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) $= \quad < \quad > \quad \in \quad \subset \quad \subseteq \quad \supset \quad \supseteq \quad \mid \quad \neq \quad \not< \quad \not> \quad \notin \quad \not\subset \quad \not\subseteq \quad \not\supset \quad \not\supseteq \quad \nmid$ (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, alors la notation $a \not\square\, b$ est une abréviation pour l'expression $\neg(a \square b)$. Pour que l'expression ait un sens, il faut que $a \square b$ soit une expression booléenne. 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.

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 $\neg\mathsf{libre}(‘y’,‘x, F’)$,

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

(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 $\neg\mathsf{libre}(‘x’,‘E’)$, $(\star x \mid x = E : P) \;=\; P[x := E]$.

(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 $\neg\mathsf{libre}(‘y’,‘R’)$ et $\neg\mathsf{libre}(‘x’,‘Q’)$,

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

(6.34) **Axiome, imbrication :** Pourvu que $\neg\mathsf{libre}(‘y’,‘R’)$,

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

(6.36) **Axiome, renommage des variables de quantification :** Pourvu que $\neg\mathsf{libre}(‘y’,‘R, P’)$,

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

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

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

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

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

(7.3) **Axiome, transfert :** $(\forall x \mid R : P) \;\equiv\; (\forall x \mid : R \Rightarrow P)$

(7.4) **Transfert :** (a) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid : \neg R \vee P)$
(b) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid : R \wedge P \;\equiv\; R)$
(c) $(\forall x \mid R : P) \;\equiv\; (\forall x \mid : R \vee P \;\equiv\; P)$

(7.6) **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) $(\forall x \mid Q \wedge R : P) \;\equiv\; (\forall x \mid Q : R \vee P \;\equiv\; P)$

(7.8) **Axiome, distributivité de $\vee$ sur $\forall$:** Pourvu que $\neg\mathsf{libre}(‘x’,‘P’)$,

$$P \;\vee\; (\forall x \mid R : Q) \;\equiv\; (\forall x \mid R : P \vee Q)$$

(7.10) Pourvu que $\neg\mathsf{libre}(‘x’,‘P’)$, $(\forall x \mid R : P) \;\equiv\; P \;\vee\; (\forall x \mid : \neg R)$

(7.11) **Distributivité de $\wedge$ sur $\forall$:** Pourvu que $\neg\mathsf{libre}(‘x’,‘P’)$,

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

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

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

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

(7.17) **Affaiblissement/renforcement du corps :** $(\forall x \mid R : P \wedge Q) \;\Rightarrow\; (\forall x \mid R : P)$

(7.18) **Monotonie de $\forall$:** $(\forall x \mid R : Q \Rightarrow P) \;\Rightarrow\; \big((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P)\big)$

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

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

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

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

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

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

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

(7.30) Pourvu que $\neg\mathsf{libre}(`x', `P')$, $(\exists x \mid R : P) \equiv P \wedge (\exists x \mid : R)$

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

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

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

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

(7.34) Affaiblissement/renforcement du corps : $(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$

(7.35) Monotonie de $\exists$: $(\forall x \mid R : Q \Rightarrow P) \Rightarrow \big((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P)\big)$

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

(7.37) Échange de $\forall, \exists$: Pourvu que $\neg\mathsf{libre}(`y', `R')$ et $\neg\mathsf{libre}(`x', `Q')$,

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

(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 $\{n_0,\ n_0+1,\ n_0+2,\ \ldots\}$:

$$P.n_0 \wedge (\forall n \mid n_0 \leq n : P.n \Rightarrow P(n+1)) \Rightarrow (\forall n \mid n_0 \leq n : P.n)$$

(8.7) $b^0 = 1$
$b^{n+1} = b \cdot b^n$ (si $n \geq 0$)

(8.10) $0! = 1$
$k! = k \cdot (k-1)!$ (si $k > 0$)

(8.14) Induction sur $\{n_0,\ n_0+1,\ n_0+2,\ \ldots\}$, deux cas de base :

$$P.n_0 \wedge P(n_0+1) \wedge (\forall n \mid n_0 \leq n : P.n \wedge P(n+1) \Rightarrow P(n+2)) \Rightarrow (\forall n \mid n_0 \leq n : P.n)$$

(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,

$$\{R[x := E]\}\ \ x := E\ \ \{R\}$$

(10.11) Définition de l'affectation : $\{\mathsf{dom}.`E' \wedge R[x := E]\}\ \ x := E\ \ \{R\}$

(10.20) Axiome : $\{Q\}\ S\ \{R\} \equiv Q \Rightarrow \mathsf{wp}(S, R)$

(10.21) Axiome de l'affectation : $\mathsf{wp}(x := E, R) \equiv \mathsf{dom}.`E' \wedge R[x := E]$

(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 : $\{Q\}$ **skip** $\{R\} \equiv Q \Rightarrow R$

(10.33) Axiome de l'instruction conditionnelle :

$$\{Q\}\ \mathsf{IF}\ \{R\} \equiv \{Q \wedge B\}\ S_1\ \{R\} \wedge \{Q \wedge \neg B\}\ S_2\ \{R\}$$

(10.37) Axiome du bloc begin-end : $\{Q\}$ **begin** S **end** $\{R\} \equiv \{Q\}\ S\ \{R\}$.

(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. $\{P\}$ **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

$$\{P\}\ \textbf{while}\ B\ \textbf{do}\ S\ \{P \wedge \neg B\}$$

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 $\neg\mathsf{libre}(`x', `F')$,

$$F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$$

(11.6) Appartenance, cas particulier : $F \in \{x \mid R : x\} \equiv R[x := F]$

(11.8) **Axiome, extensionnalité :** $S = T \;\equiv\; (\forall x \,|\!: x \in S \;\equiv\; x \in T)$

(11.9) $S = \{x \mid x \in S : x\}$

(11.10) Pourvu que $\neg\mathsf{libre}(`y', `R, E')$, $\{x \mid R : E\} \;=\; \{y \mid (\exists x \mid R : y = E)\}$

(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) $\{x \mid Q\} = \{x \mid R\} \;\equiv\; (\forall x \,|\!: Q \equiv R)$

(11.17) **Métathéorème :** $\{x \mid Q\} = \{x \mid R\}$ est un théorème si et seulement si $(\forall x \,|\!: Q \equiv R)$ 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) $v \in \sim S \;\equiv\; v \notin S \qquad$ (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) $S \cap T = \emptyset \;\equiv\; (\forall x \,|\!: x \in S \;\Rightarrow\; x \notin T)$

(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) $(\forall x \,|\!: P \Rightarrow Q) \;\equiv\; \{x \mid P\} \subseteq \{x \mid Q\}$

(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) $\#(\mathcal{P}S) \;=\; 2^{\#S} \qquad$ (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) $\rho^0 = \mathbf{I}_B$ $\rho^{n+1} = \rho^n \circ \rho$ (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	$(\forall b,c \mid: b \preceq c \vee b \succeq c)$	