NOTES DE COURS

LOGIQUE ET TECHNIQUES DE PREUVE

IFT-10540

et

MATHÉMATIQUES POUR INFORMATICIENS

MAT-22257

Jules Desharnais
Département d'informatique et de génie logiciel
Université Laval
Québec

Automne 2006

Table des matières

Chapitre 0

Introduction

? ? ? ? ? ? ? ? ? ? ? ?

Les propositions suivantes sont-elles vraies ?

1. Si Superman voulait et pouvait prévenir le mal, il le ferait. Si Superman ne pouvait prévenir le mal, il serait impuissant ; s'il ne voulait pas prévenir le mal, il serait malveillant. Superman ne prévient pas le mal. Si Superman existe, il n'est ni impuissant, ni malveillant. Par conséquent, Superman n'existe pas.

2. v est dans le tableau $b[1..10]$ signifie que si la valeur v est dans $b[11..20]$ alors elle n'est pas dans $b[11..20]$.

Le programme fait-il ce que les assertions prétendent qu'il fait ?

Vérifiez le programme suivant. Les variables a, b, i et n sont entières.

$\{0 \leq n\}$
$b, i := 1, 0\,;$
$\{\text{Invariant } 0 \leq i \leq n \ \wedge \ b = a^i\}$
$\{\text{Fonction majorante } n - i\}$
while $i < n$ **do**
begin
$i := i + 1\,;$
$b := a \cdot b$
end
$\{b = a^n\}$

Chapitre 1

Substitution textuelle et règle de Leibniz

1.1 Préliminaires

Syntaxe des expressions mathématiques conventionnelles

Elles sont construites avec
- des *constantes* (comme 42, 3.14),
- des *variables* (comme a, x, y),
- des *opérateurs* (comme $+, \cdot, \div, =, <$).

Par exemple,

$$13$$
$$z$$
$$x + 3 + z^2$$
$$x + 5 > 8 \div x^2$$

sont des expressions.

Définition de la syntaxe des expressions simples :
- Une constante est une expression.
- Une variable est une expression.
- Si E est une expression, alors (E) est une expression.
- Si $\circ$ est un opérateur unaire préfixe et E une expression, alors $\circ E$ est une expression, avec opérande E. Exemple : $-$ peut être utilisé comme opérateur unaire préfixe, de sorte que -18 est une expression.
- Si $\star$ est un opérateur binaire infixe, et si D et E sont deux expressions, alors $D \star E$ est une expression. Par exemple, $8 + 14$ et $(-18) \cdot (t + 4)$ sont des expressions.

Les parenthèses expriment l'agrégation : $2 \cdot (5 + 13)$.

Priorité (*préséance*) des opérateurs : voyez la table 1.1.

TAB. 1.1 – **Préséance (priorité) des opérateurs**

(1)	$[x := e]$ (substitution textuelle)	(priorité élevée)
(2)	$.$ (application de fonction)	
(3)	$+ \quad - \quad \neg \quad \mathcal{P}$ (opérateurs unaires préfixes)	
(4)	$\cdot \quad / \quad \div \quad \mathsf{mod} \quad \mathsf{pgcd} \quad \times \quad \circ \quad \bullet$	
(5)	$+ \quad - \quad \cup \quad \cap$ (opérateurs binaires)	
(6)	$\downarrow \quad \uparrow$	
(7)	$= \quad < \quad > \quad \in \quad \subset \quad \subseteq \quad \supset \quad \supseteq \quad \mid \quad \neq \quad \not< \quad \not> \quad \notin \quad \not\subset \quad \not\subseteq \quad \not\supset \quad \not\supseteq \quad \not\mid$ (conjonctifs, voir page 16)	
(8)	$\vee \quad \wedge$	
(9)	$\Rightarrow \quad \Leftarrow \quad \not\Rightarrow \quad \not\Leftarrow$	
(10)	$\equiv \quad \not\equiv$	(priorité faible)

Les opérateurs binaires non associatifs sont associatifs à gauche, sauf $\Rightarrow$, qui est associatif à droite. Si $\square$ est un opérateur binaire et que $a \square b$ est une expression booléenne, alors la notation $a \not\square b$ est une abréviation pour l'expression $\neg(a \square b)$. L'opérateur $\not\square$ a la même préséance que $\square$. On voit des exemples de tels opérateurs aux lignes (7, 9, 10). Vous pouvez utiliser cette abréviation en tout temps et il n'est pas nécessaire de donner un numéro de loi pour la justifier *si un tel numéro de loi n'existe pas*.

À cause des conventions de préséance,

$$2 \cdot 3 + 8 \;=\; (2 \cdot 3) + 8.$$

(1.1) Exercice. Ajoutez les parenthèses qui font qu'on n'aurait plus besoin de règles de priorité.

1. $a \subseteq b \cup c \;\Rightarrow\; a \cap b = a \cup c$
2. $a \cap b \cup c$

Notion d'état

Un *état* est une liste de variables avec leur valeur :

$$(a, 8.91), (x, 10), (y, 5)$$

L'évaluation d'une expression dans un état E se fait en remplaçant toutes les variables de E par leur valeur et en calculant la valeur de l'expression résultante :

$$a + x \cdot (x + y) \;=\; 8.91 + 10 \cdot (10 + 5) \;=\; 158.91$$

1.2 Substitution textuelle

(1.2) Notation. *Substitution textuelle.*
Soient E et R des expressions, et x une variable.

$$E[x := R]$$

dénote l'expression E avec *TOUTES* les occurrences de x remplacées par (R).

Expression	Résultat	Suppression des parenthèses inutiles
$x[x := t+5]$	$(t+5)$	$t+5$
$(y+x)[y := t+5]$	$((t+5)+x)$	$t+5+x$
$(x \cdot y)[x := t+5]$	$((t+5) \cdot y)$	$(t+5) \cdot y$
$(y+y)[y := 5]$	$((5)+(5))$	$5+5$
$(y+10)[x := 5]$	$(y+10)$	$y+10$

Présentation que nous adopterons :

$$\begin{array}{ll} & (x+2)[x := t+2] \\ = & \quad \langle \text{ Substitution } \rangle \\ & ((t+2)+2) \\ = & \quad \langle \text{ Suppression des parenthèses inutiles } \rangle \\ & t+2+2 \end{array}$$

Notez que si on demande simplement d'effectuer la substitution

$$(x+2)[x := t+2],$$

le calcul *doit s'arrêter* à cette étape, sans réduire l'expression à la forme $t+4$. On n'utilise pas de lois de l'arithmétique, sauf l'associativité (qui permet de supprimer des parenthèses).

(1.3) Notation. *Substitution textuelle simultanée.*
Soient
- E une expression,
- $x : x_1, \ldots, x_n$ une liste de variables *DISTINCTES*,
- $R : R_1, \ldots, R_n$ une liste d'expressions.

$$E[x := R]$$

dénote l'expression E dans laquelle *TOUTES* les occurrences des variables de la liste x ont été remplacées simultanément par les expressions correspondantes de la liste R, mises entre parenthèses.

$$
\begin{array}{ll}
 & (b+a)[a,b \;:=\; b\cdot b, c] \\
= & \qquad \langle \text{ Substitution } \rangle \\
 & ((c)+(b\cdot b)) \\
= & \qquad \langle \text{ Suppression des parenthèses inutiles } \rangle \\
 & c+b\cdot b
\end{array}
$$

(1.4) Exercice. Effectuez les substitutions suivantes, puis éliminez les parenthèses superflues.

1. $(x + x \cdot 2)[x \;:=\; x \cdot y]$
2. $(x + y \cdot x)[x, y \;:=\; b + 2, x + 2]$

(1.5) Notation. *Priorité de la substitution textuelle :*
La substitution a priorité sur toutes les autres opérations.

$$
\begin{array}{l}
(x+y)[x,y \;:=\; 2,3] \quad = \quad 2+3 \\
x+y[x,y \;:=\; 2,3] \quad = \quad x+3
\end{array}
$$

(1.6) Notation. *Associativité à gauche de la substitution :*

$$E[x \;:=\; Q][y \;:=\; R] \quad = \quad (E[x \;:=\; Q])[y \;:=\; R]$$

(1.7) Exercice. Effectuez les substitutions requises, puis éliminez les parenthèses superflues.

$$(x + y \cdot x)[x \;:=\; y + 2][y \;:=\; y \cdot x]$$

(1.8) Exercice. Considérez les opérateurs suivants. La priorité 1 est la plus élevée et 7 la plus faible.

Priorité	Opérateur
1	$[x \;:=\; e]$ (Substitution)
2	$\top \; \Vert$
3	$\heartsuit$
4	$\diamondsuit$
5	$\clubsuit$
6	$\spadesuit$
7	$\star \; \dagger \; \triangle$

Effectuez les substitutions et supprimez les parenthèses superflues.

$$((a \Vert b) \top b \triangle a)[a \;:=\; b \diamond a][b \;:=\; c \top c]$$

1.3 Règles d'inférence

$$\text{Règle d'inférence} \longrightarrow \left\{ \begin{array}{ll} \dfrac{A, B, C}{D} & \longleftarrow \text{prémisses} \\ & \longleftarrow \text{conclusion} \end{array} \right.$$

On parle aussi d'*hypothèses*, au lieu de *prémisses*.

La règle dit que si A, B, C sont des théorèmes, alors D est un théorème.

Règle de *Substitution*

(1.9) Substitution : $\dfrac{E}{E[v := F]}$

Exemple :

$$\frac{2 \cdot a - a = a}{(2 \cdot a - a = a)[a := 5 + t]}$$

Après avoir fait la substitution, on obtient

$$\frac{2 \cdot a - a = a}{2 \cdot (5 + t) - (5 + t) = 5 + t}$$

Cet exemple est une instance de la règle, avec

$$\begin{array}{l} E : 2 \cdot a - a = a \\ v : a \\ F : 5 + t \end{array}$$

1.4 Raisonner sur l'égalité

Soient X et Y des expressions.

– si X et Y ont la même valeur,

$$(X = Y) = \mathsf{vrai} \ ;$$

– si X et Y n'ont pas la même valeur,

$$(X = Y) = \mathsf{faux} \ .$$

On veut pouvoir raisonner au sujet de l'égalité $X = Y$ sans toujours devoir évaluer X et Y. À cette fin, nous nous dotons de lois comme

$$(x = y) = (y = x) \ .$$

Lois de l'égalité

Soient x, y des variables et X, Y des expressions.

(1.10) Réflexivité : $x = x$

(1.11) Symétrie (commutativité) : $(x = y) = (y = x)$

(1.12) Transitivité : $\dfrac{X = Y, \quad Y = Z}{X = Z}$

Loi énoncée par Leibniz (il y a 350 ans) :

> Deux expressions sont égales si et seulement si le remplacement de l'une par l'autre dans n'importe quelle expression E ne change pas la valeur de E.

Conséquence de cette loi :

(1.13) Leibniz : $\dfrac{X = Y}{E[z := X] = E[z := Y]}$

Exemple : la règle de Leibniz avec

$$X : b + 3 \qquad Y : c + 5 \qquad E : d + z \qquad z : z$$

donne

$$\frac{b + 3 \;=\; c + 5}{(d + z)[z := b + 3] \;=\; (d + z)[z := c + 5]}$$

c'est-à-dire

$$\frac{b + 3 \;=\; c + 5}{d + b + 3 \;=\; d + c + 5}$$

(1.14) Exercice. Voici une instance incomplète de la règle de Leibniz (1.13). Complétez la partie manquante et donnez l'expression E correspondante. Donnez toutes les réponses possibles.

(*) $$\frac{7 = y + 1}{7 \cdot x + 7 \cdot y = ?}$$

(1.15) Exercice. Considérez les opérateurs de l'exercice (1.8). Voici une instance incomplète de la règle de Leibniz (1.13) qui utilise ces opérateurs. Complétez la partie manquante et donnez l'expression E correspondante. Donnez toutes les réponses possibles.

$$\frac{a \triangle b = c \| d \diamond e}{? = f \triangle c \| d \diamond e}$$

1.5 Règle de Leibniz et évaluation des fonctions

(1.16) Notation. *Application d'une fonction à un argument.*
Afin de réduire le nombre de symboles, nous utiliserons habituellement

$$f.x \quad \text{au lieu de} \quad f(x)$$

et nous écrirons (par exemple)

$$f(a+5) \quad \text{et non} \quad f.(a+5)$$

lorsque l'argument est entre parenthèses.

Autre formulation de la règle de Leibniz :

(1.17) Leibniz : $\dfrac{X = Y}{g.X = g.Y}$

1.6 Problèmes

1. Effectuez les substitutions textuelles suivantes, puis supprimez les parenthèses superflues :
   (a) $(a + b \cdot 3)[b, a := a \cdot b, a \cdot a]$
   (b) $((x + y) \cdot z)[x, y := x, y]$
   (c) $(x + x \cdot 2)[x, y := x, z][x := y]$
   (d) $(x + x \cdot y + x \cdot y \cdot z)[x, y := y, x][y := 2 \cdot y]$
2. La règle d'inférence de Leibniz (1.13) donne lieu à une infinité de règles d'inférence particulières obtenues en assignant une expression à ses trois paramètres E, X et Y. Il y a ci-dessous des cas particuliers de la règle de Leibniz, avec une partie manquante. Trouvez la partie manquante et donnez l'expression E correspondante. Donnez toutes les réponses possibles.
   (a) $\dfrac{x = x + 2}{4 \cdot x + y = ?}$
   (b) $\dfrac{a = b + 2}{? = 3 \cdot (b + 2) + 3 \cdot b + 1}$
3. Cet exercice porte sur la règle de Leibniz (1.13). On vous donne l'expression $E[z := X]$ ainsi que l'indice $X = Y$. Trouvez l'expression résultante $E[z := Y]$.

	$E[z := X]$	$X = Y$
(a)	$(x + y) \cdot w$	$w = x \cdot y$
(b)	$p \cap q$	$q = q \cup r$

4. Cet exercice porte sur la règle de Leibniz (1.13). Pour chacune des paires d'expressions $E[z := X]$ et $E[z := Y]$ ci-dessous, donnez les expressions X et Y telles que $E[z := X] = E[z := Y]$. Indiquez ensuite quelle est l'expression E. Donnez toutes les réponses possibles.

	$E[z := X]$	$E[z := Y]$
(a)	$x \cdot y \cdot x$	$y \cdot x \cdot x$
(b)	$p \Rightarrow q \wedge (r \vee p)$	$p \Rightarrow q \wedge q$

5. Utilisez la table de préséance suivante pour faire les substitutions demandées. À l'exception de la substitution, tous les opérateurs sont des opérateurs binaires. La priorité 1 est la plus élevée et 7 la plus faible.

Priorité	Opérateur
1	$[x := e]$ (Substitution)
2	$\top \parallel$
3	$\heartsuit$
4	$\diamondsuit$
5	$\clubsuit$
6	$\spadesuit$
7	$\star \dagger \triangle$

(a) $((x \top y) \| z \diamondsuit x)[x := y \heartsuit x]$

(b) $((x \heartsuit y) \top (z \star x \heartsuit y) \star x)[x := z \diamondsuit z]$

(c) $(x \heartsuit y \spadesuit x \star z \diamondsuit x \heartsuit y)[x, y := x \top y, y \triangle x]$

(d) $((x \star y) \dagger x)[x, y := x \diamondsuit x, x \triangle x]$

(e) $(x \top x \triangle x)[x, y := y, z]$

(f) $(x \top x \triangle x)[x := y][y := z]$

(g) $((x \star y) \dagger x)[x := x \diamondsuit x][y := x \triangle x]$

(h) $(x \heartsuit y \spadesuit x \star z \diamondsuit x \heartsuit y)[x := x \top y][y := y \triangle x]$

6. Nous aimerions que les expressions $X = X$ et $(X = Y) = (Y = X)$ soient des théorèmes, où X et Y sont des expressions quelconques. Cependant les axiomes (1.10) et (1.11) sont restreints au cas où X et Y sont des variables (x et y). Perd-on de la généralité avec (1.10) et (1.11) ?

7. La loi de Leibniz dit que deux expressions sont égales si et seulement si le remplacement de l'une par l'autre dans n'importe quelle expression E ne change pas la valeur de E. Cette loi peut être décomposée en deux parties (les symboles X et Y sont ajoutés pour que le passage à la règle (1.13) soit plus clair) :
   – Si deux expressions X et Y sont égales, alors le remplacement de l'une par l'autre dans n'importe quelle expression E ne change pas la valeur de E.
   – Si, quelle que soit l'expression E, le remplacement d'une expression X par une expression Y dans E ne change pas la valeur de E, alors X et Y sont égales.

La règle (1.13) correspond à la première partie. En effet, la règle (1.13) dit que si $X = Y$, alors $E[z := X] = E[z := Y]$. Démontrez la deuxième partie. Plus précisément, montrez que si $E[z := X] = E[z := Y]$ est un théorème pour toute expression E, alors $X = Y$.

Chapitre 2

Expressions booléennes

2.1 Syntaxe des expressions booléennes

Une *expression booléenne* est construite à partir des constantes vrai et faux, de variables booléennes, qui peuvent prendre les valeurs vrai et faux (seulement) et des opérateurs booléens. Les opérateurs booléens les plus couramment utilisés sont :

$\equiv, =, \Leftrightarrow$	égalité, équivalence
$\not\equiv, \neq$	inégalité, inéquivalence
$\neg$	négation, non
$\vee$	disjonction, ou
$\wedge$	conjonction, et
$\Rightarrow$	implication, si ...alors
$\Leftarrow$	conséquence

Définition des opérateurs booléens

Voici les tables de tous les opérateurs unaires et binaires. Dans ces tables, v et f signifient respectivement vrai et faux.

	id	$\neg$
v	v	f
f	f	v

								$\equiv$			$\not\equiv$						
		$\vee$	$\Leftarrow$		$\Rightarrow$			$=$	$\wedge$	$\not\wedge$	$\neq$					$\not\vee$	
v	v	v	v	v	v	v	v	v	v	f	f	f	f	f	f	f	f
v	f	v	v	v	v	f	f	f	f	v	v	v	v	f	f	f	f
f	v	v	v	f	f	v	v	f	f	v	v	f	f	v	v	f	f
f	f	v	f	v	f	v	f	v	f	v	f	v	f	v	f	v	f

où $\not\wedge$: nand et $\not\vee$: nor.

Remarques sur quelques opérateurs booléens

1. On peut vérifier à partir de la table des opérateurs booléens que

$$\begin{array}{rcl@{\qquad}rcl} (p \neq q) & \equiv & \neg(p = q) & (p \neq q) & = & \neg(p = q) \\ (p \not\equiv q) & \equiv & \neg(p \equiv q) & (p \not\equiv q) & = & \neg(p \equiv q) \\ (p \not\wedge q) & \equiv & \neg(p \wedge q) & (p \not\wedge q) & = & \neg(p \wedge q) \\ (p \not\vee q) & \equiv & \neg(p \vee q) & (p \not\vee q) & = & \neg(p \vee q) \\ (p \Rightarrow q) & \equiv & (q \Leftarrow p) & (p \Rightarrow q) & = & (q \Leftarrow p) \end{array}$$

2. (a) $p = q$ se prononce « *p égale q* ».

   (b) $p \equiv q$ se prononce « *p est équivalent à q* ».

   (c) Dans $p \Rightarrow q$ et $q \Leftarrow p$, p s'appelle *l'antécédent* et q le *conséquent*.

3. $(p \vee q) \equiv$ vrai si

$$\begin{array}{rl} & p \equiv \text{vrai} \\ \text{ou} & q \equiv \text{vrai} \\ \text{ou} & p \equiv \text{vrai et } q \equiv \text{vrai} . \end{array}$$

   Par conséquent,

$$\textit{j'ai une auto rouge} \ \vee \ \textit{j'étudie l'informatique}$$

   est vrai si j'ai une auto rouge, ou si j'étudie l'informatique, ou si j'ai une auto rouge et que j'étudie l'informatique. On dit que l'opérateur $\vee$ est le *ou inclusif*.

   Pour exprimer le *ou exclusif*, on utilise l'inégalité (ou l'inéquivalence), car elle est vraie quand exactement l'un de ses opérandes est vrai. Ainsi

$$\textit{j'ai une auto rouge} \not\equiv \textit{j'étudie l'informatique}$$

   exprime que j'ai une auto rouge ou que j'étudie l'informatique, mais pas les deux.

4. $(p \Rightarrow q) \equiv$ faux seulement lorsque $p \equiv$ vrai et $q \equiv$ faux .
   Intuitivement, l'expression

$$x > 2 \ \Rightarrow \ x > 0$$

   est vraie. Vérifions cela pour quelques valeurs de x $(3, 1, 0)$:

   (a)
   $(x > 2 \ \Rightarrow \ x > 0)[x := 3]$
   $=$ $\langle$ Substitution $\rangle$
   $3 > 2 \ \Rightarrow \ 3 > 0$
   $=$ $\langle$ Évaluation de $3 > 2$ et $3 > 0$ $\rangle$
   vrai $\Rightarrow$ vrai
   $=$ $\langle$ Définition de $\Rightarrow$ (table des opérateurs booléens) $\rangle$
   vrai

(b) $(x > 2 \Rightarrow x > 0)[x := 1] \;=\; (\mathsf{faux} \Rightarrow \mathsf{vrai}) \;=\; \mathsf{vrai}$

(c) $(x > 2 \Rightarrow x > 0)[x := 0] \;=\; (\mathsf{faux} \Rightarrow \mathsf{faux}) \;=\; \mathsf{vrai}$

Si $0 > 2$ *alors* $0 > 0$ est donc vrai, tout comme

Si je suis le pape Jean-Paul II, alors tu as traversé l'Atlantique à la nage.

puisque je ne suis pas Jean-Paul II.

2.2 Tables de vérité

Les tables de vérité sont utilisées pour évaluer les expressions booléennes.

Évaluation de $\neg p \wedge (q \Rightarrow r)$

p	q	r	$\neg p$	$q \Rightarrow r$	$\neg p \wedge (q \Rightarrow r)$
v	v	v	f	v	f
v	v	f	f	f	f
v	f	v	f	v	f
v	f	f	f	v	f
f	v	v	v	v	v
f	v	f	v	f	f
f	f	v	v	v	v
f	f	f	v	v	v

Les colonnes p, q, r définissent l'état. Tous les états possibles sont énumérés. Les autres colonnes traitent les sous-expressions de l'expression donnée. Pour l'état

$$(p, \mathsf{vrai}),\ (q, \mathsf{vrai}),\ (r, \mathsf{faux}),$$

l'expression est fausse : $\big(\neg p \wedge (q \Rightarrow r)\big)[p, q, r := \mathsf{vrai}, \mathsf{vrai}, \mathsf{faux}] \;=\; \mathsf{faux}$

(2.1) Exercice. Donnez la table de vérité de l'expression

$$\Big(\big(p \equiv q\big) \equiv r\Big) \;\equiv\; \Big(p \equiv \big(q \equiv r\big)\Big)\ .$$

On dit qu'un opérateur binaire $\star$ est associatif si, et seulement si,

$$a \star (b \star c) \;=\; (a \star b) \star c\ .$$

L'exercice ci-dessus montre que l'équivalence ($\equiv$) et l'égalité ($=$) sont associatives (car on obtient bien sûr le même résultat avec l'égalité qu'avec l'équivalence). Les opérateurs $\not\equiv, \neq$, $\vee, \wedge$ et $+$ (sur les entiers ou les réels) sont eux aussi associatifs.

Lorsqu'un opérateur $\star$ est associatif, on omet en général les parenthèses et on écrit simplement

$$a \star b \star c$$

au lieu de

$$a \star (b \star c) \quad \text{ou de} \quad (a \star b) \star c \ .$$

Considérez par exemple l'addition sur les entiers. On écrit $x + y + z$ au lieu de $x + (y + z)$ ou de $(x + y) + z$. C'est ce que nous ferons pour tous les opérateurs associatifs, à l'exception de l'égalité ($=$). La section suivante explique la différence de traitement entre l'équivalence et l'égalité.

2.3 Égalité versus équivalence

(2.2) Notation. Supposons que $\circ$ et $\star$ sont des opérateurs dits *conjonctifs* (ligne (j) de la table de préséance des opérateurs). Ceci signifie que

$$a \circ b \star c \quad \text{est une abréviation de} \quad a \circ b \ \wedge \ b \star c \ .$$

Par exemple,

$$a < b = c \quad \text{est une abréviation de} \quad a < b \ \wedge \ b = c \ ,$$
$$a = b = c \quad \text{est une abréviation de} \quad a = b \ \wedge \ b = c \ .$$

En ce qui concerne l'omission des parenthèses, l'égalité ($=$) est considérée comme un opérateur conjonctif même si elle est associative. Les expressions

$$a = b = c \qquad \text{et} \qquad a \equiv b \equiv c$$

peuvent donner des résultats différents.

$$(\mathsf{faux} = \mathsf{faux} = \mathsf{vrai}) \quad \neq \quad (\mathsf{faux} \equiv \mathsf{faux} \equiv \mathsf{vrai})$$

$$\begin{array}{ll} & \mathsf{faux} = \mathsf{faux} = \mathsf{vrai} \\ = & \qquad \langle \ = \text{ est conjonctive} \ \rangle \\ & (\mathsf{faux} = \mathsf{faux}) \wedge (\mathsf{faux} = \mathsf{vrai}) \\ = & \qquad \langle \ \text{Évaluation des} = \ \rangle \\ & \mathsf{vrai} \wedge \mathsf{faux} \\ = & \qquad \langle \ \text{Évaluation de} \wedge \ \rangle \\ & \mathsf{faux} \end{array}$$

$$\begin{array}{ll} & \mathsf{faux} \equiv \mathsf{faux} \equiv \mathsf{vrai} \\ = & \qquad \langle \ \text{Évaluation de} \equiv \text{gauche} \ \rangle \\ & \mathsf{vrai} \equiv \mathsf{vrai} \\ = & \qquad \langle \ \text{Évaluation de} \equiv \ \rangle \\ & \mathsf{vrai} \end{array}$$

Ces preuves démontrent

$$\begin{array}{lcl}(\mathsf{faux} = \mathsf{faux} = \mathsf{vrai}) & = & \mathsf{faux}\\ (\mathsf{faux} \equiv \mathsf{faux} \equiv \mathsf{vrai}) & = & \mathsf{vrai}\end{array}$$

On pourrait se passer de la convention de conjonctivité des opérateurs. C'est du *sucre syntaxique*. Avant de manipuler des expressions qui utilisent des opérateurs conjonctifs, il vaut mieux éliminer le sucre syntaxique.

Le format de preuve permet d'éliminer des parenthèses

$$\begin{array}{ll}
 & (\mathsf{faux} = \mathsf{faux} = \mathsf{vrai})\\
= & \quad \langle\ = \text{ est conjonctive }\rangle\\
 & ((\mathsf{faux} = \mathsf{faux}) \wedge (\mathsf{faux} = \mathsf{vrai}))\\
= & \quad \langle\ \text{Évaluation des } = \rangle\\
 & (\mathsf{vrai} \wedge \mathsf{faux})\\
= & \quad \langle\ \text{Évaluation de } \wedge\ \rangle\\
 & \mathsf{faux}
\end{array}$$

$\rightsquigarrow$

$$\begin{array}{ll}
 & \mathsf{faux} = \mathsf{faux} = \mathsf{vrai}\\
= & \quad \langle\ = \text{ est conjonctive }\rangle\\
 & (\mathsf{faux} = \mathsf{faux}) \wedge (\mathsf{faux} = \mathsf{vrai})\\
= & \quad \langle\ \text{Évaluation des } = \rangle\\
 & \mathsf{vrai} \wedge \mathsf{faux}\\
= & \quad \langle\ \text{Évaluation de } \wedge\ \rangle\\
 & \mathsf{faux}
\end{array}$$

Par convention, il n'est pas nécessaire de mettre les lignes séparées par les opérateurs de la colonne gauche entre parenthèses. Ces opérateurs sont évalués en dernier, même s'ils ont une priorité élevée.

Remplacement de $=$ par $\equiv$ et vice versa

Parfois, on veut utiliser $\equiv$ au lieu de $=$, ou l'inverse. Le changement peut être fait, moyennant certaines précautions. Il faut tenir compte de la priorité des opérateurs et des conventions d'écriture des opérateurs conjonctifs et associatifs. Voici un exemple.

$$\begin{array}{ll}
 & a \equiv b \equiv c\\
= & \quad \langle\ \text{Ajout de parenthèses }\rangle\\
 & (a \equiv b) \equiv c\\
= & \quad \langle\ \equiv \text{ remplacé par } = \rangle\\
 & (a = b) = c
\end{array}$$

$$\begin{array}{ll}
 & a = b = c\\
= & \quad \langle\ = \text{ est conjonctif }\rangle\\
 & a = b \wedge b = c\\
= & \quad \langle\ \text{Ajout de parenthèses }\rangle\\
 & (a = b) \wedge (b = c)\\
= & \quad \langle\ = \text{ remplacé par } \equiv \rangle\\
 & (a \equiv b) \wedge (b \equiv c)
\end{array}$$

Remarque : quand on remplace $=$ par $\equiv$, il faut souvent ajouter des parenthèses, car $=$ a une priorité assez élevée, alors que $\equiv$ a une priorité faible.

2.4 Satisfiabilité et validité

(2.3) Définition. Soit P une expression booléenne.

1. P est *satisfaite* dans un état si elle a la valeur vrai dans cet état.
2. P est *satisfiable* s'il y a un état dans lequel elle est satisfaite.
3. P est *valide* si elle est satisfaite dans tous les états.
4. Une *tautologie* est une expression booléenne valide.

Par exemple :

1. $p \Rightarrow q$ est satisfaite dans l'état $(p, \mathsf{faux}),\ (q, \mathsf{vrai})$.
2. Par l'item précédent, $p \Rightarrow q$ est satisfiable.
3. $p \Rightarrow q$ n'est pas valide, car elle n'est pas satisfaite dans l'état $(p, \mathsf{vrai}),\ (q, \mathsf{faux})$.

2.5 Modélisation de propositions énoncées en français

Une *proposition* est un énoncé qui peut être vrai ou faux. Par exemple :

(2.4) Montréal a quatre universités et Québec en a une.

Pourquoi traduire une proposition française en expression booléenne ?

1. Cela force la résolution des ambigüités de la langue française.
2. Cela permet de manipuler et de simplifier les expressions selon les lois de la logique propositionnelle (chapitre 3). C'est beaucoup plus sûr que de raisonner en français.

Traduction triviale (simpliste) : une variable pour toute la proposition

Donnons le nom p à la proposition (2.4) :

p : Montréal a quatre universités et Québec en a une.

p est une *variable booléenne* (parfois appelée variable propositionnelle) qui peut prendre la valeur vrai ou la valeur faux, selon que la proposition est vraie ou fausse.

Traduction raffinée : tient compte des sous-propositions

Donnons les noms q et r aux deux sous-propositions de (2.4) :

q : Montréal a quatre universités,
r : Québec a une université.

Remarquez comment il faut modifier la phrase française : « Québec en a une » n'a pas de sens prise isolément. La proposition (2.4) s'écrit alors

$$q \text{ et } r, \qquad \text{ou mieux,} \qquad q \wedge r \ .$$

(2.5) Traduction d'une proposition en expression booléenne

1. Introduire des variables booléennes pour dénoter les sous-propositions.
2. Remplacer ces sous-propositions par les variables booléennes correspondantes.
3. Traduire le résultat de l'étape 2 en expression booléenne, en utilisant les correspondances « évidentes » entre certains mots et les opérateurs logiques. Voyez la table ci-dessous pour un exemple.

Tab. 2.3 – Traduction de certains mots en opérateurs

et, mais	deviennent	$\wedge$
ou	devient	$\vee$
ne pas, non	deviennent	$\neg$
il n'est pas vrai que	devient	$\neg$
si p alors q	devient	$p \Rightarrow q$

L'implication

Revoyez ce que dit la section 2.1 de l'implication. En posant

jp : je suis le pape Jean-Paul II
at : tu as traversé l'Atlantique à la nage
$g2$: $x > 2$
$g0$: $x > 0$

on peut traduire

si je suis le pape Jean-Paul II, alors tu as traversé l'Atlantique à la nage

par

$$jp \Rightarrow at$$

et

$$\text{si } x > 2, \text{ alors } x > 0$$

par

$$g2 \Rightarrow g0 \ .$$

Remarque : au chapitre 7, nous étendrons le langage des expressions booléennes pour pouvoir utiliser des variables autres que booléennes, comme x dans $x > 2$.

L'implication : autres exemples

À traduire :

(a) si vous ne faites pas les exercices, vous coulerez ;

(b) faites les exercices ou vous coulerez ;

(c) tous les nombres pairs sont divisibles par 4
(peut aussi s'écrire : si un nombre est pair, il est divisible par 4).

Posons	ex : (vous) faites les exercices
	co : vous coulerez
	p : être pair
	q : être divisible par 4

Traduction :	(a)	$\neg ex \Rightarrow co$
	(b)	$ex \vee co$
	(c)	$p \Rightarrow q$

(a) et (b) ont le même sens en français. On peut aussi vérifier que

$$\neg ex \Rightarrow co \ \equiv \ ex \vee co \ .$$

Traduction de « ou »

Voyez la section 2.1.

Si et seulement si (abréviation : ssi)

« Si et seulement si » est traduit par $\equiv$. Par exemple, soit la définition

Un triangle est équilatéral si, et seulement si, il a trois côtés égaux.

Posons

trois : le triangle a trois côtés égaux,
équi : le triangle est équilatéral.

La définition se traduit par $trois \equiv équi$ et peut être décomposée en deux parties :

1. Un triangle est équilatéral s'il a trois côtés égaux,

   ce qui se traduit par $trois \Rightarrow équi$.

2. Un triangle est équilatéral seulement s'il a trois côtés égaux,

   c'est-à-dire : tout triangle équilatéral a forcément trois côtés égaux

   c'est-à-dire : si un triangle est équilatéral, alors il a trois côtés égaux

   ce qui se traduit par $équi \Rightarrow trois$ ou par $trois \Leftarrow équi$.

Remarque : on peut vérifier au moyen des tables de vérité que $(p \Rightarrow q) \wedge (p \Leftarrow q) \equiv p \equiv q$.

Implication versus équivalence

Posons

aime : j'aime ce que je mange,
orange : je mange une orange.

1. Implication :

   j'aime ce que je mange si je mange une orange

   se traduit par

   $$orange \Rightarrow aime .$$

   Je peux manger une pomme et aimer ça.

2. Équivalence :

   j'aime ce que je mange ssi je mange une orange

   se traduit par

   $$aime \equiv orange .$$

   Je n'aime qu'une chose, les oranges. C'est-à-dire que

   si je mange une orange, j'aime ;
   si j'aime, c'est une orange.

La plupart du temps, les définitions des concepts dans les livres de mathématiques utilisent « si » plutôt que « si et seulement si ». Par exemple, la définition d'un triangle équilatéral peut avoir la forme

(*) Un triangle est équilatéral s'il a trois côtés égaux.

Il faut traduire la définition par $\boxed{trois \equiv équi}$ et non par $trois \Rightarrow équi$, car la définition signifie

Si un triangle est équilatéral, alors il a trois côtés égaux. Si un triangle a trois côtés égaux, c'est un triangle équilatéral.

Une définition plus élégante que (*) serait

Un triangle équilatéral est un triangle qui a trois côtés égaux.

La définition la plus claire est

Un triangle est équilatéral ssi il a trois côtés égaux.

Remarque : l'usage de « si » au lieu de « si et seulement si » est une convention malheureuse, mais il faut s'y habituer. Cependant, nous éviterons de l'utiliser.

Nécessité et suffisance

Posons

sec : rester sec,
imp : porter un imperméable.

La proposition

pour rester sec, il suffit de porter un imperméable

signifie que si on porte un imperméable, on reste sec, ce qui se traduit par

$$imp \Rightarrow sec \ .$$

La proposition

pour rester sec, il est nécessaire de porter un imperméable

signifie que si on reste sec, c'est forcément qu'on porte un imperméable, ce qu'on traduit par

$$sec \Rightarrow imp \ .$$

La proposition

pour rester sec, il est nécessaire et suffisant de porter un imperméable

se traduit par

$$sec \equiv imp \ .$$

Qu'en pensez-vous ?

(2.6) Exercice. Voici quelques définitions.

1. Une personne riche est une personne qui a un million de dollars.
2. Une personne pauvre est une personne qui a un dollar.
3. Un triangle isocèle est un triangle qui a deux côtés égaux.
4. Une personne tiguedi est une personne avec un bidule de trois gugusses.

Questions :

1. Une personne qui a deux millions de dollars en banque est-elle riche ?
2. Une personne qui a mille dollars en banque est-elle riche ? Est-elle pauvre ?
3. Un triangle équilatéral est-il isocèle ?
4. Une personne avec un bidule de quatre gugusses est-elle tiguedi ?

Superman

Si Superman voulait et pouvait prévenir le mal, il le ferait. Si Superman ne pouvait prévenir le mal, il serait impuissant ; s'il ne voulait pas prévenir le mal, il serait malveillant. Superman ne prévient pas le mal. Si Superman existe, il n'est ni impuissant, ni malveillant. Par conséquent, Superman n'existe pas.

Définition des variables booléennes	
pp :	Superman peut prévenir le mal
v :	Superman veut prévenir le mal
i :	Superman est impuissant
m :	Superman est malveillant
p :	Superman prévient le mal
e :	Superman existe

Traduction des quatre premières phrases	
F_0 :	$\mathsf{pp} \wedge \mathsf{v} \Rightarrow \mathsf{p}$
F_1 :	$(\neg\mathsf{pp} \Rightarrow \mathsf{i}) \wedge (\neg\mathsf{v} \Rightarrow \mathsf{m})$
F_2 :	$\neg\mathsf{p}$
F_3 :	$\mathsf{e} \Rightarrow \neg\mathsf{i} \wedge \neg\mathsf{m}$

Le paragraphe affirme que « Superman n'existe pas » est une conséquence des quatre premières phrases :

$$F_0 \wedge F_1 \wedge F_2 \wedge F_3 \Rightarrow \neg\mathsf{e}$$

Remarque 1 : l'introduction de F_0, F_1, F_2, F_3 permet une formulation concise.
Remarque 2 : Nous apprendrons dans les chapitres suivants comment déterminer si cette expression est un théorème. Nous pourrions aussi vérifier sa validité au moyen d'une table de vérité, mais il y a $2^6 = 64$ états à vérifier.

(2.7) Exercice. Le problème de l'autobus tardif a trois hypothèses :

1. Si Bill prend l'autobus, alors il manque son rendez-vous si l'autobus est en retard.
2. Bill ne devrait pas aller à la maison s'il manque son rendez-vous et qu'il se sent déprimé.
3. Si Bill n'obtient pas l'emploi, il se sent déprimé et il ne devrait pas aller à la maison.

Le problème a huit conjectures :

4. Si Bill prend l'autobus, alors il obtient l'emploi si l'autobus est en retard.

5. Bill obtient l'emploi, s'il manque son rendez-vous et qu'il devrait aller à la maison.
6. Si l'autobus est en retard et que Bill est déprimé et qu'il s'en va à la maison, alors il ne devrait pas prendre l'autobus.
7. Bill ne prend pas l'autobus si l'autobus est en retard et que Bill n'obtient pas l'emploi.
8. Si Bill ne manque pas son rendez-vous, alors il ne devrait pas aller à la maison et il n'obtient pas l'emploi.
9. Bill se sent déprimé si l'autobus est en retard ou qu'il manque son rendez-vous.
10. Si Bill prend l'autobus et que l'autobus est en retard et qu'il s'en va à la maison, alors il obtient l'emploi.
11. Si Bill prend l'autobus mais qu'il n'obtient pas l'emploi, alors soit l'autobus est à l'heure ou il ne devrait pas aller à la maison.

Traduisez les trois hypothèses et les huit conjectures en expressions booléennes. Pour la traduction des conjectures, utilisez les variables booléennes introduites lors de la traduction des hypothèses. Donnez la formule qui exprime que la conjecture 11 est une conséquence des hypothèses.

(2.8) Exercice. Le problème de M. Centprises a cinq hypothèses :

1. Si M. Centprises a peur des grosses truites, alors il tombe à l'eau s'il pêche une grosse truite.
2. Si M. Centprises met un gros appât à son hameçon et qu'il est un bon pêcheur, alors il pêchera une grosse truite.
3. Si M. Centprises prend un bouillon, c'est parce qu'il est tombé à l'eau.
4. Si les gros appâts dégoûtent M. Centprises, alors il ne met pas de gros appât à son hameçon.
5. Si M. Centprises est un bon pêcheur, il n'est pas dégoûté par les gros appâts ou n'a pas peur des grosses truites.

Le problème a quatre conjectures :

1. Si M. Centprises n'est pas dégoûté par les gros appâts et qu'il a peur des grosses truites, alors il tombera à l'eau.
2. Si M. Centprises a peur des grosses truites et qu'il met un gros appât, alors il prendra un bouillon.
3. Si M. Centprises est un bon pêcheur et qu'il a peur des grosses truites, alors il tombera à l'eau s'il utilise de gros appâts.
4. Si M. Centprises ne pêche pas une grosse truite et qu'il utilise de gros appâts, alors il n'est pas un bon pêcheur et il n'est pas dégoûté par les gros appâts.

Traduisez les cinq hypothèses et les quatre conjectures en expressions booléennes. Pour la traduction des conjectures, utilisez les variables booléennes introduites lors de la traduction des hypothèses.

2.6 Problèmes

1. Évaluez les expressions dans les deux états E_0 et E_1 donnés.

		État E_0				État E_1			
	expression	m	n	p	q	m	n	p	q
(a)	$\neg m \wedge n$	v	f	v	v	f	v	v	v
(b)	$(m \equiv n \wedge p) \Rightarrow q$	f	v	f	v	v	v	f	f

2. Construisez la table de vérité de chacune des expressions suivantes afin de déterminer sa valeur dans tous les états. Dites si l'expression est satisfiable et si elle est valide.
   (a) $(\neg b \equiv c) \vee b$
   (b) $(p \equiv q) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
3. Traduisez les phrases suivantes en expressions booléennes.
   (a) Exactement l'une de p et q a la valeur vrai.
   (b) Aucune, deux ou quatre des variables p, q, r et s ont la valeur vrai.
4. Nommez les proposition primitives (comme $x < y$ et $x = y$) dans les phrases suivantes et traduisez ces phrases en expressions booléennes.
   (a) Aucune des expressions suivantes n'est vraie : $x < y$, $y < z$ et $v = w$.
   (b) Quand $x < y$, alors $y < z$; quand $x \geq y$, alors $v = w$.
   (c) Si l'exécution du programme P débute avec $x < y$, alors l'exécution se termine avec $y = 2^x$.

Chapitre 3

Logique propositionnelle

3.1 Préliminaires

Calcul : méthode de raisonnement au moyen de symboles.

La logique équationnelle E (calcul des propositions)

1. Un ensemble d'axiomes (par exemple, $p \vee q \equiv q \vee p$).
2. Trois règles d'inférence
   - **Leibniz :** $\dfrac{P = Q}{E[r := P] = E[r := Q]}$
   - **Transitivité :** $\dfrac{P = Q, \quad Q = R}{P = R}$
   - **Substitution :** $\dfrac{P}{P[r := Q]}$

Conventions :
- $P, Q, R, \ldots$ sont des expressions booléennes.
- $p, q, r, \ldots$ sont des variables booléennes.

Remarquez que les trois règles d'inférence ci-dessus sont simplement (1.13), (1.12) et (1.9), réécrites avec cette convention.

Un théorème, c'est

1. soit un axiome,
2. soit la conclusion d'une règle dont les prémisses sont des théorèmes,
3. soit une expression dont on démontre, en utilisant les règles d'inférence, qu'elle est égale à un axiome ou à un théorème précédemment démontré.

(3.1) Remarque. Un *axiome* est une expression dont on assume qu'elle est un théorème sans en donner la démonstration. Nous choisirons comme axiomes des expressions valides.

Il y a plusieurs manières d'axiomatiser cette logique :
- Différents choix d'axiomes.
- Différents ordres d'introduction des opérateurs :
  - Notre choix : $\equiv$ (et $=$), $\neg$ et $\not\equiv$ (et $\neq$), $\vee$, $\wedge$, $\Rightarrow$, $\Leftarrow$
  - Autre possibilité : $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\equiv$, $\not\equiv$

3.2 Équivalence et vrai

(3.2) Axiome, associativité de $\equiv$: $\big((p \equiv q) \equiv r\big) \;\equiv\; \big(p \equiv (q \equiv r)\big)$

L'associativité permet d'ajouter ou de supprimer des parenthèses. On peut écrire

$$p \equiv q \equiv r \qquad \text{ou} \qquad (p \equiv q) \equiv r \qquad \text{ou} \qquad p \equiv (q \equiv r).$$

(3.3) Axiome, commutativité (symétrie) de $\equiv$: $p \equiv q \equiv q \equiv p$

On voit mieux la commutativité avec les parenthèses : $(p \equiv q) \;\equiv\; (q \equiv p)$.

Premier théorème : $p \equiv p \equiv q \equiv q$

$$\begin{array}{ll} & p \;\equiv\; p \equiv q \equiv q \\ = & \qquad \langle \text{ Commutativité de } \equiv \text{ (3.3) —} p \equiv q \equiv q \text{ remplacé par } p \;\rangle \\ & p \equiv p \\ = & \qquad \langle \text{ Commutativité de } \equiv \text{ (3.3) —premier } p \text{ remplacé par } p \equiv q \equiv q \;\rangle \\ & p \equiv q \equiv q \;\equiv\; p \qquad \text{—Commutativité de } \equiv \text{ (3.3)} \end{array}$$

(3.4) Axiome, identité (élément neutre) de $\equiv$: $\mathsf{vrai} \equiv p \equiv p$

(3.5) Remarque. Un élément U est *l'identité* (ou *l'élément neutre*) d'une opération $\circ$ ssi $b = b \circ U = U \circ b$, quel que soit b. U est une *identité à gauche* ssi $b = U \circ b$ pour tout b. U est une *identité à droite* ssi $b = b \circ U$ pour tout b.

Par (3.3) et (3.4), $\boxed{p = (p \equiv \mathsf{vrai}) = (\mathsf{vrai} \equiv p)}$ et c'est pour cela que vrai est l'élément neutre de $\equiv$. Par exemple, montrons $p = (p \equiv \mathsf{vrai})$.

$$
\begin{array}{ll}
 & p = (p \equiv \mathsf{vrai}) \\
= & \quad \langle \text{ Remplacement de } = \text{ par } \equiv \rangle \\
 & p \equiv (p \equiv \mathsf{vrai}) \\
= & \quad \langle \text{ Commutativité de } \equiv \text{ (3.3), avec } q := p \equiv \mathsf{vrai} \rangle \\
 & (p \equiv \mathsf{vrai}) \equiv p \\
= & \quad \langle \text{ Commutativité de } \equiv \text{ (3.3), avec } q := \mathsf{vrai} \rangle \\
 & (\mathsf{vrai} \equiv p) \equiv p \\
= & \quad \langle \text{ Associativité de } \equiv \text{ (3.2) } \rangle \\
 & \mathsf{vrai} \equiv p \equiv p \qquad \text{—Identité de } \equiv \text{ (3.4)}
\end{array}
$$

À cause de (3.4), nous écrivons habituellement

$$P$$

plutôt que

$$P \equiv \mathsf{vrai}$$

ou

$$\mathsf{vrai} \equiv P$$

(3.6) Théorème : vrai

Démonstration.

$$
\begin{array}{ll}
 & \mathsf{vrai} \\
= & \quad \langle \text{ Identité de } \equiv \text{ (3.4), avec } p := \mathsf{vrai} \rangle \\
 & \mathsf{vrai} \equiv \mathsf{vrai} \\
= & \quad \langle \text{ Identité de } \equiv \text{ (3.4) —Remplacement du 2}^{\text{e}}\ \mathsf{vrai} \rangle \\
 & \mathsf{vrai} \equiv p \equiv p \qquad \text{—Identité de } \equiv \text{ (3.4)}
\end{array}
$$

(3.7) Théorème, réflexivité de $\equiv$: $p \equiv p$

(3.8) Exercice. Démontrez le théorème (3.7).

Usage des substitutions dans les transformations

Considérons la transformation suivante :

$$
\begin{array}{lll}
 & & q \equiv p \equiv (p \equiv \mathsf{vrai}) \\
\textbf{(3.9)} & = & \quad \langle \text{ Commutativité de } \equiv \text{ (3.3), avec } q := p \equiv \mathsf{vrai} \rangle \\
 & & q \equiv (p \equiv \mathsf{vrai}) \equiv p
\end{array}
$$

La transformation est justifiée au moyen du théorème (3.3), avec la substitution $q := p \equiv \mathsf{vrai}$. Même si elle n'est pas explicitement mentionnée, la règle de substitution (1.9) est utilisée. En effet, ce qui suit est une instance de la règle :

$$\frac{p \equiv q \equiv q \equiv p}{(p \equiv q \equiv q \equiv p)[q := p \equiv \mathsf{vrai}]} .$$

En faisant la substitution, on obtient

$$\frac{p \equiv q \equiv q \equiv p}{p \equiv (p \equiv \mathsf{vrai}) \;\equiv\; (p \equiv \mathsf{vrai}) \equiv p} .$$

Comme $p \equiv q \equiv q \equiv p$ est un thèorème (3.3), $p \equiv (p \equiv \mathsf{vrai}) \;\equiv\; (p \equiv \mathsf{vrai}) \equiv p$ est aussi un théorème. *C'est ce théorème, qui est généré par la règle de substitution, qui est utilisé pour justifier la transformation.*

Considérons la transformation suivante :

$$\begin{array}{ll} & E \\ = & \qquad\qquad \langle \text{ Théorème } T, \text{ avec } p := G \rangle \\ & F \end{array}$$

Puisque T est un théorème, $T[p := G]$ en est un, par la règle de substitution. C'est le théorème $T[p := G]$ qui est utilisé pour transformer E en F.

Remarquez que la substitution $p := G$ est faite dans T, pas dans E.

Revoyez l'exemple précédent et remarquez que

la substitution $q := p \equiv \mathsf{vrai}$ est faite dans le théorème (3.3), pas dans l'expression à transformer.

Usage de la règle de Leibniz dans les transformations

Reconsidérons la transformation (3.9) :

$$\begin{array}{lll} & q \equiv p \equiv (p \equiv \mathsf{vrai}) & \\ \textbf{(3.9)} \qquad = & \qquad \langle \text{ Commutativité de } \equiv \text{ (3.3), avec } q := p \equiv \mathsf{vrai} \rangle & \\ & q \equiv (p \equiv \mathsf{vrai}) \equiv p & \end{array}$$

Nous venons de voir que la justification est en fait une description du théorème

$$p \equiv (p \equiv \mathsf{vrai}) \;\equiv\; (p \equiv \mathsf{vrai}) \equiv p \; .$$

Appliquons la règle de Leibniz (1.13) avec ce théorème comme prémisse :

$$\frac{(p \equiv (p \equiv \mathsf{vrai})) \quad = \quad ((p \equiv \mathsf{vrai}) \equiv p)}{(q \equiv z)[z := p \equiv (p \equiv \mathsf{vrai})] \quad = \quad (q \equiv z)[z := (p \equiv \mathsf{vrai}) \equiv p]}$$

Puisque la prémisse est un théorème, la conclusion est un théorème. En effectuant les substitutions dans la conclusion, on obtient la transformation (3.9).

- La règle de substitution et la règle de Leibniz sont utilisées presque partout. Pour cette raison, elles ne sont normalement pas mentionnées.
- La règle de Leibniz peut sembler complexe, mais elle dit simplement que si $X = Y$, on peut utiliser Y partout où X est utilisée et vice versa. C'est le principe du remplacement d'une expression par une expression égale. Vous avez utilisé cette règle depuis le secondaire sans le savoir.

Après tous ces commentaires sur la présentation des preuves, vous devriez revoir celles qui ont déjà été présentées dans ce chapitre.

(3.10) Exercice. Dites quelle règle de substitution et quelle règle de Leibniz sont utilisées dans la transformation suivante (c'est-à-dire, précisez les valeurs de E, F, X, Y, v, z utilisées dans (1.9) et (1.13)).

$$\begin{array}{ll} & (x+1)^2 - 1 \\ = & \qquad \langle \text{ Théorème } (x+y)^2 = x^2 + 2 \cdot x \cdot y + y^2, \text{ avec } y := 1 \rangle \\ & x^2 + 2 \cdot x \cdot 1 + 1^2 - 1 \end{array}$$

Recommandations utiles

- Ne tentez pas d'évaluer les expressions booléennes à démontrer. Lorsque nous sortirons du contexte restreint de la logique des propositions, il ne sera plus possible de construire des tables de vérité. Il faut s'habituer à dériver des théorèmes sans se préoccuper de leur signification.
- Il y a beaucoup de théorèmes. Vous n'avez pas à les mémoriser. Il suffit d'être familier avec leur utilisation et leur organisation, de manière à trouver ceux qu'il faut pour compléter une preuve.
- Le développement d'une preuve élégante peut demander plusieurs itérations, surtout pour les preuves difficiles. Il ne faut pas se contenter du premier jet. Pratique, pratique, ...

On peut montrer que

- Tous les axiomes déjà présentés et ceux qui viendront sont valides (on peut le vérifier au moyen des tables de vérité).
- Tous les théorèmes sont valides.
- Toutes les expressions valides sont des théorèmes (c'est-à-dire qu'elles peuvent être démontrées).

3.3 Négation, inéquivalence et faux

(3.11) Axiome, définition de faux : $\mathsf{faux} \equiv \neg\mathsf{vrai}$

(3.12) Axiome, distributivité de $\neg$ sur $\equiv$: $\neg(p \equiv q) \;\equiv\; \neg p \equiv q$

Les deux axiomes précédents définissent la négation.

(3.13) Axiome, définition de $\not\equiv$: $(p \not\equiv q) \;\equiv\; \neg(p \equiv q)$

Théorèmes reliant $\equiv, \not\equiv, \neg$ et faux

(3.14) $\neg p \equiv q \;\equiv\; p \equiv \neg q$

(3.15) Double négation : $\neg\neg p \equiv p$

(3.16) Négation de faux : $\neg\mathsf{faux} \equiv \mathsf{vrai}$

(3.17) $(p \not\equiv q) \;\equiv\; \neg p \equiv q$

(3.18) $\neg p \equiv p \equiv \mathsf{faux}$

(3.19) Commutativité (symétrie) de $\not\equiv$: $(p \not\equiv q) \;\equiv\; (q \not\equiv p)$

(3.20) Associativité de $\not\equiv$: $\big((p \not\equiv q) \not\equiv r\big) \;\equiv\; \big(p \not\equiv (q \not\equiv r)\big)$

(3.21) Associativité mutuelle : $\big((p \not\equiv q) \equiv r\big) \;\equiv\; \big(p \not\equiv (q \equiv r)\big)$

(3.22) Interchangeabilité mutuelle : $p \not\equiv q \equiv r \;\equiv\; p \equiv q \not\equiv r$

La double négation (3.15) affirme que la négation est son propre inverse (note : on dit qu'une fonction g est l'*inverse* d'une fonction f si $g(f.x) = x$ pour tout x).

L'associativité mutuelle (3.21) permet d'éliminer des parenthèses, ce qui est exploité en (3.22).

Autre méthode pour prouver $P \equiv Q$

Avant d'introduire cette méthode de manière générale, voici un exemple. Démontrons le théorème (3.14).

$$
\begin{array}{ll}
 & \neg p \equiv q \\
= & \qquad \langle \text{ Distributivité de } \neg \text{ sur } \equiv (3.12) \rangle \\
 & \neg(p \equiv q) \\
= & \qquad \langle \text{ Commutativité de } \equiv (3.3) \rangle \\
 & \neg(q \equiv p) \\
= & \qquad \langle \text{ Distributivité de } \neg \text{ sur } \equiv (3.12), \text{ avec } p, q := q, p \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & \neg q \equiv p \\
= & \qquad \langle \text{ Commutativité de } \equiv \text{ (3.3), avec } p, q := \neg q, p \rangle \\
 & p \equiv \neg q
\end{array}
$$

Nous avons montré que $\neg p \equiv q$ est égal à (équivalent à) $p \equiv \neg q$. Intuitivement, nous avons donc démontré $\neg p \equiv q \equiv p \equiv \neg q$ (c'est l'expression (3.14)). Cependant, selon la définition de théorème (page 27), nous aurions dû montrer que l'expression (3.14) est égale à un théorème pour démontrer qu'elle est elle-même un théorème.

La preuve précédente peut être transformée dans le format standard (les noms de lois sont omis pour cette comparaison) :

nouvelle méthode

$$
\begin{array}{ll}
 & \neg p \equiv q \\
= & \qquad \langle \text{ (3.12) } \rangle \\
 & \neg(p \equiv q) \\
= & \qquad \langle \text{ (3.3) } \rangle \\
 & \neg(q \equiv p) \\
= & \qquad \langle \text{ (3.12), avec } p, q := q, p \rangle \\
 & \neg q \equiv p \\
= & \qquad \langle \text{ (3.3), avec } p, q := \neg q, p \rangle \\
 & p \equiv \neg q
\end{array}
$$

méthode standard

$$
\begin{array}{ll}
 & \neg p \equiv q \equiv p \equiv \neg q \\
= & \qquad \langle \text{ (3.12) } \rangle \\
 & \neg(p \equiv q) \equiv p \equiv \neg q \\
= & \qquad \langle \text{ (3.3) } \rangle \\
 & \neg(q \equiv p) \equiv p \equiv \neg q \\
= & \qquad \langle \text{ (3.12), avec } p, q := q, p \rangle \\
 & \neg q \equiv p \equiv p \equiv \neg q \\
= & \qquad \langle \text{ (3.3), avec } p, q := \neg q, p \rangle \\
 & p \equiv \neg q \equiv p \equiv \neg q \\
= & \qquad \langle \text{ (3.4), avec } p := p \equiv \neg q \rangle \\
 & \mathsf{vrai} \qquad \text{—(3.6)}
\end{array}
$$

Autre méthode pour prouver $P \equiv Q$ (suite et fin)

nouvelle méthode — transformable en — méthode standard

$$
\begin{array}{ll}
 & P \\
= & \quad \langle \text{ Indice } 0 \rangle \\
 & R \\
= & \quad \langle \text{ Indice } 1 \rangle \\
 & \vdots \\
= & \quad \langle \text{ Indice } n \rangle \\
 & Q
\end{array}
\quad \rightsquigarrow \quad
\begin{array}{ll}
 & P \equiv Q \\
= & \quad \langle \text{ Indice } 0 \rangle \\
 & R \equiv Q \\
= & \quad \langle \text{ Indice } 1 \rangle \\
 & \vdots \quad \vdots \quad \vdots \\
= & \quad \langle \text{ Indice } n \rangle \\
 & Q \equiv Q \\
= & \quad \langle \text{ Identité de } \equiv (3.4) \rangle \\
 & \mathsf{vrai} \qquad \text{—}(3.6)
\end{array}
$$

(3.23) Méthode de démonstration : Pour montrer que $P \equiv Q$ est un théorème, transformer P en Q ou Q en P en utilisant la règle de Leibniz.

Heuristique pour la découverte des preuves

Heuristique : qui aide à la découverte. Une méthode heuristique est une méthode raisonnable, mais qui ne donne pas forcément les résultats escomptés. En informatique, on dit souvent *une heuristique* plutôt qu'*une méthode heuristique*.

(3.24) Heuristique. Identifiez les théorèmes applicables en cherchant ceux qui ont des expressions ou sous-expressions similaires à celles de la loi à démontrer. Les opérateurs qui apparaissent dans une expression booléenne et la forme de ses sous-expressions restreignent le choix des théorèmes qui peuvent être utilisés pour la manipuler.

(3.25) Exemple. Reprenons la preuve du théorème (3.14), $\neg p \equiv q \equiv p \equiv \neg q$.

Attention : : nous ne pouvons utiliser que les théorèmes qui précèdent (3.14).

- (3.2) ne correspond pas du tout à (3.14).
- (3.3) permet de permuter les opérandes ; pas très utile.
- (3.4) permet seulement d'ajouter vrai.
- (3.6) est inutile.
- (3.7) permet seulement de remplacer une expression par elle-même.
- (3.11) et (3.13) ne correspondent pas du tout.
- (3.12) a un côté droit intéressant : $\neg p \equiv q$, qui apparaît dans (3.14).

Ceci donne la première transformation. La dernière ligne de la preuve est connue, c'est $p \equiv \neg q$. On voit qu'il faut trouver un moyen d'amener $\neg$ sur q, mais après la première

transformation, p et q ne sont pas à la bonne place pour pouvoir réutiliser (3.12) à cette fin. Ceci fait penser à l'usage de la commutativité de $\equiv$. Le reste est facile.

$$
\begin{array}{ll}
 & \neg p \equiv q \\
= & \quad \langle \text{ Distributivité de } \neg \text{ sur } \equiv (3.12) \rangle \\
 & \neg(p \equiv q) \\
= & \quad \langle \text{ Commutativité de } \equiv (3.3) \rangle \\
 & \neg(q \equiv p) \\
= & \quad \langle \text{ Distributivité de } \neg \text{ sur } \equiv (3.12), \text{ avec } p, q := q, p \rangle \\
 & \neg q \equiv p \\
= & \quad \langle \text{ Commutativité de } \equiv (3.3), \text{ avec } p, q := \neg q, p \rangle \\
 & p \equiv \neg q
\end{array}
$$

(3.26) Remarque.

1. Il est souvent plus facile de progresser « par les deux bouts », c'est-à-dire en faisant quelques transformations à partir de la première ligne et quelques autres à partir de la dernière. Il suffit ensuite de compléter le milieu. .
2. Il y a souvent plusieurs preuves possibles. C'est en explorant plusieurs preuves qu'on peut trouver la plus élégante.

Principe de structuration des preuves

(3.27) Principe. Structurez les preuves pour éviter de répéter la même sous-expression sur plusieurs lignes.

(3.28) Exemple. La preuve de gauche est plus courte (en terme de lignes), mais elle répète « $\equiv$ faux » à chaque ligne. La preuve de droite est préférable. C'est la preuve de (3.18).

$$
\begin{array}{ll}
 & \neg p \equiv p \equiv \mathsf{faux} \\
= & \quad \langle \text{ distributivité de } \neg \text{ sur } \equiv \\
 & \quad (3.12), \text{ avec } q := p \rangle \\
 & \neg(p \equiv p) \equiv \mathsf{faux} \\
= & \quad \langle \text{ Identité de } \equiv (3.4) \rangle \\
 & \neg \mathsf{vrai} \equiv \mathsf{faux} \qquad \text{—Définition de faux (3.11)}
\end{array}
$$

$$
\begin{array}{ll}
 & \neg p \equiv p \\
= & \quad \langle \text{ distributivité de } \neg \text{ sur } \equiv \\
 & \quad (3.12), \text{ avec } q := p \rangle \\
 & \neg(p \equiv p) \\
= & \quad \langle \text{ Identité de } \equiv (3.4) \rangle \\
 & \neg \mathsf{vrai} \\
= & \quad \langle \text{ Définition de faux (3.11)} \rangle \\
 & \mathsf{faux}
\end{array}
$$

Heuristique : élimination des définitions

(3.29) Heuristique d'élimination des définitions. Pour démontrer un théorème qui contient un opérateur $\circ$ défini en termes d'un autre opérateur, disons $\bullet$, faites l'expansion de la définition de $\circ$ pour obtenir une formule contenant $\bullet$; ensuite, exploitez les propriétés de $\bullet$ pour manipuler la formule ; finalement, réintroduisez $\circ$ en utilisant sa définition, si applicable.

(3.30) Exemple. Démontrons (3.19), $(p \not\equiv q) \equiv (q \not\equiv p)$. Ici, $\circ$ est $\not\equiv$ et $\bullet$ est $\equiv$.

$$
\begin{array}{ll}
& p \not\equiv q \\
= & \quad \langle \text{ Définition de } \not\equiv \text{ (3.13) } \rangle \\
& \neg(p \equiv q) \\
= & \quad \langle \text{ Commutativité de } \equiv \text{ (3.3) } \rangle \\
& \neg(q \equiv p) \\
= & \quad \langle \text{ Définition de } \not\equiv \text{ (3.13), avec } p, q := q, p \rangle \\
& q \not\equiv p
\end{array}
$$

(3.31) Exercice. Démontrez l'associativité de $\not\equiv$ (3.20) en utilisant l'heuristique d'élimination des définitions (3.29) —éliminez $\not\equiv$, puis utilisez une propriété de $\equiv$, et finalement réintroduisez $\not\equiv$.

Mention de l'associativité et de la commutativité

Les lois d'associativité et de commutativité sont très simples. À partir d'ici, elles seront fréquemment utilisées sans mention. Ce qui doit guider la décision de mentionner ou non les usages de l'associativité et de la commutativité, c'est l'objectif d'avoir une preuve facile à lire.

Dans les examens, vous n'aurez pas à mentionner les usages de l'associativité et de la commutativité, à moins que cela ne soit explicitement requis.

3.4 Disjonction

La disjonction est définie par les cinq axiomes suivants.

(3.32) Axiome, commutativité (symétrie) de $\vee$: $p \vee q \equiv q \vee p$

(3.33) Axiome, associativité de $\vee$: $(p \vee q) \vee r \equiv p \vee (q \vee r)$

(3.34) Axiome, idempotence de $\vee$: $p \vee p \equiv p$

(3.35) Remarque. On dit qu'un opérateur $\circ$ est *idempotent* ssi $x \circ x = x$ pour tout x. La multiplication $\cdot$ et l'addition $+$ d'entiers ne sont pas idempotentes, mais $\vee$ et $\wedge$ le sont.

(3.36) Axiome, distributivité de $\vee$ sur $\equiv$: $p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$

(3.37) Axiome, tiers exclu : $p \vee \neg p$ ou encore $p \vee \neg p \equiv \mathsf{vrai}$

La loi du tiers exclu signifie que p est vrai ou que $\neg p$ est vrai. Cela vient du fait qu'il n'y a que deux valeurs de vérité, vrai et faux.

Théorèmes sur $\vee$

(3.38) Zéro de $\vee$: $p \vee \mathsf{vrai} \equiv \mathsf{vrai}$

(3.39) Remarque. Z est un *zéro* d'une opération binaire $\circ$ ssi $x \circ Z = Z \circ x = Z$, pour tout x. Z est un *zéro à gauche* ssi $x \circ Z = Z$, pour tout x. Z est un *zéro à droite* ssi $Z \circ x = Z$, pour tout x. Le terme *zéro* est utilisé parce que 0 est un zéro de $\cdot$.

(3.40) Identité (élément neutre) de $\vee$: $p \vee \mathsf{faux} \equiv p$

(3.41) Distributivité de $\vee$ sur $\vee$: $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$

(3.42) $p \vee q \equiv p \vee \neg q \equiv p$

Heuristique : du plus structuré au moins structuré

(3.43) Heuristique : Pour démontrer $P \equiv Q$, transformez l'expression la plus structurée (soit P, soit Q) en l'autre expression.

(3.44) Exemple. Preuve du théorème (3.38), $p \vee \mathsf{vrai} \equiv \mathsf{vrai}$.

$p \vee \mathsf{vrai}$
$=$ ⟨ Identité de $\equiv$ (3.4) ⟩
$p \vee (p \equiv p)$
$=$ ⟨ Distributivité de $\vee$ sur $\equiv$ (3.36), avec $q, r := p, p$ ⟩
$p \vee p \equiv p \vee p$
$=$ ⟨ Identité de $\equiv$ (3.4), avec $p := p \vee p$ ⟩
vrai

vrai
$=$ ⟨ Identité de $\equiv$ (3.4), avec $p := p \vee p$ ⟩
$p \vee p \equiv p \vee p$
$=$ ⟨ Distributivité de $\vee$ sur $\equiv$ (3.36), avec $q, r := p, p$ ⟩
$p \vee (p \equiv p)$
$=$ ⟨ Identité de $\equiv$ (3.4) ⟩
$p \vee \mathsf{vrai}$

À gauche, seuls (3.32) à (3.36) peuvent s'appliquer, ce qui suggère d'introduire $\equiv$. À droite, l'expression vrai peut être transformée de plusieurs manières.

Principe de structuration des preuves

(3.45) Principe. Structurez les preuves de manière à minimiser les surprises (les lapins sortis d'un chapeau) —chaque étape devrait sembler évidente, en considérant la structure des expressions et le but de la manipulation.

(3.46) Exercice. Démontrez le théorème (3.42), $p \vee q \equiv p \vee \neg q \equiv p$. Notez que le patron $p \vee q \equiv p \vee \neg q$ correspond au côté droit de l'axiome de distributivité (3.36), avec $r := \neg q$; considérez donc la transformation de $p \vee q \equiv p \vee \neg q$ en p.

3.5 Conjonction

La conjonction est définie par l'axiome suivant.

(3.47) Axiome, De Morgan : $p \wedge q \equiv \neg(\neg p \vee \neg q)$

(3.48) De Morgan, formes alternatives :
(a) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
(b) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
(c) $p \vee q \equiv \neg(\neg p \wedge \neg q)$

Attention : On dit « loi de De Morgan » et non pas « loi de Morgan ». Ce mathématicien s'appelait Augustus De Morgan.

Propriétés élémentaires de $\wedge$

Les théorèmes suivants découlent des lois de De Morgan (3.47) et (3.48).

(3.49) Commutativité (symétrie) de $\wedge$: $p \wedge q \equiv q \wedge p$

(3.50) Associativité de $\wedge$: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

(3.51) Idempotence de $\wedge$: $p \wedge p \equiv p$

(3.52) Identité de $\wedge$: $p \wedge \mathsf{vrai} \equiv p$

(3.53) Zéro de $\wedge$: $p \wedge \mathsf{faux} \equiv \mathsf{faux}$

(3.54) Distributivité de $\wedge$ sur $\wedge$: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$

(3.55) Contradiction : $p \wedge \neg p \equiv \mathsf{faux}$

(3.56) Exercice. Démontrez le théorème (3.49), c'est-à-dire $p \wedge q \equiv q \wedge p$.

Théorèmes reliant $\wedge$ et $\vee$

(3.57) Règle d'or : $p \wedge q \equiv p \equiv q \equiv p \vee q$

Il y a plusieurs manières de lire la règle d'or. En voici deux :

1. $(p \wedge q) \equiv (p \equiv q \equiv p \vee q)$: c'est alors une définition de $\wedge$. C'est ainsi que le manuel de Gries et Schneider [4] introduit la conjonction. Nous avons utilisé une loi de De Morgan (3.47) à cette fin.

2. $(p \equiv q) \equiv (p \wedge q \equiv p \vee q)$: cette lecture indique que p est équivalent à q ssi la conjonction et la disjonction de p et q sont équivalentes.

Truc pour se rappeler de la règle : elle contient $\boxed{p,\ q,\ p \vee q,\ p \wedge q}$. L'ordre est arbitraire, car $\equiv$ est commutative.

Ce théorème est assez complexe. C'est une bonne idée de faire sa table de vérité pour se convaincre de sa validité.

(3.58) Exercice. Démontrez la règle d'or (3.57), c'est-à-dire $p \wedge q \equiv p \equiv q \equiv p \vee q$.

(3.59) Distributivité de $\vee$ sur $\wedge$: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(3.60) Distributivité de $\wedge$ sur $\vee$: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(3.61) Absorption :
(a) $p \wedge (p \vee q) \equiv p$
(b) $p \vee (p \wedge q) \equiv p$
(c) $p \wedge (\neg p \vee q) \equiv p \wedge q$
(d) $p \vee (\neg p \wedge q) \equiv p \vee q$

On parle d'*absorption* parce que la sous-expression q est absorbée par p dans les cas (a) et (b), et parce que $\neg p$ est absorbée et disparaît dans les cas (c) et (d).

Théorèmes reliant $\wedge$ et $\equiv$

(3.62) $p \wedge q \equiv p \wedge \neg q \equiv \neg p$

Ce théorème est similaire au théorème (3.42), $p \vee q \equiv p \vee \neg q \equiv p$.

(3.63) $p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$

Comparez ce théorème avec l'axiome de distributivité de $\vee$ sur $\equiv$ (3.36),

$$p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r.$$

Pour la conjonction, la distributivité ne tient donc pas.

(3.64) $p \wedge (p \equiv q) \equiv p \wedge q$

(3.65) Remplacement : $(p \equiv q) \wedge (r \equiv p) \;\equiv\; (p \equiv q) \wedge (r \equiv q)$

Définitions alternatives de $\equiv$ et $\not\equiv$

(3.66) Définition de $\equiv$: $p \equiv q \;\equiv\; (p \wedge q) \vee (\neg p \wedge \neg q)$

(3.67) Ou exclusif : $p \not\equiv q \;\equiv\; (\neg p \wedge q) \vee (p \wedge \neg q)$

Plusieurs auteurs utilisent ces théorèmes pour définir $\equiv$ et $\not\equiv$. Selon (3.66), $p \equiv q$ est vrai lorsque p et q sont toutes deux vrai ou toutes deux faux. Selon (3.67), $p \not\equiv q$ est vrai lorsque p et q ont des valeurs différentes.

Suites d'équivalences

La suite d'équivalences

(3.68) $P_0 \equiv P_1 \equiv \ldots \equiv P_n$

est égale à vrai si, et seulement si, il y a nombre pair de P_i qui sont faux. En effet, parce que vrai est l'identité de $\equiv$ (3.4), chaque sous-expression faux $\equiv$ faux peut être remplacée par vrai, jusqu'à ce qu'il ne reste qu'une occurrence de faux, auquel cas la valeur de la séquence est faux, ou aucune occurrence, auquel cas la valeur de la séquence est vrai. Par exemple,

$$(\text{faux} \equiv \text{faux} \equiv \text{faux} \equiv \text{vrai}) \;\equiv\; \text{faux}.$$

Cette remarque permet les formalisations suivantes :

p et q sont tous deux vrai ou tous deux faux : $p \equiv q$
Exactement l'un de p et q est vrai : $\neg(p \equiv q)$ ou $p \not\equiv q$
Zéro, deux ou quatre de p, q, r et s sont vrai : $p \equiv q \equiv r \equiv s$
Un ou trois de p, q, r et s sont vrai : $\neg(p \equiv q \equiv r \equiv s)$

Revoyez le problème 3 du chapitre 2. Vous constaterez qu'il est possible de lui donner une solution beaucoup plus simple en utilisant le truc ci-dessus.

Structuration de preuves au moyen de lemmes

Un *lemme* est un théorème de moindre importance utilisé dans la preuve d'un théorème auquel on s'intéresse davantage. Il n'est pas toujours clair si une loi doit être appelée un lemme ou un théorème.

(3.69) Principe. Les lemmes aident à structurer les preuves et peuvent même contribuer à réduire leur longueur. Ils peuvent aussi révéler des faits intéressants.

(3.70) Exemple. Preuve de l'associativité de $\wedge$ (3.50), $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

Commençons avec la transformation du côté gauche de l'équivalence. La seule loi applicable est la règle d'or (3.57) ; notez que ceci constitue une application de l'heuristique d'élimination des définitions (3.29).

Remarque : faute d'espace (c'est petit, un transparent), les substitutions ne sont pas toutes indiquées.

$$
\begin{array}{ll}
 & (p \wedge q) \wedge r \\
= & \qquad \langle \text{ Règle d'or (3.57) } \rangle \\
 & (p \equiv q \equiv p \vee q) \wedge r \\
= & \qquad \langle \text{ Règle d'or (3.57), avec } p, q := (p \equiv q \equiv p \vee q),\ r \ \rangle \\
 & p \equiv q \equiv p \vee q \ \equiv \ r \ \equiv \ (p \equiv q \equiv p \vee q) \vee r \\
= & \qquad \langle \text{ Distributivité de } \vee \text{ sur } \equiv \text{ (3.36), deux fois (le dernier } r \text{ est distribué sur} \\
 & \qquad \text{la formule entre parenthèses qui le précède) } \rangle \\
 & p \equiv q \equiv p \vee q \equiv r \equiv p \vee r \equiv q \vee r \equiv p \vee q \vee r \\
= & \qquad \langle \text{ Commutativité et associativité de } \equiv \text{ et } \vee \ \rangle \\
 & p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r
\end{array}
$$

Nous avons donc montré

(3.71) $(p \wedge q) \wedge r \quad \equiv \quad p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r.$

Ce résultat indique que $(p \wedge q) \wedge r$ est équivalent à l'équivalence de toutes les disjonctions non vides possibles de p, q et r. C'est un résultat suffisamment intéressant en soi pour le mettre en évidence comme dans l'équation ci-dessus (ce qui permet d'y référer ailleurs).

Complétons la démonstration :

$$
\begin{array}{ll}
 & p \wedge (q \wedge r) \\
= & \qquad \langle \text{ Commutativité de } \wedge \text{ (3.49) } \rangle \\
 & (q \wedge r) \wedge p \\
= & \qquad \langle \text{ (3.71), avec } p, q, r := q, r, p \ \rangle \\
 & q \equiv r \equiv p \equiv q \vee r \equiv r \vee p \equiv p \vee q \equiv q \vee r \vee p \\
= & \qquad \langle \text{ Commutativité de } \equiv \text{ et } \vee \ \rangle \\
 & p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r \\
= & \qquad \langle \text{ (3.71) } \rangle \\
 & (p \wedge q) \wedge r
\end{array}
$$

Notez que le lemme (3.71) est utilisé deux fois.

Utilisation de la règle d'or

La règle d'or (3.57) est $\boxed{p \wedge q \;\equiv\; p \;\equiv\; q \;\equiv\; p \vee q.}$ Elle contient quatre termes reliés par des équivalences. Elle peut être utilisée de plusieurs façons, selon la manière de regrouper les termes. Voici deux exemples.

1. Remplacement d'un terme par les trois autres :

$$\begin{array}{ll} & \underline{p \wedge (\neg p \vee q)} \\ = & \qquad\qquad \langle \text{ Règle d'or, avec } q := \neg p \vee q \rangle \\ & \underline{p} \;\equiv\; \underline{\neg p \vee q} \;\equiv\; \underline{p \vee \neg p \vee q} \end{array}$$

2. Remplacement des deux premiers termes par les deux autres :

$$\begin{array}{ll} & \underline{p \wedge (q \equiv r)} \;\equiv\; \underline{p} \\ = & \qquad\qquad \langle \text{ Règle d'or, avec } q := q \equiv r \rangle \\ & \underline{p \vee (q \equiv r)} \;\equiv\; \underline{q \equiv r} \end{array}$$

(3.72) Heuristique. Exploitez la possibilité de faire des regroupements différents dans des théorèmes comme la règle d'or.

3.6 Implication

(3.73) Axiome, définition de $\Rightarrow$: $p \Rightarrow q \;\equiv\; p \vee q \;\equiv\; q$

(3.74) Axiome, conséquence : $p \Leftarrow q \;\equiv\; q \Rightarrow p$

À cause de la similarité de $\Rightarrow$ et $\Leftarrow$, nous donnons par la suite seulement les théorèmes qui concernent $\Rightarrow$. On en dérive facilement des théorèmes pour $\Leftarrow$ en utilisant (3.74).

L'implication peut être définie de plusieurs manières. Les théorèmes (3.75) et (3.76) ci-dessous sont parfois utilisés comme définition de l'implication.

(3.75) Définition alternative de $\Rightarrow$: $p \Rightarrow q \;\equiv\; \neg p \vee q$

(3.76) Définition alternative de $\Rightarrow$: $p \Rightarrow q \;\equiv\; p \wedge q \;\equiv\; p$

(3.77) Contrapositivité : $p \Rightarrow q \;\equiv\; \neg q \Rightarrow \neg p$

Divers théorèmes sur l'implication

(3.78) $p \Rightarrow (q \equiv r) \;\equiv\; p \wedge q \;\equiv\; p \wedge r$

(3.79) Distributivité de $\Rightarrow$ sur $\equiv$: $p \Rightarrow (q \equiv r) \;\equiv\; p \Rightarrow q \;\equiv\; p \Rightarrow r$

(3.80) $p \Rightarrow (q \Rightarrow r) \;\equiv\; (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$

(3.81) Transfert : $p \wedge q \;\Rightarrow\; r \;\equiv\; p \Rightarrow (q \Rightarrow r)$

(3.82) $p \wedge (p \Rightarrow q) \;\equiv\; p \wedge q$

(3.83) $p \wedge (q \Rightarrow p) \;\equiv\; p$

(3.84) $p \vee (p \Rightarrow q) \;\equiv\; \mathsf{vrai}$

(3.85) $p \vee (q \Rightarrow p) \equiv q \Rightarrow p$

(3.86) $p \vee q \;\Rightarrow\; p \wedge q \;\equiv\; p \equiv q$

Les théorèmes (3.78) et (3.79) montrent comment éliminer $\equiv$ du conséquent d'une implication, alors que (3.81) permet de transférer un facteur d'une conjonction de l'antécédent au conséquent d'une implication (*très utile*).

Implication et constantes booléennes

(3.87) Réflexivité de $\Rightarrow$: $p \Rightarrow p \;\equiv\; \mathsf{vrai}$ ou encore $p \Rightarrow p$

(3.88) Zéro à droite de $\Rightarrow$: $p \Rightarrow \mathsf{vrai} \;\equiv\; \mathsf{vrai}$ ou encore $p \Rightarrow \mathsf{vrai}$

(3.89) Identité à gauche de $\Rightarrow$: $\mathsf{vrai} \Rightarrow p \;\equiv\; p$

(3.90) $p \Rightarrow \mathsf{faux} \;\equiv\; \neg p$

(3.91) $\mathsf{faux} \Rightarrow p \;\equiv\; \mathsf{vrai}$ ou encore $\mathsf{faux} \Rightarrow p$

On peut voir que les deux formulations de trois des théorèmes sont équivalentes en utilisant le fait que vrai est l'élément neutre de $\equiv$ (3.4).

Les théorèmes (3.88) et (3.89) montrent que l'implication n'est pas symétrique (commutative) ; c'est pourquoi un symbole non symétrique ($\Rightarrow$) la représente.

Affaiblissement, renforcement et Modus ponens

(3.92) Affaiblissement, renforcement :

(a) $p \;\Rightarrow\; p \vee q$
(b) $p \wedge q \;\Rightarrow\; p$
(c) $p \wedge q \;\Rightarrow\; p \vee q$
(d) $p \vee (q \wedge r) \;\Rightarrow\; p \vee q$
(e) $p \wedge q \;\Rightarrow\; p \wedge (q \vee r)$

Quand on utilise (3.92) pour remplacer l'antécédent par le conséquent, on parle d'*affaiblissement* ; quand on remplace le conséquent par l'antécédent, on parle de *renforcement*.

(3.93) Modus ponens : $p \wedge (p \Rightarrow q) \;\Rightarrow\; q$

La loi (3.93) est très utile et joue un rôle fondamental dans certaines présentations de la logique propositionnelle.

Formes d'analyse par cas

(3.94) $(p \Rightarrow r) \wedge (q \Rightarrow r) \;\equiv\; (p \vee q \;\Rightarrow\; r)$

(3.95) $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \;\equiv\; r$

Nous expliquerons plus tard comment ces deux lois peuvent être utilisées pour faire des *preuves par cas*.

(3.96) Exercice. Démontrez le théorème (3.94), c'est-à-dire

$$(p \Rightarrow r) \wedge (q \Rightarrow r) \;\equiv\; (p \vee q \;\Rightarrow\; r).$$

Implication mutuelle et transitivité

(3.97) Implication mutuelle : $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\equiv\; p \equiv q$

Cette loi est souvent prise comme définition de $\equiv$, ce qui lui donne alors un rôle moins important que celui de $\Rightarrow$. Notre approche consiste à considérer $\equiv$ comme un opérateur primordial (c'est pour cela qu'on parle de logique équationnelle).

(3.98) Antisymétrie : $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\Rightarrow\; (p \equiv q)$

On dit qu'une relation $\circ$ est *antisymétrique* si $x \circ y \wedge y \circ x \;\Rightarrow\; x = y$, quels que soient x et y. Par exemple, $\leq$ et $\geq$ sur les entiers et les réels sont antisymétriques.

Cette loi est une simple conséquence du théorème (3.97). On dit que c'est un *corollaire* du théorème (3.97).

(3.99) Transitivité :
(a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

Au chapitre 4, ces lois serviront à introduire une nouvelle variante du format de preuve.

(3.100) Métathéorème : Deux théorèmes quelconques sont équivalents.

Un *métathéorème* est une propriété de la logique qui ne peut s'exprimer au moyen de la logique (ici, la logique propositionnelle). Pour énoncer le métathéorème précédent au moyen de la logique, il faudrait que celle-ci permette entre autres de décrire la notion de *séquence d'expressions*, puisqu'un théorème est la dernière expression d'une séquence d'expressions qui sont des théorèmes.

(3.101) Exemple. Montrons le théorème de transitivité (3.99c).

$$
\begin{array}{ll}
 & (p \Rightarrow q) \wedge (q \equiv r) \;\Rightarrow\; (p \Rightarrow r) \\
= & \qquad \langle \text{ Implication mutuelle (3.97), avec } p, q \;:=\; q, r \;\rangle \\
 & (p \Rightarrow q) \wedge (q \Rightarrow r) \wedge (r \Rightarrow q) \;\Rightarrow\; (p \Rightarrow r) \\
= & \qquad \langle \text{ Transfert (3.81), avec } p, q, r \;:=\; r \Rightarrow q,\; (p \Rightarrow q) \wedge (q \Rightarrow r),\; p \Rightarrow r \\
 & \qquad \&\;\text{ Commutativité de } \wedge \text{ (3.49)} \;\rangle \\
 & (r \Rightarrow q) \;\Rightarrow\; \big((p \Rightarrow q) \wedge (q \Rightarrow r) \;\Rightarrow\; (p \Rightarrow r)\big) \\
= & \qquad \langle \text{ Transitivité (3.99a) } \&\; \mathsf{vrai} \text{ est un théorème (3.6) } \& \\
 & \qquad \text{Métathéorème (3.100)} \;\rangle \\
 & (r \Rightarrow q) \Rightarrow \mathsf{vrai} \qquad \text{—Zéro à droite de } \Rightarrow \text{ (3.88), avec } p \;:=\; r \Rightarrow q
\end{array}
$$

Remarque : ceci peut se prouver sans faire appel au métathéorème (3.100).

Voici une preuve qui n'utilise pas le métathéorème.

$$
\begin{array}{ll}
 & (p \Rightarrow q) \wedge (q \equiv r) \;\Rightarrow\; (p \Rightarrow r) \\
= & \qquad \langle \text{ Transfert (3.81), avec } p, q \;:=\; (p \Rightarrow q) \wedge (q \equiv r),\; p \;\rangle \\
 & (p \Rightarrow q) \wedge (q \equiv r) \wedge p \;\Rightarrow\; r \\
= & \qquad \langle \text{ (3.82) } \&\; \text{Commutativité de } \wedge \text{ (3.49)} \;\rangle \\
 & p \wedge q \wedge (q \equiv r) \;\Rightarrow\; r \\
= & \qquad \langle \text{ (3.64), avec } p, q \;:=\; q, r \;\rangle \\
 & p \wedge q \wedge r \;\Rightarrow\; r \qquad \text{— Affaiblissement (3.92b), avec } p, q \;:=\; r,\; p \wedge q \\
 & \qquad\qquad\qquad\qquad \text{Commutativité de } \wedge \text{ (3.49) } \&
\end{array}
$$

Démonstration de théorèmes concernant l'implication

L'heuristique d'élimination des définitions (3.29) peut aussi être appliquée à l'implication. Notez qu'on peut utiliser l'axiome (3.73) ainsi que les théorèmes (3.75) et (3.76) pour éliminer l'implication. Par exemple, voici la preuve de (3.78) :

$$
\begin{array}{ll}
 & p \;\Rightarrow\; (q \equiv r) \\
= & \qquad \langle \text{ Définition de l'implication (3.76), avec } q \;:=\; q \equiv r \;\rangle \\
 & p \wedge (q \equiv r) \;\equiv\; p \\
= & \qquad \langle \text{ (3.63) } \rangle \\
 & p \wedge q \;\equiv\; p \wedge r
\end{array}
$$

(3.102) Remarque. Ce chapitre contient un grand nombre de théorèmes. À la première lecture, essayez de comprendre ce que signifie chacun d'eux et essayez de vous convaincre que c'est un théorème. Ce ne sera évidemment pas possible pour tous, car certains sont assez complexes. Faites ensuite des exercices pour pratiquer leur usage. En faisant des exercices, vous devriez développer une plus grande compréhension des théorèmes. À l'occasion, vous pouvez aussi faire la table de vérité d'un théorème ; cela peut aider à comprendre de quoi il parle.

3.7 Problèmes

1. Dites quelle règle de substitution et quelle règle de Leibniz sont utilisées dans les transformations suivantes (autrement dit, précisez les valeurs de E, F, X, Y, v, z utilisées dans (1.9) et (1.13)). Après avoir donné les règles, effectuez les substitutions qu'elles contiennent.

   (a) $\neg p \equiv p \equiv \mathsf{faux}$

   $=$ $\langle$ Commutativité de $\equiv$ (3.3), avec $p, q := \mathsf{faux}, p$ $\rangle$

   $\neg p \equiv \mathsf{faux} \equiv p$

   (b) $\neg p \equiv \mathsf{faux} \equiv p$

   $=$ $\langle$ (3.14), avec $q := \mathsf{faux}$ $\rangle$

   $\neg\mathsf{faux}$

   (c) $\neg\mathsf{faux}$

   $=$ $\langle$ Négation de faux (3.16) $\rangle$

   vrai

2. Démontrez le théorème (3.14) de trois manières différentes : tout d'abord, transformez $\neg p \equiv q \equiv p \equiv \neg q$ en un théorème ; ensuite, transformez $\neg p \equiv p$ en $q \equiv \neg q$; finalement, transformez $\neg p$ en $q \equiv p \equiv \neg q$. Comparez ces trois preuves et celle donnée à la page 32. Laquelle est la plus simple ou la plus courte ?
3. Démontrez le théorème sur la double négation (3.15), $\neg\neg p \equiv p$.
4. Démontrez le théorème (3.17), $(p \not\equiv q) \equiv \neg p \equiv q$.
5. Démontrez le théorème (3.18) en transformant $\neg p \equiv p \equiv \mathsf{faux}$ en vrai en utilisant le théorème (3.14). La preuve requiert au plus deux utilisations de la règle de Leibniz.
6. Utilisez l'heuristique d'élimination des définitions (3.29) pour démontrer le théorème d'interchangeabilité mutuelle (3.22), $p \not\equiv q \equiv r \equiv p \equiv q \not\equiv r$. Éliminez $\not\equiv$, utilisez une propriété de $\equiv$ et réintroduisez $\not\equiv$.
7. Démontrez la distributivité de $\vee$ sur $\vee$ (3.41), $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$.
8. La dérivation suivante démontre le théorème (3.20) sur l'associativité de $\not\equiv$. Pour chacune des transformations, donnez les paramètres de la règle de substitution et de la règle de Leibniz qui sont utilisées, c'est-à-dire, donnez les valeurs de E, F, X, Y, v, z qu'il faut

employer dans (1.9) et (1.13) (il n'est pas nécessaire de donner les règles elles-mêmes). Les transformations sont numérotées pour pouvoir y référer dans la réponse.

$$
\begin{array}{ll}
 & (p \not\equiv q) \not\equiv r \\
= & \qquad \langle\ 1.\ (3.17)\ \rangle \\
 & (\neg p \equiv q) \not\equiv r \\
= & \qquad \langle\ 2.\ \text{Commutativité de } \not\equiv\ (3.19),\ \text{avec } p, q\ :=\ \neg p \equiv q, r\ \rangle \\
 & r \not\equiv (\neg p \equiv q) \\
= & \qquad \langle\ 3.\ (3.17),\ \text{avec } p, q\ :=\ r, \neg p \equiv q\ \rangle \\
 & \neg r \equiv (\neg p \equiv q) \\
= & \qquad \langle\ 4.\ \text{Commutativité de } \equiv\ (3.3),\ \text{avec } p, q\ :=\ \neg r, \neg p \equiv q\ \rangle \\
 & (\neg p \equiv q) \equiv \neg r \\
= & \qquad \langle\ 5.\ \text{Associativité de } \equiv\ (3.2),\ \text{avec } p, r\ :=\ \neg p, \neg r\ \rangle \\
 & \neg p \equiv (q \equiv \neg r) \\
= & \qquad \langle\ 6.\ (3.17),\ \text{avec } q\ :=\ q \equiv \neg r\ \rangle \\
 & p \not\equiv (q \equiv \neg r) \\
= & \qquad \langle\ 7.\ \text{Commutativité de } \equiv\ (3.3),\ \text{avec } p, q\ :=\ q, \neg r\ \rangle \\
 & p \not\equiv (\neg r \equiv q) \\
= & \qquad \langle\ 8.\ (3.17),\ \text{avec } p\ :=\ r\ \rangle \\
 & p \not\equiv (r \not\equiv q) \\
= & \qquad \langle\ 9.\ \text{Commutativité de } \not\equiv\ (3.19),\ \text{avec } p\ :=\ r\ \rangle \\
 & p \not\equiv (q \not\equiv r)
\end{array}
$$

9. Démontrez le théorème d'absorption (3.61d), $p \vee (\neg p \wedge q) \equiv p \vee q$.
10. Démontrez le théorème de remplacement (3.65),

$$(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \wedge (r \equiv q),$$

en montrant que le côté gauche et le côté droit sont tous deux équivalents à

$$p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p.$$

La transformation du côté gauche (ou du côté droit) de cette expression peut se faire en appliquant la distributivité de $\vee$ sur $\equiv$ (3.36) trois fois.

11. Démontrez la réflexivité de $\Rightarrow$ (3.87), $p \Rightarrow p \equiv \mathsf{vrai}$.
12. Démontrez le théorème de l'affaiblissement/renforcement (3.92c), $p \wedge q \Rightarrow p \vee q$.
13. Démontrez le modus ponens (3.93), $p \wedge (p \Rightarrow q) \Rightarrow q$.

Chapitre 4

Assouplissement du style de preuve

4.1 Une abréviation pour la démonstration d'implications

Théorèmes additionnels sur l'implication

(4.1) $p \Rightarrow (q \Rightarrow p)$

(4.2) Monotonie de $\vee$: $(p \Rightarrow q) \;\Rightarrow\; (p \vee r \;\Rightarrow\; q \vee r)$

(4.3) Monotonie de $\wedge$: $(p \Rightarrow q) \;\Rightarrow\; (p \wedge r \;\Rightarrow\; q \wedge r)$

(4.4) Remarque. Une fonction booléenne f est dite *monotone* ssi

$$(x \Rightarrow y) \;\Rightarrow\; (f.x \Rightarrow f.y)$$

(une fonction booléenne est une fonction qui s'applique à vrai ou à faux et qui retourne vrai ou faux).
Une fonction f sur les réels est dite *monotone* ssi

$$x \leq y \;\Rightarrow\; f.x \leq f.y \;.$$

Exemple : la fonction $f(x) = x + 10$ est monotone.

Remarquez la similitude entre $\Rightarrow$ et $\leq$.

Similitude entre $\leq$ et $\Rightarrow$

Supposons $x \geq 0$. Démontrons $x^2 + x \leq (x+1)^2 + 5$.

$$
\begin{array}{ll}
 & x^2 + x \\
\leq & \quad \langle\ \ldots\ \rangle \\
 & x^2 + 2 \cdot x + 1 \\
= & \quad \langle\ \ldots\ \rangle \\
 & (x+1)^2 \\
\leq & \quad \langle\ \ldots\ \rangle \\
 & (x+1)^2 + 5
\end{array}
$$

$$
\begin{array}{ll}
 & (x+1)^2 + 5 \\
\geq & \quad \langle\ \ldots\ \rangle \\
 & (x+1)^2 \\
= & \quad \langle\ \ldots\ \rangle \\
 & x^2 + 2 \cdot x + 1 \\
\geq & \quad \langle\ \ldots\ \rangle \\
 & x^2 + x
\end{array}
$$

Le résultat découle de la transitivité des suites de $\leq$ et $=$ pour la preuve gauche, et des suites de $\geq$ et $=$ pour la preuve droite (il ne faut pas mettre des $\geq$ et $\leq$ dans la colonne gauche d'une même preuve).

Et maintenant, voici une preuve où $\Rightarrow$ joue un rôle similaire à celui de $\leq$ ci-dessus.

Démonstration de $(p \Rightarrow q) \ \Rightarrow \ (p \vee r \ \Rightarrow \ q \vee r)$ (4.2)

$$
\begin{array}{ll}
 & p \vee r \ \Rightarrow \ q \vee r \\
= & \quad \langle\ (3.73)\ \rangle \\
 & p \vee r \vee q \vee r \ \equiv \ q \vee r \\
= & \quad \langle\ (3.34)\ \rangle \\
 & p \vee q \vee r \ \equiv \ q \vee r \\
= & \quad \langle\ (3.36)\ \rangle \\
 & (p \vee q \ \equiv \ q) \vee r \\
\Leftarrow & \quad \langle\ (3.92\text{a})\ \rangle \\
 & p \vee q \ \equiv \ q \\
= & \quad \langle\ (3.73)\ \rangle \\
 & p \Rightarrow q
\end{array}
$$

$$
\begin{array}{ll}
 & p \Rightarrow q \\
= & \quad \langle\ (3.73)\ \rangle \\
 & p \vee q \ \equiv \ q \\
\Rightarrow & \quad \langle\ (3.92\text{a}),\ \textit{surprise}\ \rangle \\
 & (p \vee q \ \equiv \ q) \vee r \\
= & \quad \langle\ (3.36)\ \rangle \\
 & p \vee q \vee r \ \equiv \ q \vee r \\
= & \quad \langle\ (3.34)\ \rangle \\
 & p \vee r \vee q \vee r \ \equiv \ q \vee r \\
= & \quad \langle\ (3.73)\ \rangle \\
 & p \vee r \ \Rightarrow \ q \vee r
\end{array}
$$

Le résultat découle des lois de transitivité (3.99).

(4.5) Exercice. Donnez une autre démonstration de la monotonie de $\vee$ (4.2). Voici le début de la démonstration.

$$
\begin{array}{ll}
 & p \vee r \ \Rightarrow \ q \vee r \\
= & \quad \langle\ \text{Définition alternative de } \Rightarrow\ (3.75),\ \text{avec } p, q \ := \ p \vee r, q \vee r\ \rangle
\end{array}
$$

4.2 Techniques de démonstration additionnelles

Assumer l'antécédent

Pratique courante en mathématique. Pour démontrer $P \Rightarrow Q$, on dit
« supposons P et démontrons Q ».

Montrons

$$(p \wedge p' \equiv p) \wedge (q \wedge q' \equiv q) \;\Rightarrow\; (p \wedge q \;\Rightarrow\; p' \wedge q') \;.$$

Supposons $p \wedge p' \equiv p$ **et** $q \wedge q' \equiv q$. **Montrons** $p \wedge q \;\Rightarrow\; p' \wedge q'$.

$$\begin{array}{ll} & p \wedge q \\ = & \quad \langle \text{ Hypothèse } p \wedge p' \equiv p \;\rangle \\ & p \wedge p' \wedge q \\ = & \quad \langle \text{ Hypothèse } q \wedge q' \equiv q \;\rangle \\ & p \wedge p' \wedge q \wedge q' \\ \Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec } p,\; q \;:=\; p' \wedge q',\; p \wedge q \;\rangle \\ & p' \wedge q' \end{array}$$

(4.6) Théorème de déduction (généralisé) : Si l'ajout de $P_1, \ldots, P_n$ à la liste des axiomes de la logique propositionnelle **E**, *avec les variables de $P_1, \ldots, P_n$ considérées comme des constantes*, permet de démontrer Q, alors

$$P_1 \wedge \ldots \wedge P_n \;\Rightarrow\; Q$$

est un théorème.

Remarque : on parle de « théorème de déduction » (terme consacré), mais il s'agit en fait d'un métathéorème.

Il est important de considérer les variables de l'antécédent comme des constantes. Si on ne respecte pas cette contrainte, on peut démontrer des propositions non valides. Faisons cette erreur et montrons $(b \equiv c) \Rightarrow (d \equiv c)$, qui n'est pas valide.

Supposons $b \equiv c$ (preuve incorrecte)

$$\begin{array}{ll} & d \\ = & \quad \langle \text{ Hypothèse } b \equiv c, \text{ avec } b \;:=\; d, \text{ c'est-à-dire } d \equiv c \;\rangle \\ & c \end{array}$$

Assumer l'antécédent (preuve hiérarchique)

Montrons

$$(p \Rightarrow p') \;\Rightarrow\; \big((q \Rightarrow q') \;\Rightarrow\; (p \wedge q \;\Rightarrow\; p' \wedge q')\big)\ .$$

Supposons $p \Rightarrow p'$ (ce qui est équivalent à $p \wedge p' \equiv p$) et montrons $(q \Rightarrow q') \;\Rightarrow\; (p \wedge q \;\Rightarrow\; p' \wedge q')$

Supposons $q \Rightarrow q'$ (ce qui est équivalent à $q \wedge q' \equiv q$) et montrons $p \wedge q \;\Rightarrow\; p' \wedge q'$

$$\begin{array}{ll} & p \wedge q \\ = & \quad \langle \text{ Hypothèse } p \wedge p' \equiv p \ \rangle \\ & p \wedge p' \wedge q \\ = & \quad \langle \text{ Hypothèse } q \wedge q' \equiv q \ \rangle \\ & p \wedge p' \wedge q \wedge q' \\ \Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec } p,\ q := p' \wedge q',\ p \wedge q \ \rangle \\ & p' \wedge q' \end{array}$$

Règle du modus ponens

Supposons que P et $P \Rightarrow Q$ soient des théorèmes. Nous pouvons alors montrer que Q est un théorème :

$$\begin{array}{ll} & P \Rightarrow Q \qquad \text{—C'est un théorème par hypothèse} \\ = & \quad \langle \ \mathsf{vrai} \text{ est un théorème (3.6)} \ \ \& \\ & \quad\ \ P \text{ est un théorème par hypothèse} \ \ \& \\ & \quad\ \ \text{Deux théorèmes quelconques sont équivalents (Métathéorème (3.100))} \ \rangle \\ & \mathsf{vrai} \Rightarrow Q \\ = & \quad \langle \text{ (3.89), avec } p := Q \ \rangle \\ & Q \end{array}$$

Nous pouvons exprimer ce résultat sous la forme d'une règle :

Règle du modus ponens : $\dfrac{P, \quad P \Rightarrow Q}{Q}$

Cette règle est très utile, mais comme les autres règles introduites jusqu'ici, on omet souvent de la mentionner lorsqu'on l'utilise.

Exemple d'utilisation de la règle du modus ponens

Supposons que $p \Rightarrow q$ soit un théorème. Montrons que $p \wedge r \wedge s \;\Rightarrow\; q \wedge r$ est un théorème :

$$
\begin{array}{ll}
 & p \wedge r \wedge s \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec } p, q := p \wedge r, s \rangle \\
 & p \wedge r \\
\Rightarrow & \quad \langle \ p \Rightarrow q \text{ est un théorème par hypothèse } \ \& \\
 & \quad \text{Monotonie de } \wedge \text{ (4.3), } (p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r) \ \ \& \\
 & \quad \text{Règle du modus ponens (permet de conclure que } p \wedge r \Rightarrow q \wedge r \text{ est un} \\
 & \quad \text{théorème) } \rangle \\
 & q \wedge r
\end{array}
$$

On peut écrire simplement :

$$
\begin{array}{ll}
 & p \wedge r \wedge s \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec } p, q := p \wedge r, s \rangle \\
 & p \wedge r \\
\Rightarrow & \quad \langle \text{ Hypothèse } p \Rightarrow q \ \ \& \ \ \text{Monotonie de } \wedge \text{ (4.3) } \rangle \\
 & q \wedge r
\end{array}
$$

Attention : piège dans lequel il est facile de tomber

Supposons que $p \Rightarrow q$ soit un théorème. Voici une dérivation *INCORRECTE*.

$$
\begin{array}{ll}
 & p \wedge r \\
= & \quad \langle \text{ Hypothèse } p \Rightarrow q \ \ \& \ \ \text{Monotonie de } \wedge \text{ (4.3) } \rangle \\
 & q \wedge r
\end{array}
$$

On peut voir que $p \wedge r \equiv q \wedge r$ n'est pas un théorème, même en assumant que $p \Rightarrow q$ en est aussi un. Dans l'état

$$(p, \mathsf{faux}), (q, \mathsf{vrai}), (r, \mathsf{vrai})$$

la valeur de

$$p \Rightarrow q$$

est vrai et celle de

$$p \wedge r \equiv q \wedge r$$

est faux. C'est une erreur semblable à celle qui consisterait à conclure

$$x + z = y + z$$

à partir de

$$x < y \ .$$

4.3 Problèmes

1. Démontrez la monotonie de $\wedge$ (4.3), $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$, en utilisant la méthode de la section 4.1. Commencez avec le conséquent, puisqu'il est plus structuré.
2. Démontrez $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \Rightarrow q \wedge s)$, en utilisant le style de preuve de la section 4.1. Avant de débuter cette preuve, considérez la possibilité d'utiliser le théorème de transfert (3.81) pour déplacer $p \wedge r$ dans l'antécédent.
3. Démontrez $(\neg p \Rightarrow q) \Rightarrow ((p \Rightarrow q) \Rightarrow q)$, en utilisant la méthode qui consiste à assumer l'antécédent.
4. Démontrez le modus ponens (3.93), $p \wedge (p \Rightarrow q) \Rightarrow q$, en utilisant la méthode qui consiste à assumer l'antécédent.

Chapitre 5

Application du calcul propositionnel : résolution d'énigmes

Vérification d'arguments exprimés en français : exemple de Superman

Supposons F_0, F_1, F_2, F_3 et montrons $\neg\mathsf{e}$.

$\neg\mathsf{e}$

$\Leftarrow$ $\langle$ Contrapositivité (3.77) sur F_3, avec $p, q := \mathsf{e}, \neg\mathsf{i} \wedge \neg\mathsf{m}$ $\rangle$

$\neg(\neg\mathsf{i} \wedge \neg\mathsf{m})$

$=$ $\langle$ De Morgan (3.48a), avec $p, q := \neg\mathsf{i}, \neg\mathsf{m}$ & Double négation (3.15) deux fois : (1) avec $p := \mathsf{i}$; (2) avec $p := \mathsf{m}$ $\rangle$

$\mathsf{i} \vee \mathsf{m}$

$\Leftarrow$ $\langle$ Le 1er opérande de $\wedge$ dans F_1 $(\neg\mathsf{pp} \Rightarrow \mathsf{i})$ est un théorème par hypothèse & Monotonie de $\vee$ (4.2), avec $p, q, r := \neg\mathsf{pp}, \mathsf{i}, \mathsf{m}$ & Règle du modus ponens $\rangle$

$\neg\mathsf{pp} \vee \mathsf{m}$

$\Leftarrow$ $\langle$ Le 2e opérande de $\wedge$ dans F_1 $(\neg\mathsf{v} \Rightarrow \mathsf{m})$ est un théorème par hypothèse & Monotonie de $\vee$ (4.2), avec $p, q, r := \neg\mathsf{v}, \mathsf{m}, \neg\mathsf{pp}$ & Règle du modus ponens $\rangle$

$\neg\mathsf{pp} \vee \neg\mathsf{v}$

$=$ $\langle$ De Morgan (3.48a), avec $p, q := \mathsf{pp}, \mathsf{v}$ $\rangle$

$\neg(\mathsf{pp} \wedge \mathsf{v})$

$\Leftarrow$ $\langle$ Contrapositivité (3.77) sur F_0, avec $p, q := \mathsf{pp} \wedge \mathsf{v}, \mathsf{p}$ $\rangle$

$\neg\mathsf{p}$

$=$ $\langle$ F_2 est un théorème par hypothèse & vrai est un théorème (3.6) & Métathéorème (3.100) $\rangle$

vrai

Nous avons montré $\mathsf{vrai} \Rightarrow \neg\mathsf{e}$, ce qui est équivalent à $\neg\mathsf{e}$, puisque vrai est l'identité à gauche de $\Rightarrow$ (3.89). Nous concluons que

$$F_0 \wedge F_1 \wedge F_2 \wedge F_3 \;\Rightarrow\; \neg\mathsf{e}$$

est un théorème, de sorte que l'argument sur Superman est correct.

Construction d'un contre-exemple

Lorsqu'on n'arrive pas à démontrer une proposition ou que celle-ci ne semble pas valide, on peut réussir à trouver un contre-exemple (et il est alors inutile de continuer les tentatives de preuve).

Pour montrer qu'une expression P n'est pas valide, il suffit de trouver un état (même partiellement défini) pour lequel P a la valeur faux : cet état est le contre-exemple.

TAB. 5.1 – Contre-exemples pour des expressions simples

expression	contre-exemple 1	contre-exemple 2
$p \wedge q$	$p = \mathsf{faux}$	$q = \mathsf{faux}$
$p \vee q$	$p = q = \mathsf{faux}$	
$p \equiv q$	$p = \mathsf{vrai}, q = \mathsf{faux}$	$p = \mathsf{faux}, q = \mathsf{vrai}$
$p \not\equiv q$	$p = q = \mathsf{vrai}$	$p = q = \mathsf{faux}$
$p \Rightarrow q$	$p = \mathsf{vrai}, q = \mathsf{faux}$	

Contre-exemple : conjecture 4 du problème de l'autobus

Rappel : les trois hypothèses sont

$$(1)\ \mathsf{pa} \Rightarrow (\mathsf{ar} \Rightarrow \mathsf{mr}) \qquad (2)\ \mathsf{mr} \wedge d \Rightarrow \neg\mathsf{am} \qquad (3)\ \neg e \Rightarrow d \wedge \neg\mathsf{am}\ .$$

La conjecture (4) est

$$(4)\ \mathsf{pa} \Rightarrow (\mathsf{ar} \Rightarrow e)\ .$$

On veut savoir si

$$(1) \wedge (2) \wedge (3) \;\Rightarrow\; (4)\ .$$

Tentons de trouver un contre-exemple. Pour cela, il faut avoir

$$(1) \wedge (2) \wedge (3) \;\equiv\; \mathsf{vrai} \qquad \text{et} \qquad (4) \;\equiv\; \mathsf{faux}\ .$$

Cherchons ce qui peut donner $(4) \equiv \mathsf{faux}$ (plus simple que $(1) \wedge (2) \wedge (3) \equiv \mathsf{vrai}$). Il faut

$$\boxed{\mathsf{pa} \equiv \mathsf{vrai}} \qquad \text{et} \qquad \mathsf{ar} \Rightarrow e \equiv \mathsf{faux}\ ,$$

d'où

$$\boxed{\mathsf{ar} \equiv \mathsf{vrai}} \qquad \text{et} \qquad \boxed{e \equiv \mathsf{faux}} \ .$$

Avec ces valeurs, voyons si on peut avoir $(1) \wedge (2) \wedge (3) \equiv \mathsf{vrai}$.

$$\begin{array}{ll} & \big(\mathsf{pa} \Rightarrow (\mathsf{ar} \Rightarrow \mathsf{mr})\big) \wedge \big(\mathsf{mr} \wedge d \Rightarrow \neg\mathsf{am}\big) \wedge \big(\neg e \Rightarrow d \wedge \neg\mathsf{am}\big) \\ = & \qquad \langle \text{ Substitution de variables par leur valeur } \rangle \\ & \big(\mathsf{vrai} \Rightarrow (\mathsf{vrai} \Rightarrow \mathsf{mr})\big) \wedge \big(\mathsf{mr} \wedge d \Rightarrow \neg\mathsf{am}\big) \wedge \big(\neg\mathsf{faux} \Rightarrow d \wedge \neg\mathsf{am}\big) \\ = & \qquad \langle \text{ Il faut prendre } \boxed{\mathsf{mr} \equiv \mathsf{vrai}} \ \ \& \ \ \neg\mathsf{faux} \equiv \mathsf{vrai} \ \rangle \\ & \big(\mathsf{vrai} \Rightarrow (\mathsf{vrai} \Rightarrow \mathsf{vrai})\big) \wedge \big(\mathsf{vrai} \wedge d \Rightarrow \neg\mathsf{am}\big) \wedge \big(\mathsf{vrai} \Rightarrow d \wedge \neg\mathsf{am}\big) \\ = & \qquad \langle \text{ Identité à gauche de } \Rightarrow \ (3.89) \ \ \& \ \ \text{Identité de } \wedge \ (3.52) \ \rangle \\ & \mathsf{vrai} \wedge (d \Rightarrow \neg\mathsf{am}) \wedge (d \wedge \neg\mathsf{am}) \\ = & \qquad \langle \text{ Il faut prendre } \boxed{d \equiv \mathsf{vrai}} \text{ et } \boxed{\mathsf{am} \equiv \mathsf{faux}} \ \rangle \\ & \mathsf{vrai} \end{array}$$

Il y a donc un contre-exemple, qui est

$$\boxed{(\mathsf{pa}, \mathsf{vrai}), (\mathsf{ar}, \mathsf{vrai}), (e, \mathsf{faux}), (\mathsf{mr}, \mathsf{vrai}), (d, \mathsf{vrai}), (\mathsf{am}, \mathsf{faux})}$$

Par conséquent, la conjecture (4) ne découle pas des hypothèses (1), (2) et (3).

(5.1) Exercice. Les conjectures du problème de M. Centprises (exercice (2.8)) sont-elles une conséquence des hypothèses ? Si oui, donnez une preuve ; sinon, donnez un contre-exemple.

Comment trouver un sens à une phrase tordue

> v est dans le tableau $b[1..10]$ signifie que si la valeur v est dans $b[11..20]$ alors elle n'est pas dans $b[11..20]$.

Associons des variables booléennes aux propositions primitives :

$$\begin{array}{ll} x : & v \text{ est dans } b[1..10] \ , \\ y : & v \text{ est dans } b[11..20] \ . \end{array}$$

L'énoncé est alors formalisé ainsi : $\boxed{x \equiv y \Rightarrow \neg y \ .}$ Simplifions cette expression.

$$
\begin{array}{ll}
& x \equiv y \Rightarrow \neg y \\
= & \qquad \langle \text{ Définition alternative de l'implication (3.75) } \rangle \\
& x \equiv \neg y \vee \neg y \\
= & \qquad \langle \text{ Idempotence de } \vee \text{ (3.34) } \rangle \\
& x \equiv \neg y
\end{array}
$$

Traduisons l'expression simplifiée en français :

La valeur v est dans $b[1..10]$ ssi elle n'est pas dans $b[11..20]$.

Autrement dit, si la valeur v est dans la première moitié de b elle n'est pas dans la deuxième moitié et si elle n'est pas dans la deuxième moitié elle est dans la première.

Enigme : le dilemme du soupirant de Portia

Adapté de Shakespeare, *Le marchand de Venise*.

Portia a un coffret d'or et un coffret d'argent. Elle a placé son portrait dans l'un deux. Sur les coffrets, elle a écrit :

Coffret d'or :	Le portrait n'est pas ici.
Coffret d'argent :	Exactement l'une de ces inscriptions est vraie.

Portia explique à son soupirant que chaque inscription peut être vraie ou fausse, mais que le portrait est placé dans les coffrets d'une manière qui est cohérente avec les inscriptions. S'il peut choisir le coffret avec son portrait, elle le mariera —dans ce temps-là, c'est ce que les souspirants désiraient.

Comment le soupirant peut-il résoudre le problème ?

Introduisons des variables booléennes pour nommer les propositions primitives.

co :	Le portrait est dans le coffret d'or.
ca :	Le portrait est dans le coffret d'argent.
o :	Le portrait n'est pas ici. (Ceci est l'inscription sur le coffret d'or.)
a :	Exactement l'une de o et a a la valeur vrai. (Ceci est l'inscription sur le coffret d'argent.)

Le fait que le portrait soit dans exactement l'un des coffrets s'écrit

$$F_0 : co \equiv \neg ca \ .$$

L'inscription o sur le coffret d'or est la négation de co :

$$F_1 : o \equiv \neg co \ .$$

L'inscription a est équivalente à $a \equiv \neg o$ (raisonnement similaire à F_0), mais on ne sait si elle est vraie. Tout ce qu'on sait, c'est qu'elle affirme $a \equiv \neg o$:

$$F_2 : a \equiv (a \equiv \neg o) .$$

Essayons de dériver co ou ca. Le point de départ est F_2, qui est l'expression qui a le plus de structure.

$$\begin{array}{ll} & a \equiv a \equiv \neg o \qquad \text{—Hypothèse } F_2 \\ = & \qquad \langle \text{ Commutativité de } \equiv \text{ (3.3), qui donne } \neg o \equiv a \equiv a \equiv \neg o \ \rangle \\ & \neg o \\ = & \qquad \langle \ F_1 \ \ \& \ \text{Double négation (3.15)} \ \rangle \\ & co \end{array}$$

Le portrait est donc dans le coffret d'or.

Il faut s'assurer que F_0, F_1 et F_2 ne sont pas contradictoires, c'est-à-dire qu'il y a une affectation de valeurs à o, a, co, ca qui rend $F_0 \wedge F_1 \wedge F_2$ vrai. Sinon, n'importe quoi pourrait être démontré à partir de cette incohérence. Dans ce cas, les hypothèses du problème ne pourraient être satisfaites et nous conclurions qu'il n'a pas de solution.

Les deux états

$$\begin{array}{rcccc} & (co, \mathsf{vrai}), & (ca, \mathsf{faux}), & (o, \mathsf{faux}), & (a, \mathsf{faux}) \\ \text{et} & (co, \mathsf{vrai}), & (ca, \mathsf{faux}), & (o, \mathsf{faux}), & (a, \mathsf{vrai}) \end{array}$$

montrent que F_0, F_1 et F_2 sont cohérentes (vérifiez). Notez que ces deux états diffèrent seulement par la valeur de a. L'inscription sur le coffret d'argent peut être vraie ou fausse.

5.1 Problèmes

1. Formalisez chacun des arguments suivants et soit montrez que c'est un théorème, soit trouvez un contre-exemple.
   (a) Le programme ne termine pas ou n devient éventuellement 0. Si n devient 0, m deviendra éventuellement 0. Le programme termine. Par conséquent, m deviendra éventuellement 0.
   (b) Si l'initialisation est correcte et si la boucle termine, alors P est vrai dans l'état final. P est vrai dans l'état final. Par conséquent, si l'initialisation est correcte, la boucle termine.
   (c) S'il y a un homme sur la lune, la lune est faite en fromage, et si la lune est faite en fromage, alors je suis un singe. Il n'y a pas d'homme sur la lune ou la lune n'est pas faite en fromage. Par conséquent, la lune n'est pas faite en fromage ou je suis un singe.

(d) Si Réjean trompe Thérèse, alors môman est fâchée ou pôpa est triste. Pôpa est triste. Par conséquent, si môman est fâchée alors Réjean ne trompe pas Thérèse.

2. Supposons que Portia place son portrait dans l'un de trois coffrets et qu'elle place les inscriptions suivantes sur ceux-ci :

Coffret d'or :	Le portrait est ici.
Coffret d'argent :	Le portrait est ici.
Coffret de plomb :	Au moins deux de ces inscriptions sont fausses.

Quel coffret son soupirant doit-il choisir ? Formalisez le problème et calculez la réponse.

3. La série de questions qui suit concerne une île avec des chevaliers et des filous. Les chevaliers disent toujours la vérité et les filous mentent toujours. Pour formaliser ces questions, utilisez les identificateurs suivants :

b : B est un chevalier.
c : C est un chevalier.
d : D est un chevalier.

Si B énonce « X », ceci donne lieu à l'expression $b \equiv X$, puisque si b, alors B est un chevalier et dit la vérité, de sorte que X, et si $\neg b$, alors B est un filou et ment, de sorte que $\neg X$. Il en est de même pour les énoncés de C et D.

(a) Quelqu'un demande à B « Êtes-vous un chevalier ? ». B réplique « Si je suis un chevalier, je vais manger mon chapeau ». Montrez que B devra manger son chapeau.

(b) B, C et D discutent ensemble. C dit « Il y a un chevalier parmi nous ». D dit « Vous mentez ». Pouvez-vous dire qui est chevalier et qui est filou ?

Indice : On peut décrire le fait qu'un ou trois de ces personnages soient des chevaliers par l'expression $b \equiv c \equiv d$, puisque cette expression a la valeur vrai exactement lorsque le nombre d'opérandes faux est pair. Pour restreindre à un chevalier, il suffit de faire la conjonction de cette expression avec $\neg(b \wedge c \wedge d)$. Voyez la discussion à la page 46 du manuel.

4. À l'exercice 2.7, nous avons traduit les hypothèses et les conjectures relatives à l'autobus tardif. Déterminez maintenant quelles conjectures sont une conséquence des trois hypothèses.

Chapitre 6

Quantification

6.1 Types

Un type est un ensemble de valeurs. Voici les types de base :

TAB. 6.1 – Quelques types élémentaires

nom	symbole	type (ensemble de valeurs)
entiers (relatifs)	$\mathbb{Z}$	$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
naturels	$\mathbb{N}$	$0, 1, 2, 3, \ldots$
entiers positifs	$\mathbb{Z}^+, \mathbb{N}^+$	$1, 2, 3, 4, \ldots$
entiers négatifs	$\mathbb{Z}^-$	$-1, -2, -3, -4, \ldots$
rationnels	$\mathbb{Q}$	i/j, où i, j entiers, $j \neq 0$
réels	$\mathbb{R}$	tous les nombres réels
réels positifs	$\mathbb{R}^+$	tous les nombres réels positifs
booléens	$\mathbb{B}$	vrai, faux

Typage des expressions

La notation $E{:}t$ signifie que l'expression E a le type t.

déclaration	signification
$E{:}t$	E a le type t
$1{:}\mathbb{N}$	1 a le type $\mathbb{N}$
$1{:}\mathbb{R}$	1 a le type $\mathbb{R}$
vrai:$\mathbb{B}$	vrai a le type $\mathbb{B}$

On peut typer complètement une expression en donnant le type des sous-expressions :

$$((x{:}\mathbb{R} + y{:}\mathbb{R})^{k:\mathbb{Z}}){:}\mathbb{R} \ .$$

(6.1) Remarque. La notion de type est une notion syntaxique. La correction du typage dépend seulement de la séquence de symboles de l'expression donnée et non pas de son évaluation. Par exemple,

$$(1/(x{:}\mathbb{Z})){:}\mathbb{R}$$

est une expression (bien typée) même si elle n'est pas définie lorsque $x = 0$ (elle ne peut être évaluée dans l'état $x = 0$). C'est comme un programme accepté par le compilateur, mais qui plante à l'exécution.

Typage des fonctions

La notation

(6.2) $f : t_1 \times \cdots \times t_n \to r$

exprime que f est une fonction avec n arguments (paramètres)de types $t_1, \ldots, t_n$ avec un résultat de type r.

fonction	type	application typique
plus	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$	plus$(1, 3)$ ou $1 + 3$
non	$\mathbb{B} \to \mathbb{B}$	non.vrai ou $\neg$vrai
plus-petit-que	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{B}$	plus-petit-que$(5, 3)$ ou $5 < 3$

Considérons la fonction f avec le type donné en (6.2). L'expression $f(a_1, \ldots, a_n)$ s'appelle l'*application* de la fonction f aux arguments $a_1, \ldots, a_n$. Toutefois, c'est une expression *si et seulement si* chaque argument a_i a le type t_i. Par conséquent,

$f(a_1, \ldots, a_n)$ n'est pas une expression s'il y a une erreur de typage.

Quand il y a une erreur de type, on parle en général d'expression mal typée.

$E{:}t$ versus $E \in t$

Pour n'importe quelle expression E et n'importe quel type t,

$$E \in t$$

est une expression.

La valeur de $E \in t$ est la valeur de la proposition « E est dans l'ensemble t ».

Par exemple, $5 \in \mathbb{Z}$ a la valeur vrai, alors que $5 \in \mathbb{B}$ a la valeur faux. On peut écrire

(6.3) $i \in \mathbb{N} \Rightarrow -i \leq 0$,

ce qui signifie que si i est un nombre naturel, alors $-i \leq 0$.

La relation entre $E{:}t$ et $E \in t$ est la suivante :

Si E a le type t, c'est-à-dire $E{:}t$, alors $E \in t$ a la valeur vrai dans tous les états pour lesquels E est définie, sinon elle a la valeur faux.

Par exemple, si E est $(1/x){:}\mathbb{R}$, alors

$(1/5) \in \mathbb{R}$ a la valeur vrai et $(1/0) \in \mathbb{R}$ a la valeur faux .

Restrictions pour un typage correct

(6.4) Dans une substitution textuelle $E[x := F]$, x et F doivent avoir le même type.

(6.5) L'égalité $b = c$ est définie si et seulement si b et c ont le même type. C'est-à-dire que le type de l'opérateur $=$ est $t \times t \to \mathbb{B}$, pour n'importe quel type t.

Ainsi, $5 =$ vrai est mal typée. Dans ce cas, on ne parle même pas de son évaluation. Dans un langage de programmation typé, le compilateur rejetterait un programme contenant cette « expression ». Le programme ne pourrait jamais être exécuté.

Nous laissons tomber certains points dans cette brève introduction aux types. Pour bien expliquer les typages suivants,

$$1{:}\mathbb{N}, \quad 1{:}\mathbb{Z}, \quad 1{:}\mathbb{R},$$
$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad + : \mathbb{R} \times \mathbb{R} \to \mathbb{R},$$
$$= : t \times t \to \mathbb{B},$$

il faudrait introduire les notions de *sous-type*, de *surcharge* des opérateurs et de *polymorphisme*.

(6.6) Exercice. Supposons

$$f{:}S \to S, \qquad g{:}S \times T \to V, \qquad a{:}S, \qquad b{:}T.$$

Les expressions suivantes sont-elles bien typées ? Si oui, donnez le type de l'expression (c'est-à-dire le type de la valeur produite par l'évaluation de l'expression). Sinon, dites pourquoi.

1. $g(f.a, b)$
2. $f(g(a, b))$

6.2 Syntaxe et interprétation de la quantification

Vous êtes familiers avec des expressions comme $\sum_{i=1}^{3} i^2$ et $\prod_{k=1}^{5} k+2$ et vous savez que

$$\begin{aligned} \textstyle\sum_{i=1}^{3} i^2 &= 1^2+2^2+3^2 \\ \textstyle\prod_{k=1}^{5} k+2 &= 3\cdot 4\cdot 5\cdot 6\cdot 7 \end{aligned}$$

Par la suite, nous utiliserons une notation linéaire au lieu de la notation ci-dessus :

$$(\textstyle\sum i \mid 1\le i\le 3 : i^2) \qquad \text{ou} \qquad (+i \mid 1\le i\le 3 : i^2)$$

$$(\textstyle\prod k \mid 1\le k\le 5 : k+2) \qquad \text{ou} \qquad (\cdot k \mid 1\le k\le 5 : k+2)$$

Ces expressions sont appelées des *quantifications*. Les opérateurs $\sum$ et $\prod$ (ou $+$ et $\cdot$ utilisés de cette manière) sont appelés des *quantificateurs*.

Pourquoi la notation linéaire $(\sum i \mid 1\le i\le 3 : i^2)$?

1. Les parenthèses indiquent explicitement la *portée* de la *variable de quantification* i, c'est-à-dire les endroits où i peut être utilisée (à l'intérieur des parenthèses). Notez que $\sum i$ (ou $+i$) agit comme une déclaration qui introduit une variable locale i ; la variable est locale parce qu'elle est visible seulement à l'intérieur des parenthèses, comme nous le verrons. C'est exactement la même notion qu'en programmation, où une fonction ou une procédure peuvent introduire des variables locales.
2. Elle permet des expressions plus générales pour définir le *domaine* de i (les valeurs que i peut prendre). Par exemple,

$$(+i \mid 1\le i\le 7 \wedge \mathsf{pair}.i : 3\cdot i) \;=\; 3\cdot 2+3\cdot 4+3\cdot 6\ .$$

3. Elle s'étend facilement au cas où il y a plus d'une variable de quantification :

$$(+i,j \mid 1\le i\le 2 \wedge 3\le j\le 4 : i^j) \;=\; 1^3+1^4+2^3+2^4$$

   La notation standard est $\sum_{i=1}^{2}\sum_{j=3}^{4} i^j$.

4. Surtout, la notation linéaire permet de démontrer des propriétés générales des quantificateurs. C'est le but de ce chapitre.

Forme générale de la quantification : $(\star x{:}t_1, y{:}t_2 \mid R : P)$

1. $\star$ est un opérateur commutatif, associatif, avec identité (élément neutre) u.

$$\begin{aligned} \textbf{Commutativité :}\quad & a\star b \;=\; b\star a \\ \textbf{Associativité :}\quad & (a\star b)\star c \;=\; a\star(b\star c) \\ \textbf{Identité } u\textbf{ :}\quad & u\star a \;=\; a \;=\; a\star u \end{aligned}$$

2. Les variables x et y sont distinctes. Ce sont les *variables de quantification*, ou encore, les *variables liées par la quantification*. Il peut y en avoir une ou plus.
3. t_1 et t_2 sont les types des variables de quantification. Si $t_1 = t_2$, on peut écrire $(\star x, y{:}t_1 \mid R : P)$. Les types sont souvent omis s'ils sont évidents selon le contexte.
4. R, une expression booléenne, est le *domaine* de quantification. Elle décrit les valeurs que peuvent prendre x et y. Abréviation : on peut écrire

$$(\star x{:}t \mid : P) \qquad \text{au lieu de} \qquad (\star x{:}t \mid \mathsf{vrai} : P)\ .$$

5. P, une expression, est le *corps* de la quantification.
6. Le type du résultat de la quantification est le type de P.
7. L'expression dénote l'application de $\star$ aux valeurs P telles que x et y satisfont R .

Quantification : exemples et notations

1. Exemples :

$$\begin{array}{rcl}
(+i \mid 0 \le i < 4 : i \cdot 8) & = & 0 \cdot 8 + 1 \cdot 8 + 2 \cdot 8 + 3 \cdot 8 \\
(\cdot\, i \mid 0 \le i < 3 : i + (i+1)) & = & (0 + (0+1)) \cdot (1 + (1+1)) \cdot (2 + (2+1)) \\
(\wedge j \mid 0 \le j < 2 : j \cdot d \neq 6) & \equiv & 0 \cdot d \neq 6 \ \wedge\ 1 \cdot d \neq 6 \\
(\vee k \mid 0 \le k < 21 : b[k] = 0) & \equiv & b[0] = 0 \ \vee\ \cdots\ \vee\ b[20] = 0
\end{array}$$

2. Notations communes (à gauche) :

$$\begin{array}{rcl}
\sum_{i=1}^{n} x_i & \text{pour} & (+i \mid 1 \le i \le n : x_i) \\
\forall i.\ 1 \le i \ \Rightarrow\ x_i = 0 & \text{pour} & (\wedge\, i \mid 1 \le i : x_i = 0) \\
(\forall i) 1 \le i \ \Rightarrow\ x_i = 0 & \text{pour} & (\wedge\, i \mid 1 \le i : x_i = 0) \\
\exists i : 1 \le i \ \wedge\ x_i = 0 & \text{pour} & (\vee\, i \mid 1 \le i : x_i = 0)
\end{array}$$

3. Nous céderons partiellement à la convention et utiliserons

$$\begin{array}{rcl}
(\sum x \mid R : P) & \text{au lieu de} & (+x \mid R : P) \\
(\prod x \mid R : P) & \text{au lieu de} & (\cdot\, x \mid R : P) \\
(\exists x \mid R : P) & \text{au lieu de} & (\vee x \mid R : P) \\
(\forall x \mid R : P) & \text{au lieu de} & (\wedge x \mid R : P)
\end{array}$$

(6.7) Exercice. Quelle est l'erreur dans l'expression suivante ?

$$(+k{:}\mathbb{N} \mid 0 \le k < n : k > x)$$

Occurrence d'une variable dans une expression

Occurrence : cas, circonstance (Petit Robert).

Une variable peut apparaître plusieurs fois dans une expression. Chaque apparition s'appelle une *occurrence*. Les apparitions des variables comprises entre un quantificateur et la barre verticale qui suit le quantificateur ne comptent pas comme des occurrences de ces variables.

(6.8) Exemple. Dans l'expression

$$s^2 + t + 5 = t + t^3 - s \ ,$$

la variable s a deux occurrences et la variable t a trois occurrences. Dans l'expression

$$\underline{i} \wedge (\forall i{:}\mathbb{N} \mid : x \cdot \underline{i} = 0) \ ,$$

la variable i a deux occurrences (elles sont soulignées) et la variable x en a une.

Portée d'une variable de quantification

Dans l'expression

$$(\star x{:}t \mid R : P) \ ,$$

la *portée* de la variable de quantification x (les endroits où elle peut apparaître) est l'expression du domaine et l'expression du corps. Plus simplement, la portée est tout ce qui se trouve entre les parenthèses. On parle aussi de la portée du quantificateur $\forall x$, plutôt que de la portée de la variable de quantification x.

(6.9) Exemple. Dans l'expression

$$(\forall j{:}\mathbb{Z} \mid j > 10 : (\forall i{:}\mathbb{N} \mid 5 \leq i \leq 25 : x \cdot i + j > 0)) \ ,$$

la portée de la variable de quantification j est tout ce qui se trouve entre les parenthèses externes et la portée de la variable i est tout ce qui se trouve entre les parenthèses internes.

Variables libres et variables liées

Une occurrence d'une variable x qui est dans la portée d'une variable de quantification x est dite *liée*. Si une occurrence d'une variable x n'est pas liée, elle est dite *libre*. Si une occurrence de x est liée, elle est dite *liée à la variable de quantification x* la plus rapprochée dans la portée de laquelle elle se trouve.

(6.10) Exemple. Dans les expressions suivantes, les occurrences libres des variables sont indiquées par une flèche ↑ . Les occurrences liées sont reliées à la variable de quantification qui les lie.

$$E_1 : \quad \underset{\uparrow}{i} \wedge (\forall i{:}\mathbb{N} \mid : \underset{\uparrow}{x} \cdot i = 0)$$

$$E_2 : \quad (\forall j{:}\mathbb{Z} \mid j > 10 : (\forall i{:}\mathbb{N} \mid 5 \leq i \leq 25 : \underset{\uparrow}{x} \cdot i + j > 0))$$

$$E_3 : \quad (\forall i{:}\mathbb{Z} \mid i > 10 : (\forall i{:}\mathbb{N} \mid 5 \leq i \leq 25 : \underset{\uparrow}{x} \cdot i + \underset{\uparrow}{j} > 0))$$

(6.11) Définition. On dit que la variable x est *libre* dans l'expression E ssi x a au moins une occurrence libre dans E ; on dit que x est *liée* dans E ssi x a au moins une occurrence liée dans E.

La notation « libre(‘v’,‘e’) » signifie *qu'au moins une* des variables de la liste v de variables a une occurrence libre dans *au moins une* des expressions de la liste d'expressions e. Notons qu'on ne peut évaluer une expression de la forme libre(‘v’,‘e’) tant qu'on n'a pas une liste explicite de variables et une expression concrète pour e.

(6.12) Exemple. Réutilisons les expressions de l'exemple 6.10.

1. La variable x est libre dans E_1, E_2 et E_3 :

   libre(‘x’,‘E_1’) libre(‘x’,‘E_2’) libre(‘x’,‘E_3’)

2. La variable i est libre dans E_1 : libre(‘i’,‘E_1’) .
   Elle est liée dans E_1, E_2, E_3 .
3. La variable j est libre dans E_3 : libre(‘j’,‘E_3’) .
   Elle est liée dans E_2 .

Considérons

$$(\forall i{:}\mathbb{N} \mid : x \cdot i = 0) \;=\; \Big(x \cdot 0 = 0 \;\wedge\; x \cdot 1 = 0 \;\wedge\; x \cdot 2 = 0 \;\wedge\; \cdots\Big) \; .$$

La quantification a la valeur vrai dans tout état tel que $x = 0$ et elle a la valeur faux sinon, c'est-à-dire

$$(\forall i{:}\mathbb{N} \mid : x \cdot i = 0) \;\equiv\; x = 0 \; .$$

La valeur de l'expression dépend de x, qui est libre dans l'expression, mais elle ne dépend pas de i, dont toutes les occurrences sont liées :

$$(\forall i{:}\mathbb{N} \mid : x \cdot i = 0) \;\equiv\; (\forall j{:}\mathbb{N} \mid : x \cdot j = 0) \; .$$

Nous introduirons plus tard un axiome qui permet de renommer les variables liées (c'est l'axiome (6.36)).

(6.13) Exercice. Dites si les occurrences des variables dans l'expression suivante sont libres ou liées. Si liées, dites à quelle variable de quantification. Quelles sont les variables libres ? les variables liées ?

$$a > 10 \ \wedge \ (\forall a, b \mid a \leq b + c : (\exists b, c \mid: f(a + b) = a^2) \ \wedge \ a = c^2)$$

Substitution textuelle pour les quantifications

(6.14) Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}x, F\text{'})$,

$$(\star y \mid R : P)[x := F] \quad = \quad (\star y \mid R[x := F] : P[x := F]) \ .$$

Si l'une des variables de la liste y est libre dans $\text{`}x, F\text{'}$, il faut remplacer cette variable par une variable nouvelle —c'est-à-dire une variable qui n'apparaît pas dans $\text{`}x, F\text{'}$— avant de faire la substitution.

(6.15) Exemple.

$$(\sum x \mid 1 \leq x \leq 2 : y)[y := y + z] \quad = \quad (\sum x \mid 1 \leq x \leq 2 : y + z)$$

$$(\forall i \mid 0 \leq i < n : b[i] = n)[n := m] \quad = \quad (\forall i \mid 0 \leq i < m : b[i] = m)$$

(6.16) Exercice. Faites les substitutions suivantes, si possible. Si ce n'est pas possible, dites pourquoi.

1. $(\exists k \mid \mathsf{pair}.k : k > x + y)[x := y + z]$
2. $(\exists k \mid \mathsf{pair}.k : k > x + y)[k := y + z]$
3. $(\exists k \mid \mathsf{pair}.k : k > x + y)[x := k + z]$

6.3 Lois de la quantification

(6.17) Leibniz :

(1) $$\frac{P = Q}{(\star x \mid E[z := P] : S) \;=\; (\star x \mid E[z := Q] : S)}$$

(2) $$\frac{R \;\Rightarrow\; P = Q}{(\star x \mid R : E[z := P]) \;=\; (\star x \mid R : E[z := Q])}$$

(3) $$\frac{P = Q}{(\star x \mid R : E[z := P]) \;=\; (\star x \mid R : E[z := Q])}$$

(4) $$\frac{P = Q}{(\star x \mid E[z := P] : F[z := P]) \;=\; (\star x \mid E[z := Q] : F[z := Q])}$$

– (3) est un cas particulier de (2), car si $P = Q$, alors $R \;\Rightarrow\; P = Q$.
– (4) est une combinaison de (1) et (3).

Exemple d'application de la règle de Leibniz (6.17)

$$\frac{x + x = 2 \cdot x}{(\sum x \mid 0 \le x < 9 : z[z := x + x]) \;=\; (\sum x \mid 0 \le x < 9 : z[z := 2 \cdot x])}$$

c'est-à-dire, après la substitution

$$\frac{x + x = 2 \cdot x}{(\sum x \mid 0 \le x < 9 : x + x) \;=\; (\sum x \mid 0 \le x < 9 : 2 \cdot x)}$$

(6.18) Remarque. Cette dernière règle (celle qui est encadrée) ne peut être obtenue avec la règle de Leibniz (1.13), à cause du renommage qu'il faut parfois faire lors de la substitution dans les quantifications. En effet,

$$\frac{x + x = 2 \cdot x}{(\sum x \mid 0 \le x < 9 : z)[z := x + x] \;=\; (\sum x \mid 0 \le x < 9 : z)[z := 2 \cdot x]}$$

donne

$$\frac{x + x = 2 \cdot x}{(\sum y \mid 0 \le y < 9 : x + x) \;=\; (\sum y \mid 0 \le y < 9 : 2 \cdot x)}$$

Axiomes de la quantification

(6.19) Axiome, domaine vide : $(\star x \mid \mathsf{faux} : P) = u$
(où u est l'élément neutre de $\star$) .

(6.20) Exemple. $(\sum i \mid 4 < i < 4 : i^2) \;=\; 0$.

(6.21) Axiome du point : Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}E\text{'})$,

$$(\star x \mid x = E : P) \;=\; P[x := E] \ .$$

(6.22) Exemple. $(\prod y \mid y = 5 : y + t) \;=\; 5 + t$.

(6.23) Axiome, distributivité : Pourvu que chaque quantification soit définie,

$$(\star x \mid R : P) \;\star\; (\star x \mid R : Q) \;=\; (\star x \mid R : P \star Q) \ .$$

(6.24) Exemple.

$$\begin{aligned} & (\prod y{:}\mathbb{N} \mid 1 \le y^2 \le 10 : y + t) \cdot (\prod y{:}\mathbb{N} \mid 1 \le y^2 \le 10 : y^2) \\ = \; & (\prod y{:}\mathbb{N} \mid 1 \le y^2 \le 10 : (y + t) \cdot y^2) \end{aligned}$$

Exemple de quantification non définie : $(\prod y{:}\mathbb{N} \mid 0 < y : y)$.

(6.25) Axiome, division du domaine : Pourvu que $R \wedge S \equiv \mathsf{faux}$ et que chaque quantification soit définie,

$$(\star x \mid R \vee S : P) \;=\; (\star x \mid R : P) \;\star\; (\star x \mid S : P) \ .$$

(6.26) Exemple.

$$\begin{aligned} & (\sum i \mid 0 \le i < 20 : i^2) \\ = \; & (\sum i \mid 0 \le i < 10 \;\vee\; 10 \le i < 20 : i^2) \\ = \; & (\sum i \mid 0 \le i < 10 : i^2) \;+\; (\sum i \mid 10 \le i < 20 : i^2) \end{aligned}$$

(6.27) Axiome, division du domaine (généralisation de (6.25)) : Pourvu que chaque quantification soit définie,

$$(\star x \mid R \vee S : P) \;\star\; (\star x \mid R \wedge S : P) \;=\; (\star x \mid R : P) \;\star\; (\star x \mid S : P) \ .$$

(6.28) Exemple.

$$
\begin{aligned}
& (\sum i \mid (0 \le i < 20) : i) \ + \ (\sum i \mid 5 \le i < 10 : i) \\
= \ & (\sum i \mid 0 \le i < 10 \ \vee \ 5 \le i < 20 : i) \ + \ (\sum i \mid 0 \le i < 10 \ \wedge \ 5 \le i < 20 : i) \\
= \ & (\sum i \mid 0 \le i < 10 : i) \ + \ (\sum i \mid 5 \le i < 10 : i)
\end{aligned}
$$

(6.29) Axiome, division du domaine si $\star$ est idempotent : Pourvu que chaque quantification soit définie,

$$(\star x \mid R \vee S : P) \ = \ (\star x \mid R : P) \ \star \ (\star x \mid S : P) \ .$$

En effet, si $\star$ est idempotent ($e \star e = e$), on peut répéter l'opération sans changer la valeur du résultat.

(6.30) Exemple.

$$
\begin{aligned}
& (\exists i \mid 0 \le i < 10 \ \vee \ 5 \le i < 20 : i^2 = 36) \\
= \ & (\exists i \mid 0 \le i < 10 : i^2 = 36) \ \vee \ (\exists i \mid 5 \le i < 20 : i^2 = 36)
\end{aligned}
$$

(6.31) Axiome, échange des variables de quantification : Pourvu que chaque quantification soit définie et que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R\text{'})$ et $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}Q\text{'})$,

$$(\star x \mid R : (\star y \mid Q : P)) \ = \ (\star y \mid Q : (\star x \mid R : P)) \ .$$

(6.32) Exemple.

$$
\begin{aligned}
& (\sum i{:}\mathbb{Z} \mid 1 \le i < 10 : (\sum x{:}\mathbb{Z} \mid x^2 \le 10 : x^i)) \\
= \ & (\sum x{:}\mathbb{Z} \mid x^2 \le 10 : (\sum i{:}\mathbb{Z} \mid 1 \le i < 10 : x^i))
\end{aligned}
$$

(6.33) Exercice. La loi (6.31) peut-elle être utilisée pour justifier l'équation suivante ?

$$(\prod i \mid i + j < 10 : (\prod j \mid j < 5 : j)) \ = \ (\prod j \mid j < 5 : (\prod i \mid i + j < 10 : j))$$

(6.34) Axiome, imbrication : Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R\text{'})$,

$$(\star x, y \mid R \wedge Q : P) \ = \ (\star x \mid R : (\star y \mid Q : P)) \ .$$

(6.35) Exemple.

$$
\begin{aligned}
& (\sum i, j \mid 0 \le i < 10 \ \wedge \ 0 \le j < 10 : i \cdot j) \\
= \ & (\sum i \mid 0 \le i < 10 : (\sum j \mid 0 \le j < 10 : i \cdot j))
\end{aligned}
$$

(6.36) Axiome, renommage des variables de quantification :
Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R, P\text{'})$,

$$(\star x \mid R : P) \;=\; (\star y \mid R[x := y] : P[x := y]) \ .$$

(6.37) Exemple.

$$(\prod i \mid 0 \le i < 10 : i + k) \;=\; (\prod j \mid 0 \le j < 10 : j + k)$$

(6.38) Exercice. Est-ce un renommage correct ?

$$(\sum k{:}\mathbb{N} \mid k^2 < 10 : k^2 + x) \;=\; (\sum x{:}\mathbb{N} \mid x^2 < 10 : x^2 + x)$$

Évaluez les deux sommes. Qu'en concluez-vous ?

Plusieurs des lois, par exemple l'axiome d'imbrication (6.34), ont une condition de la forme « Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$ ». Lorsque cette condition n'est pas satisfaite, il n'est pas possible d'appliquer la loi. Si on tient à l'appliquer, on peut parfois y arriver en utilisant l'axiome de renommage des variables de quantification (6.36) pour renommer la variable de quantification x. On choisit habituellement un nouveau nom de variable qui n'apparaît pas dans l'expression traitée. Supposons que cette variable soit z. Comme z est un nouveau nom de variable, il se peut qu'on ait $\neg\mathsf{libre}(\text{`}z\text{'},\text{`}P\text{'})$ et qu'on puisse appliquer la loi.

Appliquons cette démarche à un exemple concret. Supposons qu'on veuille appliquer l'axiome d'imbrication (6.34) à l'expression

$$(\sum i \mid 0 \le i < j : (\sum j \mid 0 \le j < 10 : i \cdot j))$$

(on veut désimbriquer). On ne peut appliquer l'axiome d'imbrication à cette expression, car $\mathsf{libre}(\text{`}j\text{'},\text{`}0 \le i < j\text{'})$. Renommons la variable j par la nouvelle variable k, qui n'apparaît pas dans l'expression ci-dessus. Comme c'est une nouvelle variable, on obtient automatiquement la précondition de l'axiome de renommage (6.36), soit dans ce cas-ci

$$\neg\mathsf{libre}(\text{`}k\text{'},\text{`}0 \le j < 10, i \cdot j\text{'}).$$

L'expression obtenue par renommage est

$$(\sum i \mid 0 \le i < j : (\sum k \mid 0 \le k < 10 : i \cdot k)).$$

On a maintenant $\neg\mathsf{libre}(\text{`}k\text{'},\text{`}0 \le i < j\text{'})$, de sorte qu'on peut appliquer l'axiome d'imbrication et obtenir

$$(\sum i, k \mid 0 \le i < j \ \wedge \ 0 \le k < 10 : i \cdot k).$$

Généralisation de l'axiome de renommage (6.36)

Nous voulons pouvoir faire des transformations comme

$$(\sum i \mid 2 \le i \le 10 : i^2) \;=\; (\sum k \mid 0 \le k \le 8 : (k+2)^2) \ ,$$

c'est-à-dire un renommage des variables de quantification accompagné d'une transformation des expressions. Les variables i et k sont reliées ainsi :

$$i = k + 2 \qquad \text{ou encore} \qquad k = i - 2 \ .$$

En posant $f.x = x + 2$, on a $i = f.k$. La fonction f a un inverse, qu'on note f^{-1}. Ici, $f^{-1}.y = y - 2$. Les fonctions f et f^{-1} sont reliées par la propriété

$$\boxed{y = f.x \ \equiv \ x = f^{-1}.y}$$

Il est facile de montrer $f(f^{-1}.y) = y$ et $f^{-1}(f.x) = x$.

Exemple de fonctions qui n'ont pas d'inverse : $f.x = x \cdot 0$, $g.x = \sin .x$.

(6.39) Changement des variables de quantification : Pourvu que f ait un inverse et que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R, P\text{'})$,

$$(\star x \mid R : P) \ = \ (\star y \mid R[x := f.y] : P[x := f.y]) \ .$$

6.4 Manipulation des domaines

(6.40) Théorème, extraction d'un terme : Soit $n{:}\mathbb{N}$.

$$(\star i{:}\mathbb{N} \mid k \le i < n+1 : P) \ = \ (\star i{:}\mathbb{N} \mid k \le i < n : P) \ \star \ P[i := n]$$
$$(\star i{:}\mathbb{N} \mid k \le i < n+1 : P) \ = \ P[i := k] \ \star \ (\star i{:}\mathbb{N} \mid k < i < n+1 : P)$$

Exemple :

$$(\forall i \mid 0 \le i < n+1 : b[i] = 0) \ = \ (\forall i \mid 0 \le i < n : b[i] = 0) \ \wedge \ b[n] = 0$$
$$(\textstyle\prod i \mid 5 \le i \le 10 : i^2) \ = \ 5^2 \cdot (\textstyle\prod i \mid 5 < i \le 10 : i^2)$$

Démonstration. (le type $\mathbb{N}$ est omis)

$$\begin{array}{ll} & (\star i \mid 0 \le i < n+1 : P) \\ = & \qquad \langle \ 0 \le i < n+1 \ \equiv \ 0 \le i < n \ \vee \ i = n \ \rangle \\ & (\star i \mid 0 \le i < n \ \vee \ i = n : P) \\ = & \qquad \langle \text{ Division du domaine (6.25) — } 0 \le i < n \ \wedge \ i = n \ \equiv \ \mathsf{faux} \ \rangle \\ & (\star i \mid 0 \le i < n : P) \ \star \ (\star i \mid i = n : P) \\ = & \qquad \langle \ \textit{Axiome} \text{ du point (6.21)} \ \rangle \\ & (\star i \mid 0 \le i < n : P) \ \star \ P[i := n] \end{array}$$

6.5 Problèmes

1. Voici les types de cinq fonctions a, b, c, d et e :

   $$a{:}A \to B \qquad b{:}B \to C \qquad c{:}C \to A \qquad d{:}A \times C \to D \qquad e{:}B \times B \to E$$

   Dites si les expressions ci-dessous sont bien typées. Si une expression est bien typée, donnez son type (c'est-à-dire le type du résultat). Dans le cas contraire, expliquez pourquoi elle est mal typée. Supposez $u{:}A$, $w{:}B$, $x{:}C$, $y{:}D$ et $z{:}E$.

   (a) $e(a.u, w)$

   (b) $b.x$

   (c) $e(a(c.x), a.u)$

   (d) $a(c(b(a.y)))$

   (e) $d(c.x, c.x)$

2. Effectuez les substitutions textuelles suivantes. Si nécessaire, renommez la variable de quantification en utilisant la loi (6.36).

   (a) $(\star x \mid 0 \le x + r < n : x + v)[v := 3]$

   (b) $(\star x \mid 0 \le x < r : (\star y \mid 0 \le y : x + y + n))[n := x + y]$

   (c) $(\star x \mid 0 \le x < r : (\star y \mid 0 \le y : x + y + n))[r := y]$

3. Démontrez le théorème suivant, dans lequel $0 \le n$.

   $$(\sum i \mid 0 \le i < n + 1 : b[i]) \;=\; b[0] + (\sum i \mid 1 \le i < n + 1 : b[i])$$

4. Démontrez le théorème suivant, dans lequel $0 \le n$.

   $$(\wedge i \mid 0 \le i < n + 1 : b[i] = 0) \;\equiv\; b[0] = 0 \;\wedge\; (\wedge i \mid 0 < i < n + 1 : b[i] = 0)$$

5. Démontrez le théorème suivant.

   $$(+i \mid 0 \le i \le n : i) \;=\; (+i \mid 0 \le i \le n \wedge \mathsf{pair}.i : i) \;+\; (+i \mid 0 \le i \le n \wedge \mathsf{impair}.i : i)$$

Chapitre 7

Le calcul des prédicats

La logique des prédicats

C'est une extension de la logique propositionnelle qui permet l'usage de variables de types autres que $\mathbb{B}$. Cette extension accroît la puissance de la logique.

Formules de la logique des prédicats

Ce sont des expressions booléennes dans lesquelles certaines variables booléennes sont remplacées par l'un des items suivants :

- Des *prédicats*, c'est-à-dire des applications de fonctions booléennes à des arguments de types autres que $\mathbb{B}$. Voici des exemples de prédicats :
  - $\mathsf{égale}(x, 5)$, normalement écrit en notation infixe $x = 5$,
  - $\mathsf{plus\text{-}petit\text{-}que}(x, y + 5)$, normalement écrit en notation infixe $x < y + 5$.
- Des quantifications universelles ou existentielles.

Exemple de formule : $x < y \wedge x = z \;\Rightarrow\; q(x, z + x)$.

Axiomatisation de la logique des prédicats

Axiomes : ceux de la logique propositionnelle + axiomes des quantifications.
Règles : substitution (1.9), transitivité (1.12), Leibniz (1.13), (6.17).

7.1 Quantification existentielle

La disjonction $\vee$ est
- associative
- commutative
- a faux comme élément neutre.

On peut donc l'utiliser comme quantificateur : $(\vee x \mid R : P)$. Nous écrirons :

$$(\exists x \mid R : P).$$

Prononciations possibles :
- *il existe x dans le domaine R tel que P*,
- *il existe un x satisfaisant R tel que P*,
- *il existe un x satisfaisant R et P*,
- *il existe un x tel que R et P*.

Par exemple,

$(\exists x \mid x \geq 0 : x - a = 0)$,
il existe un x satisfaisant $x \geq 0$ tel que $x - a = 0$,
plus simplement : il existe un x plus grand ou égal à zéro tel que $x - a = 0$.

L'opérateur $\exists$ est appelé *quantificateur existentiel*. Il satisfait les lois de l'opérateur $\star$ du chapitre 6. En particulier, puisque $\vee$ est idempotent, $\exists$ satisfait l'axiome de division du domaine (6.29).

Transfert pour quantification existentielle

(7.1) Axiome, transfert : $(\exists x \mid R : P) \equiv (\exists x \mid : R \wedge P)$

Théorème de transfert pour $\exists$

(7.2) Transfert : $(\exists x \mid Q \wedge R : P) \equiv (\exists x \mid Q : R \wedge P)$

(7.3) Exercice. Démontrez la loi de transfert (7.2).

Distributivité et quantification existentielle

(7.4) Axiome, distributivité de $\wedge$ sur $\exists$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$$

(7.5) Exercice. L'expression suivante est-elle un théorème ?

$$x = 0 \wedge (\exists x{:}\mathbb{N} \mid : x > 0) \equiv (\exists x{:}\mathbb{N} \mid : x = 0 \wedge x > 0)$$

(7.6) Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$(\exists x \mid R : P) \equiv P \wedge (\exists x \mid : R)$$

(7.7) Distributivité de $\vee$ sur $\exists$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$(\exists x \mid : R) \Rightarrow \big((\exists x \mid R : P \vee Q) \equiv P \vee (\exists x \mid R : Q)\big)$$

(7.8) $(\exists x \mid R : \mathsf{faux}) \equiv \mathsf{faux}$

Manipulation du domaine et du corps

(7.9) Affaiblissement/renforcement du domaine :

$$(\exists x \mid R : P) \Rightarrow (\exists x \mid Q \vee R : P)$$

(7.10) Exercice. Évaluez les expressions suivantes.

$$(\exists x{:}\mathbb{R} \mid x < -1 : x \neq 0) \Rightarrow (\exists x{:}\mathbb{R} \mid x < -1 \vee x > 1 : x \neq 0)$$
$$(\exists x{:}\mathbb{R} \mid x < -1 : x > 0) \Rightarrow (\exists x{:}\mathbb{R} \mid x < -1 \vee x > 1 : x > 0)$$

(7.11) Affaiblissement/renforcement du corps :

$$(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$$

Introduction de $\exists$

(7.12) $\exists$-Introduction : $P[x := E] \Rightarrow (\exists x \mid : P)$

(7.13) Exemple. La formule $x > 5 \Rightarrow (\exists y \mid : x > y)$ découle directement de ce théorème, car

$$\begin{array}{ll} & x > 5 \\ = & \quad \langle \text{ Substitution } \rangle \\ & (x > y)[y := 5] \\ \Rightarrow & \quad \langle \exists\text{-Introduction (7.12)} \rangle \\ & (\exists y \mid : x > y) \end{array}$$

7.2 Quantification universelle

La conjonction $\wedge$ est
- associative
- commutative
- a vrai comme élément neutre.

On peut donc l'utiliser comme quantificateur : $(\wedge x \mid R : P)$. Nous écrirons :

$$(\forall x \mid R : P).$$

Prononciations possibles :
- *pour tout x satisfaisant R, P est satisfait*,
- *tout x satisfaisant R satisfait aussi P*,
- *quel que soit x, si R alors P*,
- *pour tout x tel que R, P*.

Par exemple,

$(\forall i \mid i > 10 : i^2 > 100)$,
pour tout i tel que i est plus grand que 10, i^2 est plus grand que 100.

L'opérateur $\forall$ est appelé *quantificateur universel*. Il satisfait les lois de l'opérateur $\star$ du chapitre 6. En particulier, puisque $\wedge$ est idempotent, $\forall$ satisfait l'axiome de division du domaine (6.29).

(7.14) Exercice. Vrai ou faux ?

$$(\forall n \mid 0 \leq n < 0 : 2 = 3)$$

Généralisation des lois de De Morgan

(7.15) Axiome, De Morgan : $(\forall x \mid R : P) \equiv \neg(\exists x \mid R : \neg P)$

Cette loi est une généralisation de $p \wedge q \equiv \neg(\neg p \vee \neg q)$.

(7.16) De Morgan :
(a) $(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$
(b) $(\forall x \mid R : \neg P) \equiv \neg(\exists x \mid R : P)$
(c) $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$

Théorèmes de transfert pour $\forall$

(7.17) Transfert :
(a) $(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$
(b) $(\forall x \mid R : P) \equiv (\forall x \mid : \neg R \vee P)$
(c) $(\forall x \mid R : P) \equiv (\forall x \mid : R \wedge P \equiv R)$
(d) $(\forall x \mid R : P) \equiv (\forall x \mid : R \vee P \equiv P)$

Dans (7.17a), notez la différence avec l'axiome de transfert pour $\exists$ (7.1) : au lieu de $R \wedge P$, on a $R \Rightarrow P$. Ceci correspond bien à la manière de lire la quantification universelle. En effet, « pour tout x satisfaisant R, P est satisfait », c'est la même chose que « pour tout x, si R alors P ».

(7.18) Exercice. Démontrez la loi de transfert (7.17a).

(7.19) Exercice. Démontrez le théorème (7.17b).

(7.20) Transfert :
$$\begin{array}{lll} \text{(a)} & (\forall x \mid Q \wedge R : P) & \equiv \ (\forall x \mid Q : R \Rightarrow P) \\ \text{(b)} & (\forall x \mid Q \wedge R : P) & \equiv \ (\forall x \mid Q : \neg R \vee P) \\ \text{(c)} & (\forall x \mid Q \wedge R : P) & \equiv \ (\forall x \mid Q : R \wedge P \equiv R) \\ \text{(d)} & (\forall x \mid Q \wedge R : P) & \equiv \ (\forall x \mid Q : R \vee P \equiv P) \end{array}$$

Distributivité et quantification universelle

Les théorèmes suivants correspondent aux théorèmes correspondants pour $\exists$.

(7.21) Distributivité de $\vee$ sur $\forall$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,
$$P \vee (\forall x \mid R : Q) \ \equiv \ (\forall x \mid R : P \vee Q)$$

(7.22) Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,
$$(\forall x \mid R : P) \ \equiv \ P \vee (\forall x \mid : \neg R)$$

(7.23) Distributivité de $\wedge$ sur $\forall$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,
$$(\exists x \mid : R) \ \Rightarrow \ \big((\forall x \mid R : P \wedge Q) \ \equiv \ P \wedge (\forall x \mid R : Q)\big)$$

(7.24) $(\forall x \mid R : \mathsf{vrai}) \ \equiv \ \mathsf{vrai}$

(7.25) Exercice. Évaluez l'expression suivante.
$$(\forall n{:}\mathbb{Z} \mid : n > 0 \equiv n^3 > 0) \ \Rightarrow \ ((\forall n{:}\mathbb{Z} \mid : n > 0) \ \equiv \ (\forall n{:}\mathbb{Z} \mid : n^3 > 0))$$

(7.26) $(\forall x \mid R : P \equiv Q) \ \Rightarrow \ \big((\forall x \mid R : P) \ \equiv \ (\forall x \mid R : Q)\big)$

Manipulation du domaine et du corps

Les théorèmes suivants ressemblent aux théorèmes correspondants pour $\exists$.

(7.27) Affaiblissement/renforcement du domaine :
$$(\forall x \mid Q \vee R : P) \ \Rightarrow \ (\forall x \mid Q : P)$$

(7.28) Exercice. Évaluez l'expression suivante.

$$(\forall x{:}\mathbb{R} \mid x < -1 \vee x > 1 : x \neq 0) \;\Rightarrow\; (\forall x{:}\mathbb{R} \mid x < -1 : x \neq 0)$$

(7.29) Affaiblissement/renforcement du corps :

$$(\forall x \mid R : P \wedge Q) \;\Rightarrow\; (\forall x \mid R : P)$$

Élimination du quantificateur universel

(7.30) Élimination : $(\forall x \mid : P) \;\Rightarrow\; P[x := E]$

(7.31) Exemple. La quantification suivante est une loi de l'arithmétique :

(7.32) $(\forall i{:}\mathbb{Z} \mid : \mathsf{pair}.i \equiv \mathsf{pair}(i^2))$

Démontrons

$$B \vee \mathsf{pair}(x+y) \;\equiv\; B \vee \mathsf{pair}((x+y)^2)$$

vrai —(3.6)

$=$ ⟨ (7.32) & Métathéorème (3.100) & vrai est un théorème (3.6) ⟩

$(\forall i{:}\mathbb{Z} \mid : \mathsf{pair}.i \equiv \mathsf{pair}(i^2))$

$\Rightarrow$ ⟨ (7.30), avec $x, P, E := i,\ \mathsf{pair}.i \equiv \mathsf{pair}(i^2),\ x+y$ ⟩

$\big(\mathsf{pair}.i \equiv \mathsf{pair}(i^2)\big)[i := x+y]$

$=$ ⟨ Substitution ⟩

$\mathsf{pair}(x+y) \;\equiv\; \mathsf{pair}((x+y)^2)$

et donc $B \vee \mathsf{pair}(x+y) \;\equiv\; B \vee \mathsf{pair}((x+y)^2)$.

Présentation standard :

$$\begin{array}{ll} & B \vee \mathsf{pair}(x+y) \\ = & \quad \langle \quad (7.32), \\ & \quad (7.30) \ \rangle \\ & B \vee \mathsf{pair}((x+y)^2) \end{array}$$

Métathéorème sur la quantification universelle

(7.33) Métathéorème : P est un théorème ssi $(\forall x \mid : P)$ est un théorème.

Voici une démonstration pour le cas particulier où l'expression P est

$$x^2 + 2 \cdot x + 2 \;=\; (x+1)^2 + 1.$$

($\Rightarrow$) À voir : si P est un théorème, alors $(\forall x \mid : P)$ est un théorème. Si P est un théorème, c'est qu'il y a une preuve de P. Par exemple :

$$
\begin{array}{ll}
& x^2 + 2 \cdot x + 2 \;=\; (x+1)^2 + 1 \\
= & \qquad \langle\ 2 = 1 + 1\ \rangle \\
& (x^2 + 2 \cdot x + 1) + 1 \;=\; (x+1)^2 + 1 \\
= & \qquad \langle\ x^2 + 2 \cdot x + 1 = (x+1)^2\ \rangle \\
& (x+1)^2 + 1 \;=\; (x+1)^2 + 1 \\
= & \qquad \langle\ \text{Réflexivité de l'égalité (1.10), avec } x := (x+1)^2 + 1\ \rangle \\
& \mathsf{vrai} \qquad \text{—(3.4)}
\end{array}
$$

Cette preuve peut être transformée en une preuve de $(\forall x \mid\!: P)$ utilisant les mêmes justifications. Cette preuve utilise de manière implicite la règle de Leibniz (6.17).

$$
\begin{array}{ll}
& (\forall x \mid\!: x^2 + 2 \cdot x + 2 \;=\; (x+1)^2 + 1) \\
= & \qquad \langle\ 2 = 1 + 1\ \rangle \\
& (\forall x \mid\!: (x^2 + 2 \cdot x + 1) + 1 \;=\; (x+1)^2 + 1) \\
= & \qquad \langle\ x^2 + 2 \cdot x + 1 = (x+1)^2\ \rangle \\
& (\forall x \mid\!: (x+1)^2 + 1 \;=\; (x+1)^2 + 1) \\
= & \qquad \langle\ \text{Réflexivité de l'égalité (1.10)}\ \rangle \\
& (\forall x \mid\!: \mathsf{vrai}) \\
= & \qquad \langle\ (7.24)\ \rangle \\
& \mathsf{vrai} \qquad \text{—(3.4)}
\end{array}
$$

($\Leftarrow$) À voir : si $(\forall x \mid\!: P)$ est un théorème, alors P est un théorème. Ceci découle directement de (7.30), avec $E := x$, et de la règle du modus ponens, en notant que $P[x := x] = P$:

$$\frac{(\forall x \mid\!: P), \qquad (\forall x \mid\!: P) \Rightarrow P[x := x]}{P[x := x]}$$

7.3 Monotonie et échange des quantificateurs

Monotonie du quantificateur universel

(7.34) Monotonie de $\forall$:

$$(\forall x \mid R : Q \Rightarrow P) \;\Rightarrow\; \big((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P)\big)$$

Remarquez que cette propriété est une généralisation de la monotonie de la conjonction (4.3).

Une loi analogue en arithmétique est

$$(\forall i \mid R : a_i \le b_i) \;\Rightarrow\; \big((\textstyle\prod i \mid R : a_i) \le (\prod i \mid R : b_i)\big).$$

(7.35) Exercice. Évaluez l'expression suivante.

$$(\forall x{:}\mathbb{R} \mid{:}\ x^2 \geq 0 \Rightarrow x^2+1>0) \ \Rightarrow\ ((\forall x{:}\mathbb{R} \mid{:}\ x^2 \geq 0) \ \Rightarrow\ (\forall x{:}\mathbb{R} \mid{:}\ x^2+1>0))$$

Monotonie du quantificateur existentiel

(7.36) Monotonie de $\exists$:

$$(\forall x \mid R : Q \Rightarrow P) \ \Rightarrow\ \big((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P)\big)$$

Remarquez que cette propriété est une généralisation de la monotonie de la disjonction (4.2). C'est bien un $\forall$ qui va dans l'antécédent, tout comme pour la monotonie de $\forall$.

Une loi analogue en arithmétique est

$$(\forall i \mid R : a_i \leq b_i) \ \Rightarrow\ \big((\textstyle\sum i \mid R : a_i) \leq (\sum i \mid R : b_i)\big).$$

Échange des quantificateurs

(7.37) Échange de $\forall, \exists$: Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R\text{'})$ et $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}Q\text{'})$,

$$(\exists x \mid R : (\forall y \mid Q : P)) \ \Rightarrow\ (\forall y \mid Q : (\exists x \mid R : P))$$

Par exemple, il existe un x tel que pour tout y, $x \cdot y = 0$

implique pour tout y, il existe un x tel que $x \cdot y = 0$.

La loi contient une implication et l'implication inverse ne tient pas. Par exemple,

pour tout $y{:}\mathbb{Z}$, il existe un $x{:}\mathbb{Z}$ tel que $x + y = 0$

est un théorème, mais pas

il existe un $x{:}\mathbb{Z}$ tel que pour tout $y{:}\mathbb{Z}$, $x + y = 0$.

7.4 Du français à la logique des prédicats

Voici quelques exemples de traduction du français en logique des prédicats.

1. Il y a un entier compris entre 80 et n qui est en même temps un multiple de x :

$$(\exists i{:}\mathbb{Z} \mid 80 \leq i \leq n : \mathsf{mult}(i, x))$$

où $\mathsf{mult}(i, x)$ exprime que i est un multiple de x. Notez qu'il faut en général introduire des prédicats (comme mult). La formalisation nous a forcés à décider ce que signifie exactement « entre 80 et n ». Il est aussi possible de formaliser $\mathsf{mult}(i, x)$:

$$(\exists m{:}\mathbb{Z} \mid : i = m \cdot x) \ .$$

2. Tous les entiers pairs sont des multiples de 2 :

$$(\forall x{:}\mathbb{Z} \mid \mathsf{pair}.x : \mathsf{mult}(x, 2))$$

3. Chaque chapitre a au moins 3 pages :

$$(\forall c{:}\mathsf{Chap} \mid : \mathsf{nb\_pages}.c \geq 3) \ ,$$

où Chap est l'ensemble des chapitres.

4. Les entiers pairs sont des multiples de 2 (sous-entendu : tous les entiers pairs sont des multiples de 2) :

$$(\forall x{:}\mathbb{Z} \mid \mathsf{pair}.x : \mathsf{mult}(x, 2))$$

La phrase « un entier pair est un multiple de 2 » a la même traduction.

5. Il existe un nombre naturel pair qui est divisible par 3 :

$$(\exists x{:}\mathbb{N} \mid \mathsf{pair}.x : \mathsf{divisible}(x, 3))$$

ou encore

$$(\exists x{:}\mathbb{N} \mid : \mathsf{pair}.x \wedge \mathsf{divisible}(x, 3))$$

6. Il y a un chapitre avec un nombre pair de pages :

$$(\exists c{:}\mathsf{Chap} \mid : \mathsf{pair}(\mathsf{nb\_page}.c))$$

7. Les entiers ne sont pas tous pairs

$=$ ⟨ Formalisation ⟩

$\neg(\forall z{:}\mathbb{Z} \mid : \mathsf{pair}.z)$

$=$ ⟨ De Morgan (7.16c) ⟩

$(\exists z{:}\mathbb{Z} \mid : \neg\mathsf{pair}.z)$

$=$ ⟨ Retour au français ⟩

Il y a un entier qui n'est pas pair

8. Chaque étudiant en informatique a pris un cours de mathématiques et a réussi un cours de programmation.
   Définition des prédicats :

   $\mathsf{pris}(e,c)$: l'étudiant e a pris le cours c
   $\mathsf{réussi}(e,c)$: l'étudiant e a réussi le cours c
   $\mathsf{info}(e)$: l'étudiant e est en informatique
   $\mathsf{math}(c)$: le cours c est un cours de mathématiques
   $\mathsf{prog}(c)$: le cours c est un cours de programmation

   Soient les types

   C : l'ensemble des cours ,
   E : l'ensemble des étudiants .

   La formule qui correspond à la phrase est alors

   $$(\forall e{:}\mathsf{E} \mid \mathsf{info}.e : (\exists c, c'{:}\mathsf{C} \mid{:}\ \mathsf{math}.c \wedge \mathsf{pris}(e,c) \wedge \mathsf{prog}.c' \wedge \mathsf{réussi}(e,c'))) \ ,$$

   ou encore

   $$(\forall e{:}\mathsf{E} \mid \mathsf{info}.e : (\exists c{:}\mathsf{C} \mid{:}\ \mathsf{math}.c \wedge \mathsf{pris}(e,c)) \ \wedge \ (\exists c{:}\mathsf{C} \mid{:}\ \mathsf{prog}.c \wedge \mathsf{réussi}(e,c))) \ ,$$

   ou encore (pas très mnémonique)

   $$(\forall t{:}\mathsf{E} \mid \mathsf{info}.t : (\exists a{:}\mathsf{C} \mid{:}\ \mathsf{math}.a \wedge \mathsf{pris}(t,a)) \ \wedge \ (\exists b{:}\mathsf{C} \mid{:}\ \mathsf{prog}.b \wedge \mathsf{réussi}(t,b))) \ .$$

(7.38) Exercice. Démontrez la propriété suivante.

$$\begin{array}{ll} & (\exists c{:}\mathsf{C} \mid{:}\ \mathsf{math}.c \wedge \mathsf{pris}(e,c)) \ \wedge \ (\exists c{:}\mathsf{C} \mid{:}\ \mathsf{prog}.c \wedge \mathsf{réussi}(e,c)) \\ = & (\exists c, c'{:}\mathsf{C} \mid{:}\ \mathsf{math}.c \wedge \mathsf{pris}(e,c) \wedge \mathsf{prog}.c' \wedge \mathsf{réussi}(e,c')) \end{array}$$

7.5 Problèmes

(7.39) Remarque. Plusieurs axiomes et théorèmes du chapitre 6 viennent avec la précondition « pourvu que chaque quantification soit définie ». Les quantifications universelles et existentielles sont toujours définies, même si les domaines sont infinis, de sorte qu'il n'est pas nécessaire de faire cette vérification pour ces quantifications booléennes.

1. Démontrez que la distributivité de $\wedge$ sur $\exists$ (7.4), c'est-à-dire $P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$ —pourvu que x ne soit pas libre dans P, ce qui, rappelons-le, signifie qu'il n'y a pas d'*occurrence* libre de x dans P— découle d'une expression similaire avec tous les domaines vrai : $P \wedge (\exists x \mid{:}\ Q) \equiv (\exists x \mid{:}\ P \wedge Q)$ (pourvu que x ne soit pas libre dans P). Ceci signifie que nous aurions pu utiliser un axiome plus simple.

2. Puisque $\vee$ est idempotent, la règle Division du domaine pour opérateur $\star$ idempotent (6.29) s'applique et donne

$$(\exists x \mid Q \vee R : P) \;\equiv\; (\exists x \mid Q : P) \;\vee\; (\exists x \mid R : P).$$

   Cependant, il est possible de démontrer cette expression sans utiliser l'axiome (6.29). Développez une telle preuve. Il peut s'avérer utile d'amener Q et R dans le corps de la quantification.

3. Démontrez la loi Affaiblissement/renforcement du corps (7.11), c'est-à-dire

$$(\exists x \mid R : P) \;\Rightarrow\; (\exists x \mid R : P \vee Q).$$

   La distributivité de $\exists$ sur $\vee$ peut être utile.

4. Démontrez le théorème (7.20a), c'est-à-dire

$$(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : R \Rightarrow P).$$

5. Démontrez la loi (7.24), c'est-à-dire $(\forall x \mid R : \mathsf{vrai}) \;\equiv\; \mathsf{vrai}$.

6. Démontrez que si x n'est pas libre dans Q,

$$(\exists x \mid : R) \;\Rightarrow\; \big((\forall x \mid R : P) \;\Rightarrow\; Q \;\equiv\; (\exists x \mid R : P \Rightarrow Q)\big).$$

7. Traduisez les phrases suivantes en logique des prédicats.
   (a) Un cube d'entier n'est jamais pair. (Utilisez seulement l'addition et la multiplication ; n'utilisez pas la division, mod, ou des prédicats comme $\mathsf{pair}.x$ ou $\mathsf{impair}.x$.)
   (b) Aucun entier n'est plus grand que tous les autres.

8. Traduisez les formules suivantes en français. Ce faisant, ne faites pas qu'une simple traduction littérale ; essayez plutôt d'extraire la signification de chaque formule et de l'exprimer de manière naturelle en français.
   (a) $(\forall x{:}\mathbb{R} \mid x \neq m : f.x > f.m)$
   (b) $(\forall z{:}\mathbb{Z} \mid \mathsf{pair}.z : (\exists w{:}\mathbb{Z} \mid \mathsf{impair}.w : z = w + 1))$

9. Formalisez les phrases suivantes en logique des prédicats.
   (a) Tout le monde aime quelqu'un.
   (b) Il y a quelqu'un qui aime quelqu'un.
   (c) Tout le monde aime tout le monde.
   (d) Personne n'aime tout le monde.
   (e) Il y a quelqu'un qui n'aime personne.

Chapitre 8

Induction mathématique

8.1 Induction sur les nombres naturels

La technique de *preuve par induction* (aussi dite de *preuve par récurrence*) permet de démontrer des propriétés de certains types d'ensembles infinis.

Soit le prédicat P défini par

(8.1) $P.n: \quad (\sum i \mid 1 \leq i \leq n : 2 \cdot i - 1) \;=\; n^2$

Notez que n est libre dans P. La notation $P.n$ indique que l'on considère P comme une fonction de n.

Ce qui suit est une vérification de (8.1) pour $n \leq 4$.

n	$(\sum i \mid 1 \leq i \leq n : 2 \cdot i - 1)$	n^2
0	0	0
1	1	1
2	$1+3$	4
3	$1+3+5$	9
4	$1+3+5+7$	16
$\vdots$	$\vdots$	$\vdots$

Nous voulons montrer que $P.n$ (qu'on appelle le *prédicat d'induction*) est vrai pour tout n. Autrement dit, nous voulons montrer

$$(\forall n{:}\mathbb{N} \mid : P.n) \ .$$

Pour notre problème, c'est

$$(\forall n{:}\mathbb{N} \mid : (\sum i \mid 1 \leq i \leq n : 2 \cdot i - 1) \;=\; n^2) \ .$$

La preuve est faite au moyen de l'*axiome d'induction* suivant :

(8.2) Induction mathématique (faible) sur $\mathbb{N}$:

$$\underline{P.0} \;\wedge\; \underline{(\forall n{:}\mathbb{N} \mid{:}\; P.n \;\Rightarrow\; P(n+1))} \;\Rightarrow\; \underline{(\forall n{:}\mathbb{N} \mid{:}\; P.n)}$$

Selon cet axiome, pour prouver $(\forall n{:}\mathbb{N} \mid{:}\; P.n)$, il suffit de procéder en deux étapes :

1. *Étape de base :* Démontrer $P.0$.
2. *Étape d'induction :* Démontrer $(\forall n{:}\mathbb{N} \mid{:}\; P.n \;\Rightarrow\; P(n+1))$. Dans ce contexte, l'expression $P.n$ est appelée l'*hypothèse d'induction*.

La dérivation suivante montre pourquoi le fait que $(\forall n{:}\mathbb{N} \mid{:}\; P.n)$ est un théorème découle de l'axiome d'induction (8.2) et de la preuve de

$$P.0 \qquad \text{et} \qquad (\forall n{:}\mathbb{N} \mid{:}\; P.n \;\Rightarrow\; P(n+1)) :$$

$$\begin{array}{ll}
 & P.0 \;\wedge\; (\forall n{:}\mathbb{N} \mid{:}\; P.n \;\Rightarrow\; P(n+1)) \;\Rightarrow\; (\forall n{:}\mathbb{N} \mid{:}\; P.n) \qquad \text{—(8.2)} \\
= & \qquad \langle\ \text{Preuves du cas de base et de l'hypothèse d'induction} \;\;\&\;\; \\
 & \qquad\ \ \mathsf{vrai} \text{ est un théorème (3.6)} \;\;\&\;\; \text{Métathéorème (3.100)}\ \rangle \\
 & \mathsf{vrai} \;\wedge\; \mathsf{vrai} \;\Rightarrow\; (\forall n{:}\mathbb{N} \mid{:}\; P.n) \\
= & \qquad \langle\ \text{Identité de } \wedge \text{ (3.52), avec } p := \mathsf{vrai}\ \rangle \\
 & \mathsf{vrai} \;\Rightarrow\; (\forall n{:}\mathbb{N} \mid{:}\; P.n) \\
= & \qquad \langle\ \text{Identité à gauche de } \Rightarrow \text{ (3.89), avec } p := (\forall n{:}\mathbb{N} \mid{:}\; P.n)\ \rangle \\
 & (\forall n{:}\mathbb{N} \mid{:}\; P.n)
\end{array}$$

Justification intuitive de l'axiome d'induction (8.2)

Supposons que

$$P.0$$
$$\text{et} \quad (\forall n{:}\mathbb{N} \mid{:}\; P.n \;\Rightarrow\; P(n+1))$$

aient été démontrés. Considérons les valeurs successives de n et les expressions correspondantes $P.n \;\Rightarrow\; P(n+1)$.

n	$P.n \;\Rightarrow\; P(n+1)$	Conclusion
0	$P.0 \;\Rightarrow\; P.1$	$P.1$ (puisque $P.0$ par hypothèse)
1	$P.1 \;\Rightarrow\; P.2$	$P.2$ (puisque $P.1$)
2	$P.2 \;\Rightarrow\; P.3$	$P.3$ (puisque $P.2$)
3	$P.3 \;\Rightarrow\; P.4$	$P.4$ (puisque $P.3$)
4	$P.4 \;\Rightarrow\; P.5$	$P.5$ (puisque $P.4$)
$\vdots$	$\vdots \;\Rightarrow\; \vdots$	$\vdots \qquad \vdots \qquad \vdots$

On voit comment nous pourrions démontrer $P.k$, pour un $k \in \mathbb{N}$ arbitraire, en un nombre fini d'étapes. Il est donc raisonnable de conclure que

$$(\forall n{:}\mathbb{N} \mid{:}\ P.n)$$

est un théorème. C'est justement ce que fait l'axiome d'induction.

Exemple de preuve par induction

Montrons

$$(\forall n{:}\mathbb{N} \mid{:}\ (\sum i \mid 1 \leq i \leq n : 2 \cdot i - 1) \ = \ n^2) \ .$$

La preuve se fait en trois étapes.

1. Définition du prédicat d'induction P :

$$P.n : \quad (\sum i \mid 1 \leq i \leq n : 2 \cdot i - 1) \ = \ n^2 \ .$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:}\ P.n)$.

2. Étape de base : il faut prouver $P.0$, c'est-à-dire

$$(\sum i \mid 1 \leq i \leq 0 : 2 \cdot i - 1) \ = \ 0^2 \ .$$

$$\begin{array}{ll} & (\sum i \mid 1 \leq i \leq 0 : 2 \cdot i - 1) \\ = & \quad \langle \ 1 \leq i \leq 0 \ \equiv \ \mathsf{faux} \ \ \& \ \text{Domaine vide (6.19)} \ \rangle \\ & 0 \\ = & \quad \langle \ 0^2 = 0 \cdot 0 = 0 \ \rangle \\ & 0^2 \end{array}$$

3. Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \mid{:}\ P.n \ \Rightarrow \ P(n+1))$. Par le métathéorème (7.33), il suffit de montrer $P.n \ \Rightarrow \ P(n+1)$. Supposons $P.n$ et montrons $P(n+1)$, c'est-à-dire

$$(\sum i \mid 1 \leq i \leq n+1 : 2 \cdot i - 1) \ = \ (n+1)^2 \ .$$

$$\begin{array}{ll} & (\sum i \mid 1 \leq i \leq n+1 : 2 \cdot i - 1) \\ = & \quad \langle \ \text{Extraction d'un terme (6.40)} \ \rangle \\ & (\sum i \mid 1 \leq i \leq n : 2 \cdot i - 1) \ + \ 2 \cdot (n+1) - 1 \\ = & \quad \langle \ \text{Hypothèse d'induction } P.n \ \rangle \\ & n^2 \ + \ 2 \cdot (n+1) - 1 \\ = & \quad \langle \ \text{Arithmétique} \ \rangle \\ & (n+1)^2 \end{array}$$

Remarque : Notre but était de prouver $P(n+1)$ à partir de $P.n$. Pour cela, nous avons transformé le côté gauche de $P(n+1)$ de manière à faire apparaître le côté gauche de $P.n$. C'est une technique générale pour démontrer le cas d'induction : on transforme une partie de l'expression de $P(n+1)$ pour faire apparaître la partie correspondante de $P.n$.

Sur la présentation des preuves par induction

Pour définir le prédicat d'induction, il peut être nécessaire de formaliser le problème, si l'énoncé est un mélange de français et de mathématiques.

Remarquez bien la présentation en trois étapes ainsi que les explications qui sont données. À l'examen —car il y aura une preuve par induction à l'examen—, vous devrez faire la présentation de cette manière. En particulier, vous devrez expliquer chaque étape en écrivant, par exemple pour l'étape de base,

Étape de base : il faut prouver $P.0$, c'est-à-dire ...

(8.3) Remarque. Reconsidérons l'exemple précédent. Pour montrer

$$P.n \;\Rightarrow\; P(n+1)$$

à l'étape d'induction, on peut assumer l'antécédent, comme il a été fait plus tôt, ou on peut procéder de la manière suivante :

$$\begin{array}{ll} & P(n+1) \\ = & \qquad \langle \text{ Définition de } P \rangle \\ & (\sum i \mid 1 \le i \le n+1 : 2\cdot i - 1) \;=\; (n+1)^2 \\ = & \qquad \langle \text{ Extraction d'un terme (6.40) } \rangle \\ & (\sum i \mid 1 \le i \le n : 2\cdot i - 1) \;+\; 2\cdot(n+1) - 1 \;=\; (n+1)^2 \\ = & \qquad \langle \text{ Arithmétique } \rangle \\ & (\sum i \mid 1 \le i \le n : 2\cdot i - 1) \;+\; 2\cdot n + 1 \;=\; n^2 + 2\cdot n + 1 \\ = & \qquad \langle \text{ Arithmétique } \rangle \\ & (\sum i \mid 1 \le i \le n : 2\cdot i - 1) \;=\; n^2 \\ = & \qquad \langle \text{ Définition de } P \rangle \\ & P.n \end{array}$$

Nous avons en fait démontré plus que ce qui est nécessaire ($\equiv$ au lieu de $\Rightarrow$).

(8.4) Exercice. Montrez par induction que, pour tout $k \ge 0$,

$$(\sum i \mid 0 \le i < k : 2^i) \;=\; 2^k - 1.$$

Induction débutant à d'autres nombres naturels que 0

Supposons qu'il faille montrer qu'une certaine propriété est vraie pour les nombres naturels

$$n_0,\ n_0+1,\ n_0+2,\ \ldots,$$

où $n_0 \in \mathbb{N}$. C'est possible en utilisant une version légèrement modifiée de l'axiome d'induction (8.2) :

(8.5) Induction mathématique (faible) sur $\{n_0,\ n_0+1,\ n_0+2,\ \ldots\}$:

$$\underline{P.n_0} \ \wedge\ \underline{(\forall n \mid n_0 \leq n : P.n \ \Rightarrow\ P(n+1))} \ \Rightarrow\ \underline{(\forall n \mid n_0 \leq n : P.n)}$$

Exemple d'une preuve par induction débutant à 3

Montrons $2 \cdot n + 1 < 2^n$, pour tout $n \geq 3$.

Il faut d'abord formaliser le problème. Ce qu'il faut prouver est

$$(\forall n \mid 3 \leq n : 2 \cdot n + 1 < 2^n)\ .$$

1. Définition du prédicat d'induction P : Choisissons le prédicat d'induction

   $$P.n : \quad 2 \cdot n + 1 < 2^n\ .$$

   Il faut montrer $(\forall n \mid 3 \leq n : P.n)$.

2. Étape de base : il faut prouver $P.3$, c'est-à-dire $2 \cdot 3 + 1 < 2^3$, ce qui est direct en utilisant des propriétés arithmétiques simples :

   $$2 \cdot 3 + 1 \ =\ 7 \ <\ 8 \ =\ 2^3\ .$$

3. Étape d'induction : Nous devons montrer $(\forall n \mid 3 \leq n : P.n \ \Rightarrow\ P(n+1))$. Supposons $3 \leq n$ et $P.n$, et montrons $P(n+1)$, c'est-à-dire

   $$2 \cdot (n+1) + 1 < 2^{n+1}\ .$$

   $$\begin{array}{ll} & 2^{n+1} \\ = & \quad \langle \text{ Arithmétique } \ \& \ \text{ Remarquez comment on fait ressortir } 2^n, \text{ qui est une sous-expression de } P.n \ \rangle \\ & 2 \cdot 2^n \\ > & \quad \langle \text{ Hypothèse d'induction } P.n \ \ \& \ \text{ Monotonie de } \cdot \text{ pour des nombres positifs } \rangle \end{array}$$

$$
\begin{array}{ll}
 & 2 \cdot (2 \cdot n + 1) \\
= & \quad \langle \text{ Arithmétique } \& \text{ Le but est de faire ressortir } 2 \cdot (n+1) + 1, \text{ qui est l'objectif final } \rangle \\
 & 2 \cdot (n+1) + 1 + 2 \cdot n - 1 \\
> & \quad \langle\ 2 \cdot n - 1 > 0, \text{ car } n \geq 3 \ \ \& \ \text{Monotonie de } + \ \rangle \\
 & 2 \cdot (n+1) + 1
\end{array}
$$

(8.6) Remarque. L'étape d'induction de la preuve précédente commence par :

> Nous devons montrer $(\forall n \mid 3 \leq n : P.n \ \Rightarrow \ P(n+1))$. Supposons $3 \leq n$ et $P.n$, et montrons $P(n+1)$, c'est-à-dire
>
> $$2 \cdot (n+1) + 1 < 2^{n+1} \ .$$

Si on veut donner tous les détails, il faut plutôt dire :

> Nous devons montrer $(\forall n \mid 3 \leq n : P.n \ \Rightarrow \ P(n+1))$. Par transfert (7.17a) et transfert (3.81), ceci est équivalent à
>
> $$(\forall n \mid : 3 \leq n \ \wedge \ P.n \ \Rightarrow \ P(n+1)).$$
>
> Grâce au métathéorème (7.33), il suffit de montrer
>
> $$3 \leq n \wedge P.n \ \Rightarrow \ P(n+1).$$
>
> Supposons $3 \leq n$ et $P.n$, et montrons $P(n+1)$, c'est-à-dire
>
> $$2 \cdot (n+1) + 1 < 2^{n+1} \ .$$

Comme la formulation est toujours la même, on omet habituellement l'invocation des transferts et celle du métathéorème (7.33).

8.2 Définitions inductives

L'exponentiation peut être définie en utilisant le quantificateur $\prod$:

$$b^n \ = \ (\prod i \mid 1 \leq i \leq n : b) \ .$$

On peut aussi définir l'exponentiation de manière *récursive*. Ce qui caractérise la récursion, c'est que la fonction définie est utilisée dans la définition. La plupart des langages de programmation permettent de définir des fonctions de manière récursive. Voici deux définitions équivalentes de b^n.

(8.7) $b^0 = 1$
$b^{n+1} = b \cdot b^n \quad (\text{si } n \geq 0)$

(8.8) $b^0 = 1$
$b^n = b \cdot b^{n-1} \quad (\text{si } n \geq 1)$

Le premier cas (b^0) est appelé le *cas de base*. L'autre est le *cas d'induction*. La définition est dite *inductive*. En utilisant trois fois le cas d'induction et une fois le cas de base, on obtient

$$b^3 \;=\; b \cdot b^2 \;=\; b \cdot b \cdot b^1 \;=\; b \cdot b \cdot b \cdot b^0 = \; b \cdot b \cdot b \cdot 1 = \; b \cdot b \cdot b \;.$$

Preuves par induction pour définitions inductives

Les définitions inductives se prêtent bien aux preuves inductives. Montrons par induction que, quels que soient les nombres naturels m et n, $b^{m+n} = b^m \cdot b^n$.

Formalisons le problème. Ce qu'il faut prouver est $(\forall m, n{:}\mathbb{N} \mid{:}\; b^{m+n} = b^m \cdot b^n)$. Il faut transformer cette formule pour l'amener sous la forme $(\forall n{:}\mathbb{N} \mid{:}\; P.n)$:

$$\begin{array}{ll} & (\forall m, n{:}\mathbb{N} \mid{:}\; b^{m+n} = b^m \cdot b^n) \\ = & \qquad \langle \text{ Imbrication (6.34) } \;\&\; \neg\mathsf{libre}(\text{`}m\text{'},\text{`}\mathsf{vrai}\text{'}) \rangle \\ & (\forall n{:}\mathbb{N} \mid{:}\; (\forall m{:}\mathbb{N} \mid{:}\; b^{m+n} = b^m \cdot b^n)) \end{array}$$

1. Définition du prédicat d'induction P : Choisissons comme prédicat d'induction

   $$P.n : \quad (\forall m{:}\mathbb{N} \mid{:}\; b^{m+n} = b^m \cdot b^n) \;.$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:}\; P.n)$.
2. Étape de base : il faut prouver $P.0$, c'est-à-dire $(\forall m{:}\mathbb{N} \mid{:}\; b^{m+0} = b^m \cdot b^0)$. Par le métathéorème (7.33), il suffit de montrer $b^{m+0} = b^m \cdot b^0$.

   $$\begin{array}{ll} & b^m \cdot b^0 \\ = & \qquad \langle \text{ Définition (8.7) de } b^0 \rangle \\ & b^m \cdot 1 \\ = & \qquad \langle \text{ 1 est l'élément neutre de la multiplication} \rangle \\ & b^m \\ = & \qquad \langle \text{ 0 est l'élément neutre de l'addition} \rangle \\ & b^{m+0} \end{array}$$

3. Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \mid{:}\; P.n \;\Rightarrow\; P(n+1))$. Supposons $P.n$ et montrons $P(n+1)$, c'est-à-dire

   $$(\forall m{:}\mathbb{N} \mid{:}\; b^{m+(n+1)} = b^m \cdot b^{n+1}) \;.$$

   Par le métathéorème (7.33), il suffit de montrer $b^{m+(n+1)} = b^m \cdot b^{n+1}$.

$$
\begin{array}{ll}
& b^{m+(n+1)} \\
= & \quad \langle \text{ Associativité et commutativité de l'addition } \& \text{ But : isoler } n, \text{ afin de pouvoir utiliser l'hypothèse d'induction } \rangle \\
& b^{(m+1)+n} \\
= & \quad \langle \text{ Hypothèse d'induction, avec } m := m+1, \text{ car le corps de } P.n \text{ est } \mathsf{vrai} \text{ pour tout } m \rangle \\
& b^{m+1} \cdot b^n \\
= & \quad \langle \text{ Définition (8.7) } \rangle \\
& (b \cdot b^m) \cdot b^n \\
= & \quad \langle \text{ Associativité et commutativité de la multiplication } \rangle \\
& b^m \cdot (b \cdot b^n) \\
= & \quad \langle \text{ Définition (8.7) } \rangle \\
& b^m \cdot b^{n+1}
\end{array}
$$

(8.9) Remarque. Nous aurions pu écrire la formule à démontrer ainsi :

$$(\forall m{:}\mathbb{N} \mid{:}\ (\forall n{:}\mathbb{N} \mid{:}\ b^{m+n} = b^m \cdot b^n)) \ ,$$

prendre comme prédicat d'induction $P.m : (\forall n{:}\mathbb{N} \mid{:}\ b^{m+n} = b^m \cdot b^n)$ et montrer par induction $(\forall m{:}\mathbb{N} \mid{:}\ P.m)$.

Autre exemple de preuve par induction : la factorielle

Voici une définition de la fonction *factorielle de k*, notée $k!$ et définie inductivement comme suit :

(8.10) $0! = 1$
$k! = k \cdot (k-1)! \quad (\text{si } k > 0)$

Intuitivement, $k! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot k$. Montrons

$$(\forall k{:}\mathbb{N} \mid{:}\ k! = (\textstyle\prod i \mid 1 \le i \le k : i)) \ .$$

1. Définition du prédicat d'induction P : Choisissons le prédicat d'induction

$$P.k : \quad k! = (\textstyle\prod i \mid 1 \le i \le k : i) \ .$$

Il faut montrer $(\forall k{:}\mathbb{N} \mid{:}\ P.k)$.

2. Étape de base : il faut prouver $P.0$, c'est-à-dire $0! = (\prod i \mid 1 \le i \le 0 : i)$.

$$
\begin{array}{ll}
& (\textstyle\prod i \mid 1 \le i \le 0 : i) \\
= & \quad \langle \ 1 \le i \le 0 \equiv \mathsf{faux} \ \& \ \text{Domaine vide (6.19)} \ \rangle \\
& 1 \\
= & \quad \langle \text{ Définition (8.10) } \rangle \\
& 0!
\end{array}
$$

3. Étape d'induction : Nous devons montrer $(\forall k{:}\mathbb{N} \mid{:}\ P.k \Rightarrow P(k+1))$. Supposons $P.k$ et montrons $P(k+1)$, c'est-à-dire

$$(k+1)! = (\prod i \mid 1 \le i \le k+1 : i) \ .$$

$$\begin{array}{ll} & (\prod i \mid 1 \le i \le k+1 : i) \\ = & \quad \langle \text{ Extraction d'un terme (6.40) } \rangle \\ & (\prod i \mid 1 \le i \le k : i) \cdot (k+1) \\ = & \quad \langle \text{ Hypothèse d'induction } \rangle \\ & k! \cdot (k+1) \\ = & \quad \langle \text{ Définition (8.10) ; notons que } k+1 > 0, \text{ de sorte que la définition est applicable } \rangle \\ & (k+1)! \end{array}$$

Définition inductive à plus d'un cas de base : les nombres de Fibonacci

Voici une définition inductive des nombres de Fibonacci, notés F_n, pour $n{:}\mathbb{N}$.

(8.11)
$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \quad (\text{si } n \ge 2) \end{aligned}$$

On remarque qu'il y a deux cas de base et, surtout, que mis à part F_0 et F_1, les nombres de Fibonacci sont définis en terme des *DEUX* nombres précédents dans la séquence, contrairement à ce qui est fait pour l'exponentiation ou la factorielle.

Les premiers nombres de Fibonacci sont 0, 1, 1, 2, 3, 5, 8, 13.
Soient

$$\phi = (1+\sqrt{5})/2 \qquad \text{et} \qquad \hat{\phi} = (1-\sqrt{5})/2$$

(ϕ est appelé le *nombre d'or*).

(8.12) Exercice. Démontrez $\phi^2 = \phi + 1$.

Sachant que

(8.13) $\phi^2 = \phi + 1 \qquad$ et $\qquad \hat{\phi}^2 = \hat{\phi} + 1$,

nous montrerons que pour tout $n \ge 1$,

$$F_n \le \phi^{n-1} \ .$$

Mais avant ...

Preuves par induction à deux cas de base

Puisque la définition des nombres de Fibonacci a deux cas de base, il faut modifier l'axiome d'induction (8.5) pour pouvoir utiliser deux cas de base :

(8.14) Induction sur $\{n_0,\ n_0+1,\ n_0+2,\ \ldots\}$, deux cas de base :

$$\underline{P.n_0} \ \wedge\ \underline{P(n_0+1)} \ \wedge\ \underline{(\forall n \mid n_0 \leq n : P.n \ \wedge\ P(n+1) \ \Rightarrow\ P(n+2))}$$
$$\Rightarrow\ \underline{(\forall n \mid n_0 \leq n : P.n)}$$

Il faut donc démontrer deux cas de base. À l'étape d'induction, la démonstration de $P(n+2)$ *peut nécessiter* les deux hypothèses d'induction $P.n$ et $P(n+1)$.

Montrons maintenant que pour tout $n \geq 1$, $F_n \leq \phi^{n-1}$.

La propriété à démontrer est

$$(\forall n \mid n \geq 1 : F_n \leq \phi^{n-1}) \ .$$

1. Définition du prédicat d'induction P : Choisissons comme prédicat d'induction

   $$P.n : \quad F_n \leq \phi^{n-1} \ .$$

   Il faut montrer $(\forall n \mid n \geq 1 : P.n)$.
2. Étape de base 1 : il faut prouver $P.1$, c'est-à-dire $F_1 \leq \phi^{1-1}$. Par la définition (8.11) et en utilisant des propriétés mathématiques simples,

   $$F_1 = 1 = \phi^0 = \phi^{1-1} \ .$$

3. Étape de base 2 : il faut prouver $P.2$, c'est-à-dire $F_2 \leq \phi^{2-1}$. Par la définition (8.11) et en utilisant des propriétés mathématiques simples,

   $$F_2 = F_1 + F_0 = 1 + 0 = 1 \leq (1+\sqrt{5})/2 = \phi = \phi^{2-1} \ .$$

4. Étape d'induction : Nous devons montrer

   $$(\forall n{:}\mathbb{N} \mid n \geq 1 : P.n \ \wedge\ P(n+1) \ \Rightarrow\ P(n+2))$$

   Supposons $n \geq 1$, $P.n$ et $P(n+1)$, et montrons $P(n+2)$, c'est-à-dire $F_{n+2} \leq \phi^{(n+2)-1}$.

   $$\begin{array}{ll} & F_{n+2} \\ = & \quad \langle \text{ Définition des nombres de Fibonacci (8.11) \ \& la définition est applicable, car } n+2 \geq 2 \ \rangle \\ & F_{n+1} + F_n \\ \leq & \quad \langle \text{ Hypothèses d'induction } P.n \text{ et } P(n+1) \ \rangle \\ & \phi^n + \phi^{n-1} \\ = & \quad \langle \text{ Factorisation de } \phi^{n-1} \ \rangle \end{array}$$

$$
\begin{array}{ll}
& \phi^{n-1} \cdot (\phi + 1) \\
= & \qquad \langle \text{ Par (8.13), } \phi + 1 = \phi^2 \ \rangle \\
& \phi^{n-1} \cdot \phi^2 \\
= & \qquad \langle \text{ Arithmétique : } (n-1) + 2 = (n+2) - 1 \ \rangle \\
& \phi^{(n+2)-1}
\end{array}
$$

(8.15) Exercice. Montrez $F_m^2 = F_{m-1} \cdot F_{m+1} - (-1)^m$, pour tout $m \geq 1$.

Autre preuve par induction sur les nombres de Fibonacci

Montrons

(8.16) $F_{n+m} = F_m \cdot F_{n+1} + F_{m-1} \cdot F_n \qquad$ (pour tout $n \geq 0$ et tout $m \geq 1$) .

Formalisation : La propriété à démontrer est

$$(\forall n{:}\mathbb{N} \mid{:} (\forall m \mid m \geq 1 : F_{n+m} = F_m \cdot F_{n+1} + F_{m-1} \cdot F_n)) \ .$$

1. Définition du prédicat d'induction P : Choisissons comme prédicat d'induction

   $$P.n : \quad (\forall m \mid m \geq 1 : F_{n+m} = F_m \cdot F_{n+1} + F_{m-1} \cdot F_n) \ .$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:} P.n)$.
   La preuve qui suit montre que même si les nombres de Fibonacci ont une définition inductive à deux cas de base, il n'est pas toujours nécessaire de faire une preuve par induction de leurs propriétés en utilisant deux cas de base. Pour cela, il suffit que tous les usages de la définition soient légaux, c'est-à-dire qu'on pose $F_n = F_{n-1} + F_{n-2}$ seulement si $n \geq 2$. Nous utilisons l'axiome d'induction (8.2).
2. Étape de base : il faut prouver $P.0$, c'est-à-dire

   $$(\forall m \mid m \geq 1 : F_m = F_m \cdot F_1 + F_{m-1} \cdot F_0) \ .$$

   $$
   \begin{array}{ll}
   & (\forall m \mid m \geq 1 : F_m = F_m \cdot F_1 + F_{m-1} \cdot F_0) \\
   = & \qquad \langle \text{ Définition des nombres de Fibonacci (8.11) } \rangle \\
   & (\forall m \mid m \geq 1 : F_m = F_m \cdot 1 + F_{m-1} \cdot 0) \\
   = & \qquad \langle \text{ Arithmétique } \rangle \\
   & (\forall m \mid m \geq 1 : F_m = F_m) \\
   = & \qquad \langle \ F_m = F_m \equiv \mathsf{vrai} \ \ \& \ \ (7.24) \ \rangle \\
   & \mathsf{vrai}
   \end{array}
   $$

3. Étape d'induction : Nous devons montrer

   $$(\forall n{:}\mathbb{N} \mid{:} P.n \ \Rightarrow \ P(n+1))$$

Supposons $P.n$ et montrons $P(n+1)$, c'est-à-dire

$$(\forall m \mid m \geq 1 : F_{n+1+m} = F_m \cdot F_{n+1+1} + F_{m-1} \cdot F_{n+1}) \ .$$

Montrons que le corps de cette quantification est un théorème, pour un $m \geq 1$ arbitraire.

$$\begin{array}{ll} & F_m \cdot F_{n+1+1} + F_{m-1} \cdot F_{n+1} \\ = & \quad \langle \text{ Définition des nombres de Fibonacci (8.11) ; on peut utiliser le cas inductif, car } n+2 \geq 2 \ \rangle \\ & F_m \cdot (F_{n+1} + F_n) + F_{m-1} \cdot F_{n+1} \\ = & \quad \langle \text{ Arithmétique } \rangle \\ & (F_m + F_{m-1}) \cdot F_{n+1} + F_m \cdot F_n \\ = & \quad \langle \text{ Définition des nombres de Fibonacci (8.11) ; on peut utiliser le cas inductif, car } m+1 \geq 2, \text{ puisque } m \geq 1 \ \rangle \\ & F_{m+1} \cdot F_{n+1} + F_m \cdot F_n \\ = & \quad \langle \text{ Le corps de l'hypothèse d'induction est un théorème, pour tout } m \text{ (par le métathéorème (7.33)) ; utilisons-le avec } m := m+1 \ \rangle \\ & F_{n+m+1} \\ = & \quad \langle \text{ Hyper simple } \rangle \\ & F_{n+1+m} \end{array}$$

(8.17) Remarque. Dans la preuve précédente, on montre

$$(\forall m \mid m \geq 1 : F_{n+1+m} = F_m \cdot F_{n+1+1} + F_{m-1} \cdot F_{n+1})$$

en disant :

> Montrons que le corps de cette quantification est un théorème, pour un $m \geq 1$ arbitraire.

C'est une formulation standard. La justification complète est la suivante :

> Par transfert (7.17a), la propriété à démontrer est équivalente à
>
> $$(\forall m \mid : m \geq 1 \ \Rightarrow \ F_{n+1+m} = F_m \cdot F_{n+1+1} + F_{m-1} \cdot F_{n+1}) \ .$$
>
> Par le métathéorème (7.33), il suffit de montrer
>
> $$m \geq 1 \ \Rightarrow \ F_{n+1+m} = F_m \cdot F_{n+1+1} + F_{m-1} \cdot F_{n+1} \ .$$
>
> Supposons $m \geq 1$ et montrons $F_{n+1+m} = F_m \cdot F_{n+1+1} + F_{m-1} \cdot F_{n+1}$.

8.3 Problèmes

1. Démontrez par induction que pour tout $n \geq 0$,

$$(\sum i \mid 0 \leq i < n : 2 \cdot i + 1) \;=\; n^2.$$

2. Démontrez par induction sur n que $n^2 \leq 2^n$ pour tout $n \geq 4$.
3. Démontrez par induction que si $x \neq y$, alors $x^n - y^n$ est divisible par $x - y$, pour tout $n \geq 0$. Indice : soustrayez et additionnez $x \cdot y^n$ à $x^{n+1} - y^{n+1}$.
4. Montrez par induction que $F_n < 2^n$, pour tout $n \geq 0$.
5. Montrez par induction que $F_n = (\phi^n - \hat{\phi}^n)/\sqrt{5}$, pour tout $n \geq 0$.

Chapitre 9

Autres techniques de preuve

Ce chapitre présente plusieurs techniques de preuve qui s'appuient sur certaines lois des chapitres 3 et 4. Grâce à ces lois, la présentation des techniques devient très simple. L'utilisation de ces techniques ne nécessite pas vraiment l'apprentissage de nouvelles aptitudes, sauf peut-être de savoir laquelle d'entre elles il faut utiliser pour réussir la démontration d'une propriété donnée.

La section 9.1 présente quelques lois utilisées dans ce chapitre. Certaines de ces lois sont très utiles pour la manipulation d'expressions dont le type n'est pas forcément booléen.

Dans ce chapitre, la multiplication est dénotée par la juxtaposition, c'est-à-dire que nous écrivons xy au lieu de $x \cdot y$, comme on le fait habituellement en mathématiques.

9.1 Quelques lois additionnelles

L'axiome de Leibniz

(9.1) Axiome, Leibniz : $(e = f) \Rightarrow (E[z := e] = E[z := f])$

ou encore $(e = f) \Rightarrow (E[z := e] = E[z := f])$

Dans cet axiome, e, f et E sont des expressions arbitraires qui ne sont pas forcément booléennes.

(9.2) Remarque. Rappelons la règle de Leibniz : $\dfrac{X = Y}{E[z := X] = E[z := Y]}$. Elle dit que

si $X = Y$ est un théorème,
alors $E[z := X] = E[z := Y]$ est un théorème.

Pour la logique propositionnelle, on peut montrer que ceci est équivalent à

si $X = Y$ est vrai dans *TOUS* les états,
alors $E[z := X] = E[z := Y]$ est vrai dans *TOUS* les états.

L'axiome (9.1) dit que

si $X = Y$ est vrai dans *UN* état,
alors $E[z := X] = E[z := Y]$ est vrai dans *CET* état.

Il y a donc une différence entre la règle et l'axiome de Leibniz.Cette différence se manifeste comme suit.

Dans le problème 7 du chapitre 1, nous avons montré que si $E[z := X] = E[z := Y]$ est un théorème pour toute expression E, alors $X = Y$ est un théorème. Étant donnée la similitude entre la règle de Leibniz et l'axiome (9.1), on pourrait donc croire que ce dernier peut être renforcé en

$$e = f \quad \equiv \quad E[z := e] = E[z := f].$$

Mais cette expression n'est pas un théorème ; on peut le voir en y choisissant

$$e := \mathsf{vrai}, \qquad f := \mathsf{faux}, \qquad E := \mathsf{faux} \wedge z,$$

ce que fait la dérivation suivante :

$$\begin{array}{ll} & \mathsf{vrai} = \mathsf{faux} \ \equiv \ (\mathsf{faux} \wedge z)[z := \mathsf{vrai}] = (\mathsf{faux} \wedge z)[z := \mathsf{faux}] \\ = & \qquad \langle \text{ Substitution et } (\mathsf{vrai} = \mathsf{faux}) \equiv \mathsf{faux} \ \rangle \\ & \mathsf{faux} \ \equiv \ (\mathsf{faux} \wedge \mathsf{vrai}) \ = \ (\mathsf{faux} \wedge \mathsf{faux}) \\ = & \qquad \langle \text{ Évaluation des } \wedge \ \ \& \ \ (\mathsf{faux} = \mathsf{faux}) \equiv \mathsf{vrai} \ \rangle \\ & \mathsf{faux} \ \equiv \ \mathsf{vrai} \\ = & \ \mathsf{faux} \end{array}$$

Lois de substitution

(9.3) Substitution : (a) $(e = f) \wedge E[z := e] \ \equiv \ (e = f) \wedge E[z := f]$
(b) $(e = f) \Rightarrow E[z := e] \ \equiv \ (e = f) \Rightarrow E[z := f]$
(c) $q \wedge (e = f) \ \Rightarrow \ E[z := e] \ \equiv \ q \wedge (e = f) \ \Rightarrow \ E[z := f]$

Remplacement de variables par des constantes booléennes

(9.4) Remplacement par vrai : (a) $p \Rightarrow E[z := p] \ \equiv \ p \Rightarrow E[z := \mathsf{vrai}]$
(b) $p \wedge q \ \Rightarrow \ E[z := p] \ \equiv \ p \wedge q \ \Rightarrow \ E[z := \mathsf{vrai}]$

(9.5) Remplacement par faux : (a) $E[z := p] \Rightarrow p \ \equiv \ E[z := \mathsf{faux}] \Rightarrow p$
(b) $E[z := p] \ \Rightarrow \ p \vee q \ \equiv \ E[z := \mathsf{faux}] \ \Rightarrow \ p \vee q$

(9.6) Remplacement par vrai : $p \wedge E[z := p] \equiv p \wedge E[z := \mathsf{vrai}]$

(9.7) Remplacement par faux : $p \vee E[z := p] \equiv p \vee E[z := \mathsf{faux}]$

(9.8) Shannon : $E[z := p] \equiv (p \wedge E[z := \mathsf{vrai}]) \vee (\neg p \wedge E[z := \mathsf{faux}])$

(9.9) Exemple. Illustration des théorèmes sur le remplacement de variables booléennes par des constantes. Montrons $p \wedge q \Rightarrow (p \equiv q)$.

$$
\begin{array}{ll}
 & p \wedge q \Rightarrow (p \equiv q) \\
= & \quad \langle \text{ Remplacement par } \mathsf{vrai} \text{ (9.4b), avec l'expression } E : z \equiv q \ \rangle \\
 & p \wedge q \Rightarrow (\mathsf{vrai} \equiv q) \\
= & \quad \langle \text{ Remplacement par } \mathsf{vrai} \text{ (9.4b), avec } p, q := q, p \text{ et } E : \mathsf{vrai} \equiv z \ \rangle \\
 & p \wedge q \Rightarrow (\mathsf{vrai} \equiv \mathsf{vrai}) \\
= & \quad \langle \text{ Identité de } \equiv \text{ (3.4), avec } q := \mathsf{vrai} \ \rangle \\
 & p \wedge q \Rightarrow \mathsf{vrai} \qquad \text{—Zéro à droite de } \Rightarrow \text{ (3.88), avec } p := p \wedge q
\end{array}
$$

9.2 Preuves par cas

(9.10) Métathéorème sur les preuves par cas : Si

$$E[z := \mathsf{vrai}] \quad \text{et} \quad E[z := \mathsf{faux}]$$

sont des théorèmes, alors

$$E[z := p]$$

est un théorème.

Démonstration.

$$
\begin{array}{ll}
 & E[z := p] \\
= & \quad \langle \text{ Shannon (9.8) } \rangle \\
 & (p \wedge E[z := \mathsf{vrai}]) \vee (\neg p \wedge E[z := \mathsf{faux}]) \\
= & \quad \langle \text{ Hypothèses du métathéorème \& Par (3.6) et le métathéorème (3.100),} \\
 & \quad \text{tout théorème est équivalent à } \mathsf{vrai} \ \rangle \\
 & (p \wedge \mathsf{vrai}) \vee (\neg p \wedge \mathsf{vrai}) \\
= & \quad \langle \text{ Identité de } \wedge \text{ (3.52), deux fois (1) directement (2) avec } p := \neg p \ \rangle \\
 & p \vee \neg p \qquad \text{—Tiers exclu (3.37)}
\end{array}
$$

Exemple de preuve par cas basée sur (9.10)

Preuve par cas de $p \wedge \neg p \equiv \mathsf{faux}$ selon (9.10).
Cas $p := \mathsf{vrai}$

$$
\begin{array}{ll}
 & (p \wedge \neg p \equiv \mathsf{faux})[p := \mathsf{vrai}] \\
= & \quad \langle \text{ Substitution } \rangle \\
 & \mathsf{vrai} \wedge \neg \mathsf{vrai} \equiv \mathsf{faux} \\
= & \quad \langle \text{ Identité de } \wedge \text{ (3.52), avec } p := \neg\mathsf{vrai} \ \ \& \ \ (3.11) \ \rangle \\
 & \mathsf{faux} \equiv \mathsf{faux} \qquad \text{—Réflexivité de } \equiv \text{ (3.7)}
\end{array}
$$

Cas $p := \mathsf{faux}$

$$
\begin{array}{ll}
 & (p \wedge \neg p \equiv \mathsf{faux})[p := \mathsf{faux}] \\
= & \quad \langle \text{ Substitution } \rangle \\
 & \mathsf{faux} \wedge \neg \mathsf{faux} \equiv \mathsf{faux} \\
= & \quad \langle \text{ Zéro de } \wedge \text{ (3.53), avec } p := \neg\mathsf{faux} \ \rangle \\
 & \mathsf{faux} \equiv \mathsf{faux} \qquad \text{—Réflexivité de } \equiv \text{ (3.7)}
\end{array}
$$

Une preuve directe plus simple se fait en trois transformations (essayez).

(9.11) Exercice. Montrez la formule suivante par cas.

$$(p \vee q) \wedge r \ \equiv \ (p \wedge r) \ \vee \ (q \wedge r)$$

Preuve par cas générale (nombre quelconque de cas)

Pour montrer Q par cas, on distingue d'abord n cas $P_1, \ldots, P_n$ (expressions booléennes) tels que

$$P_1 \vee \cdots \vee P_n$$

est un théorème (c'est-à-dire que toutes les possibilités sont traitées). On démontre ensuite $P_i \Rightarrow Q$ pour chaque $1 \leq i \leq n$. Lorsque $n = 3$, cette méthode s'appuie sur le théorème

(9.12) $(p \vee q \vee r) \ \wedge \ (p \Rightarrow s) \ \wedge \ (q \Rightarrow s) \ \wedge \ (r \Rightarrow s) \ \ \Rightarrow \ \ s$

La figure 9.1 montre ce qu'est le format de présentation des preuves par cas.

Voici un exemple illustrant cette technique. Montrons que pour pour tout $n \in \mathbb{N}^+$, $n^3 - n$ est divisible par 3.

Ce qu'il faut montrer est

$$(\forall n{:}\mathbb{N}^+ \mid{:}\ n^3 - n \text{ est divisible par } 3).$$

Par le métathéorème (7.33), il suffit de montrer que $n^3 - n$ est divisible par 3.

Notons d'abord que $n^3 - n = n(n+1)(n-1)$. N'importe quel $n \in \mathbb{N}^+$ peut s'écrire sous la forme $n = 3p + q$, pour des valeurs appropriées de $p \in \mathbb{N}$ et $q \in \{0, 1, 2\}$. Nous considérerons trois cas : $q = 0$, $q = 1$ et $q = 2$, ce qui couvre toutes les valeurs possibles de q (c'est-à-dire que $q = 0 \ \vee \ q = 1 \ \vee \ q = 2$ est un théorème).

Preuve de Q par cas : $P_1, \ldots, P_n$
Preuve de $P_1 \vee \cdots \vee P_n$

1. Cas P_1 : preuve de $P_1 \Rightarrow Q$

⋮ ⋮ ⋮

n. Cas P_n : preuve de $P_n \Rightarrow Q$

FIG. 9.1 – Format de présentation des preuves par cas

1. Cas $q = 0$: supposons $q = 0$ et montrons que $n^3 - n$ est divisible par 3.

$$\begin{array}{ll} & n^3 - n \\ = & \quad \langle \text{ Remarque ci-dessus } \rangle \\ & n(n+1)(n-1) \\ = & \quad \langle \text{ Hypothèses } n = 3p + q \text{ et } q = 0 \rangle \\ & 3p(3p+1)(3p-1) \end{array}$$

Comme $3p(3p+1)(3p-1)$ est divisible par 3, $n^3 - n$ l'est aussi.

2. Cas $q = 1$: supposons $q = 1$ et montrons que $n^3 - n$ est divisible par 3.

$$\begin{array}{ll} & n^3 - n \\ = & \quad \langle \text{ Remarque ci-dessus } \rangle \\ & n(n+1)(n-1) \\ = & \quad \langle \text{ Hypothèses } n = 3p + q \text{ et } q = 1 \rangle \\ & (3p+1)(3p+2)(3p) \\ = & \quad \langle \text{ Factorisation pour mettre le facteur 3 en évidence } \rangle \\ & 3(3p+1)(3p+2)p \end{array}$$

Comme $3(3p+1)(3p+2)p$ est divisible par 3, $n^3 - n$ l'est aussi.

3. Cas $q = 2$: supposons $q = 2$ et montrons que $n^3 - n$ est divisible par 3.

$$\begin{array}{ll} & n^3 - n \\ = & \quad \langle \text{ Remarque ci-dessus } \rangle \\ & n(n+1)(n-1) \\ = & \quad \langle \text{ Hypothèses } n = 3p + q \text{ et } q = 2 \rangle \\ & (3p+2)(3p+3)(3p+1) \\ = & \quad \langle \text{ Factorisation pour mettre le facteur 3 en évidence } \rangle \\ & 3(3p+2)(p+1)(3p+1) \end{array}$$

Comme $3(3p+2)(p+1)(3p+1)$ est divisible par 3, $n^3 - n$ l'est aussi.

(9.13) Exercice. Montrez que, pour tout $x, y{:}\mathbb{R}$, $|x+y| \leq |x|+|y|$, où $|x|$ est la *valeur absolue* de x, définie par

$$|x| = x \quad \text{si } x \geq 0,$$
$$|x| = -x \quad \text{si } x \leq 0.$$

Remarques :

1. La définition pourrait aussi être $|x| = x$ si $x \geq 0$ et $|x| = -x$ si $x < 0$.
2. La preuve doit bien sûr être basée sur la définition donnée, pas sur ce que vous savez de la valeur absolue. Si vous voulez utiliser une propriété de la valeur absolue, démontrez-la à partir de la définition ci-dessus. Le même principe s'applique lors d'un examen.

9.3 Preuves par implication mutuelle

(9.14) Méthode de preuve :
Pour démontrer $P \equiv Q$, montrez $P \Rightarrow Q$ et $Q \Rightarrow P$.

Cette méthode découle du théorème (3.97) $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$.

9.4 Preuves par contradiction

À partir de (3.90), $p \Rightarrow \mathsf{faux} \equiv \neg p$, on obtient facilement

(9.15) Preuve par contradiction : $\neg p \Rightarrow \mathsf{faux} \equiv p$.

C'est la base des *preuves par contradiction*, aussi dites *preuves par l'absurde* : au lieu de montrer p, on montre $\neg p \Rightarrow \mathsf{faux}$. Cette démonstration se fait souvent en disant « supposons $\neg p$ et dérivons une contradiction ».

(9.16) Exercice. Montrez $p \wedge q \Rightarrow p$ par contradiction.

(9.17) Exemple. Considérons la fonction Arrêt définie par l'expression suivante :

(9.18) $\mathsf{Arrêt}(P) \equiv P$ s'arrête .

Cette expression indique que Arrêt analyse P et détermine si P s'arrête. Le code partiel du programme implantant la fonction Arrêt pourrait avoir la forme

fonction Arrêt(P : texte) : $\mathbb{B}$
début . . .fin

(9.19) Théorème : Le programme implantant la fonction Arrêt n'existe pas.

Démonstration. Le programme suivant est utilisé dans la preuve :

programme B début tant que Arrêt("appelle B") faire rien fin

“appelle B” s’arrête
$=$ ⟨ Par définition de B (négation de la condition de la boucle) ⟩
$\neg$Arrêt(“appelle B”)
$=$ ⟨ Définition de Arrêt (9.18) ⟩
$\neg$(“appelle B” s’arrête)

Et le clou final :

Le programme implantant Arrêt existe
$\Rightarrow$ ⟨ Dérivation précédente ⟩
“appelle B” s’arrête $\equiv$ $\neg$(“appelle B” s’arrête)
$=$ ⟨ (3.18), avec $p := B$ s’arrête ⟩
faux

Par conséquent, le programme implantant Arrêt n’existe pas (9.15). On dit que Arrêt est une fonction *non calculable*.

(9.20) Exemple. Voici un autre exemple de preuve par contradiction. Montrons que $\sqrt{2}$ est irrationnel, c’est-à-dire qu’on ne peut pas l’exprimer par un rapport d’entiers. Appelons P la proposition « $\sqrt{2}$ est irrationnel » et montrons $\neg P \Rightarrow$ faux.

$\neg P$
$=$ ⟨ La négation de P est « $\sqrt{2}$ est rationnel » ⟩
$\sqrt{2}$ est rationnel
$=$ ⟨ Un nombre rationnel positif peut s’exprimer comme le rapport de deux nombres naturels positifs sans facteur commun (1 ne compte pas comme facteur commun) ⟩
$(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ \sqrt{2} = a/b \ \wedge\ a, b$ sans facteur commun$)$
$=$ ⟨ $\sqrt{2} = a/b \ \equiv\ 2 = a^2/b^2$ (on élève au carré les deux côtés de l’égalité) ⟩
$(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2 = a^2/b^2 \ \wedge\ a, b$ sans facteur commun$)$
$=$ ⟨ $2 = a^2/b^2 \ \equiv\ 2b^2 = a^2$ (en multipliant les deux côtés de l’équation par b^2) ⟩
$(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ a, b$ sans facteur commun$)$
$=$ ⟨ Idempotence de $\wedge$ (3.51) ⟩
$(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ 2b^2 = a^2 \ \wedge\ a, b$ sans facteur commun$)$
$\Rightarrow$ ⟨ $2b^2 = a^2$ signifie que a^2 est pair, d’où a est pair aussi. Puisque a est pair, $a = 2c$ pour un certain entier c. Autrement dit, $2b^2 = a^2 \Rightarrow (\exists c{:}\mathbb{Z}^+ \mid{:}\ a = 2c)$. & Monotonie de $\wedge$ (4.3) & Monotonie de $\exists$ (7.36). Remarque : cette justification est standard, mais certains détails sont omis ⟩
$(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ (\exists c{:}\mathbb{Z}^+ \mid{:}\ a = 2c) \ \wedge\ a, b$ sans facteur commun$)$
$=$ ⟨ $\neg$libre(‘c’,‘$2b^2 = a^2 \ \wedge\ a, b$ sans facteur commun’) & Distributivité de $\wedge$ sur $\exists$ (7.4) ⟩

$(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ (\exists c{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ a = 2c \ \wedge\ a, b \text{ sans facteur commun}))$

$=$ $\langle\ \neg\mathsf{libre}(\text{`}c\text{'},\text{`}\mathsf{vrai}\text{'})\ \ \&\ \ \text{Imbrication (6.34)}\ \rangle$

$(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ a = 2c \ \wedge\ a, b \text{ sans facteur commun})$

$=$ $\langle\ \text{(9.3a), avec } e, f, E := a,\ 2c,\ 2b^2 = z^2\ \ \&\ \ (2c)^2 = 4c^2\ \rangle$

$(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = 4c^2 \ \wedge\ a = 2c \ \wedge\ a, b \text{ sans facteur commun})$

$=$ $\langle\ 2b^2 = 4c^2 \ \equiv\ b^2 = 2c^2)\ \rangle$

$(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}\ b^2 = 2c^2 \ \wedge\ a = 2c \ \wedge\ a, b \text{ sans facteur commun})$

$\Rightarrow$ $\langle\ b^2 = 2c^2 \Rightarrow \mathsf{pair}.b\ \ \&\ \ \text{Monotonie de } \wedge \text{ (4.3)}\ \ \&\ \ \text{Monotonie de } \exists \text{ (7.36)}\ \rangle$

$(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}\ \mathsf{pair}.b \ \wedge\ a = 2c \ \wedge\ a, b \text{ sans facteur commun})$

$=$ $\langle\ a = 2c$ signifie que a est pair. Puis que b aussi est pair, a et b ont un facteur commun (2). Nous avons donc « a, b ont un facteur commun » et « a, b sans facteur commun ». Cette proposition a la forme $p \wedge \neg p$. Elle la valeur faux et elle entraîne la fausseté de tout le corps de la quantification (par (3.53)). $\rangle$

$(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}\ \mathsf{faux})$

$=$ $\langle\ \text{(7.8)}\ \rangle$

faux.

Dans ce qui suit, nous commentons cette preuve de l'irrationnalité de $\sqrt{2}$. La preuve y est identifiée par la lettre E (pour *équationnelle*). Le but est de comparer cette preuve avec une preuve classique (identifiée par la lettre C ci-dessous).

Voici une preuve classique de l'irrationnalité de $\sqrt{2}$, tirée de

> Kenneth A. Ross et Charles R. B. Wright. *Discrete Mathematics*. Prentice Hall, Upper Saddle River, New Jersey, 1999.

Nous voulons montrer que $\sqrt{2}$ est irrationnel, c'est-à-dire que si $x \in \mathbb{R}$ et $x^2 = 2$, alors x n'est pas un nombre rationnel. Procédons par contradiction et supposons que $x \in \mathbb{R}$, que $x^2 = 2$ et que x est rationnel. Alors, par définition de ce qu'est un nombre rationnel, on doit avoir $x = a/b$ avec $a, b \in \mathbb{Z}$ et $b \neq 0$. Puisqu'on peut réduire la fraction, on peut supposer que a et b n'ont pas de facteur commun. En particulier, a et b ne sont pas tous deux pairs. Puisque $2 = x^2 = (a/b)^2$, on a $a^2 = 2b^2$ et donc a^2 est pair. Ceci implique que a est pair, puisque sinon a^2 serait impair. On en tire que $a = 2c$ pour un certain $c \in \mathbb{Z}$, d'où $(2c)^2 = 2b^2$ et donc $2c^2 = b^2$. Par conséquent, b^2 et b sont aussi pairs. Mais alors a et b sont tous deux pairs, ce qui contredit une assertion antérieure. On en conclut que $\sqrt{2}$ est irrationnel.

Réécrivons cette preuve en numérotant certaines assertions.

(C 1) Nous voulons montrer que $\sqrt{2}$ est irrationnel,

(C 2) c'est-à-dire que si $x \in \mathbb{R}$ et $x^2 = 2$, alors x n'est pas un nombre rationnel.

(C 3) Procédons par contradiction et supposons que $x \in \mathbb{R}$, que $x^2 = 2$ et que x est rationnel.

(C 4) Alors, par définition de ce qu'est un nombre rationnel, on doit avoir $x = a/b$ avec $a, b \in \mathbb{Z}$ et $b \neq 0$.

(C 5) Puisqu'on peut réduire la fraction, on peut supposer que a et b n'ont pas de facteur commun.

(C 6) En particulier, a et b ne sont pas tous deux pairs.

(C 7) Puisque $2 = x^2 = (a/b)^2$, on a $a^2 = 2b^2$ et donc a^2 est pair.

(C 8) Ceci implique que a est pair, puisque sinon a^2 serait impair.

(C 9) On en tire que $a = 2c$ pour un certain $c \in \mathbb{Z}$,

(C10) d'où $(2c)^2 = 2b^2$ et donc $2c^2 = b^2$.

(C11) Par conséquent, b^2 et b sont aussi pairs.

(C12) Mais alors a et b sont tous deux pairs, ce qui contredit une assertion antérieure.

(C13) On en conclut que $\sqrt{2}$ est irrationnel.

Réécrivons également la preuve de l'exemple 9.20 en numérotant ses lignes.

(E 1) Montrons que $\sqrt{2}$ est irrationnel,

(E 2) c'est-à-dire qu'on ne peut pas l'exprimer par un rapport d'entiers.

(E 3) Appelons P la proposition « $\sqrt{2}$ est irrationnel »

(E 4) et montrons $\neg P \Rightarrow$ faux.

(E 5) $\neg P$

(E 6) $=$ $\langle$ La négation de P est « $\sqrt{2}$ est rationnel » $\rangle$

(E 7) $\sqrt{2}$ est rationnel

(E 8) $=$ $\langle$ Un nombre rationnel positif peut s'exprimer comme le rapport de deux nombres naturels positifs sans facteur commun (1 ne compte pas comme facteur commun) $\rangle$

(E 9) $(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ \sqrt{2} = a/b \ \wedge\ a, b$ sans facteur commun$)$

(E10) $=$ $\langle\ \sqrt{2} = a/b \ \equiv\ 2 = a^2/b^2$ (on élève au carré les deux côtés de l'égalité) $\rangle$

(E11) $(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2 = a^2/b^2 \ \wedge\ a, b$ sans facteur commun$)$

(E12) $=$ $\langle\ 2 = a^2/b^2 \ \equiv\ 2b^2 = a^2$ (en multipliant les deux côtés de l'équation par b^2) $\rangle$

(E13) $(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ a, b$ sans facteur commun$)$

(E14) $=$ $\langle$ Idempotence de $\wedge$ (3.51) $\rangle$

(E15) $(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ 2b^2 = a^2 \ \wedge\ a, b$ sans facteur commun$)$

(E16) $\Rightarrow$ $\langle\ 2b^2 = a^2$ signifie que a^2 est pair, d'où a est pair aussi. Puisque a est pair, $a = 2c$ pour un certain entier c. Autrement dit, $2b^2 = a^2 \Rightarrow (\exists c{:}\mathbb{Z}^+ \mid{:}\ a = 2c)$. & Monotonie de $\wedge$ (4.3) & Monotonie de $\exists$ (7.36). Remarque : cette justification est standard, mais certains détails sont omis $\rangle$

(E17) $(\exists a, b{:}\mathbb{Z}^+ \mid{:}\ 2b^2 = a^2 \ \wedge\ (\exists c{:}\mathbb{Z}^+ \mid{:}\ a = 2c) \ \wedge\ a, b$ sans facteur commun$)$

(E18) = $\langle$ $\neg$libre('c','$2b^2 = a^2 \ \wedge$ a, b sans facteur commun') & Distributivité de $\wedge$ sur $\exists$ (7.4) $\rangle$

(E19) $(\exists a, b{:}\mathbb{Z}^+ \mid{:} (\exists c{:}\mathbb{Z}^+ \mid{:} 2b^2 = a^2 \ \wedge \ a = 2c \ \wedge \ a, b$ sans facteur commun))

(E20) = $\langle$ $\neg$libre('c','vrai') & Imbrication (6.34) $\rangle$

(E21) $(\exists a, b, c{:}\mathbb{Z}^+ \mid{:} 2b^2 = a^2 \ \wedge \ a = 2c \ \wedge \ a, b$ sans facteur commun)

(E22) = $\langle$ (9.3a), avec $e, f, E := a, \ 2c, \ 2b^2 = z^2$ & $(2c)^2 = 4c^2$ $\rangle$

(E23) $(\exists a, b, c{:}\mathbb{Z}^+ \mid{:} 2b^2 = 4c^2 \ \wedge \ a = 2c \ \wedge \ a, b$ sans facteur commun)

(E24) = $\langle$ $2b^2 = 4c^2 \ \equiv \ b^2 = 2c^2)$ $\rangle$

(E25) $(\exists a, b, c{:}\mathbb{Z}^+ \mid{:} b^2 = 2c^2 \ \wedge \ a = 2c \ \wedge \ a, b$ sans facteur commun)

(E26) $\Rightarrow$ $\langle$ $b^2 = 2c^2 \Rightarrow$ pair.b & Monotonie de $\wedge$ (4.3) & Monotonie de $\exists$ (7.36) $\rangle$

(E27) $(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}$ pair.$b \ \wedge \ a = 2c \ \wedge \ a, b$ sans facteur commun)

(E28) = $\langle$ $a = 2c$ signifie que a est pair. Puis que b aussi est pair, a et b ont un facteur commun (2). Nous avons donc « a, b ont un facteur commun » et « a, b sans facteur commun ». Cette proposition a la forme $p \wedge \neg p$. Elle la valeur faux et elle entraîne la fausseté de tout le corps de la quantification (par (3.53)). $\rangle$

(E29) $(\exists a, b, c{:}\mathbb{Z}^+ \mid{:}$ faux)

(E30) = $\langle$ (7.8) $\rangle$

(E31) faux.

Comparons maintenant les deux preuves.

1. C1, E1 : les deux preuves indiquent ce qui est démontré. Lorsque la propriété à démontrer est déjà énoncée sous forme de théorème, la preuve n'a évidemment pas à répéter ce qu'il faut démontrer.
2. C2, E2 : les deux preuves donnent leur définition de ce que signifie « $\sqrt{2}$ est irrationnel ». Dans la preuve C, on voit que « est rationnel » est la négation de « est irrationnel », ce qu'on retrouve en E6 dans la preuve formelle. En fait, le but de C2 est surtout d'introduire une variable x, égale à $\sqrt{2}$, qui est utilisée plus loin (la preuve E évite d'introduire une telle variable et utilise $\sqrt{2}$ partout). La formulation « si $x \in \mathbb{R}$ et $x^2 = 2$, alors x n'est pas un nombre rationnel » pourrait être formalisée par

   $$(\forall x \mid{:} x \in \mathbb{R} \ \wedge \ x^2 = 2 \ \Rightarrow \ x \text{ n'est pas un nombre rationnel}).$$

   C'est cette proprété qui est démontrée par contradiction.
3. E3 : cette partie de la preuve sert seulement à donner un nom à la propriété à démontrer. Ce nom est ensuite utilisé en E4 et E5 pour bien montrer que la structure de la preuve par contradiction est conforme à sa caractérisation dans les notes de cours. Normalement, le nom P ne serait pas introduit et la preuve commencerait à la ligne E7.
4. C3 : on indique que la preuve procède par contradiction et on suppose la négation de la propriété à démontrer. Il n'est pas clair pourquoi « $x \in \mathbb{R}$, $x^2 = 2$ et x est rationnel »

est la négation de « si $x \in \mathbb{R}$ et $x^2 = 2$, alors x n'est pas un nombre rationnel ». On sent bien que dans « supposons $x \in \mathbb{R}$, $x^2 = 2$ et x est rationnel », la variable x est quantifiée existentiellement (on suppose l'existence d'un x avec certaines propriétés), alors que dans « si $x \in \mathbb{R}$ et $x^2 = 2$, alors x n'est pas un nombre rationnel », x est quantifiée universellement, tel que mentionné dans le commentaire sur C2. Voici l'explication détaillée de cette négation :

$$
\begin{aligned}
& \neg(\forall x \mid: x \in \mathbb{R} \wedge x^2 = 2 \;\Rightarrow\; x \text{ n'est pas un nombre rationnel}) \\
= & \qquad \langle \text{ De Morgan (7.16c) } \rangle \\
& (\exists x \mid: \neg(x \in \mathbb{R} \wedge x^2 = 2 \;\Rightarrow\; x \text{ n'est pas un nombre rationnel})) \\
= & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75) } \rangle \\
& (\exists x \mid: \neg(\neg(x \in \mathbb{R} \wedge x^2 = 2) \;\vee\; x \text{ n'est pas un nombre rationnel})) \\
= & \qquad \langle \text{ De Morgan (3.48b) } \rangle \\
& (\exists x \mid: \neg\neg(x \in \mathbb{R} \wedge x^2 = 2) \;\wedge\; \neg(x \text{ n'est pas un nombre rationnel})) \\
= & \qquad \langle \text{ Double négation (3.15), deux fois } \rangle \\
& (\exists x \mid: x \in \mathbb{R} \wedge x^2 = 2 \;\wedge\; x \text{ est un nombre rationnel})
\end{aligned}
$$

5. C4, C5, E8 : les deux preuves assument connue la définition d'un nombre rationnel (c'est un nombre qui peut s'exprimer comme le rapport de deux entiers). La preuve C explique pourquoi on peut supposer que les deux entiers n'ont pas de facteur commun, alors que la preuve E suppose que c'est connu. La preuve E précise que les deux entiers sont positifs, vu que $\sqrt{2} > 0$. La preuve C mentionne que $b \neq 0$, mais cette mention est inutile, car elle n'est pas utilisée par la suite.
6. C4, E9 : les deux preuves introduisent les variables a et b. Dans la preuve C, elles sont implicitement quantifiées existentiellement (« avec $a, b \in \mathbb{Z}$ »), alors que la quantification est explicite dans la preuve E. Dans les preuves formelles, il y a une technique dite *d'introduction d'un témoin* qui permet de ne pas traîner inutilement des quantificateurs existentiels (de même que (7.33) permet d'éliminer le quantificateur universel, bien que ce soit un peu plus compliqué dans le cas du quantificateur existentiel). Nous n'avons pas vu cette technique dans le cours.
7. C6 : on attire l'attention sur un fait qui est utilisé plus loin ; c'est que la preuve C dérive la contradiction que a et b ne sont pas tous deux pairs et qu'ils sont tous deux pairs. La preuve E dérive plutôt la contradiction que a et b ont et n'ont pas de facteur commun.
8. C7 correspond à E10, E11, E12 et E13. Ces manipulations sont simples et la preuve E pourrait passer directement de E9 à E13.
9. C8 correspond à une partie de E16.
10. C9, E17 : on indique que a est pair.
11. L'usage de l'idempotence en E14 est artificiel (c'est vraiment le coup du lapin sorti du chapeau). En fait, il y a une transformation beaucoup plus naturelle, qui permet de passer directement de E13 à E17 (et avec une équivalence au lieu d'une implication). Mais pour cela, il faut utiliser la loi $(p \Rightarrow q) \wedge (p \Rightarrow r) \;\equiv\; p \Rightarrow q \wedge r$, qui n'est pas donnée dans les notes de cours.

12. C10 : pour déduire $(2c)^2 = 2b^2$, il faut se rappeler que $a = 2c$ (ligne C9) et que $a^2 = 2b^2$ (ligne C7). Dans la preuve E, on y arrive à la ligne E23, après quelques transformations.
13. C11, E27 : on déduit que b est pair.
14. C12, E28, E29 : on met en évidence la contradiction.
15. E30, E31 : simple transformation pour réduire la contradiction à sa plus simple expression, faux.
16. C13 : la preuve rappelle ce qu'on veut démontrer. Cette mention est facultative.
17. On peut remarquer que les deux preuves utilisent essentiellement les mêmes arguments. La preuve E est plus longue surtout parce qu'elle indique explicitement toutes les lois de la logique qui sont utilisées. Elle est aussi plus longue parce qu'elle traîne certaines sous-expressions pendant plusieurs étapes (par exemple, « a, b sans facteur commun ». La preuve C procède autrement : chaque fois qu'une nouvelle propriété est démontrée, elle est ajoutée à l'ensemble des propriétés connues et on peut l'utiliser n'importe où par la suite ; dans la preuve E, on peut utiliser seulement ce qui apparaît à la ligne précédente et ce qui a été supposé avant le début de la dérivation qui débute par $\neg P$. Ceci permet par contre à la preuve E de laisser tomber certaines informations intermédiaires dont on n'a plus besoin par la suite (comme $2b^2 = a^2$ en E21), avec l'assurance qu'on n'a plus à s'en préoccuper. Dans le cas d'une très longue preuve, le fait d'accumuler des tas de résultats intermédiaires peut compliquer la lecture, à moins de numéroter ceux qui sont utilisés suffisamment loin pour qu'on risque de ne plus s'en rappeler et d'y référer par leur numéro. Les preuves ci-dessus sont très simples et l'avantage est plutôt du côté de la preuve C. Pour des preuves plus complexes, l'idéal est de combiner les deux styles de présentation, en choisissant le plus approprié. Ceci dit, il est beaucoup plus facile de vérifier une preuve complète et bien formalisée, avec toutes les justifications, qu'une preuve informelle où plusieurs détails sont omis.

Voici un autre exemple de preuve par contradiction. Montrons qu'il n'y a pas de solution entière positive à l'équation $x^2 - y^2 = 1$.

Ce qu'il faut montrer est

$$\neg(\exists x, y{:}\mathbb{N}^+ \mid{:}\ x^2 - y^2 = 1).$$

La preuve par contradiction va comme suit.

$$\begin{array}{ll} & \neg\neg(\exists x, y{:}\mathbb{N}^+ \mid{:}\ x^2 - y^2 = 1) \\ = & \qquad \langle \text{ Double négation (3.15) } \rangle \\ & (\exists x, y{:}\mathbb{N}^+ \mid{:}\ x^2 - y^2 = 1) \\ = & \qquad \langle \text{ Décomposition de } x^2 - y^2 \rangle \\ & (\exists x, y{:}\mathbb{N}^+ \mid{:}\ (x+y)(x-y) = 1) \\ = & \qquad \langle \text{ Comme } x+y \text{ et } x-y \text{ sont des entiers, il n'y a que ces deux possibilités } \rangle \\ & (\exists x, y{:}\mathbb{N}^+ \mid{:}\ (x+y = 1 \wedge x-y = 1) \ \vee \ (x+y = -1 \wedge x-y = -1)) \end{array}$$

$=$ ⟨ En additionnant les deux premières équations, on obtient $2x = 2$, d'où $x = 1$ et $y = 0$. En faisant de même avec les deux dernières équations, on obtient $x = -1$ et $y = 0$ ⟩

$(\exists x, y{:}\mathbb{N}^+ \mid{:}\ (x = 1 \wedge y = 0) \ \vee \ (x = -1 \wedge y = 0))$

$=$ ⟨ On ne peut avoir $y = 0$, puisque $y \in \mathbb{N}^+$ ⟩

$(\exists x, y{:}\mathbb{N}^+ \mid{:}\ (x = 1 \wedge \mathsf{faux}) \ \vee \ (x = -1 \wedge \mathsf{faux}))$

$=$ ⟨ Zéro de $\wedge$ (3.53) ⟩

$(\exists x, y{:}\mathbb{N}^+ \mid{:}\ \mathsf{faux} \vee \mathsf{faux})$

$=$ ⟨ Identité de $\vee$ (3.40) ⟩

$(\exists x, y{:}\mathbb{N}^+ \mid{:}\ \mathsf{faux})$

$=$ ⟨ (7.8) ⟩

faux.

Remarquez qu'on a bien des égalités (équivalences) entre chaque paire de formules. Comme nous n'avons besoin que de l'implication $\neg\neg(\exists x, y{:}\mathbb{N}^+ \mid{:}\ x^2 - y^2 = 1) \ \Rightarrow \ \mathsf{faux}$, il est possible d'utiliser des implications dans la dérivation lorsque l'implication inverse n'est pas évidente. Par exemple,

$(\exists x, y{:}\mathbb{N}^+ \mid{:}\ (x + y)(x - y) = 1)$

$\Rightarrow$ ⟨ Comme $x + y$ et $x - y$ sont des entiers, il n'y a que ces deux possibilités
&
Monotonie de $\exists$ (7.36) ⟩

$(\exists x, y{:}\mathbb{N}^+ \mid{:}\ (x + y = 1 \wedge x - y = 1) \ \vee \ (x + y = -1 \wedge x - y = -1))$

9.5 Preuves par contraposition

(9.21) Méthode de preuve :
Pour démontrer $P \Rightarrow Q$, montrez $\neg Q \Rightarrow \neg P$.

Cette méthode découle du théorème (3.77) $p \Rightarrow q \ \equiv \ \neg q \Rightarrow \neg p$.

(9.22) Exemple. Montrons $x + y \geq 2 \ \Rightarrow \ x \geq 1 \vee y \geq 1$.
Appliquons la méthode et démontrons $\neg(x \geq 1 \vee y \geq 1) \Rightarrow \neg(x + y \geq 2)$.

$\neg(x \geq 1 \vee y \geq 1)$

$=$ ⟨ De Morgan (3.48b), avec $p, q := x \geq 1, \ y \geq 1$ ⟩

$\neg(x \geq 1) \wedge \neg(y \geq 1)$

$=$ ⟨ Arithmétique (définition de $\geq$) ⟩

$$
\begin{array}{ll}
 & x < 1 \wedge y < 1 \\
\Rightarrow & \quad \langle \text{ Arithmétique } \rangle \\
 & x + y < 2 \\
= & \quad \langle \text{ Arithmétique (définition de } \geq) \rangle \\
 & \neg(x + y \geq 2)
\end{array}
$$

9.6 Problèmes

1. Démontrez le théorème de substitution (9.3b),

$$e = f \;\Rightarrow\; E[z := e] \;\equiv\; e = f \;\Rightarrow\; E[z := f].$$

2. Démontrez le théorème d'affaiblissement/renforcement (3.92e), $p \wedge q \;\Rightarrow\; p \wedge (q \vee r)$, en utilisant le remplacement par vrai (9.4b). Normalement, il n'est pas permis d'utiliser un théorème qui suit le théorème à démontrer, mais puisque l'exercice le demande, c'est ce qu'il faut faire.
3. Soit $x \downarrow y$ le minimum de deux entiers, défini par

$$x \downarrow y \;=\; (\textbf{si } x \leq y \textbf{ alors } x \textbf{ sinon } y).$$

   Montrez que $\downarrow$ est commutatif, c'est-à-dire $b \downarrow c = c \downarrow b$. Combien de cas devez-vous considérer ? Vous pouvez utiliser les règles usuelles de l'arithmétique des entiers, comme $b \leq c \;\equiv\; b = c \vee b < c$ et $b < c \equiv c > b$.

Chapitre 10

Prédicats et programmation

10.1 Instruction d'affectation

L'affectation est une instruction fournie par les langages de programmation dits *impératifs*. La syntaxe varie selon les langages :

1. $x := E$ (Algol, PL1, Pascal, Eiffel, Ada, ...)
   C'est la notation la plus répandue et c'est celle que nous utiliserons.
2. $x = E$ (FORTRAN, C, ...)
   Cette notation est malheureuse, car elle amène une confusion entre les notions d'affectation et d'égalité.
3. $x \leftarrow E$ (APL)

Dans cette instruction, x est une variable et E est une expression. L'effet de l'instruction est de placer la valeur de E dans la variable x.

Supposons un programme avec les variables entières v, w, x. *L'état du programme* est la liste de ses variables avec leur valeur, par exemple

$$(v, 10),\ (w, 6),\ (x, 13)\ .$$

Après l'exécution de l'affectation $v := v + x$, l'état est

$$(v, 23),\ (w, 6),\ (x, 13)\ .$$

Prononciation : $x := E$, $x = E$ et $x \leftarrow E$ se prononcent « x devient E ».

État initial, état final

Soit S un programme ou une instruction d'un programme. Un *état* de S est une liste de valeurs de ses variables. L'*état initial* est l'état avant l'exécution de S. L'*état final* est l'état après l'exécution de S.

On parle souvent de *programme* au lieu d'*instruction*, même si, strictement parlant, une instruction est une partie de programme.

Triplets de Hoare (1969)

Un *triplet de Hoare* [5] est une expression booléenne —qui a donc la valeur vrai ou la valeur faux dans un état donné— de la forme

(10.1) $\{P\}\ \ S\ \ \{Q\}$.

Dans cette expression, S est une instruction (ou un programme), P est une expression booléenne appelée la *précondition* et Q est une expression booléenne appelée la *postcondition*. Par définition, cette formule correspond à la proposition suivante :

> Si l'état initial satisfait P, alors l'exécution de S se termine normalement et l'état final satisfait Q.

L'expression $\{P\}\ \ S\ \ \{Q\}$ est *valide* si elle a la valeur vrai dans tous les états.

(10.2) Exercice. L'exécution de $x := x + 1$ se termine-t-elle normalement ?

(10.3) Exemple. L'expression

$$\{\mathsf{pair}.x\}\ \ x := x + 1\ \ \{\mathsf{impair}.x\}$$

est valide, mais pas

$$\{0 \leq x \leq 10\}\ \ x := x^2\ \ \{0 \leq x \leq 10\}\ ,$$

car elle a la valeur faux pour tout état initial tel que $\boxed{4 \leq x \leq 10}$.

(10.4) Exercice. Les triplets de Hoare suivants sont-ils valides ? Les variables sont $x, y{:}\mathbb{Z}$.

1. $\{x \geq y\}\ \ x := x + 1\ \ \{x > y\}$
2. $\{\mathsf{vrai}\}\ \ y := x + y + 1\ \ \{y > x\}$

Définition axiomatique de l'affectation

(10.5) Définition de l'affectation : Pourvu que E soit définie dans tous les états,

$$\{R[x\ :=\ E]\}\ \ x := E\ \ \{R\}$$

Cette définition est en fait un axiome que l'on impose à l'affectation et qui détermine le comportement de l'affectation en établissant un lien entre l'état initial et l'état final. On dit que l'on définit ainsi la *sémantique* de l'affectation (sa signification). Cette sémantique est dite *axiomatique*. On peut aussi donner une sémantique *opérationnelle* en expliquant comment l'affectation est exécutée (ceci peut se faire de manière mathématique). Le cours *Langages de programmation* aborde la notion de sémantique de manière plus approfondie.

(10.6) Exemple.

1. $\{(\mathsf{pair}.x)[x := x+1]\}\ \ x := x+1\ \ \{\mathsf{pair}.x\}$
   $=$ ⟨ Substitution ⟩
   $\{\mathsf{pair}(x+1)\}\ \ x := x+1\ \ \{\mathsf{pair}.x\}$
   $=$ ⟨ Définition de pair et impair ⟩
   $\{\mathsf{impair}.x\}\ \ x := x+1\ \ \{\mathsf{pair}.x\}$
   Si la valeur initiale de x est impaire, alors l'exécution de l'instruction $x := x+1$ se termine normalement et la valeur finale de x est paire.

2. $\{(x > 100)[x := x^2]\}\ \ x := x^2\ \ \{x > 100\}$
   $=$ ⟨ Substitution ⟩
   $\{x^2 > 100\}\ \ x := x^2\ \ \{x > 100\}$
   $=$ ⟨ Racine carrée ⟩
   $\{x < -10 \vee x > 10\}\ \ x := x^2\ \ \{x > 100\}$
   Si la valeur initiale de x est inférieure à -10 ou supérieure à 10, alors l'exécution de $x := x^2$ se termine normalement et la valeur finale de x satisfait $x > 100$.

3. $\{(x \neq 5)[x := 5]\}\ \ x := 5\ \ \{x \neq 5\}$
   $=$ ⟨ Substitution ⟩
   $\{5 \neq 5\}\ \ x := 5\ \ \{x \neq 5\}$
   $=$ ⟨ Évaluation de $5 \neq 5$ ⟩
   $\{\mathsf{faux}\}\ \ x := 5\ \ \{x \neq 5\}$
   Cette expression signifie que si l'état initial satisfait faux, alors l'exécution de $x := 5$ se termine normalement et l'état final satisfait $x \neq 5$. Comme aucun état ne peut satisfaire faux, l'expression est trivialement vraie.

(10.7) Remarque. Dans la définition (10.5), x et E peuvent être des listes (substitution et affectation multiples).

Traitement des fonctions partielles

La définition de l'affectation (10.5) s'applique seulement si E est définie dans tous les états (on dit que E est *totale*). Il existe des expressions qui ne sont pas totales (on dit qu'elles sont *partielles*).

(10.8) Exemple.

1. $1/x$ n'est pas définie si $x = 0$.
2. Si $c[0..10]$:tableau, l'expression $c[12]$ n'est pas définie.

(10.9) Définition. Le *domaine* d'une expression E est noté dom.‘E’. Ce prédicat est vrai dans un état si et seulement si E est définie dans cet état.

(10.10) Exemple.

1. dom.‘$1/x$’ $\equiv$ $x \neq 0$.
2. Si c[0..10]:tableau, alors dom.‘$c[i]$’ $\equiv$ $0 \leq i \leq 10$.

(10.11) Définition de l'affectation : $\{\text{dom.‘}E\text{’} \wedge R[x := E]\}\ \ x := E\ \ \{R\}$

(10.12) Exemple. Si c[0..10]:tableau, alors

$$\{\text{dom.‘}c[i]\text{’} \wedge (x = 25)[x := c[i]]\}\ \ x := c[i]\ \ \{x = 25\}$$

c'est-à-dire $\{0 \leq i \leq 10 \wedge c[i] = 25\}\ \ x := c[i]\ \ \{x = 25\}$.

10.2 Spécification de programmes

Une spécification de programme a la forme

$$\{Q\}\ \ x := ?\ \ \{R\}$$

- Q, la *précondition*, est une expression *booléenne* qui décrit les états initiaux pour lesquels l'exécution du programme est définie.
- x est la liste des variables qui *peuvent* être modifiées par le programme (elles ne sont pas forcément modifiées).
- R, la *postcondition*, est une expression *booléenne* qui caractérise les états finaux du programme.

Exemple de spécification

Supposons b:$\mathbb{Z}$. La spécification

$$\{b = 0\}\ \ b := ?\ \ \{b^2 = 25\}$$

spécifie un programme qui débute l'exécution dans l'état $(b, 0)$ et qui la termine soit dans l'état $(b, -5)$, soit dans l'état $(b, 5)$. On dit que la spécification est *non déterministe*, car elle permet plusieurs états finaux pour un état initial donné.

(10.13) Exercice.

1. Donnez deux instructions qui satisfont la spécification

$$\{b = 0\}\ \ b := ?\ \ \{b^2 = 25\}$$

(on dit que les instructions sont correctes par rapport à la spécification).

2. Expliquez la spécification suivante. Que spécifie-t-elle ?

$$\{x > y\} \quad x, y := ? \quad \{x < y\}$$

Que pourrait-être « ? ».

Exemples de spécifications : trouver x dans b

(10.14) Notation. La déclaration

$$b[0..n-1]\text{:tableau}$$

indique que la variable b est un tableau à n cases indicées de 0 à $n-1$. Pour préciser que le tableau contient des entiers (par exemple), nous écrivons

$$b[0..n-1]\text{:tableau de } \mathbb{Z} \ .$$

L'expression

$$x \in b[0..n-1]$$

est une abréviation de

$$(\exists j \mid 0 \leq j < n : x = b[j]) \ .$$

Supposons

$$x, i, n{:}\mathbb{Z}, \quad b[0..n-1]\text{:tableau de } \mathbb{Z}.$$

La spécification

$$\{x \in b[0..n-1]\} \quad i := ? \quad \{0 \leq i < n \ \wedge \ x = b[i]\}$$

spécifie un programme qui peut s'appliquer à un tableau qui contient la valeur x. Après l'exécution du programme, i doit contenir l'indice de x dans b. La variable i est la seule qui peut être modifiée.

Avec la spécification

$$\{0 \leq n\} \quad i := ? \quad \{(0 \leq i < n \ \wedge \ x = b[i]) \ \vee \ (i = n \ \wedge \ x \notin b[0..n-1])\}$$

x n'est pas forcément dans b. Après l'exécution du programme, i doit contenir l'indice de x si x est dans b et la valeur n dans le cas contraire. Notez qu'il peut y avoir plusieurs valeurs finales possible pour i, s'il y a plus d'une occurrence de x dans b.

(10.15) Exercice. Soit $b[0..n-1]$:tableau de $\mathbb{Z}$, où $n \geq 0$, et soient j et k deux variables entières satisfaisant $0 \leq j \leq k < n$.

Traduisez les phrases suivantes en expressions booléennes.

1. Aucune valeur de $b[j..k]$ n'est 0.
2. Les valeurs de $b[j..k]$ sont en ordre croissant.

(10.16) Exercice. Expliquez la spécification suivante. Ensuite, modifiez-la pour qu'elle décrive un programme qui produit *le plus petit indice* i tel que $b[i] = x$ si x est dans b et la valeur n dans le cas contraire (c'est presque ce qu'elle fait déjà).

$$\{0 \leq n\} \quad i := ? \quad \{(0 \leq i < n \ \wedge \ x \notin b[0..i-1]) \ \wedge \ (x = b[i] \ \vee \ i = n)\}$$

Variables rigides

Les variables *rigides* sont utilisées dans les spécifications pour référer à l'état initial dans la postcondition ou à l'état final dans la précondition. Il faut choisir des identificateurs qui ne sont pas des variables du programme. Le présent texte utilise une police sans sérif pour les variables rigides (*pour l'écriture manuelle, utilisez des majuscules*). Puisque ces variables ne sont pas des variables du programme, elles ont la même valeur dans la précondition et la postcondition (d'où le qualificatif *rigide*).

(10.17) Exemple. Soit la spécification

$$\{x = \mathsf{X}\} \quad x := ? \quad \{x^2 = \mathsf{X}\}$$

La valeur finale de x doit satisfaire $x^2 = \mathsf{X}$, c'est-à-dire qu'elle doit être égale à la racine carrée de la valeur initiale de x, puisque la précondition exige $x = \mathsf{X}$.

10.3 Plus faibles préconditions

Rappelons que si $p \Rightarrow q$, on dit que p est *plus forte* que q. La condition (proposition) faux est très forte, car faux $\Rightarrow q$, quelle que soit la condition q ; elle est tellement forte qu'elle est contradictoire. Par contre, vrai est très faible. On a vrai $\Rightarrow q$ seulement si $q =$ vrai. N'importe quel état satisfait vrai, car vrai n'impose aucune contrainte.

Soit S une instruction. Quand le triplet de Hoare

$$\{Q\} \quad S \quad \{R\}$$

est-il un théorème ? C'en est un si la précondition Q est suffisamment forte (par exemple, c'en est un si $Q =$ faux). Ça peut ne pas en être un si Q est trop faible. Par exemple, si $Q =$ vrai, alors l'instruction S doit terminer dans un état qui satisfait R, *quel que soit l'état initial*. Ça peut être impossible.

Nous nous intéressons à la condition Q la plus faible qui fait que

$$\{Q\} \quad S \quad \{R\}$$

soit un théorème. La condition Q décrit alors le plus grand ensemble d'états pour lesquels l'exécution de l'instruction S se termine dans un état qui satisfait R.

(10.18) Notation. Soit S une instruction quelconque. La plus faible précondition Q telle que $\{Q\}\ \ S\ \ \{R\}$ est un théorème est notée $\mathsf{wp}(S, R)$.

« wp » est une abréviation de *weakest precondition*. Cette notation est due à Dijkstra [1, 2].

(10.19) Remarque. Par définition de wp,

$$\{\mathsf{wp}(S, R)\}\ \ S\ \ \{R\}$$

est un théorème.

Avec wp, nous pouvons exprimer une condition équivalente à $\{Q\}\ \ S\ \ \{R\}$:

(10.20) Axiome : $\{Q\}\ \ S\ \ \{R\}\ \ \equiv\ \ Q \Rightarrow \mathsf{wp}(S, R)$.

$\{Q\}\ \ S\ \ \{R\}$ est donc un théorème ssi la condition Q est au moins aussi forte que wp(S,R).

La fonction wp peut être utilisée pour définir la sémantique des diverses instructions d'un langage de programmation. Elle est à la base d'un calcul appelé le wp-*calcul*, employé pour la dérivation de programmes à partir de spécifications [1, 2, 3]. Nous l'utiliserons pour la définition de l'affectation et de la séquence. Elle peut aussi être utilisée pour définir les instructions conditionnelles et les boucles, mais nous procéderons autrement, par simplicité, vu que notre objectif est de donner quelques outils mathématiques pour la *vérification* de programmes, même s'ils ne sont pas aussi appropriés que le wp-calcul pour la *dérivation* de programmes.

10.4 Axiome de l'affectation

L'axiome que nous utiliserons comme définition de l'affectation est le suivant.

(10.21) Axiome de l'affectation :

$$\mathsf{wp}(x := E, R)\ \ \equiv\ \ \mathsf{dom}.\text{`}E\text{'} \wedge R[x\ :=\ E].$$

Si les expressions de la liste E sont totales, on obtient une forme simplifiée.

(10.22) Axiome de l'affectation si E totale :

$$\mathsf{wp}(x := E, R)\ \ \equiv\ \ R[x\ :=\ E].$$

(10.23) Remarque. En utilisant ces axiomes et la remarque (10.19), on retrouve les définitions (10.11) et (10.5). L'axiome (10.22) est un peu plus intéressant que la définition (10.5), car il précise que la précondition $R[x\ :=\ E]$ ne peut être affaiblie (par définition de wp). La même remarque s'applique à l'axiome (10.21) versus la définition (10.11).

Preuves de $\{Q\}\ \ x := E\ \ \{R\}$

Si $\boxed{\{Q\}\ \ x := E\ \ \{R\}}$ est un théorème, on dit que l'instruction $x := E$ est *correcte* par rapport à la spécification $\boxed{\{Q\}\ \ x := ?\ \ \{R\}}$, ou encore que $x := E$ est une *implantation* de la spécification $\{Q\}\ \ x := ?\ \ \{R\}$. Par les axiomes (10.20) et (10.22), $R[x := E]$ est *la plus faible précondition* Q telle que $x := E$ est une implantation de la spécification $\{Q\}\ \ x := ?\ \ \{R\}$ (lorsque E est totale).

(10.24) Exercice. Reprenons les exemples illustrant l'évaluation de la validité des triplets de Hoare donnés à l'exercice (10.4) pour maintenant illustrer l'usage de (10.20) et de l'axiome de l'affectation (10.22).

Les triplets de Hoare suivants sont-ils des théorèmes ? Les variables sont $x, y{:}\mathbb{Z}$.

1. $\{x \geq y\}\ \ x := x + 1\ \ \{x > y\}$
2. $\{\mathsf{vrai}\}\ \ y := x + y + 1\ \ \{y > x\}$

(10.25) Remarque. Dans la partie 3 de l'exemple (10.6), nous avons conclu que l'expression $\{\mathsf{faux}\}\ \ x := 5\ \ \{x \neq 5\}$ est trivialement vraie. Nous pouvons maintenant le vérifier.

$$
\begin{array}{ll}
 & \{\mathsf{faux}\}\ \ x := 5\ \ \{x \neq 5\} \\
= & \qquad \langle\ (10.20)\ \rangle \\
 & \mathsf{faux} \Rightarrow \mathsf{wp}(x := 5, x \neq 5) \qquad \text{—(3.91), avec } p := \mathsf{wp}(x := 5, x \neq 5)
\end{array}
$$

(10.26) Exercice. Cet exercice est relié à l'exercice (10.24), où on montre que le triplet

$$\{\mathsf{vrai}\}\ \ y := x + y + 1\ \ \{y > x\}$$

n'est pas valide.

Quelle est la plus faible condition Q telle que

$$\{Q\}\ \ y := x + y + 1\ \ \{y > x\}\ ?$$

Exemple d'une preuve de $\{Q\}\ \ x := E\ \ \{R\}$

Soit $b[0..n-1]{:}\mathsf{tableau}$ et soit le prédicat

$$P : \quad 0 \leq j \leq n\ \ \wedge\ \ x = (\sum k \mid 0 \leq k < j : b[k]).$$

Montrons que l'instruction

$$x, j := \ x + b[j],\ j + 1$$

implante la spécification

(10.27) $\{P \wedge \mathsf{J} = j \neq n\}\ \ x, j := ?\ \ \{P \wedge j = \mathsf{J} + 1\}$

Par définition de la notion d'implantation, il faut montrer

$$\{P \wedge \mathsf{J} = j \neq n\} \;\; x, j := \; x + b[j], \; j + 1 \;\; \{P \wedge j = \mathsf{J} + 1\}.$$

Selon l'axiome (10.20), il faut montrer

$$P \wedge \mathsf{J} = j \neq n \quad \Rightarrow \quad \mathsf{wp}((x, j := \; x + b[j], \; j + 1), \; P \wedge j = \mathsf{J} + 1).$$

Assumons l'antécédent et démontrons le conséquent. En tenant compte de $j \neq n$ et de la définition de P, l'antécédent est

(10.28) $\mathsf{J} = j \;\wedge\; 0 \leq j < n \;\wedge\; x = (\sum k \mid 0 \leq k < j : b[k])$.

$$\begin{array}{ll}
& \mathsf{wp}((x, j := \; x + b[j], \; j + 1), \; P \wedge j = \mathsf{J} + 1) \\
= & \qquad \langle \text{ L'expression } x + b[j] \text{ est totale, puisque } 0 \leq j < n \text{ par hypothèse } \; \& \\
& \qquad \;\; \text{L'expression } j + 1 \text{ est totale } \; \& \; \text{Axiome de l'affectation (10.22) } \rangle \\
& (P \wedge j = \mathsf{J} + 1)[x, j \; := \; x + b[j], \; j + 1] \\
= & \qquad \langle \text{ Définition de } P \; \rangle \\
& (0 \leq j \leq n \;\wedge\; x = (\sum k \mid 0 \leq k < j : b[k]) \;\wedge\; j = \mathsf{J} + 1)[x, j \; := \; x + b[j], \; j + 1] \\
= & \qquad \langle \text{ Substitution } \; \& \; (6.14) \; \& \; \neg\mathsf{libre}(\text{`}k\text{'}, \text{`}x, j, x + b[j], j + 1\text{'}) \; \rangle \\
& (0 \leq j + 1 \leq n \\
& \wedge\; x + b[j] = (\sum k \mid 0 \leq k < j + 1 : b[k]) \;\wedge\; j + 1 = \mathsf{J} + 1) \\
\Leftarrow & \qquad \langle \text{ Arithmétique } \; \& \; 0 \leq j \; \Rightarrow \; 0 \leq j + 1 \; \& \; \text{Monotonie de } \wedge \text{ (4.3), avec} \\
& \qquad \;\; p, q, r \; := \; 0 \leq j, 0 \leq j + 1, x + b[j] = (\sum k \mid 0 \leq k < j + 1 : b[k]) \;\wedge\; j = \mathsf{J} \; \rangle \\
& 0 \leq j < n \;\wedge\; x + b[j] = (\sum k \mid 0 \leq k < j + 1 : b[k]) \;\wedge\; j = \mathsf{J} \\
= & \qquad \langle \text{ Extraction d'un terme (6.40), avec } j, n, P \; := \; k, \; j, \; b[k] \; \rangle \\
& 0 \leq j < n \;\wedge\; x + b[j] = (\sum k \mid 0 \leq k < j : b[k]) + b[j] \;\wedge\; j = \mathsf{J} \\
= & \qquad \langle \text{ Arithmétique } \rangle \\
& 0 \leq j < n \;\wedge\; x = (\sum k \mid 0 \leq k < j : b[k]) \;\wedge\; j = \mathsf{J} \qquad \text{—Ceci est (10.28)}
\end{array}$$

10.5 Séquence

Soient S_1 et S_2 deux instructions. Dans beaucoup de langages, la séquence des instructions S_1 et S_2 est dénotée par $S_1; S_2$. Cette séquence est exécutée en exécutant d'abord S_1, puis S_2 si l'exécution de S_1 se termine.

On peut définir axiomatiquement la séquence par la formule

$$\{P\} \;\; S_1 \;\; \{Q\} \;\; \wedge \;\; \{Q\} \;\; S_2 \;\; \{R\} \;\; \Rightarrow \;\; \{P\} \;\; S_1; S_2 \;\; \{R\}$$

(voir [5], par exemple).

L'inconvénient de cette approche, c'est que pour montrer

$$\{P\} \;\; S_1; S_2 \;\; \{R\},$$

il faut trouver un prédicat Q convenable, puis montrer

$$\{P\} \;\; S_1 \;\; \{Q\} \qquad \text{et} \qquad \{Q\} \;\; S_2 \;\; \{R\}.$$

Nous utiliserons plutôt une méthode basée sur l'axiome suivant. Elle n'oblige pas à inventer un prédicat.

(10.29) Axiome de la séquence :

$$\mathsf{wp}(S_1; S_2, R) \;\equiv\; \mathsf{wp}(S_1, \mathsf{wp}(S_2, R)).$$

Ainsi, pour calculer la plus faible précondition $\mathsf{wp}(S_1; S_2, R)$, il faut d'abord calculer $\mathsf{wp}(S_2, R)$, puis $\mathsf{wp}(S_1, \mathsf{wp}(S_2, R))$. On propage donc la postcondition R à rebours.

Pour montrer

$$\{P\} \;\; S_1; S_2 \;\; \{R\},$$

il suffit de montrer

$$P \;\Rightarrow\; \mathsf{wp}(S_1; S_2, R),$$

par l'axiome (10.20).

Exemple : plus faible précondition d'une séquence d'affectations

Soient les expressions totales E et F. Quelle est la plus faible précondition qui assure que la séquence

$$x := E;\; y := F$$

termine dans un état qui satisfait la postcondition R ? C'est-à-dire, quelle est la plus faible précondition Q qui fait que l'expression suivante est un théorème ?

$$\{Q\} \;\; x := E;\; y := F \;\; \{R\}$$

Réponse : La précondition Q désirée est $\mathsf{wp}(x := E;\; y := F,\; R)$. Calculons-la.

$$\begin{array}{ll} & \mathsf{wp}(x := E;\; y := F,\; R) \\ = & \qquad \langle \text{ Axiome de la séquence (10.29) } \rangle \\ & \mathsf{wp}(x := E,\; \mathsf{wp}(y := F,\; R)) \\ = & \qquad \langle \text{ Axiome de l'affectation (10.22) } \;\&\; F \text{ est totale par hypothèse } \rangle \\ & \mathsf{wp}(x := E,\; R[y := F]) \\ = & \qquad \langle \text{ Axiome de l'affectation (10.22) } \;\&\; E \text{ est totale par hypothèse } \rangle \\ & R[y := F][x := E] \end{array}$$

La précondition recherchée est donc

$$R[y := F][x := E].$$

Rappel : La substitution est associative à gauche. Remarquez comment les substitutions se font dans l'ordre inverse de l'exécution. C'est dû à la propagation arrière de la postcondition imposée par l'axiome (10.29).

(10.30) Exercice. Montrez

$$\{y = \mathsf{X} \ \wedge \ x = \mathsf{Y}\} \ \ t := x; \ x := y; \ y := t \ \ \{x = \mathsf{X} \ \wedge \ y = \mathsf{Y}\}.$$

Dites ce que fait le programme.

10.6 Instruction skip

(10.31) Axiome de l'instruction skip : $\{Q\}$ **skip** $\{R\} \quad \equiv \quad Q \Rightarrow R.$

On en tire $\{R\}$ **skip** $\{R\}$. L'instruction **skip** ne fait rien. Pour établir la postcondition R, il suffit que la précondition R soit vraie.

10.7 Instruction conditionnelle

L'instruction conditionnelle, que nous dénoterons par IF, a la forme suivante dans plusieurs langages de programmation :

(10.32) IF **:** **if** B **then** S_1 **else** S_2

où B est une expression booléenne et S_1 et S_2 sont des instructions. IF est exécutée de la manière suivante : si B a la valeur vrai, S_1 est exécutée, sinon S_2 est exécutée.

Quand l'expression

$$\{Q\} \ \ \mathsf{IF} \ \ \{R\}$$

est-elle un théorème ?

- Si B, c'est S_1 qui est exécutée et qui doit satisfaire R.
- Si $\neg B$, c'est S_2 qui est exécutée et qui doit satisfaire R.

Annotons IF pour refléter cela :

$\{Q\}$
if B **then** $\{Q \wedge B\} \ \ S_1 \ \ \{R\}$
else $\{Q \wedge \neg B\} \ \ S_2 \ \ \{R\}$
$\{R\}$

(10.33) Axiome de l'instruction conditionnelle :

$$\{Q\}\ \mathsf{IF}\ \{R\} \quad \equiv \quad \{Q \wedge B\}\ S_1\ \{R\} \quad \wedge \quad \{Q \wedge \neg B\}\ S_2\ \{R\}.$$

On déduit de cet axiome que pour prouver $\{Q\}\ \mathsf{IF}\ \{R\}$ il suffit de prouver

$$\{Q \wedge B\}\ S_1\ \{R\} \quad \text{et} \quad \{Q \wedge \neg B\}\ S_2\ \{R\}.$$

(10.34) Exemple. Pour montrer

$\{\mathsf{vrai}\}$
if $x \leq y$ **then skip else** $x, y := y, x$
$\{x \leq y\}$

il suffit de montrer

$\{\mathsf{vrai} \wedge x \leq y\}$ **skip** $\{x \leq y\}$
$\{\mathsf{vrai} \wedge \neg(x \leq y)\}$ $x, y := y, x$ $\{x \leq y\}$

ce qui est trivial. (Remarque : il ne faut pas écrire $\neg x \leq y$, mais $\neg(x \leq y)$, car $\neg$ a préséance sur $\leq$.) Évidemment, on peut aussi écrire $x > y$.

(10.35) Exercice. Supposons $x, y, z{:}\mathbb{Z}$. Montrez

$\{\mathsf{vrai}\}$
if $x \leq y$ **then** $z := x$ **else** $z := y$
$\{z = \mathsf{min}(x, y)\}$,

où $\mathsf{min}(x, y)$ est le minimum de x et y.

10.8 Bloc begin-end

Les mots clés **begin** et **end** servent à regrouper en une seule instruction une séquence d'instructions. Ils agissent comme les parenthèses pour les expressions mathématiques.

(10.36) Exemple.

1. **if** $x > 1$ **then begin** $x := 5; y := 10$ **end else begin** $x := 15; y := 20$ **end**
   est lue comme
   if $x > 1$ **then** $(x := 5; y := 10)$ **else** $(x := 15; y := 20)$.

2. **if** $x > 1$ **then** $x := 5$ **else** $x := 15; y := 20$
   est lue comme
   (**if** $x > 1$ **then** $x := 5$ **else** $x := 15); y := 20$.

3. **if** $x > 1$ **then** $x := 5; y := 10$ **else** $x := 15$
   est syntaxiquement incorrecte.

(10.37) Axiome du bloc begin-end :

$$\{Q\} \quad \textbf{begin } S \textbf{ end} \quad \{R\} \quad \equiv \quad \{Q\} \quad S \quad \{R\},$$

où S est une instruction.

10.9 Itération (boucle)

Le traitement des boucles est plus complexe et plus intéressant que celui des autres instructions. Il nécessite en particulier l'usage des techniques de preuve par induction.

Syntaxe de la boucle

La syntaxe suivante est utilisée dans plusieurs langages de programmation :

$$\textbf{while } B \textbf{ do } S.$$

1. B est une expression booléenne appelée la *garde* ou encore le *test* de la boucle ;
2. S est une instruction appelée le *corps* de la boucle.

Exécution de while B do S

La boucle **while** B **do** S est exécutée de la manière suivante :

1. si le test B est faux, l'exécution se termine sans changer l'état ;
2. si le test B est vrai, le corps S est exécuté, puis la boucle **while** B **do** S est exécutée à nouveau.

Chaque exécution de S est appelée une *itération*.

(10.38) Exemple. Supposons que l'état initial est $(x, 2), (y, 5), (z, 8)$. La boucle

$$\textbf{while } x \neq 0 \textbf{ do begin } x := x - 1; y := y + 2 \textbf{ end}$$

passe par les états suivants lorsqu'elle est exécutée.

Étape	État
État initial	$(x,2),(y,5),(z,8)$
Après le test $x \neq 0$	$(x,2),(y,5),(z,8)$
Après $x := x-1$	$(x,1),(y,5),(z,8)$
Après $y := y+2$	$(x,1),(y,7),(z,8)$
Après le test $x \neq 0$	$(x,1),(y,7),(z,8)$
Après $x := x-1$	$(x,0),(y,7),(z,8)$
Après $y := y+2$	$(x,0),(y,9),(z,8)$
Après le test $x \neq 0$	$(x,0),(y,9),(z,8)$

Invariant de boucle

(10.39) $\{0 \leq n\}$
$i, f := 0, 1\,;$
$\{\text{Invariant } 0 \leq i \leq n \ \wedge \ f = i!\}$
while $i \neq n$ **do**
begin
$i := i+1\,;$
$f := f \cdot i$
end
$\{f = n!\}$

Un invariant de boucle est un prédicat qui est vrai avant et après chaque itération d'une boucle (pourvu qu'il soit vrai avant la première itération). Dans le programme ci-contre, le prédicat

$$0 \leq i \leq n \ \wedge \ f = i!$$

est un invariant de la boucle, ce qui est explicitement indiqué par le mot « Invariant ».

(10.40) Remarque.

1. Le programme ci-dessus calcule la factorielle de n, comme l'indique la postcondition. Comme le programme ne modifie par n, la valeur finale de f est la factorielle de la valeur initiale de n. Pour la définition de la factorielle, voir (8.10).
2. Remarque : les diverses *annotations* entre $\{\}$ sont appelées des *assertions*.

Théorème sur les invariants de boucle

(10.41) Théorème d'invariance : Supposons

1. $\{P \wedge B\} \ \ S \ \ \{P\}$
(c'est-à-dire que l'exécution de S se termine dans un état qui satisfait P si elle débute dans un état qui satisfait P et B) ;
2. $\{P\} \quad$ **while** B **do** $S \ \ \{\mathsf{vrai}\}$
(c'est-à-dire que l'exécution de la boucle se termine si elle débute dans un état qui satisfait P).

Alors

$$\{P\} \quad \textbf{while } B \textbf{ do } S \ \ \{P \wedge \neg B\}$$

est un théorème.

Démonstration. Par définition d'un triplet de Hoare (10.1), il faut montrer

1. que la boucle se termine si l'exécution débute dans un état qui satisfait P. Ceci est assuré par l'hypothèse 2 ;
2. que $P \wedge \neg B$ est satisfait dans l'état final.
   (a) $\neg B = \mathsf{vrai}$ dans l'état final, car la boucle se termine seulement lorsque $B = \mathsf{faux}$.
   (b) La preuve que $P = \mathsf{vrai}$ dans l'état final est une preuve par induction qui montre que $P = \mathsf{vrai}$ après un nombre quelconque $n \geq 0$ d'itérations de la boucle. Ceci est vrai en particulier pour la dernière itération qui mène dans l'état final. Notons que le nombre d'itérations menant à l'état final dépend de l'état initial.

   La propriété à démontrer est

   $$(\forall n{:}\mathbb{N} \mid{:} \text{ si l'exécution débute dans un état qui satisfait } P, \text{ alors l'état atteint après } n \text{ itérations satisfait } P).$$

   i. Définition du prédicat d'induction Q : Choisissons comme prédicat d'induction

   $$Q.n : \quad \text{si l'exécution débute dans un état qui satisfait } P, \text{ alors l'état atteint après } n \text{ itérations satisfait } P.$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:} Q.n)$.

   ii. Étape de base : il faut prouver $Q.0$, c'est-à-dire

   $$\text{si l'exécution débute dans un état qui satisfait } P, \text{ alors l'état atteint après 0 itération satisfait } P.$$

   Ceci est trivial, puisque l'état atteint est l'état initial.

   iii. Étape d'induction : Nous devons montrer

   $$(\forall n{:}\mathbb{N} \mid{:} Q.n \Rightarrow Q(n+1)).$$

   Supposons $Q.n$ et montrons $Q(n+1)$, c'est-à-dire

   $$\text{si l'exécution débute dans un état qui satisfait } P, \text{ alors l'état atteint après } n+1 \text{ itérations satisfait } P.$$

   Par l'hypothèse d'induction, l'état atteint après n itérations satisfait P. Cet état est l'état juste avant l'itération $n+1$. Puisqu'il y a une nouvelle itération (l'itération $n+1$), le test de boucle B est vrai. Par conséquent, l'état avant l'itération $n+1$ satisfait $P \wedge B$. Par l'hypothèse 1 du théorème, l'état atteint après l'itération satisfait P.

(10.42) Exercice. Utilisez le théorème d'invariance (10.41) pour montrer le triplet de Hoare suivant. Les variables f, i et n sont entières (c'est-à-dire $f, i, n{:}\mathbb{Z}$).

$\{\text{Invariant } 0 \leq i \leq n \ \wedge \ f = i!\}$
while $i \neq n$ **do**
begin

$i := i + 1$;
$f := f \cdot i$
end
$\{0 \leq i \leq n \ \wedge \ f = i! \ \wedge \ i = n\}$

Montrez également que la postcondition implique $f = n!$.

Vérification des boucles initialisées

Il y a habituellement une initialisation avant une boucle. Nous sommes donc intéressés à démontrer des triples de Hoare de la forme

$$\{Q\} \quad S'; \textbf{while } B \textbf{ do } S \quad \{R\},$$

où l'instruction S' est l'initialisation de la boucle. Pour montrer ce triplet, il faut avoir un invariant de boucle P (normalement fourni par le programmeur). Le programme annoté avec l'invariant est

$$\{Q\} \quad S'; \ \{\text{Invariant } P\} \ \ \textbf{while } B \textbf{ do } S \quad \{R\}.$$

(10.43) Vérification d'une boucle initialisée : Pour que

$$\{Q\} \quad S'; \ \{\text{Invariant } P\} \ \ \textbf{while } B \textbf{ do } S \quad \{R\}$$

soit un théorème, il suffit que
(a) P soit vrai avant l'exécution de la boucle : $\{Q\} \quad S' \quad \{P\}$;
(b) P soit un invariant de la boucle : $\{P \wedge B\} \quad S \quad \{P\}$;
(c) l'exécution de la boucle se termine ;
(d) R soit vrai à la fin de l'exécution : $P \wedge \neg B \ \Rightarrow \ R$.

(10.44) Exercice. Appliquez la procédure de vérification de boucle (10.43) au programme suivant. Les variables f, i et n sont entières.

$\{0 \leq n\}$
$i, f := 0, 1$;
$\{\text{Invariant } 0 \leq i \leq n \ \wedge \ f = i!\}$
while $i \neq n$ **do**
begin
$i := i + 1$;
$f := f \cdot i$
end
$\{f = n!\}$

Preuves de terminaison

Dans la solution de l'exercice (10.42), nous avons utilisé un argument informel pour montrer que l'exécution de la boucle se termine (pas de boucle infinie). Voici une manière formelle de montrer la terminaison. Elle est basée sur l'usage d'une *fonction majorante* M définie par une expression à valeur entière qui *majore* le nombre d'itérations restant à exécuter. Dans ce qui suit, l'expression de la fonction majorante M est parfois donnée comme une assertion dans un programme.

(10.45) Preuve de terminaison : Pour montrer que l'exécution de

$\{\text{Invariant } P\}$
$\{\text{Fonction majorante } M\}$
while B **do** S

se termine, il suffit que
(a) M soit une fonction à valeur entière ;
(b) M décroisse à chaque itération : $\{P \wedge B \wedge M = \mathsf{X}\}\ \ S\ \ \{M < \mathsf{X}\}$;
(c) tant qu'il reste une itération, $M > 0 : P \wedge B \Rightarrow M > 0$.

Démonstration. La preuve se fait par induction sur la valeur de M. La propriété à démontrer est

$$(\forall n{:}\mathbb{N} \mid{:} \text{ si } M \leq n, \text{ alors l'exécution de la boucle se termine}).$$

Notons que si la valeur initiale de M est n, cette propriété garantit que la boucle se termine.

1. Définition du prédicat d'induction Q : Choisissons comme prédicat d'induction

   $$Q.n : \quad \text{si } M \leq n, \text{ alors l'exécution de la boucle se termine.}$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:} Q.n)$.
2. Étape de base : il faut prouver $Q.0$, c'est-à-dire

   $$\text{si } M \leq 0, \text{ alors l'exécution de la boucle se termine.}$$

   Supposons $M \leq 0$ et montrons que l'exécution se termine.

   $P \wedge B \Rightarrow M > 0$ —Hypothèse (c)
   $=$ ⟨ P est vrai initialement (tel qu'affirmé par la précondition) et c'est un invariant. Il est donc vrai, peu importe que la boucle soit au début de son exécution on non ⟩
   $\mathsf{vrai} \wedge B \Rightarrow M > 0$
   $=$ ⟨ Identité de $\wedge$ (3.52), avec $p := B$ ⟩
   $B \Rightarrow M > 0$

$$
\begin{array}{ll}
= & \quad \langle \text{ Contrapositivité (3.77), avec } p, q := B, M > 0 \rangle \\
& \neg(M > 0) \Rightarrow \neg B \\
= & \quad \langle \text{ Arithmétique } \rangle \\
& M \leq 0 \Rightarrow \neg B \\
= & \quad \langle \text{ Hypothèse } M \leq 0 \rangle \\
& \mathsf{vrai} \Rightarrow \neg B \\
= & \quad \langle \text{ Identité à gauche de } \Rightarrow \text{ (3.89), avec } p := \neg B \rangle \\
& \neg B
\end{array}
$$

Puisque $\neg B$ est vrai, la boucle se termine immédiatement.

3. Étape d'induction : Nous devons montrer

$$(\forall n{:}\mathbb{N} \mid{:}\ Q.n \Rightarrow Q(n+1)).$$

Supposons $Q.n$ et montrons $Q(n+1)$, c'est-à-dire

si $M \leq n+1$, alors l'exécution de la boucle se termine.

Si B est faux, alors la boucle se termine immédiatement. Si B est vrai, alors le corps S de la boucle est exécuté une fois et, après cette exécution, $M \leq n$, par les hypothèses (a) et (b). Par l'hypothèse d'induction, l'exécution de la boucle se termine donc.

(10.46) Remarque. Pour les preuves par induction qui ont été présentées jusqu'ici, la propriété à démontrer était facile à formaliser. Pour la preuve précédente, c'est plus difficile. On peut penser que la propriété suivante conviendrait :

$$(\forall n{:}\mathbb{N} \mid{:}\ \text{si initialement } M = n, \text{ alors l'exécution de la boucle se termine}).$$

Ce n'est pas le cas. À l'étape d'induction, l'hypothèse (10.45c) garantit seulement $M \leq n$, pas $M = n$.

Remarque dans la remarque : En fait, cette propriété convient si on utilise un principe d'induction appelé *principe d'induction forte* ou encore *principe généralisé d'induction*. Voir par exemple [6]. Le principe généralisé n'est pas plus puissant que l'axiome (8.2), mais il permet plus de souplesse dans la formulation des propriétés.

(10.47) Exercice. Montrez que la boucle du programme de l'exercice (10.44) se termine. Utilisez la fonction majorante $M = n - i$.

Vérification de programmes annotés

Certains problèmes à la fin du chapitre demandent de vérifier un programme annoté S. Ce qu'on veut, c'est une preuve de

$$\{Q\} \quad S \quad \{R\},$$

où Q et R sont respectivement la précondition et la postcondition fournies avec le programme. La vérification est facile si les fonctions majorantes et les invariants de boucle sont donnés en annotation (et s'ils sont corrects, bien sûr). La principale difficulté rencontrée par les vérificateurs automatiques, c'est justement d'inventer les fonctions majorantes et les invariants appropriés lorsqu'ils ne sont pas fournis par le programmeur.

10.10 Problèmes

1. Considérez un segment de tableau $b[0..n-1]$, où $0 \leq n$. Soient j et k deux variables entières satisfaisant $0 \leq j \leq k < n$. La notation $b[j..k]$ désigne le sous-tableau de b qui consiste en $b[j], b[j+1], \ldots, b[k]$. Le segment $b[j..k]$ est vide si $j = k+1$.

   Traduisez les phrases suivantes en expressions booléennes. Par exemple, la première peut s'écrire $(\forall i \mid j \leq i \leq k : b[i] = 0)$. Certains énoncés sont ambigus ; dans ce cas, écrivez toutes les interprétations raisonnables. Simplifiez les expressions lorsque c'est possible. Vous pouvez utiliser des abréviations —par exemple, $x \in b[0..n-1]$ au lieu de $(\exists i \mid 0 \leq i < n : x = b[i])$.

   (a) Tous les éléments de $b[j..k]$ sont nuls.

   (b) Les valeurs de $b[0..n-1]$ qui ne sont pas dans $b[j..k]$ sont dans $b[j..k]$.

   (c) Chaque élément de $b[0..j]$ est moindre que x et chaque valeur de $b[j+1..k-1]$ excède x.

2. Formalisez les spécifications suivantes énoncées en français. Assurez-vous d'introduire les restrictions nécessaires. De plus, si certaines parties de la spécification sont ambigües, résolvez-les d'une manière raisonnable (il peut y avoir plus d'une réponse). Vous pouvez écrire $x \uparrow y$ pour le maximum de x et y. Notez que $\uparrow$ est commutatif et associatif, et peut donc être utilisé comme quantificateur (voyez le chapitre 6). Cependant, $\uparrow$ sur $\mathbb{Z}$ n'a pas d'élément identité (élément neutre), et donc certains axiomes qui requièrent cette propriété ne s'appliquent pas.

   (a) Le tableau b contient la liste des étudiants de l'Université Laval et le tableau c contient la liste des personnes qui ont un emploi à temps partiel dans la région de Québec. Les deux listes sont triées alphabétiquement. Trouvez la première personne qui apparaît dans les deux listes.

   (b) Le tableau b est trié en ordre non décroissant. Trouvez l'indice de l'élément le plus à droite (c'est-à-dire l'élément avec l'indice le plus élevé) qui égale x. Tenez compte du cas où x n'est pas dans b.

3. Formalisez les spécifications suivantes. Certaines requièrent l'emploi de variables rigides pour indiquer les modifications aux variables du programme. Assurez-vous d'indiquer les restrictions nécessaires sur les entrées. Si la spécification française est ambigüe ou vague, précisez-la d'une manière convenable (il peut y avoir plus d'une manière).

   (a) Doublez la valeur de chaque élément du tableau d'entiers b.

   (b) Permutez les tableaux b et c.

4. Utilisez la méthode (10.33) pour démontrer que le programme annoté suivant est correct. Considérez que les variables ont le type $x, y, z{:}\mathbb{Z}$. La division / est alors la division entière qui tronque le résultat s'il est fractionnaire (ainsi, $6/2 = 3$ et $5/2 = 2$).

$$\begin{array}{l}
\{y > 0 \ \wedge \ z \cdot x^y = \mathsf{X}\} \\
\quad \textbf{if } \mathsf{impair}.y \ \textbf{ then } z, y := z \cdot x, \ y - 1 \textbf{ else } x, y := x \cdot x, \ y/2 \\
\{y \geq 0 \ \wedge \ z \cdot x^y = \mathsf{X}\}
\end{array}$$

5. Vérifiez le programme

$$\begin{array}{l}
\{0 \leq n\} \\
\quad x, j := 0, 0\,; \\
\{\text{Invariant } 0 \leq j \leq n \ \wedge \ x = (\sum k \mid 0 \leq k < j : b[k])\} \\
\{\text{Fonction majorante } n - j\} \\
\quad \textbf{while } j \neq n \textbf{ do} \\
\qquad x, j := \ x + b[j], \ j + 1 \\
\{x = (\sum k \mid 0 \leq k < n : b[k])\},
\end{array}$$

dans lequel les variables ont les types

$$j, n{:}\mathbb{Z}, \qquad x{:}\mathbb{R}, \qquad b[0..n-1]{:}\mathsf{tableau\ de}\ \mathbb{R}.$$

6. Vérifiez le programme suivant. Les variables a, b, i et n sont entières.

$$\begin{array}{l}
\{0 \leq n\} \\
\quad b, i := 1, 0\,; \\
\{\text{Invariant } 0 \leq i \leq n \ \wedge \ b = a^i\} \\
\{\text{Fonction majorante } n - i\} \\
\quad \textbf{while } i < n \textbf{ do} \\
\qquad \textbf{begin} \\
\qquad i := i + 1\,; \\
\qquad b := a \cdot b \\
\qquad \textbf{end} \\
\{b = a^n\}
\end{array}$$

Chapitre 11

Théorie des ensembles

11.1 Compréhension et appartenance

Un *ensemble* est une collection de valeurs. On peut définir un ensemble par *énumération* (on dit aussi en *extension*) et par *compréhension*.

Énumération

Une manière de définir un *ensemble* est d'*énumérer* (lister) ses *éléments* entre accolades { } :

$$\{8, 4, -3.5, 10\}$$

est l'ensemble qui contient les éléments 8, 4, -3.5 et 10.

Soit l'état

$$(a, 5),\ (b, 13),\ (c, 8).$$

L'évaluation de l'expression

$$\{b, c\}$$

dans cet état donne l'ensemble

$$\{13, 8\}.$$

Compréhension

Lorsque le nombre de ses éléments est trop grand pour les énumérer, on définit un ensemble par *compréhension*, c'est-à-dire en utilisant des expressions qui décrivent les *propriétés* de ses éléments :

$$\{n{:}\mathbb{Z} \mid 0 \leq n \leq 8 : 2^n\}$$

est l'ensemble qui *contient* les valeurs de la forme 2^n, où $0 \leq n \leq 8$, c'est-à-dire

$$\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8\} ,$$

ou encore, en développant,

$$\{1, 2, 4, 8, 16, 32, 64, 128, 256\} .$$

Une énumération peut être vue comme une abréviation d'une compréhension :

$$\{5, 12, 7\} \quad = \quad \{x \mid x = 5 \ \vee \ x = 12 \ \vee \ x = 7 : x\}$$

ou, en général,

(11.1) $\{e_0, \ldots, e_{n-1}\} \quad = \quad \{x \mid x = e_0 \ \vee \ \ldots \ \vee \ x = e_{n-1} : x\} .$

Forme générale d'une expression de compréhension

La forme générale ressemble à une quantification :

(11.2) $\{x{:}t \mid R : E\}$

x est une liste de variables de quantification, R est l'expression booléenne décrivant le domaine et E est l'expression du corps. Si $E{:}t_1$, alors

$$\{x{:}t \mid R : E\}{:}\mathsf{ensemble}(t_1) .$$

La valeur de $\{x{:}t \mid R : E\}$ dans un état s s'obtient en calculant $E[x := v]$ pour toute valeur v de type t telle que $R[x := v]$ est vrai dans l'état s.

(11.3) Exemple.

$\{i{:}\mathbb{Z} \mid 0 < i < 50 \ \wedge \ \mathsf{pair}.i : i\}$	Ensemble des entiers positifs pairs inférieurs à 50
$\{i{:}\mathbb{Z} \mid 0 < 2 \cdot i < 50 : 2 \cdot i\}$	Ensemble des entiers positifs pairs inférieurs à 50
$\{x, y{:}\mathbb{Z} \mid 1 \leq x \leq 2 \leq y \leq 3 : x^y\}$	$\{1^2, 1^3, 2^2, 2^3\}$
$\{x{:}\mathbb{Z} \mid 0 \leq x < 3 : x^y\}$	$\{0^y, 1^y, 2^y\}$ $= \{0, 1, 8\}$ dans l'état $(x, 5), (y, 3)$
$\{x{:}\mathbb{Z} \mid 0 \leq x < 0 : x^y\}$	$\{\}$ l'*ensemble vide*, aussi noté $\emptyset$
$\{x{:}\mathbb{Z} \mid \mathsf{faux} : x^y\}$	$\{\}$ l'*ensemble vide*, aussi noté $\emptyset$
$\{x{:}\mathbb{Z} \mid x = 5 : x\}$	$\{5\}$ un tel ensemble à un élément s'appelle un *singleton*

Appartenance et égalité

Soit une expression e de type t et soit une expression S de type $\mathsf{ensemble}(t)$. L'expression

$$e \in S$$

se prononce

$$\begin{array}{rl} & e \textit{ appartient à } S \\ \text{ou encore} & e \textit{ est un élément de } S\ . \end{array}$$

Elle a la valeur vrai si e est un élément de S et la valeur faux sinon.

(11.4) Exemple.

$$\begin{array}{rcl} 10 \in \{5,10,2,3\} & \equiv & \mathsf{vrai} \\ 8 \in \{5,10,2,3\} & \equiv & \mathsf{faux} \\ \big(\neg(10 \in \{5,10,2,3\})\big) & = & \big(10 \notin \{5,10,2,3\}\big) \quad = \quad \mathsf{faux} \end{array}$$

(11.5) Axiome, appartenance : Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}F\text{'})$,

$$F \in \{x \mid R : E\} \ \equiv \ (\exists x \mid R : F = E)\ .$$

Par exemple,

$$(8 \in \{n \mid 0 \le n < 10 : 2^n\}) \quad = \quad (\exists n \mid 0 \le n < 10 : 8 = 2^n) \quad = \quad \mathsf{vrai}\ .$$

(11.6) Appartenance, cas particulier : $F \in \{x \mid R : x\} \ \equiv \ R[x := F]$

Par exemple,

$$\begin{array}{ll} & 13 \in \{n \mid 0 \le n < 10 : n\} \\ = & \qquad \langle \text{ Appartenance, cas particulier (11.6) } \rangle \\ & (0 \le n < 10)[n := 13] \\ = & \qquad \langle \text{ Substitution } \rangle \\ & 0 \le 13 < 10 \\ = & \qquad \langle \text{ Arithmétique } \rangle \\ & \mathsf{faux} \end{array}$$

Extensionnalité

(11.7) Notation. Pour le reste du chapitre,

$$S, T, U, V : \mathsf{ensemble}(t)\ ,$$

c'est-à-dire que les symboles S, T, U, V sont des variables de type $\mathsf{ensemble}(t)$, où le type t dépend des circonstances.

(11.8) Axiome, extensionnalité : $S = T \ \equiv \ (\forall x \mid : x \in S \equiv x \in T)$

Autrement dit, deux ensembles sont égaux si, et seulement si, ils ont les mêmes éléments. L'axiome d'entensionnalité donne une méthode pour démontrer l'égalité de deux ensembles. Cette méthode est utilisée dans la preuve qui suit.

(11.9) $S = \{x \mid x \in S : x\}$.

Démonstration. Nous voulons montrer l'égalité des ensembles S et $\{x \mid x \in S : x\}$. Par extensionnalité (11.8), cela revient à montrer

$$(\forall v \mid: v \in S \;\equiv\; v \in \{x \mid x \in S : x\}) \;.$$

Par le métathéorème (7.33), pour démontrer cette formule, il suffit de montrer

$$v \in S \;\equiv\; v \in \{x \mid x \in S : x\}$$

pour un v arbitraire.

$$\begin{array}{ll} & v \in \{x \mid x \in S : x\} \\ = & \qquad \langle \text{ Appartenance, cas particulier (11.6) } \rangle \\ & (x \in S)[x := v] \\ = & \qquad \langle \text{ Substitution } \rangle \\ & v \in S \end{array}$$

Quelques remarques

1. L'ensemble $\{\{\,\}\}$ (qui est égal à $\{\emptyset\}$) *n'est pas vide*. Il contient un élément, soit l'ensemble $\{\,\}$ (ou encore $\emptyset$).
2. L'expression $e \in \{e\}$ a la valeur vrai.
3. Par l'abréviation (11.1), et puisque $\vee$ est idempotent et commutatif,
   (a) les répétitions d'éléments ne comptent pas. Par exemple,
   $$\{2, 3, 2\} = \{2, 3\} \;;$$
   (b) l'ordre d'énumération des éléments n'est pas important. Par exemple,
   $$\{1, 2, 3\} = \{3, 2, 1\} = \{1, 3, 2\} \;.$$
4. Les ensembles peuvent être éléments d'autres ensembles. Par exemple,
   $$\{\{1, 2\}, \emptyset, \{2, 3, 4\}\}$$
   contient les éléments $\{1, 2\}$, $\emptyset$ et $\{2, 3, 4\}$.
5. Un ensemble peut contenir des éléments de types différents : $\{2, \text{vrai}\}$.

La forme traditionnelle de la compréhension

La notation mathématique traditionnelle pour la compréhension est

$$\{x \mid R\} \;,$$

où x est une variable. C'est une abréviation de $\{x \mid R : x\}$. Nous l'utiliserons assez souvent. Par exemple,

$$\begin{aligned} \{n \mid 0 \leq n < 5\} &= \{0,1,2,3,4\} \\ \{i \mid 0 \leq i < 10 \ \wedge \ \mathsf{impair}.i\} &= \{1,3,5,7,9\} \end{aligned}$$

On voit aussi parfois

$$\{E \mid R\} \ ,$$

où E est une expression. Par exemple,

$$\{x + y \mid x > y\} \ .$$

Nous n'utiliserons pas cette forme, car elle n'indique pas explicitement quelles sont les variables liées. Ainsi, il n'est pas clair si l'ensemble ci-dessus est égal à

$$\{x, y \mid x > y : x + y\} \quad \text{ou à} \quad \{x \mid x > y : x + y\} \quad \text{ou à} \quad \{y \mid x > y : x + y\} \ .$$

En fait, la forme traditionnelle est suffisante, par le théorème suivant, qui montre que pour transformer la forme générale $\{x \mid R : E\}$ sous la forme conventionnelle $\{y \mid Q\}$, il suffit de prendre $Q := (\exists x \mid R : y = E)$.

(11.10) Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R, E\text{'})$,

$$\{x \mid R : E\} \ = \ \{y \mid (\exists x \mid R : y = E)\} \ .$$

À gauche, la forme étendue ; à droite, la forme conventionnelle.

(11.11) Exemple.

$$\begin{array}{ll} & \{t \mid 0 \leq t \leq 5 : t^2\} \\ = & \qquad \langle \ \neg\mathsf{libre}(\text{`}s\text{'},\text{`}0 \leq t \leq 5, t^2\text{'}) \ \ \& \ \ (11.10) \ \rangle \\ & \{s \mid (\exists t \mid 0 \leq t \leq 5 : s = t^2)\} \\ = & \qquad \langle \text{ Expansion du quantificateur } \rangle \\ & \{s \mid s = 0^2 \ \vee \ s = 1^2 \ \vee \ s = 2^2 \ \vee \ s = 3^2 \ \vee \ s = 4^2 \ \vee \ s = 5^2\} \\ = & \qquad \langle \text{ Élimination de l'abréviation } \rangle \\ & \{s \mid s = 0^2 \ \vee \ s = 1^2 \ \vee \ s = 2^2 \ \vee \ s = 3^2 \ \vee \ s = 4^2 \ \vee \ s = 5^2 : s\} \\ = & \qquad \langle \ (11.1) \ \rangle \\ & \{0, 1, 4, 9, 16, 25\} \end{array}$$

En utilisant la notation traditionnelle, (11.6) devient :

(11.12) Appartenance, cas particulier, notation traditionnelle :

$$F \in \{x \mid R\} \ \equiv \ R[x := F]$$

Ensembles versus prédicats

(11.13) $x \in \{x \mid R\} \;\equiv\; R$

(11.14) Exemple. $n \in \{n \mid n < 100\} \;\equiv\; n < 100$.

Notez que dans le théorème (11.13), x a deux significations.

1. La première occurrence de x est libre ainsi que celles qui apparaissent dans le dernier R (s'il y en a).
2. Les occurrences de x dans le premier R (s'il y en a) sont liées.

Le théorème (11.13) permet de définir des ensembles de deux manières. Par exemple, les deux définitions suivantes de l'ensemble P des nombres entiers pairs sont équivalentes :

$$P = \{n \mid \mathsf{pair}.n\}$$
$$n \in P \;\equiv\; \mathsf{pair}.n$$

(11.15) Définition. Le prédicat R est dit le *prédicat caractéristique* de l'ensemble $\{x \mid R\}$.

Du théorème (11.13), on tire le théorème suivant qui exprime le fait que deux ensembles définis par des prédicats caractéristiques différents sont égaux si et seulement si les deux prédicats sont équivalents :

(11.16) $\{x \mid Q\} = \{x \mid R\} \;\equiv\; (\forall x \mid : Q \equiv R)$

Par exemple, $\{n \mid n^2 \geq 10\} = \{n \mid n^2 > 9\}$, car $(\forall n \mid : n^2 \geq 10 \;\equiv\; n^2 > 9)$.

(11.17) Métathéorème : $\{x \mid Q\} = \{x \mid R\}$ est un théorème si et seulement si $(\forall x \mid : Q \equiv R)$ est un théorème.

Avec le métathéorème (11.17), nous avons trois méthodes pour démontrer l'égalité d'ensembles.

(11.18) Méthodes de démonstration de l'égalité d'ensembles $S = T$:

(a) Par la règle de Leibniz.

(b) Par l'axiome d'extensionnalité (11.8), il suffit de prouver

$$v \in S \;\equiv\; v \in T$$

pour un v arbitraire.

(c) Par (11.17), il suffit de montrer $Q \equiv R$ pour conclure

$$\{x \mid Q\} \;=\; \{x \mid R\} \;.$$

11.2 Opérations sur les ensembles

Cardinalité des ensembles finis

La *cardinalité* ou la *taille* d'un ensemble fini S, dénotée par $\#S$, est le nombre d'éléments de S. Elle est définie ainsi :

(11.19) Axiome, cardinalité : $\#S = (\sum x \mid x \in S : 1)$

La notation $|S|$ pour la cardinalité de S est aussi très fréquemment employée dans la littérature.

(11.20) Remarque. Par le métathéorème (7.33), il n'est pas nécessaire d'écrire (11.19) ainsi :

$$(\forall S \mid : \#S = (\sum x \mid x \in S : 1)) \ .$$

C'est comme lorsqu'on définit la commutativité de l'addition. On écrit simplement $x+y = y+x$ au lieu de $(\forall x, y \mid : x + y = y + x)$.

Sous-ensemble et surensemble

Diagrammes de Venn de $S \subseteq T$ et $\{3,5,7\} \subseteq \{2,3,4,5,6,7,8\}$

(11.21) Axiome, sous-ensemble : $S \subseteq T \ \equiv \ (\forall x \mid x \in S : x \in T)$

Si $S \subseteq T$, on dit que S *est un sous-ensemble de* T, ou que S *est inclus dans* T, ou que T *contient* S. Le symbole $\subseteq$ s'appelle l'*inclusion*5 .

(11.22) Axiome, sous-ensemble propre : $S \subset T \ \equiv \ S \subseteq T \ \wedge \ S \neq T$

Si $S \subset T$, on dit que S *est un sous-ensemble propre de* T, ou que S *est strictement inclus dans* T, ou que T *contient strictement* S. Le symbole $\subset$ s'appelle l'*inclusion stricte*.

(11.23) Axiome, surensemble : $T \supseteq S \ \equiv \ S \subseteq T$

(11.24) Axiome, surensemble propre : $T \supset S \ \equiv \ S \subset T$

Les opérateurs $\subseteq, \subset, \supseteq, \supset$ sont conjonctifs et ont la même préséance que $=$.

Ensemble universel U

L'ensemble qui contient tous les éléments dont on veut parler dans un contexte donné s'appelle *l'ensemble universel* ; on le dénote par $\mathbf{U}$. Par exemple, dans un contexte où tous les ensembles contiennent des entiers, on a

$$\mathbf{U} = \mathsf{ensemble}(\mathbb{Z}) \ .$$

Complément

Supposons l'ensemble universel $\mathbf{U}$ donné. Le *complément* d'un ensemble S, noté $\sim S$, est l'ensemble des éléments qui appartiennent à $\mathbf{U}$ mais pas à S.

(11.25) Axiome, complément : $v \in \sim S \;\equiv\; v \in \mathbf{U} \wedge v \notin S$

Par exemple, si $\mathbf{U} = \mathbb{Z}$, alors $\sim\{n \mid \mathsf{pair}.n\} = \{n \mid \mathsf{impair}.n\}$.

(11.26) $v \in \sim S \;\equiv\; v \notin S \qquad (\text{où } v \in \mathbf{U})$

(11.27) $\sim\sim S = S$

Remarquons que les notations S^C et $\overline{S}$ sont aussi utilisées pour dénoter le complément de S.

Union, intersection et différence

(11.28) Axiome, union : $v \in S \cup T \;\equiv\; v \in S \vee v \in T$

(11.29) Axiome, intersection : $v \in S \cap T \;\equiv\; v \in S \wedge v \in T$

(11.30) Axiome, différence : $v \in S - T \;\equiv\; v \in S \wedge v \notin T$

(11.31) Exemple.

$$\begin{array}{rcl} \{0,1,2\} \cup \{2,3,4\} & = & \{0,1,2,3,4\} \\ \{0,1,2\} \cap \{2,3,4\} & = & \{2\} \\ \{0,1,2\} - \{2,3,4\} & = & \{0,1\} \end{array}$$

Des axiomes (11.25) et (11.30), on tire

$$\sim S = \mathbf{U} - S \ .$$

Les ensembles S et T sont dits *disjoints* s'ils n'ont pas d'éléments en commun, c'est-à-dire si

$$S \cap T = \emptyset \ .$$

Par exemple, $\{0,1,2\}$ et $\{5,8\}$ sont disjoints, mais pas $\{2,5,8\}$ et $\{2,8,15\}$.

Ensemble puissance

L'*ensemble puissance* d'un ensemble S, noté $\mathcal{P}S$, est l'ensemble des sous-ensembles de S.

(11.32) Axiome, ensemble puissance : $v \in \mathcal{P}S \;\equiv\; v \subseteq S$

(11.33) Exemple.

$$\mathcal{P}\{1,2,3\} = \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\ \}$$

$$\big(\{1,3\} \in \mathcal{P}\{1,2,3\}\big) = \big(\{1,3\} \subseteq \{1,2,3\}\big) = \mathsf{vrai}$$

$$\big(\{1,4\} \in \mathcal{P}\{1,2,3\}\big) = \big(\{1,4\} \subseteq \{1,2,3\}\big) = \mathsf{faux}$$

TAB. 11.1 – Typage des expressions ensemblistes

Expression	Type du résultat	De même pour
$\emptyset$	ensemble(t)	$\mathbf{U}$, S
$\{e_1{:}t, \ldots, e_n{:}t\}$	ensemble(t)	
$\{x \mid R{:}\mathbb{B} : E{:}t\}$	ensemble(t)	
$x{:}t \in S{:}$ensemble(t)	$\mathbb{B}$	
$S{:}$ensemble(t) $= T{:}$ensemble(t)	$\mathbb{B}$	
$\#S{:}$ensemble(t)	$\mathbb{N}$	
$S{:}$ensemble(t) $\subseteq T{:}$ensemble(t)	$\mathbb{B}$	$\subset$, $\supseteq$, $\supset$
$\sim S{:}$ensemble(t)	ensemble(t)	
$S{:}$ensemble(t) $\cup\, T{:}$ensemble(t)	ensemble(t)	$\cap$, $-$
$\mathcal{P}S{:}$ensemble(t)	ensemble(ensemble(t))	

Typage des expressions ensemblistes

Supposons que les éléments de l'ensemble universel $\mathbf{U}$ ont le type t. La table 11.1 donne le typage de diverses expressions ensemblistes (données avec les types des opérandes).

11.3 Théorèmes sur les opérations ensemblistes

Lien entre les expressions ensemblistes et les expressions booléennes

Vous constaterez que $\emptyset$, $\mathbf{U}$, $\sim$, $\cup$, $\cap$ ont des propriétés très semblables à celles de faux, vrai, $\neg$, $\vee$, $\wedge$, respectivement.

Même si les opérateurs ensemblistes et logiques ont des propriété similaires, il est important de ne pas les confondre.

ATTENTION : à l'examen, faites très attention d'écrire lisiblement, de manière à distinguer $\vee$ de $\cup$, et $\wedge$ de $\cap$.

Propriétés des opérateurs ensemblistes

Dans les propriétés qui suivent, il faut bien distinguer la variable U, qui est de type ensemble, de l'ensemble universel $\mathbf{U}$ (les polices sont différentes). Quand vous écrivez à la main, évitez d'utiliser la variable U, car elle peut être confondue avec $\mathbf{U}$ et avec $\cup$. De même, évitez d'utiliser la variable V, car elle peut être confondue avec $\vee$.

Propriétés de $\cup$

(11.34) Commutativité de $\cup$: $S \cup T = T \cup S$

(11.35) Associativité de $\cup$: $(S \cup T) \cup U = S \cup (T \cup U)$

(11.36) Idempotence de $\cup$: $S \cup S = S$

(11.37) Zéro de $\cup$: $S \cup \mathbf{U} = \mathbf{U}$

(11.38) Identité (élément neutre) de $\cup$: $S \cup \emptyset = S$

(11.39) Affaiblissement : $S \subseteq S \cup T$

(11.40) Tiers exclu : $S \cup {\sim}S = \mathbf{U}$

Propriétés de $\cap$

(11.41) Commutativité de $\cap$: $S \cap T = T \cap S$

(11.42) Associativité de $\cap$: $(S \cap T) \cap U = S \cap (T \cap U)$

(11.43) Idempotence de $\cap$: $S \cap S = S$

(11.44) Zéro de $\cap$: $S \cap \emptyset = \emptyset$

(11.45) Identité (élément neutre) de $\cap$: $S \cap \mathbf{U} = S$

(11.46) Affaiblissement : $S \cap T \subseteq S$

(11.47) Contradiction : $S \cap {\sim}S = \emptyset$

Combinaison de $\cup$ et $\cap$

(11.48) Distributivité de $\cup$ sur $\cap$: $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$

(11.49) Distributivité de $\cap$ sur $\cup$: $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

(11.50) De Morgan : (a) ${\sim}(S \cup T) = {\sim}S \cap {\sim}T$
(b) ${\sim}(S \cap T) = {\sim}S \cup {\sim}T$

Monotonie de $\cup$ et $\cap$

(11.51) Monotonie de $\cup$: $S \subseteq T \wedge U \subseteq V \Rightarrow S \cup U \subseteq T \cup V$

(11.52) Monotonie de $\cap$: $S \subseteq T \wedge U \subseteq V \Rightarrow S \cap U \subseteq T \cap V$

Autres propriétés de $\cup$ et $\cap$

(11.53) $S \subseteq T \equiv S \cup T = T$

(11.54) $S \subseteq T \;\equiv\; S \cap T = S$

(11.55) $S \cup T = \mathbf{U} \;\equiv\; (\forall x \mid x \in \mathbf{U} : x \notin S \;\Rightarrow\; x \in T)$

(11.56) $S \cap T = \emptyset \;\equiv\; (\forall x \mid : x \in S \;\Rightarrow\; x \notin T)$

Propriétés de $-$

(11.57) $S - T \;=\; S \cap {\sim}T$

(11.58) $S - T \;\subseteq\; S$

(11.59) $S - \emptyset \;=\; S$

(11.60) $S \cap (T - S) \;=\; \emptyset$

(11.61) $S \cup (T - S) \;=\; S \cup T$

(11.62) $S \;-\; (T \cup U) \;=\; (S - T) \cap (S - U)$

(11.63) $S \;-\; (T \cap U) \;=\; (S - T) \cup (S - U)$

Implication versus inclusion

(11.64) $(\forall x \mid : P \Rightarrow Q) \;\equiv\; \{x \mid P\} \;\subseteq\; \{x \mid Q\}$

Propriétés de $\subseteq$

(11.65) **Antisymétrie :** $S \subseteq T \;\wedge\; T \subseteq S \;\equiv\; S = T$

(11.66) **Réflexivité :** $S \subseteq S$

(11.67) **Transitivité :** $S \subseteq T \;\wedge\; T \subseteq U \;\Rightarrow\; S \subseteq U$

(11.68) $\emptyset \subseteq S$

(11.69) $S \subset T \;\equiv\; S \subseteq T \;\wedge\; \neg(T \subseteq S)$

(11.70) $S \subset T \;\equiv\; S \subseteq T \;\wedge\; (\exists x \mid x \in T : x \notin S)$

(11.71) $S \subseteq T \;\equiv\; S \subset T \;\vee\; S = T$

(11.72) $S \not\subset S$

(11.73) $S \subset T \;\Rightarrow\; S \subseteq T$

(11.74) $S \subset T \;\Rightarrow\; T \not\subseteq S$

(11.75) $S \subseteq T \;\Rightarrow\; T \not\subset S$

(11.76) $S \subseteq T \;\wedge\; \neg(U \subseteq T) \;\Rightarrow\; \neg(U \subseteq S)$

(11.77) $(\exists x \mid x \in S : x \notin T) \;\Rightarrow\; S \neq T$

(11.78) **Transitivité :**
(a) $S \subseteq T \;\wedge\; T \subset U \;\Rightarrow\; S \subset U$
(b) $S \subset T \;\wedge\; T \subseteq U \;\Rightarrow\; S \subset U$
(c) $S \subset T \;\wedge\; T \subset U \;\Rightarrow\; S \subset U$

Preuve de (11.76)

$$
\begin{aligned}
& S \subseteq T \wedge \neg(U \subseteq T) \Rightarrow \neg(U \subseteq S) \\
= & \quad \langle \text{ Transfert (3.81) } \rangle \\
& S \subseteq T \Rightarrow (\neg(U \subseteq T) \Rightarrow \neg(U \subseteq S)) \\
= & \quad \langle \text{ Contrapositivité (3.77) } \rangle \\
& S \subseteq T \Rightarrow (U \subseteq S \Rightarrow U \subseteq T) \\
= & \quad \langle \text{ Transfert (3.81) } \rangle \\
& U \subseteq S \wedge S \subseteq T \Rightarrow U \subseteq T \qquad \text{—Transitivité (11.67)}
\end{aligned}
$$

Théorèmes sur l'opérateur $\mathcal{P}$

(11.79) $\mathcal{P}\emptyset = \{\emptyset\}$

(11.80) $S \in \mathcal{P}S$

(11.81) $\#(\mathcal{P}S) = 2^{\#S}$ (pour tout ensemble fini S)

11.4 Union et intersection de familles d'ensembles

Les opérateurs $\cup$ et $\cap$ sont commutatifs, associatifs et idempotents. On peut donc les utiliser comme quantificateurs :

(11.82) $(\cup x \mid R : E)$

(11.83) $(\cap x \mid R : E)$

Par exemple,

$$
\begin{aligned}
& (\cup i \mid 0 \leq i < 4 : \{2^i, 3^i\}) \\
= & \ \{2^0, 3^0\} \cup \{2^1, 3^1\} \cup \{2^2, 3^2\} \cup \{2^3, 3^3\} \\
= & \ \{2^0, 3^0, 2^1, 3^1, 2^2, 3^2, 2^3, 3^3\} \\
= & \ \{1, 2, 3, 4, 9, 8, 27\}
\end{aligned}
$$

Notez que (11.82) et (11.83) satisfont les lois générales de la quantification (6.19)–(6.36). De plus, comme $\cup$ est défini avec $\vee$ et $\cap$ avec $\wedge$, d'autres propriétés peuvent être dérivées à partir des propriétés de $\exists$ et $\forall$.

Partitions

Un ensemble d'ensembles S est une *partition* d'un autre ensemble T si

(i) l'ensemble vide n'est pas un élément de S,

(ii) les ensembles éléments de S sont disjoints deux à deux et

(iii) l'union des ensembles éléments de S est T,

autrement dit, si

(11.84) Partition :
$$\begin{aligned} &\emptyset \notin S \ \wedge \\ &(\forall u, v \mid u \in S \ \wedge \ v \in S \wedge u \neq v : u \cap v = \emptyset) \ \wedge \\ &(\cup u \mid u \in S : u) \ = \ T \end{aligned}$$

Par exemple,

1. $\{\{1,3,5\},\ \{0,2\},\ \{4,6\}\}$ est une partition de $\{0,1,2,3,4,5,6\}$;
2. $\{\{1,2,3,5\},\ \{0,2\},\ \{4,6\}\}$ n'est pas une partition de $\{0,1,2,3,4,5,6\}$;
3. $\{\{1,3\},\ \{0,2\},\ \{4,6\}\}$ n'est pas une partition de $\{0,1,2,3,4,5,6\}$.

11.5 Problèmes

1. Définissez l'ensemble suivant par compréhension (sous forme abrégée ou non).

   L'ensemble des nombres premiers compris entre 10 et 30. Vous pouvez utiliser la fonction booléenne premier.i qui retourne la valeur de « i est premier ».

2. Décrivez l'ensemble suivant en français.

$$\{x, y{:}\mathbb{Z} \mid 0 \leq x \ \wedge \ 2 \leq y \leq 3 : x^y\}$$

3. Utilisez le fait que $\{b\}$ et $\{b, c\}$ sont des abréviations de

$$\{x \mid x = b : x\} \quad \text{et} \quad \{x \mid x = b \ \vee \ x = c : x\},$$

   respectivement, pour démontrer

$$v \in \{b\} \ \equiv \ v = b \quad \text{et} \quad v \in \{b, c\} \ \equiv \ v = b \ \vee \ v = c.$$

4. Démontrez (11.16), $\{x \mid Q\} = \{x \mid R\} \ \equiv \ (\forall x \mid{:}\ Q \equiv R)$.
5. Démontrez le théorème (11.48), $S \cup (T \cap U) \ = \ (S \cup T) \cap (S \cup U)$.
6. Démontrez le théorème (11.51), $S \subseteq T \ \wedge \ U \subseteq V \ \Rightarrow \ S \cup U \subseteq T \cup V$. Pour cette démonstration, vous pouvez utiliser le théorème

$$(p \Rightarrow q) \ \wedge \ (r \Rightarrow s) \ \Rightarrow \ (p \vee r \ \Rightarrow \ q \vee s)$$

   (pour la démonstration d'une propriété similaire, voyez le problème 2 du chapitre 4).
7. Démontrez le théorème (11.58), $S - T \ \subseteq \ S$.
8. Démontrez le théorème (11.78a), $S \subseteq T \ \wedge \ T \subset U \ \Rightarrow \ S \subset U$.

Chapitre 12

Relations et fonctions

12.1 n-uplets et produits cartésiens

Un *n-uplet* est une *liste ordonnée* de n éléments $b_1, \ldots, b_n$, notée

$$\langle b_1, b_2, \ldots, b_n \rangle \ .$$

La liste est dite *ordonnée* parce que l'ordre des éléments est important (cela n'a rien à voir avec le fait que les éléments de la liste soient triés ou non). Par exemple, voici deux triplets différents :

$$\langle 4, 2, 3 \rangle \neq \langle 3, 2, 4 \rangle.$$

Un 2-uplet s'appelle une *paire ordonnée* ou un *couple ordonné* (on dit souvent simplement *paire* ou *couple*). Par exemple, $\langle 13, 4 \rangle$ est un couple.

La notation

$$(b_1, \ldots, b_n)$$

est aussi très fréquemment utilisée dans la littérature pour désigner un n-uplet.

(12.1) Axiome, égalité de couples : $\langle b, c \rangle = \langle b', c' \rangle \ \equiv \ b = b' \wedge c = c'$

Par exemple, $\langle 2, 3 \rangle \neq \langle 3, 2 \rangle$.

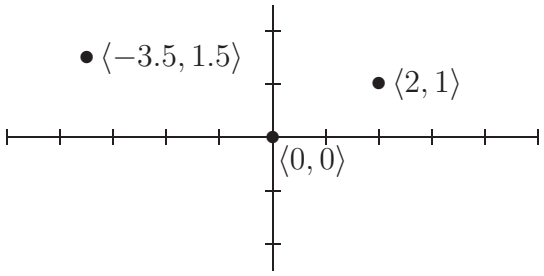
Produits cartésiens

(12.2) Axiome, produit cartésien : $S \times T \ = \ \{b, c \mid b \in S \wedge c \in T : \langle b, c \rangle\}$

(12.3) Exemple.

1. $\{3, 5\} \times \{\mathsf{a}, \mathsf{b}, \mathsf{c}\} \ = \ \{\langle 3, \mathsf{a} \rangle, \langle 3, \mathsf{b} \rangle, \langle 3, \mathsf{c} \rangle, \langle 5, \mathsf{a} \rangle, \langle 5, \mathsf{b} \rangle, \langle 5, \mathsf{c} \rangle\}$
   Notez que les lettres en police sans sérif (a,b,c) sont des constantes de type caractère et non des variables. En programmation, on écrirait 'a', 'b', 'c'.

2. $\mathbb{R} \times \mathbb{R}$ est l'ensemble des points dans le plan



$\mathbb{R} \times \mathbb{R}$, avec trois de ses couples

Théorèmes sur le produit cartésien

(12.4) Appartenance : $\langle x, y\rangle \in S \times T \equiv x \in S \wedge y \in T$

(12.5) $\langle x, y\rangle \in S \times T \equiv \langle y, x\rangle \in T \times S$

(12.6) $S = \emptyset \Rightarrow S \times T = T \times S = \emptyset$

(12.7) $S \times T = T \times S \equiv S = \emptyset \vee T = \emptyset \vee S = T$

(12.8) Distributivité de $\times$ sur $\cup$:

$$\begin{aligned} S \times (T \cup U) &= (S \times T) \cup (S \times U) \\ (S \cup T) \times U &= (S \times U) \cup (T \times U) \end{aligned}$$

(12.9) Distributivité de $\times$ sur $\cap$:

$$\begin{aligned} S \times (T \cap U) &= (S \times T) \cap (S \times U) \\ (S \cap T) \times U &= (S \times U) \cap (T \times U) \end{aligned}$$

(12.10) Distributivité de $\times$ sur $-$:

$$S \times (T - U) = (S \times T) - (S \times U)$$

(12.11) Monotonie : $T \subseteq U \Rightarrow S \times T \subseteq S \times U$

(12.12) $S \subseteq U \wedge T \subseteq V \Rightarrow S \times T \subseteq U \times V$

(12.13) $S \times T \subseteq S \times U \wedge S \neq \emptyset \Rightarrow T \subseteq U$

(12.14) $(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$

(12.15) Si S et T sont des ensembles finis, $\#(S \times T) = \#S \cdot \#T$

Produit cartésien de n ensembles

$$S_1 \times \ldots \times S_n = \{s_1, \ldots, s_n \mid s_1 \in S_1 \wedge \ldots \wedge s_n \in S_n : \langle s_1, \ldots, s_n\rangle\}$$

Par exemple, $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ est l'ensemble des points dans l'espace 3-D.

Notation $f{:}A \times B \to C$

Cette notation pour les fonctions utilise le produit cartésien. Elle indique que la fonction f s'applique à un couple, autrement dit, qu'elle a deux arguments (de types A et B).

12.2 Relations

Un ensemble R tel que

$$R \subseteq B_1 \times \ldots \times B_n$$

est appelé une *relation n-aire sur $B_1 \times \ldots \times B_n$*. Si $n = 2$, la relation est dite *binaire*. Si $n = 1$, la relation est dite *unaire*. Une relation n-aire contient donc des n-uplets. Une relation $R \subseteq B \times B$ est dite

sur B, plutôt que *sur $B \times B$*.

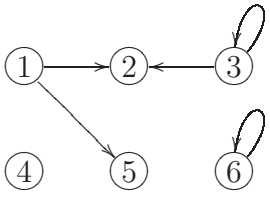
Cette terminologie courante est malheureusement ambigüe.

(12.16) Remarque. Dans les sections 12.2, 12.3 et 12.4, le terme *relation* désigne une *relation binaire*.

Exemples de relations binaires

1. La *relation vide* sur $B \times C$ est l'ensemble vide $\emptyset$.
2. La *relation identité* sur B est $\mathbf{I}_B = \{x \mid x \in B : \langle x, x \rangle\}$.
3. La relation parent_de sur l'ensemble des personnes relie les parents à leurs enfants. Par exemple, Paul parent_de Marie indique que Paul est un parent de Marie.
4. $\{b, c \mid b$ est l'origine d'un arc et c est la destination d'un arc : $\langle b, c \rangle\}$ est une relation sur l'ensemble des sommets d'un graphe. Par exemple,

$$\{\ \langle 1,2\rangle, \langle 1,5\rangle, \langle 3,2\rangle, \langle 3,3\rangle, \langle 6,6\rangle\ \}$$



5. $\{b, c \mid P$ débute l'exécution dans l'état b et la termine dans l'état $c : \langle b, c \rangle\}$ est une relation qui décrit l'action d'un programme P.

Notations pour l'appartenance à une relation

Il y a deux notations utiles que nous utiliserons pour désigner le fait qu'un couple $\langle b, c\rangle$ est un élément d'une relation ρ.

Relation	Couple	Notation 1	Notation 2
ρ	$\langle b, c\rangle$	$\langle b, c\rangle \in \rho$	$b\ \rho\ c$
Parent_de	$\langle$Paul, Marie$\rangle$	$\langle$Paul, Marie$\rangle \in$ Parent_de	Paul Parent_de Marie
$<$	$\langle 2, 5\rangle$	$\langle 2, 5\rangle \in\ <$	$2 < 5$

De même que

$$3 < 5 < 4 \text{ signifie } 3 < 5 \ \wedge\ 5 < 4,$$

$$b\ \rho\ c\ \rho\ d \text{ signifie } b\ \rho\ c\ \ \wedge\ \ c\ \rho\ d.$$

La priorité de ρ dans l'expression $b\ \rho\ c$ est la même que celle de $<$. Voyez l'entrée (j) de la table de préséance des opérateurs. Par exemple,

$$b\ \rho\ c\ \wedge\ c\ \sigma\ d\ \equiv\ (b\ \rho\ c)\ \wedge\ (c\ \sigma\ d)\ .$$

Domaine et image d'une relation

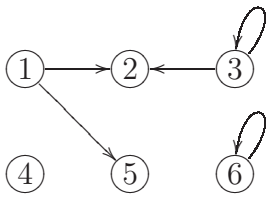
Le *domaine* Dom.ρ et l'*image* Im.ρ d'une relation sont définis comme suit :

(12.17) $\mathsf{Dom}.\rho\ =\ \{b \mid (\exists c \mid : b\ \rho\ c)\}$

(12.18) $\mathsf{Im}.\rho\ =\ \{c \mid (\exists b \mid : b\ \rho\ c)\}$

Par exemple,

$$\mathsf{Dom}.\{\ \langle 1,2\rangle, \langle 1,5\rangle, \langle 3,2\rangle, \langle 3,3\rangle, \langle 6,6\rangle\ \}\ =\ \{1,3,6\}$$
$$\mathsf{Im}.\{\ \langle 1,2\rangle, \langle 1,5\rangle, \langle 3,2\rangle, \langle 3,3\rangle, \langle 6,6\rangle\ \}\ =\ \{2,3,5,6\}$$



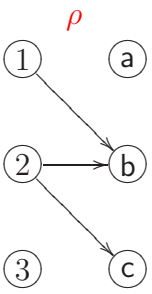
Le domaine est l'ensemble des éléments qui apparaissent comme première composante d'un couple. L'image est l'ensemble des éléments qui apparaissent comme deuxième composante d'un couple.

Opérations sur les relations

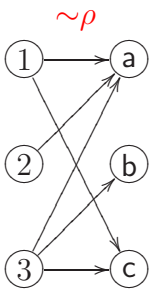
(12.19) Soient $\rho \subseteq B \times C$ et $\sigma \subseteq B \times C$.

Union	$\rho \cup \sigma$	comme pour d'autres ensembles
Intersection	$\rho \cap \sigma$	comme pour d'autres ensembles
Complément	$\sim\rho \;=\; (B \times C) - \rho$	$B \times C$ est l'ensemble universel
Inverse	$\langle b, c\rangle \in \rho^{-1} \equiv \langle c, b\rangle \in \rho$	pour tous $b{:}B$, $c{:}C$

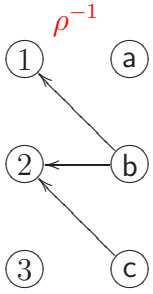
(12.20) Exemple. Supposons $B = \{1, 2, 3\}$ et $C = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$.



$\{\langle 1, \mathsf{b}\rangle, \langle 2, \mathsf{b}\rangle, \langle 2, \mathsf{c}\rangle\}$



$\{\langle 1, \mathsf{a}\rangle, \langle 1, \mathsf{c}\rangle, \langle 2, \mathsf{a}\rangle$
$\langle 3, \mathsf{a}\rangle, \langle 3, \mathsf{b}\rangle, \langle 3, \mathsf{c}\rangle\}$



$\{\langle \mathsf{b}, 1\rangle, \langle \mathsf{b}, 2\rangle, \langle \mathsf{c}, 2\rangle\}$

(12.21) Cas particulier de (11.9) : Soit ρ une relation.

$$\rho = \{b, c \mid \langle b, c\rangle \in \rho : \langle b, c\rangle\}$$

(12.22) Cas particulier de (11.6) :

$$\langle b, c\rangle \in \{x, y \mid R : \langle x, y\rangle\} \;\equiv\; R[x, y := b, c]$$
$$\langle b, c\rangle \in \{b, c \mid R : \langle b, c\rangle\} \;\equiv\; R$$

(12.23) Théorème : Soient ρ et σ deux relations.

(a) $\mathsf{Dom}(\rho^{-1}) \;=\; \mathsf{Im}.\rho$

(b) $\mathsf{Im}(\rho^{-1}) \;=\; \mathsf{Dom}.\rho$

(c) $\rho \subseteq B \times C \;\equiv\; \rho^{-1} \subseteq C \times B$

(d) $(\rho^{-1})^{-1} = \rho$

(e) $\rho \subseteq \sigma \;\equiv\; \rho^{-1} \subseteq \sigma^{-1}$

(f) $\mathbf{I}_B^{-1} \;=\; \mathbf{I}_B$

Produit de relations

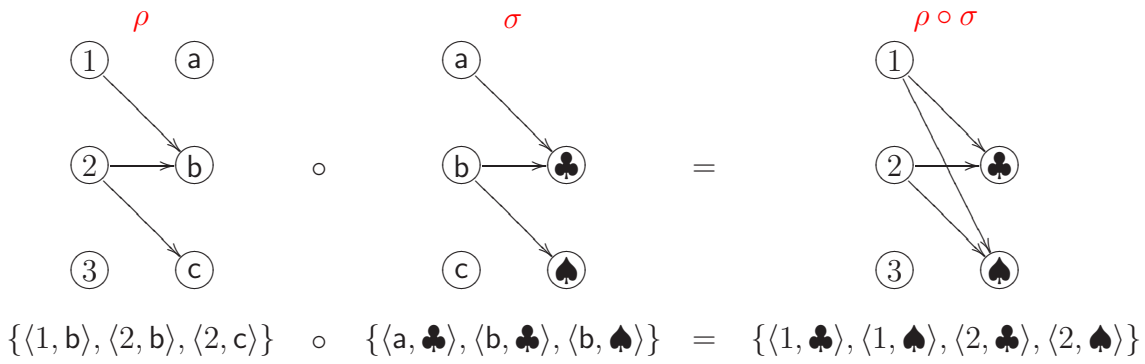
Soient les relations $\rho \subseteq B \times C$ et $\sigma \subseteq C \times D$. Le *produit* (aussi dit *produit relatif* ou *composition*) des relations ρ et σ, noté $\rho \circ \sigma$, est défini comme suit :

(12.24) Définition de $\circ$: $\langle b, d\rangle \in \rho \circ \sigma \;\equiv\; (\exists c{:}C \mid{:}\; \langle b, c\rangle \in \rho \wedge \langle c, d\rangle \in \sigma)$

ou encore, en utilisant la notation alternative et en laissant tomber le type de c,

(12.25) Définition de $\circ$: $b\ \rho \circ \sigma\ d \;\equiv\; (\exists c \mid{:}\; b\ \rho\ c\ \sigma\ d)$

(12.26) Exemple. Supposons $B = \{1, 2, 3\}$, $C = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ et $D = \{\spadesuit, \clubsuit\}$.



$\{\langle 1, \mathsf{b}\rangle, \langle 2, \mathsf{b}\rangle, \langle 2, \mathsf{c}\rangle\} \;\circ\; \{\langle \mathsf{a}, \clubsuit\rangle, \langle \mathsf{b}, \clubsuit\rangle, \langle \mathsf{b}, \spadesuit\rangle\} \;=\; \{\langle 1, \clubsuit\rangle, \langle 1, \spadesuit\rangle, \langle 2, \clubsuit\rangle, \langle 2, \spadesuit\rangle\}$

(12.27) Associativité de $\circ$: $\rho \circ (\sigma \circ \theta) \;=\; (\rho \circ \sigma) \circ \theta$

(12.28) Distributivité de $\circ$ sur $\cup$:
$$\rho \circ (\sigma \cup \theta) \;=\; \rho \circ \sigma \cup \rho \circ \theta$$
$$(\sigma \cup \theta) \circ \rho \;=\; \sigma \circ \rho \cup \theta \circ \rho$$

(12.29) (Sous)-distributivité de $\circ$ sur $\cap$:
$$\rho \circ (\sigma \cap \theta) \;\subseteq\; \rho \circ \sigma \cap \rho \circ \theta$$
$$(\sigma \cap \theta) \circ \rho \;\subseteq\; \sigma \circ \rho \cap \theta \circ \rho$$

Démonstration de (12.27) : par l'axiome d'extensionnalité (11.8) et le métathéorème (7.33), il suffit de montrer $\langle a, d\rangle \in \rho \circ (\sigma \circ \theta) \;\equiv\; \langle a, d\rangle \in (\rho \circ \sigma) \circ \theta$.

$a\ \rho \circ (\sigma \circ \theta)\ d$
$=$ ⟨ Définition (12.25) de $\circ$ ⟩
$(\exists b \mid{:}\; a\ \rho\ b\ \wedge\ b\ \sigma \circ \theta\ d)$
$=$ ⟨ Définition (12.25) de $\circ$ ⟩
$(\exists b \mid{:}\; a\ \rho\ b\ \wedge\ (\exists c \mid{:}\; b\ \sigma\ c\ \wedge\ c\ \theta\ d))$
$=$ ⟨ $\neg$libre(‘c’,‘$a\ \rho\ b$’) & Distributivité de $\wedge$ sur $\exists$ (7.4) ⟩
$(\exists b \mid{:}\; (\exists c \mid{:}\; a\ \rho\ b\ \wedge\ b\ \sigma\ c\ \wedge\ c\ \theta\ d))$
$=$ ⟨ $\neg$libre(‘c’,‘vrai’) & Imbrication (6.34) ⟩
$(\exists b, c \mid{:}\; a\ \rho\ b\ \wedge\ b\ \sigma\ c\ \wedge\ c\ \theta\ d)$
$=$ ⟨ Le reste de la preuve est semblable à ce qui précède, mais dans l'ordre inverse ; complétez-la ⟩
$a\ (\rho \circ \sigma) \circ \theta\ d$

Autres lois sur les relations

(12.30) Identité de $\circ$ (où $\rho \subseteq B \times C$) : $\mathbf{I}_B \circ \rho = \rho \circ \mathbf{I}_C = \rho$

(12.31) $\langle x, y\rangle \in \mathbf{I}_B \equiv x = y$

(12.32) Zéro de $\circ$: $\emptyset \circ \rho = \rho \circ \emptyset = \emptyset$

(12.33) Monotonie de $\circ$: $\rho \subseteq \sigma \Rightarrow \rho \circ \theta \subseteq \sigma \circ \theta$

(12.34) Monotonie de $\circ$: $\rho \subseteq \sigma \Rightarrow \theta \circ \rho \subseteq \theta \circ \sigma$

(12.35) $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$

(12.36) $\emptyset^{-1} = \emptyset$

(12.37) $(\rho \cup \sigma)^{-1} = \rho^{-1} \cup \sigma^{-1}$

(12.38) $(\rho \cap \sigma)^{-1} = \rho^{-1} \cap \sigma^{-1}$

Puissances d'une relation

Définition inductive des puissances d'une relation ρ sur l'ensemble B.

(12.39) $\rho^0 = \mathbf{I}_B$ (relation identité sur B)
$\rho^{n+1} = \rho^n \circ \rho$ (si $n \geq 0$)

Ainsi,

$$\rho^1 = \rho$$
$$\rho^2 = \rho \circ \rho$$
$$\rho^3 = \rho \circ \rho \circ \rho$$

(12.40) Exemple.

1. $\mathsf{parent\_de}^2 = \mathsf{parent\_de} \circ \mathsf{parent\_de} = \mathsf{grand\text{-}parent\_de}$
2. Posons $\mathsf{succ\_de} = \{b{:}\mathbb{Z} \mid : \langle b+1, b\rangle\}$. Par exemple, $5\ \mathsf{succ\_de}\ 4$.

   On peut montrer
   (a) $\mathsf{succ\_de}^2 = \{b{:}\mathbb{Z} \mid : \langle b+2, b\rangle\}$
   (b) $\mathsf{succ\_de}^n = \{b{:}\mathbb{Z} \mid : \langle b+n, b\rangle\}$ (par induction, bien sûr)

(12.41) $\rho^m \circ \rho^n = \rho^{m+n}$

(12.42) $(\rho^m)^n = \rho^{m \cdot n}$

Classes de relations (propriétés des relations)

TAB. 12.1 – Classes de relations ρ sur un ensemble B

	Propriété	Définition 1	Définition 2
(a)	réflexivité	$(\forall b \mid : b\ \rho\ b)$	$\mathbf{I}_B \subseteq \rho$
(b)	irréflexivité	$(\forall b \mid : \neg(b\ \rho\ b))$	$\mathbf{I}_B \cap \rho = \emptyset$
(c)	symétrie	$(\forall b, c \mid : b\ \rho\ c\ \equiv\ c\ \rho\ b)$	$\rho^{-1} = \rho$
(d)	antisymétrie	$(\forall b, c \mid : b\ \rho\ c\ \wedge\ c\ \rho\ b\ \Rightarrow\ b = c)$	$\rho \cap \rho^{-1} \subseteq \mathbf{I}_B$
(e)	asymétrie	$(\forall b, c \mid : b\ \rho\ c\ \Rightarrow\ \neg(c\ \rho\ b))$	$\rho \cap \rho^{-1} = \emptyset$
(f)	transitivité	$(\forall b, c, d \mid : b\ \rho\ c\ \wedge\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d)$	$\rho = (\cup i \mid i > 0 : \rho^i)$ $\rho^2 \subseteq \rho$

Exemples.

Propriété	$=$	$<$	$\leq$	$\subset$	$\subseteq$	$\Rightarrow$
réflexivité	×		×		×	×
irréflexivité		×		×		
symétrie	×					

Propriété	$=$	$<$	$\leq$	$\subset$	$\subseteq$	$\Rightarrow$
antisymétrie	×	×	×	×	×	×
asymétrie		×		×		
transitivité	×	×	×	×	×	×

Définition $\rho^2 \subseteq \rho$ de la transitivité)

Montrons que cette définition est équivalente à la définition 1 de la transitivité. C'est-à-dire, montrons

$$\rho^2 \subseteq \rho\ \equiv\ (\forall b, c, d \mid : b\ \rho\ c\ \wedge\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d)\ .$$

$\rho^2 \subseteq \rho$

$=$ ⟨ Définition de la puissance d'une relation (12.39) ⟩

$\rho \circ \rho \subseteq \rho$

$=$ ⟨ Sous-ensemble (11.21) & Remarquez que nous utilisons le fait que les ensembles de l'expression ci-dessus sont des relations et contiennent des couples ordonnés (ce sont des notions de typage) ⟩

$(\forall b, d \mid b\ \rho \circ \rho\ d : b\ \rho\ d)$

$=$ ⟨ Transfert (7.17b) ⟩

$(\forall b, d \mid : \neg(b\ \rho \circ \rho\ d)\ \vee\ b\ \rho\ d)$

$=$ ⟨ Définition du produit de relations (12.25) ⟩

$(\forall b, d \mid : \neg(\exists c \mid : b\ \rho\ c\ \rho\ d)\ \vee\ b\ \rho\ d)$

$=$ ⟨ De Morgan (7.16b) ⟩

$$
\begin{array}{ll}
 & (\forall b, d \mid: (\forall c \mid: \neg(b\ \rho\ c\ \rho\ d))\ \vee\ b\ \rho\ d) \\
= & \quad \langle\ \neg\mathsf{libre}(\text{`}d\text{'},\text{`}\mathsf{vrai}\text{'})\ \ \&\ \ \text{Imbrication (6.34)}\ \ \& \\
 & \qquad \neg\mathsf{libre}(\text{`}c\text{'},\text{`}b\ \rho\ d\text{'})\ \ \&\ \ \text{Distributivité de } \vee \text{ sur } \forall \text{ (7.21)}\ \rangle \\
 & (\forall b \mid: (\forall d \mid: (\forall c \mid: \neg(b\ \rho\ c\ \rho\ d)\ \vee\ b\ \rho\ d))) \\
= & \quad \langle\ \neg\mathsf{libre}(\text{`}c\text{'},\text{`}\mathsf{vrai}\text{'})\ \ \&\ \ \neg\mathsf{libre}(\text{`}d\text{'},\text{`}\mathsf{vrai}\text{'})\ \ \& \\
 & \qquad \text{Échange des variables de quantification (6.31)}\ \ \&\ \ \text{Définition de l'implication (3.75)}\ \rangle \\
 & (\forall b \mid: (\forall c \mid: (\forall d \mid: b\ \rho\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d))) \\
 & \quad \langle\ \neg\mathsf{libre}(\text{`}c, d\text{'},\text{`}\mathsf{vrai}\text{'})\ \ \&\ \ \text{Imbrication (6.34) deux fois}\ \ \&\ \ \text{Notation page 12}\ \rangle \\
 & (\forall b, c, d \mid: b\ \rho\ c\ \wedge\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d)
\end{array}
$$

Remarquez que cette preuve pourrait être quelque peu simplifiée si nous disposions d'un théorème de la forme

$$(*) \qquad (\star x \mid R : P) = (\star y \mid R : P),$$

où la liste de variables y est une permutation de la liste x. La fin de la preuve deviendrait :

$$
\begin{array}{ll}
 & (\forall b, d \mid: (\forall c \mid: \neg(b\ \rho\ c\ \rho\ d))\ \vee\ b\ \rho\ d) \\
= & \quad \langle\ \neg\mathsf{libre}(\text{`}c\text{'},\text{`}b\ \rho\ d\text{'})\ \ \&\ \ \text{Distributivité de } \vee \text{ sur } \forall \text{ (7.21)}\ \rangle \\
 & (\forall b, d \mid: (\forall c \mid: \neg(b\ \rho\ c\ \rho\ d)\ \vee\ b\ \rho\ d)) \\
= & \quad \langle\ \neg\mathsf{libre}(\text{`}c\text{'},\text{`}\mathsf{vrai}\text{'})\ \ \&\ \ \text{Imbrication (6.34)}\ \ \& \\
 & \qquad \text{Définition de l'implication (3.75)}\ \rangle \\
 & (\forall b, d, c \mid: b\ \rho\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d) \\
 & \quad \langle\ (*) \text{ ci-dessus}\ \ \&\ \ \text{Notation page 12}\ \rangle \\
 & (\forall b, d, c \mid: b\ \rho\ c\ \wedge\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d)
\end{array}
$$

Fermeture transitive et fermeture transitive réflexive

(12.43) Définition. Soit ρ une relation sur un ensemble.

- La *fermeture transitive* de ρ, notée ρ^+, est la plus petite relation transitive qui contient ρ.
- La *fermeture transitive réflexive* de ρ, notée ρ^*, est la plus petite relation transitive et réflexive qui contient ρ.

(12.44) Remarque. Quand on dit que la relation ρ est *plus petite* que la relation σ, cela signifie $\rho \subseteq \sigma$. On dit aussi que σ *contient* ρ.

(12.45) Théorème : Soit ρ une relation sur un ensemble B.

(a) $\rho^+ \;=\; (\cup i \mid 0 < i : \rho^i)$

(b) $\rho^* \;=\; \rho^+ \cup \mathbf{I}_B \;=\; (\cup i \mid 0 \leq i : \rho^i)$

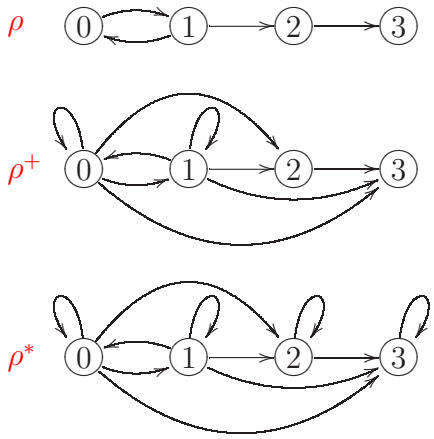
Pour démontrer (12.45a), il faut montrer que

1. $(\cup i \mid 0 < i : \rho^i)$ contient ρ, ce qui est évident,
2. $(\cup i \mid 0 < i : \rho^i)$ est transitive, ce qui est partiellement démontré ci-dessous,
3. toute autre relation transitive qui contient ρ et qui est transitive contient aussi $(\cup i \mid 0 < i : \rho^i)$. Cette preuve ne sera pas donnée.

(12.45b) se démontre de manière similaire.

Exemples de fermetures transitives

1. Rappelons que $\mathsf{succ\_de} = \{b{:}\mathbb{Z} \mid : \langle b+1, b\rangle\}$.
   $a \;\mathsf{succ\_de}^+\; b \;\equiv\; a > b$
   $a \;\mathsf{succ\_de}^*\; b \;\equiv\; a \geq b$
2. $a \;\mathsf{parent\_de}^+\; b \;\equiv\; a$ est un ancêtre de b
   $a \;\mathsf{parent\_de}^*\; b \;\equiv\; a$ est un ancêtre de b ou $a = b$
3. Soit $\rho = \{\langle 0,1\rangle, \langle 1,0\rangle, \langle 1,2\rangle, \langle 2,3\rangle\}$ une relation sur l'ensemble $\{0,1,2,3\}$.
   $\rho^+ = \{\langle 0,0\rangle, \langle 0,1\rangle, \langle 0,2\rangle, \langle 0,3\rangle, \langle 1,0\rangle, \langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,3\rangle\}$
   $\rho^* = \{\langle 0,0\rangle, \langle 0,1\rangle, \langle 0,2\rangle, \langle 0,3\rangle, \langle 1,0\rangle, \langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,3\rangle\}$



Preuve partielle de la transitivité de $(\cup i \mid 0 < i : \rho^i)$

Par définition de la transitivité (table 12.1) et de la puissance d'une relation (12.39), il faut montrer

$$(\cup i \mid 0 < i : \rho^i) \;\circ\; (\cup i \mid 0 < i : \rho^i) \;\subseteq\; (\cup i \mid 0 < i : \rho^i).$$

Les idées à la base de la preuve sont simples et on peut les résumer ainsi :

$$
\begin{array}{ll}
& (\cup i \mid 0 < i : \rho^i) \circ (\cup i \mid 0 < i : \rho^i) \\
= & \qquad \langle \text{ Définition de la quantification } \rangle \\
& (\rho \cup \rho^2 \cup \rho^3 \cup \ldots) \circ (\rho \cup \rho^2 \cup \rho^3 \cup \ldots) \\
= & \qquad \langle \text{ Distributivité de } \circ \text{ sur } \cup \ (12.28) \ \ \& \ \ (12.41) \ \rangle \\
& \rho^2 \cup \rho^3 \cup \rho^4 \cup \ldots \\
\subseteq & \qquad \langle \text{ Affaiblissement } (11.39) \ \rangle \\
& \rho \cup \rho^2 \cup \rho^3 \cup \rho^4 \cup \ldots \\
= & \qquad \langle \text{ Définition de la quantification } \rangle \\
& (\cup i \mid 0 < i : \rho^i)
\end{array}
$$

Relations d'équivalence

(12.46) Définition. Une *relation d'équivalence* est une relation qui est réflexive, symétrique et transitive.

(12.47) Définition. Soit ρ une relation d'équivalence sur un ensemble B, et soit $b \in B$. La *classe d'équivalence de b par la relation ρ*, notée $[b]_\rho$, est le sous-ensemble des éléments de B qui sont équivalents par la relation ρ :

$$x \in [b]_\rho \ \equiv \ x \ \rho \ b \ .$$

Si le contexte rend la relation ρ évidente, on écrit simplement $[b]$.

(12.48) Exemple.

1. L'égalité sur $\mathbb{Z}$ (ou sur tout autre ensemble) est une relation d'équivalence. La classe d'équivalence de n, c'est-à-dire $[n]_=$, contient n comme seul élément ; autrement dit, $[n]_= = \{n\}$.
2. La relation S sur l'ensemble des personnes définie par

   $$a \ S \ b \ \equiv \ a \text{ et } b \text{ ont le même sexe}$$

   est une relation d'équivalence. Les classes d'équivalence $[\mathsf{Marie}]_S$ et $[\mathsf{Paul}]_S$ contiennent respectivement l'ensemble des femmes et l'ensemble des hommes. On a

   $$[\mathsf{Marie}]_S = [\grave{\mathsf{E}}\mathsf{ve}]_S = \ldots$$

   et

   $$[\mathsf{Paul}]_S = [\mathsf{Adam}]_S = \ldots$$
3. Les relations $<$ et $\leq$ sur $\mathbb{Z}$ ou sur $\mathbb{R}$ ne sont pas des relations d'équivalence, car elles ne sont pas symétriques.

4. La relation $\overset{3}{=}$ définie sur $\mathbb{Z}$ par

$$b \overset{3}{=} c \;\equiv\; b - c \text{ est divisible par } 3 \,,$$

ou encore, de manière équivalente, par

$$b \text{ et } c \text{ ont le même reste par la division par } 3 \,,$$

est une relation d'équivalence. Les classes d'équivalence sont

$$\begin{aligned}[0] = [3] = [6] = \ldots &= \{0, 3, 6, \ldots\} \\ [1] = [4] = [7] = \ldots &= \{1, 4, 7, \ldots\} \\ [2] = [5] = [8] = \ldots &= \{2, 5, 8, \ldots\}\end{aligned}$$

Notez que chaque relation d'équivalence sur un ensemble B induit une partition de B (voyez (11.84) pour la définition d'une partition). En effet, tout élément de B est dans une et une seule classe d'équivalence.

Autres propriétés des relations $\rho \subseteq B \times C$

	Propriété	Définition 1	Définition 2
(a)	totalité	$(\forall b{:}B \mid : (\exists c{:}C \mid : b\ \rho\ c))$	$\mathsf{Dom}.\rho = B$
(b)	surjectivité	$(\forall c{:}C \mid : (\exists b{:}B \mid : b\ \rho\ c))$	$\mathsf{Im}.\rho = C$
(c)	déterminisme	$(\forall b, c, c' \mid b\ \rho\ c \ \wedge\ b\ \rho\ c' : c = c')$	$\rho^{-1} \circ \rho \subseteq \mathbf{I}_C$
(d)	injectivité	$(\forall b, b', c \mid b\ \rho\ c \ \wedge\ b'\ \rho\ c : b = b')$	$\rho \circ \rho^{-1} \subseteq \mathbf{I}_B$

Exemples. Soient les relations $\rho, \sigma, \tau, \theta$ données ci-dessous. Supposons que $=$, $<$, $\leq$, ρ, σ sont des relations sur $\mathbb{N}$, que $\subset, \subseteq$ sont des relations sur $\mathcal{P}\mathbb{N}$ et que $\Rightarrow$ est une relation sur $\{\mathsf{faux}, \mathsf{vrai}\}$.

$$\rho = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\} \qquad \sigma = \{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$$
$$\tau = \{a, b{:}\mathbb{Z} \mid a + 1 = b : \langle a, b\rangle\} \qquad \theta = \{a, b{:}\mathbb{Z} \mid a = b^2 : \langle a, b\rangle\}$$

Propriété	$=$	$<$	$\leq$	$\subset$	$\subseteq$	$\Rightarrow$	ρ	σ	τ	θ
totalité	×	×	×		×	×			×	
surjectivité	×		×		×	×			×	×
déterminisme	×						×		×	
injectivité	×								×	×

Définition de relations par compréhension : notation usuelle

À la page 138 du chapitre 11, nous avons introduit la notation traditionnelle pour la compréhension ensembliste,

$$\{x \mid R\} \ ;$$

c'est une abréviation de

$$\{x \mid R : x\} \ .$$

On peut faire la même chose avec les relations. La notation usuelle pour définir une relation par compréhension est

$$\{\langle b, c\rangle \mid R\} \ ;$$

c'est une abréviation de

$$\{b, c \mid R : \langle b, c\rangle\} \ ,$$

où b et c sont des variables (et pas des expressions arbitraires).

(12.49) Exemple.

$$\{\langle a{:}\mathbb{Z}, b{:}\mathbb{Z}\rangle \mid a + 1 = b\} \ = \ \{a{:}\mathbb{Z}, b{:}\mathbb{Z} \mid a + 1 = b : \langle a, b\rangle\} \ .$$

12.3 Fonctions

Les fonctions sont des relations avec une propriété particulière.

(12.50) Définition. Une relation binaire $f \subseteq B \times C$ est une *fonction* ssi f est déterministe, c'est-à-dire, rappelons-le, ssi

$$(\forall b, c, c' \mid b \ f \ c \ \wedge \ b \ f \ c' : c = c') \ .$$

Par exemple,

1. $\{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$ est une fonction.
2. $g = \{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$ n'est pas une fonction, car $1 \ g \ 2 \wedge 1 \ g \ 3$, mais $2 \neq 3$.
3. $\{a, b{:}\mathbb{Z} \mid a + 1 = b : \langle a, b\rangle\}$ est une fonction.
4. $h = \{a, b{:}\mathbb{Z} \mid a = b^2 : \langle a, b\rangle\}$ n'est pas une fonction. Par exemple, $\langle 4, 2\rangle \in f$ et $\langle 4, -2\rangle \in f$.

Quand f est une fonction, on écrit habituellement $f.a = b$ plutôt que $\langle a, b\rangle \in f$ ou $a \ f \ b$.

Fonctions : notation, fonctions partielles

(12.51) Définition. Soit $f \subseteq B \times C$ une fonction. Si f est totale (c'est-à-dire si elle est une relation totale), on note son type de la manière suivante :

$$f{:}B \to C \ .$$

Si f n'est pas totale, on dit qu'elle est une *fonction partielle* et on note son type de la manière suivante :

$$f{:}B \rightsquigarrow C \ .$$

Une fonction totale est dite une *application*. Le terme *fonction* désigne une fonction totale ou partielle.

(12.52) Remarque. Pour d'autres auteurs (très nombreux), le terme *fonction* désigne une *fonction totale*.

Fonctions : bijectivité

(12.53) Définition. Une application injective et surjective est dite *bijective*.

(12.54) Exemple.

fonction	type	commentaire
$d.x = 1/x$	$d{:}\mathbb{R} \rightsquigarrow \mathbb{R}$	non bijective, car partielle
$g.x = x - 3$	$g{:}\mathbb{Z} \to \mathbb{Z}$	application bijective
$h.x = 0$	$h{:}\mathbb{Z} \to \mathbb{Z}$	application non bijective, car non injective et non surjective
$f.x = x$	$f{:}\mathbb{Z} \to \mathbb{Z}$	application bijective (fonction identité)
$f.x = x$	$f{:}\mathbb{N} \to \mathbb{Z}$	application non bijective (car non surjective)

Inverse d'une fonction

(12.55) Définition. Soit $f{:}B \to C$. La fonction $g{:}C \to B$ est dite *l'inverse* de f ssi

$$f(g.c) = c \quad \text{et} \quad g(f.b) = b \ , \quad \text{quels que soient } b{:}B \text{ et } c{:}C.$$

Autrement dit,

$$g \circ f = \mathbf{I}_C \quad \text{et} \quad f \circ g = \mathbf{I}_B \ .$$

Si une fonction f a un inverse, elle est dite *inversible*.

Par exemple, la fonction $g{:}\mathbb{Z} \to \mathbb{Z}$ définie par $g.x = x - 3$ est l'inverse de la fonction $f{:}\mathbb{Z} \to \mathbb{Z}$ définie par $f.x = x + 3$.

Remarques :

1. On peut montrer que si g est l'inverse de f, alors $g = f^{-1}$.
2. Directement de la définition d'inverse, on voit que si g est l'inverse de f, alors f est l'inverse de g.

(12.56) Théorème : Soit $f{:}B \to C$. L'application f est inversible ssi elle est bijective.

(12.57) Remarque. Vous n'avez pas à étudier la composition de fonctions, notée • (page 281 du manuel), ni les inverses à gauche et à droite (page 283).

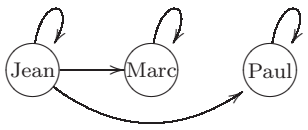
12.4 Relations d'ordre

(12.58) Définition. Une relation binaire ρ sur un ensemble B est dite une *relation d'ordre partiel* sur B, ou encore un *ordre partiel* sur B, ssi elle est réflexive, antisymétrique et transitive. Si ρ est un ordre partiel sur B, la paire $\langle B, \rho\rangle$ est appelée un *ensemble partiellement ordonné*.

Une relation d'ordre compare les éléments d'un ensemble. Nous utiliserons le symbole $\preceq$ pour désigner un ordre partiel quelconque et nous écrirons indifféremment $a \preceq b$ ou $b \succeq a$.

(12.59) Exemple. Voici des exemples d'ensembles partiellement ordonnés.

1. $\langle \mathbb{N}, \leq \rangle$
2. $\langle \mathcal{P}\mathbb{N}, \subseteq \rangle$
3. $\langle \{\mathsf{Jean}, \mathsf{Marc}, \mathsf{Paul}\},$
   $\big\{\langle \mathsf{Jean}, \mathsf{Jean}\rangle, \langle \mathsf{Jean}, \mathsf{Marc}\rangle, \langle \mathsf{Jean}, \mathsf{Paul}\rangle, \langle \mathsf{Marc}, \mathsf{Marc}\rangle, \langle \mathsf{Paul}, \mathsf{Paul}\rangle\big\}\rangle$



(12.60) Définition. Une relation binaire $\prec$ sur un ensemble B est dite une *relation d'ordre partiel strict* sur B, ou encore un *ordre partiel strict* sur B, ssi elle est transitive et irréflexive.

(12.61) Théorème : Si ρ est un ordre partiel sur un ensemble B, alors

$$\rho - \mathbf{I}_B$$

est un ordre partiel strict. Si ρ est un ordre partiel strict sur B, alors

$$\rho \cup \mathbf{I}_B$$

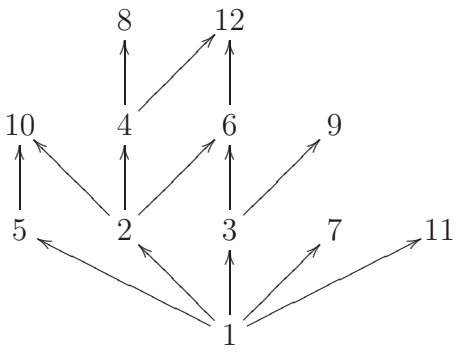
est un ordre partiel.

Pour passer d'un ordre partiel à un ordre partiel strict, il suffit donc d'enlever les couples de la forme $\langle b, b\rangle$. Pour passer d'un ordre partiel strict à un ordre partiel, il suffit d'ajouter les couples $\langle b, b\rangle$.

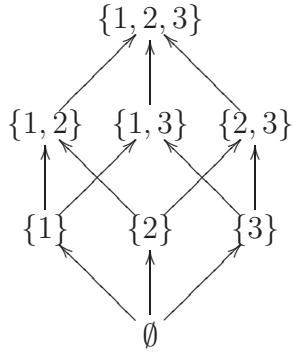
Par exemple, $<$ est un ordre partiel strict sur $\mathbb{Z}$ et $\subset$ est un ordre partiel strict sur $\mathcal{P}\mathbb{Z}$. Les ordres partiels correspondants sont $\leq$ et $\subseteq$.

Diagrammes de Hasse

On peut représenter les ensembles ordonnés $\langle B, \preceq \rangle$ finis et suffisamment petits par un diagramme appelé *diagramme de Hasse*. Les éléments de B sont les sommets du diagramme et certains couples de la relation sont représentés par des arcs (lignes entre les sommets). Si $b \prec c$, alors le sommet b est placé plus bas que le sommet c. Si $b \prec c$ et qu'il n'y a pas d'élément d tel que $b \prec d \prec c$, un arc est tracé entre b et c. Par exemple, voici les diagrammes de Hasse de deux ordres ($\mid$ est la relation « divise »)



$\langle \{i \mid 1 \leq i \leq 12\}, \mid \rangle$



$\langle \mathcal{P}\{1,2,3\},\ \subseteq \rangle$

Ensembles totalement ordonnés

(12.62) Définition. Un ordre partiel $\preceq$ sur B est appelé un *ordre total* ssi

$$(\forall b, c \mid : b \preceq c \vee b \succeq c) \ ,$$

autrement dit, ssi deux éléments quelconques b et c sont comparables. Dans ce cas, la paire $\langle B, \preceq \rangle$ est appelée un *ensemble totalement ordonné* ou une *chaîne*.

Par exemple,

1. $\langle \mathbb{R}, \leq \rangle$ est un ensemble totalement ordonné.
2. $\langle \mathcal{P}\mathbb{N}, \subseteq \rangle$ n'est pas totalement ordonné. Par exemple, on n'a ni $\{1\} \subseteq \{2\}$ ni $\{2\} \subseteq \{1\}$.

12.5 Bases de données relationnelles

Rappelons qu'une relation n-aire sur le produit cartésien $B_1 \times \cdots \times B_n$ est un sous-ensemble de $B_1 \times \cdots \times B_n$. Une telle relation peut être présentée sous la forme d'une table dont les lignes sont les n-uplets de la relation et dont les colonnes contiennent des noms pour les n composantes des n-uplets. Ces noms sont appelés des *attributs*.

Les tables 12.2 et 12.3 donnent deux exemples de relations.

Chaque relation a un *schéma*, de la forme

$$Nom\_rel(Attribut_1, \ldots, Attribut_n) \ ,$$

qui donne le nom de la relation et de ses attributs. Par exemple, le schéma de la relation de la table 12.2 est

$$\text{Cours(Nom, Sigle, Crédits, Session)} \ .$$

Si on considère Nom, Sigle, Crédits, Session comme des ensembles de noms, de sigles, de nombres de crédits et de nombres dénotant des sessions, alors

$$\text{Cours} \subseteq \text{Nom} \times \text{Sigle} \times \text{Crédits} \times \text{Session} \ .$$

TAB. 12.2 – La relation Cours(Nom, Sigle, Crédits, Session)

Sigle	Nom	Crédits	Session
IFT-10540	Logique et structures discrètes	4	1
IFT-10544	Systèmes d'exploitation I	3	3
IFT-17582	Algorithmique et programmation	4	1
IFT-17583	Structure interne des ordinateurs	4	1
IFT-17588	Analyse d'algorithmes	3	3

Construction de requêtes : la sélection

L'opérateur de sélection est noté σ. L'opération $\sigma(R, F)$ retourne l'ensemble des n-uplets de la relation R qui satisfont le prédicat F. Par conséquent,

$$\sigma(R, F) = \{t \mid t \in R \ \wedge \ F\} \ .$$

Par exemple (table 12.2),

$\sigma(\text{Cours}, \text{Crédits} = 3)$

$=$

Sigle	Nom	Crédits	Session
IFT-10544	Systèmes d'exploitation I	3	3
IFT-17588	Analyse d'algorithmes	3	3

Construction de requêtes : la projection

L'opérateur de projection est noté π. L'opération $\pi(R, A_1, \ldots, A_m)$ garde seulement les attributs $A_1, \ldots, A_m$, élimine les autres et élimine les m-uplets en double. Par exemple (table 12.2),

TAB. 12.3 – La relation Horaire(Sigle, Groupe, Jour, Heure, Local)

Sigle	Groupe	Jour	Heure	Local
IFT-10540	A	Mer	10h30	2551PLT
IFT-10540	B	Ven	10h30	2551PLT
IFT-10542	A	Lun	8h30	2341PLT
IFT-10542	B	Mer	8h30	3840VCH
IFT-10544	A	Mar	8h30	2751PLT
IFT-10544	B	Jeu	8h30	3880VCH
IFT-17582	A	Mar	10h30	1112PLT

$\pi(\text{Horaire}, \text{Sigle}, \text{Heure}) =$

Sigle	Heure
IFT-10540	10h30
IFT-10542	8h30
IFT-10544	8h30
IFT-17582	10h30

TAB. 12.4 – La relation Cours $\bowtie$ Horaire

Sigle	Nom	Crédits	Session	Groupe	Jour	Heure	Local
IFT-10540	LSD	4	1	A	Mer	10h30	2551PLT
IFT-10540	LSD	4	1	B	Ven	10h30	2551PLT
IFT-10544	SEx	3	3	A	Mar	8h30	2751PLT
IFT-10544	SEx	3	3	B	Jeu	8h30	3880VCH
IFT-17582	Algo	4	1	A	Mar	10h30	1112PLT

Construction de requêtes : la jointure

L'opérateur de jointure est un opérateur binaire noté $\bowtie$. Étant données deux relations Q et R, la relation $Q \bowtie R$ ressemble au produit cartésien de Q et R : elle a tous les attributs de Q et R, mais un attribut qui est un attribut et de Q et de R apparaît une seule fois dans $Q \bowtie R$. De plus, seulement les n-uplets qui ont la même valeur pour cet attribut commun sont conservés. Par exemple, la relation

Cours $\bowtie$ Horaire)

est donnée dans la (table 12.2) (une abréviation est utilisée pour les noms de cours).

Requêtes complexes

On peut combiner les trois opérateurs $\sigma, \pi, \bowtie$ pour former des requêtes complexes. Par exemple, la requête suivante vise à connaître les sigles et les noms des cours qui se donnent dans les locaux 2551 ou 2751 du pavillon Pouliot :

$$\pi\big(\sigma(\text{Cours} \bowtie \text{Horaire}, \text{Local} = 2551\text{PLT} \vee \text{Local} = 2751\text{PLT}), \text{Sigle}, \text{Nom}\big)$$

Le résultat est

Sigle	Nom
IFT-10540	Logique et structures discrètes
IFT-10544	Systèmes d'exploitation I

Remarque : dans une application réelle, tout cours de la relation Horaire devrait être un cours de la relation Cours. Les exemples ci-dessus ont été choisis pour illustrer les différents opérateurs plutôt que pour décrire une situation réelle.

12.6 Problèmes

1. Démontrez le théorème d'appartenance (12.4), $\langle x, y\rangle \in S \times T \equiv x \in S \wedge y \in T$.
2. Démontrez le théorème (12.5), $\langle x, y\rangle \in S \times T \equiv \langle y, x\rangle \in T \times S$.
3. Démontrez la distributivité de $\times$ sur $-$ (12.10), $S \times (T - U) = (S \times T) - (S \times U)$.
4. Démontrez le théorème (12.14), $(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$.
5. Soient ρ et σ les relations suivantes sur l'ensemble $\{b, c, d, e\}$:

   $$\rho = \{\langle b, b\rangle, \langle b, c\rangle, \langle c, d\rangle\}$$
   $$\sigma = \{\langle b, c\rangle, \langle c, d\rangle, \langle d, b\rangle\}$$

   Calculez $\rho \circ \sigma$, $\sigma \circ \rho$, ρ^2 et ρ^3.
6. Démontrez la sous-distributivité de $\circ$ sur $\cap$ (12.29),

   $$\rho \circ (\sigma \cap \theta) \subseteq \rho \circ \sigma \cap \rho \circ \theta \qquad \text{et} \qquad (\sigma \cap \theta) \circ \rho \subseteq \sigma \circ \rho \cap \theta \circ \rho.$$

7. Soit la relation $\rho \subseteq B \times B$. Démontrez le théorème (12.41), $\rho^m \circ \rho^n = \rho^{m+n}$, par induction.
8. La table (12.1) définit six classes de relations de deux manières différentes. Montrez que les deux définitions de l'asymétrie sont équivalentes.
9. La table (12.1) définit six classes de relations de deux manières différentes. Montrez que les deux définitions de l'asymétrie sont équivalentes.
10. Quelles propriétés de la table (12.1) les relations suivantes possèdent-elles ?

(a) $b \rho c$ ssi b et c sont des entiers tous deux négatifs ou tous deux positifs.

(b) $b \rho c$ ssi b et c sont des entiers tels que $b - c$ est un multiple de 5.

(c) $\emptyset$, où $\emptyset$ est une relation sur un ensemble non vide B.

(d) $\mathbf{I}_B$, la relation identité sur un ensemble non vide B.

(e) $B \times B$, où B est un ensemble non vide contenant au moins deux éléments.

(f) $=$ sur $\mathbb{Z}$.

(g) $<$ sur $\mathbb{Z}$.

(h) $\leq$ sur $\mathbb{Z}$

(i) $b \rho c$ ssi b est le père de c.

(j) $b \rho c$ ssi b est le père de c ou vice-versa.

(k) $b \rho c$ ssi b est c ou le père de c.

11. Trouvez un plus petit ensemble non vide et une relation sur cet ensemble qui n'est ni symétrique ni antisymétrique.

12. Considérons les relations binaires sur un ensemble B. On dit qu'une propriété est *préservée par une opération* si l'application de l'opération à des relations qui ont la propriété produit une relation qui a la propriété. Par exemple, l'union de deux relations symétriques est symétrique, de sorte que l'union préserve la symétrie. Inscrivez un O dans chaque entrée [ligne, colonne] de la table suivante si l'opération de la colonne préserve la propriété de la ligne et inscrivez un N dans le cas contraire. Pour chaque N, donnez un contre-exemple.

	$\rho \cup \sigma$	$\rho \cap \sigma$	$\rho - \sigma$	$(B \times B) - \rho$
Réflexivité				
Irréflexivité				
Symétrie				
Antisymétrie				
Transitivité				

13. Soient les relations $\rho \subseteq \mathbb{Z} \times \mathbb{Z}$ et $\sigma \subseteq \mathbb{Z} \times \mathbb{Z}$ définies par

$$\begin{aligned} \rho &= \{b, c \mid b + 3 = c : \langle b, c \rangle\}, \\ \sigma &= \{b, c \mid b^2 = c : \langle b, c \rangle\}. \end{aligned}$$

Calculez $\rho \circ \sigma$ et $\sigma \circ \rho$.

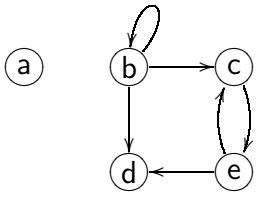
Chapitre 13

Théorie des graphes

13.1 Graphes et chemins

Graphes orientés

Un *graphe orienté* est un couple $\langle S, A\rangle$, où S est un ensemble fini non vide et A une relation sur S. Un élément de S est appelé un *sommet* et un élément (un couple) de A est appelé un *arc*. La composante a d'un arc $\langle a, b\rangle$ est dite l'*origine* de l'arc et la composante b est dite la *cible* ou la *destination* de l'arc. Un arc de la forme $\langle a, a\rangle$ s'appelle une *boucle*. Un sommet qui n'apparaît dans aucun arc est dit *isolé*. Si $\langle a, b\rangle \in A$, les sommets a et b sont dits *adjacents*.

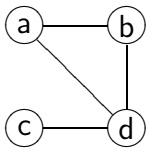


$G = \langle S, A\rangle$
où
$S = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$
$A = \{\langle \mathsf{b}, \mathsf{b}\rangle, \langle \mathsf{b}, \mathsf{c}\rangle, \langle \mathsf{b}, \mathsf{d}\rangle, \langle \mathsf{c}, \mathsf{e}\rangle, \langle \mathsf{e}, \mathsf{c}\rangle, \langle \mathsf{e}, \mathsf{d}\rangle\}$

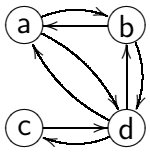
FIG. 13.1 – Un graphe orienté G

Graphes non orientés

Un *graphe non orienté* est un couple $\langle S, A\rangle$, où S est un ensemble fini non vide et A un ensemble de couples non ordonnés d'éléments de S. Un élément de S est appelé un *sommet* et un élément de A est appelé une *arête*. Une arête est représentée par un ensemble de deux sommets. Un sommet qui n'apparaît dans aucune arête est dit *isolé*. Si $\{a, b\} \in A$, les sommets a et b sont dits *adjacents*.



$G = \langle S, A \rangle$
où
$S = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}$
$A = \big\{\{\mathsf{a}, \mathsf{b}\}, \{\mathsf{a}, \mathsf{d}\}, \{\mathsf{b}, \mathsf{d}\}, \{\mathsf{c}, \mathsf{d}\}\big\}$



$G' = \langle S, A' \rangle$
où
$S = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}$
$A' = \big\{\langle \mathsf{a}, \mathsf{b}\rangle, \langle \mathsf{b}, \mathsf{a}\rangle, \langle \mathsf{a}, \mathsf{d}\rangle, \langle \mathsf{d}, \mathsf{a}\rangle,$
$\langle \mathsf{b}, \mathsf{d}\rangle, \langle \mathsf{d}, \mathsf{b}\rangle, \langle \mathsf{c}, \mathsf{d}\rangle, \langle \mathsf{d}, \mathsf{c}\rangle\big\}$

FIG. 13.2 – Un graphe non orienté G et une représentation équivalente par un graphe orienté G'

Degré d'un sommet ou d'un graphe

On dit que l'arête $\{a, b\}$ et l'arc $\langle a, b\rangle$ sont *incidents* aux sommets a et b. Le *degré d'un sommet* s, noté $\mathsf{deg}.s$, est le nombre d'arêtes ou d'arcs dans lesquels s apparaît (c'est-à-dire le nombre d'arêtes ou d'arcs incidents), les boucles comptant pour 2. Le *degré d'un graphe* est le degré du sommet qui a le degré le plus élevé.

Par exemple, dans la figure 13.1,

$$\mathsf{deg.a} = 0, \qquad \mathsf{deg.b} = 4, \qquad \mathsf{deg.d} = 2 \qquad \text{et} \qquad \mathsf{deg}.G = 4$$

(le degré de tout sommet isolé, comme a, est 0). Dans la figure 13.2, pour le graphe non orienté,

$$\mathsf{deg.a} = 2, \qquad \mathsf{deg.c} = 1, \qquad \mathsf{deg.d} = 3 \qquad \text{et} \qquad \mathsf{deg}.G = 3.$$

Puisque que tout arc incident (de même pour les arêtes) contribue 2 aux degrés des sommets, on obtient le théorème suivant.

(13.1) Théorème : La somme des degrés des sommets d'un graphe $\langle S, A\rangle$ (orienté ou non) est $2 \cdot \#A$.

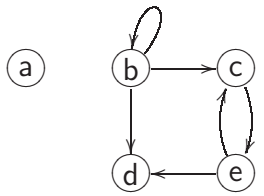
(13.2) Corollaire : Dans un graphe (orienté ou non), le nombre de sommets de degré impair est pair.

Chemins

Un *chemin* dans un graphe orienté est une séquence (suite) de sommets et d'arcs telle que

1. la séquence débute par un sommet et se termine par un sommet ;
2. les sommets et les arcs alternent ;
3. chaque arc est précédé par son sommet origine et est suivi par son sommet cible ;
4. aucun arc n'apparaît plus d'une fois.

Par exemple, dans la figure ci-contre,



$$\langle \mathsf{c}, \langle \mathsf{c}, \mathsf{e}\rangle, \mathsf{e}, \langle \mathsf{e}, \mathsf{d}\rangle, \mathsf{d}\rangle$$

et

$$\langle \mathsf{b}, \langle \mathsf{b}, \mathsf{c}\rangle, \mathsf{c}, \langle \mathsf{c}, \mathsf{e}\rangle, \mathsf{e}\langle \mathsf{e}, \mathsf{c}\rangle, \mathsf{c}\rangle$$

sont des chemins, mais pas

$$\langle \mathsf{b}, \langle \mathsf{b}, \mathsf{c}\rangle, \mathsf{c}, \langle \mathsf{c}, \mathsf{e}\rangle, \mathsf{e}\langle \mathsf{e}, \mathsf{c}\rangle, \mathsf{c}, \langle \mathsf{c}, \mathsf{e}\rangle, \mathsf{e}\rangle$$

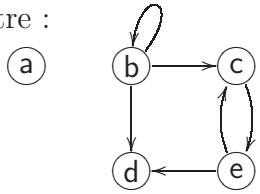
ni

$$\langle \mathsf{b}, \langle \mathsf{b}, \mathsf{c}\rangle, \mathsf{c}, \langle \mathsf{e}, \mathsf{c}\rangle, \mathsf{c}\rangle \ .$$

La *longueur* d'un chemin est le nombre d'arcs de ce chemin :

$$\text{longueur de } \langle \mathsf{c}, \langle \mathsf{c}, \mathsf{e}\rangle, \mathsf{e}\rangle = 1 \qquad \text{et} \qquad \text{longueur de } \langle \mathsf{c}\rangle = 0 \ .$$

La description des chemins peut être simplifiée en donnant seulement la suite de sommets, puisque les arcs peuvent être ajoutés à partir de la séquence de sommets. Les séquences de sommets suivantes sont donc des chemins du graphe ci-contre :



$\langle \mathsf{b}, \mathsf{c}, \mathsf{e}\rangle$ (longueur 2)
$\langle \mathsf{d}\rangle$ (longueur 0)

Un chemin pourrait aussi être décrit en donnant seulement la séquence d'arcs.

Un *chemin simple* est un chemin dans lequel aucun sommet n'apparaît plus d'une fois, sauf que *le premier et le dernier peuvent être les mêmes*. Par exemple,

$$\langle \mathsf{b}\rangle, \quad \langle \mathsf{b}, \mathsf{c}, \mathsf{e}, \mathsf{d}\rangle, \quad \langle \mathsf{c}, \mathsf{e}, \mathsf{c}\rangle$$

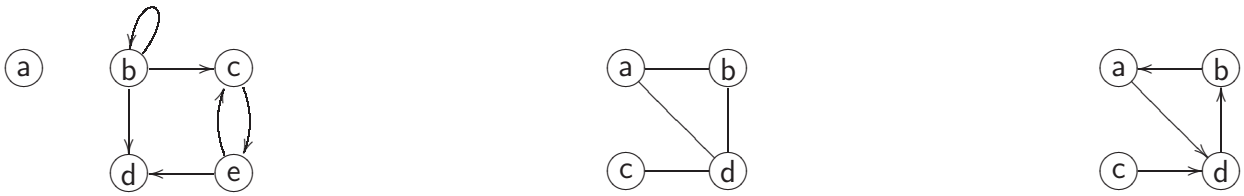
sont des chemins simples du graphe ci-dessus, mais pas $\langle \mathsf{b}, \mathsf{c}, \mathsf{e}, \mathsf{c}\rangle$.

Un chemin est un *cycle* s'il contient au moins un arc et que le premier et le dernier sommet du chemin sont identiques.

(13.3) Remarque. Des définitions similaires peuvent être données pour les graphes non orientés.

Un graphe non orienté est dit *connexe* s'il y a un chemin entre n'importe quelle paire de sommets. Un graphe orienté est dit *connexe* si, en transformant ses arcs en arêtes non orientées, on obtient un graphe non orienté connexe.

Par exemple, le graphe de gauche ci-dessous n'est pas connexe, mais les deux autres le sont.

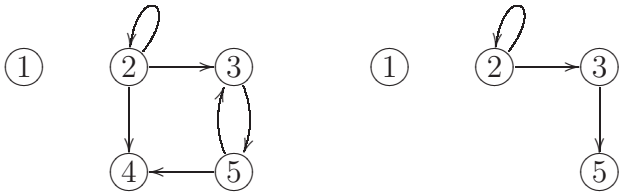


Sous-graphes

Un graphe $\langle S', A' \rangle$ est un *sous-graphe* du graphe $\langle S, A \rangle$ ssi

$$S' \subseteq S \qquad \text{et} \qquad A' \subseteq A \ .$$

Notez que parce que $\langle S', A' \rangle$ est un graphe, les extrémités des arcs ou des arêtes de A' sont dans S'. Le graphe de droite ci-dessous est un sous-graphe du graphe de gauche.



Cette notion s'applique aussi aux graphes non orientés.

13.2 Représentation matricielle des graphes

Les matrices sont l'une des structures de données utilisées en informatique pour représenter les graphes et les relations.

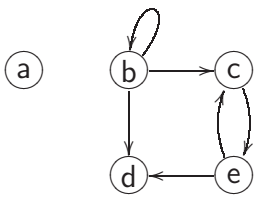
Soit le graphe orienté $G = \langle S, A \rangle$, où

$$S = \{s_1, \ldots, s_n\} \ .$$

La *matrice d'adjacence* M_G de G est une matrice booléenne telle que

$$M_G[i, j] \ \equiv \ \langle s_i, s_j \rangle \in A \ .$$

Voici un graphe et sa matrice d'adjacence (on suppose que les sommets sont ordonnés dans l'ordre $\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}$). La deuxième matrice utilise la notation usuelle, où 0 et 1 représentent faux et vrai, respectivement. Nous utiliserons la notation usuelle.



$$\begin{pmatrix} \mathsf{f} & \mathsf{f} & \mathsf{f} & \mathsf{f} & \mathsf{f} \\ \mathsf{f} & \mathsf{v} & \mathsf{v} & \mathsf{v} & \mathsf{f} \\ \mathsf{f} & \mathsf{f} & \mathsf{f} & \mathsf{f} & \mathsf{v} \\ \mathsf{f} & \mathsf{f} & \mathsf{f} & \mathsf{f} & \mathsf{f} \\ \mathsf{f} & \mathsf{f} & \mathsf{v} & \mathsf{v} & \mathsf{f} \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

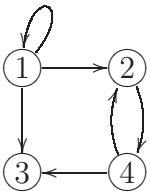
Opérations sur les graphes et les matrices

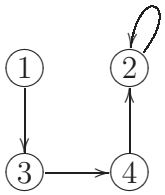
Nous allons définir cinq opérations sur les graphes et sur les matrices d'adjacence de ces graphes. Ce sont des opérations qui s'appliquent aussi aux relations.

Soient les graphes orientés

$$G = \langle S, A\rangle \ , \quad G_1 = \langle S, A_1\rangle \quad \text{et} \quad G_2 = \langle S, A_2\rangle \ .$$

À des fins d'illustration, nous utiliserons les deux graphes qui suivent :

G_1 : 

G_2 : 

Leurs matrices sont

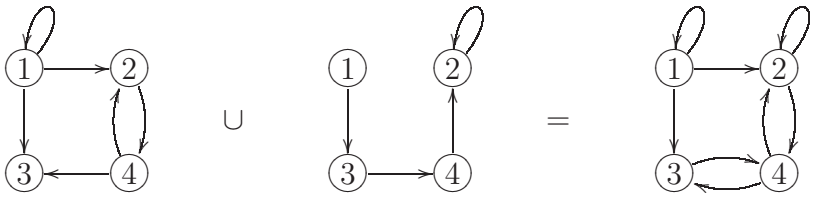
$$M_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Union

$$G_1 \cup G_2 \ = \ \langle S, A_1\rangle \cup \langle S, A_2\rangle \ = \ \langle S, A_1 \cup A_2\rangle$$

$$M_1 \cup M_2 \qquad \text{est définie par} \qquad (M_1 \cup M_2)[i,j] \ = \ M_1[i,j] \vee M_2[i,j]$$

C'est-à-dire que l'union des matrices est obtenue en faisant la disjonction des entrées correspondantes. Notez que l'opérateur ensembliste $\cup$ est *surchargé* pour pouvoir l'appliquer non seulement à des ensembles, mais aussi à des graphes et à des matrices.



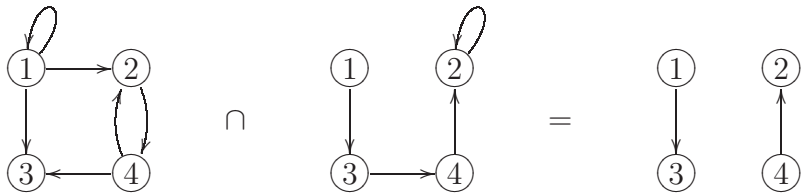
$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad \cup \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Intersection

$$G_1 \cap G_2 \;=\; \langle S, A_1\rangle \cap \langle S, A_2\rangle \;=\; \langle S, A_1 \cap A_2\rangle$$

$$M_1 \cap M_2 \qquad \text{est définie par} \qquad (M_1 \cap M_2)[i,j] \;=\; M_1[i,j] \wedge M_2[i,j]$$

C'est-à-dire que l'union des matrices est obtenue en faisant la conjonction des entrées correspondantes.



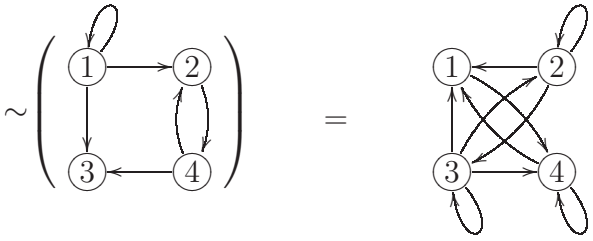
$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \cap \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Complément

$$\sim G \;=\; \sim\langle S, A\rangle \;=\; \langle S, \sim A\rangle$$

$$\sim M \qquad \text{est défini par} \qquad (\sim M)[i,j] \;=\; \neg(M[i,j])$$

C'est-à-dire que le complément d'une matrice est obtenu en faisant la négation des entrées.



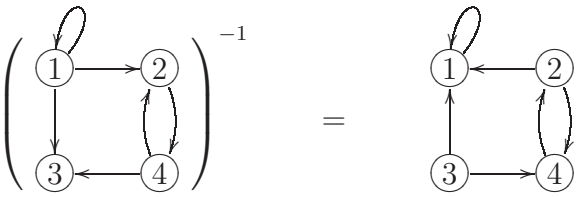
$$\sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Inverse

$$G^{-1} \;=\; \langle S, A\rangle^{-1} \;=\; \langle S, A^{-1}\rangle$$

$$M^{-1} \qquad \text{est défini par} \qquad (M^{-1})[i,j] \;=\; M[j,i]$$

C'est-à-dire que l'inverse d'une matrice est obtenu en transposant la matrice.



$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}^{-1} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

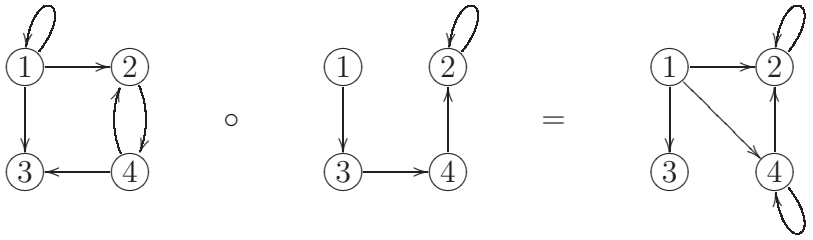
Produit

$$G_1 \circ G_2 \;=\; \langle S, A_1\rangle \circ \langle S, A_2\rangle \;=\; \langle S, A_1 \circ A_2\rangle$$

$$M_1 \circ M_2 \qquad \text{est défini par} \qquad (M_1 \circ M_2)[i,j] \;=\; (\vee k \mid: M_1[i,k] \wedge M_2[k,j])$$

Le produit des matrices est obtenu en faisant une opération similaire au produit matriciel en algèbre linéaire, en remplaçant $+$ par $\vee$ et $\cdot$ par $\wedge$. Rappelons que le produit de matrices en algèbre linéaire est défini par

$$(M_1 M_2)[i,j] \;=\; (\sum k \mid: M_1[i,k] \cdot M_2[k,j])\ .$$



$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \;\circ\; \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Par exemple, l'entrée $[1, 2]$ vient de $(1 \wedge 0) \vee (1 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 1) = 1$.

Propriétés des relations sous forme matricielle

Les propriétés des relations se transposent aux matrices à partir de leur définition.

Totalité : au moins un 1 par ligne
Déterminisme (fonction) : au plus un 1 par ligne
Surjectivité : au moins un 1 par colonne
Injectivité : au plus un 1 par colonne
Application : exactement un 1 par ligne
Application bijective : exactement un 1 par ligne et par colonne

	$\begin{pmatrix}1&0&0\\0&0&1\\1&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&0\\1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0\\0&1&1\\1&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&1&0\\1&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$
Totalité	×			×	×
Déterminisme		×		×	×
Surjectivité			×		×
Injectivité					×
Application				×	×
Application bijective					×

13.3 Classes de graphes particulières

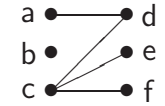
Graphes complets

Un *graphe complet* à n sommets, noté K_n, est un graphe non orienté sans boucle tel qu'il y a une arête entre chaque paire de sommets distincts.

K_1 K_2 K_3 K_4 K_5

Graphes bipartites

Un *graphe bipartite* (ou *biparti*) est un graphe non orienté tel que l'ensemble des sommets peut être partitionné en deux sous-ensembles disjoints X et Y tels que chaque arête du graphe a la forme $\{x, y\}$, avec $x \in X$ et $y \in Y$.



$X = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$
$Y = \{\mathsf{d}, \mathsf{e}, \mathsf{f}\}$

13.4 Isomorphisme

Deux graphes $\langle S, A\rangle$ et $\langle S', A'\rangle$ sont dits *isomorphes* (ce qui signifie *avoir la même forme*) ssi il existe une application bijective $f{:}S \to S'$ telle que

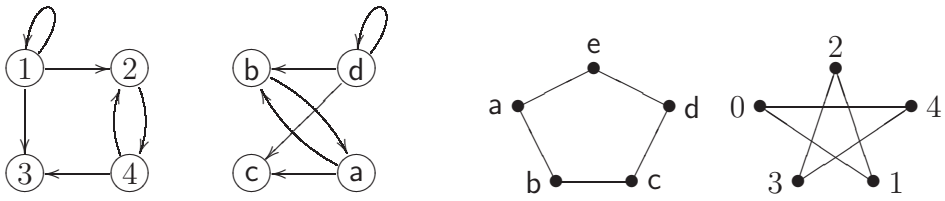
$$(\forall v, w \mid{:}\ \langle v, w\rangle \in A \ \equiv\ \langle f.v, f.w\rangle \in A')$$

dans le cas des graphes orientés, et

$$(\forall v, w \mid{:}\ \{v, w\} \in A \ \equiv\ \{f.v, f.w\} \in A')$$

dans le cas des graphes non orientés.

Par exemple, voici deux paires de graphes isomorphes. L'application bijective qui décrit l'isomorphisme est aussi donnée.



Bijection : $\{\langle 1, \mathsf{d}\rangle, \langle 2, \mathsf{b}\rangle, \langle 3, \mathsf{c}\rangle, \langle 4, \mathsf{a}\rangle\}$ $\{\langle \mathsf{a}, 0\rangle, \langle \mathsf{b}, 1\rangle, \langle \mathsf{c}, 2\rangle, \langle \mathsf{d}, 3\rangle, \langle \mathsf{e}, 4\rangle\}$

Tous les algorithmes connus pour déterminer si deux graphes donnés sont isomorphes prennent un temps exponentiel dans le nombre des sommets et sont donc inefficaces pour de grands graphes.

13.5 Circuits Hamiltoniens

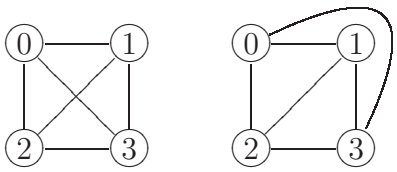
Un *chemin Hamiltonien* est un chemin qui contient chaque sommet exactement une fois, sauf que le premier et le dernier sommet peuvent être identiques. Un *circuit Hamiltonien* est un chemin Hamiltonien qui est un cycle.

Le graphe de gauche ci-dessous n'a pas de circuit Hamiltonien, mais contient le chemin Hamiltonien $\langle 1, 2, 4, 3\rangle$. Le graphe de droite contient les circuits Hamiltoniens $\langle 0, 1, 2, 3, 4, 0\rangle$ et $\langle 0, 1, 2, 4, 3, 0\rangle$.

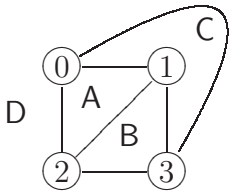
Tous les algorithmes connus pour déterminer si deux graphes donnés contiennent des chemins ou des circuits Hamiltoniens prennent un temps exponentiel dans le nombre des sommets et sont donc inefficaces pour de grands graphes.

13.6 Graphes planaires

Un graphe est dit *planaire* s'il peut être dessiné dans le plan sans croisement d'arcs ou d'arêtes. Par exemple, le graphe complet K_4 peut être dessiné des deux manières données ci-contre. Comme le graphe de droite ne contient pas de croisement, K_4 est planaire.



Un graphe planaire divise le plan en régions *internes* et une région *externe*. Dans le graphe ci-contre, les régions internes sont A, B, C et la région externe est D.



(13.4) Théorème : Pour tout graphe planaire connexe avec s sommets, a arêtes et r régions,

$$r = a - s + 2 \ .$$

Par exemple, pour le graphe ci-dessus, $r = 4$, $a = 6$ et $s = 4$.

Coloriage de cartes ou de graphes planaires

Étant donnée une carte, combien faut-il de couleurs pour colorier les pays de sorte que deux pays adjacents aient des couleurs différentes ?

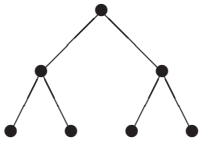
Étant donné un graphe planaire, combien faut-il de couleurs pour colorier les régions du graphe de sorte que deux régions adjacentes aient des couleurs différentes ?

Pendant 100 ans, les mathématiciens ont travaillé sur cette question. La conjecture était que quatre couleurs suffisent. Ce n'est que récemment, en 1977, que Appel et Haken ont montré qu'en effet, quatre couleurs suffisent. La preuve a été complétée en faisant appel aux ordinateurs pour examiner les nombreux cas possibles.

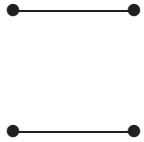
Ces preuves par ordinateur, très longues et difficilement vérifiables par les humains, soulèvent des controverses. La raison principale : le programme utilisé et les logiciels sous-jacents (comme le système d'exploitation) sont-ils corrects ?

13.7 Arbres

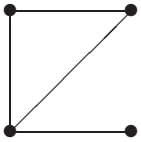
Un *arbre* (*non orienté*) est un graphe non orienté connexe sans boucle et sans cycle.



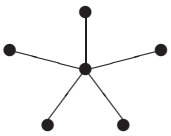
Arbre



Non-arbre
(non connexe)



Non-arbre
(cycle)



Arbre

On peut aussi définir la notion d'arbre orienté, mais nous ne le ferons pas.

Propriétés des arbres

(13.5) Théorème : Entre deux sommets quelconques d'un arbre, il y a un chemin simple unique.

(13.6) Théorème : Un arbre avec au moins deux sommets a au moins deux sommets de degré 1.

(13.7) Théorème : Pour tout arbre $\langle S, A\rangle$, $\#S = 1 + \#A$.

(13.8) Théorème : Soit $G = \langle S, A\rangle$ un graphe non orienté sans boucle. Les énoncés suivants sont équivalents :

(a) G est un arbre.

(b) G est connexe et l'enlèvement d'une arête quelconque produit deux arbres.

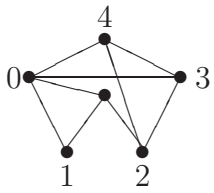
(c) G n'a pas de cycle et $\#S = 1 + \#A$.

(d) G est connexe et $\#S = 1 + \#A$.

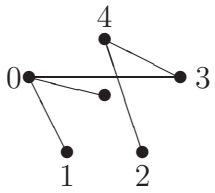
(e) G n'a pas de cycle et l'ajout d'une arête introduit exactement un cycle.

Arbres générateurs

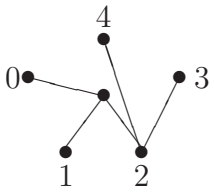
Un *arbre générateur* d'un graphe non orienté G est un sous-graphe de G qui est un arbre et qui contient tous les sommets de G.



G



Arbre générateur 1

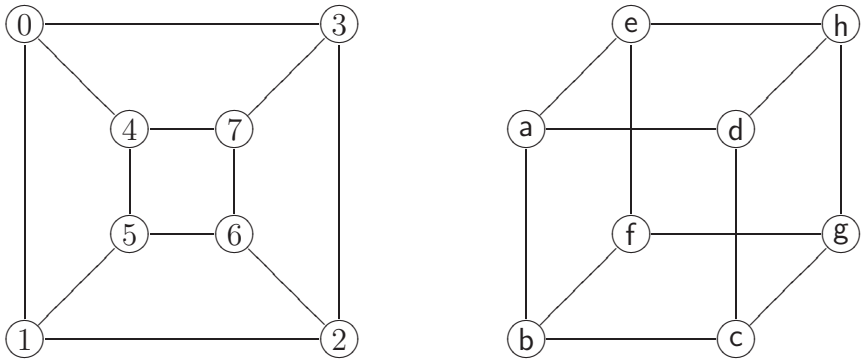


Arbre générateur 2

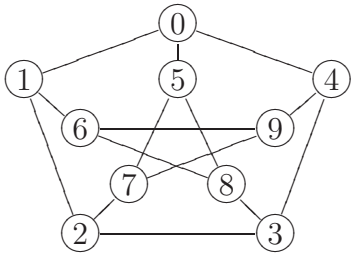
Il y a plusieurs autres arbres générateurs pour ce graphe.

13.8 Problèmes

1. Démontrez le corollaire (13.2), qui énonce qu'il y a un nombre pair de sommets de degré impair dans n'importe quel graphe.
2. Démontrez par induction que le graphe complet K_n a $n \cdot (n-1)/2$ arêtes.
3. Montrez que les deux graphes suivants sont isomorphes.



4. Trouvez un chemin Hamiltonien dans le graphe suivant.



5. Prouvez ou trouvez un contre-exemple : si un graphe $G = \langle S, A\rangle$ n'a pas de boucle et si $\#S = 1 + \#A$, alors G est un arbre.
6. Voici deux relations sur l'ensemble $S = \{1, 2, 3, 4\}$:

$$\begin{aligned} \rho_1 &= \{\langle 2,3\rangle, \langle 3,3\rangle, \langle 4,3\rangle\} \\ \rho_2 &= \{\langle 1,2\rangle, \langle 2,4\rangle, \langle 3,1\rangle, \langle 4,3\rangle\} \end{aligned}$$

   (a) Calculez $\rho_1 \cup \rho_2$, $\rho_1 \cap \rho_2$, $\sim\rho_1$, ρ_2^{-1}, $\rho_1 \circ \rho_2$, ρ_1^2, ρ_2^2, ρ_1^*, ρ_2^+.

   (b) Donnez la représentation graphique des graphes $\langle S, \rho_1\rangle$, $\langle S, \rho_2\rangle$, $\langle S, \rho_2^2\rangle$.

   (c) Donnez les matrices des relations ρ_1, ρ_2, ρ_2^*.

   (d) Dites lesquelles des propriétés suivantes les relations ρ_1, ρ_2, ρ_2^* possèdent : réflexivité, irréflexivité, symétrie, antisymétrie, asymétrie, transitivité, équivalence, totalité, surjectivité, déterminisme, injectivité, fonction, application, application bijective, ordre partiel, ordre partiel strict, ordre total.

7. Calculez le produit suivant :

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Chapitre 14

Solution des problèmes

14.1 Problèmes du chapitre 1

1. Effectuez les substitutions textuelles suivantes, puis supprimez les parenthèses superflues :
   (a) $(a + b \cdot 3)[b, a := a \cdot b, a \cdot a]$
   (b) $((x + y) \cdot z)[x, y := x, y]$
   (c) $(x + x \cdot 2)[x, y := x, z][x := y]$
   (d) $(x + x \cdot y + x \cdot y \cdot z)[x, y := y, x][y := 2 \cdot y]$

   Solution.

   (a)
   $$\begin{aligned} & (a + b \cdot 3)[b, a := a \cdot b, a \cdot a] \\ = & \quad \langle \text{ Substitution } \rangle \\ & ((a \cdot a) + (a \cdot b) \cdot 3) \\ = & \quad \langle \text{ Suppression des parenthèses inutiles } \rangle \\ & a \cdot a + a \cdot b \cdot 3 \end{aligned}$$

   (b)
   $$\begin{aligned} & ((x + y) \cdot z)[x, y := x, y] \\ = & \quad \langle \text{ Substitution } \rangle \\ & (((x) + (y)) \cdot z) \\ = & \quad \langle \text{ Suppression des parenthèses inutiles } \rangle \\ & (x + y) \cdot z \end{aligned}$$

   (c)
   $$\begin{aligned} & (x + x \cdot 2)[x, y := x, z][x := y] \\ = & \quad \langle \text{ La substitution textuelle est associative à gauche } \rangle \\ & \big((x + x \cdot 2)[x, y := x, z]\big)[x := y] \end{aligned}$$

$$
\begin{array}{ll}
= & \langle \text{ Susbtitution } \rangle \\
& \big((x) + (x) \cdot 2\big)[x := y] \\
= & \langle \text{ Susbtitution } \rangle \\
& \Big(\big((y)\big) + \big((y)\big) \cdot 2\Big) \\
= & \langle \text{ Suppression des parenthèses inutiles } \rangle \\
& y + y \cdot 2
\end{array}
$$

Voici une autre solution :

$$
\begin{array}{ll}
& (x + x \cdot 2)[x, y := x, z][x := y] \\
= & \langle \text{ La substitution textuelle est associative à gauche } \rangle \\
& \big((x + x \cdot 2)[x, y := x, z]\big)[x := y] \\
= & \langle \text{ Susbtitution } \rangle \\
& \big((x) + (x) \cdot 2\big)[x := y] \\
= & \langle \text{ Suppression des parenthèses inutiles } \rangle \\
& (x + x \cdot 2)[x := y] \\
= & \langle \text{ Susbtitution } \rangle \\
& \big((y) + (y) \cdot 2\big) \\
= & \langle \text{ Suppression des parenthèses inutiles } \rangle \\
& y + y \cdot 2
\end{array}
$$

(d)

$$
\begin{array}{ll}
& (x + x \cdot y + x \cdot y \cdot z)[x, y := y, x][y := 2 \cdot y] \\
= & \langle \text{ La substitution textuelle est associative à gauche } \rangle \\
& \big((x + x \cdot y + x \cdot y \cdot z)[x, y := y, x]\big)[y := 2 \cdot y] \\
= & \langle \text{ Substitution } \rangle \\
& \big((y) + (y) \cdot (x) + (y) \cdot (x) \cdot z\big)[y := 2 \cdot y] \\
= & \langle \text{ Substitution } \rangle \\
& \Big(\big((2 \cdot y)\big) + \big((2 \cdot y)\big) \cdot (x) + \big((2 \cdot y)\big) \cdot (x) \cdot z\Big) \\
= & \langle \text{ Suppression des parenthèses inutiles } \rangle \\
& 2 \cdot y + 2 \cdot y \cdot x + 2 \cdot y \cdot x \cdot z
\end{array}
$$

2. La règle d'inférence de Leibniz (1.13) donne lieu à une infinité de règles d'inférence particulières obtenues en assignant une expression à ses trois paramètres E, X et Y. ll y a ci-dessous des cas particuliers de la règle de Leibniz, avec une partie manquante. Trouvez la partie manquante et donnez l'expression E correspondante. Donnez toutes les réponses possibles.

(a) $\dfrac{x = x + 2}{4 \cdot x + y = ?}$

(b) $\dfrac{a = b + 2}{? = 3 \cdot (b + 2) + 3 \cdot b + 1}$

Solution.

(a) **Solution 1 :** $\dfrac{x = x + 2}{4 \cdot x + y = 4 \cdot (x + 2) + y}$; $E = 4 \cdot z + y$

Solution 2 : $\dfrac{x = x + 2}{4 \cdot x + y = 4 \cdot x + y}$; $E = 4 \cdot x + y$

(b) **Solution 1 :** $\dfrac{a = b + 2}{3 \cdot a + 3 \cdot b + 1 = 3 \cdot (b + 2) + 3 \cdot b + 1}$; $E = 3 \cdot z + 3 \cdot b + 1$

Solution 2 : $\dfrac{a = b + 2}{3 \cdot (b + 2) + 3 \cdot b + 1 = 3 \cdot (b + 2) + 3 \cdot b + 1}$; $E = 3 \cdot (b+2) + 3 \cdot b + 1$

3. Cet exercice porte sur la règle de Leibniz (1.13). On vous donne l'expression $E[z := X]$ ainsi que l'indice $X = Y$. Trouvez l'expression résultante $E[z := Y]$.

	$E[z := X]$	$X = Y$
(a)	$(x + y) \cdot w$	$w = x \cdot y$
(b)	$p \cap q$	$q = q \cup r$

Solution.

(a) **Solution 1 :** Il s'agit de résoudre $\dfrac{w = x \cdot y}{(x + y) \cdot w = ?}$. Nous pouvons déduire $E = (x+y) \cdot z$ en remplaçant X (c'est-à-dire w) par z. Pour connaître $E[z := Y]$, nous n'avons qu'à effectuer la substitution (l'expression Y est connue, c'est $x \cdot y$).

$$
\begin{array}{ll}
 & E[z := Y] \\
= & \qquad \langle\ E = (x + y) \cdot z,\ Y = x \cdot y\ \rangle \\
 & \big((x + y) \cdot z\big)[z := x \cdot y] \\
= & \qquad \langle\ \text{Substitution}\ \rangle \\
 & \big((x + y) \cdot (x \cdot y)\big) \\
= & \qquad \langle\ \text{Suppression des parenthèse inutiles}\ \rangle \\
 & (x + y) \cdot x \cdot y
\end{array}
$$

Solution 2 : En prenant $E = (x+y) \cdot w$, nous obtenons $E[z := Y] = (x+y) \cdot w$.

(b) **Solution 1 :** En prenant $E = p \cap z$, nous obtenons $E[z := Y] = p \cap (q \cup r)$. Il ne faut pas supprimer les parenthèses, car $\cap$ et $\cup$ ont la même préséance. L'expression sans parenthèses serait donc ambigüe.

Solution 2 : En prenant $E = p \cap q$, nous obtenons $E[z := Y] = p \cap q$.

4. Cet exercice porte sur la règle de Leibniz (1.13). Pour chacune des paires d'expressions $E[z := X]$ et $E[z := Y]$ ci-dessous, donnez les expressions X et Y telles que $E[z := X] = E[z := Y]$. Indiquez ensuite quelle est l'expression E. Donnez toutes les réponses possibles.

	$E[z := X]$	$E[z := Y]$
(a)	$x \cdot y \cdot x$	$y \cdot x \cdot x$
(b)	$p \Rightarrow q \wedge (r \vee p)$	$p \Rightarrow q \wedge q$

Solution.

(a) Il s'agit de résoudre : $\dfrac{?}{x \cdot y \cdot x = y \cdot x \cdot x}$.

	X	Y	Z
Solution 1	$x \cdot y$	$y \cdot x$	$z \cdot x$
Solution 2	$x \cdot y \cdot x$	$y \cdot x \cdot x$	z

(b)

	X	Y	Z
Solution 1	$r \vee p$	q	$p \Rightarrow q \wedge z$
Solution 2	$p \Rightarrow q \wedge (r \vee p)$	$p \Rightarrow q \wedge q$	z
Solution 3	$q \wedge (r \vee p)$	$q \wedge q$	$p \Rightarrow z$

5. Utilisez la table de préséance suivante pour faire les substitutions demandées. À l'exception de la substitution, tous les opérateurs sont des opérateurs binaires. La priorité 1 est la plus élevée et 7 la plus faible.

Priorité	Opérateur
1	$[x := e]$ (Substitution)
2	$\top \parallel$
3	$\heartsuit$
4	$\diamondsuit$
5	$\clubsuit$
6	$\spadesuit$
7	$\star \dagger \triangle$

(a) $((x \top y) \| z \diamondsuit x)[x := y \heartsuit x]$

(b) $((x \heartsuit y) \top (z \star x \heartsuit y) \star x)[x := z \diamondsuit z]$

(c) $(x \heartsuit y \spadesuit x \star z \diamondsuit x \heartsuit y)[x, y := x \top y, y \triangle x]$

(d) $((x \star y) \dagger x)[x, y := x \diamondsuit x, x \triangle x]$

(e) $(x \top x \triangle x)[x, y := y, z]$

(f) $(x \top x \triangle x)[x := y][y := z]$

(g) $((x \star y) \dagger x)[x := x \diamondsuit x][y := x \triangle x]$

(h) $(x \heartsuit y \spadesuit x \star z \diamondsuit x \heartsuit y)[x := x \top y][y := y \triangle x]$

Solution.

(a) $((x \top y) \| z \diamondsuit x)[x := y \heartsuit x]$

$=$ ⟨ Substitution ⟩

$(((y \heartsuit x) \top y) \| z \diamondsuit (y \heartsuit x))$

$=$ ⟨ Suppression des parenthèses inutiles ⟩

$((y \heartsuit x) \top y) \| z \diamondsuit y \heartsuit x$

(b) $((x \heartsuit y) \top (z \star x \heartsuit y) \star x)[x := z \diamondsuit z]$

$=$ ⟨ Substitution ⟩

$(((z \diamondsuit z) \heartsuit y) \top (z \star (z \diamondsuit z) \heartsuit y) \star (z \diamondsuit z))$

$=$ ⟨ Suppression des parenthèses inutiles ⟩

$((z \diamondsuit z) \heartsuit y) \top (z \star (z \diamondsuit z) \heartsuit y) \star z \diamondsuit z$

(c) $(x \heartsuit y \spadesuit x \star z \diamondsuit x \heartsuit y)[x, y := x \top y, y \triangle x]$

$=$ ⟨ Substitution ⟩

$((x \top y) \heartsuit (y \triangle x) \spadesuit (x \top y) \star z \diamondsuit (x \top y) \heartsuit (y \triangle x))$

$=$ ⟨ Suppression des parenthèses inutiles ⟩

$x \top y \heartsuit (y \triangle x) \spadesuit x \top y \star z \diamondsuit x \top y \heartsuit (y \triangle x)$

(d) $((x \star y) \dagger x)[x, y := x \diamondsuit x, x \triangle x]$

$=$ ⟨ Substitution ⟩

$(((x \diamondsuit x) \star (x \triangle x)) \dagger (x \diamondsuit x))$

$=$ ⟨ Suppression des parenthèses inutiles ⟩

$(x \diamondsuit x \star (x \triangle x)) \dagger x \diamondsuit x$

(e) $(x \top x \triangle x)[x, y := y, z]$

$=$ ⟨ Substitution ⟩

$((y) \top (y) \triangle (y))$

$=$ ⟨ Suppression des parenthèses inutiles ⟩

$y \top y \triangle y$

(f) $(x \top x \triangle x)[x := y][y := z]$

$=$ ⟨ Substitution ⟩

$((y) \top (y) \triangle (y))[y := z]$

$=$ ⟨ Substitution ⟩

$(((z)) \top ((z)) \triangle ((z)))$

⟨ Suppression des parenthèses inutiles ⟩

$$z \top z \triangle z$$

(g) $((x \star y) \dagger x)[x := x \diamondsuit x][y := x \triangle x]$

$=$ $\langle$ Substitution $\rangle$

$(((x \diamondsuit x) \star y) \dagger (x \diamondsuit x))[y := x \triangle x]$

$=$ $\langle$ Substitution $\rangle$

$(((x \diamondsuit x) \star (x \triangle x)) \dagger (x \diamondsuit x))$

$\langle$ Suppression des parenthèses inutiles $\rangle$

$(x \diamondsuit x \star (x \triangle x)) \dagger x \diamondsuit x$

(h) $(x \heartsuit y \spadesuit x \star z \diamondsuit x \heartsuit y)[x := x \top y][y := y \triangle x]$

$=$ $\langle$ Substitution $\rangle$

$((x \top y) \heartsuit y \spadesuit (x \top y) \star z \diamondsuit (x \top y) \heartsuit y)[y := y \triangle x]$

$=$ $\langle$ Substitution $\rangle$

$((x \top (y \triangle x)) \heartsuit (y \triangle x) \spadesuit (x \top (y \triangle x)) \star z \diamondsuit (x \top (y \triangle x)) \heartsuit (y \triangle x))$

$\langle$ Suppression des parenthèses inutiles $\rangle$

$x \top (y \triangle x) \heartsuit (y \triangle x) \spadesuit x \top (y \triangle x) \star z \diamondsuit x \top (y \triangle x) \heartsuit (y \triangle x)$

6. Nous aimerions que les expressions $X = X$ et $(X = Y) = (Y = X)$ soient des théorèmes, où X et Y sont des expressions quelconques. Cependant les axiomes (1.10) et (1.11) sont restreints au cas où X et Y sont des variables (x et y). Perd-on de la généralité avec (1.10) et (1.11) ?

Solution. On ne perd pas de généralité, car on peut démontrer

$$X = X \quad \text{et} \quad (X = Y) = (Y = X)$$

en utilisant la règle de substitution (1.9) et les axiomes (1.10) et (1.11). Considérons les instances suivantes de la règle de substitution :

$$\frac{x = x}{(x = x)[x := X]} \qquad \frac{(x = y) = (y = x)}{\big((x = y) = (y = x)\big)[x, y := X, Y]}$$

Après avoir fait les substitutions, nous obtenons

$$\frac{x = x}{X = X} \qquad \frac{(x = y) = (y = x)}{(X = Y) = (Y = X)}$$

Puisque $x = x$ et $(x = y) = (y = x)$ sont des théorèmes (axiomes (1.10) et (1.11)), $X = X$ et $(X = Y) = (Y = X)$ en sont aussi, par la règle de substitution.

7. La loi de Leibniz dit que deux expressions sont égales si et seulement si le remplacement de l'une par l'autre dans n'importe quelle expression E ne change pas la valeur de E. Cette loi peut être décomposée en deux parties (les symboles X et Y sont ajoutés pour que le passage à la règle (1.13) soit plus clair) :
   – Si deux expressions X et Y sont égales, alors le remplacement de l'une par l'autre dans n'importe quelle expression E ne change pas la valeur de E.
   – Si, quelle que soit l'expression E, le remplacement d'une expression X par une expression Y dans E ne change pas la valeur de E, alors X et Y sont égales.

   La règle (1.13) correspond à la première partie. En effet, la règle (1.13) dit que si $X = Y$, alors $E[z := X] = E[z := Y]$. Démontrez la deuxième partie. Plus précisément, montrez que si $E[z := X] = E[z := Y]$ est un théorème pour toute expression E, alors $X = Y$.

   Solution. Supposons que $E[z := X] = E[z := Y]$ soit un théorème pour toute expression E. En considérant le cas particulier où E est l'expression z, on obtient $z[z := X] = z[z := Y]$, c'est-à-dire, en faisant la substitution, $X = Y$.

14.2 Problèmes du chapitre 2

1. Évaluez les expressions dans les deux états E_0 et E_1 donnés.

		État E_0				État E_1			
	expression	m	n	p	q	m	n	p	q
(a)	$\neg m \wedge n$	v	f	v	v	f	v	v	v
(b)	$(m \equiv n \wedge p) \Rightarrow q$	f	v	f	v	v	v	f	f

   Solution. Évaluons les expressions en respectant la préséance des opérateurs (la sous-expression à évaluer est soulignée). La table des opérateurs booléens est utilisée pour évaluer les sous-expressions.

(a)

État E_0

$$
\begin{array}{ll}
 & \neg m \wedge n \\
= & \quad \langle \text{ Définition de } E_0 \rangle \\
 & \underline{\neg \mathsf{vrai}} \wedge \mathsf{faux} \\
= & \quad \langle \neg \mathsf{vrai} \equiv \mathsf{faux} \rangle \\
 & \underline{\mathsf{faux} \wedge \mathsf{faux}} \\
= & \quad \langle (\mathsf{faux} \wedge \mathsf{faux}) \equiv \mathsf{faux} \rangle \\
 & \mathsf{faux}
\end{array}
$$

État E_1

$$
\begin{array}{ll}
 & \neg m \wedge n \\
= & \quad \langle \text{ Définition de } E_1 \rangle \\
 & \underline{\neg \mathsf{faux}} \wedge \mathsf{vrai} \\
= & \quad \langle \neg \mathsf{faux} \equiv \mathsf{vrai} \rangle \\
 & \underline{\mathsf{vrai} \wedge \mathsf{vrai}} \\
= & \quad \langle (\mathsf{vrai} \wedge \mathsf{vrai}) \equiv \mathsf{vrai} \rangle \\
 & \mathsf{vrai}
\end{array}
$$

   Dans le cas de l'état E_0, il est possible de donner immédiatement la réponse sans faire toute l'évaluation. Puisque l'opérande droit de la conjonction (n) a la valeur

faux, l'expression a la valeur faux. En effet, une conjonction vaut vrai seulement si ses deux opérandes sont vrai.

(b)

État E_0

$$
\begin{array}{ll}
 & (m \equiv n \wedge p) \Rightarrow q \\
= & \quad \langle \text{ Définition de } E_0 \rangle \\
 & (\mathsf{faux} \equiv \underline{\mathsf{vrai} \wedge \mathsf{faux}}) \Rightarrow \mathsf{vrai} \\
= & \quad \langle \ \mathsf{vrai} \wedge \mathsf{faux} \equiv \mathsf{faux} \ \rangle \\
 & (\underline{\mathsf{faux} \equiv \mathsf{faux}}) \Rightarrow \mathsf{vrai} \\
= & \quad \langle \ (\mathsf{faux} \equiv \mathsf{faux}) \equiv \mathsf{vrai} \ \rangle \\
 & \underline{\mathsf{vrai} \Rightarrow \mathsf{vrai}} \\
= & \quad \langle \ \mathsf{vrai} \Rightarrow \mathsf{vrai} \equiv \mathsf{vrai} \ \rangle \\
 & \mathsf{vrai}
\end{array}
$$

État E_1

$$
\begin{array}{ll}
 & (m \equiv n \wedge p) \Rightarrow q \\
= & \quad \langle \text{ Définition de } E_1 \rangle \\
 & (\mathsf{vrai} \equiv \underline{\mathsf{vrai} \wedge \mathsf{faux}}) \Rightarrow \mathsf{faux} \\
= & \quad \langle \ \mathsf{vrai} \wedge \mathsf{faux} \equiv \mathsf{faux} \ \rangle \\
 & (\underline{\mathsf{vrai} \equiv \mathsf{faux}}) \Rightarrow \mathsf{faux} \\
= & \quad \langle \ (\mathsf{vrai} \equiv \mathsf{faux}) \equiv \mathsf{faux} \ \rangle \\
 & \underline{\mathsf{faux} \Rightarrow \mathsf{faux}} \\
= & \quad \langle \ \mathsf{faux} \Rightarrow \mathsf{faux} \equiv \mathsf{vrai} \ \rangle \\
 & \mathsf{vrai}
\end{array}
$$

Dans le cas de l'état E_0, il est possible de donner immédiatement la réponse sans faire toute l'évaluation. Puisque $q \equiv \mathsf{vrai}$, l'expression a la valeur vrai. En effet, lorsque l'opérande droit d'une implication est vrai, l'implication vaut vrai.

2. Construisez la table de vérité de chacune des expressions suivantes afin de déterminer sa valeur dans tous les états. Dites si l'expression est satisfiable et si elle est valide.
   (a) $(\neg b \equiv c) \vee b$
   (b) $(p \equiv q) \ \equiv \ (p \wedge q) \ \vee \ (\neg p \wedge \neg q)$

Solution.

(a)

b	c	$\neg b$	$\neg b \equiv c$	$(\neg b \equiv c) \vee b$
v	v	f	f	v
v	f	f	v	v
f	v	v	v	v
f	f	v	f	f

L'expression est satisfiable, mais elle n'est pas valide.

(b)

p	q	$p \equiv q$	$p \wedge q$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$	$(p \equiv q) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
v	v	v	v	f	f	f	v	v
v	f	f	f	f	v	f	f	v
f	v	f	f	v	f	f	f	v
f	f	v	f	v	v	v	v	v

L'expression est valide et donc satisfiable.

3. Traduisez les phrases suivantes en expressions booléennes.
   (a) Exactement l'une de p et q a la valeur vrai.
   (b) Aucune, deux ou quatre des variables p, q, r et s ont la valeur vrai.

Solution.

(a) La proposition $p \wedge \neg q$ a la valeur vrai lorsque p a la valeur vrai et q la valeur faux ; elle exprime donc que seule p a la valeur vrai. De même, la proposition $\neg p \wedge q$ exprime que seule q a la valeur vrai. La proposition

$$(p \wedge \neg q) \vee (\neg p \wedge q)$$

est donc la solution demandée. Veuillez noter que les parenthèses sont nécessaires. Sans elles, l'expression est ambigüe (elle pourrait avoir une valeur différente si les parenthèses étaient placées différemment).

(b) Il faut d'abord comprendre de cet énoncé qu'il est vrai si *exactement* zéro, deux ou quatre des variables p, q, r et s ont la valeur vrai.

i. Méthode directe et simple : Considérons les propositions suivantes et leur interprétation (ce qu'elles signifient lorsqu'elles ont la valeur vrai) :

$p \wedge q \wedge r \wedge s$	les quatres variables ont la valeur vrai
$p \wedge q \wedge \neg r \wedge \neg s$	p et q ont la valeur vrai, les autres ont la valeur faux
$p \wedge \neg q \wedge r \wedge \neg s$	p et r ont la valeur vrai, les autres ont la valeur faux
$p \wedge \neg q \wedge \neg r \wedge s$	p et s ont la valeur vrai, les autres ont la valeur faux
$\neg p \wedge q \wedge r \wedge \neg s$	q et r ont la valeur vrai, les autres ont la valeur faux
$\neg p \wedge q \wedge \neg r \wedge s$	q et s ont la valeur vrai, les autres ont la valeur faux
$\neg p \wedge \neg q \wedge r \wedge s$	r et s ont la valeur vrai, les autres ont la valeur faux
$\neg p \wedge \neg q \wedge \neg r \wedge \neg s$	les quatre variables ont la valeur faux

La réponse est la disjonction de ces huit cas :

$$(p \wedge q \wedge r \wedge s) \vee (p \wedge q \wedge \neg r \wedge \neg s) \vee (p \wedge \neg q \wedge r \wedge \neg s) \vee (p \wedge \neg q \wedge \neg r \wedge s) \vee (\neg p \wedge q \wedge r \wedge \neg s) \vee (\neg p \wedge q \wedge \neg r \wedge s) \vee (\neg p \wedge \neg q \wedge r \wedge s) \vee (\neg p \wedge \neg q \wedge \neg r \wedge \neg s)$$

En faisant la table de vérité, on peut vérifier que cette expression a la valeur vrai exactement lorsqu'aucune, deux ou quatre des variables p, q, r et s ont la valeur vrai.

ii. Méthode élégante : Nous verrons au chapitre 3 que l'expression suivante est aussi une solution :

$$p \equiv q \equiv r \equiv s \ .$$

Ceci illustre bien que l'approche directe et intuitive (la première réponse) ne donne pas toujours de très bons résultats, dans le sens qu'elle produit une expression beaucoup plus longue.

4. Nommez les proposition primitives (comme $x < y$ et $x = y$) dans les phrases suivantes et traduisez ces phrases en expressions booléennes.
   (a) Aucune des expressions suivantes n'est vraie : $x < y$, $y < z$ et $v = w$.
   (b) Quand $x < y$, alors $y < z$; quand $x \geq y$, alors $v = w$.
   (c) Si l'exécution du programme P débute avec $x < y$, alors l'exécution se termine avec $y = 2^x$.

   Solution. Assignons les noms suivants aux propositions primitives :

   xpy : $x < y$
   ypz : $y < z$
   vew : $v = w$
   dp : l'exécution du programme P débute avec $x < y$
   te : l'exécution se termine avec $y = 2^x$

   (f) $\neg xpy \wedge \neg ypz \wedge \neg vew$ ou encore $\neg(xpy \vee ypz \vee vew)$.

   (h) $(xpy \Rightarrow ypz) \wedge (\neg xpy \Rightarrow vew)$.
   Nous avons tenu compte du fait que la négation de $x < y$ est $x \geq y$ (du moins pour les entiers et les réels). Il est aussi possible d'introduire un nouveau nom pour la proposition $x \geq y$.

   (j) $dp \Rightarrow te$.

14.3 Problèmes du chapitre 3

1. Dites quelle règle de substitution et quelle règle de Leibniz sont utilisées dans les transformations suivantes (autrement dit, précisez les valeurs de E, F, X, Y, v, z utilisées dans (1.9) et (1.13)). Après avoir donné les règles, effectuez les substitutions qu'elles contiennent.

   (a) $\neg p \equiv p \equiv \mathsf{faux}$
   $=$ $\langle$ Commutativité de $\equiv$ (3.3), avec $p, q := \mathsf{faux}, p$ $\rangle$
   $\neg p \equiv \mathsf{faux} \equiv p$

   (b) $\neg p \equiv \mathsf{faux} \equiv p$
   $=$ $\langle$ (3.14), avec $q := \mathsf{faux}$ $\rangle$
   $\neg\mathsf{faux}$

   (c) $\neg\mathsf{faux}$
   $=$ $\langle$ Négation de faux (3.16) $\rangle$
   vrai

Solution.

(a) i. Règle de substitution

$$\frac{p \equiv q \equiv q \equiv p}{(p \equiv q \equiv q \equiv p)[p, q := \mathsf{faux}, p]}$$

Une fois la substitution faite, on obtient

$$\frac{p \equiv q \equiv q \equiv p}{\mathsf{faux} \equiv p \equiv p \equiv \mathsf{faux}}\ .$$

ii. Règle de Leibniz

$$\frac{(\mathsf{faux} \equiv p) \ = \ (p \equiv \mathsf{faux})}{(\neg p \equiv z)[z := \mathsf{faux} \equiv p] \ = \ (\neg p \equiv z)[z := p \equiv \mathsf{faux}]}$$

Une fois les substitutions faites, on obtient

$$\frac{(\mathsf{faux} \equiv p) \ = \ (p \equiv \mathsf{faux})}{(\neg p \equiv \mathsf{faux} \equiv p) \ = \ (\neg p \equiv p \equiv \mathsf{faux})}\ .$$

Remarquez l'introduction des parenthèses, qui sont nécessaires à cause de la préséance de $=$ sur $\equiv$.

(b) i. Règle de substitution

$$\frac{\neg p \equiv q \ \equiv \ p \equiv \neg q}{(\neg p \equiv q \ \equiv \ p \equiv \neg q)[q := \mathsf{faux}]}$$

Une fois la substitution faite, on obtient

$$\frac{\neg p \equiv q \ \equiv \ p \equiv \neg q}{\neg p \equiv \mathsf{faux} \ \equiv \ p \equiv \neg \mathsf{faux}}\ .$$

ii. Règle de Leibniz : il n'est pas nécessaire d'utiliser la règle de Leibniz, car la conclusion de la règle de substitution donne directement la transformation à appliquer. Toutefois, il est quand même possible d'utiliser la règle suivante (si on tient absolument à en utiliser une).

$$\frac{(\neg p \equiv \mathsf{faux} \equiv p) \ = \ \neg \mathsf{faux}}{z[z := \neg p \equiv \mathsf{faux} \equiv p] \ = \ z[z := \neg \mathsf{faux}]}$$

Une fois les substitutions faites, on obtient

$$\frac{(\neg p \equiv \mathsf{faux} \equiv p) \ = \ \neg \mathsf{faux}}{(\neg p \equiv \mathsf{faux} \equiv p) \ = \ \neg \mathsf{faux}}\ .$$

La conclusion est identique à la prémisse, qui est elle-même la conclusion de la règle de substitution. On voit ainsi d'une autre manière qu'il est inutile d'appliquer la règle de Leibniz, car elle ne permet pas de conclure quoi que ce soit de nouveau.

(c) i. Règle de substitution : elle n'est pas utilisée.

ii. Règle de Leibniz : il n'est pas nécessaire d'utiliser la règle de Leibniz, car le théorème (3.16) donne directement la transformation à appliquer. On pourrait bien sûr faire comme à l'item précédent et donner une solution triviale.

2. Démontrez le théorème (3.14) de trois manières différentes : tout d'abord, transformez $\neg p \equiv q \equiv p \equiv \neg q$ en un théorème ; ensuite, transformez $\neg p \equiv p$ en $q \equiv \neg q$; finalement, transformez $\neg p$ en $q \equiv p \equiv \neg q$. Comparez ces trois preuves et celle donnée à la page 32. Laquelle est la plus simple ou la plus courte ?

Solution.

(a) $\neg p \equiv q \equiv p \equiv \neg q$

$=$ $\langle$ Distributivité de $\neg$ sur $\equiv$ (3.12) $\rangle$

$\neg(p \equiv q) \equiv p \equiv \neg q$

$=$ $\langle$ Commutativité de $\equiv$ (3.3) $\rangle$

$\neg(q \equiv p) \equiv p \equiv \neg q$

$=$ $\langle$ Distributivité de $\neg$ sur $\equiv$ (3.12), avec $p, q := q, p$ $\rangle$

$\neg q \equiv p \equiv p \equiv \neg q$ —Commutativité de $\equiv$ (3.3), avec $p, q := \neg q, p$

(b) $\neg p \equiv p$

$=$ $\langle$ Distributivité de $\neg$ sur $\equiv$ (3.12), avec $q := p$ $\rangle$

$\neg(p \equiv p)$

$=$ $\langle$ Commutativité de $\equiv$ (3.3). Notez que c'est un usage assez surprenant de la commutativité. En effet, le théorème (3.3) est utilisé pour se reformuler lui-même comme $p \equiv p \equiv q \equiv q$. $\rangle$

$\neg(q \equiv q)$

$=$ $\langle$ Distributivité de $\neg$ sur $\equiv$ (3.12), avec $p := q$ $\rangle$

$\neg q \equiv q$

$=$ $\langle$ Commutativité de $\equiv$ (3.3), avec $p, q := \neg q, q$ $\rangle$

$q \equiv \neg q$

Ceci est en fait une preuve de $\neg p \equiv p \equiv q \equiv \neg q$, qui est équivalent au théorème à démontrer, par commutativité de $\equiv$.

(c) $\neg p$

$=$ $\langle$ Commutativité de $\equiv$ (3.3) $\rangle$

$\neg(q \equiv q \equiv p)$

$=$ $\langle$ Distributivité de $\neg$ sur $\equiv$ (3.12), avec $p,\ q := q,\ q \equiv p$ $\rangle$

$\neg q \equiv q \equiv p$

$=$ $\langle$ Commutativité de $\equiv$ (3.3), avec $p,\ q := \neg q,\ q \equiv p$ $\rangle$

$q \equiv p \equiv \neg q$

Ces trois preuves ont une complexité similaire. Cependant, la première répète « $\equiv p \equiv \neg q$ » plusieurs fois et elle contient un peu plus de symboles que les autres. La deuxième fait appel à la commutativité de $\equiv$ sans mention. La dernière devrait être présentée dans l'ordre inverse, du plus structuré au plus simple (mais il faut bien respecter l'énoncé). La preuve de la page 32 et la dernière ci-dessus sont préférables et sont aussi les plus faciles à comprendre. Il est plus facile de trouver la preuve de la page 32, ce qui peut sembler être un avantage décisif, mais c'est la facilité de lecture qui compte le plus ; cependant, la preuve de la page 32 l'emporte aussi par cet aspect et c'est donc elle qui est la meilleure.

3. Démontrez le théorème sur la double négation (3.15), $\neg\neg p \equiv p$.

   Solution.

   $$\begin{array}{ll} & \neg\neg p \equiv p \\ = & \quad \langle\ (3.14), \text{ avec } p, q := \neg p, p\ \rangle \\ & \neg p \equiv \neg p \\ = & \quad \langle\ \text{Identité de } \equiv \ (3.4), \text{ avec } p := \neg p\ \rangle \\ & \mathsf{vrai} \end{array}$$

4. Démontrez le théorème (3.17), $(p \not\equiv q) \equiv \neg p \equiv q$.

   Solution.

   $$\begin{array}{ll} & p \not\equiv q \\ = & \quad \langle\ \text{Définition de } \not\equiv \ (3.13)\ \rangle \\ & \neg(p \equiv q) \\ = & \quad \langle\ \text{Distributivité de } \neg \text{ sur } \equiv \ (3.12)\ \rangle \\ & \neg p \equiv q \end{array}$$

5. Démontrez le théorème (3.18) en transformant $\neg p \equiv p \equiv \mathsf{faux}$ en vrai en utilisant le théorème (3.14). La preuve requiert au plus deux utilisations de la règle de Leibniz.

   Solution.

   $$\begin{array}{ll} & \neg p \equiv p \equiv \mathsf{faux} \\ = & \quad \langle\ \text{Commutativité de } \equiv \ (3.3), \text{ avec } q := \mathsf{faux}\ \rangle \\ & \neg p \equiv \mathsf{faux} \equiv p \\ = & \quad \langle\ (3.14), \text{ avec } q := \mathsf{faux}\ \rangle \end{array}$$

$$
\begin{array}{ll}
& \neg\mathsf{faux} \\
= & \quad \langle \text{ Négation de } \mathsf{faux} \ (3.16) \ \rangle \\
& \mathsf{vrai} \qquad \text{—}(3.6)
\end{array}
$$

La règle de Leibniz n'est pas nécessaire pour les deux dernières étapes (voyez la solution du problème 1 de ce chapitre).

6. Utilisez l'heuristique d'élimination des définitions (3.29) pour démontrer le théorème d'interchangeabilité mutuelle (3.22), $p \not\equiv q \equiv r \equiv p \equiv q \not\equiv r$. Éliminez $\not\equiv$, utilisez une propriété de $\equiv$ et réintroduisez $\not\equiv$.

Solution.

(a) Première preuve.

$$
\begin{array}{ll}
& p \not\equiv q \equiv r \\
= & \quad \langle \text{ Définition de } \not\equiv \ (3.13), \text{ avec } q := q \equiv r \ \rangle \\
& \neg(p \equiv q \equiv r) \\
= & \quad \langle \text{ Définition de } \not\equiv \ (3.13), \text{ avec } p, q := p \equiv q, r \ \rangle \\
& p \equiv q \not\equiv r
\end{array}
$$

(b) Voici une deuxième preuve, moins bonne, car elle est plus longue sans être plus claire.

$$
\begin{array}{ll}
& p \not\equiv q \equiv r \\
= & \quad \langle \text{ Définition de } \not\equiv \ (3.13) \ \rangle \\
& \neg(p \equiv q) \equiv r \\
= & \quad \langle \text{ Distributivité de } \neg \text{ sur } \equiv \ (3.12), \text{ avec } p, q := p \equiv q, r \ \rangle \\
& \neg((p \equiv q) \equiv r) \\
= & \quad \langle \text{ Définition de } \not\equiv \ (3.13), \text{ avec } p, q := p \equiv q, r \ \rangle \\
& (p \equiv q) \not\equiv r \\
= & \quad \langle \text{ Commutativité de } \not\equiv \ (3.19), \text{ avec } p, q := p \equiv q, r \ \rangle \\
& r \not\equiv (p \equiv q) \\
= & \quad \langle \text{ L'associativité mutuelle (3.21) permet de supprimer les parenthèses } \rangle \\
& r \not\equiv p \equiv q \\
= & \quad \langle \text{ Commutativité de } \not\equiv \ (3.19), \text{ avec } p, q := r, p \equiv q \ \rangle \\
& p \equiv q \not\equiv r
\end{array}
$$

7. Démontrez la distributivité de $\vee$ sur $\vee$ (3.41), $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$.

Solution.

$$
\begin{array}{ll}
 & (p \vee q) \vee (p \vee r) \\
= & \qquad \langle \text{ L'associativité de } \vee \text{ (3.33) permet de supprimer les parenthèses } \rangle \\
 & (p \vee q) \vee p \vee r \\
= & \qquad \langle \text{ Associativité de } \vee \text{ (3.33) } \rangle \\
 & p \vee (q \vee p) \vee r \\
= & \qquad \langle \text{ Commutativité de } \vee \text{ (3.32) } \rangle \\
 & p \vee (p \vee q) \vee r \\
= & \qquad \langle \text{ Associativité de } \vee \text{ (3.33) } \rangle \\
 & p \vee p \vee (q \vee r) \\
= & \qquad \langle \text{ Idempotence de } \vee \text{ (3.34) } \rangle \\
 & p \vee (q \vee r)
\end{array}
$$

8. La dérivation suivante démontre le théorème (3.20) sur l'associativité de $\not\equiv$. Pour chacune des transformations, donnez les paramètres de la règle de substitution et de la règle de Leibniz qui sont utilisées, c'est-à-dire, donnez les valeurs de E, F, X, Y, v, z qu'il faut employer dans (1.9) et (1.13) (il n'est pas nécessaire de donner les règles elles-mêmes). Les transformations sont numérotées pour pouvoir y référer dans la réponse.

$$
\begin{array}{ll}
 & (p \not\equiv q) \not\equiv r \\
= & \qquad \langle \text{ 1. (3.17) } \rangle \\
 & (\neg p \equiv q) \not\equiv r \\
= & \qquad \langle \text{ 2. Commutativité de } \not\equiv \text{ (3.19), avec } p, q := \neg p \equiv q, r \rangle \\
 & r \not\equiv (\neg p \equiv q) \\
= & \qquad \langle \text{ 3. (3.17), avec } p, q := r, \neg p \equiv q \rangle \\
 & \neg r \equiv (\neg p \equiv q) \\
= & \qquad \langle \text{ 4. Commutativité de } \equiv \text{ (3.3), avec } p, q := \neg r, \neg p \equiv q \rangle \\
 & (\neg p \equiv q) \equiv \neg r \\
= & \qquad \langle \text{ 5. Associativité de } \equiv \text{ (3.2), avec } p, r := \neg p, \neg r \rangle \\
 & \neg p \equiv (q \equiv \neg r) \\
= & \qquad \langle \text{ 6. (3.17), avec } q := q \equiv \neg r \rangle \\
 & p \not\equiv (q \equiv \neg r) \\
= & \qquad \langle \text{ 7. Commutativité de } \equiv \text{ (3.3), avec } p, q := q, \neg r \rangle \\
 & p \not\equiv (\neg r \equiv q) \\
= & \qquad \langle \text{ 8. (3.17), avec } p := r \rangle
\end{array}
$$

$$
\begin{array}{ll}
& p \not\equiv (r \not\equiv q) \\
= & \qquad \langle \text{ 9. Commutativité de } \not\equiv \text{ (3.19), avec } p := r \ \rangle \\
& p \not\equiv (q \not\equiv r)
\end{array}
$$

Solution.

	Substitution			Leibniz		
	E	v	F	E	X	Y
1				$z \not\equiv r$	$p \not\equiv q$	$\neg p \equiv q$
2	$(p \not\equiv q) \equiv (q \not\equiv p)$	p, q	$\neg p \equiv q,\ r$			
3	$(p \not\equiv q) \equiv \neg p \equiv q$	p, q	$r,\ \neg p \equiv q$			
4	$p \equiv q \equiv q \equiv p$	p, q	$\neg r,\ \neg p \equiv q$			
5	$((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$	p, r	$\neg p,\ \neg r$			
6	$(p \not\equiv q) \equiv \neg p \equiv q$	q	$q \equiv \neg r$			
7	$p \equiv q \equiv q \equiv p$	p, q	$q, \neg r$	$p \not\equiv z$	$q \equiv \neg r$	$\neg r \equiv q$
8	$(p \not\equiv q) \equiv \neg p \equiv q$	p	r	$p \not\equiv z$	$\neg r \equiv q$	$r \not\equiv q$
9	$(p \not\equiv q) \equiv (q \not\equiv p)$	p	r	$p \not\equiv z$	$r \not\equiv q$	$q \not\equiv r$

9. Démontrez le théorème d'absorption (3.61d), $p \vee (\neg p \wedge q) \equiv p \vee q$.

Solution. Remarquez comment les propriétés de commutativité sont mentionnées —ce qui aide à comprendre la preuve— sans en faire des transformations séparées.
Voici trois preuves différentes. J'ai une légère préférence pour la première (plus courte, plus facile à comprendre, mais pas nécessairement plus facile à trouver).

(a)
$$
\begin{array}{ll}
& p \vee (\neg p \wedge q) \\
= & \qquad \langle \text{ Règle d'or (3.57), avec } p := \neg p \ \rangle \\
& p \vee (\neg p \equiv q \equiv \neg p \vee q) \\
= & \qquad \langle \text{ (3.42), avec } p, q := q, p \ \ \& \ \text{Commutativité de } \equiv \text{ (3.3)} \ \ \& \\
& \qquad \ \ \text{Commutativité de } \vee \text{ (3.32) } \rangle \\
& p \vee (\neg p \equiv p \vee q) \\
= & \qquad \langle \text{ (3.36), avec } q, r := \neg p,\ p \vee q \ \rangle \\
& p \vee \neg p \equiv p \vee p \vee q \\
= & \qquad \langle \text{ Tiers exclu (3.37) } \ \& \ \text{ Idempotence de } \vee \text{ (3.34) } \rangle \\
& \mathsf{vrai} \equiv p \vee q \\
= & \qquad \langle \text{ Identité de } \equiv \text{ (3.4), avec } p := p \vee q \ \rangle \\
& p \vee q
\end{array}
$$

(b)
$$
\begin{array}{ll}
& p \vee (\neg p \wedge q) \\
= & \qquad \langle \text{ Règle d'or (3.57), avec } p := \neg p \ \rangle
\end{array}
$$

$$
\begin{array}{ll}
& p \vee (\neg p \equiv q \equiv \neg p \vee q) \\
= & \quad \langle \text{ Distributivité de } \vee \text{ sur } \equiv (3.36), \text{ avec } q, r := \neg p,\ q \equiv \neg p \vee q \ \rangle \\
& p \vee \neg p \ \equiv \ p \vee (q \equiv \neg p \vee q) \\
= & \quad \langle \text{ Distributivité de } \vee \text{ sur } \equiv (3.36), \text{ avec } r := \neg p \vee q \ \rangle \\
& p \vee \neg p \equiv p \vee q \equiv p \vee \neg p \vee q \\
= & \quad \langle \text{ Tiers exclu (3.37), (deux fois) } \rangle \\
& \mathsf{vrai} \equiv p \vee q \equiv \mathsf{vrai} \vee q \\
= & \quad \langle \text{ Zéro de } \vee \text{ (3.38), avec } p := q \ \ \& \ \text{ Commutativité de } \vee \text{ (3.32) } \rangle \\
& \mathsf{vrai} \equiv p \vee q \equiv \mathsf{vrai} \\
= & \quad \langle \text{ Réflexivité de } \equiv \text{ (3.7), avec } p := \mathsf{vrai} \equiv p \vee q \ \rangle \\
& p \vee q
\end{array}
$$

(c)

$$
\begin{array}{ll}
& p \vee (\neg p \wedge q) \\
= & \quad \langle \text{ Règle d'or (3.57), avec } q := \neg p \wedge q \ \rangle \\
& p \wedge \neg p \wedge q \equiv p \equiv \neg p \wedge q \\
= & \quad \langle \text{ Contradiction (3.55) } \rangle \\
& \mathsf{faux} \wedge q \equiv p \equiv \neg p \wedge q \\
= & \quad \langle \text{ Zéro de } \wedge \text{ (3.53), avec } p := q \ \ \& \ \text{ Commutativité de } \wedge \text{ (3.49) } \rangle \\
& \mathsf{faux} \equiv p \equiv \neg p \wedge q \\
= & \quad \langle \text{ (3.18) } \ \& \ \text{ Commutativité de } \equiv \text{ (3.3) } \rangle \\
& \neg p \equiv \neg p \wedge q \\
= & \quad \langle \text{ Règle d'or (3.57), avec } p := \neg p \ \ \& \ \text{ Commutativité de } \equiv \text{ (3.3) } \rangle \\
& q \equiv \neg p \vee q \\
= & \quad \langle \text{ (3.42), avec } p, q := q, p \ \ \& \ \text{ Commutativité de } \equiv \text{ (3.3) } \ \& \\
& \qquad \text{Commutativité de } \vee \text{ (3.32) } \rangle \\
& p \vee q
\end{array}
$$

10. Démontrez le théorème de remplacement (3.65),

$$(p \equiv q) \ \wedge \ (r \equiv p) \ \equiv \ (p \equiv q) \ \wedge \ (r \equiv q),$$

en montrant que le côté gauche et le côté droit sont tous deux équivalents à

$$p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p.$$

La transformation du côté gauche (ou du côté droit) de cette expression peut se faire en appliquant la distributivité de $\vee$ sur $\equiv$ (3.36) trois fois.

Solution.

(a) Terme de gauche

$$
\begin{array}{ll}
 & (p \equiv q) \wedge (r \equiv p) \\
= & \quad \langle \text{ Règle d'or (3.57), avec } p, q := p \equiv q,\ r \equiv p \ \rangle \\
 & p \equiv q \ \equiv \ r \equiv p \ \equiv \ (p \equiv q) \vee (r \equiv p) \\
= & \quad \langle \text{ Commutativité de } \equiv \text{ (3.3) } \rangle \\
 & p \equiv q \equiv p \ \equiv \ r \ \equiv \ (p \equiv q) \vee (r \equiv p) \\
= & \quad \langle \text{ Réflexivité de } \equiv \text{ (3.7), avec } p := p \equiv q \ \rangle \\
 & q \equiv r \ \equiv \ (p \equiv q) \vee (r \equiv p) \\
= & \quad \langle \text{ Distributivité de } \vee \text{ sur } \equiv \text{ (3.36), avec } p, q, r := p \equiv q,\ r,\ p \ \rangle \\
 & q \equiv r \ \equiv \ (p \equiv q) \vee r \ \equiv \ (p \equiv q) \vee p \\
= & \quad \langle \text{ Distributivité de } \vee \text{ sur } \equiv \text{ (3.36) deux fois} \\
 & \quad \ \ (1) \text{ avec } p, q, r := r, p, q \ \ (2) \text{ avec } p, q, r := p, p, q \ \ \& \\
 & \quad \ \ \text{Commutativité de } \vee \text{ (3.32) } \rangle \\
 & q \ \equiv \ r \ \equiv \ p \vee r \ \equiv \ q \vee r \ \equiv \ p \vee p \ \equiv \ q \vee p \\
= & \quad \langle \text{ Idempotence de } \vee \text{ (3.34) } \ \& \ \text{ Commutativité de } \equiv \text{ (3.3) et } \vee \text{ (3.32)} \\
 & \quad \rangle \\
 & p \ \equiv \ q \ \equiv \ r \ \equiv \ p \vee q \ \equiv \ q \vee r \ \equiv \ r \vee p
\end{array}
$$

(b) Terme de droite

$$
\begin{array}{ll}
 & (p \equiv q) \wedge (r \equiv q) \\
= & \quad \langle \text{ Règle d'or (3.57), avec } p, q := p \equiv q,\ r \equiv q \ \rangle \\
 & p \equiv q \ \equiv \ r \equiv q \ \equiv \ (p \equiv q) \vee (r \equiv q) \\
= & \quad \langle \text{ Commutativité de } \equiv \text{ (3.3) } \rangle \\
 & q \equiv p \equiv q \ \equiv \ r \ \equiv \ (p \equiv q) \vee (r \equiv q) \\
= & \quad \langle \text{ Réflexivité de } \equiv \text{ (3.7), avec } p := q \equiv p \ \rangle \\
 & p \equiv r \ \equiv \ (p \equiv q) \vee (r \equiv q) \\
= & \quad \langle \text{ Distributivité de } \vee \text{ sur } \equiv \text{ (3.36), avec } p, q, r := p \equiv q,\ r,\ q \ \rangle \\
 & p \equiv r \ \equiv \ (p \equiv q) \vee r \ \equiv \ (p \equiv q) \vee q \\
= & \quad \langle \text{ Distributivité de } \vee \text{ sur } \equiv \text{ (3.36) deux fois} \\
 & \quad \ \ (1) \text{ avec } p, q, r := r, p, q \ \ (2) \text{ avec } p, q, r := q, p, q \ \ \& \\
 & \quad \ \ \text{Commutativité de } \vee \text{ (3.32) } \rangle \\
 & p \ \equiv \ r \ \equiv \ p \vee r \ \equiv \ q \vee r \ \equiv \ p \vee q \ \equiv \ q \vee q \\
= & \quad \langle \text{ Idempotence de } \vee \text{ (3.34), avec } p := q \ \ \& \\
 & \quad \ \ \text{Commutativité de } \equiv \text{ (3.3) et } \vee \text{ (3.32) } \rangle \\
 & p \ \equiv \ q \ \equiv \ r \ \equiv \ p \vee q \ \equiv \ q \vee r \ \equiv \ r \vee p
\end{array}
$$

11. Démontrez la réflexivité de $\Rightarrow$ (3.87), $p \Rightarrow p \equiv \mathsf{vrai}$.

Solution. On peut démontrer $p \Rightarrow p \equiv \mathsf{vrai}$ ou encore $p \Rightarrow p$, puisque c'est équivalent. Voici plusieurs preuves.

(a)
$$\begin{aligned} & p \Rightarrow p \\ = & \quad \langle \text{ Définition de l'implication (3.75), avec } q := p \rangle \\ & \neg p \vee p \\ = & \quad \langle \text{ Tiers exclu (3.37) } \rangle \\ & \mathsf{vrai} \qquad \text{—(3.6)} \end{aligned}$$

(b)
$$\begin{aligned} & p \Rightarrow p \\ = & \quad \langle \text{ Définition de l'implication (3.75), avec } q := p \rangle \\ & \neg p \vee p \qquad \text{—Tiers exclu (3.37)} \end{aligned}$$

(c)
$$\begin{aligned} & p \Rightarrow p \\ = & \quad \langle \text{ Définition de l'implication (3.73), avec } q := p \rangle \\ & p \vee p \equiv p \qquad \text{—Idempotence de } \vee \text{ (3.34)} \end{aligned}$$

12. Démontrez le théorème de l'affaiblissement/renforcement (3.92c), $p \wedge q \Rightarrow p \vee q$.

Solution.
$$\begin{aligned} & p \wedge q \Rightarrow p \vee q \\ = & \quad \langle \text{ Définition de l'implication (3.76), avec } p, q := p \wedge q,\ p \vee q \rangle \\ & p \wedge q \wedge (p \vee q) \equiv p \wedge q \\ = & \quad \langle \text{ Commutativité de } \wedge \text{ (3.49) } \ \& \ \text{ Absorption (3.61a) } \rangle \\ & p \wedge q \equiv p \wedge q \qquad \text{—Réflexivité de } \equiv \text{ (3.7), avec } p := p \wedge q \end{aligned}$$

13. Démontrez le modus ponens (3.93), $p \wedge (p \Rightarrow q) \Rightarrow q$.

Solution.
$$\begin{aligned} & p \wedge (p \Rightarrow q) \Rightarrow q \\ = & \quad \langle \text{ (3.82) } \rangle \\ & p \wedge q \Rightarrow q \qquad \text{—Affaiblissement (3.92b), avec } p, q := q, p \end{aligned}$$

14.4 Problèmes du chapitre 4

1. Démontrez la monotonie de $\wedge$ (4.3), $(p \Rightarrow q) \;\Rightarrow\; (p \wedge r \Rightarrow q \wedge r)$, en utilisant la méthode de la section 4.1. Commencez avec le conséquent, puisqu'il est plus structuré.

   Solution.

   $$\begin{array}{ll} & p \wedge r \;\Rightarrow\; q \wedge r \\ = & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75), avec } p, q \;:=\; p \wedge r,\; q \wedge r \;\rangle \\ & \neg(p \wedge r) \;\vee\; (q \wedge r) \\ = & \qquad \langle \text{ De Morgan (3.48a), avec } q \;:=\; r \;\rangle \\ & \neg p \vee \neg r \vee (q \wedge r) \\ = & \qquad \langle \text{ Double négation (3.15), avec } p \;:=\; r \;\;\&\;\; \text{Commutativité de } \wedge \text{ (3.49)} \\ & \qquad \rangle \\ & \neg p \vee \neg r \vee (\neg\neg r \wedge q) \\ = & \qquad \langle \text{ Absorption (3.61d), avec } p \;:=\; \neg r \;\rangle \\ & \neg p \vee \neg r \vee q \\ = & \qquad \langle \text{ Commutativité de } \vee \text{ (3.32)} \;\rangle \\ & \neg p \vee q \vee \neg r \\ \Leftarrow & \qquad \langle \text{ Renforcement (3.92a), avec } p, q \;:=\; \neg p \vee q,\; r \;\rangle \\ & \neg p \vee q \\ = & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75)} \;\rangle \\ & p \Rightarrow q \end{array}$$

2. Démontrez $(p \Rightarrow q) \wedge (r \Rightarrow s) \;\Rightarrow\; (p \wedge r \Rightarrow q \wedge s)$, en utilisant le style de preuve de la section 4.1. Avant de débuter cette preuve, considérez la possibilité d'utiliser le théorème de transfert (3.81) pour déplacer $p \wedge r$ dans l'antécédent.

   Solution. Suivons la suggestion et utilisons le théorème (3.81) dans le but d'amener $p \wedge r$ dans l'antécédent, ce qui nous facilitera la tâche.

   $$\begin{array}{ll} & (p \Rightarrow q) \wedge (r \Rightarrow s) \;\Rightarrow\; (p \wedge r \Rightarrow q \wedge s) \\ = & \qquad \langle \text{ Transfert (3.81), avec } p, q, r \;:=\; (p \Rightarrow q) \wedge (r \Rightarrow s),\; p \wedge r,\; q \wedge s \;\rangle \\ & (p \Rightarrow q) \wedge (r \Rightarrow s) \wedge p \wedge r \;\Rightarrow\; q \wedge s \end{array}$$

   Maintenant, montrons que l'expression ainsi dérivée est un théorème. Nous débutons par l'antécédent, qui est plus structuré. Voici trois preuves.

   (a)
   $$\begin{array}{ll} & (p \Rightarrow q) \wedge (r \Rightarrow s) \wedge p \wedge r \\ = & \qquad \langle \text{ Commutativité de } \wedge \text{ (3.49)} \;\rangle \\ & p \wedge (p \Rightarrow q) \wedge r \wedge (r \Rightarrow s) \end{array}$$

$=$ $\langle$ (3.82) deux fois (1) directement (2) avec $p, q := r, s$ $\rangle$

$p \wedge q \wedge r \wedge s$

$=$ $\langle$ Commutativité de $\wedge$ (3.49) $\rangle$

$q \wedge s \wedge p \wedge r$

$\Rightarrow$ $\langle$ Affaiblissement (3.92b), avec $p, q := q \wedge s,\ p \wedge r$ $\rangle$

$q \wedge s$

(b) $(p \Rightarrow q) \wedge (r \Rightarrow s) \wedge p \wedge r$

$=$ $\langle$ Commutativité de $\wedge$ (3.49) $\rangle$

$p \wedge (p \Rightarrow q) \wedge r \wedge (r \Rightarrow s)$

$\Rightarrow$ $\langle$ Modus ponens (3.93) &
Monotonie de $\wedge$ (4.3), avec $p, q, r := p \wedge (p \Rightarrow q),\ q,\ r \wedge (r \Rightarrow s)$
&
Règle du modus ponens, avec $P := p \wedge (p \Rightarrow q) \Rightarrow q$ et
$Q := p \wedge (p \Rightarrow q) \wedge r \wedge (r \Rightarrow s) \ \Rightarrow\ q \wedge r \wedge (r \Rightarrow s)$ $\rangle$

$q \wedge r \wedge (r \Rightarrow s)$

$\Rightarrow$ $\langle$ Modus ponens (3.93), avec $p, q := r, s$ &
Monotonie de $\wedge$ (4.3), avec $p, q, r := r \wedge (r \Rightarrow s),\ s,\ q$ &
Règle du modus ponens, avec $P := r \wedge (r \Rightarrow s) \Rightarrow s$ et
$Q := q \wedge r \wedge (r \Rightarrow s) \ \Rightarrow\ q \wedge s$ &
Commutativité de $\wedge$ (3.49) $\rangle$

$q \wedge s$

(c) La preuve précédente est très détaillée, en particulier pour bien faire comprendre l'usage de la mononotonie de $\wedge$ et de la règle du modus ponens. Habituellement, l'usage d'une telle règle n'est pas mentionné et la preuve peut être simplifiée comme ceci :

$(p \Rightarrow q) \wedge (r \Rightarrow s) \wedge p \wedge r$

$=$ $\langle$ Commutativité de $\wedge$ (3.49) $\rangle$

$p \wedge (p \Rightarrow q) \wedge r \wedge (r \Rightarrow s)$

$\Rightarrow$ $\langle$ Modus ponens (3.93) &
Monotonie de $\wedge$ (4.3), avec $p, q, r := p \wedge (p \Rightarrow q),\ q,\ r \wedge (r \Rightarrow s)$ $\rangle$

$q \wedge r \wedge (r \Rightarrow s)$

$\Rightarrow$ $\langle$ Modus ponens (3.93), avec $p, q := r, s$ &
Monotonie de $\wedge$ (4.3), avec $p, q, r := r \wedge (r \Rightarrow s),\ s,\ q$ &
Commutativité de $\wedge$ (3.49) $\rangle$

$q \wedge s$

3. Démontrez $(\neg p \Rightarrow q) \;\Rightarrow\; ((p \Rightarrow q) \Rightarrow q)$, en utilisant la méthode qui consiste à assumer l'antécédent.

   Solution. Voici trois preuves.

   (a) Assumons $\neg p \Rightarrow q$, ce qui est équivalent à $\neg p \wedge q \equiv \neg p$, par (3.76) avec $p := \neg p$.

   $$\begin{array}{ll} & p \Rightarrow q \\ = & \quad \langle \text{ Définition alternative de } \Rightarrow \text{ (3.75) } \rangle \\ & \neg p \vee q \\ = & \quad \langle \text{ Hypothèse : } \neg p \equiv \neg p \wedge q \ \rangle \\ & (\neg p \wedge q) \vee q \\ = & \quad \langle \text{ Absorption (3.61b), avec } p, q := q, \neg p \ \ \& \\ & \quad \text{Commutativité de } \vee \text{ (3.32) et } \wedge \text{ (3.49) } \rangle \\ & q \end{array}$$

   Remarquez que nous avons même montré une propriété plus forte, soit

   $$(\neg p \Rightarrow q) \;\Rightarrow\; (p \Rightarrow q \;\equiv\; q).$$

   (b) Assumons $\neg p \Rightarrow q$, ce qui est équivalent à $\neg p \vee q \equiv q$, par (3.73) avec $p := \neg p$.

   $$\begin{array}{ll} & p \Rightarrow q \\ = & \quad \langle \text{ Définition alternative de } \Rightarrow \text{ (3.75) } \rangle \\ & \neg p \vee q \\ = & \quad \langle \text{ Hypothèse } \neg p \vee q \equiv q \ \rangle \\ & q \end{array}$$

   Cette preuve, comme la précédente, démontre une propriété plus forte que celle qui est demandée.

   (c) Assumons $\neg p \Rightarrow q$.

   $$\begin{array}{ll} & p \Rightarrow q \\ = & \quad \langle \text{ Définition de } \Rightarrow \text{ (3.75) } \rangle \\ & \neg p \vee q \\ \Rightarrow & \quad \langle \text{ Hypothèse } \neg p \Rightarrow q \ \ \& \ \ \text{Monotonie de } \vee \text{ (4.2), avec } p, q, r := \neg p, q, q \\ & \quad \& \\ & \quad \text{Règle du modus ponens } \rangle \\ & q \vee q \\ = & \quad \langle \text{ Idempotence de } \vee \text{ (3.34), avec } p := q \ \rangle \\ & q \end{array}$$

4. Démontrez le modus ponens (3.93), $p \wedge (p \Rightarrow q) \Rightarrow q$, en utilisant la méthode qui consiste à assumer l'antécédent.

   Solution. Assumons p ainsi que $p \Rightarrow q$ (revoyez le théorème de déduction (4.6), qui énonce qu'il est possible d'assumer séparément les opérandes de la conjonction qui constitue l'antécédent).

   $$\begin{array}{ll} & q \\ = & \quad \langle \text{ Hypothèse } p \Rightarrow q, \text{ qui est équivalente à } p \vee q \equiv q, \text{ par (3.73) } \rangle \\ & p \vee q \\ = & \quad \langle \text{ Hypothèse } p \ \ \& \ \mathsf{vrai} \text{ est un théorème (3.6) } \ \& \text{ Métathéorème (3.100) } \rangle \\ & \mathsf{vrai} \vee q \\ = & \quad \langle \text{ Zéro de } \vee \text{ (3.38), avec } p := q \ \ \& \ \text{ Commutativité de } \vee \text{ (3.32) } \rangle \\ & \mathsf{vrai} \end{array}$$

14.5 Problèmes du chapitre 5

1. Formalisez chacun des arguments suivants et soit montrez que c'est un théorème, soit trouvez un contre-exemple.

   (a) Le programme ne termine pas ou n devient éventuellement 0. Si n devient 0, m deviendra éventuellement 0. Le programme termine. Par conséquent, m deviendra éventuellement 0.

   Solution. Associons les identificateurs suivants aux propositions primitives :

   $$\begin{aligned} t &: \text{le programme termine} \\ n0 &: n \text{ devient 0} \\ m0 &: m \text{ devient 0} \end{aligned}$$

   L'expression booléenne est

   $$(\neg t \vee n0) \ \wedge \ (n0 \Rightarrow m0) \ \wedge \ t \ \ \Rightarrow \ \ m0.$$

   En voici la preuve.

   $$\begin{array}{ll} & (\neg t \vee n0) \ \wedge \ (n0 \Rightarrow m0) \ \wedge \ t \\ = & \quad \langle \text{ Absorption (3.61c), avec } p, q := t, n0 \ \rangle \\ & n0 \ \wedge \ (n0 \Rightarrow m0) \ \wedge \ t \\ = & \quad \langle \text{ (3.82), avec } p, q := n0, m0 \ \rangle \\ & n0 \wedge m0 \wedge t \\ \Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec } p, q := m0, n0 \wedge t \ \rangle \\ & m0 \end{array}$$

(b) Si l'initialisation est correcte et si la boucle termine, alors P est vrai dans l'état final. P est vrai dans l'état final. Par conséquent, si l'initialisation est correcte, la boucle termine.

Solution. Associons les identificateurs suivants aux propositions primitives :

c : l'initialisation est correcte
t : la boucle termine
f : P est vrai dans l'état final

L'expression booléenne est

$$(c \wedge t \Rightarrow f) \wedge f \;\Rightarrow\; (c \Rightarrow t).$$

L'expression n'est pas un théorème. Voici un contre-exemple :

$$(c, \mathsf{vrai}),\ (t, \mathsf{faux}),\ (f, \mathsf{vrai})$$

(c) S'il y a un homme sur la lune, la lune est faite en fromage, et si la lune est faite en fromage, alors je suis un singe. Il n'y a pas d'homme sur la lune ou la lune n'est pas faite en fromage. Par conséquent, la lune n'est pas faite en fromage ou je suis un singe.

Solution. Associons les identificateurs suivants aux propositions primitives :

h : il y a un homme sur la lune
f : la lune est faite en fromage
s : je suis un singe

L'expression booléenne est alors

$$(h \Rightarrow f) \wedge (f \Rightarrow s) \wedge (\neg h \vee \neg f) \;\Rightarrow\; \neg f \vee s.$$

Notons que le conséquent est équivalent à $f \Rightarrow s$, par la définition alternative de $\Rightarrow$ (3.75), avec $p, q := f, s$. Or, $f \Rightarrow s$ est aussi un opérande de la conjonction dans l'antécédent. Ceci est un bon indice que l'expression est probablement un théorème. En voici la preuve.

$$\begin{array}{ll} & (h \Rightarrow f) \wedge (f \Rightarrow s) \wedge (\neg h \vee \neg f) \\ \Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec } p, q := (h \Rightarrow f) \wedge (\neg h \vee \neg f),\ (f \Rightarrow s) \rangle \\ & f \Rightarrow s \\ = & \quad \langle \text{ Définition alternative de } \Rightarrow \text{ (3.75), avec } p, q := f, s \rangle \\ & \neg f \vee s \end{array}$$

(d) Si Réjean trompe Thérèse, alors môman est fâchée ou pôpa est triste. Pôpa est triste. Par conséquent, si môman est fâchée alors Réjean ne trompe pas Thérèse.

Solution. Associons les identificateurs suivants aux propositions primitives :

R : Réjean trompe Thérèse
M : Môman est fâchée
P : Pôpa est triste

L'expression booléenne est alors

$$(R \Rightarrow M \vee P) \wedge P \Rightarrow (M \Rightarrow \neg R).$$

L'expression n'est pas un théorème. Voici un contre-exemple :

$$(R, \mathsf{vrai}),\ (M, \mathsf{vrai}),\ (P, \mathsf{vrai})$$

2. Supposons que Portia place son portrait dans l'un de trois coffrets et qu'elle place les inscriptions suivantes sur ceux-ci :

Coffret d'or :	Le portrait est ici.
Coffret d'argent :	Le portrait est ici.
Coffret de plomb :	Au moins deux de ces inscriptions sont fausses.

Quel coffret son soupirant doit-il choisir ? Formalisez le problème et calculez la réponse.

Solution. Le soupirant devrait noter que la situation est symétrique en ce qui concerne les coffrets d'or et d'argent, car les inscriptions sur ces deux coffrets sont identiques et l'inscription sur le coffret de plomb ne mentionne aucun de ces deux coffrets. Si le portrait était dans le coffret d'or ou dans le coffret d'argent, il n'y aurait pas assez d'information pour déterminer lequel des deux contient le portrait. Par conséquent, le soupirant devrait choisir le coffret de plomb !

Armés de cet indice, voyons si nous pouvons démontrer que le coffret de plomb contient effectivement le portrait.

Introduisons les variables booléennes suivantes :

o : Le portrait est dans le coffret d'or.
a : Le portrait est dans le coffret d'argent.
p : Le portrait est dans le coffret de plomb.

Le fait que le portrait soit dans exactement l'un des coffrets entraîne les deux propriétés suivantes :

$$F_0 : \ p \equiv \neg o \wedge \neg a$$
$$F_1 : \ o \wedge a \equiv \mathsf{faux}$$

Notez que nous pourrions également ajouter des propriétés comme $o \equiv \neg a \wedge \neg p$ et $o \wedge p \equiv \mathsf{faux}$. Cependant, il s'avère que nous n'en avons pas besoin.

Des inscriptions io et ia sur les coffrets d'or et d'argent on peut dire $io \equiv o$ et $ia \equiv a$. Par conséquent, nous utiliserons o et a à la place de io et ia. Le cas de l'inscription ip sur le coffret de plomb est plus complexe. Il vaut mieux l'exprimer comme deux implications : si l'inscription est vraie, alors les deux autres inscriptions sont fausses ;

si elle est fausse, alors au plus une des inscriptions est fausse, ce qui signifie que les deux autres sont vraies. On a donc

$$\begin{array}{ll} F_2: & ip \Rightarrow \neg o \wedge \neg a \\ F_3: & \neg ip \Rightarrow o \wedge a \end{array}$$

Assumons F_0, F_1, F_2, F_3 et montrons p :

$$\begin{array}{ll} & \mathsf{vrai} \qquad \text{—(3.6)} \\ = & \qquad \langle \text{ Tiers exclu (3.37), avec } p := ip \ \ \& \ \mathsf{vrai} \text{ est un théorème (3.6)} \\ & \qquad \text{Métathéorème (3.100) } \rangle \\ & ip \vee \neg ip \\ \Rightarrow & \qquad \langle \ F_2 \ \ \& \ \text{Monotonie de } \vee \text{ (4.2), avec } p, q, r := ip,\ \neg o \wedge \neg a,\ \neg ip \ \rangle \\ & (\neg o \wedge \neg a) \vee \neg ip \\ \Rightarrow & \qquad \langle \ F_3 \ \ \& \ \text{Monotonie de } \vee \text{ (4.2), avec } p, q, r := \neg ip,\ o \wedge a,\ \neg o \wedge \neg a \ \rangle \\ & (\neg o \wedge \neg a) \vee (o \wedge a) \\ = & \qquad \langle \ F_0 \ \ \& \ \ F_1 \ \rangle \\ & p \vee \mathsf{faux} \\ = & \qquad \langle \text{ Identité de } \vee \text{ (3.40) } \rangle \\ & p \end{array}$$

Nous avons montré $\mathsf{vrai} \Rightarrow p$, ce qui est équivalent à p (3.89). Le portrait est donc dans le coffret de plomb.

Les expressions F_0, F_1, F_2 et F_3 ne sont pas contradictoires, car elles sont toutes vraies dans l'état suivant

$$(o, \mathsf{faux}), \quad (a, \mathsf{faux}), \quad (p, \mathsf{vrai}), \quad (ip, \mathsf{vrai}) \ .$$

3. La série de questions qui suit concerne une île avec des chevaliers et des filous. Les chevaliers disent toujours la vérité et les filous mentent toujours. Pour formaliser ces questions, utilisez les identificateurs suivants :

$$\begin{array}{ll} b: & B \text{ est un chevalier.} \\ c: & C \text{ est un chevalier.} \\ d: & D \text{ est un chevalier.} \end{array}$$

Si B énonce « X », ceci donne lieu à l'expression $b \equiv X$, puisque si b, alors B est un chevalier et dit la vérité, de sorte que X, et si $\neg b$, alors B est un filou et ment, de sorte que $\neg X$. Il en est de même pour les énoncés de C et D.

(a) Quelqu'un demande à B « Êtes-vous un chevalier ? ». B réplique « Si je suis un chevalier, je vais manger mon chapeau ». Montrez que B devra manger son chapeau.

Solution. Si l'on utilise c pour désigner la proposition « je vais manger mon chapeau », la réplique de B se formalise comme $b \Rightarrow c$. Nous devons donc prendre comme axiome l'expression $b \equiv b \Rightarrow c$ (selon les conseils de l'énoncé du problème). Simplifions cette expression :

$$\begin{array}{ll} & b \equiv (b \Rightarrow c) \qquad \text{—Axiome de notre formalisation du problème} \\ = & \qquad \langle \text{ Définition de } \Rightarrow \ (3.76), \text{ avec } p, q := b, c \ \rangle \\ & b \wedge c \end{array}$$

Donc B est un chevalier et doit manger son chapeau.

(b) B, C et D discutent ensemble. C dit « Il y a un chevalier parmi nous ». D dit « Vous mentez ». Pouvez-vous dire qui est chevalier et qui est filou ?
Indice : On peut décrire le fait qu'un ou trois de ces personnages soient des chevaliers par l'expression $b \equiv c \equiv d$, puisque cette expression a la valeur vrai exactement lorsque le nombre d'opérandes faux est pair. Pour restreindre à un chevalier, il suffit de faire la conjonction de cette expression avec $\neg(b \wedge c \wedge d)$. Voyez la discussion à la page 46 du manuel.

Solution. Suivant l'indice donné, la formalisation de « Il y a un chevalier parmi nous » est $(b \equiv c \equiv d) \wedge \neg(b \wedge c \wedge d)$. Puisque c'est C qui fait cette affirmation, nous prenons comme axiome

$$c \equiv (b \equiv c \equiv d) \wedge \neg(b \wedge c \wedge d).$$

L'affirmation de D est équivalente à $\neg c$, de sorte que notre deuxième axiome est

$$d \equiv \neg c.$$

Simplifions la conjonction de ces deux faits :

$$\begin{array}{ll} & (d \equiv \neg c) \ \wedge \ (c \equiv (b \equiv c \equiv d) \wedge \neg(b \wedge c \wedge d)) \qquad \text{—Axiome par hypothèse} \\ = & \qquad \langle \text{ Substitution (9.3a),} \\ & \qquad\ e, f, E := d, \ \neg c, \ c \equiv (b \equiv c \equiv z) \wedge \neg(b \wedge c \wedge z) \ \rangle \\ & (d \equiv \neg c) \ \wedge \ (c \equiv (b \equiv c \equiv \neg c) \wedge \neg(b \wedge c \wedge \neg c)) \\ = & \qquad \langle \ (3.18), \text{ avec } p := c \ \ \& \ \text{ Contradiction (3.55), avec } p := c \ \rangle \\ & (d \equiv \neg c) \ \wedge \ (c \equiv (b \equiv \mathsf{faux}) \wedge \neg(b \wedge \mathsf{faux})) \\ = & \qquad \langle \ (3.18), \text{ avec } p := b \ \ \& \ \text{ Zéro de } \wedge \ (3.53), \text{ avec } p := b \ \rangle \\ & (d \equiv \neg c) \ \wedge \ (c \equiv \neg b \wedge \neg \mathsf{faux}) \\ = & \qquad \langle \ \text{Négation de faux } (3.16) \ \rangle \\ & (d \equiv \neg c) \ \wedge \ (c \equiv \neg b \wedge \mathsf{vrai}) \\ = & \qquad \langle \ \text{Identité de } \wedge \ (3.52), \text{ avec } p := \neg b \ \rangle \\ & (d \equiv \neg c) \ \wedge \ (c \equiv \neg b) \\ = & \qquad \langle \ (3.14, \text{ avec } p, q := c, b \ \rangle \\ & (d \equiv \neg c) \ \wedge \ (b \equiv \neg c) \end{array}$$

Par conséquent, B et D sont similaires —tous deux chevaliers ou tous deux filous— et C est différent de ses deux comparses. Il n'est pas possible d'en dire plus.

Remarque : l'indice donné dans l'énoncé du problème suggère assez fortement qu'il faut interpréter « Il y a un chevalier parmi nous » comme signifiant qu'il y a *exactement* un chevalier parmi eux. Toutefois, n'était de cet indice, j'aurais interprété cette proposition comme signifiant qu'il y a au moins un chevalier parmi eux (la langue naturelle est ambigüe). Montrez que dans ce cas, tout ce qu'on peut dire, c'est que C et D sont différents.

4. À l'exercice 2.7, nous avons traduit les hypothèses et les conjectures relatives à l'autobus tardif. Déterminez maintenant quelles conjectures sont une conséquence des trois hypothèses.

Solution. Rappelons la formalisation des trois hypothèses (numérotées 1, 2, 3 dans le tableau qui suit) et des huit conjectures (numéros 4 à 11).

1	$\mathsf{pa} \Rightarrow (\mathsf{mr} \Leftarrow \mathsf{ar})$	$\mathsf{pa} \Rightarrow (\mathsf{ar} \Rightarrow \mathsf{mr})$	$\mathsf{pa} \wedge \mathsf{ar} \Rightarrow \mathsf{mr}$
2	$\neg\mathsf{am} \Leftarrow \mathsf{mr} \wedge d$	$\mathsf{mr} \wedge d \Rightarrow \neg\mathsf{am}$	
3	$\neg e \Rightarrow d \wedge \neg\mathsf{am}$		
4	$\mathsf{pa} \Rightarrow (e \Leftarrow \mathsf{ar})$	$\mathsf{pa} \Rightarrow (\mathsf{ar} \Rightarrow e)$	$\mathsf{pa} \wedge \mathsf{ar} \Rightarrow e$
5	$e \Leftarrow \mathsf{mr} \wedge \mathsf{am}$	$\mathsf{mr} \wedge \mathsf{am} \Rightarrow e$	
6	$\mathsf{ar} \wedge d \wedge \mathsf{am} \Rightarrow \neg\mathsf{pa}$		
7	$\neg\mathsf{pa} \Leftarrow \mathsf{ar} \wedge \neg e$	$\mathsf{ar} \wedge \neg e \Rightarrow \neg\mathsf{pa}$	
8	$\neg\mathsf{mr} \Rightarrow \neg\mathsf{am} \wedge \neg e$		
9	$d \Leftarrow \mathsf{ar} \vee \mathsf{mr}$	$\mathsf{ar} \vee \mathsf{mr} \Rightarrow d$	
10	$\mathsf{pa} \wedge \mathsf{ar} \wedge \mathsf{am} \Rightarrow e$		
11	$\mathsf{pa} \wedge \neg e \Rightarrow \neg\mathsf{ar} \vee \neg\mathsf{am}$		

Avant de procéder avec chacune des conjectures, démontrons deux lemmes qui seront utilisés par la suite. Le premier lemme est

$$(*) \qquad (\mathsf{mr} \wedge d \Rightarrow \neg\mathsf{am}) \;\equiv\; (\mathsf{mr} \wedge \mathsf{am} \Rightarrow \neg d).$$

En voici la preuve :

$$\begin{array}{ll}
 & \mathsf{mr} \wedge d \Rightarrow \neg\mathsf{am} \\
= & \qquad \langle \text{ Transfert (3.81), avec } p, q, r \;:=\; \mathsf{mr}, d, \neg\mathsf{am} \;\rangle \\
 & \mathsf{mr} \Rightarrow (d \Rightarrow \neg\mathsf{am}) \\
= & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75), avec } p, q \;:=\; d, \neg\mathsf{am} \;\rangle \\
 & \mathsf{mr} \Rightarrow (\neg d \vee \neg\mathsf{am}) \\
= & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75), avec } p, q \;:=\; \mathsf{am}, \neg d \;\rangle \\
 & \mathsf{mr} \Rightarrow (\mathsf{am} \Rightarrow \neg d) \\
= & \qquad \langle \text{ Transfert (3.81), avec } p, q, r \;:=\; \mathsf{mr}, \mathsf{am}, \neg d \;\rangle \\
 & \mathsf{mr} \wedge \mathsf{am} \Rightarrow \neg d
\end{array}$$

De la même manière, on démontre le deuxième lemme,

(**) $$(\mathsf{mr} \wedge d \Rightarrow \neg \mathsf{am}) \;\equiv\; (d \wedge \mathsf{am} \Rightarrow \neg \mathsf{mr}).$$

Procédons maintenant à l'étude des huit conjectures.

(a) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (4)$? Regardez la matière de ce chapitre ; ce problème y a été résolu. On y donne un contre-exemple.

(b) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (5)$? Oui. En voici la preuve. Assumons les trois hypothèses.

$$\begin{array}{ll}
 & \mathsf{mr} \wedge \mathsf{am} \\
\Rightarrow & \quad \langle \text{ Hypothèse 2 } \& \text{ lemme (*) ci-dessus } \rangle \\
 & \neg d \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92a), avec } p, q := \neg d, \mathsf{am} \rangle \\
 & \neg d \vee \mathsf{am} \\
= & \quad \langle \text{ De Morgan (3.48a), avec } p, q := d, \neg \mathsf{am} \ \& \\
 & \quad \text{ Double négation (3.15), avec } p := \mathsf{am} \rangle \\
 & \neg (d \wedge \neg \mathsf{am}) \\
\Rightarrow & \quad \langle \text{ Contraposée de l'hypothèse 3 } \& \\
 & \quad \text{ Contrapositivité (3.77), avec } p, q := \neg e,\ d \wedge \neg \mathsf{am} \ \& \\
 & \quad \text{ Double négation (3.15, avec } p := e \rangle \\
 & e
\end{array}$$

(c) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (6)$? Oui. En voici la preuve. Assumons les trois hypothèses.

$$\begin{array}{ll}
 & \mathsf{ar} \wedge d \wedge \mathsf{am} \\
\Rightarrow & \quad \langle \text{ Hypothèse 2 } \& \text{ lemme (**) ci-dessus } \& \\
 & \quad \text{ Monotonie de } \wedge \text{ (4.3), avec } p, q, r := d \wedge \mathsf{am},\ \neg \mathsf{mr},\ \mathsf{ar} \rangle \\
 & \mathsf{ar} \wedge \neg \mathsf{mr} \\
= & \quad \langle \text{ De Morgan (3.48b), avec } p, q := \neg \mathsf{ar}, \mathsf{mr} \ \& \\
 & \quad \text{ Double négation (3.15), avec } p := \mathsf{ar} \rangle \\
 & \neg (\neg \mathsf{ar} \vee \mathsf{mr}) \\
= & \quad \langle \text{ Définition de } \Rightarrow \text{ (3.75), avec } p, q := \mathsf{ar}, \mathsf{mr} \rangle \\
 & \neg (\mathsf{ar} \Rightarrow \mathsf{mr}) \\
\Rightarrow & \quad \langle \text{ Contraposée de l'hypothèse 1 } \& \\
 & \quad \text{ Contrapositivité (3.77), avec } p, q := \mathsf{pa},\ \mathsf{ar} \Rightarrow \mathsf{mr} \rangle \\
 & \neg \mathsf{pa}
\end{array}$$

(d) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (7)$? Non. Voici un contre-exemple.

$$(\mathsf{pa}, \mathsf{vrai}),\ \ (\mathsf{mr}, \mathsf{vrai}),\ \ (\mathsf{ar}, \mathsf{vrai}),\ \ (d, \mathsf{vrai})\ \ (\mathsf{am}, \mathsf{faux})\ \ (e, \mathsf{faux})\ .$$

(e) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (8)$? Non. Voici un contre-exemple.

$$(\mathsf{mr}, \mathsf{faux}), \quad (\mathsf{pa}, \mathsf{faux}), \quad (e, \mathsf{vrai})$$

(f) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (9)$? Non. Voici un contre-exemple.

$$(\mathsf{mr}, \mathsf{vrai}), \quad (d, \mathsf{faux}), \quad (e, \mathsf{vrai})$$

(g) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (10)$? Oui. En voici la preuve. Assumons les trois hypothèses.

$$\begin{array}{ll}
 & \mathsf{pa} \wedge \mathsf{ar} \wedge \mathsf{am} \\
\Rightarrow & \quad \langle \text{ Hypothèse 1 } \& \\
 & \quad \text{Monotonie de } \wedge \text{ (4.3), avec } p, q, r := \mathsf{pa},\ \mathsf{ar} \Rightarrow \mathsf{mr},\ \mathsf{ar} \wedge \mathsf{am} \ \rangle \\
 & (\mathsf{ar} \Rightarrow \mathsf{mr}) \wedge \mathsf{ar} \wedge \mathsf{am} \\
\Rightarrow & \quad \langle \text{ Modus ponens (3.93), avec } p, q := \mathsf{ar}, \mathsf{mr} \ \& \\
 & \quad \text{Monotonie de } \wedge \text{ (4.3), avec } p, q, r := \mathsf{ar} \wedge (\mathsf{ar} \Rightarrow \mathsf{mr}),\ \mathsf{mr},\ \mathsf{am} \ \rangle \\
 & \mathsf{mr} \wedge \mathsf{am} \\
\Rightarrow & \quad \langle \text{ Hypothèse 2 } \& \text{ lemme (*) ci-dessus } \rangle \\
 & \neg d \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92a), avec } p, q := \neg d, \mathsf{am} \ \rangle \\
 & \neg d \vee \mathsf{am} \\
= & \quad \langle \text{ De Morgan (3.48a), avec } p, q := d, \neg\mathsf{am} \ \& \\
 & \quad \text{Double négation (3.15), avec } p := \mathsf{am} \ \rangle \\
 & \neg(d \wedge \neg\mathsf{am}) \\
\Rightarrow & \quad \langle \text{ Contraposée de l'hypothèse 3 } \& \\
 & \quad \text{Contrapositivité (3.77), avec } p, q := \neg e,\ d \wedge \neg\mathsf{am} \ \& \\
 & \quad \text{Double négation (3.15, avec } p := e \ \rangle \\
 & e
\end{array}$$

(h) A-t-on $(1) \wedge (2) \wedge (3) \Rightarrow (11)$? Oui. En voici la preuve.

$$\begin{array}{ll}
 & \mathsf{pa} \wedge \neg e \ \Rightarrow \ \neg\mathsf{ar} \vee \neg\mathsf{am} \\
= & \quad \langle \text{ Définition de l'implication (3.75), avec } p, q := \mathsf{pa} \wedge \neg e,\ \neg\mathsf{ar} \vee \\
 & \quad \neg\mathsf{am} \ \rangle \\
 & \neg(\mathsf{pa} \wedge \neg e) \vee \neg\mathsf{ar} \vee \neg\mathsf{am} \\
= & \quad \langle \text{ De Morgan (3.48a), avec } p, q := \mathsf{pa}, \neg e \ \& \\
 & \quad \text{Double négation (3.15), avec } p := e \ \rangle \\
 & \neg\mathsf{pa} \vee e \vee \neg\mathsf{ar} \vee \neg\mathsf{am} \\
= & \quad \langle \text{ De Morgan (3.48a), avec } p, q := \mathsf{pa}, \mathsf{ar} \ \rangle
\end{array}$$

$$
\begin{array}{ll}
& \neg(\mathsf{pa} \wedge \mathsf{ar}) \vee e \vee \neg \mathsf{am} \\
= & \qquad \langle \text{ De Morgan (3.48a), avec } p, q := \mathsf{pa} \wedge \mathsf{ar},\ \mathsf{am} \ \rangle \\
& \neg(\mathsf{pa} \wedge \mathsf{ar} \wedge \mathsf{am}) \vee e \\
= & \qquad \langle \text{ Définition de l'implication (3.75), avec } p, q := \mathsf{pa} \wedge \mathsf{ar} \wedge \mathsf{am},\ e \ \rangle \\
& \mathsf{pa} \wedge \mathsf{ar} \wedge \mathsf{am} \Rightarrow e
\end{array}
$$

Cette dernière expression est l'expression de la conjecture 10, dont nous avons montré à l'item précédent qu'elle découle des hypothèses.

14.6 Problèmes du chapitre 6

1. Voici les types de cinq fonctions a, b, c, d et e :

   $a{:}A \to B$ $\qquad$ $b{:}B \to C$ $\qquad$ $c{:}C \to A$ $\qquad$ $d{:}A \times C \to D$ $\qquad$ $e{:}B \times B \to E$

   Dites si les expressions ci-dessous sont bien typées. Si une expression est bien typée, donnez son type (c'est-à-dire le type du résultat). Dans le cas contraire, expliquez pourquoi elle est mal typée. Supposez $u{:}A$, $w{:}B$, $x{:}C$, $y{:}D$ et $z{:}E$.

   (a) $e(a.u, w)$
   (b) $b.x$
   (c) $e(a(c.x), a.u)$
   (d) $a(c(b(a.y)))$
   (e) $d(c.x, c.x)$

   Solution.

   (a) Bien typée. Type E.
   (b) Mal typée : l'argument de b doit avoir le type B, mais x à le type C.
   (c) Bien typée. Type E.
   (d) Mal typée : l'argument de a doit avoir le type A, mais y a le type D.
   (e) Mal typée : le deuxième argument de d doit avoir le type C, mais a ici le type A (c'est le type du résultat de c).

2. Effectuez les substitutions textuelles suivantes. Si nécessaire, renommez la variable de quantification en utilisant la loi (6.36).

   (a) $(\star x \mid 0 \leq x + r < n : x + v)[v := 3]$
   (b) $(\star x \mid 0 \leq x < r : (\star y \mid 0 \leq y : x + y + n))[n := x + y]$
   (c) $(\star x \mid 0 \leq x < r : (\star y \mid 0 \leq y : x + y + n))[r := y]$

Solution.

(a) $(\star x \mid 0 \leq x + r < n : x + 3)$

(b) $(\star z \mid 0 \leq z < r : (\star w \mid 0 \leq w : z + w + x + y))$

Voici, avec tous les détails, comment cette réponse a été obtenue.

$$
\begin{array}{ll}
 & (\star x \mid 0 \leq x < r : (\star y \mid 0 \leq y : x + y + n))[n := x + y] \\
= & \quad \langle \text{ Il faut d'abord tenir compte de la quantification externe. La variable de quantification est } x. \text{ Or, il y a une occurrence libre de } x \text{ dans } `n, x + y'. \text{ Il faut donc renommer la variable de quantification } x. \text{ Selon l'axiome de renommage (6.36), il faut choisir un nom qui n'a aucune occurrence libre dans } `0 \leq x < r,\ (\star y \mid 0 \leq y : x + y + n)'. \text{ Choisissons } `z' \text{ et appliquons (6.36). } \rangle \\
 & (\star z \mid (0 \leq x < r)[x := z] : (\star y \mid 0 \leq y : x + y + n)[x := z])[n := x + y] \\
= & \quad \langle \text{ La première substitution est une substitution simple. La deuxième peut se faire en appliquant (6.14), car } \neg\mathsf{libre}(`y', `x, z'). \rangle \\
 & (\star z \mid 0 \leq z < r : (\star y \mid (0 \leq y)[x := z] : (x + y + n)[x := z]))[n := x + y] \\
= & \quad \langle \text{ Substitution, deux fois } \rangle \\
 & (\star z \mid 0 \leq z < r : (\star y \mid 0 \leq y : z + y + n))[n := x + y] \\
= & \quad \langle \neg\mathsf{libre}(`z', `n, x + y'), \text{ (6.14) } \rangle \\
 & (\star z \mid (0 \leq z < r)[n := x + y] : (\star y \mid 0 \leq y : z + y + n)[n := x + y]) \\
= & \quad \langle \text{ La substitution de gauche peut se faire. Pour celle de droite, il faut renommer la variable de quantification selon (6.36), car (6.14) ne peut être appliquée, puisque } \mathsf{libre}(`y', `n, x + y'). \rangle \\
 & (\star z \mid 0 \leq z < r : (\star w \mid (0 \leq y)[y := w] : (z + y + n)[y := w])[n := x + y]) \\
= & \quad \langle \text{ Substitution, deux fois } \rangle \\
 & (\star z \mid 0 \leq z < r : (\star w \mid 0 \leq w : z + w + n)[n := x + y]) \\
= & \quad \langle \neg\mathsf{libre}(`w', `n, x + y'), \text{ (6.14) } \rangle \\
 & (\star z \mid 0 \leq z < r : (\star w \mid (0 \leq w)[n := x + y] : (z + w + n)[n := x + y])) \\
= & \quad \langle \text{ Substitution, deux fois } \rangle \\
 & (\star z \mid 0 \leq z < r : (\star w \mid 0 \leq w : z + w + x + y))
\end{array}
$$

(c) $(\star x \mid 0 \leq x < y : (\star y \mid 0 \leq y : x + y + n))$ ou
$(\star x \mid 0 \leq x < y : (\star z \mid 0 \leq z : x + z + n))$.

Voici quelques explications sur ces réponses, car la substitution dans la quantification interne pose un problème spécial.

$$
\begin{array}{ll}
 & (\star x \mid 0 \leq x < r : (\star y \mid 0 \leq y : x + y + n))[r := y] \\
= & \quad \langle \text{ (6.14), car } \neg\mathsf{libre}(`x', `r, y') \rangle \\
 & (\star x \mid 0 \leq x < y : (\star y \mid 0 \leq y : x + y + n)[r := y])
\end{array}
$$

Puisque libre('y','r, y'), il faudrait renommer la variable de quantification y, puis faire la substitution. Cependant, comme r n'apparaît pas dans la quantification, il n'y a aucune substitution à faire. Pour cette raison, il est aussi possible de ne pas renommer. Ceci explique les deux réponses.

3. Démontrez le théorème suivant, dans lequel $0 \leq n$.

$$(\sum i \mid 0 \leq i < n+1 : b[i]) \;=\; b[0] + (\sum i \mid 1 \leq i < n+1 : b[i])$$

Solution. La preuve est directe en utilisant le théorème Extraction d'un terme (6.40) avec la substitution $P := b[i]$ —notez que nous nous permettons d'utiliser les lois de l'arithmétique, comme $1 \leq i \;\equiv\; 0 < i$. On peut aussi donner une preuve qui n'utilise pas (6.40), histoire d'illustrer la manière de faire des preuves avec les quantificateurs :

$(\sum i \mid 0 \leq i < n+1 : b[i])$
$=$ ⟨ Arithmétique ⟩
$(\sum i \mid 0 \leq i < 1 \;\vee\; 1 \leq i < n+1 : b[i])$
$=$ ⟨ Division du domaine (6.25), avec $x, R, S, P := i,\; 0 \leq i < 1,\; 1 \leq i < n+1,\; b[i]$ (on a bien $0 \leq i < 1 \;\wedge\; 1 \leq i < n+1 \;\equiv$ faux, et toutes les quantifications sont définies, car les domaines sont finis) ⟩
$(\sum i \mid 0 \leq i < 1 : b[i]) \;+\; (\sum i \mid 1 \leq i < n+1 : b[i])$
$=$ ⟨ $0 \leq i < 1 \;\equiv\; i = 0$ & Comme ¬libre('i','0'), on peut appliquer l'axiome du point (6.21), avec $x, E, P := i, 0, b[i]$ ⟩
$(b[i])[i := 0] \;+\; (\sum i \mid 1 \leq i < n+1 : b[i])$
$=$ ⟨ Substitution ⟩
$b[0] + (\sum i \mid 1 \leq i < n+1 : b[i])$

4. Démontrez le théorème suivant, dans lequel $0 \leq n$.

$$(\wedge i \mid 0 \leq i < n+1 : b[i] = 0) \;\equiv\; b[0] = 0 \;\wedge\; (\wedge i \mid 0 < i < n+1 : b[i] = 0)$$

Solution. La preuve est directe par le théorème Extraction d'un terme (6.40), avec $P := b[i] = 0$. On peut aussi donner une preuve qui n'utilise pas (6.40) :

$(\wedge i \mid 0 \leq i < n+1 : b[i] = 0)$
$=$ ⟨ Arithmétique ⟩
$(\wedge i \mid 0 \leq i < 1 \;\vee\; 1 \leq i < n+1 : b[i] = 0)$
$=$ ⟨ Division du domaine pour quantificateur idempotent (6.29), avec $x, R, S, P := i,\; 0 \leq i < 1,\; 1 \leq i < n+1,\; b[i] = 0$ (toutes les quantifications sont définies, car les domaines sont finis) ⟩

$$
\begin{array}{ll}
& (\wedge i \mid 0 \leq i < 1 : b[i] = 0) \ \wedge \ (\wedge i \mid 1 \leq i < n+1 : b[i] = 0) \\
= & \quad \langle \ 0 \leq i < 1 \ \equiv \ i = 0 \ \ \& \text{ Comme } \neg\mathsf{libre}(\text{`}i\text{'},\text{`}0\text{'}), \text{ on peut appliquer} \\
& \quad \text{l'axiome du point (6.21), avec } x, E, P \ := \ i, 0, b[i] = 0 \ \rangle \\
& (b[i] = 0)[i \ := \ 0] \ \wedge \ (\wedge i \mid 1 \leq i < n+1 : b[i] = 0) \\
= & \quad \langle \text{ Substitution } \rangle \\
& b[0] = 0 \ \wedge \ (\wedge i \mid 1 \leq i < n+1 : b[i] = 0)
\end{array}
$$

5. Démontrez le théorème suivant.

$$(+i \mid 0 \leq i \leq n : i) \ = \ (+i \mid 0 \leq i \leq n \ \wedge \ \mathsf{pair}.i : i) \ + \ (+i \mid 0 \leq i \leq n \ \wedge \ \mathsf{impair}.i : i)$$

Solution. On voit facilement de manière intuitive que le domaine des i compris entre 0 et n de la quantification gauche est séparé en deux domaines du côté droit de l'équation ; ces domaines sont ceux des i pairs compris entre 0 et n et des i impairs compris entre 0 et n. Ils sont disjoints et leur disjonction est égale au domaine de la quantification gauche. Il est alors assez évident qu'il faut appliquer un axiome de division du domaine. Il y en a trois :

(a) (6.25) : c'est celui qui est appliqué ci-dessous.

(b) (6.27) : c'est l'axiome le plus général et il pourrait être appliqué. Toutefois, on remarque que le côté gauche de (6.27) ne correspond pas directement au côté gauche de notre problème, car il a deux quantifications au lieu d'une seule. C'est ce qui nous amène à essayer d'abord (6.25).

(c) (6.29), division du domaine pour un opérateur idempotent. Comme l'addition n'est pas idempotente, il ne peut s'appliquer.

Pour appliquer (6.25), identifions d'abord R et S. Comme ce sont les domaines des deux quantifications de droite dans (6.25), on tire immédiatement de notre problème les expressions suivantes :

$$
\begin{array}{l}
R \ := \ 0 \leq i \leq n \ \wedge \ \mathsf{pair}.i \ , \\
S \ := \ 0 \leq i \leq n \ \wedge \ \mathsf{impair}.i \ .
\end{array}
$$

Il reste à démontrer que $R \vee S$ est bien le domaine de la quantification gauche de notre problème et que $R \wedge S \ \equiv \ \mathsf{faux}$ (c'est une précondition de (6.25)). Voici ces preuves :

$$
\begin{array}{ll}
& R \vee S \\
= & \quad \langle \text{ Définition de } R \text{ et } S \ \rangle \\
& (0 \leq i \leq n \ \wedge \ \mathsf{pair}.i) \ \vee \ (0 \leq i \leq n \ \wedge \ \mathsf{impair}.i) \\
= & \quad \langle \text{ Distributivité de } \wedge \text{ sur } \vee \text{ (3.60)}, \\
& \quad \text{avec } p, q, r \ := \ 0 \leq i \leq n, \ \mathsf{pair}.i, \ \mathsf{impair}.i \ \rangle \\
& 0 \leq i \leq n \ \wedge \ (\mathsf{pair}.i \ \vee \ \mathsf{impair}.i) \\
= & \quad \langle \text{ Par définition de } \mathsf{pair} \text{ et } \mathsf{impair}, \text{ un nombre entier est soit pair, soit} \\
& \quad \text{impair. } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& 0 \le i \le n \ \wedge \ \mathsf{vrai} \\
= & \qquad \langle \text{ Identité de } \wedge \text{ (3.52), avec } p := 0 \le i \le n \ \rangle \\
& 0 \le i \le n
\end{array}
$$

et

$$
\begin{array}{ll}
& R \wedge S \\
= & \qquad \langle \text{ Définition de } R \text{ et } S \ \rangle \\
& (0 \le i \le n \ \wedge \ \mathsf{pair}.i) \ \wedge \ (0 \le i \le n \ \wedge \ \mathsf{impair}.i) \\
= & \qquad \langle \text{ Commutativité de } \wedge \text{ (3.49) } \ \& \ \text{ idempotence de } \wedge \text{ (3.51) } \rangle \\
& 0 \le i \le n \ \wedge \ \mathsf{pair}.i \ \wedge \ \mathsf{impair}.i \\
= & \qquad \langle \ \mathsf{pair}.i \wedge \mathsf{impair}.i \ \equiv \ \mathsf{faux} \ \ \& \ \text{ Zéro de } \wedge \text{ (3.53), avec } p := 0 \le i < n \\
& \qquad \rangle \\
& \mathsf{faux}
\end{array}
$$

Ces résultats sont maintenant utilisés :

$$
\begin{array}{ll}
& (+i \mid 0 \le i \le n : i) \\
= & \qquad \langle \text{ Résultats ci-dessus } \ \& \ \text{ Division du domaine (6.25),} \\
& \qquad \ \text{avec } x, R, S, P := i, \ 0 \le i \le n \wedge \mathsf{pair}.i, \ 0 \le i \le n \wedge \mathsf{impair}.i, \ i. \\
& \qquad \ \text{Toutes les quantifications sont définies, car les domaines sont finis.} \\
& \qquad \rangle \\
& (+i \mid 0 \le i \le n \wedge \mathsf{pair}.i : i) \ + \ (+i \mid 0 \le i \le n \wedge \mathsf{impair}.i : i)
\end{array}
$$

14.7 Problèmes du chapitre 7

1. Démontrez que la distributivité de $\wedge$ sur $\exists$ (7.4), c'est-à-dire $P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$ —pourvu que x ne soit pas libre dans P, ce qui, rappelons-le, signifie qu'il n'y a pas d'*occurrence* libre de x dans P— découle d'une expression similaire avec tous les domaines vrai : $P \wedge (\exists x \mid : Q) \equiv (\exists x \mid : P \wedge Q)$ (pourvu que x ne soit pas libre dans P). Ceci signifie que nous aurions pu utiliser un axiome plus simple.

   Solution.

$$
\begin{array}{ll}
& P \wedge (\exists x \mid R : Q) \\
= & \qquad \langle \text{ Transfert (7.1), avec } P := Q \ \rangle \\
& P \wedge (\exists x \mid : R \wedge Q) \\
= & \qquad \langle \text{ C'est la transformation donnée dans l'énoncé, avec } Q := R \wedge Q \\
& \qquad \ \& \ \neg \mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'}), \text{ par hypothèse } \rangle \\
& (\exists x \mid : P \wedge R \wedge Q) \\
= & \qquad \langle \text{ Transfert (7.1), avec } P := P \wedge Q \ \rangle \\
& (\exists x \mid R : P \wedge Q)
\end{array}
$$

2. Puisque $\vee$ est idempotent, la règle Division du domaine pour opérateur $\star$ idempotent (6.29) s'applique et donne

$$(\exists x \mid Q \vee R : P) \;\equiv\; (\exists x \mid Q : P) \vee (\exists x \mid R : P).$$

Cependant, il est possible de démontrer cette expression sans utiliser l'axiome (6.29). Développez une telle preuve. Il peut s'avérer utile d'amener Q et R dans le corps de la quantification.

Solution.

$$\begin{array}{ll} & (\exists x \mid Q : P) \vee (\exists x \mid R : P) \\ = & \quad \langle \text{ Transfert (7.1) deux fois : (1) avec } R := Q, \text{ (2) directement } \rangle \\ & (\exists x \mid\!: Q \wedge P) \vee (\exists x \mid\!: R \wedge P) \\ = & \quad \langle \text{ Distributivité (6.23), avec } P, Q, R := Q \wedge P,\ R \wedge P,\ \mathsf{vrai} \rangle \\ & (\exists x \mid\!: (Q \wedge P) \vee (R \wedge P)) \\ = & \quad \langle \text{ (3.60), avec } p, q, r := P, Q, R \rangle \\ & (\exists x \mid\!: (Q \vee R) \wedge P) \\ = & \quad \langle \text{ Transfert (7.1), avec } R := Q \vee R \rangle \\ & (\exists x \mid Q \vee R : P) \end{array}$$

3. Démontrez la loi Affaiblissement/renforcement du corps (7.11), c'est-à-dire

$$(\exists x \mid R : P) \;\Rightarrow\; (\exists x \mid R : P \vee Q).$$

La distributivité de $\exists$ sur $\vee$ peut être utile.

Solution.

$$\begin{array}{ll} & (\exists x \mid R : P \vee Q) \\ = & \quad \langle \text{ Distributivité de } \exists \text{ sur } \vee \text{ (6.23) } \rangle \\ & (\exists x \mid R : P) \vee (\exists x \mid R : Q) \\ \Leftarrow & \quad \langle \text{ Affaiblissement (3.92a), avec } p, q := (\exists x \mid R : P),\ (\exists x \mid R : Q) \rangle \\ & (\exists x \mid R : P) \end{array}$$

4. Démontrez le théorème (7.20a), c'est-à-dire

$$(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : R \Rightarrow P).$$

Solution. Pour cette preuve, il est assez clair qu'il faut transférer du domaine au corps, ce que permet la loi (7.17a). C'est un bel exemple de preuve qu'on peut faire en progressant par les deux bouts (après un transfert à chaque extrémité, on voit bien ce qu'il reste à faire).

$$
\begin{array}{ll}
 & (\forall x \mid Q \wedge R : P) \\
= & \quad \langle \text{ Transfert (7.17a) } \rangle \\
 & (\forall x \mid\!: Q \wedge R \Rightarrow P) \\
= & \quad \langle \text{ Transfert (3.81), avec } p, q, r := Q, R, P \rangle \\
 & (\forall x \mid\!: Q \Rightarrow (R \Rightarrow P)) \\
= & \quad \langle \text{ Transfert (7.17a) } \rangle \\
 & (\forall x \mid Q : R \Rightarrow P)
\end{array}
$$

5. Démontrez la loi (7.24), c'est-à-dire $(\forall x \mid R : \mathsf{vrai}) \equiv \mathsf{vrai}$.

Solution. Voici deux preuves :

(a)
$$
\begin{array}{ll}
 & (\forall x \mid R : \mathsf{vrai}) \\
= & \quad \langle \text{ De Morgan (7.15), avec } P := \mathsf{faux} \rangle \\
 & \neg(\exists x \mid R : \neg\mathsf{vrai}) \\
= & \quad \langle \text{ Définition de } \mathsf{faux} \text{ (3.11) } \rangle \\
 & \neg(\exists x \mid R : \mathsf{faux}) \\
= & \quad \langle \text{ (7.8) } \rangle \\
 & \neg\mathsf{faux} \\
= & \quad \langle \text{ Négation de } \mathsf{faux} \text{ (3.16) } \rangle \\
 & \mathsf{vrai}
\end{array}
$$

(b)
$$
\begin{array}{ll}
 & (\forall x \mid R : \mathsf{vrai}) \\
= & \quad \langle \text{ (7.22), avec } P := \mathsf{vrai} \ \ \& \ \ x \text{ n'est pas libre dans } \mathsf{vrai} \rangle \\
 & \mathsf{vrai} \vee (\forall x \mid\!: \neg R) \\
= & \quad \langle \text{ Zéro de } \vee \text{ (3.38), avec } p := (\forall x \mid\!: \neg R) \rangle \\
 & \mathsf{vrai}
\end{array}
$$

6. Démontrez que si x n'est pas libre dans Q,

$$(\exists x \mid\!: R) \ \Rightarrow \ \big((\forall x \mid R : P) \ \Rightarrow \ Q \ \equiv \ (\exists x \mid R : P \Rightarrow Q)\big).$$

Solution. Supposons l'antécédent et prouvons le conséquent.

$$
\begin{array}{ll}
 & (\forall x \mid R : P) \Rightarrow Q \\
= & \quad \langle \text{ Définition de l'implication (3.75), avec } p, q := (\forall x \mid R : P),\ Q \ \rangle \\
 & \neg(\forall x \mid R : P) \vee Q \\
= & \quad \langle \text{ De Morgan (7.16c) } \rangle \\
 & (\exists x \mid R : \neg P) \vee Q \\
= & \quad \langle \text{ Hypothèse } (\exists x \mid : R) \ \ \& \ \ \& \text{ Hypothèse } \neg\mathsf{libre}(\text{`}x\text{'},\text{`}Q\text{'}) \ \ \& \\
 & \quad \ \vee \text{ se distribue sur } \exists \text{ (7.7), avec } P, Q := Q, \neg P \ \rangle \\
 & (\exists x \mid R : \neg P \vee Q) \\
= & \quad \langle \text{ Définition de l'implication (3.75), avec } p, q := P, Q \ \rangle \\
 & (\exists x \mid R : P \Rightarrow Q)
\end{array}
$$

7. Traduisez les phrases suivantes en logique des prédicats.
   (a) Un cube d'entier n'est jamais pair. (Utilisez seulement l'addition et la multiplication ; n'utilisez pas la division, mod, ou des prédicats comme pair.x ou impair.x.)
   (b) Aucun entier n'est plus grand que tous les autres.

   Solution.
   (a) $(\forall z{:}\mathbb{Z} \mid : \neg(\exists i{:}\mathbb{Z} \mid : z \cdot z \cdot z = 2 \cdot i))$
   (b) $\neg(\exists z{:}\mathbb{Z} \mid : (\forall w{:}\mathbb{Z} \mid : z > w))$

8. Traduisez les formules suivantes en français. Ce faisant, ne faites pas qu'une simple traduction littérale ; essayez plutôt d'extraire la signification de chaque formule et de l'exprimer de manière naturelle en français.
   (a) $(\forall x{:}\mathbb{R} \mid x \neq m : f.x > f.m)$
   (b) $(\forall z{:}\mathbb{Z} \mid \mathsf{pair}.z : (\exists w{:}\mathbb{Z} \mid \mathsf{impair}.w : z = w + 1))$

   Solution.
   (a) $f.m$ est la valeur minimale de f. Ou encore : la fonction f atteint sa valeur minimale en m.
   (b) Tout entier pair est le successeur d'un entier impair.

9. Formalisez les phrases suivantes en logique des prédicats.
   (a) Tout le monde aime quelqu'un.
   (b) Il y a quelqu'un qui aime quelqu'un.

(c) Tout le monde aime tout le monde.
(d) Personne n'aime tout le monde.
(e) Il y a quelqu'un qui n'aime personne.

Solution. Soit P l'ensemble des personnes. Définissons $\mathsf{aime}(x, y)$: la personne x aime la personne y.
(a) $(\forall x{:}P \mid{:}\ (\exists y{:}P \mid{:}\ \mathsf{aime}(x, y)))$
(b) $(\exists x{:}P \mid{:}\ (\exists y{:}P \mid{:}\ \mathsf{aime}(x, y)))$
(c) $(\forall x{:}P \mid{:}\ (\forall y{:}P \mid{:}\ \mathsf{aime}(x, y)))$
(d) $\neg(\exists x{:}P \mid{:}\ (\forall y{:}P \mid{:}\ \mathsf{aime}(x, y)))$
(e) $(\exists x{:}P \mid{:}\ \neg(\exists y{:}P \mid{:}\ \mathsf{aime}(x, y)))$

14.8 Problèmes du chapitre 8

1. Démontrez par induction que pour tout $n \geq 0$,

$$(\sum i \mid 0 \leq i < n : 2 \cdot i + 1) \;=\; n^2.$$

Solution. Formalisation : La propriété à démontrer est

$$(\forall n{:}\mathbb{N} \mid{:}\ (\sum i \mid 0 \leq i < n : 2 \cdot i + 1) \;=\; n^2).$$

(a) Définition du prédicat d'induction P : Prenons comme prédicat d'induction

$$P.n : \quad (\sum i \mid 0 \leq i < n : 2 \cdot i + 1) \;=\; n^2.$$

Il faut montrer $(\forall n{:}\mathbb{N} \mid{:}\ P.n)$.
(b) Étape de base : Il faut prouver $P.0$, c'est-à-dire

$$(\sum i \mid 0 \leq i < 0 : 2 \cdot i + 1) \;=\; 0.$$

Ceci est immédiat par l'axiome du domaine vide (6.19).
(c) Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \mid{:}\ P.n \;\Rightarrow\; P(n+1))$. Supposons $P.n$ et montrons $P(n+1)$, c'est-à-dire

$$(\sum i \mid 0 \leq i < n+1 : 2 \cdot i + 1) \;=\; (n+1)^2.$$

$$\begin{array}{ll} & (\sum i \mid 0 \leq i < n+1 : 2 \cdot i + 1) \\ = & \quad \langle \text{ Extraction d'un terme (6.40) } \rangle \\ & (\sum i \mid 0 \leq i < n : 2 \cdot i + 1) + 2 \cdot n + 1 \\ = & \quad \langle \text{ Hypothèse d'induction } P.n \rangle \\ & n^2 + 2 \cdot n + 1 \\ = & \quad \langle \text{ Arithmétique } \rangle \\ & (n+1)^2 \end{array}$$

2. Démontrez par induction sur n que $n^2 \leq 2^n$ pour tout $n \geq 4$.

   Solution. Formalisation : Il faut montrer

   $$(\forall n{:}\mathbb{N} \mid n \geq 4 : n^2 \leq 2^n).$$

   (a) Définition du prédicat d'induction P : Prenons comme prédicat d'induction

   $$P.n : \quad n^2 \leq 2^n.$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid n \geq 4 : P.n)$.

   (b) Étape de base : il faut prouver $P.4$, c'est-à-dire $4^2 \leq 2^4$, ce qui est immédiat, puisque $4^2 = 16 = 2^4$.

   (c) Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \mid n \geq 4 : P.n \Rightarrow P(n+1))$. Supposons $P.n$ et $n \geq 4$, et montrons $P(n+1)$, c'est-à-dire

   $$(n+1)^2 \leq 2^{n+1}.$$

   $$\begin{array}{ll} & (n+1)^2 \\ = & \quad \langle \text{ Arithmétique } \rangle \\ & n^2 + 2 \cdot n + 1 \\ \leq & \quad \langle \text{ Hypothèse d'induction } P.n \ \ \& \ \text{ Monotonie de } + \rangle \\ & 2^n + 2 \cdot n + 1 \\ < & \quad \langle \text{ Hypothèse } n \geq 4 \ \ \& \ \text{On peut montrer par induction que } \\ & \quad 2 \cdot n + 1 < 2^n \text{ pour tout } n \geq 3 \ \ \& \ \text{ Monotonie de } + \rangle \\ & 2^n + 2^n \\ = & \quad \langle \text{ Arithmétique } \rangle \\ & 2 \cdot 2^n \\ = & \quad \langle \text{ Propriété de l'exponentiation } \rangle \\ & 2^{n+1} \end{array}$$

3. Démontrez par induction que si $x \neq y$, alors $x^n - y^n$ est divisible par $x - y$, pour tout $n \geq 0$. Indice : soustrayez et additionnez $x \cdot y^n$ à $x^{n+1} - y^{n+1}$.

   Solution. Le type des variables x et y n'est pas clair à partir de l'énoncé. Toutefois, si elles étaient réelles, le problème de divisibilité ne se poserait pas. Nous pouvons donc supposer qu'elles sont entières, c'est-à-dire $x, y{:}\mathbb{Z}$. Si nous supposions $x, y{:}\mathbb{N}$, cela poserait le problème que $x - y$ n'est pas nécessairement une valeur de $\mathbb{N}$, car $x - y$ peut être négatif ; il vaut mieux travailler entièrement sur $\mathbb{Z}$.
   Nous utiliserons la notation $x \,|\, y$, qui signifie « x divise y », ce qui est équivalent à « y est divisible par x ». Comme

   $$x \,|\, y \ \equiv \ (\exists z{:}\mathbb{Z} \mid : y = x \cdot z),$$

il serait possible d'utiliser cette dernière expression. Toutefois, cela ne ferait qu'alourdir la preuve. Remarquons qu'avec cette définition de $x \,|\, y$, on a que 0 divise 0. Dans ce cas, la condition $x \neq y$ n'est pas vraiment nécessaire dans l'énoncé de notre problème. Toutefois le résultat de la division de 0 par 0 est quelconque, et $0/0$ n'est pas défini. Si on voulait imposer que 0 ne divise pas 0, il faudrait alors écrire

$$x \,|\, y \;\equiv\; x \neq 0 \;\wedge\; (\exists z \,|:\, y = x \cdot z).$$

L'expression à démontrer est

$$x \neq y \;\Rightarrow\; (\forall n{:}\mathbb{N} \,|:\, (x-y) \,|\, (x^n - y^n)).$$

Assumons l'antécédent et montrons le conséquent par induction.

(a) Définition du prédicat d'induction P : Prenons comme prédicat d'induction

$$P.n: \quad (x-y) \,|\, (x^n - y^n).$$

Il faut montrer $(\forall n{:}\mathbb{N} \,|:\, P.n)$.

(b) Étape de base : il faut prouver $P.0$.

$$\begin{array}{ll} & P.0 \\ = & \quad \langle \text{ Définition de } P \rangle \\ & (x-y) \,|\, (x^0 - y^0) \\ = & \quad \langle\; x^0 = y^0 = 1 \;\rangle \\ & (x-y) \,|\, 0 \\ = & \quad \langle \text{ Tout nombre différent de 0 divise 0 } \;\&\; \text{ Hypothèse } x \neq y \;\rangle \\ & \mathsf{vrai} \end{array}$$

Nous pourrions aussi dire : Il faut prouver $P.0$, c'est-à-dire $(x-y) \,|\, (x^0 - y^0)$. Comme $x^0 = y^0 = 1$, on voit que $x^0 - y^0 = 0$, et comme $x \neq y$ et que tout nombre différent de 0 divise 0, $P.0$ est vrai.

(c) Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \,|:\, P.n \;\Rightarrow\; P(n+1))$. Supposons $P.n$ et montrons $P(n+1)$, c'est-à-dire

$$(x-y) \,|\, (x^{n+1} - y^{n+1}).$$

$$\begin{array}{ll} & (x-y) \,|\, (x^{n+1} - y^{n+1}) \\ = & \quad \langle \text{ Arithmétique } \;\&\; \text{ Indice donné } \rangle \\ & (x-y) \,|\, (x^{n+1} - x \cdot y^n + x \cdot y^n - y^{n+1}) \\ = & \quad \langle \text{ Factorisation et lois de l'exponentiation } \rangle \\ & (x-y) \,|\, \big(x \cdot (x^n - y^n) + (x-y) \cdot y^n\big) \\ \Leftarrow & \quad \langle \text{ Arithmétique : quels que soient } s,t,u,\; s \,|\, t \;\wedge\; s \,|\, u \;\Rightarrow\; s \,|\, (t+u) \\ & \quad \rangle \end{array}$$

$$
\begin{array}{ll}
 & (x-y) \,|\, \big(x \cdot (x^n - y^n)\big) \;\wedge\; (x-y) \,|\, \big((x-y) \cdot y^n\big) \\
= & \qquad \langle \text{ Hypothèse d'induction } P.n \;\;\&\;\; \text{Arithmétique : } s|(t \cdot u) \text{ si } s|t \;\rangle \\
 & \mathsf{vrai} \wedge \mathsf{vrai} \\
= & \qquad \langle \text{ Identité de } \wedge \text{ (3.52), avec } p := \mathsf{vrai} \;\rangle \\
 & \mathsf{vrai}
\end{array}
$$

Nous pourrions aussi utiliser la présentation suivante :

$$
\begin{array}{ll}
 & x^{n+1} - y^{n+1} \\
= & \qquad \langle \text{ Arithmétique } \;\&\; \text{ Indice donné } \rangle \\
 & x^{n+1} - x \cdot y^n + x \cdot y^n - y^{n+1} \\
= & \qquad \langle \text{ Factorisation et lois de l'exponentiation } \rangle \\
 & x \cdot (x^n - y^n) + (x-y) \cdot y^n
\end{array}
$$

Par l'hypothèse d'induction, $x - y$ divise le premier terme. Puisque l divise $l \cdot m$, quels que soient l et m, on voit que $x-y$ divise le deuxième terme. Par conséquent, $x - y$ divise leur somme et divise donc $x^{n+1} - y^{n+1}$.

4. Montrez par induction que $F_n < 2^n$, pour tout $n \geq 0$.

   Solution. Formalisation : La propriété à démontrer est

   $$(\forall n{:}\mathbb{N} \mid{:}\; F_n < 2^n).$$

   (a) Définition du prédicat d'induction P : Choisissons comme prédicat d'induction

   $$P.n : \quad F_n < 2^n.$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:}\; P.n)$.

   (b) Étape de base 1 : il faut prouver $P.0$, c'est-à-dire $F_0 < 2^0$. Par la définition (8.11) et en utilisant des propriétés mathématiques simples,

   $$F_0 = 0 < 1 = 2^0 \ .$$

   (c) Étape de base 2 : il faut prouver $P.1$, c'est-à-dire $F_1 < 2^1$. Par la définition (8.11) et en utilisant des propriétés mathématiques simples,

   $$F_1 = 1 < 2 = 2^1.$$

   (d) Étape d'induction : Nous devons montrer

   $$(\forall n{:}\mathbb{N} \mid{:}\; P.n \;\wedge\; P(n+1) \;\Rightarrow\; P(n+2))$$

   Supposons $P.n$ et $P(n+1)$, et montrons $P(n+2)$, c'est-à-dire $F_{n+2} < 2^{n+2}$.

$$
\begin{array}{ll}
& F_{n+2} \\
= & \quad \langle \text{ Définition des nombres de Fibonacci (8.11) (on peut utiliser la définition inductive, car } n+2>1) \rangle \\
& F_{n+1} + F_n \\
< & \quad \langle \text{ Hypothèses d'induction } P.n \text{ et } P(n+1) \rangle \\
& 2^{n+1} + 2^n \\
< & \quad \langle \text{ Arithmétique} \rangle \\
& 2^{n+1} + 2^{n+1} \\
= & \quad \langle \text{ Arithmétique} \rangle \\
& 2^{n+2}
\end{array}
$$

5. Montrez par induction que $F_n = (\phi^n - \hat{\phi}^n)/\sqrt{5}$, pour tout $n \geq 0$.

   Solution. Rappelons la définition de ϕ et $\hat{\phi}$ (page 95) :

   $$\phi = (1+\sqrt{5})/2 \qquad \text{et} \qquad \hat{\phi} = (1-\sqrt{5})/2.$$

   La propriété à démontrer est

   $$(\forall n{:}\mathbb{N} \mid{:}\ F_n = (\phi^n - \hat{\phi}^n)/\sqrt{5}).$$

   (a) Définition du prédicat d'induction P : Choisissons comme prédicat d'induction

   $$P.n: \quad F_n = (\phi^n - \hat{\phi}^n)/\sqrt{5}.$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid{:}\ P.n)$.

   (b) Étape de base 1 : Il faut prouver $P.0$, c'est-à-dire $F_n = (\phi^0 - \hat{\phi}^0)/\sqrt{5}$. Par la définition (8.11) et en utilisant des propriétés mathématiques simples,

   $$F_0 = 0 = (1-1)/\sqrt{5} = (\phi^0 - \hat{\phi}^0)/\sqrt{5}.$$

   (c) Étape de base 2 : Il faut prouver $P.1$, c'est-à-dire $F_1 = (\phi^1 - \hat{\phi}^1)/\sqrt{5}$.

$$
\begin{array}{ll}
& (\phi^1 - \hat{\phi}^1)/\sqrt{5} \\
= & \quad \langle \text{ Arithmétique } (x^1 = x \text{ pour tout } x) \ \ \& \ \ \text{Définition de } \phi \text{ et } \hat{\phi} \rangle \\
& \big((1+\sqrt{5})/2) - (1-\sqrt{5})/2\big)/\sqrt{5} \\
= & \quad \langle \text{ Arithmétique} \rangle \\
& 1 \\
= & \quad \langle \text{ Définition des nombres de Fibonacci (8.11} \rangle \\
& F_1
\end{array}
$$

(d) Étape d'induction : Nous devons montrer

$$(\forall n{:}\mathbb{N} \mid{:}\ P.n \ \wedge\ P(n+1) \ \Rightarrow\ P(n+2)).$$

Supposons $P.n$ et $P(n+1)$, et montrons $P(n+2)$, c'est-à-dire

$$F_{n+2} = (\phi^{n+2} - \hat{\phi}^{n+2})/\sqrt{5}.$$

$$\begin{array}{ll} & F_{n+2} \\ = & \quad \langle\ \text{Définition des nombres de Fibonacci (8.11) (on peut utiliser la définition inductive, car } n+2 > 1)\ \rangle \\ & F_{n+1} + F_n \\ = & \quad \langle\ \text{Hypothèses d'induction } P.n \text{ et } P(n+1)\ \rangle \\ & (\phi^{n+1} - \hat{\phi}^{n+1})/\sqrt{5} + (\phi^n - \hat{\phi}^n)/\sqrt{5} \\ = & \quad \langle\ \text{Factorisation}\ \rangle \\ & \big(\phi^n \cdot (\phi+1) - \hat{\phi}^n \cdot (\hat{\phi}+1)\big)/\sqrt{5} \\ = & \quad \langle\ (8.13)\ \rangle \\ & (\phi^n \cdot \phi^2 - \hat{\phi}^n \cdot \hat{\phi}^2)/\sqrt{5} \\ = & \quad \langle\ \text{Arithmétique}\ \rangle \\ & (\phi^{n+2} - \hat{\phi}^{n+2})/\sqrt{5} \end{array}$$

14.9 Problèmes du chapitre 9

1. Démontrez le théorème de substitution (9.3b),

$$e = f \ \Rightarrow\ E[z := e] \ \equiv\ e = f \ \Rightarrow\ E[z := f].$$

Solution. Voici deux preuves. La première est la plus directe. Cependant, si on ne réalise pas que la loi (3.79) donne immédiatement la réponse, on peut s'en sortir quand même. On se doute bien qu'il faut utiliser l'axiome de Leibniz (9.1), car c'est l'une des deux seules lois applicables qui contient $e = f$. La deuxième preuve part de cet axiome et élimine l'implication.

(a)
$$\begin{array}{ll} & e = f \ \Rightarrow\ E[z := e] \ \equiv\ e = f \ \Rightarrow\ E[z := f] \\ = & \quad \langle\ \text{Distributivité de } \Rightarrow \text{ sur } \equiv \text{ (3.79)}, \\ & \quad\ \text{avec } p, q, r := e = f,\ E[z := e],\ E[z := f]\ \rangle \\ & e = f \ \Rightarrow\ (E[z := e] \equiv E[z := f]) \qquad \text{—Axiome de Leibniz (9.1)} \end{array}$$

Remarquons que l'axiome de Leibniz est utilisé avec $\equiv$ au lieu de $=$ entre les expressions $E[z := e]$ et $E[z := f]$. C'est correct, car ces expressions sont booléennes (ça se voit en regardant la loi à démontrer).

(b) La preuve débute avec l'axiome de Leibniz dans lequel $\equiv$ remplace l'une des égalités (voir la note à l'item précédent).

$$
\begin{array}{ll}
& e = f \;\Rightarrow\; (E[z := e] \equiv E[z := f]) \qquad \text{—Axiome de Leibniz (9.1)} \\
= & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75), avec } p, q := e = f,\ E[z := e] \equiv E[z := f] \rangle \\
& \neg(e = f) \;\vee\; (E[z := e] \equiv E[z := f]) \\
= & \qquad \langle \text{ Distributivité de } \vee \text{ sur } \equiv \text{ (3.36), avec } p, q, r := \neg(e = f),\ E[z := e],\ E[z := f] \rangle \\
& \neg(e = f) \;\vee\; E[z := e] \;\equiv\; \neg(e = f) \;\vee\; E[z := f]) \\
= & \qquad \langle \text{ Définition de } \Rightarrow \text{ (3.75) deux fois} \\
& \qquad\quad \text{(1) avec } p, q := e = f,\ E[z := e] \\
& \qquad\quad \text{(2) avec } p, q := e = f,\ E[z := f] \rangle \\
& e = f \;\Rightarrow\; E[z := e] \;\equiv\; e = f \;\Rightarrow\; E[z := f]
\end{array}
$$

2. Démontrez le théorème d'affaiblissement/renforcement (3.92e), $p \wedge q \;\Rightarrow\; p \wedge (q \vee r)$, en utilisant le remplacement par vrai (9.4b). Normalement, il n'est pas permis d'utiliser un théorème qui suit le théorème à démontrer, mais puisque l'exercice le demande, c'est ce qu'il faut faire.

Solution.

$$
\begin{array}{ll}
& p \wedge q \;\Rightarrow\; p \wedge (q \vee r) \\
= & \qquad \langle \text{ Remplacement de } p \text{ par vrai dans le conséquent (9.4b), avec } E := z \wedge (q \vee r) \rangle \\
& p \wedge q \;\Rightarrow\; \mathsf{vrai} \wedge (q \vee r) \\
= & \qquad \langle \text{ Remplacement de } q \text{ par } \mathsf{vrai} \text{ dans le conséquent (9.4b), avec } p, q := q, p \text{ et } E := \mathsf{vrai} \wedge (z \vee r) \rangle \\
& p \wedge q \;\Rightarrow\; \mathsf{vrai} \wedge (\mathsf{vrai} \vee r) \\
= & \qquad \langle \text{ Absorption (3.61a), avec } p, q := \mathsf{vrai}, r \rangle \\
& p \wedge q \;\Rightarrow\; \mathsf{vrai} \qquad \text{—Zéro à droite de } \Rightarrow \text{ (3.88), avec } p := p \wedge q
\end{array}
$$

3. Soit $x \downarrow y$ le minimum de deux entiers, défini par

$$x \downarrow y \;=\; (\textbf{si } x \leq y \textbf{ alors } x \textbf{ sinon } y).$$

Montrez que $\downarrow$ est commutatif, c'est-à-dire $b \downarrow c = c \downarrow b$. Combien de cas devez-vous considérer ? Vous pouvez utiliser les règles usuelles de l'arithmétique des entiers, comme $b \leq c \;\equiv\; b = c \vee b < c$ et $b < c \equiv c > b$.

Solution. Nous considérerons trois cas : $b < c, b = c$ et $b > c$. Sur les entiers, il est clair que $b < c \;\vee\; b = c \;\vee\; b > c$ est un théorème.

(a) Cas $b < c$: supposons $b < c$ et montrons $b \downarrow c = c \downarrow b$.

$$
\begin{array}{ll}
 & b \downarrow c \\
= & \qquad \langle \text{ Définition de } \downarrow \rangle \\
 & \textbf{si } b \leq c \textbf{ alors } b \textbf{ sinon } c \\
= & \qquad \langle \text{ Hypothèse } b < c, \text{ d'où } b \leq c \rangle \\
 & b \\
= & \qquad \langle \text{ Hypothèse } b < c, \text{ d'où } c > b, \text{ d'où } \neg(c \leq b) \rangle \\
 & \textbf{si } c \leq b \textbf{ alors } c \textbf{ sinon } b \\
= & \qquad \langle \text{ Définition de } \downarrow \rangle \\
 & c \downarrow b
\end{array}
$$

(b) Cas $b = c$: supposons $b = c$ et montrons $b \downarrow c = c \downarrow b$.

$$
\begin{array}{ll}
 & b \downarrow c \\
= & \qquad \langle \text{ Définition de } \downarrow \rangle \\
 & \textbf{si } b \leq c \textbf{ alors } b \textbf{ sinon } c \\
= & \qquad \langle \text{ Hypothèse } b = c, \text{ d'où } b \leq c \rangle \\
 & b \\
= & \qquad \langle \text{ Hypothèse } b = c \rangle \\
 & c \\
= & \qquad \langle \text{ Hypothèse } b = c, \text{ d'où } c \leq b \rangle \\
 & \textbf{si } c \leq b \textbf{ alors } c \textbf{ sinon } b \\
= & \qquad \langle \text{ Définition de } \downarrow \rangle \\
 & c \downarrow b
\end{array}
$$

(c) Cas $b > c$: supposons $b > c$ et montrons $b \downarrow c = c \downarrow b$.

$$
\begin{array}{ll}
 & b \downarrow c \\
= & \qquad \langle \text{ Définition de } \downarrow \rangle \\
 & \textbf{si } b \leq c \textbf{ alors } b \textbf{ sinon } c \\
= & \qquad \langle \text{ Hypothèse } b > c, \text{ d'où } \neg(b \leq c) \rangle \\
 & c \\
= & \qquad \langle \text{ Hypothèse } b > c, \text{ d'où } c \leq b \rangle \\
 & \textbf{si } c \leq b \textbf{ alors } c \textbf{ sinon } b \\
= & \qquad \langle \text{ Définition de } \downarrow \rangle \\
 & c \downarrow b
\end{array}
$$

14.10 Problèmes du chapitre 10

1. Considérez un segment de tableau $b[0..n-1]$, où $0 \leq n$. Soient j et k deux variables entières satisfaisant $0 \leq j \leq k < n$. La notation $b[j..k]$ désigne le sous-tableau de b qui consiste en $b[j], b[j+1], \ldots, b[k]$. Le segment $b[j..k]$ est vide si $j = k+1$.

   Traduisez les phrases suivantes en expressions booléennes. Par exemple, la première peut s'écrire $(\forall i \mid j \leq i \leq k : b[i] = 0)$. Certains énoncés sont ambigus ; dans ce cas, écrivez toutes les interprétations raisonnables. Simplifiez les expressions lorsque c'est possible. Vous pouvez utiliser des abréviations —par exemple, $x \in b[0..n-1]$ au lieu de $(\exists i \mid 0 \leq i < n : x = b[i])$.

   (a) Tous les éléments de $b[j..k]$ sont nuls.

   (b) Les valeurs de $b[0..n-1]$ qui ne sont pas dans $b[j..k]$ sont dans $b[j..k]$.

   (c) Chaque élément de $b[0..j]$ est moindre que x et chaque valeur de $b[j+1..k-1]$ excède x.

   Solution.

   (a) $(\forall i \mid j \leq i \leq k : b[i] = 0)$, ou encore $\neg(\exists i \mid j \leq i \leq k : b[i] \neq 0)$.

   (b) Au premier abord, cette phrase semble contradictoire, mais il s'avère que ce n'est pas le cas. Tout d'abord, réécrivons-la comme suit :

   > Pour tout v dans $b[0..n-1]$, si v n'est pas dans $b[j..k]$, alors v est dans $b[j..k]$.

   Nous ne pouvons prouver que c'est une traduction correcte de la phrase donnée, car les deux sont en français et le français est ambigu (ce n'est pas un langage formel). Cependant, si nous sommes d'accord sur l'équivalence des deux phrases, nous pouvons poursuivre. Nous traduisons la deuxième phrase ainsi :

   $$(\forall v \mid v \in b[0..n-1] : v \notin b[j..k] \;\Rightarrow\; v \in b[j..k]).$$

   Nous pouvons maintenant simplifier cette expression :

   $$\begin{array}{ll} & (\forall v \mid v \in b[0..n-1] : \neg(v \in b[j..k]) \;\Rightarrow\; v \in b[j..k]) \\ = & \quad \langle \text{ Définition de l'implication (3.75),} \\ & \quad\quad \text{avec } p, q := v \in b[j..k],\ v \in b[j..k] \ \rangle \\ & (\forall v \mid v \in b[0..n-1] : \neg\neg(v \in b[j..k]) \;\vee\; v \in b[j..k]) \\ = & \quad \langle \text{ Double négation (3.15), avec } p := v \in b[j..k] \ \rangle \\ & (\forall v \mid v \in b[0..n-1] : v \in b[j..k] \;\vee\; v \in b[j..k]) \\ = & \quad \langle \text{ Idempotence de } \vee \text{ (3.34), avec } p := v \in b[j..k] \ \rangle \\ & (\forall v \mid v \in b[0..n-1] : v \in b[j..k]) \end{array}$$

   Cette formule peut être retraduite en français ainsi : chaque valeur de $b[0..n-1]$ est aussi une valeur de $b[j..k]$.

(c) $(\forall i \mid 0 \le i \le j : b[i] < x) \wedge (\forall i \mid j+1 \le i < k : b[i] > x)$, ou encore $(\forall y \mid y \in b[0..j] : y < x) \wedge (\forall y \mid y \in b[j+1..k-1] : y > x)$.

Exercice : montrez l'équivalence de ces deux formulations, en remplaçant les abréviations par leur définition. C'est intuitivement évident, mais ce n'est pas si facile à montrer.

Étendons la définition des relations $=, <$, etc., aux paires (*entier*, *tableau*), ou aux paires (*tableau*, *entier*) —par exemple, $x < b[0..j]$ est equivalent à

$$(\forall i \mid 0 \le i \le j : x < b[i]).$$

On peut alors abrévier la première formule de la manière suivante : $b[0..j] < x < b[j+1..k-1]$.

2. Formalisez les spécifications suivantes énoncées en français. Assurez-vous d'introduire les restrictions nécessaires. De plus, si certaines parties de la spécification sont ambigües, résolvez-les d'une manière raisonnable (il peut y avoir plus d'une réponse). Vous pouvez écrire $x \uparrow y$ pour le maximum de x et y. Notez que $\uparrow$ est commutatif et associatif, et peut donc être utilisé comme quantificateur (voyez le chapitre 6). Cependant, $\uparrow$ sur $\mathbb{Z}$ n'a pas d'élément identité (élément neutre), et donc certains axiomes qui requièrent cette propriété ne s'appliquent pas.

(a) Le tableau b contient la liste des étudiants de l'Université Laval et le tableau c contient la liste des personnes qui ont un emploi à temps partiel dans la région de Québec. Les deux listes sont triées alphabétiquement. Trouvez la première personne qui apparaît dans les deux listes.

(b) Le tableau b est trié en ordre non décroissant. Trouvez l'indice de l'élément le plus à droite (c'est-à-dire l'élément avec l'indice le plus élevé) qui égale x. Tenez compte du cas où x n'est pas dans b.

Solution.

(a) Supposons que les tableaux sont $b[0..m-1]$ et $c[0..n-1]$. Supposons aussi qu'il y a au moins un nom qui apparaît dans les deux tableaux. La précondition suivante exprime cette supposition et elle exprime aussi que b et c sont triés (la relation $\le$ sur les entrées des tableaux est une relation sur l'ensemble des noms).

$$\begin{aligned} Q: \quad & (\exists i, j \mid 0 \le i < m \wedge 0 \le j < n : b[i] = c[j]) \\ & \wedge (\forall i \mid 0 \le i < m-1 : b[i] \le b[i+1]) \\ & \wedge (\forall i \mid 0 \le i < n-1 : c[i] \le c[i+1]). \end{aligned}$$

Il n'est pas nécessaire d'ajouter $0 \le m$ et $0 \le n$ dans la précondition ; en effet, ceci découle de Q. Par exemple, $0 \le m$ découle de l'existence d'un i tel que $0 \le i < m$. Exigeons que les indices de la première personne qui apparaît dans les deux tableaux soient mis dans les variables h et k, de sorte que la postcondition est

$$R: b[h] = c[k] \wedge (\forall i \mid 0 \le i < h : b[i] \notin c[0..k]) \wedge (\forall j \mid 0 \le j < k : c[j] \notin b[0..h]).$$

La spécification est alors $\{Q\}\ \ h, k := ?\ \ \{R\}$.

(b) Soit le tableau $b[0..n-1]$. Nous spécifions que l'algorithme doit placer dans i l'indice de l'élément le plus à droite qui égale x, si x est dans b, et qu'il doit donner à i la valeur -1 dans le cas contraire (il faut choisir une valeur qui n'est pas un indice de b). La spécification est

$$\{Q\}\ \ i := ?\ \ \{R\},$$

où

$$Q : 0 \leq n\ \wedge\ (\forall i \mid 0 \leq i < n-1 : b[i] \leq b[i+1])$$

et

$$R : (x \notin b[0..n-1] \wedge i = -1) \vee (x = b[i] \wedge 0 \leq i < n \wedge x \notin b[i+1..n-1]).$$

Le premier opérande de $\vee$ traite le cas où x n'est pas dans le tableau. Le deuxième opérande traite l'autre cas.

Le fait d'ajouter $0 \leq n$ dans la précondition ajoute une contrainte de « réalisme », car elle élimine les tableaux avec un nombre négatif de cases. Elle n'est cependant pas critique. Supposons qu'on prend comme précondition

$$Q' : (\forall i \mid 0 \leq i < n-1 : b[i] \leq b[i+1]).$$

Prenons $n = -1$. Dans ce cas,

$$\begin{array}{ll} & Q' \\ = & \quad \langle\ \text{Définition de } Q' \text{ et de } n\ \rangle \\ & (\forall i \mid 0 \leq i < -2 : b[i] \leq b[i+1]) \\ = & \quad \langle\ 0 \leq i < 2\ \equiv\ \mathsf{faux}\ \rangle \\ & (\forall i \mid \mathsf{faux} : b[i] \leq b[i+1]) \\ = & \quad \langle\ \text{Domaine vide (6.19), avec } P := b[i] \leq b[i+1], \text{ en notant que} \\ & \quad \text{l'élément neutre de } \wedge \text{ est } \mathsf{vrai}\ \rangle \\ & \mathsf{vrai} \end{array}$$

D'autre part,

$$\begin{array}{ll} & R \\ = & \quad \langle\ \text{Définition de } R \text{ et de } n\ \rangle \\ & (x \notin b[0..-2] \wedge i = -1) \vee (x = b[i] \wedge 0 \leq i < -1 \wedge x \notin b[i+1..-2]) \\ = & \quad \langle\ x \notin b[0..-2]\ \equiv\ \mathsf{vrai}\ \ \&\ \ 0 \leq i < -1\ \equiv\ \mathsf{faux}\ \rangle \\ & (\mathsf{vrai} \wedge i = -1) \vee (x = b[i] \wedge \mathsf{faux} \wedge x \notin b[i+1..-2]) \\ = & \quad \langle\ \text{Identité de } \wedge \text{ (3.52), avec } p := i = -1\ \ \& \\ & \quad\ \ \text{Zéro de } \wedge \text{ (3.53), avec } p := x = b[i] \wedge x \notin b[i+1..-2]\ \rangle \\ & i = -1 \vee \mathsf{faux} \\ = & \quad \langle\ \text{Identité de } \vee \text{ (3.40), avec } p := i = -1\ \rangle \\ & i = -1 \end{array}$$

Un programme qui implanterait cette spécification devrait terminer pour n'importe quel état initial en donnant à i la valeur -1, qui indique que x n'est pas dans le tableau, ce qui est correct.

Dans cet exercice, nous avons utilisé la propriété $(\forall x \mid \mathsf{faux} : P) \equiv \mathsf{vrai}$, qui découle de la loi (6.19). C'est une propriété qui est souvent utilisée et qu'il faut mémoriser.

3. Formalisez les spécifications suivantes. Certaines requièrent l'emploi de variables rigides pour indiquer les modifications aux variables du programme. Assurez-vous d'indiquer les restrictions nécessaires sur les entrées. Si la spécification française est ambigüe ou vague, précisez-la d'une manière convenable (il peut y avoir plus d'une manière).
   (a) Doublez la valeur de chaque élément du tableau d'entiers b.
   (b) Permutez les tableaux b et c.

   Solution.
   (a) Supposons $b[0..n-1]$:tableau. La spécification est alors

   $$\{b = \mathsf{B}\} \quad b := ? \quad \{(\forall i \mid 0 \leq i < n : b[i] = 2 \cdot \mathsf{B}[i])\}$$

   (b) Cette spécification est ambigüe. On se demande s'il faut permuter b et permuter c, ou bien s'il faut interchanger b et c (les permuter). C'est cette dernière interprétation que nous retenons. Voici une spécification possible :

   $$\{b = \mathsf{B} \wedge c = \mathsf{C}\} \quad b, c := ? \quad \{b = \mathsf{C} \wedge c = \mathsf{B}\}.$$

   On traite ici les tableaux b et c comme des variables entières ou réelles. Toutefois, certains langages ne permettraient pas d'implanter cette spécification. Pour plusieurs langages, la taille d'un tableau fait partie du type et la spécification ci-dessus pourrait être implantée seulement si la taille des tableaux est la même, c'est-à-dire seulement si

   $$b[0..n-1]\text{:tableau} \quad \text{et} \quad c[0..n-1]\text{:tableau}.$$

   Avec une telle déclaration, nous pouvons aussi donner la spécification suivante :

   $$\{b = \mathsf{B} \wedge c = \mathsf{C}\} \quad b, c := ? \quad \{(\forall i \mid 0 \leq i < n : b[i] = \mathsf{C}[i] \wedge c[i] = \mathsf{B}[i])\}.$$

4. Utilisez la méthode (10.33) pour démontrer que le programme annoté suivant est correct. Considérez que les variables ont le type x, y, z:$\mathbb{Z}$. La division / est alors la division entière qui tronque le résultat s'il est fractionnaire (ainsi, $6/2 = 3$ et $5/2 = 2$).

   $\{y > 0 \wedge z \cdot x^y = \mathsf{X}\}$
   if impair.y **then** $z, y := z \cdot x,\ y - 1$ **else** $x, y := x \cdot x,\ y/2$
   $\{y \geq 0 \wedge z \cdot x^y = \mathsf{X}\}$

Solution. Selon (10.33), il y a deux cas à démontrer, soit

$$\{Q \wedge B\}\ \ S_1\ \ \{R\} \quad \text{et} \quad \{Q \wedge \neg B\}\ \ S_2\ \ \{R\},$$

avec

$$\begin{array}{l} B := \mathsf{impair}.y \\ Q := y > 0 \wedge z \cdot x^y = \mathsf{X} \\ R := y \geq 0 \wedge z \cdot x^y = \mathsf{X} \\ S_1 := (z, y := z \cdot x,\ y - 1) \\ S_2 := (x, y := x \cdot x,\ y/2) \end{array}$$

(a) $\{Q \wedge B\}\ \ S_1\ \ \{R\}$

$$\begin{array}{ll} & \{Q \wedge B\}\ \ S_1\ \ \{R\} \\ = & \quad \langle \text{ Définition de } Q,\ B,\ S_1 \text{ et } R \ \rangle \\ & \{y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{impair}.y\}\ \ z, y := z \cdot x,\ y - 1\ \ \{y \geq 0 \wedge z \cdot x^y = \mathsf{X}\} \\ = & \quad \langle \text{ (10.20) } \rangle \\ & y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{impair}.y \ \Rightarrow\ \mathsf{wp}(z, y := z \cdot x,\ y - 1,\ y \geq 0 \wedge z \cdot x^y = \mathsf{X}) \\ = & \quad \langle \text{ Axiome de l'affectation (10.22) \ \& \ Les expressions } z \cdot x \text{ et } y - 1 \text{ sont totales sur } \mathbb{Z} \ \rangle \\ & y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{impair}.y \ \Rightarrow\ (y \geq 0 \wedge z \cdot x^y = \mathsf{X})[z, y\ :=\ z \cdot x,\ y - 1] \\ = & \quad \langle \text{ Substitution } \rangle \\ & y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{impair}.y \ \Rightarrow\ y - 1 \geq 0 \wedge z \cdot x \cdot x^{y-1} = \mathsf{X} \\ = & \quad \langle \text{ Arithmétique \ \& \ Propriété de l'exponentiation : } x^m \cdot x^n = x^{m+n} \ \rangle \\ & y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{impair}.y \ \Rightarrow\ y > 0 \wedge z \cdot x^y = \mathsf{X} \\ & \quad \text{—Affaiblissement (3.92b), avec } p, q\ :=\ y > 0 \wedge z \cdot x^y = \mathsf{X},\ \mathsf{impair}.y \end{array}$$

(b) $\{Q \wedge \neg B\}\ \ S_2\ \ \{R\}$

$$\begin{array}{ll} & \{Q \wedge \neg B\}\ \ S_2\ \ \{R\} \\ = & \quad \langle \text{ Définition de } Q,\ B,\ S_2 \text{ et } R \ \ \& \ \ \neg\mathsf{impair}.y \equiv \mathsf{pair}.y \ \rangle \\ & \{y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{pair}.y\}\ \ x, y := x \cdot x,\ y/2\ \ \{y \geq 0 \wedge z \cdot x^y = \mathsf{X}\} \\ = & \quad \langle \text{ (10.20) } \rangle \\ & y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{pair}.y \ \Rightarrow\ \mathsf{wp}(x, y := x \cdot x,\ y/2,\ y \geq 0 \wedge z \cdot x^y = \mathsf{X}) \end{array}$$

Pour prouver la dernière ligne, assumons l'antécédent et prouvons le conséquent.

$$y > 0 \wedge z \cdot x^y = \mathsf{X} \wedge \mathsf{pair}.y \ \Rightarrow\ (y \geq 0 \wedge z \cdot x^y = \mathsf{X})[x, y\ :=\ x \cdot x, y/2].$$

$$\begin{array}{ll} & \mathsf{wp}(x, y := x \cdot x,\ y/2,\ y \geq 0 \wedge z \cdot x^y = \mathsf{X}) \\ = & \quad \langle \text{ Axiome de l'affectation (10.22) \ \& \ Les expressions } x \cdot x \text{ et } y/2 \text{ sont totales sur } \mathbb{Z} \ \rangle \end{array}$$

$$
\begin{array}{ll}
 & (y \geq 0 \ \wedge \ z \cdot x^y = \mathsf{X})[x, y \ := \ x \cdot x, y/2] \\
= & \quad \langle \text{ Substitution } \rangle \\
 & y/2 \geq 0 \ \wedge \ z \cdot (x \cdot x)^{y/2} = \mathsf{X} \\
= & \quad \langle \text{ À cause de l'hypothèse } \mathsf{pair}.y,\ (x \cdot x)^{y/2} = x^y \text{ (cette remarque utilise la propriété de l'exponentiation } (x^m)^n = x^{m \cdot n}) \ \rangle \\
 & y/2 \geq 0 \ \wedge \ z \cdot x^y = \mathsf{X} \\
= & \quad \langle \text{ Arithmétique, en utilisant l'hypothèse } \mathsf{pair}.y \text{ (il faut utiliser l'hypothèse ; par exemple, on n'a pas } -1/2 \geq 0 \ \equiv \ -1 \geq 0, \text{ à cause de la division entière) } \rangle \\
 & y \geq 0 \ \wedge \ z \cdot x^y = \mathsf{X} \qquad \text{—Ceci est vrai par hypothèse}
\end{array}
$$

5. Vérifiez le programme

$$
\begin{array}{l}
\{0 \leq n\} \\
\quad x, j := 0, 0 \,; \\
\{\text{Invariant } 0 \leq j \leq n \ \wedge \ x = (\sum k \mid 0 \leq k < j : b[k])\} \\
\{\text{Fonction majorante } n - j\} \\
\quad \textbf{while } j \neq n \textbf{ do} \\
\qquad x, j := \ x + b[j], \ j + 1 \\
\{x = (\sum k \mid 0 \leq k < n : b[k])\},
\end{array}
$$

dans lequel les variables ont les types

$$j, n{:}\mathbb{Z}, \qquad x{:}\mathbb{R}, \qquad b[0..n-1]{:}\mathsf{tableau\ de}\ \mathbb{R}.$$

Solution. Utilisons la procédure de vérification d'une boucle initialisée (10.43) et le théorème sur les preuves de terminaison (10.45), avec les instanciations suivantes.

$$
\begin{array}{lcl}
Q & := & 0 \leq n \\
P & := & 0 \leq j \leq n \ \wedge \ x = (\sum k \mid 0 \leq k < j : b[k]) \\
B & := & j \neq n \\
R & := & x = (\sum k \mid 0 \leq k < n : b[k]) \\
M & := & n - j \\
S' & := & (x, j := 0, 0) \\
S & := & (x, j := \ x + b[j], \ j + 1)
\end{array}
$$

(a) Il faut montrer $\{Q\} \ \ S' \ \ \{P\}$.

$$
\begin{array}{ll}
 & \{Q\} \ \ S' \ \ \{P\} \\
= & \quad \langle \ (10.20) \ \rangle \\
 & Q \Rightarrow \mathsf{wp}(S', P) \\
= & \quad \langle \text{ Définition de } Q,\ S' \text{ et } P \ \rangle \\
 & 0 \leq n \ \Rightarrow \ \mathsf{wp}((x, j := 0, 0), \ 0 \leq j \leq n \ \wedge \ x = (\sum k \mid 0 \leq k < j : b[k]))
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ Axiome de l'affectation (10.22) } \& \text{ L'expression 0 est totale } \rangle \\
& 0 \le n \;\Rightarrow\; \big(0 \le j \le n \;\wedge\; x = (\sum k \mid 0 \le k < j : b[k])\big)[x, j \;:=\; 0, 0] \\
= & \langle \text{ Substitution } \& \text{ (6.14) } \& \neg\mathsf{libre}(\text{`}k\text{'},\text{`}x, j, 0, 0\text{'}) \rangle \\
& 0 \le n \;\Rightarrow\; 0 \le 0 \le n \;\wedge\; 0 = (\sum k \mid 0 \le k < 0 : b[k]) \\
= & \langle\; 0 \le 0 \equiv \mathsf{vrai} \;\; \& \;\; 0 \le k < 0 \equiv \mathsf{faux} \;\; \& \text{ Domaine vide (6.19)} \\
& \quad \& \text{ 0 est l'élément neutre de } + \;\; \& \text{ Lecture conjonctive de } \le \\
& \rangle \\
& 0 \le n \;\Rightarrow\; \mathsf{vrai} \;\wedge\; 0 \le n \;\wedge\; 0 = 0 \\
= & \langle \text{ Identité de } \wedge \text{ (3.52), avec } p \;:=\; 0 \le n \;\; \& \;\; 0 = 0 \;\equiv\; \mathsf{vrai} \;\rangle \\
& 0 \le n \;\Rightarrow\; 0 \le n \;\wedge\; \mathsf{vrai} \\
= & \langle \text{ Identité de } \wedge \text{ (3.52), avec } p \;:=\; 0 \le n \;\rangle \\
& 0 \le n \;\Rightarrow\; 0 \le n \qquad \text{—Reflexivité de } \Rightarrow \text{ (3.87), avec } p \;:=\; 0 \le n
\end{array}
$$

(b) Il faut vérifier $\{P \wedge B\} \;\; S \;\; \{P\}$.

$$
\begin{array}{ll}
& \{P \wedge B\} \;\; S \;\; \{P\} \\
= & \langle \text{ (10.20) } \rangle \\
& P \wedge B \Rightarrow \mathsf{wp}(S, P) \\
= & \langle \text{ Définition de } P,\ B \text{ et } S \;\rangle \\
& 0 \le j \le n \;\wedge\; x = (\sum k \mid 0 \le k < j : b[k]) \;\wedge\; j \ne n \\
& \Rightarrow\; \mathsf{wp}\big((x, j := x + b[j], j + 1),\; 0 \le j \le n \;\wedge\; x = (\sum k \mid 0 \le k < j : b[k])\big)
\end{array}
$$

Montrons que le conséquent de la dernière formule peut être déduit de l'antécédent (en fait, la dérivation suivante montre même que l'antécédent et le conséquent sont équivalents).

$$
\begin{array}{ll}
& \mathsf{wp}((x, j := x + b[j],\;\; j + 1),\;\; 0 \le j \le n \;\wedge\; x = (\sum k \mid 0 \le k < j : b[k])) \\
= & \langle \text{ Axiome de l'affectation (10.21) } \& \text{ L'expression } j + 1 \text{ est} \\
& \quad \text{totale, mais } \mathsf{dom}.\text{`}x + b[j]\text{'} \;\equiv\; 0 \le j < n. \text{ On a donc} \\
& \quad \mathsf{dom}.\text{`}x + b[j],\, j + 1\text{'} \;\equiv\; 0 \le j < n \text{ (c'est la conjonction des} \\
& \quad \text{domaines des deux expressions) } \rangle \\
& 0 \le j < n \\
& \wedge\; \big(0 \le j \le n \;\wedge\; x = (\sum k \mid 0 \le k < j : b[k])\big)[x, j \;:=\; x + b[j],\;\; j + 1] \\
= & \langle \text{ Substitution } \& \text{ (6.14) } \& \neg\mathsf{libre}(\text{`}k\text{'},\text{`}x, j, x + b[j], j + 1\text{'}) \rangle \\
& 0 \le j < n \;\wedge\; 0 \le j + 1 \le n \;\wedge\; x + b[j] = (\sum k \mid 0 \le k < j + 1 : b[k]) \\
= & \langle \text{ Extraction d'un terme (6.40) } \rangle \\
& 0 \le j < n \;\wedge\; 0 \le j + 1 \le n \;\wedge\; x + b[j] = (\sum k \mid 0 \le k < j : b[k]) + b[j] \\
= & \langle \text{ Arithmétique } \rangle \\
& 0 \le j < n \;\wedge\; 0 \le j + 1 \le n \;\wedge\; x = (\sum k \mid 0 \le k < j : b[k]) \\
= & \langle\; 0 \le j \;\wedge\; 0 \le j + 1 \;\equiv\; 0 \le j \;\; \& \;\; j + 1 \le n \;\equiv\; j < n \;\rangle
\end{array}
$$

$$
\begin{array}{ll}
& 0 \le j < n \ \wedge\ x = (\sum k \mid 0 \le k < j : b[k]) \\
= & \quad \langle \text{ Arithmétique } \rangle \\
& 0 \le j \le n \ \wedge\ j \neq n \ \wedge\ x = (\sum k \mid 0 \le k < j : b[k])
\end{array}
$$

Voyez la preuve qui suit (10.27). On demande de prouver une propriété très semblable à celle qui est démontrée ici, mais la preuve est un peu différente de celle qui précède, histoire d'illustrer deux approches différentes.

(c) Il faut montrer que l'exécution de la boucle se termine. Pour cela, utilisons (10.45).

i. $n - j$ retourne un entier, puisque n et j sont des entiers.

ii. Il faut montrer $\{P \ \wedge\ B \ \wedge\ M = \mathsf{X}\}\ \ S\ \ \{M < \mathsf{X}\}$.

$$
\begin{array}{ll}
& \{P \ \wedge\ B \ \wedge\ M = \mathsf{X}\}\ \ S\ \ \{M < \mathsf{X}\} \\
= & \quad \langle \text{ (10.20) } \rangle \\
& P \ \wedge\ B \ \wedge\ M = \mathsf{X} \ \Rightarrow\ \mathsf{wp}(S, M < \mathsf{X}) \\
= & \quad \langle \text{ Définition de } P,\ B,\ M \text{ et } S \ \rangle \\
& 0 \le j \le n \ \wedge\ x = (\sum k \mid 0 \le k < j : b[k]) \ \wedge\ j \neq n \ \wedge\ n - j = \mathsf{X} \\
& \Rightarrow\ \mathsf{wp}((x, j := x + b[j],\ j + 1),\ n - j < \mathsf{X})
\end{array}
$$

Pour montrer la dernière formule, supposons l'antécédent et montrons le conséquent.

$$
\begin{array}{ll}
& \mathsf{wp}((x, j := x + b[j],\ j + 1),\ n - j < \mathsf{X}) \\
= & \quad \langle \text{ Axiome de l'affectation (10.21) } \ \& \\
& \quad\ \mathsf{dom}.\text{`}x + b[j],\ j + 1\text{'} \equiv 0 \le j < n \ \rangle \\
& 0 \le j < n \ \wedge\ (n - j < \mathsf{X})[x, j\ :=\ x + b[j],\ j + 1]) \\
= & \quad \langle \text{ Substitution } \rangle \\
& 0 \le j < n \ \wedge\ n - (j + 1) < \mathsf{X} \\
= & \quad \langle \text{ Arithmétique } \rangle \\
& 0 \le j < n \ \wedge\ n - j < \mathsf{X} + 1
\end{array}
$$

— $0 \le j < n$ est équivalent à l'hypothèse $0 \le j \le n \ \wedge\ j \neq n$ & $n - j < \mathsf{X} + 1$ découle de l'hypothèse $n - j = \mathsf{X}$

iii. Il faut montrer $P \wedge B \ \Rightarrow\ M > 0$.

$$
\begin{array}{ll}
& P \wedge B \\
= & \quad \langle \text{ Définition de } P \text{ et } B \ \rangle \\
& 0 \le j \le n \ \wedge\ x = (\sum k \mid 0 \le k < j : b[k]) \ \wedge\ j \neq n \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec} \\
& \quad\ p, q\ :=\ 0 \le j \le n \ \wedge\ j \neq n,\ x = (\sum k \mid 0 \le k < j : b[k]) \ \rangle \\
& 0 \le j \le n \ \wedge\ j \neq n \\
\Rightarrow & \quad \langle \text{ Arithmétique } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& j < n \\
= & \quad \langle \text{ Arithmétique } \rangle \\
& n - j > 0 \\
= & \quad \langle \text{ Définition de } M \rangle \\
& M > 0
\end{array}
$$

(d) Il faut montrer $P \wedge \neg B \Rightarrow R$.

$$
\begin{array}{ll}
& P \wedge \neg B \\
= & \quad \langle \text{ Définition de } P \text{ et } B \ \ \& \ \neg(j \neq n) \equiv j = n \rangle \\
& 0 \leq j \leq n \ \wedge \ x = (\sum k \mid 0 \leq k < j : b[k]) \ \wedge \ j = n \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec} \\
& \quad p, q \ := \ x = (\sum k \mid 0 \leq k < j : b[k]) \ \wedge \ j = n, \ 0 \leq j \leq n \ \rangle \\
& x = (\sum k \mid 0 \leq k < j : b[k]) \ \wedge \ j = n \\
= & \quad \langle \text{ Substitution (9.3a), avec} \\
& \quad e, f, E \ := \ j, \ n, \ x = (\sum k \mid 0 \leq k < z : b[k]) \ \rangle \\
& x = (\sum k \mid 0 \leq k < n : b[k]) \ \wedge \ j = n \\
\Rightarrow & \quad \langle \text{ Affaiblissement (3.92b), avec} \\
& \quad p, q \ := \ x = (\sum k \mid 0 \leq k < j : b[k]), \ j = n \ \rangle \\
& x = (\sum k \mid 0 \leq k < n : b[k]) \\
= & \quad \langle \text{ Définition de } R \ \rangle \\
& R
\end{array}
$$

6. Vérifiez le programme suivant. Les variables a, b, i et n sont entières.

$\{0 \leq n\}$
$\quad b, i := 1, 0\,;$
$\{\text{Invariant } 0 \leq i \leq n \ \wedge \ b = a^i\}$
$\{\text{Fonction majorante } n - i\}$
$\quad$ **while** $i < n$ **do**
$\quad\quad$ **begin**
$\quad\quad i := i + 1\,;$
$\quad\quad b := a \cdot b$
$\quad\quad$ **end**
$\{b = a^n\}$

Solution. Utilisons la procédure de vérification d'une boucle initialisée (10.43) et le

théorème sur les preuves de terminaison (10.45), avec les instanciations suivantes.

$$\begin{array}{lcl} Q & := & 0 \leq n \\ P & := & 0 \leq i \leq n \ \wedge \ b = a^i \\ B & := & i < n \\ R & := & b = a^n \\ M & := & n - i \\ S' & := & (b, i := 1, 0) \\ S & := & (\textbf{begin}\ i := i + 1; b := a \cdot b\ \textbf{end}) \end{array}$$

(a) Il faut montrer $\{Q\}\ \ S'\ \ \{P\}$.

$$\begin{array}{ll} & \{Q\}\ \ S'\ \ \{P\} \\ = & \quad \langle\ (10.20)\ \rangle \\ & Q \Rightarrow \mathsf{wp}(S', P) \\ = & \quad \langle\ \text{Définition de } Q,\ S' \text{ et } P\ \rangle \\ & 0 \leq n\ \Rightarrow\ \mathsf{wp}((b, i := 1, 0),\ 0 \leq i \leq n\ \wedge\ b = a^i) \\ = & \quad \langle\ \text{Axiome de l'affectation (10.22)}\ \ \& \\ & \quad\ \ \text{Les expressions 1 et 0 sont totales}\ \rangle \\ & 0 \leq n\ \Rightarrow\ (0 \leq i \leq n\ \wedge\ b = a^i)[b, i\ :=\ 1, 0] \\ = & \quad \langle\ \text{Substitution}\ \rangle \\ & 0 \leq n\ \Rightarrow\ 0 \leq 0 \leq n\ \wedge\ 1 = a^0 \\ = & \quad \langle\ \text{Arithmétique : } 0 \leq 0 \equiv \mathsf{vrai}\ \ \& \\ & \quad\ \ \text{Définition de l'exponentiation (8.7)}\ \ \& \\ & \quad\ \ \text{Lecture conjonctive de } \leq\ \rangle \\ & 0 \leq n\ \Rightarrow\ \mathsf{vrai}\ \wedge\ 0 \leq n\ \wedge\ \mathsf{vrai} \\ = & \quad \langle\ \text{Identité de } \wedge \text{ (3.52), deux fois avec } p\ :=\ 0 \leq n\ \rangle \\ & 0 \leq n\ \Rightarrow\ 0 \leq n \qquad \text{—Réflexivité de } \Rightarrow \text{ (3.87), avec } p\ :=\ 0 \leq n \end{array}$$

(b) Il faut montrer $\{P \wedge B\}\ \ S\ \ \{P\}$.

$$\begin{array}{ll} & \{P \wedge B\}\ \ S\ \ \{P\} \\ = & \quad \langle\ \text{Définition de } S\ \rangle \\ & \{P \wedge B\}\ \ \textbf{begin}\ i := i + 1; b := a \cdot b\ \textbf{end}\ \ \{P\} \\ = & \quad \langle\ \text{Axiome du bloc } \textbf{begin-end}\ (10.37)\ \rangle \\ & \{P \wedge B\}\ \ i := i + 1; b := a \cdot b\ \ \{P\} \\ = & \quad \langle\ (10.20)\ \rangle \\ & P \wedge B\ \ \Rightarrow\ \ \mathsf{wp}(i := i + 1; b := a \cdot b,\ \ P) \\ = & \quad \langle\ \text{Axiome de la séquence (10.29)}\ \rangle \\ & P \wedge B\ \ \Rightarrow\ \ \mathsf{wp}(i := i + 1, \mathsf{wp}(b := a \cdot b,\ \ P)) \end{array}$$

$$
\begin{array}{ll}
= & \langle \text{ Axiome de l'affectation (10.22) } \& \\
& \quad \text{L'expression } a \cdot b \text{ est totale } \rangle \\
& P \wedge B \;\Rightarrow\; \mathsf{wp}(i := i+1, P[b := a \cdot b]) \\
= & \langle \text{ Axiome de l'affectation (10.22) } \& \\
& \quad \text{L'expression } i+1 \text{ est totale } \rangle \\
& P \wedge B \;\Rightarrow\; P[b := a \cdot b][i := i+1] \\
= & \langle \text{ Définition de } P \rangle \\
& P \wedge B \;\Rightarrow\; (0 \leq i \leq n \wedge b = a^i)[b := a \cdot b][i := i+1] \\
= & \langle \text{ Substitution } \rangle \\
& P \wedge B \;\Rightarrow\; (0 \leq i \leq n \wedge a \cdot b = a^i)[i := i+1] \\
= & \langle \text{ Substitution } \rangle \\
& P \wedge B \;\Rightarrow\; 0 \leq i+1 \leq n \wedge a \cdot b = a^{i+1} \\
= & \langle \text{ Définition de } P \text{ et } B \rangle \\
& 0 \leq i \leq n \wedge b = a^i \wedge i < n \;\Rightarrow\; 0 \leq i+1 \leq n \wedge a \cdot b = a^{i+1} \\
= & \langle \text{ Arithmétique : } i \leq n \wedge i < n \;\equiv\; i < n \rangle \\
& 0 \leq i < n \wedge b = a^i \;\Rightarrow\; 0 \leq i+1 \leq n \wedge a \cdot b = a^{i+1}
\end{array}
$$

Pour démontrer la dernière ligne de cette dérivation, assumons l'antécédent $0 \leq i$, $i < n$ et $b = a^i$, et montrons $0 \leq i+1 \leq n \wedge a \cdot b = a^{i+1}$.

$$
\begin{array}{ll}
& 0 \leq i+1 \leq n \wedge a \cdot b = a^{i+1} \\
= & \langle \text{ Hypothèse } b = a^i \rangle \\
& 0 \leq i+1 \leq n \wedge a \cdot a^i = a^{i+1} \\
= & \langle \text{ Définition de l'exponentiation (8.7), avec } b, n := a, i \;\; \& \\
& \quad \text{Par l'hypothèse, on a } i \geq 0 \rangle \\
& 0 \leq i+1 \leq n \wedge \mathsf{vrai} \\
= & \langle \text{ Par l'hypothèse } 0 \leq i, \text{ on a } 0 \leq i+1 \;\; \& \\
& \quad \text{Par l'hypothèse } i < n, \text{ on a } i+1 \leq n \rangle \\
& \mathsf{vrai} \wedge \mathsf{vrai} \\
= & \langle \text{ Idempotence de } \wedge \text{ (3.51), avec } p := \mathsf{vrai} \rangle \\
& \mathsf{vrai} \qquad \text{—(3.6)}
\end{array}
$$

(c) Il faut vérifier les hypothèses (10.45a,b,c).

i. Hypothèse (a) : l'expression $n-i$ retourne une valeur entière, car les variables n et i sont entières.

ii. Hypothèse (b) : il faut montrer $\{P \wedge B \wedge M = \mathsf{X}\} \;\; S \;\; \{M < \mathsf{X}\}$.

$$
\begin{array}{ll}
& \{P \wedge B \wedge M = \mathsf{X}\} \;\; S \;\; \{M < \mathsf{X}\} \\
= & \langle \text{ Définition de } S \;\; \& \;\; \text{Axiome du bloc } \textbf{begin-end} \text{ (10.37) } \rangle
\end{array}
$$

$\{P \wedge B \wedge M = \mathsf{X}\}\ \ i := i+1; b := a \cdot b\ \ \{M < \mathsf{X}\}$

$=$ $\langle$ (10.20) $\rangle$

$P \wedge B \wedge M = \mathsf{X} \Rightarrow \mathsf{wp}(i := i+1; b := a \cdot b,\ M < \mathsf{X})$

$=$ $\langle$ Voyez la transformation de $\mathsf{wp}(i := i+1; b := a \cdot b,\ P)$ dans la preuve de l'invariance de P ci-dessus. Il suffit de remplacer P par $M < \mathsf{X}$ $\rangle$

$P \wedge B \wedge M = \mathsf{X} \Rightarrow (M < \mathsf{X})[b := a \cdot b][i := i+1]$

$=$ $\langle$ Définition de M $\rangle$

$P \wedge B \wedge n - i = \mathsf{X} \Rightarrow (n - i < \mathsf{X})[b := a \cdot b][i := i+1]$

$=$ $\langle$ Substitution $\rangle$

$P \wedge B \wedge n - i = \mathsf{X} \Rightarrow (n - i < \mathsf{X})[i := i+1]$

$=$ $\langle$ Substitution $\rangle$

$P \wedge B \wedge n - i = \mathsf{X} \Rightarrow n - (i+1) < \mathsf{X}$

$=$ $\langle$ Arithmétique $\rangle$

$P \wedge B \wedge n - i = \mathsf{X} \Rightarrow n - i < \mathsf{X} + 1$ —Arithmétique

iii. Hypothèse (c) : il faut montrer $P \wedge B \Rightarrow M > 0$.

$P \wedge B$

$=$ $\langle$ Définition de P et B $\rangle$

$0 \le i \le n \wedge b = a^i \wedge i < n$

$=$ $\langle$ Lecture conjonctive de $\le$ & $i \le n \wedge i < n \equiv i < n$ $\rangle$

$0 \le i \wedge i < n \wedge b = a^i$

$\Rightarrow$ $\langle$ Affaiblissement (3.92b), avec $p, q := i < n,\ 0 \le i \wedge b = a^i$ $\rangle$

$i < n$

$=$ $\langle$ Arithmétique $\rangle$

$n - i > 0$

$=$ $\langle$ Définition de M $\rangle$

$M > 0$

(d) Il faut montrer $P \wedge \neg B \Rightarrow R$.

$P \wedge \neg B$

$=$ $\langle$ Définition de P, B et R $\rangle$

$0 \le i \le n \wedge b = a^i \wedge \neg(i < n)$

$=$ $\langle$ Arithmétique $\rangle$

$0 \le i \le n \wedge b = a^i \wedge i \ge n$

$=$ $\langle$ Lecture conjonctive de $\leq$ &
Arithmétique : $i \leq n \wedge i \geq n \equiv i = n$ $\rangle$
$0 \leq i \wedge i = n \wedge b = a^i$
$=$ $\langle$ Substitution (9.3a), avec $e, f, E := i, n, b = a^z$ $\rangle$
$0 \leq i \wedge i = n \wedge b = a^n$
$\Rightarrow$ $\langle$ Affaiblissement (3.92b), avec $p, q := b = a^n,\ 0 \leq i \wedge i = n$ $\rangle$
$b = a^n$
$=$ $\langle$ Définition de R $\rangle$
R

14.11 Problèmes du chapitre 11

1. Définissez l'ensemble suivant par compréhension (sous forme abrégée ou non).

   L'ensemble des nombres premiers compris entre 10 et 30. Vous pouvez utiliser la fonction booléenne $\mathsf{premier}.i$ qui retourne la valeur de « i est premier ».

   Solution. Voici deux bonnes réponses :

   $$\{i{:}\mathbb{Z} \mid 10 \leq i \leq 30 \wedge \mathsf{premier}.i : i\}$$
   $$\{i{:}\mathbb{Z} \mid 10 \leq i \leq 30 \wedge \mathsf{premier}.i\} \quad \text{(forme abrégée)}$$

   Si on avait demandé de donner l'ensemble par énumération, la réponse serait

   $$\{11, 13, 17, 19, 23, 29\}.$$

2. Décrivez l'ensemble suivant en français.

   $$\{x, y{:}\mathbb{Z} \mid 0 \leq x \ \wedge \ 2 \leq y \leq 3 : x^y\}$$

   Solution. C'est l'ensemble des carrés et des cubes des entiers naturels.

3. Utilisez le fait que $\{b\}$ et $\{b, c\}$ sont des abréviations de

   $$\{x \mid x = b : x\} \quad \text{et} \quad \{x \mid x = b \vee x = c : x\},$$

   respectivement, pour démontrer

   $$v \in \{b\} \ \equiv \ v = b \quad \text{et} \quad v \in \{b, c\} \ \equiv \ v = b \vee v = c.$$

Solution. À cause des conventions sur la notation, notons que b, c et v sont des variables (et non pas des expressions arbitraires).

(a) Preuve de $v \in \{b\} \equiv v = b$:

$$
\begin{array}{ll}
 & v \in \{b\} \\
= & \quad \langle \text{ Suppression de l'abréviation } \rangle \\
 & v \in \{x \mid x = b : x\} \\
= & \quad \langle \neg\mathsf{libre}(\text{`}x\text{'},\text{`}v\text{'}) \ \& \ \text{Appartenance (11.5)} \rangle \\
 & (\exists x \mid x = b : v = x) \\
= & \quad \langle \neg\mathsf{libre}(\text{`}x\text{'},\text{`}b\text{'}) \ \& \ \text{Axiome du point (6.21)} \rangle \\
 & (v = x)[x := b] \\
= & \quad \langle \text{ Substitution } \rangle \\
 & v = b
\end{array}
$$

(b) Preuve de $v \in \{b, c\} \equiv v = b \vee v = c$:

$$
\begin{array}{ll}
 & v \in \{b, c\} \\
= & \quad \langle \text{ Suppression de l'abréviation } \rangle \\
 & v \in \{x \mid x = b \vee x = c : x\} \\
= & \quad \langle \neg\mathsf{libre}(\text{`}x\text{'},\text{`}v\text{'}) \ \& \ \text{Appartenance (11.5)} \rangle \\
 & (\exists x \mid x = b \vee x = c : v = x) \\
= & \quad \langle \vee \text{ est idempotent (3.34) } \& \text{ Division du domaine (6.29) } \& \\
 & \quad \text{Toutes les quantifications sont définies, puisque ce sont des} \\
 & \quad \text{quantifications existentielles et que les expressions des corps et} \\
 & \quad \text{des domaines sont définies } \rangle \\
 & (\exists x \mid x = b : v = x) \vee (\exists x \mid x = c : v = x) \\
= & \quad \langle \neg\mathsf{libre}(\text{`}x\text{'},\text{`}b, c\text{'}) \ \& \ \text{Axiome du point (6.21), deux fois} \rangle \\
 & (v = x)[x := b] \vee (v = x)[x := c] \\
= & \quad \langle \text{ Substitution } \rangle \\
 & v = b \vee v = c
\end{array}
$$

4. Démontrez (11.16), $\{x \mid Q\} = \{x \mid R\} \equiv (\forall x \mid : Q \equiv R)$.

Solution.

$$
\begin{array}{ll}
 & \{x \mid Q\} = \{x \mid R\} \\
= & \quad \langle \text{ Extensionalité (11.8) } \rangle \\
 & (\forall x \mid : x \in \{x \mid Q\} \equiv x \in \{x \mid R\}) \\
= & \quad \langle \text{ (11.13), deux fois } \rangle
\end{array}
$$

$$(\forall x \mid : Q \equiv R)$$

5. Démontrez le théorème (11.48), $S \cup (T \cap U) \;=\; (S \cup T) \cap (S \cup U)$.

   Solution. Par extensionnalité (11.8), il suffit de montrer

   $$(\forall x \mid : x \in S \cup (T \cap U) \;\equiv\; x \in (S \cup T) \cap (S \cup U)).$$

   Par le métathéorème (7.33), pour démontrer cette formule, il suffit de montrer

   $$x \in S \cup (T \cap U) \;\equiv\; x \in (S \cup T) \cap (S \cup U).$$

   $$\begin{array}{ll} & x \in S \cup (T \cap U) \\ = & \quad \langle \text{ Union (11.28) } \rangle \\ & x \in S \;\vee\; x \in T \cap U \\ = & \quad \langle \text{ Intersection (11.29) } \rangle \\ & x \in S \;\vee\; (x \in T \;\wedge\; x \in U) \\ = & \quad \langle \text{ Distributivité de } \vee \text{ sur } \wedge \text{ (3.59), avec } p, q, r := x \in S,\; x \in T,\; x \in U \rangle \\ & (x \in S \;\vee\; x \in T) \;\wedge\; (x \in S \;\vee\; x \in U) \\ = & \quad \langle \text{ Union (11.28), deux fois } \rangle \\ & x \in S \cup T \;\wedge\; x \in S \cup U \\ = & \quad \langle \text{ Intersection (11.29) } \rangle \\ & x \in (S \cup T) \cap (S \cup U) \end{array}$$

   Cette preuve est typique et suit une démarche semblable à celle qui peut être utilisée pour la démonstration de plusieurs propriétés présentées dans ce chapitre. Remarquez comment les opérateurs ensemblistes $(\cup, \cap)$ sont éliminés pour être remplacés par les opérateurs booléens correspondants $(\vee, \wedge)$. On utilise ensuite les propriétés des opérateurs booléens (ici, la distributivité de $\vee$ sur $\wedge$) pour finalement réintroduire les opérateurs ensemblistes. La démarche applique donc l'heuristique d'élimination des définitions (3.29).

   Ce chapitre introduit plusieurs nouveaux opérateurs. Notez bien leur priorité et remarquez comment les parenthèses sont manipulées dans la preuve ci-dessus.

6. Démontrez le théorème (11.51), $S \subseteq T \;\wedge\; U \subseteq V \;\Rightarrow\; S \cup U \subseteq T \cup V$. Pour cette démonstration, vous pouvez utiliser le théorème

   $$(p \Rightarrow q) \;\wedge\; (r \Rightarrow s) \;\Rightarrow\; (p \vee r \;\Rightarrow\; q \vee s)$$

   (pour la démonstration d'une propriété similaire, voyez le problème 2 du chapitre 4).

Solution.

$$
\begin{array}{ll}
& S \cup U \subseteq T \cup V \\
= & \qquad \langle \text{ Sous-ensemble (11.21) } \rangle \\
& (\forall x \mid x \in S \cup U : x \in T \cup V) \\
= & \qquad \langle \text{ Définition de } \cup \text{ (11.28), deux fois } \rangle \\
& (\forall x \mid x \in S \vee x \in U : x \in T \vee x \in V) \\
= & \qquad \langle \text{ Transfert (7.17a) } \rangle \\
& (\forall x \mid : x \in S \vee x \in U \Rightarrow x \in T \vee x \in V) \\
\Leftarrow & \qquad \langle \text{ Par le théorème donné dans l'énoncé,} \\
& \qquad\quad (x \in S \Rightarrow x \in T) \wedge (x \in U \Rightarrow x \in V) \\
& \qquad \Rightarrow (x \in S \vee x \in U \Rightarrow x \in T \vee x \in V) \\
& \qquad \text{est un théorème. Par le métathéorème (7.33),} \\
& \qquad (\forall x \mid : (x \in S \Rightarrow x \in T) \wedge (x \in U \Rightarrow x \in V) \\
& \qquad\quad \Rightarrow (x \in S \vee x \in U \Rightarrow x \in T \vee x \in V)) \\
& \qquad \text{est aussi un théorème } \ \& \\
& \qquad \text{Monotonie de } \forall \text{ (7.34) } \rangle \\
& (\forall x \mid : (x \in S \Rightarrow x \in T) \wedge (x \in U \Rightarrow x \in V)) \\
= & \qquad \langle \text{ Distributivité (6.23) } \ \& \text{ Toutes les quantifications sont définies,} \\
& \qquad \text{puisque ce sont des quantifications universelles et que les expressions} \\
& \qquad \text{des corps et des domaines sont définies } \rangle \\
& (\forall x \mid : x \in S \Rightarrow x \in T) \wedge (\forall x \mid : x \in U \Rightarrow x \in V) \\
= & \qquad \langle \text{ Transfert (7.17a), deux fois } \rangle \\
& (\forall x \mid x \in S : x \in T) \wedge (\forall x \mid x \in U : x \in V) \\
= & \qquad \langle \text{ Sous-ensemble (11.21), deux fois } \rangle \\
& S \subseteq T \wedge U \subseteq V
\end{array}
$$

7. Démontrez le théorème (11.58), $S - T \subseteq S$.

Solution.

$$
\begin{array}{ll}
& S - T \subseteq S \\
= & \qquad \langle \text{ (11.57) } \rangle \\
& S \cap {\sim}T \subseteq S \qquad \text{—Affaiblissement (11.46)}
\end{array}
$$

8. Démontrez le théorème (11.78a), $S \subseteq T \wedge T \subset U \Rightarrow S \subset U$.

Solution. C'est l'un des problèmes les plus difficiles de cette série. Voici deux preuves. La première, très élégante, a été trouvée par Claude Bolduc, étudiant du cours à l'automne 2000.

(a)
$$
\begin{array}{ll}
& S \subseteq T \wedge T \subset U \\
= & \qquad \langle\ (11.69)\ \rangle \\
& S \subseteq T \wedge T \subseteq U \wedge \neg(U \subseteq T) \\
= & \qquad \langle\ \text{Idempotence de } \wedge\ (3.51), \text{ avec } p := S \subseteq T\ \rangle \\
& S \subseteq T \wedge S \subseteq T \wedge T \subseteq U \wedge \neg(U \subseteq T) \\
\Rightarrow & \qquad \langle\ \text{Transitivité (11.67)}\ \ \&\ \ \text{Monotonie de } \wedge\ (4.3)\ \rangle \\
& S \subseteq U \wedge S \subseteq T \wedge \neg(U \subseteq T) \\
\Rightarrow & \qquad \langle\ (11.76)\ \ \&\ \ \text{Monotonie de } \wedge\ (4.3)\ \rangle \\
& S \subseteq U \wedge \neg(U \subseteq S) \\
& \qquad \langle\ (11.69)\ \rangle \\
& S \subset U
\end{array}
$$

(b)
$$
\begin{array}{ll}
& S \subseteq T \wedge T \subset U \\
= & \qquad \langle\ \text{Sous-ensemble propre (11.22)}\ \rangle \\
& S \subseteq T \wedge T \subseteq U \wedge T \neq U \\
= & \qquad \langle\ \text{Remarquons que notre objectif est } S \subset U, \text{ c'est-à-dire, par sous-ensemble propre (11.22), } S \subseteq U \wedge S \neq U. \text{ Nous pouvons obtenir } S \subseteq U \text{ par transitivité (11.67) à partir de } S \subseteq T \wedge T \subseteq U. \text{ Il reste à obtenir } S \neq U. \text{ Une manière de faire apparaître } S \neq U \text{ est de faire apparaître en même temps } S = U. \text{ C'est le but des deux prochaines transformations}\ \ \&\ \ \text{Identité de } \wedge\ (3.52)\ \rangle \\
& S \subseteq T \wedge T \subseteq U \wedge \mathsf{vrai} \wedge T \neq U \\
= & \qquad \langle\ \text{Tiers exclu (3.37)}\ \rangle \\
& S \subseteq T \wedge T \subseteq U \wedge (S = U \vee S \neq U) \wedge T \neq U \\
= & \qquad \langle\ \text{Distributivité de } \wedge \text{ sur } \vee\ (3.60)\ \rangle \\
& (S \subseteq T \wedge T \subseteq U \wedge S = U \wedge T \neq U) \ \vee\ (S \subseteq T \wedge T \subseteq U \wedge S \neq U \wedge T \neq U) \\
= & \qquad \langle\ \text{Substitution (9.3a), avec } e, f, E := S,\ U,\ T \subseteq z \wedge T \neq z\ \rangle \\
& (S \subseteq T \wedge T \subseteq S \wedge S = U \wedge T \neq S) \ \vee\ (S \subseteq T \wedge T \subseteq U \wedge S \neq U \wedge T \neq U) \\
= & \qquad \langle\ \text{Antisymétrie (11.65)}\ \rangle \\
& (S = T \wedge S = U \wedge T \neq S) \ \vee\ (S \subseteq T \wedge T \subseteq U \wedge S \neq U \wedge T \neq U) \\
= & \qquad \langle\ \text{Contradiction (3.55)}\ \rangle \\
& (\mathsf{faux} \wedge S = U) \ \vee\ (S \subseteq T \wedge T \subseteq U \wedge S \neq U \wedge T \neq U) \\
= & \qquad \langle\ \text{Zéro de } \wedge\ (3.53)\ \rangle \\
& \mathsf{faux} \ \vee\ (S \subseteq T \wedge T \subseteq U \wedge S \neq U \wedge T \neq U) \\
= & \qquad \langle\ \text{Identité de } \vee\ (3.40)\ \rangle \\
& S \subseteq T \wedge T \subseteq U \wedge S \neq U \wedge T \neq U \\
\Rightarrow & \qquad \langle\ \text{Affaiblissement (3.92b)}\ \rangle
\end{array}
$$

$$
\begin{array}{ll}
& S \subseteq T \wedge T \subseteq U \wedge S \neq U \\
\Rightarrow & \qquad \langle \text{ Transitivité (11.67) } \& \text{ Monotonie de } \wedge \text{ (4.3) } \rangle \\
& S \subseteq U \wedge S \neq U \\
= & \qquad \langle \text{ Sous-ensemble propre (11.22) } \rangle \\
& S \subset U
\end{array}
$$

Remarquons que nous aurions pu réduire la longueur de la preuve quelque peu en travaillant sur les deux parties de l'expression à la fois dans les dernières étapes. Cela n'a pas été fait pour que la preuve soit plus facile à lire.

14.12 Problèmes du chapitre 12

1. Démontrez le théorème d'appartenance (12.4), $\langle x, y\rangle \in S \times T \ \equiv \ x \in S \wedge y \in T$.

   Solution.

$$
\begin{array}{ll}
& \langle x, y\rangle \in S \times T \\
= & \qquad \langle \text{ Produit cartésien (12.2) } \rangle \\
& \langle x, y\rangle \in \{b, c \mid b \in S \wedge c \in T : \langle b, c\rangle\} \\
= & \qquad \langle \neg\mathsf{libre}(\text{`}b, c\text{'},\text{`}x, y\text{'}) \ \& \ \text{Appartenance (12.4) } \rangle \\
& (\exists b, c \mid b \in S \wedge c \in T : \langle x, y\rangle = \langle b, c\rangle) \\
= & \qquad \langle \text{ Égalité de couples (12.1) } \rangle \\
& (\exists b, c \mid b \in S \wedge c \in T : x = b \wedge y = c) \\
= & \qquad \langle \text{ Transfert (7.1) deux fois } \rangle \\
& (\exists b, c \mid x = b \wedge y = c : b \in S \wedge c \in T) \\
= & \qquad \langle \neg\mathsf{libre}(\text{`}c\text{'},\text{`}x = b\text{'}) \ \& \ \text{Imbrication (6.34) } \rangle \\
& (\exists b \mid x = b : (\exists c \mid y = c : b \in S \wedge c \in T)) \\
= & \qquad \langle \neg\mathsf{libre}(\text{`}c\text{'},\text{`}y\text{'}) \ \& \ \text{Axiome du point (6.21) } \rangle \\
& (\exists b \mid x = b : (b \in S \wedge c \in T)[c := y]) \\
= & \qquad \langle \text{ Substitution } \rangle \\
& (\exists b \mid x = b : b \in S \wedge y \in T) \\
= & \qquad \langle \neg\mathsf{libre}(\text{`}b\text{'},\text{`}x\text{'}) \ \& \ \text{Axiome du point (6.21) } \rangle \\
& (b \in S \wedge y \in T)[b := x] \\
= & \qquad \langle \text{ Substitution } \rangle \\
& x \in S \wedge y \in T
\end{array}
$$

2. Démontrez le théorème (12.5), $\langle x, y\rangle \in S \times T \ \equiv \ \langle y, x\rangle \in T \times S$.

Solution.

$$
\begin{array}{ll}
 & \langle x, y\rangle \in S \times T \\
= & \qquad \langle \text{ Appartenance (12.4) } \rangle \\
 & x \in S \wedge y \in T \\
= & \qquad \langle \text{ Commutativité de } \wedge \text{ (3.49) } \rangle \\
 & y \in T \wedge x \in S \\
= & \qquad \langle \text{ Appartenance (12.4) } \rangle \\
 & \langle y, x\rangle \in T \times S
\end{array}
$$

3. Démontrez la distributivité de $\times$ sur $-$ (12.10), $S \times (T - U) = (S \times T) - (S \times U)$.

   Solution. Par extensionnalité (11.8), il suffit de montrer

   $$(\forall b, c \mid: \langle b, c\rangle \in S \times (T - U) \equiv \langle b, c\rangle \in (S \times T) - (S \times U)).$$

   Par le métathéorème (7.33), il suffit de montrer

   $$\langle b, c\rangle \in S \times (T - U) \equiv \langle b, c\rangle \in (S \times T) - (S \times U),$$

   ce que nous faisons.

$$
\begin{array}{ll}
 & \langle b, c\rangle \in (S \times T) - (S \times U) \\
= & \qquad \langle \text{ Différence (11.30) } \rangle \\
 & \langle b, c\rangle \in (S \times T) \ \wedge \ \langle b, c\rangle \notin (S \times U) \\
= & \qquad \langle \text{ Appartenance (12.4), deux fois } \rangle \\
 & b \in S \wedge c \in T \wedge \neg(b \in S \wedge c \in U) \\
= & \qquad \langle \text{ De Morgan (3.48a) } \rangle \\
 & b \in S \wedge c \in T \wedge (b \notin S \vee c \notin U) \\
= & \qquad \langle \text{ Absorption (3.61c) } \rangle \\
 & b \in S \wedge c \in T \wedge c \notin U \\
= & \qquad \langle \text{ Différence (11.30) } \rangle \\
 & b \in S \wedge c \in (T - U) \\
= & \qquad \langle \text{ Appartenance (12.4) } \rangle \\
 & \langle b, c\rangle \in S \times (T - U)
\end{array}
$$

4. Démontrez le théorème (12.14), $(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$.

Solution. Par extensionnalité (11.8), il suffit de montrer

$$(\forall b, c \mid: \langle b, c\rangle \in (S \cap T) \times (U \cap V) \;\equiv\; \langle b, c\rangle \in (S \times U) \cap (T \times V)).$$

Par le métathéorème (7.33), il suffit de montrer

$$\langle b, c\rangle \in (S \cap T) \times (U \cap V) \;\equiv\; \langle b, c\rangle \in (S \times U) \cap (T \times V),$$

ce que nous faisons.

$$\begin{array}{ll} & \langle b, c\rangle \in (S \cap T) \times (U \cap V) \\ = & \qquad \langle \text{ Appartenance (12.4) } \rangle \\ & b \in S \cap T \;\wedge\; c \in U \cap V \\ = & \qquad \langle \text{ Intersection (11.29), deux fois } \rangle \\ & b \in S \;\wedge\; b \in T \;\wedge\; c \in U \;\wedge\; c \in V \\ = & \qquad \langle \text{ Appartenance (12.4), deux fois } \rangle \\ & \langle b, c\rangle \in S \times U \;\wedge\; \langle b, c\rangle \in T \times V \\ = & \qquad \langle \text{ Intersection (11.29) } \rangle \\ & \langle b, c\rangle \in (S \times U) \cap (T \times V) \end{array}$$

5. Soient ρ et σ les relations suivantes sur l'ensemble $\{b, c, d, e\}$:

$$\begin{aligned} \rho &= \{\langle b, b\rangle, \langle b, c\rangle, \langle c, d\rangle\} \\ \sigma &= \{\langle b, c\rangle, \langle c, d\rangle, \langle d, b\rangle\} \end{aligned}$$

Calculez $\rho \circ \sigma$, $\sigma \circ \rho$, ρ^2 et ρ^3.

Solution.

$$\begin{aligned} \rho \circ \sigma &= \{\langle b, c\rangle, \langle b, d\rangle, \langle c, b\rangle\} \\ \sigma \circ \rho &= \{\langle b, d\rangle, \langle d, b\rangle, \langle d, c\rangle\} \\ \rho^2 &= \{\langle b, b\rangle, \langle b, c\rangle, \langle b, d\rangle\} \\ \rho^3 &= \{\langle b, b\rangle, \langle b, c\rangle, \langle b, d\rangle\} \end{aligned}$$

Voici en détail la manière de calculer $\sigma \circ \rho$. La manière la plus simple est de considérer toutes les combinaisons de couples venant de σ et de couples venant de ρ. Pour chaque paire de couples $\langle s, t\rangle \in \sigma$ et $\langle u, v\rangle \in \rho$, on a $\langle s, v\rangle \in \sigma \circ \rho$ si et seulement si $t = u$.

C'est ainsi que la colonne de droite dans la table ci-dessous est obtenue.

couples de σ	couples de ρ	couples de $\sigma \circ \rho$
$\langle b, c\rangle$	$\langle b, b\rangle$	
$\langle b, c\rangle$	$\langle b, c\rangle$	
$\langle b, c\rangle$	$\langle c, d\rangle$	$\langle b, d\rangle$
$\langle c, d\rangle$	$\langle b, b\rangle$	
$\langle c, d\rangle$	$\langle b, c\rangle$	
$\langle c, d\rangle$	$\langle c, d\rangle$	
$\langle d, b\rangle$	$\langle b, b\rangle$	$\langle d, b\rangle$
$\langle d, b\rangle$	$\langle b, c\rangle$	$\langle d, c\rangle$
$\langle d, b\rangle$	$\langle c, d\rangle$	

Regardez les définitions du produit ((12.24) et (12.25)) pour voir comment elles correspondent à la procédure ci-dessus.

6. Démontrez la sous-distributivité de $\circ$ sur $\cap$ (12.29),

$$\rho \circ (\sigma \cap \theta) \subseteq \rho \circ \sigma \cap \rho \circ \theta \qquad \text{et} \qquad (\sigma \cap \theta) \circ \rho \subseteq \sigma \circ \rho \cap \theta \circ \rho.$$

Solution. Seule la première inclusion sera démontrée. La démonstration de la deuxième est similaire.
Par la loi (11.21) (sous-ensemble), il suffit de démontrer

$$(\forall b, c \mid \langle b, c\rangle \in \rho \circ (\sigma \cap \theta) : \langle b, c\rangle \in \rho \circ \sigma \cap \rho \circ \theta).$$

Par transfert (7.17a), ceci est équivalent à

$$(\forall b, c \mid : \langle b, c\rangle \in \rho \circ (\sigma \cap \theta) \;\Rightarrow\; \langle b, c\rangle \in \rho \circ \sigma \cap \rho \circ \theta).$$

Par le métathéorème (7.33), il suffit de démontrer

$$\langle b, c\rangle \in \rho \circ (\sigma \cap \theta) \;\Rightarrow\; \langle b, c\rangle \in \rho \circ \sigma \cap \rho \circ \theta,$$

ce que fait la dérivation qui suit.

$$\begin{array}{ll} & \langle b, c\rangle \in \rho \circ \sigma \cap \rho \circ \theta \\ = & \qquad \langle \text{ Intersection (11.29) } \rangle \\ & \langle b, c\rangle \in \rho \circ \sigma \;\wedge\; \langle b, c\rangle \in \rho \circ \theta \\ = & \qquad \langle \text{ Définition du produit (12.24) } \rangle \\ & (\exists d \mid : \langle b, d\rangle \in \rho \wedge \langle d, c\rangle \in \sigma) \;\wedge\; (\exists d \mid : \langle b, d\rangle \in \rho \wedge \langle d, c\rangle \in \theta) \\ \Leftarrow & \qquad \langle \text{ Par la propriété (*) ci-dessous } \rangle \\ & (\exists d \mid : \langle b, d\rangle \in \rho \wedge \langle d, c\rangle \in \sigma \wedge \langle b, d\rangle \in \rho \wedge \langle d, c\rangle \in \theta) \\ = & \qquad \langle \text{ Idempotence de } \wedge \text{ (3.51) } \rangle \end{array}$$

$$
\begin{array}{ll}
 & (\exists d \mid: \langle b, d\rangle \in \rho \ \wedge\ \langle d, c\rangle \in \sigma \ \wedge\ \langle d, c\rangle \in \theta) \\
= & \qquad \langle \text{ Intersection (11.29) } \rangle \\
 & (\exists d \mid: \langle b, d\rangle \in \rho \ \wedge\ \langle d, c\rangle \in \sigma \cap \theta) \\
= & \qquad \langle \text{ Définition du produit (12.24) } \rangle \\
 & \langle b, c\rangle \in \rho \circ (\sigma \cap \theta)
\end{array}
$$

Le résultat suivant est utilisé dans la dérivation ci-dessus. C'est un résultat fort utile. Remarquez que l'implication est stricte, c'est-à-dire qu'on n'a pas l'équivalence (pour un contre-exemple à l'équivalence, prenez $P \equiv \mathsf{pair}.x$ et $Q \equiv \mathsf{impair}.x$).

$$
(*) \qquad (\exists x \mid R : P \wedge Q) \ \Rightarrow\ (\exists x \mid R : P) \ \wedge\ (\exists x \mid R : Q)
$$

Voici la démonstration de ce résultat.

$$
\begin{array}{ll}
 & (\exists x \mid R : P \wedge Q) \\
= & \qquad \langle \text{ Idempotence de } \wedge \text{ (3.51) } \rangle \\
 & (\exists x \mid R : P \wedge Q) \ \wedge\ (\exists x \mid R : P \wedge Q) \\
\Rightarrow & \qquad \langle \text{ Affaiblissement du corps (7.11), deux fois } \ \& \ \text{ Monotonie de } \wedge \text{ (4.3) } \rangle \\
 & (\exists x \mid R : (P \wedge Q) \vee P) \ \wedge\ (\exists x \mid R : (P \wedge Q) \vee Q) \\
= & \qquad \langle \text{ Absorption (3.61b), deux fois } \rangle \\
 & (\exists x \mid R : P) \ \wedge\ (\exists x \mid R : Q)
\end{array}
$$

7. Soit la relation $\rho \subseteq B \times B$. Démontrez le théorème (12.41), $\rho^m \circ \rho^n = \rho^{m+n}$, par induction.

Solution. La preuve est tout à fait semblable à celle qui concerne l'exponentiation et qui est donnée à la page 93 de ces notes. Il faut prouver $(\forall m, n{:}\mathbb{N} \mid: \rho^m \circ \rho^n = \rho^{m+n})$. Transformons cette formule pour l'amener sous la forme $(\forall n{:}\mathbb{N} \mid: P.n)$:

$$
\begin{array}{ll}
 & (\forall m, n{:}\mathbb{N} \mid: \rho^m \circ \rho^n = \rho^{m+n}) \\
= & \qquad \langle \ \neg\mathsf{libre}(\text{`}m\text{'},\text{`}\mathsf{vrai}\text{'}) \ \ \& \ \text{ Imbrication (6.34) } \rangle \\
 & (\forall n{:}\mathbb{N} \mid: (\forall m{:}\mathbb{N} \mid: \rho^m \circ \rho^n = \rho^{m+n}))
\end{array}
$$

(a) Définition du prédicat d'induction P :
Choisissons comme prédicat d'induction

$$
P.n : \quad (\forall m{:}\mathbb{N} \mid: \rho^m \circ \rho^n = \rho^{m+n}) \ .
$$

Il faut montrer $(\forall n{:}\mathbb{N} \mid: P.n)$.

(b) Étape de base : il faut prouver $P.0$, c'est-à-dire $(\forall m{:}\mathbb{N} \mid: \rho^m \circ \rho^0 = \rho^{m+0})$. Montrons $\rho^m \circ \rho^0 = \rho^{m+0}$ pour un m arbitraire (c'est suffisant, par le métathéorème (7.33).

$$
\begin{array}{ll}
& \rho^m \circ \rho^0 \\
= & \quad \langle \text{ Définition (12.39) de } \rho^0 \ \rangle \\
& \rho^m \circ \mathbf{I}_B \\
= & \quad \langle \ \mathbf{I}_B \text{ est l'élément neutre du produit (12.30)} \ \rangle \\
& \rho^m \\
= & \quad \langle \ 0 \text{ est l'élément neutre de l'addition} \ \rangle \\
& \rho^{m+0}
\end{array}
$$

(c) Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \mid{:}\ P.n \ \Rightarrow\ P(n+1))$. Supposons $P.n$ et montrons $P(n+1)$, c'est-à-dire

$$(\forall m{:}\mathbb{N} \mid{:}\ \rho^m \circ \rho^{n+1} = \rho^{m+(n+1)}) \ .$$

Par le métathéorème (7.33), il suffit de montrer $\rho^m \circ \rho^{n+1} = \rho^{m+(n+1)}$.

$$
\begin{array}{ll}
& \rho^m \circ \rho^{n+1} \\
= & \quad \langle \text{ Définition des puissances d'une relation (12.39), applicable, car } n \geq 0 \ \rangle \\
& \rho^m \circ (\rho^n \circ \rho) \\
= & \quad \langle \text{ Associativité de } \circ \text{ (12.27)} \ \rangle \\
& (\rho^m \circ \rho^n) \circ \rho \\
= & \quad \langle \text{ Hypothèse d'induction } P.n, \text{ car le corps de } P.n \text{ est } \mathsf{vrai} \text{ pour tout } m \ \rangle \\
& \rho^{m+n} \circ \rho \\
= & \quad \langle \ (12.39), \text{ applicable, car } m+n \geq 0 \ \rangle \\
& \rho^{m+n+1}
\end{array}
$$

8. La table (12.1) définit six classes de relations de deux manières différentes. Montrez que les deux définitions de l'asymétrie sont équivalentes.

Solution. Il faut montrer

$$(\forall b, c \mid{:}\ b\ \rho\ c\ \Rightarrow\ \neg(c\ \rho\ b)) \ \equiv\ \rho \cap \rho^{-1} = \emptyset.$$

Malgré que le côté gauche soit plus complexe, le début du développement du côté droit est simple. Il est clair qu'il faut introduire les variables b et c au moyen de l'extensionnalité. On obtient assez rapidement une formule aussi complexe que celle de gauche, qu'il devient facile de transformer en gardant la formule de gauche comme objectif. Si on commence la preuve avec le côté gauche, on ne voit pas aussi bien comment le transformer pour arriver au côté droit.

$$
\begin{array}{ll}
& \rho \cap \rho^{-1} = \emptyset \\
= & \quad \langle \text{ Extensionnalité (11.8) } \rangle \\
& (\forall b, c \mid: \langle b, c\rangle \in \rho \cap \rho^{-1} \ \equiv \ \langle b, c\rangle \in \emptyset) \\
= & \quad \langle \text{ Intersection (11.29) \& Appartenance à l'ensemble vide : il devrait y avoir la loi } x \in \emptyset \equiv \mathsf{faux} \text{ dans le manuel. Malheureusement, elle n'y est pas. On peut la déduire de (12.4) et d'un commentaire fait juste après (11.8). Voyez aussi l'exercice 11.4. Vous pouvez utiliser cette loi si vous en avez besoin à l'examen. } \rangle \\
& (\forall b, c \mid: \langle b, c\rangle \in \rho \ \wedge \ \langle b, c\rangle \in \rho^{-1} \ \equiv \ \mathsf{faux}) \\
= & \quad \langle \text{ Inverse (12.19) \& (3.18), } \neg p \equiv p \equiv \mathsf{faux} \ \rangle \\
& (\forall b, c \mid: \neg(\langle b, c\rangle \in \rho \ \wedge \ \langle c, b\rangle \in \rho)) \\
= & \quad \langle \text{ De Morgan (3.48a) \& Changement de notation } \rangle \\
& (\forall b, c \mid: \neg(b \ \rho \ c) \ \vee \ \neg(c \ \rho \ b)) \\
= & \quad \langle \text{ Définition de l'implication (3.75) } \rangle \\
& (\forall b, c \mid: b \ \rho \ c \ \Rightarrow \ \neg(c \ \rho \ b))
\end{array}
$$

9. La table (12.1) définit six classes de relations de deux manières différentes. Montrez que les deux définitions de l'asymétrie sont équivalentes.

Solution. Il faut montrer

$$(\forall b, c \mid: b \ \rho \ c \ \Rightarrow \ \neg(c \ \rho \ b)) \ \equiv \ \rho \cap \rho^{-1} = \emptyset.$$

Malgré que le côté gauche soit plus complexe, le début du développement du côté droit est simple. Il est clair qu'il faut introduire les variables b et c au moyen de l'extensionnalité. On obtient assez rapidement une formule aussi complexe que celle de gauche, qu'il devient facile de transformer en gardant la formule de gauche comme objectif. Si on commence la preuve avec le côté gauche, on ne voit pas aussi bien comment le transformer pour arriver au côté droit.

$$
\begin{array}{ll}
& \rho \cap \rho^{-1} = \emptyset \\
= & \quad \langle \text{ Extensionnalité (11.8) } \rangle \\
& (\forall b, c \mid: \langle b, c\rangle \in \rho \cap \rho^{-1} \ \equiv \ \langle b, c\rangle \in \emptyset) \\
= & \quad \langle \text{ Intersection (11.29) \& Appartenance à l'ensemble vide : cas particulier de (11.13) dans la liste des lois } \rangle \\
& (\forall b, c \mid: \langle b, c\rangle \in \rho \ \wedge \ \langle b, c\rangle \in \rho^{-1} \ \equiv \ \mathsf{faux}) \\
= & \quad \langle \text{ Inverse (12.19) \& (3.18), } \neg p \equiv p \equiv \mathsf{faux} \ \rangle \\
& (\forall b, c \mid: \neg(\langle b, c\rangle \in \rho \ \wedge \ \langle c, b\rangle \in \rho)) \\
= & \quad \langle \text{ De Morgan (3.48a) \& Changement de notation } \rangle \\
& (\forall b, c \mid: \neg(b \ \rho \ c) \ \vee \ \neg(c \ \rho \ b))
\end{array}
$$

$=$ ⟨ Définition de l'implication (3.75) ⟩

$(\forall b, c \mid : b \ \rho \ c \ \Rightarrow \ \neg(c \ \rho \ b))$

10. Quelles propriétés de la table (12.1) les relations suivantes possèdent-elles ?

(a) $b \ \rho \ c$ ssi b et c sont des entiers tous deux négatifs ou tous deux positifs.

(b) $b \ \rho \ c$ ssi b et c sont des entiers tels que $b - c$ est un multiple de 5.

(c) $\emptyset$, où $\emptyset$ est une relation sur un ensemble non vide B.

(d) $\mathbf{I}_B$, la relation identité sur un ensemble non vide B.

(e) $B \times B$, où B est un ensemble non vide contenant au moins deux éléments.

(f) $=$ sur $\mathbb{Z}$.

(g) $<$ sur $\mathbb{Z}$.

(h) $\leq$ sur $\mathbb{Z}$

(i) $b \ \rho \ c$ ssi b est le père de c.

(j) $b \ \rho \ c$ ssi b est le père de c ou vice-versa.

(k) $b \ \rho \ c$ ssi b est c ou le père de c.

Solution. Les propriété introduites dans la table (12.1) sont la réflexivité, l'irréflexivité, la symétrie, l'antisymétrie, l'asymétrie et la transitivité.

La table suivante contient un $\times$ dans la case [relation, propriété] ssi la relation a la propriété.

	réflexivité	irréflexivité	symétrie	antisymétrie	asymétrie	transitivité
(a)	×		×			×
(b)	×		×			×
(c)		×	×	×	×	×
(d)	×		×	×		×
(e)	×		×			×
(f)	×		×	×		×
(g)		×		×	×	×
(h)	×			×		×
(i)		×		×	×	
(j)		×	×			
(k)	×			×		

11. Trouvez un plus petit ensemble non vide et une relation sur cet ensemble qui n'est ni symétrique ni antisymétrique.

Solution. Appelons l'ensemble et la relation cherchés B et ρ, respectivement. Pour violer l'antisymétrie, il faut trouver des éléments b et c qui soient un contre-exemple à l'expression booléenne

$$b \,\rho\, c \wedge c \,\rho\, b \;\Rightarrow\; b = c.$$

Pour cela (rappelez-vous la recherche de contre-exemples, section 5.1 du manuel), il faut avoir $b \neq c$, c'est-à-dire avoir deux éléments différents, et il faut aussi avoir $b \,\rho\, c \wedge c \,\rho\, b$. La relation $\{\langle 1,2\rangle, \langle 2,1\rangle\}$ satisfait ces contraintes et elle n'est pas antisymétrique, mais elle est symétrique. Si l'ensemble B est $\{1,2\}$, les seules paires qu'on peut ajouter sont $\langle 1,1\rangle$ et $\langle 2,2\rangle$. L'ajout d'une de ces paires ou des deux préserve la symétrie de la relation. Il faut donc un ensemble avec un élément de plus, disons $B = \{1,2,3\}$. Voici une relation sur B qui n'est ni symétrique, ni antisymétrique (il y en a d'autres) :

$$\rho = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 1,3\rangle\}.$$

12. Considérons les relations binaires sur un ensemble B. On dit qu'une propriété est *préservée par une opération* si l'application de l'opération à des relations qui ont la propriété produit une relation qui a la propriété. Par exemple, l'union de deux relations symétriques est symétrique, de sorte que l'union préserve la symétrie. Inscrivez un O dans chaque entrée [ligne, colonne] de la table suivante si l'opération de la colonne préserve la propriété de la ligne et inscrivez un N dans le cas contraire. Pour chaque N, donnez un contre-exemple.

	$\rho \cup \sigma$	$\rho \cap \sigma$	$\rho - \sigma$	$(B \times B) - \rho$
Réflexivité				
Irréflexivité				
Symétrie				
Antisymétrie				
Transitivité				

Solution. Voici la réponse dans le cas de l'union. Des explications suivent. En plus des contre-exemples pour les N, on y explique la raison des O. Il faut évidemment utiliser la table (12.1) pour la définition des propriétés.

	$\rho \cup \sigma$	$\rho \cap \sigma$	$\rho - \sigma$	$(B \times B) - \rho$
Réflexivité	O			
Irréflexivité	O			
Symétrie	O			
Antisymétrie	N			
Transitivité	N			

(a) L'union préserve la réflexivité. Montrons que la réflexivité de ρ et de σ entraîne la réflexivité de $\rho \cup \sigma$.

$$\mathbf{I}_B \subseteq \rho \wedge \mathbf{I}_B \subseteq \sigma$$

$$
\begin{array}{ll}
\Rightarrow & \langle\ (11.51)\ \rangle \\
\quad \mathbf{I}_B \cup \mathbf{I}_B \subseteq \rho \cup \sigma & \\
= & \langle\ \text{Idempotence de } \cup\ (11.36\ \rangle \\
\quad \mathbf{I}_B \subseteq \rho \cup \sigma &
\end{array}
$$

(b) L'union préserve l'irréflexivité.

$$
\begin{array}{ll}
\quad \mathbf{I}_B \cap (\rho \cup \sigma) & \\
\subseteq & \langle\ \text{Distributivité de } \cap \text{ sur } \cup\ (11.49)\ \rangle \\
\quad (\mathbf{I}_B \cap \rho) \cup (\mathbf{I}_B \cap \sigma) & \\
= & \langle\ \text{Hypothèse que } \rho \text{ et } \sigma \text{ sont irréflexives}\ \rangle \\
\quad \emptyset \cup \emptyset & \\
= & \langle\ \text{Identité (élément neutre) de } \cup\ (11.38)\ \rangle \\
\quad \emptyset &
\end{array}
$$

(c) L'union préserve la symétrie.

$$
\begin{array}{ll}
\quad (\rho \cup \sigma)^{-1} & \\
= & \langle\ (12.37)\ \rangle \\
\quad \rho^{-1} \cup \sigma^{-1} & \\
= & \langle\ \text{Hypothèse que } \rho \text{ et } \sigma \text{ sont symétriques}\ \rangle \\
\quad \rho \cup \sigma &
\end{array}
$$

(d) L'union ne préserve pas l'antisymétrie. Les relations $\{\langle 1,2\rangle\}$ et $\{\langle 2,1\rangle\}$ sur l'ensemble $B = \{1,2\}$ sont antisymétriques, mais $\{\langle 1,2\rangle, \langle 2,1\rangle\}$ ne l'est pas.

(e) L'union ne préserve pas la transitivité. Les relations $\{\langle 1,2\rangle\}$ et $\{\langle 2,3\rangle\}$ sur l'ensemble $B = \{1,2,3\}$ sont transitives, mais $\{\langle 1,2\rangle, \langle 2,3\rangle\}$ ne l'est pas.

13. Soient les relations $\rho \subseteq \mathbb{Z} \times \mathbb{Z}$ et $\sigma \subseteq \mathbb{Z} \times \mathbb{Z}$ définies par

$$
\begin{array}{rcl}
\rho & = & \{b, c \mid b + 3 = c : \langle b, c\rangle\}, \\
\sigma & = & \{b, c \mid b^2 = c : \langle b, c\rangle\}.
\end{array}
$$

Calculez $\rho \circ \sigma$ et $\sigma \circ \rho$.

Solution. Voici le calcul de $\rho \circ \sigma$.

$$
\begin{array}{ll}
\quad \rho \circ \sigma & \\
= & \langle\ (12.21)\ \rangle \\
\quad \{b, c \mid \langle b, c\rangle \in \rho \circ \sigma : \langle b, c\rangle\} & \\
= & \langle\ \text{Définition de } \circ\ (12.24), \text{ avec } d := c\text{; cette transformation est détaillée ci-dessous}\ \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \{b, c \mid (\exists s \mid : \langle b, s\rangle \in \rho \ \wedge \ \langle s, c\rangle \in \sigma) : \langle b, c\rangle\} \\
= & \qquad \langle \text{ Définition de } \rho \text{ et } \sigma \ \ \& \ \ (12.22) \ \rangle \\
& \{b, c \mid (\exists s \mid : b + 3 = s \ \wedge \ s^2 = c) : \langle b, c\rangle\} \\
= & \qquad \langle \text{ Substitution (9.3a), avec } e, f, E \ := \ b + 3, s, z^2 = c \text{ ; l'objectif est} \\
& \qquad \text{de produire un terme sans } s \ \rangle \\
& \{b, c \mid (\exists s \mid : b + 3 = s \ \wedge \ (b + 3)^2 = c) : \langle b, c\rangle\} \\
= & \qquad \langle \ \neg\mathsf{libre}(\text{`}s\text{'},\text{`}(b + 3)^2 = c\text{'}) \ \ \& \ \text{Distributivité de } \wedge \text{ sur } \exists \ (7.4) \ \rangle \\
& \{b, c \mid (\exists s \mid : b + 3 = s) \ \wedge \ (b + 3)^2 = c : \langle b, c\rangle\} \\
= & \qquad \langle \text{ Sur } \mathbb{Z}, \text{ on peut toujours trouver un } s \text{ tel que } b + 3 = s \text{ ; autrement} \\
& \qquad \text{dit, quel que soit } b, \text{ la somme } b + 3 \text{ est définie } \rangle \\
& \{b, c \mid \mathsf{vrai} \ \wedge \ (b + 3)^2 = c : \langle b, c\rangle\} \\
= & \qquad \langle \text{ Identité de } \wedge \ (3.52) \ \rangle \\
& \{b, c \mid (b + 3)^2 = c : \langle b, c\rangle\}
\end{array}
$$

Intuitivement, c'est bien le résultat escompté. La relation ρ ajoute 3 et la relation σ élève au carré. Le produit $\rho \circ \sigma$ applique ρ, puis σ, et il élève donc $b + 3$ au carré.

Détaillons maintenant la deuxième transformation. Il s'agit de faire la substitution $d := c$ dans (12.24).

$$
\begin{array}{ll}
& \big(\langle b, d\rangle \in \rho \circ \sigma \ \equiv \ (\exists c \mid : \langle b, c\rangle \in \rho \wedge \langle c, d\rangle \in \sigma)\big)[d := c] \\
= & \qquad \langle \text{ Substitution dans les deux opérandes de } \equiv \ \rangle \\
& \langle b, c\rangle \in \rho \circ \sigma \ \equiv \ (\exists c \mid : \langle b, c\rangle \in \rho \wedge \langle c, d\rangle \in \sigma)[d := c] \\
= & \qquad \langle \text{ Il faut renommer, car } \mathsf{libre}(\text{`}c\text{'},\text{`}d, c\text{'}) \ \ \& \\
& \qquad\quad s \text{ est une nouvelle variable } \ \& \ \ (6.36) \ \rangle \\
& \langle b, c\rangle \in \rho \circ \sigma \ \equiv \ (\exists s \mid : \langle b, s\rangle \in \rho \wedge \langle s, d\rangle \in \sigma)[d := c] \\
= & \qquad \langle \ \neg\mathsf{libre}(\text{`}s\text{'},\text{`}d, c\text{'}) \ \ \& \ \ (6.14) \ \rangle \\
& \langle b, c\rangle \in \rho \circ \sigma \ \equiv \ (\exists s \mid : \langle b, s\rangle \in \rho \wedge \langle s, c\rangle \in \sigma)
\end{array}
$$

Habituellement, ces détails ne sont pas donnés. Cependant, les premières fois, il vaut mieux les calculer sur un brouillon, afin d'éviter les erreurs.

14.13 Problèmes du chapitre 13

1. Démontrez le corollaire (13.2), qui énonce qu'il y a un nombre pair de sommets de degré impair dans n'importe quel graphe.

   Solution. S'il y avait un nombre impair de sommets de degré impair, le total des degrés des sommets du graphe serait impair, ce qui contredirait le théorème (13.1).

   L'argument ci-dessus est tout à fait convaincant. Voici quand même une preuve plus formelle, qui utilise les notations introduites dans les chapitres précédents. Elle est

plus longue, mais elle indique toutes les lois utilisées dans l'argument très court donné ci-dessus (pas étonnant que ce type d'argument soit parfois difficile à suivre).
Soit $G = \langle S, A\rangle$ le graphe et soient S_1 et S_2 les ensembles de sommets de degré impair et pair, respectivement.

$$
\begin{array}{ll}
& \mathsf{pair}(\sum s \mid s \in S_1 : \mathsf{deg}.s) \\
= & \quad \langle\ s \in S_1 \wedge s \in S_2 \equiv \mathsf{faux}\ \ \&\ \text{Les sommes sont définies car les ensembles sont finis}\ \ \&\ \text{Par division du domaine (6.25)}, \\
& \qquad (\sum s \mid s \in S_1 : \mathsf{deg}.s) + (\sum s \mid s \in S_2 : \mathsf{deg}.s) = (\sum s \mid s \in S : \mathsf{deg}.s) \\
& \quad \rangle \\
& \mathsf{pair}\big((\sum s \mid s \in S : \mathsf{deg}.s) - (\sum s \mid s \in S_2 : \mathsf{deg}.s)\big) \\
= & \quad \langle\ (13.1)\ \rangle \\
& \mathsf{pair}\big(2 \cdot \#A - (\sum s \mid s \in S_2 : \mathsf{deg}.s)\big) \\
= & \quad \langle\ 2 \cdot \#A \text{ est pair ; la parité dépend donc de l'autre terme}\ \rangle \\
& \mathsf{pair}(\sum s \mid s \in S_2 : \mathsf{deg}.s) \\
= & \quad \langle\ \text{Chaque sommet de } S_2 \text{ a un degré pair et une somme de nombres pairs est paire}\ \rangle \\
& \mathsf{vrai}
\end{array}
$$

2. Démontrez par induction que le graphe complet K_n a $n \cdot (n-1)/2$ arêtes.

   Solution. Il faut montrer

   $$(\forall n{:}\mathbb{N} \mid n \geq 1 : K_n \text{ a } n \cdot (n-1)/2 \text{ arêtes}).$$

   Remarque : $n \geq 1$, car l'ensemble des sommets d'un graphe n'est pas vide, par définition.

   (a) Définition du prédicat d'induction P : Prenons comme prédicat d'induction

   $$P.n : \quad K_n \text{ a } n \cdot (n-1)/2 \text{ arêtes.}$$

   Il faut montrer $(\forall n{:}\mathbb{N} \mid n \geq 1 : P.n)$.

   (b) Étape de base : il faut prouver $P.1$, c'est-à-dire

   $$K_1 \text{ a } 1 \cdot (1-1)/2 \text{ arêtes,}$$

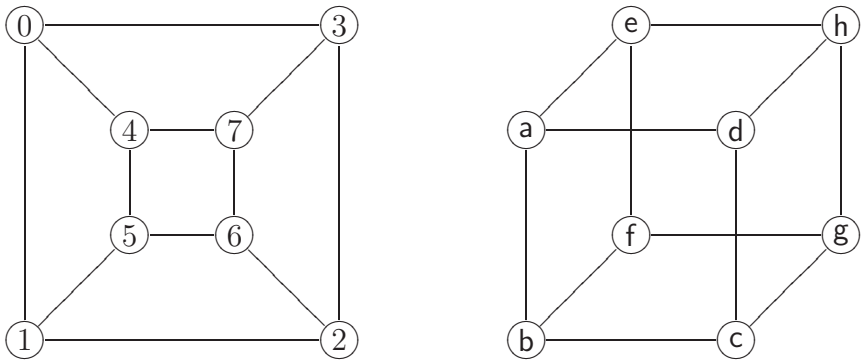
   ce qui est immédiat, puisque K_1 n'a qu'un sommet et donc pas d'arête.

   (c) Étape d'induction : Nous devons montrer $(\forall n{:}\mathbb{N} \mid n \geq 1 : P.n \Rightarrow P(n+1))$. Supposons $P.n$, et montrons $P(n+1)$, c'est-à-dire

   $$K_{n+1} \text{ a } (n+1) \cdot ((n+1)-1)/2 \text{ arêtes.}$$

$$
\begin{array}{ll}
& \text{Nombre d'arêtes de } K_{n+1} \\
= & \qquad \langle \text{ Si on enlève un sommet de } K_{n+1}, \text{ on enlève en même temps } n \\
& \qquad \text{arêtes et on obtient } K_n \ \rangle \\
& (\text{Nombre d'arêtes de } K_n) + n \\
= & \qquad \langle \text{ Hypothèse d'induction } P.n \ \rangle \\
& n \cdot (n-1)/2 + n \\
= & \qquad \langle \text{ Factorisation de } n \ \rangle \\
& n \cdot (\tfrac{n-1}{2} + 1) \\
= & \qquad \langle \text{ Arithmétique } \rangle \\
& n \cdot \tfrac{n+1}{2} \\
= & \qquad \langle \text{ Arithmétique } \rangle \\
& (n+1) \cdot ((n+1) - 1)/2
\end{array}
$$

3. Montrez que les deux graphes suivants sont isomorphes.



Solution. Posons que le graphe de gauche est $\langle S_1, A_1 \rangle$ et le graphe de droite $\langle S_2, A_2 \rangle$. Les ensembles de sommets sont

$$S_1 = \{0,1,2,3,4,5,6,7\} \qquad \text{et} \qquad S_2 = \{\mathsf{a},\mathsf{b},\mathsf{c},\mathsf{d},\mathsf{e},\mathsf{f},\mathsf{g},\mathsf{h}\}.$$

Il y a plusieurs applications bijectives $f{:}S_1 \to S_2$ qui déterminent un isomorphisme. En voici une.

$$f = \big\{\langle 0,\mathsf{a}\rangle, \langle 1,\mathsf{b}\rangle, \langle 2,\mathsf{c}\rangle, \langle 3,\mathsf{d}\rangle, \langle 4,\mathsf{e}\rangle, \langle 5,\mathsf{f}\rangle, \langle 6,\mathsf{g}\rangle, \langle 7,\mathsf{h}\rangle\big\}$$

Voici une autre manière de définir f :

$$f.0 = \mathsf{a},\ f.1 = \mathsf{b},\ f.2 = \mathsf{c},\ f.3 = \mathsf{d},\ f.4 = \mathsf{e},\ f.5 = \mathsf{f},\ f.6 = \mathsf{g},\ f.7 = \mathsf{h}.$$

Il reste à vérifier $\{v,w\} \in A_1 \equiv \{f.v, f.w\} \in A_2$ pour tout $v, w \in S_1$. Comme chaque graphe a huit sommets, cela fait $8^2 = 64$ arêtes à vérifier, ce qui est très fastidieux. Il est plus simple de procéder en deux étapes :

(a) Calculons $\{f.v, f.w\}$ pour toute arête $\{v, w\} \in A_1$ et vérifions si $\{f.v, f.w\} \in A_2$.

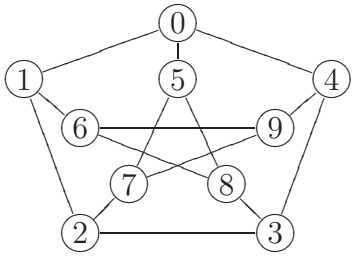
$\{v, w\}$	$\{f.v, f.w\}$	$\{f.v, f.w\} \in A_2$
$\{0, 1\}$	$\{\mathsf{a}, \mathsf{b}\}$	vrai
$\{4, 5\}$	$\{\mathsf{e}, \mathsf{f}\}$	vrai
$\{7, 6\}$	$\{\mathsf{h}, \mathsf{g}\}$	vrai
$\{3, 2\}$	$\{\mathsf{d}, \mathsf{c}\}$	vrai
$\{0, 3\}$	$\{\mathsf{a}, \mathsf{d}\}$	vrai
$\{4, 7\}$	$\{\mathsf{e}, \mathsf{h}\}$	vrai
$\{5, 6\}$	$\{\mathsf{f}, \mathsf{g}\}$	vrai
$\{1, 2\}$	$\{\mathsf{b}, \mathsf{c}\}$	vrai
$\{0, 4\}$	$\{\mathsf{a}, \mathsf{e}\}$	vrai
$\{3, 7\}$	$\{\mathsf{d}, \mathsf{h}\}$	vrai
$\{1, 5\}$	$\{\mathsf{b}, \mathsf{f}\}$	vrai
$\{2, 6\}$	$\{\mathsf{c}, \mathsf{g}\}$	vrai

(b) Il reste ensuite à vérifier que toutes les arêtes de A_2 ont ainsi été produites. C'est bien le cas. Les deux graphes sont donc isomorphes.

Cette deuxième étape permet d'éviter de vérifier que pour les 52 arêtes $\{v, w\} \notin A_1$, on a aussi $\{f.v, f.w\} \notin A_2$. Par exemple,

$\{v, w\}$	$\{f.v, f.w\}$	$\{f.v, f.w\} \in A_2$
$\{0, 2\}$	$\{\mathsf{a}, \mathsf{c}\}$	faux
$\{0, 5\}$	$\{\mathsf{a}, \mathsf{f}\}$	faux
$\ldots$	$\ldots$	$\ldots$

4. Trouvez un chemin Hamiltonien dans le graphe suivant.

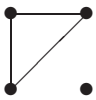


Solution. Il y en a plusieurs. En voici un :

$$\langle 0, 1, 2, 3, 4, 9, 6, 8, 5, 7 \rangle$$

5. Prouvez ou trouvez un contre-exemple : si un graphe $G = \langle S, A \rangle$ n'a pas de boucle et si $\#S = 1 + \#A$, alors G est un arbre.

Solution. L'énoncé est faux. Voici un contre-exemple.



6. Voici deux relations sur l'ensemble $S = \{1, 2, 3, 4\}$:

$$\begin{aligned} \rho_1 &= \{\langle 2,3\rangle, \langle 3,3\rangle, \langle 4,3\rangle\} \\ \rho_2 &= \{\langle 1,2\rangle, \langle 2,4\rangle, \langle 3,1\rangle, \langle 4,3\rangle\} \end{aligned}$$

   (a) Calculez $\rho_1 \cup \rho_2$, $\rho_1 \cap \rho_2$, $\sim\rho_1$, ρ_2^{-1}, $\rho_1 \circ \rho_2$, ρ_1^2, ρ_2^2, ρ_1^*, ρ_2^+.

   (b) Donnez la représentation graphique des graphes $\langle S, \rho_1\rangle$, $\langle S, \rho_2\rangle$, $\langle S, \rho_2^2\rangle$.

   (c) Donnez les matrices des relations ρ_1, ρ_2, ρ_2^*.

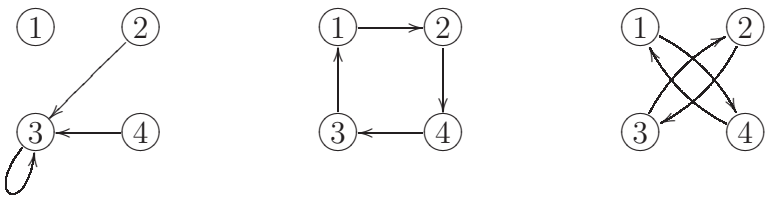
   (d) Dites lesquelles des propriétés suivantes les relations ρ_1, ρ_2, ρ_2^* possèdent :

   réflexivité, irréflexivité, symétrie, antisymétrie, asymétrie, transitivité, équivalence, totalité, surjectivité, déterminisme, injectivité, fonction, application, application bijective, ordre partiel, ordre partiel strict, ordre total.

Solution.

(a)
1. $\rho_1 \cup \rho_2 = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle, \langle 3,1\rangle, \langle 3,3\rangle, \langle 4,3\rangle\}$
2. $\rho_1 \cap \rho_2 = \{\langle 4,3\rangle\}$
3. $\sim\rho_1 = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,4\rangle,$
   $\langle 3,1\rangle, \langle 3,2\rangle, \langle 3,4\rangle, \langle 4,1\rangle, \langle 4,2\rangle, \langle 4,4\rangle\}$
4. $\rho_2^{-1} = \{\langle 2,1\rangle, \langle 4,2\rangle, \langle 1,3\rangle, \langle 3,4\rangle\}$
5. $\rho_1 \circ \rho_2 = \{\langle 2,1\rangle, \langle 3,1\rangle, \langle 4,1\rangle\}$
6. $\rho_1^2 = \rho_1$
7. $\rho_2^2 = \{\langle 1,4\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 4,1\rangle\}$
8. $\rho_1^* = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,3\rangle, \langle 4,3\rangle, \langle 4,4\rangle\}$
9. $\rho_2^+ = S \times S$
   $= \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle,$
   $\langle 3,1\rangle, \langle 3,2\rangle, \langle 3,3\rangle, \langle 3,4\rangle, \langle 4,1\rangle, \langle 4,2\rangle, \langle 4,3\rangle, \langle 4,4\rangle\}$

(b) $\langle S, \rho_1\rangle$ $\langle S, \rho_2\rangle$ $\langle S, \rho_2^2\rangle$



(c)
$$\rho_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \rho_2^* = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

(d)

	Propriété	ρ_1	ρ_2	ρ_2^*
(a)	réflexivité			×
(b)	irréflexivité		×	
(c)	symétrie			×
(d)	antisymétrie	×	×	
(e)	asymétrie		×	
(f)	transitivité	×		×
(g)	équivalence			×
(h)	totalité		×	×
(i)	surjectivité		×	×
(j)	déterminisme	×	×	
(k)	injectivité		×	
(l)	fonction	×	×	
(m)	application		×	
(n)	application bijective		×	
(o)	ordre partiel			
(p)	ordre partiel strict			
(q)	ordre total			

7. Calculez le produit suivant :
$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Solution.
$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Bibliographie

[1] E. W. Dijkstra. Guarded commands, nondeterminacy and the formal derivation of programs. *Communications of the ACM* 18, août 1975, 453–457.

[2] E. W. Dijkstra. *A Discipline of Programming*. Prentice Hall, Englewood Cliffs, 1976.

[3] E. W. Dijkstra et W. H. J. Feijen. *A Method of Programming*. Addison-Wesley publishing company, Wokingham, Angleterre.

[4] D. Gries et F. B. Schneider. *A Logical Approach to Discrete Math.* Springer-Verlag, New York, 1993.

[5] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM* 12, octobre 1969, 576–580, 583.

[6] K. H. Rosen. *Mathématiques discrètes*. Chenelière/McGraw-Hill, Montréal, 1998. Traduction de *Discrete Mathematics and its Applications*.

Annexe A

Préséance (priorité) des opérateurs

(1) $[x := e]$ (substitution textuelle) (priorité élevée)

(2) $.$ (application de fonction)

(3) $+ \quad - \quad \neg \quad \mathcal{P}$ (opérateurs unaires préfixes)

(4) $\cdot \quad / \quad \div \quad \mathsf{mod} \quad \mathsf{pgcd} \quad \times \quad \circ \quad \bullet$

(5) $+ \quad - \quad \cup \quad \cap$ (opérateurs binaires)

(6) $\downarrow \quad \uparrow$

(7) $= \quad < \quad > \quad \in \quad \subset \quad \subseteq \quad \supset \quad \supseteq \quad | \quad \neq \quad \not< \quad \not> \quad \notin \quad \not\subset \quad \not\subseteq \quad \not\supset \quad \not\supseteq \quad \not|$ (conjonctifs, voir page 16)

(8) $\vee \quad \wedge$

(9) $\Rightarrow \quad \Leftarrow \quad \not\Rightarrow \quad \not\Leftarrow$

(10) $\equiv \quad \not\equiv$ (priorité faible)

Les opérateurs binaires non associatifs sont associatifs à gauche, sauf $\Rightarrow$, qui est associatif à droite. Si $\Box$ est un opérateur binaire et que $a \Box b$ est une expression booléenne, alors la notation $a \not\Box b$ est une abréviation pour l'expression $\neg(a \Box b)$. L'opérateur $\not\Box$ a la même préséance que $\Box$. On voit des exemples de tels opérateurs aux lignes (7, 9, 10). Vous pouvez utiliser cette abréviation en tout temps et il n'est pas nécessaire de donner un numéro de loi pour la justifier *si un tel numéro de loi n'existe pas*.

Annexe B

Liste des lois

(1.9) Substitution : $\dfrac{E}{E[v := F]}$

(1.10) Réflexivité : $x = x$

(1.11) Symétrie (commutativité) : $(x = y) = (y = x)$

(1.12) Transitivité : $\dfrac{X = Y, \quad Y = Z}{X = Z}$

(1.13) Leibniz : $\dfrac{X = Y}{E[z := X] = E[z := Y]}$

(1.17) Leibniz : $\dfrac{X = Y}{g.X = g.Y}$

(3.2) Axiome, associativité de $\equiv$: $\big((p \equiv q) \equiv r\big) \;\equiv\; \big(p \equiv (q \equiv r)\big)$

(3.3) Axiome, commutativité (symétrie) de $\equiv$: $p \equiv q \equiv q \equiv p$

(3.4) Axiome, identité (élément neutre) de $\equiv$: $\mathsf{vrai} \equiv p \equiv p$

(3.6) Théorème : vrai

(3.7) Théorème, réflexivité de $\equiv$: $p \equiv p$

(3.11) Axiome, définition de faux : $\mathsf{faux} \equiv \neg\mathsf{vrai}$

(3.12) Axiome, distributivité de $\neg$ sur $\equiv$: $\neg(p \equiv q) \;\equiv\; \neg p \equiv q$

(3.13) Axiome, définition de $\not\equiv$: $(p \not\equiv q) \;\equiv\; \neg(p \equiv q)$

(3.14) $\neg p \equiv q \;\equiv\; p \equiv \neg q$

(3.15) Double négation : $\neg\neg p \equiv p$

(3.16) Négation de faux : $\neg\mathsf{faux} \equiv \mathsf{vrai}$

(3.17) $(p \not\equiv q) \;\equiv\; \neg p \equiv q$

(3.18) $\neg p \equiv p \equiv \mathsf{faux}$

(3.19) Commutativité (symétrie) de $\not\equiv$: $(p \not\equiv q) \;\equiv\; (q \not\equiv p)$

(3.20) Associativité de $\not\equiv$: $\big((p \not\equiv q) \not\equiv r\big) \;\equiv\; \big(p \not\equiv (q \not\equiv r)\big)$

(3.21) Associativité mutuelle : $\big((p \not\equiv q) \equiv r\big) \;\equiv\; \big(p \not\equiv (q \equiv r)\big)$

(3.22) Interchangeabilité mutuelle : $p \not\equiv q \equiv r \;\equiv\; p \equiv q \not\equiv r$

(3.32) Axiome, commutativité (symétrie) de $\vee$: $p \vee q \;\equiv\; q \vee p$

(3.33) Axiome, associativité de $\vee$: $(p \vee q) \vee r \;\equiv\; p \vee (q \vee r)$

(3.34) Axiome, idempotence de $\vee$: $p \vee p \equiv p$

(3.36) Axiome, distributivité de $\vee$ sur $\equiv$: $p \vee (q \equiv r) \;\equiv\; p \vee q \;\equiv\; p \vee r$

(3.37) Axiome, tiers exclu : $p \vee \neg p$ ou encore $p \vee \neg p \equiv \mathsf{vrai}$

(3.38) Zéro de $\vee$: $p \vee \mathsf{vrai} \equiv \mathsf{vrai}$

(3.40) Identité de $\vee$: $p \vee \mathsf{faux} \equiv p$

(3.41) Distributivité de $\vee$ sur $\vee$: $p \vee (q \vee r) \;\equiv\; (p \vee q) \vee (p \vee r)$

(3.42) $p \vee q \;\equiv\; p \vee \neg q \;\equiv\; p$

(3.47) Axiome, De Morgan : $p \wedge q \;\equiv\; \neg(\neg p \vee \neg q)$

(3.48) De Morgan, formes alternatives :

(a) $\neg(p \wedge q) \;\equiv\; \neg p \vee \neg q$
(b) $\neg(p \vee q) \;\equiv\; \neg p \wedge \neg q$
(c) $p \vee q \;\equiv\; \neg(\neg p \wedge \neg q)$

(3.49) Commutativité (symétrie) de $\wedge$: $p \wedge q \;\equiv\; q \wedge p$

(3.50) Associativité de $\wedge$: $(p \wedge q) \wedge r \;\equiv\; p \wedge (q \wedge r)$

(3.51) Idempotence de $\wedge$: $p \wedge p \equiv p$

(3.52) Identité de $\wedge$: $p \wedge \mathsf{vrai} \equiv p$

(3.53) Zéro de $\wedge$: $p \wedge \mathsf{faux} \equiv \mathsf{faux}$

(3.54) Distributivité de $\wedge$ sur $\wedge$: $p \wedge (q \wedge r) \;\equiv\; (p \wedge q) \wedge (p \wedge r)$

(3.55) Contradiction : $p \wedge \neg p \equiv \mathsf{faux}$

(3.57) Règle d'or : $p \wedge q \;\equiv\; p \;\equiv\; q \;\equiv\; p \vee q$

(3.59) Distributivité de $\vee$ sur $\wedge$: $p \;\vee\; (q \wedge r) \;\equiv\; (p \vee q) \;\wedge\; (p \vee r)$

(3.60) Distributivité de $\wedge$ sur $\vee$: $p \;\wedge\; (q \vee r) \;\equiv\; (p \wedge q) \;\vee\; (p \wedge r)$

(3.61) Absorption :

(a) $p \;\wedge\; (p \vee q) \equiv p$
(b) $p \;\vee\; (p \wedge q) \equiv p$
(c) $p \;\wedge\; (\neg p \vee q) \;\equiv\; p \wedge q$
(d) $p \;\vee\; (\neg p \wedge q) \;\equiv\; p \vee q$

(3.62) $p \wedge q \;\equiv\; p \wedge \neg q \;\equiv\; \neg p$

(3.63) $p \;\wedge\; (q \equiv r) \;\equiv\; p \wedge q \;\equiv\; p \wedge r \;\equiv\; p$

(3.64) $p \;\wedge\; (q \equiv p) \;\equiv\; p \wedge q$

(3.65) Remplacement : $(p \equiv q) \;\wedge\; (r \equiv p) \;\equiv\; (p \equiv q) \;\wedge\; (r \equiv q)$

(3.66) Définition de $\equiv$: $p \equiv q \;\equiv\; (p \wedge q) \;\vee\; (\neg p \wedge \neg q)$

(3.67) **Ou exclusif :** $p \not\equiv q \;\equiv\; (\neg p \wedge q) \vee (p \wedge \neg q)$

(3.71) $(p \wedge q) \wedge r \quad\equiv\quad p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r$

(3.73) **Axiome, définition de $\Rightarrow$:** $p \Rightarrow q \;\equiv\; p \vee q \;\equiv\; q$

(3.74) **Axiome, conséquence :** $p \Leftarrow q \;\equiv\; q \Rightarrow p$

(3.75) **Définition alternative de $\Rightarrow$:** $p \Rightarrow q \;\equiv\; \neg p \vee q$

(3.76) **Définition alternative de $\Rightarrow$:** $p \Rightarrow q \;\equiv\; p \wedge q \;\equiv\; p$

(3.77) **Contrapositivité :** $p \Rightarrow q \;\equiv\; \neg q \Rightarrow \neg p$

(3.78) $p \Rightarrow (q \equiv r) \;\equiv\; p \wedge q \;\equiv\; p \wedge r$

(3.79) **Distributivité de $\Rightarrow$ sur $\equiv$:** $p \Rightarrow (q \equiv r) \;\equiv\; p \Rightarrow q \;\equiv\; p \Rightarrow r$

(3.80) $p \Rightarrow (q \Rightarrow r) \;\equiv\; (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$

(3.81) **Transfert :** $p \wedge q \;\Rightarrow\; r \;\equiv\; p \Rightarrow (q \Rightarrow r)$

(3.82) $p \wedge (p \Rightarrow q) \;\equiv\; p \wedge q$

(3.83) $p \wedge (q \Rightarrow p) \;\equiv\; p$

(3.84) $p \vee (p \Rightarrow q) \;\equiv\; \mathsf{vrai}$

(3.85) $p \vee (q \Rightarrow p) \equiv q \Rightarrow p$

(3.86) $p \vee q \;\Rightarrow\; p \wedge q \;\equiv\; p \equiv q$

(3.87) **Réflexivité de $\Rightarrow$:** $p \Rightarrow p \;\equiv\; \mathsf{vrai}$ ou encore $p \Rightarrow p$

(3.88) **Zéro à droite de $\Rightarrow$:** $p \Rightarrow \mathsf{vrai} \;\equiv\; \mathsf{vrai}$ ou encore $p \Rightarrow \mathsf{vrai}$

(3.89) **Identité à gauche de $\Rightarrow$:** $\mathsf{vrai} \Rightarrow p \;\equiv\; p$

(3.90) $p \Rightarrow \mathsf{faux} \;\equiv\; \neg p$

(3.91) $\mathsf{faux} \Rightarrow p \;\equiv\; \mathsf{vrai}$ ou encore $\mathsf{faux} \Rightarrow p$

(3.92) **Affaiblissement, renforcement :**
(a) $p \;\Rightarrow\; p \vee q$
(b) $p \wedge q \;\Rightarrow\; p$
(c) $p \wedge q \;\Rightarrow\; p \vee q$
(d) $p \vee (q \wedge r) \;\Rightarrow\; p \vee q$
(e) $p \wedge q \;\Rightarrow\; p \wedge (q \vee r)$

(3.93) **Modus ponens :** $p \wedge (p \Rightarrow q) \;\Rightarrow\; q$

(3.94) $(p \Rightarrow r) \wedge (q \Rightarrow r) \;\equiv\; (p \vee q \;\Rightarrow\; r)$

(3.95) $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \;\equiv\; r$

(3.97) **Implication mutuelle :** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\equiv\; p \equiv q$

(3.98) **Antisymétrie :** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\Rightarrow\; (p \equiv q)$

(3.99) **Transitivité :**
(a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

(3.100) **Métathéorème :** Deux théorèmes quelconques sont équivalents.

(4.1) $p \Rightarrow (q \Rightarrow p)$

(4.2) Monotonie de $\vee$: $(p \Rightarrow q) \;\Rightarrow\; (p \vee r \;\Rightarrow\; q \vee r)$

(4.3) Monotonie de $\wedge$: $(p \Rightarrow q) \;\Rightarrow\; (p \wedge r \;\Rightarrow\; q \wedge r)$

(4.6) Déduction : Pour montrer $P_1 \wedge \ldots \wedge P_n \;\Rightarrow\; Q$, assumez $P_1, \ldots, P_n$ et prouvez Q.

(6.14) Définition : Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}x, F\text{'})$,

$$(\star y \mid R : P)[x := F] \;=\; (\star y \mid R[x := F] : P[x := F]) \;.$$

(6.19) Axiome, domaine vide : $(\star x \mid \mathsf{faux} : P) = u$ (où u est l'élément neutre de $\star$) .

(6.21) Axiome du point : Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}E\text{'})$, $(\star x \mid x = E : P) \;=\; P[x := E]$.

(6.23) Axiome, distributivité : Pourvu que chaque quantification soit définie,

$$(\star x \mid R : P) \;\star\; (\star x \mid R : Q) \;=\; (\star x \mid R : P \star Q) \;.$$

(6.25) Axiome, division du domaine : Pourvu que $R \wedge S \equiv \mathsf{faux}$ et que chaque quantification soit définie,

$$(\star x \mid R \vee S : P) \;=\; (\star x \mid R : P) \;\star\; (\star x \mid S : P) \;.$$

(6.27) Axiome, division du domaine (généralisation de (6.25)) :
Pourvu que chaque quantification soit définie,

$$(\star x \mid R \vee S : P) \;\star\; (\star x \mid R \wedge S : P) \;=\; (\star x \mid R : P) \;\star\; (\star x \mid S : P) \;.$$

(6.29) Axiome, division du domaine si $\star$ est idempotent :
Pourvu que chaque quantification soit définie,

$$(\star x \mid R \vee S : P) \;=\; (\star x \mid R : P) \;\star\; (\star x \mid S : P) \;.$$

(6.31) Axiome, échange des variables de quantification : Pourvu que chaque quantification soit définie et que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R\text{'})$ et $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}Q\text{'})$,

$$(\star x \mid R : (\star y \mid Q : P)) \;=\; (\star y \mid Q : (\star x \mid R : P)) \;.$$

(6.34) Axiome, imbrication : Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R\text{'})$,

$$(\star x, y \mid R \wedge Q : P) \;=\; (\star x \mid R : (\star y \mid Q : P)) \;.$$

(6.36) Axiome, renommage des variables de quantification :
Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R, P\text{'})$,

$$(\star x \mid R : P) \;=\; (\star y \mid R[x := y] : P[x := y]) \;.$$

(6.39) Changement des variables de quantification : Pourvu que f ait un inverse et que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R, P\text{'})$,

$$(\star x \mid R : P) \;=\; (\star y \mid R[x := f.y] : P[x := f.y]) \;.$$

(6.40) Théorème, extraction d'un terme : Soit $n{:}\mathbb{N}$.

$$(\star i{:}\mathbb{N} \mid k \le i < n+1 : P) \;=\; (\star i{:}\mathbb{N} \mid k \le i < n : P) \;\star\; P[i := n]$$
$$(\star i{:}\mathbb{N} \mid k \le i < n+1 : P) \;=\; P[i := k] \;\star\; (\star i{:}\mathbb{N} \mid k < i < n+1 : P)$$

(7.1) Axiome, transfert : $(\exists x \mid R : P) \;\equiv\; (\exists x \mid\!: R \wedge P)$

(7.2) Transfert : $(\exists x \mid Q \wedge R : P) \;\equiv\; (\exists x \mid Q : R \wedge P)$

(7.4) Axiome, distributivité de $\wedge$ sur $\exists$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$P \wedge (\exists x \mid R : Q) \;\equiv\; (\exists x \mid R : P \wedge Q)$$

(7.6) Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$, $(\exists x \mid R : P) \;\equiv\; P \wedge (\exists x \mid\!: R)$

(7.7) Distributivité de $\vee$ sur $\exists$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$(\exists x \mid\!: R) \;\Rightarrow\; \big((\exists x \mid R : P \vee Q) \;\equiv\; P \vee (\exists x \mid R : Q)\big)$$

(7.8) $(\exists x \mid R : \mathsf{faux}) \;\equiv\; \mathsf{faux}$

(7.9) Affaiblissement/renforcement du domaine :

$$(\exists x \mid R : P) \;\Rightarrow\; (\exists x \mid Q \vee R : P)$$

(7.11) Affaiblissement/renforcement du corps : $(\exists x \mid R : P) \;\Rightarrow\; (\exists x \mid R : P \vee Q)$

(7.12) $\exists$-Introduction : $P[x := E] \;\Rightarrow\; (\exists x \mid\!: P)$

(7.15) Axiome, De Morgan : $(\forall x \mid R : P) \;\equiv\; \neg(\exists x \mid R : \neg P)$

(7.16) De Morgan :
(a) $(\exists x \mid R : P) \;\equiv\; \neg(\forall x \mid R : \neg P)$
(b) $(\forall x \mid R : \neg P) \;\equiv\; \neg(\exists x \mid R : P)$
(c) $(\exists x \mid R : \neg P) \;\equiv\; \neg(\forall x \mid R : P)$

(7.17) Transfert :
(a) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid\!: R \Rightarrow P)$
(b) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid\!: \neg R \vee P)$
(c) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid\!: R \wedge P \;\equiv\; R)$
(d) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid\!: R \vee P \;\equiv\; P)$

(7.20) Transfert :
(a) $(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : R \Rightarrow P)$
(b) $(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : \neg R \vee P)$
(c) $(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : R \wedge P \;\equiv\; R)$
(d) $(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : R \vee P \;\equiv\; P)$

(7.21) Distributivité de $\vee$ sur $\forall$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$P \vee (\forall x \mid R : Q) \;\equiv\; (\forall x \mid R : P \vee Q)$$

(7.22) Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$, $(\forall x \mid R : P) \;\equiv\; P \vee (\forall x \mid\!: \neg R)$

(7.23) Distributivité de $\wedge$ sur $\forall$: Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'})$,

$$(\exists x \mid\!: R) \;\Rightarrow\; \big((\forall x \mid R : P \wedge Q) \;\equiv\; P \wedge (\forall x \mid R : Q)\big)$$

(7.24) $(\forall x \mid R : \mathsf{vrai}) \;\equiv\; \mathsf{vrai}$

(7.26) $(\forall x \mid R : P \equiv Q) \;\Rightarrow\; \big((\forall x \mid R : P) \;\equiv\; (\forall x \mid R : Q)\big)$

(7.27) Affaiblissement/renforcement du domaine :

$$(\forall x \mid Q \vee R : P) \;\Rightarrow\; (\forall x \mid Q : P)$$

(7.29) Affaiblissement/renforcement du corps : $(\forall x \mid R : P \wedge Q) \;\Rightarrow\; (\forall x \mid R : P)$

(7.30) Élimination : $(\forall x \mid\!: P) \;\Rightarrow\; P[x := E]$

(7.33) Métathéorème : P est un théorème ssi $(\forall x \mid\!: P)$ est un théorème.

(7.34) Monotonie de $\forall$: $(\forall x \mid R : Q \Rightarrow P) \;\Rightarrow\; \big((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P)\big)$

(7.36) Monotonie de $\exists$: $(\forall x \mid R : Q \Rightarrow P) \;\Rightarrow\; \big((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P)\big)$

(7.37) Échange de $\forall, \exists$: Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R\text{'})$ et $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}Q\text{'})$,

$$(\exists x \mid R : (\forall y \mid Q : P)) \;\Rightarrow\; (\forall y \mid Q : (\exists x \mid R : P))$$

(8.2) Induction mathématique (faible) sur $\mathbb{N}$:

$$P.0 \;\wedge\; (\forall n{:}\mathbb{N} \mid\!: P.n \;\Rightarrow\; P(n+1)) \;\Rightarrow\; (\forall n{:}\mathbb{N} \mid\!: P.n)$$

(8.5) Induction mathématique (faible) sur $\{n_0,\ n_0+1,\ n_0+2,\ \ldots\}$:

$$P.n_0 \;\wedge\; (\forall n \mid n_0 \le n : P.n \;\Rightarrow\; P(n+1)) \;\Rightarrow\; (\forall n \mid n_0 \le n : P.n)$$

(8.7) $b^0 = 1$
$b^{n+1} = b \cdot b^n \quad (\text{si } n \ge 0)$

(8.10) $0! = 1$
$k! = k \cdot (k-1)! \quad (\text{si } k > 0)$

(8.14) Induction sur $\{n_0,\ n_0+1,\ n_0+2,\ \ldots\}$, deux cas de base :

$$P.n_0 \;\wedge\; P(n_0+1) \;\wedge\; (\forall n \mid n_0 \le n : P.n \wedge P(n+1) \;\Rightarrow\; P(n+2))$$
$$\Rightarrow (\forall n \mid n_0 \le n : P.n)$$

(9.1) Axiome, Leibniz : $(e = f) \Rightarrow (E[z := e] = E[z := f])$

ou encore $(e = f) \Rightarrow (E[z := e] = E[z := f])$

(9.3) Substitution : (a) $(e = f) \wedge E[z := e] \equiv (e = f) \wedge E[z := f]$

(b) $(e = f) \Rightarrow E[z := e] \equiv (e = f) \Rightarrow E[z := f]$

(c) $q \wedge (e = f) \Rightarrow E[z := e] \equiv q \wedge (e = f) \Rightarrow E[z := f]$

(9.4) Remplacement par vrai : (a) $p \Rightarrow E[z := p] \equiv p \Rightarrow E[z := \mathsf{vrai}]$

(b) $p \wedge q \Rightarrow E[z := p] \equiv p \wedge q \Rightarrow E[z := \mathsf{vrai}]$

(9.5) Remplacement par faux : (a) $E[z := p] \Rightarrow p \equiv E[z := \mathsf{faux}] \Rightarrow p$

(b) $E[z := p] \Rightarrow p \vee q \equiv E[z := \mathsf{faux}] \Rightarrow p \vee q$

(9.6) Remplacement par vrai : $p \wedge E[z := p] \equiv p \wedge E[z := \mathsf{vrai}]$

(9.7) Remplacement par faux : $p \vee E[z := p] \equiv p \vee E[z := \mathsf{faux}]$

(9.8) Shannon : $E[z := p] \equiv (p \wedge E[z := \mathsf{vrai}]) \vee (\neg p \wedge E[z := \mathsf{faux}])$

(9.10) Preuve par cas :
Si $E[z := \mathsf{vrai}]$ et $E[z := \mathsf{faux}]$ sont des théorèmes, alors $E[z := p]$ en est un

(9.12) $(p \vee q \vee r) \wedge (p \Rightarrow s) \wedge (q \Rightarrow s) \wedge (r \Rightarrow s) \Rightarrow s$

(9.14) Preuve par implication mutuelle : Pour démontrer $P \equiv Q$, montrez $P \Rightarrow Q$ et $Q \Rightarrow P$

(9.15) Preuve par contradiction : Pour démontrer P, démontrez $\neg p \Rightarrow \mathsf{faux}$

(9.21) Preuve par contraposition : Pour démontrer $P \Rightarrow Q$, montrez $\neg Q \Rightarrow \neg P$

(10.5) Définition de l'affectation : Pourvu que E soit définie dans tous les états,

$$\{R[x := E]\} \quad x := E \quad \{R\}$$

(10.11) Définition de l'affectation : $\{\mathsf{dom}.\text{`}E\text{'} \wedge R[x := E]\} \quad x := E \quad \{R\}$

(10.20) Axiome : $\{Q\} \quad S \quad \{R\} \quad \equiv \quad Q \Rightarrow \mathsf{wp}(S, R)$

(10.21) Axiome de l'affectation : $\mathsf{wp}(x := E, R) \equiv \mathsf{dom}.\text{`}E\text{'} \wedge R[x := E]$

(10.22) Axiome de l'affectation si E totale : $\mathsf{wp}(x := E, R) \equiv R[x := E]$

(10.29) Axiome de la séquence :

$$\mathsf{wp}(S_1; S_2, R) \equiv \mathsf{wp}(S_1, \mathsf{wp}(S_2, R))$$

(10.31) Axiome de l'instruction skip : $\{Q\} \quad \textbf{skip} \quad \{R\} \quad \equiv \quad Q \Rightarrow R$

(10.33) Axiome de l'instruction conditionnelle :

$$\{Q\} \quad \mathsf{IF} \quad \{R\} \quad \equiv \quad \{Q \wedge B\} \quad S_1 \quad \{R\} \quad \wedge \quad \{Q \wedge \neg B\} \quad S_2 \quad \{R\}$$

(10.37) Axiome du bloc begin-end :

$$\{Q\} \quad \textbf{begin } S \textbf{ end} \quad \{R\} \quad \equiv \quad \{Q\} \quad S \quad \{R\}.$$

(10.41) Théorème d'invariance : Supposons

1. $\{P \wedge B\}\ \ S\ \ \{P\}$
   (c'est-à-dire que l'exécution de S se termine dans un état qui satisfait P si elle débute dans un état qui satisfait P et B) ;
2. $\{P\}\quad \textbf{while}\ B\ \textbf{do}\ S\ \ \{\mathsf{vrai}\}$
   (c'est-à-dire que l'exécution de la boucle se termine si elle débute dans un état qui satisfait P).

Alors

$$\{P\}\quad \textbf{while}\ B\ \textbf{do}\ S\ \ \{P \wedge \neg B\}$$

est un théorème.

(10.43) Vérification d'une boucle initialisée : Pour que

$$\{Q\}\ \ S';\ \{\text{Invariant } P\}\ \ \textbf{while}\ B\ \textbf{do}\ S\ \ \{R\}$$

soit un théorème, il suffit que

(a) P soit vrai avant l'exécution de la boucle : $\{Q\}\ \ S'\ \ \{P\}$;
(b) P soit un invariant de la boucle : $\{P \wedge B\}\ \ S\ \ \{P\}$;
(c) l'exécution de la boucle se termine ;
(d) R soit vrai à la fin de l'exécution : $P \wedge \neg B \Rightarrow R$.

(10.45) Preuve de terminaison : Pour montrer que l'exécution de

$\{\text{Invariant } P\}$
$\{\text{Fonction majorante } M\}$
while B **do** S

se termine, il suffit que

(a) M soit une fonction à valeur entière ;
(b) M décroisse à chaque itération : $\{P \wedge B \wedge M = \mathsf{X}\}\ \ S\ \ \{M < \mathsf{X}\}$;
(c) tant qu'il reste une itération, $M > 0 : P \wedge B \Rightarrow M > 0$.

(11.1) $\{e_0, \ldots, e_{n-1}\} \ = \ \{x \mid x = e_0 \vee \ldots \vee x = e_{n-1} : x\}$

Cas particulier : $\{\} = \emptyset = \{x \mid \mathsf{faux} : x\} = \{x \mid \mathsf{faux}\}$

(11.5) Axiome, appartenance : Pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}F\text{'})$,

$$F \in \{x \mid R : E\} \ \equiv \ (\exists x \mid R : F = E)$$

(11.6) Appartenance, cas particulier : $F \in \{x \mid R : x\} \ \equiv \ R[x := F]$

(11.8) Axiome, extensionnalité : $S = T \ \equiv \ (\forall x \mid : x \in S \equiv x \in T)$

(11.9) $S = \{x \mid x \in S : x\}$

(11.10) Pourvu que $\neg\mathsf{libre}(\text{`}y\text{'},\text{`}R, E\text{'})$, $\{x \mid R : E\} \ = \ \{y \mid (\exists x \mid R : y = E)\}$

(11.12) Appartenance, cas particulier, notation traditionnelle :

$$F \in \{x \mid R\} \;\equiv\; R[x := F]$$

(11.13) $x \in \{x \mid R\} \;\equiv\; R$

Cas particulier : $x \in \emptyset \;\equiv\; \mathsf{faux}$

(11.16) $\{x \mid Q\} = \{x \mid R\} \;\equiv\; (\forall x \mid\colon Q \equiv R)$

(11.17) **Métathéorème :** $\{x \mid Q\} = \{x \mid R\}$ est un théorème si et seulement si $(\forall x \mid\colon Q \equiv R)$ est un théorème.

(11.19) **Axiome, cardinalité :** $\#S = (\sum x \mid x \in S : 1)$

(11.21) **Axiome, sous-ensemble :** $S \subseteq T \;\equiv\; (\forall x \mid x \in S : x \in T)$

(11.22) **Axiome, sous-ensemble propre :** $S \subset T \;\equiv\; S \subseteq T \;\wedge\; S \neq T$

(11.23) **Axiome, surensemble :** $T \supseteq S \;\equiv\; S \subseteq T$

(11.24) **Axiome, surensemble propre :** $T \supset S \;\equiv\; S \subset T$

(11.25) **Axiome, complément :** $v \in {\sim}S \;\equiv\; v \in \mathbf{U} \wedge v \notin S$

(11.26) $v \in {\sim}S \;\equiv\; v \notin S \qquad (\text{où } v \in \mathbf{U})$

(11.27) ${\sim}{\sim}S = S$

(11.28) **Axiome, union :** $v \in S \cup T \;\equiv\; v \in S \vee v \in T$

(11.29) **Axiome, intersection :** $v \in S \cap T \;\equiv\; v \in S \wedge v \in T$

(11.30) **Axiome, différence :** $v \in S - T \;\equiv\; v \in S \wedge v \notin T$

(11.32) **Axiome, ensemble puissance :** $v \in \mathcal{P}S \;\equiv\; v \subseteq S$

(11.34) **Commutativité de $\cup$:** $S \cup T = T \cup S$

(11.35) **Associativité de $\cup$:** $(S \cup T) \cup U = S \cup (T \cup U)$

(11.36) **Idempotence de $\cup$:** $S \cup S = S$

(11.37) **Zéro de $\cup$:** $S \cup \mathbf{U} = \mathbf{U}$

(11.38) **Identité (élément neutre) de $\cup$:** $S \cup \emptyset = S$

(11.39) **Affaiblissement :** $S \subseteq S \cup T$

(11.40) **Tiers exclu :** $S \cup {\sim}S = \mathbf{U}$

(11.41) **Commutativité de $\cap$:** $S \cap T = T \cap S$

(11.42) **Associativité de $\cap$:** $(S \cap T) \cap U = S \cap (T \cap U)$

(11.43) **Idempotence de $\cap$:** $S \cap S = S$

(11.44) **Zéro de $\cap$:** $S \cap \emptyset = \emptyset$

(11.45) **Identité (élément neutre) de $\cap$:** $S \cap \mathbf{U} = S$

(11.46) **Affaiblissement :** $S \cap T \subseteq S$

(11.47) **Contradiction :** $S \cap {\sim}S = \emptyset$

(11.48) **Distributivité de $\cup$ sur $\cap$:** $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$

(11.49) **Distributivité de $\cap$ sur $\cup$:** $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

(11.50) **De Morgan :** (a) $\sim(S \cup T) = \sim S \cap \sim T$
(b) $\sim(S \cap T) = \sim S \cup \sim T$

(11.51) **Monotonie de $\cup$:** $S \subseteq T \wedge U \subseteq V \;\Rightarrow\; S \cup U \subseteq T \cup V$

(11.52) **Monotonie de $\cap$:** $S \subseteq T \wedge U \subseteq V \;\Rightarrow\; S \cap U \subseteq T \cap V$

(11.53) $S \subseteq T \;\equiv\; S \cup T = T$

(11.54) $S \subseteq T \;\equiv\; S \cap T = S$

(11.55) $S \cup T = \mathbf{U} \;\equiv\; (\forall x \mid x \in \mathbf{U} : x \notin S \;\Rightarrow\; x \in T)$

(11.56) $S \cap T = \emptyset \;\equiv\; (\forall x \mid : x \in S \;\Rightarrow\; x \notin T)$

(11.57) $S - T \;=\; S \cap \sim T$

(11.58) $S - T \;\subseteq\; S$

(11.59) $S - \emptyset \;=\; S$

(11.60) $S \cap (T - S) \;=\; \emptyset$

(11.61) $S \cup (T - S) \;=\; S \cup T$

(11.62) $S \;-\; (T \cup U) \;=\; (S - T) \cap (S - U)$

(11.63) $S \;-\; (T \cap U) \;=\; (S - T) \cup (S - U)$

(11.64) $(\forall x \mid : P \Rightarrow Q) \;\equiv\; \{x \mid P\} \subseteq \{x \mid Q\}$

(11.65) **Antisymétrie :** $S \subseteq T \wedge T \subseteq S \;\equiv\; S = T$

(11.66) **Réflexivité :** $S \subseteq S$

(11.67) **Transitivité :** $S \subseteq T \wedge T \subseteq U \;\Rightarrow\; S \subseteq U$

(11.68) $\emptyset \subseteq S$

(11.69) $S \subset T \;\equiv\; S \subseteq T \wedge \neg(T \subseteq S)$

(11.70) $S \subset T \;\equiv\; S \subseteq T \wedge (\exists x \mid x \in T : x \notin S)$

(11.71) $S \subseteq T \;\equiv\; S \subset T \vee S = T$

(11.72) $S \not\subset S$

(11.73) $S \subset T \;\Rightarrow\; S \subseteq T$

(11.74) $S \subset T \;\Rightarrow\; T \not\subseteq S$

(11.75) $S \subseteq T \;\Rightarrow\; T \not\subset S$

(11.76) $S \subseteq T \wedge \neg(U \subseteq T) \;\Rightarrow\; \neg(U \subseteq S)$

(11.77) $(\exists x \mid x \in S : x \notin T) \;\Rightarrow\; S \neq T$

(11.78) **Transitivité :** (a) $S \subseteq T \wedge T \subset U \;\Rightarrow\; S \subset U$
(b) $S \subset T \wedge T \subseteq U \;\Rightarrow\; S \subset U$
(c) $S \subset T \wedge T \subset U \;\Rightarrow\; S \subset U$

(11.79) $\mathcal{P}\emptyset = \{\emptyset\}$

(11.80) $S \in \mathcal{P}S$

(11.81) $\#(\mathcal{P}S) = 2^{\#S}$ (pour tout ensemble fini S)

(12.1) **Axiome, égalité de couples :** $\langle b, c\rangle = \langle b', c'\rangle \equiv b = b' \wedge c = c'$

(12.2) **Axiome, produit cartésien :** $S \times T = \{b, c \mid b \in S \wedge c \in T : \langle b, c\rangle\}$

(12.4) **Appartenance :** $\langle x, y\rangle \in S \times T \equiv x \in S \wedge y \in T$

(12.5) $\langle x, y\rangle \in S \times T \equiv \langle y, x\rangle \in T \times S$

(12.6) $S = \emptyset \Rightarrow S \times T = T \times S = \emptyset$

(12.7) $S \times T = T \times S \equiv S = \emptyset \vee T = \emptyset \vee S = T$

(12.8) **Distributivité de $\times$ sur $\cup$:**
$$S \times (T \cup U) = (S \times T) \cup (S \times U)$$
$$(S \cup T) \times U = (S \times U) \cup (T \times U)$$

(12.9) **Distributivité de $\times$ sur $\cap$:**
$$S \times (T \cap U) = (S \times T) \cap (S \times U)$$
$$(S \cap T) \times U = (S \times U) \cap (T \times U)$$

(12.10) **Distributivité de $\times$ sur $-$:** $S \times (T - U) = (S \times T) - (S \times U)$

(12.11) **Monotonie :** $T \subseteq U \Rightarrow S \times T \subseteq S \times U$

(12.12) $S \subseteq U \wedge T \subseteq V \Rightarrow S \times T \subseteq U \times V$

(12.13) $S \times T \subseteq S \times U \wedge S \neq \emptyset \Rightarrow T \subseteq U$

(12.14) $(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$

(12.15) Si S et T sont des ensembles finis, $\#(S \times T) = \#S \cdot \#T$

(12.17) $\mathsf{Dom}.\rho = \{b \mid (\exists c \mid : b\ \rho\ c)\}$

(12.18) $\mathsf{Im}.\rho = \{c \mid (\exists b \mid : b\ \rho\ c)\}$

(12.19) $\langle b, c\rangle \in \rho^{-1} \equiv \langle c, b\rangle \in \rho$ (pour tous $b{:}B$, $c{:}C$)

(12.21) Soit ρ une relation. $\rho = \{b, c \mid \langle b, c\rangle \in \rho : \langle b, c\rangle\}$

(12.22)
$$\langle b, c\rangle \in \{x, y \mid R : \langle x, y\rangle\} \equiv R[x, y := b, c]$$
$$\langle b, c\rangle \in \{b, c \mid R : \langle b, c\rangle\} \equiv R$$

(12.23) Soient ρ et σ deux relations.

(a) $\mathsf{Dom}(\rho^{-1}) = \mathsf{Im}.\rho$

(b) $\mathsf{Im}(\rho^{-1}) = \mathsf{Dom}.\rho$

(c) $\rho \subseteq B \times C \equiv \rho^{-1} \subseteq C \times B$

(d) $(\rho^{-1})^{-1} = \rho$

(e) $\rho \subseteq \sigma \equiv \rho^{-1} \subseteq \sigma^{-1}$

(f) $\mathbf{I}_B^{-1} = \mathbf{I}_B$

(12.24) **Définition de $\circ$:** $\langle b, d\rangle \in \rho \circ \sigma \equiv (\exists c \mid : \langle b, c\rangle \in \rho \wedge \langle c, d\rangle \in \sigma)$

(12.25) **Définition de $\circ$:** $b\ \rho \circ \sigma\ d \equiv (\exists c \mid : b\ \rho\ c\ \sigma\ d)$

(12.27) **Associativité de $\circ$:** $\rho \circ (\sigma \circ \theta) = (\rho \circ \sigma) \circ \theta$

(12.28) **Distributivité de $\circ$ sur $\cup$:** $\rho \circ (\sigma \cup \theta) = \rho \circ \sigma \cup \rho \circ \theta$
$(\sigma \cup \theta) \circ \rho = \sigma \circ \rho \cup \theta \circ \rho$

(12.29) **(Sous)-distributivité de $\circ$ sur $\cap$:** $\rho \circ (\sigma \cap \theta) \subseteq \rho \circ \sigma \cap \rho \circ \theta$
$(\sigma \cap \theta) \circ \rho \subseteq \sigma \circ \rho \cap \theta \circ \rho$

(12.30) **Identité de $\circ$ (où $\rho \subseteq B \times C$) :** $\mathbf{I}_B \circ \rho = \rho \circ \mathbf{I}_C = \rho$

(12.31) $\langle x, y \rangle \in \mathbf{I}_B \equiv x = y$

(12.32) **Zéro de $\circ$:** $\emptyset \circ \rho = \rho \circ \emptyset = \emptyset$

(12.33) **Monotonie de $\circ$:** $\rho \subseteq \sigma \Rightarrow \rho \circ \theta \subseteq \sigma \circ \theta$

(12.34) **Monotonie de $\circ$:** $\rho \subseteq \sigma \Rightarrow \theta \circ \rho \subseteq \theta \circ \sigma$

(12.35) $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$

(12.36) $\emptyset^{-1} = \emptyset$

(12.37) $(\rho \cup \sigma)^{-1} = \rho^{-1} \cup \sigma^{-1}$

(12.38) $(\rho \cap \sigma)^{-1} = \rho^{-1} \cap \sigma^{-1}$

(12.39) $\rho^0 = \mathbf{I}_B \qquad \rho^{n+1} = \rho^n \circ \rho \quad (\text{si } n \geq 0)$

(12.41) $\rho^m \circ \rho^n = \rho^{m+n}$

(12.42) $(\rho^m)^n = \rho^{m \cdot n}$

(12.45) (a) $\rho^+ = (\cup i \mid 0 < i : \rho^i)$
(b) $\rho^* = \rho^+ \cup \mathbf{I}_B = (\cup i \mid 0 \leq i : \rho^i)$

(12.56) Une application f est inversible ssi elle est bijective

(13.1) La somme des degrés des sommets d'un graphe $\langle S, A \rangle$ (orienté ou non) est $2 \cdot \#A$

(13.2) Dans un graphe (orienté ou non), le nombre de sommets de degré impair est pair

(13.4) **Théorème :** Pour tout graphe planaire connexe avec s sommets, a arêtes et r régions, $r = a - s + 2$

(13.5) **Théorème :** Entre deux sommets quelconques d'un arbre, il y a un chemin simple unique

(13.6) **Théorème :** Un arbre avec au moins deux sommets a au moins deux sommets de degré 1

(13.7) **Théorème :** Pour tout arbre $\langle S, A \rangle$, $\#S = 1 + \#A$

(13.8) **Théorème :** Soit $G = \langle S, A \rangle$ un graphe non orienté sans boucle. Les énoncés suivants sont équivalents :

(a) G est un arbre.

(b) G est connexe et l'enlèvement d'une arête quelconque produit deux arbres.

(c) G n'a pas de cycle et $\#S = 1 + \#A$.

(d) G est connexe et $\#S = 1 + \#A$.

(e) G n'a pas de cycle et l'ajout d'une arête introduit exactement un cycle.

Propriétés des relations

	Propriété	Définition 1	Définition 2
(a)	réflexivité	$(\forall b \mid : b\ \rho\ b)$	$\mathbf{I}_B \subseteq \rho$
(b)	irréflexivité	$(\forall b \mid : \neg(b\ \rho\ b))$	$\mathbf{I}_B \cap \rho = \emptyset$
(c)	symétrie	$(\forall b, c \mid : b\ \rho\ c\ \equiv\ c\ \rho\ b)$	$\rho^{-1} = \rho$
(d)	antisymétrie	$(\forall b, c \mid : b\ \rho\ c\ \wedge\ c\ \rho\ b\ \Rightarrow\ b = c)$	$\rho \cap \rho^{-1} \subseteq \mathbf{I}_B$
(e)	asymétrie	$(\forall b, c \mid : b\ \rho\ c\ \Rightarrow\ \neg(c\ \rho\ b))$	$\rho \cap \rho^{-1} \subseteq \emptyset$
(f)	transitivité	$(\forall b, c, d \mid : b\ \rho\ c\ \wedge\ c\ \rho\ d\ \Rightarrow\ b\ \rho\ d)$	$\rho = (\cup i \mid i > 0 : \rho^i)$ $\rho^2 \subseteq \rho$
(g)	équivalence	réflexivité + symétrie + transitivité	
(h)	totalité	$(\forall b{:}B \mid : (\exists c{:}C \mid : b\ \rho\ c))$	$\mathsf{Dom}.\rho = B$
(i)	surjectivité	$(\forall c{:}C \mid : (\exists b{:}B \mid : b\ \rho\ c))$	$\mathsf{Im}.\rho = C$
(j)	déterminisme	$(\forall b, c, c' \mid b\ \rho\ c\ \wedge\ b\ \rho\ c' : c = c')$	$\rho^{-1} \circ \rho\ \subseteq\ \mathbf{I}_C$
(k)	injectivité	$(\forall b, b', c \mid b\ \rho\ c\ \wedge\ b'\ \rho\ c : b = b')$	$\rho \circ \rho^{-1}\ \subseteq\ \mathbf{I}_B$
(l)	fonction	déterminisme	
(m)	application	fonction totale	
(n)	application bijective	application injective et surjective	
(o)	ordre partiel	réflexivité + antisymétrie + transitivité	
(p)	ordre partiel strict	irréflexivité + transitivité	
(q)	ordre total	$(\forall b, c \mid : b \preceq c \vee b \succeq c)$	

Annexe C

Examens de l'automne 2002

Cette annexe contient l'énoncé des examens qui ont été donnés à l'automne 2002.

EXAMEN PARTIEL NUMÉRO 1

IFT-10540 : Logique et techniques de preuve Samedi 5 octobre 2002, 9h30 à 12h30

NOM _____ **MATRICULE** _____

SECTION : ☐ A (Nathalie Cantin) ☐ B (Hans Bherer)

- **RÉPONDEZ À TOUTES LES QUESTIONS SUR CE QUESTIONNAIRE.** Si nécessaire, utilisez les versos, mais indiquez au recto *Suite au verso.*
- Placez votre carte d'identité sur le coin gauche de votre table.
- Vous avez droit à votre manuel et à vos notes de cours. Les calculatrices sont interdites.
- Rappel : Vous pouvez perdre jusqu'à 10% des points pour des fautes de français.
- Vérifiez que le questionnaire a 6 pages (6 questions).

Dans les questions qui suivent, des opérateurs farfelus sont utilisés. Leur préséance est donnée par la table ci-contre. À l'exception de la substitution, tous les opérateurs sont des opérateurs binaires. La priorité 1 est la plus élevée et 7 la plus faible.

Priorité	Opérateur
1	$[x := e]$ (Substitution)
2	$\top \parallel$
3	$\heartsuit$
4	$\diamondsuit$
5	$\clubsuit$
6	$\spadesuit$
7	$\star \dagger \triangle$

1 (15 points)

Effectuez les substitutions suivantes. Éliminez les parenthèses superflues. Donnez la réponse finale seulement.

1. $(a \| b \clubsuit c \star d)[b, c, d := z \diamondsuit y, x \diamondsuit w, z \top v \triangle w]$

2. $p \top p[p := q] \heartsuit (q \top r)[q := s]$

3. $a \top a[a := b \| b][b := c]$

2 (10 points)

Voici la définition de quatre opérateurs booléens. Leur préséance est donnée à la page 1 de cet examen.

		$\top$	$\diamondsuit$	$\star$	$\triangle$
v	v	v	v	f	f
v	f	f	v	v	f
f	v	v	f	f	v
f	f	f	f	f	v

1. Construisez la table de vérité de l'expression

$$b \star a \top a \diamondsuit a \ .$$

Suivez le format des notes pour la présentation de votre table.

2. L'expression est-elle satisfiable ? Votre réponse : $\boxed{}$

3. L'expression est-elle valide ? Votre réponse : $\boxed{}$

3 (20 points)

Dites quelle règle de substitution et quelle règle de Leibniz sont utilisées dans la transformation suivante (autrement dit, précisez les valeurs de E, F, X, Y, v, z utilisées dans (1.9) et (1.13)). Après avoir donné les règles, effectuez les substitutions qu'elles contiennent. Donnez votre réponse en utilisant le même format que la solution du problème 1 du chapitre 3 (donnée à la page 190 des notes).

$$
\begin{array}{ll}
 & a \vee b \vee c \vee (\neg c \wedge d) \\
= & \qquad \langle \text{ Absorption (3.61d), avec } p, q := c, d \rangle \\
 & a \vee b \vee c \vee d
\end{array}
$$

4 (20 points)

Démontrez le théorème $(\neg(p \Rightarrow q) \wedge p) \vee (\neg p \Rightarrow \neg q) \equiv q \Rightarrow p$. Vous pouvez utiliser toutes les lois jusqu'à la loi (3.76) inclusivement. Indiquez toutes les lois utilisées en donnant leur nom (lorsqu'elles en ont un) et leur numéro. Donnez aussi toutes les substitutions. Il y a deux exceptions : vous n'avez pas à mentionner les usages de l'associativité et de la commutativité. Appliquez une seule loi à chaque transformation si possible.

5 (15 points)

Notre technique de preuve utilise souvent de façon implicite la règle d'inférence (1.12) Transitivité. Expliquez comment (1.12) est utilisée dans la preuve suivante.

$$
\begin{aligned}
& (\neg r \vee \neg q) \wedge (r \vee \neg r) \\
= & \qquad \langle \text{ Tiers exclu (3.37), avec } p := r \rangle \\
& (\neg r \vee \neg q) \wedge \mathsf{vrai} \\
= & \qquad \langle \text{ Identité de } \wedge \text{ (3.52), avec } p := \neg r \vee \neg q \rangle \\
& \neg r \vee \neg q \\
= & \qquad \langle \text{ De Morgan (3.48a), avec } p := r \rangle \\
& \neg(r \wedge q)
\end{aligned}
$$

6 (20 points)

Démontrez le théorème $p \wedge (p \Rightarrow q) \Rightarrow (p \wedge \neg q \wedge \neg r \equiv \neg p)$. Vous pouvez utiliser toutes les lois jusqu'à la loi (3.81) inclusivement. Indiquez toutes les lois utilisées en donnant leur nom (lorsqu'elles en ont un) et leur numéro. Donnez aussi toutes les substitutions. Il y a deux exceptions : vous n'avez pas à mentionner les usages de l'associativité et de la commutativité). Appliquez une seule loi à chaque transformation si possible.

EXAMEN PARTIEL NUMÉRO 2

IFT-10540 : Logique et techniques de preuve Samedi 16 novembre 2002, 9h30 à 12h30

NOM _____ **MATRICULE** _____

SECTION : ☐ A (Nathalie Cantin) ☐ B (Hans Bherer)

- **RÉPONDEZ À TOUTES LES QUESTIONS SUR CE QUESTIONNAIRE.** Si nécessaire, utilisez les versos, mais indiquez au recto *Suite au verso.*
- Placez votre carte d'identité sur le coin gauche de votre table.
- Vous avez droit à votre manuel et à vos notes de cours. Les calculatrices sont interdites.
- Rappel : Vous pouvez perdre jusqu'à 10% des points pour des fautes de franÁais.
- Vérifiez que le questionnaire a 4 pages (6 questions).

1 (10 points)

La formule $(\forall x{:}\mathbb{N} \mid{:}\ x \geq 0) \wedge ((x \geq 0 \Rightarrow -x < 0) \vee (\exists x{:}\mathbb{N} \mid{:}\ x > x))$ n'est pas un théorème. Montrez-le en donnant un contre-exemple. Donnez la réponse finale seulement (ne justifiez pas votre démarche). Barème : si l'état que vous donnez est un contre-exemple, vous avez 10, sinon, vous avez 0.

Contre-exemple :

.

2 (15 points)

Soit la tranformation suivante.

$$
\begin{array}{ll}
 & (\forall p \mid p \wedge q : p) \\
= & \qquad \langle\ p \wedge q \Rightarrow (p \equiv q)\ \rangle \\
 & (\forall p \mid p \wedge q : q)
\end{array}
$$

a) Dites quelle règle de Leibniz y est utilisée implicitement.

.

b) Donnez l'instance.

3 (15 points)

Voici les types de cinq fonctions d, e, f, g et h.

$d{:}A \to B$ $\quad$ $e{:}B \to C$ $\quad$ $f{:}(A \to B) \times A \to B$ $\quad$ $g{:}B \times C \to D$ $\quad$ $h{:}A \to A$

Supposez $u{:}A,\ v{:}B,\ w{:}C,\ x{:}D$. Parmi la liste suivante, dites quelles sont les expressions qui sont **mal** typées. Répondez dans la boîte.

(a) $g(e.v)$ $\quad$ (b) $f(d.u, u)$ $\quad$ (c) $f(d, h.u)$ $\quad$ (d) $g(d(h.u), e.v)$ $\quad$ (e) $d(h)$ $\quad$ (f) $e(v, w)$

4 (20 points)

1. Placez un $\times$ devant chaque expression valide. Barème : réponse correcte, 2 points ; réponse incorrecte, -1 point. Résultat minimal pour cette question : 0.

   ☐ $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'}) \Rightarrow \neg\mathsf{libre}(\text{`}x\text{'},\text{`}\neg P\text{'})$
   ☐ $\mathsf{libre}(\text{`}x, y\text{'},\text{`}P\text{'}) \Rightarrow \mathsf{libre}(\text{`}x\text{'},\text{`}P\text{'}) \wedge \mathsf{libre}(\text{`}y\text{'},\text{`}P\text{'})$

2. Placez un **C** devant chaque expression qui est une application *correcte* de la loi indiquée et placez un **I** devant chaque expression qui est une application *incorrecte* de la loi indiquée. Barème : réponse correcte, 2 points ; réponse incorrecte, -1 point ; aucune réponse : 0. Résultat minimal pour cette question : 0.

	Loi	Expression
☐	(6.21)	$(\sum y \mid y = a^2 + x : y + x + y^2) \ = \ a^2 + x + x + (a^2 + x)^2$
☐	(6.29)	$(\prod i \mid 0 \le i \le 10 \ \vee \ 5 \le i \le 99 : i^2) \ = \ (\prod i \mid 0 \le i \le 10 : i^2) \cdot (\prod i \mid 5 \le i \le 99 : i^2)$
☐	(6.31)	$(\exists i{:}\mathbb{N} \mid i \le 99 : (\exists j{:}\mathbb{N} \mid j \le 10 : i + j \le 88))$ $\equiv$ $(\exists j{:}\mathbb{N} \mid j \le 10 : (\exists i{:}\mathbb{N} \mid i \le 99 : i + j \le 88))$
☐	(6.36)	$(\forall y \mid y \ge a^2 : y + x > y^2 + 10) \ \equiv \ (\forall z \mid z \ge a^2 : z + x > z^2 + 10)$
☐	(6.40)	$(\forall k \mid 0 \le k < 66 : k^2 = n) \ \equiv \ (\forall k \mid 0 \le k < 65 : k^2 = n) \ \wedge \ 66^2 = n$
☐	(7.22)	$(\forall t \mid 0 \le t : t < k^2) \ \equiv \ t < k^2 \ \vee \ (\forall t \mid : \neg(0 \le t))$
☐	(7.27)	$(\forall t \mid (t \ge 100 \vee t \le 10) \wedge t \ne n^2 : t^2 > 31) \ \equiv \ (\forall t \mid t \ge 100 \wedge t \ne n^2 : t^2 > 31)$
☐	(7.30)	$(\forall y{:}\mathbb{Z} \mid : (\forall k{:}\mathbb{N} \mid : (1 + y)^k \ge 1 + y)) \ \Rightarrow \ (\forall k{:}\mathbb{N} \mid : (1 + 13)^k \ge 1 + 13)$

5 (20 points)

En assumant l'antécédent, démontrez le théorème :

$$(\neg p \Rightarrow s) \wedge (\neg r \Rightarrow q) \Rightarrow (\neg(p \wedge r) \Rightarrow s \vee q \vee \neg p).$$

Indiquez les lois utilisées en donnant leur nom (lorsqu'elles en ont un) et leur numéro. Utilisez une seule loi à chaque étape lorsque c'est possible. Indiquez toutes les substitutions. Vous n'êtes pas obligé(e) d'indiquer les usages de la commutativité et de l'associativité (mais vous pouvez).

6 (20 points)

Démontrez le théorème suivant : pourvu que $\neg\mathsf{libre}(\text{`}x\text{'},\text{`}Q\text{'})$,

$$((\forall x \mid \mathsf{faux} : x) \;\Rightarrow\; ((\exists x \mid R : P) \;\Rightarrow\; Q)) \equiv (\forall x \mid R : \neg P \vee Q).$$

Vous pouvez utiliser seulement la loi (7.29) et celles qui la précèdent. Indiquez les lois utilisées en donnant leur nom (lorsqu'elles en ont un) et leur numéro. Utilisez une seule loi à chaque étape lorsque c'est possible. Vous n'avez pas à indiquer les substitutions lorsque vous utilisez les lois des chapitres 6 et 7. Vous devez donner les substitutions dans les autres cas. Vous n'êtes pas obligé(e) d'indiquer les usages de la commutativité et de l'associativité.

EXAMEN PARTIEL NUMÉRO 3

IFT-10540 : Logique et techniques de preuve Mercredi 18 décembre 2002, 9h30 à 12h30

NOM _____ **MATRICULE** _____

SECTION : ☐ A (Nathalie Cantin) ☐ B (Hans Bherer)

- **RÉPONDEZ À TOUTES LES QUESTIONS SUR CE QUESTIONNAIRE.** Si nécessaire, utilisez les versos, mais indiquez au recto *Suite au verso*.
- Placez votre carte d'identité sur le coin gauche de votre table.
- Vous avez droit à votre manuel et à vos notes de cours. Les calculatrices sont interdites.
- Rappel : Vous pouvez perdre jusqu'à 10% des points pour des fautes de français.
- Vérifiez que le questionnaire a 6 pages (5 questions).
- **Dans vos preuves, vous n'avez pas à donner les substitutions ni à mentionner les usages de la commutativité et de l'associativité.**

1 (15 points)

Montrez que le programme suivant est correct.

{vrai}
if faux **then skip else skip**
{vrai}

2 (20 points)

Montrez par induction que pour tout entier $n \geq 2$, nous avons

$$\neg(\forall i{:}\mathbb{N} \mid 1 \leq i \leq n : p_i) = (\exists i{:}\mathbb{N} \mid 1 \leq i \leq n : \neg p_i),$$

où $p_1, p_2, \ldots, p_n$ sont des variables booléennes. Vous pouvez utiliser les lois jusqu'à (6.40) inclusivement.

3 (25 points)

Soit P : $\mathsf{impair}.n^2 \Rightarrow \mathsf{impair}.n$.

a) Montrez P par contradiction.

b) Montrez P par contraposition.

4 (10 points)

Montrez que l'expression suivante n'est pas valide mais qu'elle est satisfiable.

$$\{0 \leq x\} \quad y := 2x \quad \{y = x\}$$

5 (30 points)

Soient les transformations suivantes :

$$
\begin{array}{ll}
 & S \wedge (\forall p \mid: \mathsf{vrai} \equiv p) \\
= & \qquad \langle\ J_1\ \rangle \\
 & S \wedge (\forall p \mid: p) \\
\Rightarrow & \qquad \langle\ J_2\ \rangle \\
 & S \wedge (\forall p \mid: p \vee r)
\end{array}
$$

1. Explicitez les justifications J_1 et J_2 (incluant les substitutions, l'associativité et la commutativité si utilisées).

2. Donnez toutes les règles d'inférence utilisées implicitement. Donnez, pour chacune, l'instance utilisée.

Index