après des calculs, on trouve $1729 = 10^3 + 9^3 = 12^3 + 1^3$
alors on apporte la preuve constructive de l'existence d'un tel entier ! ∎

Preuve (suite)

Exemple (Une preuve non constructive d'existence)

• Montrer qu'il existe les nombres irrationnels x, y tels que x^y est rationnel.

Preuve : [par raisonnement]

On a vu que $\sqrt{2}$ n'est pas rationnel. Considérons $\sqrt{2}^{\sqrt{2}}$.

➙ S'il est rationnel, on a alors deux nombres non rationnels $x = \sqrt{2}$ et $y = \sqrt{2}$ tels que x^y est rationnel.

➙ Mais si $\sqrt{2}^{\sqrt{2}}$ est irrationnel, alors on pose ($\sqrt{2}$ irrationnel)

$x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ et $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}.\sqrt{2})} = (\sqrt{2})^2 = 2$

➥ Et 2 est un nombre rationnel. ∎

Attention

La démonstration est faite sans que l'on précise laqeulle des 2 parties de cette preuve fonctionne !

➙ On sait que $\sqrt{2}^{\sqrt{2}}$ est irrationnel (sans l'utiliser ici).

Preuve d'unicité

Preuve d'unicité :

• Certains théorèmes portent sur l'existance d'un **unique élément** avec certaines propriétés.

➔ Preuve d'unicité en 2 parties :

➙ 1- un élément x avec telles propriétés existe

➙ 2- pour tout $y \neq x$, y n'a pas les mêmes propriétés.

➔ N.B. : montrer l'unicité de x tel que $P(x)$ est la même chose que de prouver $\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$ [ou $p(y) \rightarrow (x = y)$]

Exemple

Montrer que tout entier possède un inverse additif unique

➙ si x est un entier, il existe un y tel que $x + y = 0$

Démonstration.

Soit l'entier $z \neq y$ tel que $x + z = 0 \Rightarrow x + y = x + z \Rightarrow y = z$

➙ Ce qui contredit l'hypothèse de départ ($z \neq y$). ∎

Recherche de Contre Exemples

Contre-Exemples :
Rappel : pour montrer que $\forall x, P(x)$ est faux, il suffit de trouver un élement y (le *contre exemple*) tel que $P(y) = \textit{faux}$.

Exemple

Montrer que l'expression "tout entier positif est la somme des carrés de 3 entiers" est fausse.

Démonstration.

On cherche un contre exemple en commencant par les entiers : 1...N.

- $1 = 0^2 + 0^2 + 1^2$
- $2 = 0^2 + 1^2 + 1^2$
- $3 = 1^2 + 1^2 + 1^2$ ... $6 = 1^2 + 1^2 + 2^2$

➔ Mais pour l'entier 7, on échoue : les seuls carrés que l'on peut utiliser sont 0, 1 et 4. Or, aucune combinaison de leur somme ne donne 7. ∎

Preuves (suite)

Attention

Une erreur courante dans la prouve de $\forall x, P(x)$ est de trouver quelques éléments qui vérifient la proposition (on ne peut pas toujours enumérer **tous** les x).

➔ Ce qui pose le problème des tests exhaustifs.

➔ **Une solution** : prouver qu'il n'existe pas de contre exemple !

Exemple

Prouver que *tout entier positif est la somme des puissances 4 de 18 autres entiers !*

On peut essayer avec les puissances 4 telles que 0, 1, 16, 81, ... et de présenter 78 entiers (n) tels que la somme des 18 de ces puissances 4 donne n.

➔ On pourra s'arrêter à 78 prétendant avoir assez testé sans voir que 79 ne vérifie pas la propriété !

Erreurs dans les preuves

- **Beaucoup d'erreurs dans les preuves.**

➔ Une preuve en plusieurs étapes est juste si chaque étape est juste et si leur combinaison et leur succession (conclusions partielles) sont justes.

Exemple (où est l'erreur ?)

Preuve de $2 = 1$!

Les étapes :

1) $a = b \quad \Rightarrow \quad a^2 = ab$ (multiplication par a)
2) $a^2 - b^2 = ab - b^2$ (soustraction de b^2)
3) $(a - b)(a + b) = b(a - b)$ (mise en facteur de $(a - b)$)
4) $a + b = b$ (division par $a - b$)
5) $2b = b$ (on avait $a = b$, on remplace)
6) $2 = 1$ (on divise par b)

Erreurs dans les preuves (suite)

• Une autre source d'erreur est dans l'utilisation de l'abduction (affirmation de l'hypothèse par la conclusion).

➙ Ce qui n'est pas une règle d'inférence logique valide .

Exemple (où est l'erreur dans la preuve ?)

Théorème : si n^2 est positif, alors n est positif.

Poser $P(n)$: n psoitif et $Q(n)$: n^2 positif .

Preuve (fausse) : Supposons que n^2 est positif ;

Puisque $P(n) \rightarrow Q(n)$ (ce qui est vrai), on déduit que n est pssitif !

D'ou vient le problème ? :

On s'est servi de l'abduction en utilisant une vérité $[P(n) \rightarrow Q(n)]$ mais une déduction fallacieuse.

Un contre exemple est vite trouvé : $n = -1$.

Erreurs dans les preuves (suite)

- Une autre source d'erreur est dans l'utilisation de la règle :
  $(P(x) \rightarrow Q(x)) \wedge \neg P(x)$ donnerait $\neg Q(x)$?
  ➙ N'est pas une règle d'inférence logique valide (cf. Table).

Exemple : reprendre l'exemple précédent :
On pose $P(n)$: n psoitif et $Q(n)$: n^2 positif .
➔ Et supposons que n n'est pas positif .

Exemple (où est l'erreur ?)

Théorème : si n n'est pas positif, alors n^2 n'est pas positif.

Preuve (fausse) :
➙ On a la forme $P(n) \rightarrow Q(n)$.
➙ Puisque $\neg P(n)$, on déduirait (par erreur) $\neg Q(n)$.

Un contre exemple est vite trouvé : $n = -1$.

Erreurs dans les preuves (suite)

• Une autre source d'erreur et dans l'utilisation de la preuve par cas lorsque l'on ne respecte pas tous les cas.

Exemple (il y a une erreur)

Théorème : si n est un réel, alors n^2 est un réel positif.

Où est l'erreur ?

Soit p_1 : n est positif, p_2 : n est négatif, q : n^2 est positif.
➔ On montre $p_1 \longrightarrow q$ car si n est positif alors n^2 l'est aussi.
➔ On montre $p_2 \longrightarrow q$ car si n est négatif alors n^2 est positif. ∎

Où est le problème ?

➔ On a oublié le cas $n = 0$: dans ce cas $n^2 = 0$ n'est pas positif.
➔ Il faut donc ajouter le cas p_3 : $n = 0$, poser par exemple $p \leftrightarrow (p_1 \vee p_2 \vee p_3)$ et essayer de démontrer $p \longrightarrow q$.
Rappel : Dans ce cas, il faut $(p_1 \longrightarrow q) \wedge (p_1 \longrightarrow q) \wedge \ldots$

Erreurs dans les preuves (suite)

• Enfin, un autre cas d'erreur est la cas de **raisonnement circulaire**
➔ on utilise le théorème à démontrer comme acquis dans la preuve !

Exemple (il y a une erreur)

Théorème : n est un entier pair lorsque n^2 est un entier pair.
➔ Supposé être prouvé par :
  ➔ Supposons n^2 pair $\Longrightarrow n^2 = 4.l^2$ avec $n = 2l$
  ➔ Donc, si $n^2 = 4l^2$ alors $n = \pm\sqrt{n^2} = \pm 2l$. CQFD ? !

➔ On a utilisé $n = 2l$ dans la preuve (hypothétique) sans le démontrer !

Attention

Pourtant, l'affirmation n **est un entier pair lorsque** n^2 **est un entier pair** est elle même juste.
  ➔ C'est la méthode de preuve utilisée qui ne l'est pas.

Néanmoins, mêmes les meilleurs ne sont pas à l'abri d'1 erreur !

Exercice (preuve)

• Montrer que pour tout couple d'entiers m et n, si m et n sont pairs, alors $m + n$ est pair.

Induction Mathématique (forme faible)

- **Principe** (forme faible) :
  - $P(x_0)$ est vrai — prémisse de base
  - $(\forall k \geqslant 0)[si\ P(x_k)\ alors\ P(x_{k+1})]$ — prémices de l'induction

---

  - $\therefore\ (\forall n \geqslant 0)P(n)$ — conclusion

Rappel : le symbole $\therefore$ veut dire *par conséquent* (*therefore*).

• L'antécédent $P(x_k)$ dans $Si\ P(x_k) = vrai\ alors\ P(x_{k+1}) = vrai$ est appelé **l'hypothèse de l'induction**

• Dans une preuve par induction mathématique :
- **L'étape de base** de l'induction est la preuve du *prémisse de base*.
- **L'étape d'induction** de la preuve par induction est la preuve du *prémisse de l'induction*.

➟ On fait l'hypothèse de $P(x_k)$ et on prouve $P(x_{k+1})$.

Induction Mathématique (forme forte)

- **Principe** (forme forte) :
  On utilise la règle d'inférence suivante qui prouve que tous les éléments $x_0, x_1, \ldots x_k$ ont la même propriété $P(x_i)$:
  - $P(x_0)$ est vrai — prémisse de base
  - $(\forall k \geqslant 0)[si\ P(x_0), P(x_1), ..., P(x_k)$ sont tous vrais alors $P(x_{k+1})]$ est vrai — prémisse (fort) de l'induction
  - $\therefore\ (\forall n \geqslant 0)P(n)$ est vrai — conclusion

- En marge : le **principe de bon ordre** pour les entiers :
  Si E est un ensemble non vide d'entiers tels que chaque élément de E est plus grand qu'un certain entier donné, alors E contient un plus petit élément.
  ➥ C'est le cas de x_0 du prémisse de base de l'induction.

Induction (Exemple)

Prouver que pour tout entier $n \geqslant 1, 1+2+3+...+n = \frac{n(n+1)}{2}$.

➙ Dans cette preuve, $x_0, x_1, ...$ sont les entiers 1 .. n et $P(x_n)$ est l'équation $1+2+3+...+n = \frac{n(n+1)}{2}$.

Solution (induction faible).

Etape de base : pour n=1, on a $P(1) = \frac{1(1+1)}{2} = 1$, donc vrai

Etape d'induction : Soit l'entier $k \geqslant 1$ et supposons que P(k) est vrai

➙ $1+2+...+k = \frac{k(k+1)}{2}$ (l'hypothèse de l'induction)

➥ On prouve que P(k+1) est vraie, c-à-d. :

$$1+2+...+(k+1) = \frac{(k+1)(k+2)}{2}$$

Posons : $1+2+...+(k+1) = 1+2+...+k+(k+1)$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2}$$

$$= \frac{(k+2)(k+1)}{2}$$

∎

Induction (suite)

• L'induction Mathématique permet de prouver l'une des expressions :

- $P(0), P(1), P(2), \ldots$ est vraie ET/OU
- $P(1), P(2), P(3), \ldots$ est vraie

Dans ce cas, le principe de l'induction prend la forme :

- $P(0)$ est vrai ET/OU $P(1)$ est vrai
- $(\forall k \geqslant 0)[P(k) \rightarrow P(k+1)]$ est vrai
- $\therefore (\forall n \geqslant 0) P(n)$ est vrai

Si la preuve de $P(k+1)$ peut être obtenue à partir de $P(k)$ alors on peut utiliser le principe faible.
Par contre, si la preuve de $P(k+1)$ nécessite d'utiliser une ou plusieurs expressions $P(u), u \leq k$, alors on utilisera la forme forte.

Induction (suite)

• On peut utiliser l'induction mathématique pour prouver les expressions de la forme *pour tout entier* $n \geq k, P(n)$ *est vrai*.
• Il y a des formes alternatives à l'induction mathématique. Par exemple :

- $P(0)$ et $P(1)$ sont vrais
- $(\forall k \geqslant 0)[P(k) \rightarrow P(k+2)]$ est vrai
- $\therefore (\forall n \geqslant 0) P(n)$

Ou encore :

- $P(0)$ et $P(1)$ sont vrais
- $(\forall k \geqslant 0)[P(k) \wedge P(k+1) \rightarrow P(k+2)]$ est vrai
- $\therefore (\forall n \geqslant 0) P(n)$

• Toutes les formes de l'induction mathématique étant équivalentes, n'importe laquelle peut servir dans la preuve d'une autre forme.

Exemple d'induction

Prouver que pour tout entier $n \geq 4, 2^n < n!$.

Exemple d'induction

Dans un bureau de poste, un postier prétend qu'il peut satisfaire toute demande d'achat de timbres de plus de 8 centimes uniquement avec des timbres de 3 et 5 centimes.
➔ Prouver que $\forall n \geq 8, n = 3t + 5c$ (t=le nombre des timbres à 3 centimes et c=le nombre de timbres à 5 centimes).

Solution informelle :
- Si $n = 8$, on prend un timbre de 3 et un de 5 centimes.
- Si $n > 8$: pour l'étape k, soit on a aucun timbre de 5 centimes, soit on en a au moins un.
➔ Si aucun timbre de 5 centimes, alors forcément, on a plus de 3 timbres de 3 centimes (car $n > 8$).
    ➥ Dans ce cas, pour atteindre l'étape k+1, on remplace 3 timbres de 3 centimes par deux timbres de 5 centimes.
➔ Par contre, si on a au moins un timbre de 5 centimes à l'étape k, on le remplace par 2 timbres de 3 centimes pour atteindre l'étape k+1. ../..

Exemple d'induction

➙ Formaliser la solution (par Induction) :

Suite (timbres)

Remarque :
On considère l'expression $\forall n \geq 8, n = 3t + 5c$ (t=le nombre des timbres à 3 centimes et c=le nombre de timbres à 5 centimes).
➔ Précisons : $n = 3t + 5c, n \geq 8, t \geq 0, c \geq 0, \quad t + c \geq 2$

➙ On a $n = 3t + 5c = 3t + 3c + 2c$
$= 3(t + c) + 2c = 3q + 2c$ (on pose $t + c = q \geq 2$)
➥ C-à-d. : on peut aussi satisfaire toute demande $n \geq 8$ avec des timbres de 2 et 3 centimes.

• Si l'on relâche la condition $q \geq 2$ (la condition > 8 centimes), la formulation du problème change :
➙ On pourrait satisfaire toute demande supérieure à **un centime** !

Prouver cette nouvelle formulation.

Suite : exemple d'induction

En utilisant une forme alternative (adaptée au problème) de l'induction, montrer que
➔ $\forall n \geq 0, F_n < 2^n$ pour n entier et $F_k = Fib(k)$.
Rappel :
$Fib(0) = 0,\ Fib(1) = 1,\ Fib(n) = Fib(n-1) + Fib(n-2)\ pour\ n > 1$

Exercice : induction (suite)

Exemple

Montrer par induction Mathématique que

pour tout entier impair n, $n^2 - 1$ est divisible par 8.

Exercice

Considérons la fonction suivante :

Exemple (maximum d'un tableau)

```
fonction max( T[1..n] : tableau de n entiers) : renvoie un entier
  variables nieme, m : entiers
  Si (n=1) alors renvoyer T[1]
  Sinon
    nieme=T[n] ;
    m=max(T[1.. n-1]) ;
    Si (m > nieme) alors renoyer m
    Sinon renvoyer nieme ;
Fin Max
```

- Soit le prédicat
  $\forall n \geq 1, P(n)$: $max(T[1..n])$ trouve (et renvoie) le maximum des n premiers éléments de T .
  ➙ Démontrer par induction que $P(n)$ est vraie (et juste) : la fonction **max** calcule effectivement le maximum de $T[1..n], n \geq 1$.

Exercice

- La factorielle d'un entier N est définie par :
  $N! = N \times (N-1)!$ si $N > 1$
  $= 1$ si $N = 1$

Soit la fonction factorielle :

Exemple (factorielle)

fonction factorielle(N : entier) : renvoie entier (la valeur de $N!$)
  variable M : entier
  Si (N=1) alors renvoyer 1
  Sinon
    M=factorielle(N-1) ;
    Renvoyer N * M ;
Fin Max

- Soit le prédicat
  $\forall n \geq 1, P(n)$: $factorielle(n)$ calcule la factorielle de l'entier n.
  ➙ Démontrer par induction que $P(n)$ est vraie (et juste).

Intérêt et Justification de l'Induction I

• L'Induction Mathématique est une règle de preuve valide.

➙ Sans l'induction, il faut pouvoir démontrer une infinité de propositions.

• Par exemple : pour le cas $\sum_{i=1}^{n} i = ...$, on peut adopter la stratégie suivante qui utilise la règle **Moduls Ponens** (preuve directe) :

1. On commence par prouver que $P(1)$ est vrai.
2. On montre ensuite que $P(1) \rightarrow P(2)$ est vrai.
3. Si l'on réussit les deux premières étapes, la règle du modus ponens nous dit que $P(2)$ est vrai.
4. On montre ensuite que $P(2) \rightarrow P(3)$ est vrai.
5. Si l'on réussit les 4 premières étapes, la règle du modus ponens nous dit que $P(3)$ est vrai.
6. On montre ensuite que $P(3) \rightarrow P(4)$ est vrai.
7. Si l'on réussi les 6 premières étapes, la règle du modus ponens nous dit que $P(4)$ est vrai.
8. On poursuit de cette façon...

Intérêt et Justification de l'Induction II

- **Exemple** : soit $P(n) : \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

  1. on démontre $P(0) = \sum_{i=0}^{0} 2^i = 2^{0+1} - 1 = 2 - 1 = 1$
  2. on montre ensuite que $P(0) \rightarrow P(1)$.

     ➙ On a $\sum_{i=0}^{1} 2^i = 2 + \sum_{i=0}^{0} 2^i$

  Sachant que $P(0)$ est vrai ($\sum_{i=0}^{0} 2^i = 2^1 - 1$), on substitue cette valeur dans la dernière équation :

  $\sum_{i=0}^{1} 2^i = 2 + (2^1 - 1) = 2^2 - 1$

  Ce qui montre que $P(0) \rightarrow P(1)$.

  .....

  De même, on prouvera que .....$P(k) \rightarrow P(k+1), k \geq 0$

- Cette manière de procéder est juste mais ... fastidieuse.

  Or, on constate dans ces exemples que les traitements sont similaires modulo les valeurs de n.

  ➙ On peut donc choisir de démontrer que $P(n-1) \rightarrow P(n)$.

Intérêt et Justification de l'Induction III

Exercice : démontrer que $P(n-1) \rightarrow P(n)$ pour $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

Démonstration.

$$\text{On a } \sum_{i=0}^{n} 2^i = 2^n + \sum_{i=0}^{n-1} 2^i$$

Supposons que $P(n-1)$ est vrai : $\sum_{i=0}^{n-1} 2^i = 2^n - 1$.

On remplace dans l'équation précédente :

- $\sum_{i=0}^{n} 2^i = 2^n + (2^n - 1) = 2^{n+1} - 1$
- Ce qui démontre que $P(n-1) \rightarrow P(n)$ est vrai. ∎

• Puisque l'on a prouvé $P(n-1) \rightarrow P(n)$, dans les longues étapes fastidiuses, on pourra l'utiliser à chaque fois, dans par exemple $P(3) \rightarrow P(4)$, ... $P(154) \rightarrow P(155)$, ...

Intérêt et Justification de l'Induction IV

Remarque importante :

démontrer que $P(0) \rightarrow P(1)$, ... et .., $P(154) \rightarrow P(155)$ ne veut pas dire que que chacun de ces $p(k)$ (par exemple, $P(0), P(1), ..., P(155), ...$) est vrai.

➙ On peut en faire la démonstration par la table de vérité :
$A \rightarrow B = V$ ne permet pas de conclure sur les valeurs de A et de B.
➙ On peut affirmer la même chose par la démonstration suivante :

Démonstration.

On pose par exemple :

$$P'(n) : \sum_{i=0}^{n} 2^i = 2^{n+1} - 0,123405623$$

On pourra certes démontrer que $P'(n-1) \rightarrow P'(n),\ n > 0$; pourtant , ni $P'(n)$ ni $P'(n-1)$ ne sont vrais ! ∎

• Par contre, il suffira de démontrer $P'(0)$ (non démontrable ici) pour que toute la chaine de démonstration soit vraie (et donc prouver l' impossible : $P'(n)$ est vrai).

Intérêt et Justification de l'Induction V

- On peut illustrer ce principe par n dominos :

1. Faire tomber le premier domino de la chaîne.
2. La chaîne ne doit pas être brisée. Chaque domino en tombant doit pouvoir faire tomber le domino suivant.

Prouver $P(n) \rightarrow P(n+1)$, c'est affirmer que n'importe quel domino fera tomber le prochain.

➡ Mais, cette connaissance ne fera tomber l'ensemble que si le premier (ou le Kième, $k < n$) tombe.

Intérêt et Justification de l'Induction VI

- On peut maintenant affirmer la justesse du principe de l'induction Mathématique rappelée ci-dessous :

  Sous les deux conditions suivantes (pour $k \geq 0$) :

  Si

  ✔ $P(k)$ est vrai

  ✔ $\forall n > k, P(n-1) \rightarrow P(n)$ est vrai

  Alors $P(m)$ est vrai pour $m \geq k$.

- Rappel du principe de l'Induction **généralisée** :

  Si

  ✔ $P(k)$ est vrai

  ✔ $\forall n > k, P(k) \wedge P(k+1 \wedge ... \wedge P(n-1) \rightarrow P(n)$ est vrai

  Alors $P(m)$ est vrai pour $m \geq k$.

Exercice

- En utilisant l'induction (exemple vu plus haut),
  Montrer que pour tout entier impair n, $n^2 - 1$ est divisible par 8.

Exercice

Montrer que l'algorithme de test **palindrome** suivant est *juste*.

Exemple (version 1)

fonction palindrome(Mot[M..N] : tableau de caractères)
renvoie un résultat $\in \{T, F\}$
Soit **Mot'** = inverse(**Mot**)
Si (Mot' = Mot) alors renvoie T
Sinon renvoie F
Fin palindrome

N.B. : inverse(ϕ)=ϕ ; inverse(C : car)=C) ;
inverse(C$\oplus$Cs)=inverse(CS)$\oplus$C ($\oplus$ = concat)

- Une 2e version

Exemple

fonction palindrome(Mot[M..N] : tableau de caractères)
renvoie un résultat $\in \{T, F\}$
Si $M \geq N$ renvoie T (Mot de 0 ou 1 lettre)
Sinon Si $(Mot[N] = Mot[M]) \wedge palindrome(Mot[M+1..N-1])$
Alors renvoie T
Sinon renvoie F
Fin palindrome

Exercice

Montrer par induction que $P(n) : 2^n > n^2$ pour $n > 4$.

Exercice

- Montrer que $p(n) = \sum_{1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

Exercice

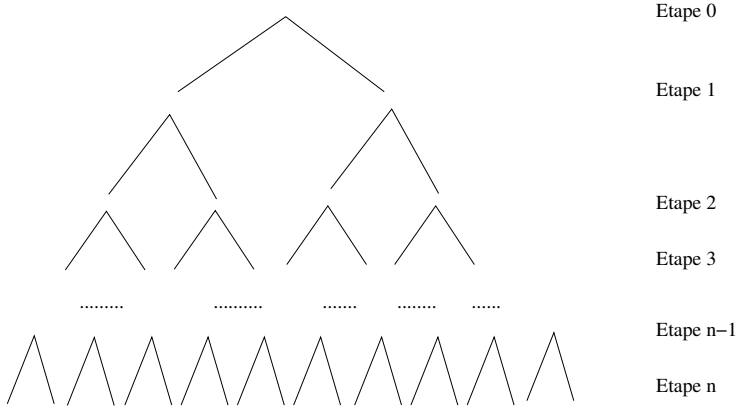
- Montrer que $2^{n+2} + 3^{2n+1}, n \geq 1$ est divisible par 7.

Exemple

Sachant que :

- On a un gateau (étape 0 : on 1 morceau)
- Couper le gateau en deux (étape 1 : on 2 morceaux)
- Puis chaque moitié en 2 (étape 2 : on a 4 morceaux)
- Puis chaque quart en 2 (étape 3 : on a 8 morceaux)
- ....
- Couper chaque ... en 2 (étape n : on a ? morceaux)

Démontrer qu'on aura 2^n morceaux après l'étape n.



Exercice (difficile)

• **Exercice** : montrer que si l'on doit découper un gateau en parts égales pour le partager entre n individus, il faudra $\lfloor log_2\ N \rfloor$ étapes comme ci-dessus.

Autrement dit ...

• Montrez que $D(n) =$ le nombre de divisions entières par 2 nécessaires pour réduire n à 1, est égal à $\lfloor\ log_2 n \rfloor$ pour $n \geq 1$.

Exercices d'Induction

1- montrez que pour $n \geq 1, \sum_{1}^{n} 2^i = 2^{n+1} - 2$

2- montrez que pour $n \geq 1, \sum_{1}^{n} n(n+1) = \frac{n(n+1)(n+2)}{3}$

3- montrez que pour $n \geq 5, 4n < 2^n$

4- montrez que pour $n \geq 1, 8^n - 3^n$ est divisible par 5.

Exercices de détente (preuve fallacieuse) !

Exercice utilisant une partie de l'hypothèse comme preuve.

- 3 jeunes vont au restaurant.
  A la fin de la soirée, la facture est de 25 euros.
  Chacun donne un billet de 10 ; le serveur revient avec 5 euros de monnaie.
  Chacun récupère un euro, laissant au serveur deux euros de pour-boire.

A la sortie du restaurant, les jeunes font leurs comptes :
Chacun a donné 9 euros : $3 \times 9 = 27$,
et deux euros au serveur $+2$
$\Rightarrow$ $= 29$ euros.

- **Où est passé l'euro qui manque ?** (différence entre 29 et 30).

Résolution : exemple

Considérons les expressions suivantes :

1. Elisabeth est un parent (mère) de Charles
2. Charles est un parent (père) de Jean
3. Si X est un parent de Y alors X est un ancètre de Y
4. Si X est parent de Y et Y ancètre de Z alors X est ancètre de Z.
5. On veut démontrer que Elisabeth est un(e) ancètre de Jean.

• Pour ce faire, on utilise la réfutation : on nie ce qu'il faut démontrer et on déduit une contradiction.
Pour simplifier, on note P : parent, A : Ancètre, ...

1. P(e, c) les prénoms (constantes) par une minuscule
2. P(c, j)
3. $\forall X, Y\ P(X, Y) \rightarrow A(X, Y)$ X, Y, Z sont les variables
4. $\forall X, Y\ (P(X, Y) \wedge A(Y, Z)) \rightarrow A(X, Z)$
5. $\neg A(e, j)$

Résolution : exemple (suite)

• Pour faciliter la résolution, on note les expressions sous forme disjonctive puis on applique la résolution :

1. P(e,c)
2. P(c, j)
3. $\neg P(X_1, Y_1) \vee A(X_1, Y_1)$ renommer les variables
4. $\neg(P(X_2, Y_2) \vee \neg A(Y_2, Z_2)) \vee A(X_2, Z2)$
5. $\neg A(e, j)$

---

6. $\neg P(e, Y_3) \vee \neg A(Y_3, j)$ par (4) et (5) avec $[X_2 = e, Z_2 = j]$
7. $\neg A(c, j)$ par (1) et (6) avec $[Y_3 = c]$
8. $\neg P(c, j)$ par (3) et (7) avec $[X_1 = c, Y_1 = j]$
9. Faux par (2) et (8)

Exercice I

Georges Boole a tenté d'apporter une preuve spirituelle avec les propositions suivantes :

- Quelque chose existe ;
- Si quelque chose existe alors, soit quelque chose a toujours existé, soit les choses qui existent maintenant sont sorties du néant ;
- Si quelque chose existe alors, soit ce quelque chose existe par la nécessité de sa propre nature, soit ce quelque chose existe par la volonté d'un autre être ;
- Si quelque chose existe par la nécessité de sa propre nature alors quelque chose a toujours existé ;
- Si quelque chose existe par la volonté d'un autre être alors l'hypothèse que "les choses qui existent maintenant sont sorties du néant" est fausse.

Exercice II

• Proposer un système propositionnel puis démontrer que l'affirmation "quelque chose a toujours existé" est vraie.

Solution : on pose

A : Quelque chose existe
B : Quelque chose a toujours existé
C : Tout ce qui existe maintenant est sorti du néant
D : Quelque chose existe par la nécessité de sa propre nature
E : Quelque chose existe par la volonté d'un autre être

Le système propositionnel est alors :

$A = T$,
$A \rightarrow (B \vee C) \wedge \neg(B \wedge C)$,
$A \rightarrow (D \vee E) \wedge \neg(D \wedge E)$,
$D \rightarrow B$,
$E \rightarrow \neg C$.

Ensuite, on peut démontrer que ce système mène à $B = T$.

Exercice : où est le zèbre ?

Exercice : ce problème est énoncé par les faits suivants :

- 5 maisons consécutives dans une rue, de couleurs différentes, habitées par des hommes de nationalités différentes, chacun avec un animal différent. Chaque homme boît une boisson différente et fume des cigarettes de marque différente.
- La maison verte est à droite de la maison de couleur ivoire.
- Celui qui fume des Winstons élève des escargots.
- On boît du lait dans la maison du milieu.
- Le Novégien est dans la première maison à gauche.
- Le fumeur de Chesterfield habite à côté de celle avec un Renard.
- Dans la maison verte, on boît du café.
- Celui qui fume des Kools est dans la maison jaune.
- Le fumeur de Lucky-Strike boit du jus d'orange.
- Le Norvégien habite à côté de la maison bleue.

.../ ...

Où est le zèbre ? (suite)

Le tableau suivant résume les informations, les complète et aide dans la résolution (raisonnement logique).

couleur	**nationalité**	**animal**	**boisson**	**cigarettes**
rouge	anglais	?	?	?
?	espagnole	chien	?	?
?	ukrainien	?	thé	?
?	japonnais	?	?	Parliment
?	norvégien	?	?	?

couleurs = {rouge, jaune, ivoire, verte, bleue}
animaux = {chien, renard, zèbre, escargots, cheval }
boissons = { eau minérale, lait, café, thé, jeu d'orange }
cigarettes = {Lucky-Strike, Kools, Winstons, Parliment, Marlboro }

Les ' ?' représentent les variables (valeurs à trouver).

Qui possède le zèbre et qui boit de l'eau minérale ?

Solution (Zèbre) I

• Une idée : numéroter les *hommes* de 1 à 5 :

➔ Anglais=3 veut dire : le 3e homme est anglais.

➔ Comment exprimer "la maison verte est à droite de la maison blanche" ?

• Une bonne idée : numéroter les maisons de 1 à 5 :

➙ Anglais=3 : l'anglais vit dans la 3e maison.

➙ Jaune=2 veut dire : la 2e maison est jaune.

➙ la maison verte est à droite de la maison blanche : Verte = Blanche +1

➔ On utilise 25 variables : 5 par catégories (voir l'énoncé).

➙ Il manque 2 variables (une pour les animaux et une pour les boissons).

➙ Pour les animaux : on connaît chien, escargots, renard, cheval, ?

➙ Pour les boissons : on a thé, café, lait, jus, ?

➔ Ces deux là viennent de la question : où est le zèbre (le 5e animal !) et Qui boit de l'eau (5e boisson).

➙ Le domaine de chaque variable est de 1 à 5 (les maisons).

➙ Imposer "tous differrents" aux 5 paquets de 5 variables.

Solution (Zèbre) II

➙ **Une solution** :

- Anglais=3, Espagnole=4, Jap=5, Italien=2, Norvégien=1
- Thé=2, Café=5, Lait=3, jus=4, eau=1
- Rouge=3, Verte=5, Blanche=4, Jaune=1, bleu=2
- Peinter=5, sculteur=3, Diplomate=1, Violoniste=4, Docteur=2
- Chien=4, escargot=3, Renard=1, Cheval=2, Zèbre=5.

➙ Japonais a le zèbre

➙ Norvégian boit de l'eau.

Solution I

• Le prédicat **zebre** renvoie [Painter, Sculptor, Diplomat, Violinist, Doctor] :-

[Red, Green, White, Yellow, Blue] : : 1..5 ,
[English, Spaniard, Japanese, Italian, Norwegian] : : 1..5 ,
[Dog, Snails, Fox, Horse, Zebra] : : 1..5 ,
[Painter, Sculptor, Diplomat, Violinist, Doctor] : : 1..5 ,
[Tea, Coffee, Milk, Juice, Water] : : 1..5 ,
English = Red, Spaniard = Dog, Japanese = Painter,
Italian = Tea, Norwegian = 1, Green = Coffee,
Green = White + 1, Sculptor = Snails, Diplomat = Yellow,
Milk = 3, |Norwegian , Blue| = 1, Violinist = Juice,
|Fox , Doctor|= 1, |Horse , Diplomat|= 1,
tous different([Red, Green, White, Yellow, Blue]),
tous different([English, Spaniard, Japanese, Italian, Norwegian]),
ftous different([Dog, Snails, Fox, Horse, Zebra]),
tous different([Painter, Sculptor, Diplomat, Violinist, Doctor]),
tous different([Tea, Coffee, Milk, Juice, Water]).

Solution II

- Test :
  zebre([English, Spaniard, Japanese, Italian, Norwegian]) ?

Réponse :

English = 3
Italian = 2
Japanese = 5
Norwegian = 1
Spaniard = 4

Vers la forme clausale (optionnel)

Vers la forme clausale :

• But : transformer une expression logique en une forme clausale
➔ La forme clausale est utilisable dans les langages de programmation logiques

Un programme (logique) = une conjonction de clauses .
La forme de chaque clause :

$$(Q_1 \vee Q_2 \vee \cdots \vee Q_n) \vee \neg(P_1 \wedge P_2 \wedge \cdots \wedge P_n)$$
$$P \quad \rightarrow \quad Q$$

➔ Pourquoi obtenir une conjonction de (disjonction SI conjonction)
➥ La forme $P \rightarrow Q$ (disjonction SI conjonction) permet de construire un prédicat ;
➥ la conjonction de ces prédicats donnera un **programme**.

• Exemple : de $A \vee B \vee \neg C \vee \neg D \vee \neg E$,
on peut obtenir la forme $(C \wedge D \wedge E) \rightarrow (A \vee B)$

Vers la forme clausale du premier ordre I

• Il existe un algorithme simple qui permet de transformer une expression de la logique du premier ordre en un ensemble de clauses.
➔ Une partie de cet algorithme a été vue plus haut (rentrer les négations à l'intérieur des expressions).
Important : on suppose qu'il n'y a pas deux quantifieurs sur une même variable (on renomme les variables si nécessaire).

1. Ecrire toute expression $W_1 \leftrightarrow W_2$ en
$$(W_1 \leftarrow W_2) \wedge (W_2 \leftarrow W_1)$$
2. Ecrire toute expression $W_1 \leftarrow W_2$ en $W_1 \vee \neg W_2$
3. Distribuer au maximum la négation (à l'intérieur) :

Ecrire $\neg(\exists x)W$	en	$(\forall x)\neg W$
Ecrire $\neg(\forall x)W$	en	$(\exists x)\neg W$
Ecrire $\neg(W_1 \vee W_2)$	en	$\neg W_1 \wedge \neg W_2$
Ecrire $\neg(W_1 \wedge W_2)$	en	$\neg W_1 \vee \neg W_2$
Ecrire $\neg\neg W$	en	W

../..

Vers la forme clausale du premier ordre II

4. Distribuer au maximum les occurrences de 'OU'
   Ecrire $W \vee (W_1 \wedge W_2)$ en $(W \vee W_1) \wedge (W \vee W_2)$
   Ecrire $W_1 \vee (\forall x W_2)$ en $\forall x (W_1 \vee W_2)$
   Ecrire $W_1 \vee (\exists x W_2)$ en $\exists x (W_1 \vee W_2)$

   Dans les 2 derniers cas, x ne figure pas dans W_1 (par hypothèse).
   On respecte l'ordre ici : distribution de $\vee$ sur $\wedge$ d'abord.

5. Distribuer au maximum les occurrences de $\forall$
   Ecrire $\forall x (W_1 \wedge W_2)$ en $(\forall x W_1) \wedge (\forall x W_2)$
   Si à cette étape, aucun quantifieur existentiel n'est présent, la conversion est terminée. Sinon :

6. Remplacer toute forme close (sans aucun variable libre) :
   $(\forall x_1 \forall x_2 \ldots x_n) \exists y W(y)$ par
   $(\forall x_1 \forall x_2 \ldots \forall x_n)\ W(\mathbf{f}(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}))$
   où **f** est un symbole fonctionnel propre à l'expression.
   Ce processus est appelé **skolémisation** et **f** le symbole de fonction skolem. ../..
   Si $n = 0$ (aucun x_i), on remplace simplement $\exists y W(y)$ en $W(c)$ où **c** est la *constante de skolem*.

Vers la forme clausale du premier ordre III

7. A ce stade, si l'étape (5) de distribution de $\forall$ est encore applicable, alors on l'applique.

L'expression est maintenant sous la forme d'une conjonction de clauses.

➔ Supprimer alors tous les quantifieurs ainsi que les occurrences de $\wedge$ (entre les clauses).

Exemple I

Exemple

soit l'expression suivante (définition de sous-ensemble) :

$$\forall x \forall y \; s(x,y) \leftrightarrow \forall u(u \in x \rightarrow u \in y)$$

$$\begin{array}{ll}
\forall x \forall y[(s(x,y) \leftarrow \forall u(u \in y \leftarrow u \in x)) & \\
\quad \wedge (\forall u(u \in y \leftarrow u \in x) \leftarrow s(x,y))] & \text{après étape 1} \\
\forall x \forall y[(s(x,y) \vee \neg \forall u(u \in y \vee \neg u \in x)) & \\
\quad \wedge (\forall u(u \in y \vee \neg u \in x) \vee \neg s(x,y))] & \text{après étape 2} \\
\forall x \forall y[(s(x,y) \vee (\exists u(\neg u \in y \wedge u \in x))) & \\
\quad \wedge (\forall u(u \in y \vee \neg u \in x) \vee \neg s(x,y))] & \text{après étape 3} \\
\forall x \forall y[\exists u((s(x,y) \vee \neg u \in y) \wedge (s(x,y) \vee u \in x)) & \\
\quad \wedge (\forall u(u \in y \vee \neg u \in x) \vee \neg s(x,y))] & \text{après étape 4} \\
\forall x \forall y \exists u((s(x,y) \vee \neg u \in y) \wedge (s(x,y) \vee u \in x)) & \\
\quad \wedge \forall x \forall y \forall u(u \in y \vee \neg u \in x \vee \neg s(x,y))] & \text{après étape 5} \\
\forall x \forall y((s(x,y) \vee \neg \mathbf{f}(\mathbf{x},\mathbf{y}) \in \mathbf{y}) \wedge (s(x,y) \vee \mathbf{f}(\mathbf{x},\mathbf{y}) \in \mathbf{x})) & \\
\quad \wedge \forall x \forall y \forall u(u \in y \vee \neg u \in x \vee \neg s(x,y))] & \text{après étape 6}
\end{array}$$

../..

Exemple(suite)

- Finalement, l'étape 7 produit un ensemble de clauses :

1. $s(x,y) \leftarrow f(x,y) \in y$
2. $s(x,y) \leftarrow \neg f(x,y) \in x$
3. $u \in y \leftarrow u \in x \wedge s(x,y)$

Interprétation : supposons $f(x,y)$ désigne **un** même élément (arbitraire) représené par la figure ci-contre.

➙ Pour mieux comprendre, considérer la forme originelle qui a produit les deux premières clauses : $s(x,y) \vee \exists u(u \notin y \wedge u \in x)$.

➙ Une autre manière comprendre ce résultat est d'envisager la contraposée des clauses 1 et 2.

➙ La 3e clause a une interprétation simple et directe : elle décrit en quelque sorte une proprité de la relation sous ensemble.

Exercice (Forme clausale)

Considérons la relation *grand-père* : (**gp** : grandpère, **p** : parent (père ou mère))

➔ $\forall x, \forall y \; gp(x, y) \longleftrightarrow \exists z \; (p(x, z) \wedge p(z, y))$

Procédez à la mise sous forme normale clausale de cette relation.

Forme Clausale (suite)

Retour à la conversions en forme clausale :
Les étapes 1 à 5 de la conversion en forme clausale présèrvent les équivalences puisque les ré écritures utilisent les équivalences standard de la logique du premier ordre.

➔ Si ces étapes suffisent, alors la conjonction **C** des clauses résultantes est équivalente à l'expressions **S** initiale.
➔ On note $\mathbf{C} \equiv \mathbf{S}$
➔ Cependant, si la skolémisation de l'étape 6 est nécessaire, alors l'équivalence n'est pas garantie.
➔ On aura alors des propriétés plus faibles :

1. **C** est staisfiable ssi **S** l'est et
2. $\mathbf{C} \models \mathbf{S}$ (*C modélise S* ou, S est déduite de C par calcul).

Forme Clausale (suite)

Raison et exemple : soit $\exists x, p(X)$ skolémisé en $p(a)$
➔ Soit l'interprétation sur le domaine {0,1} avec 'a' associé à 0 et 'p' associé à $\{X : X > 0\}$;
➙ Cette interprétation est alors un modèle pour $\exists x, p(X)$ mais pas pour p(a).

➔ En d'autres termes, dire qu'une proposition est valide pour un élément dans le domaine **n'implique pas** qu'elle est valide pour n'importe quelque élément arbitraire du domaine.
Par contre, l'inverse doit être vraie, quelque soit le domaine et et quelque soit la proposition.
➤ La propriété $C \models S$ ci-dessus doit toujours être vérifiée.

➙ Dans les exemples *sous-ensemble* et *grand-père* ci-dessus, la fonction *f(x,y)* nécessite à chaque fois une interprétation précise.

Quelques équivalences utiles I

• Dans les équivalences suivantes, les quantifications universelles implicites (de la forme $\forall x_1, x_2, \ldots W \ldots$ tout à gauche des expressions) sont supprimées.
➔ Ces mêmes quantificateurs seront donc implicitement présents dans les propositions équivalentes (à droite).
• Ces équivalences sont utilisées et utilisables dans les 7 étapes de conversion en forme clausale précédente.
• Nous avions vu quelques une des ces équivalences dans les pages ci-dessus.
• Les conjonctions à droite des équivalences deviennent naturellement les clauses d'un programme.

1. $W \leftarrow (W1 \wedge W2) \rightleftharpoons$ inchangé.
2. $W \leftarrow (W1 \vee W2) \rightleftharpoons (W \leftarrow W1) \wedge (W \leftarrow W2)$
3. $W \leftarrow (W1 \leftarrow W2) \rightleftharpoons (W \leftarrow W1) \wedge (W \leftarrow \neg W2)$
4. $W \leftarrow (W1 \leftrightarrow W2) \rightleftharpoons (W \leftarrow W1 \wedge W2) \wedge (W \leftarrow \neg W1 \wedge \neg W2)$
5. $(W \vee W1) \leftarrow W2 \rightleftharpoons (W \leftarrow \neg W1 \wedge W2)$
6. $(W \wedge W1) \leftarrow W2 \rightleftharpoons (W \leftarrow W2) \wedge (W1 \leftarrow W2)$

Quelques équivalences utiles II

7. $(W \leftarrow W1) \leftarrow W2 \rightleftharpoons W \leftarrow W1 \wedge W2$
8. $W \leftarrow \exists y\ W1(Y) \rightleftharpoons \exists y(W \leftarrow W1(y))$ Pas de y dans W.
9. $\forall y\ W(y) \leftarrow W1 \rightleftharpoons \forall y\ (W(y) \leftarrow W1)$ parenthésage
   - ➙ la variable y ne figure pas dans $W1$.
   - ➙ Dans ces 2 dernières, le champ de y est élargi. .
10. $W \leftarrow \forall y\ W1(y) \rightleftharpoons W \leftarrow W1(\mathbf{f}(\mathbf{X_1}, \mathbf{X_2}, \ldots, \mathbf{X_n}))$
    - ➙ **f** est la fonction de Skolem.
    - ➙ Rappel : $X_1, X_2, \ldots, X_n$ sont des variables liées par les quantifieurs implicités externs.

Quelques références