a Practical Theory of Programming

2020-11-1 edition

Eric C.R. Hehner

Department of Computer Science
University of Toronto
Toronto ON M5S 2E4 Canada

The first edition of this book was published by
Springer-Verlag Publishers, New York, 1993
ISBN 0-387-94106-1   QA76.6.H428

The current edition is available free at
www.cs.utoronto.ca/~hehner/aPToP

An on-line course based on this book is at
www.cs.utoronto.ca/~hehner/FMSD

The author's website is
www.cs.utoronto.ca/~hehner

The cover picture is an inukshuk, which is a human-like figure made of piled stones. Inukshuks are found throughout arctic Canada. They are built by the Inuit people, who use them to mean “You are on the right path.”.

11.4 Laws

11.4.0 Binary

Let a, b, c, d, and e be binary.

Binary Laws

$\top$

$\neg\bot$

Law of Excluded Middle (Tertium non Datur)

$a \lor \neg a$

Law of Noncontradiction

$\neg(a \land \neg a)$

Base Laws

$\neg(a \land \bot)$

$a \lor \top$

$a \Rightarrow \top$

$\bot \Rightarrow a$

Identity Laws

$\top \land a \;=\; a$

$\bot \lor a \;=\; a$

$\top \Rightarrow a \;=\; a$

$\top = a \;=\; a$

Idempotent Laws

$a \land a \;=\; a$

$a \lor a \;=\; a$

Reflexive Laws

$a \Rightarrow a$

$a = a$

Laws of Indirect Proof

$\neg a \Rightarrow \bot \;=\; a$ (Reductio ad Absurdum)

$\neg a \Rightarrow a \;=\; a$

Law of Specialization

$a \land b \Rightarrow a$

Associative Laws

$a \land (b \land c) \;=\; (a \land b) \land c$

$a \lor (b \lor c) \;=\; (a \lor b) \lor c$

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

$a \ne (b \ne c) \;=\; (a \ne b) \ne c$

$a = (b \ne c) \;=\; (a = b) \ne c$

Mirror Law

$a \Leftarrow b \;=\; b \Rightarrow a$

Law of Double Negation

$\neg\neg a \;=\; a$

Duality Laws (deMorgan)

$\neg(a \land b) \;=\; \neg a \lor \neg b$

$\neg(a \lor b) \;=\; \neg a \land \neg b$

Laws of Exclusion

$a \Rightarrow \neg b \;=\; b \Rightarrow \neg a$

$a = \neg b \;=\; a \ne b \;=\; \neg a = b$

Laws of Inclusion

$a \Rightarrow b \;=\; \neg a \lor b$ (Material Implication)

$a \Rightarrow b \;=\; (a \land b \;=\; a)$

$a \Rightarrow b \;=\; (a \lor b \;=\; b)$

Absorption Laws

$a \land (a \lor b) \;=\; a$

$a \lor (a \land b) \;=\; a$

Laws of Direct Proof

$(a \Rightarrow b) \land a \Rightarrow b$ (Modus Ponens)

$(a \Rightarrow b) \land \neg b \Rightarrow \neg a$ (Modus Tollens)

$(a \lor b) \land \neg a \Rightarrow b$(Disjunctive Syllogism)

Transitive Laws

$(a \land b) \land (b \land c) \Rightarrow (a \land c)$

$(a \Rightarrow b) \land (b \Rightarrow c) \Rightarrow (a \Rightarrow c)$

$(a = b) \land (b = c) \Rightarrow (a = c)$

$(a \Rightarrow b) \land (b = c) \Rightarrow (a \Rightarrow c)$

$(a = b) \land (b \Rightarrow c) \Rightarrow (a \Rightarrow c)$

Distributive Laws (Factoring)

$a \land (b \land c) \;=\; (a \land b) \land (a \land c)$

$a \land (b \lor c) \;=\; (a \land b) \lor (a \land c)$

$a \lor (b \land c) \;=\; (a \lor b) \land (a \lor c)$

$a \lor (b \lor c) \;=\; (a \lor b) \lor (a \lor c)$

$a \lor (b \Rightarrow c) \;=\; (a \lor b) \Rightarrow (a \lor c)$

$a \lor (b = c) \;=\; (a \lor b) = (a \lor c)$

$a \Rightarrow (b \land c) \;=\; (a \Rightarrow b) \land (a \Rightarrow c)$

$a \Rightarrow (b \lor c) \;=\; (a \Rightarrow b) \lor (a \Rightarrow c)$

$a \Rightarrow (b \Rightarrow c) \;=\; (a \Rightarrow b) \Rightarrow (a \Rightarrow c)$

$a \Rightarrow (b = c) \;=\; (a \Rightarrow b) = (a \Rightarrow c)$

Symmetry Laws (Commutative Laws)
$$a \land b = b \land a$$
$$a \lor b = b \lor a$$
$$a = b = b = a$$
$$a \ne b = b \ne a$$

Antisymmetry Law (Double Implication)
$$(a \Rightarrow b) \land (b \Rightarrow a) = a = b$$

Laws of Discharge
$$a \land (a \Rightarrow b) = a \land b$$
$$a \Rightarrow (a \land b) = a \Rightarrow b$$

Antimonotonic Law
$$a \Rightarrow b \Longrightarrow (b \Rightarrow c) \Rightarrow (a \Rightarrow c)$$

Monotonic Laws
$$a \Rightarrow b \Longrightarrow c \land a \Rightarrow c \land b$$
$$a \Rightarrow b \Longrightarrow c \lor a \Rightarrow c \lor b$$
$$a \Rightarrow b \Longrightarrow (c \Rightarrow a) \Rightarrow (c \Rightarrow b)$$

Law of Generalization
$$a \Rightarrow a \lor b$$

Antidistributive Laws
$$a \land b \Rightarrow c = (a \Rightarrow c) \lor (b \Rightarrow c)$$
$$a \lor b \Rightarrow c = (a \Rightarrow c) \land (b \Rightarrow c)$$

Laws of Portation
$$a \land b \Rightarrow c = a \Rightarrow (b \Rightarrow c)$$
$$a \land b \Rightarrow c = a \Rightarrow \neg b \lor c$$

Laws of Conflation
$$(a \Rightarrow b) \land (c \Rightarrow d) \Longrightarrow a \land c \Rightarrow b \land d$$
$$(a \Rightarrow b) \land (c \Rightarrow d) \Longrightarrow a \lor c \Rightarrow b \lor d$$

Contrapositive Law
$$a \Rightarrow b = \neg b \Rightarrow \neg a$$

Laws of Equality and Difference
$$a{=}b = (a \land b) \lor (\neg a \land \neg b)$$
$$a{\ne}b = (a \land \neg b) \lor (\neg a \land b)$$

Law of Resolution
$$a \land c \Longrightarrow (a \lor b) \land (\neg b \lor c) = (a \land \neg b) \lor (b \land c) \Longrightarrow a \lor c$$

Case Creation Laws
$$a = \textbf{if } b \textbf{ then } b{\Rightarrow}a \textbf{ else } \neg b \Rightarrow a \textbf{ fi}$$
$$a = \textbf{if } b \textbf{ then } b{\land}a \textbf{ else } \neg b \land a \textbf{ fi}$$
$$a = \textbf{if } b \textbf{ then } b{=}a \textbf{ else } b{\ne}a \textbf{ fi}$$

Case Analysis Laws
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = (a \land b) \lor (\neg a \land c)$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = (a{\Rightarrow}b) \land (\neg a \Rightarrow c)$$

One Case Laws
$$\textbf{if } a \textbf{ then } \top \textbf{ else } b \textbf{ fi} = a{\lor}b$$
$$\textbf{if } a \textbf{ then } \bot \textbf{ else } b \textbf{ fi} = \neg a \land b$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } \top \textbf{ fi} = a{\Rightarrow}b$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } \bot \textbf{ fi} = a{\land}b$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } \neg b \textbf{ fi} = a{=}b$$
$$\textbf{if } a \textbf{ then } \neg b \textbf{ else } b \textbf{ fi} = a{\ne}b$$

Case Absorption Laws
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } a{\land}b \textbf{ else } c \textbf{ fi}$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } a{\Rightarrow}b \textbf{ else } c \textbf{ fi}$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } a{=}b \textbf{ else } c \textbf{ fi}$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } b \textbf{ else } \neg a \land c \textbf{ fi}$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } b \textbf{ else } a{\lor}c \textbf{ fi}$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } b \textbf{ else } a{\ne}c \textbf{ fi}$$

Case Distributive Laws (Case Factoring)
$$\neg\ \textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} = \textbf{if } a \textbf{ then } \neg b \textbf{ else } \neg c \textbf{ fi}$$
$$\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ fi} \land d = \textbf{if } a \textbf{ then } b{\land}d \textbf{ else } c{\land}d \textbf{ fi}$$
and similarly replacing $\land$ by any of $\lor\ =\ \ne\ \Rightarrow\ \Leftarrow$
$$\textbf{if } a \textbf{ then } b \land c \textbf{ else } d \land e \textbf{ fi} = \textbf{if } a \textbf{ then } b \textbf{ else } d \textbf{ fi} \land \textbf{if } a \textbf{ then } c \textbf{ else } e \textbf{ fi}$$
and similarly replacing $\land$ by any of $\lor\ =\ \ne\ \Rightarrow\ \Leftarrow$

End of Binary

11.4.1 Generic

The operators $=$ $\ne$ **if then else fi** apply to every type of expression (but the first operand of **if then else fi** must be binary), with the laws

$x = x$	reflexivity	**if** $\top$ **then** x **else** y **fi** $= x$	case base
$x{=}y \;=\; y{=}x$	symmetry	**if** $\bot$ **then** x **else** y **fi** $= y$	case base
$x{=}y \land y{=}z \;\Rightarrow\; x{=}z$	transitivity	**if** a **then** x **else** x **fi** $= x$	case idempotent
$x{=}y \;\Rightarrow\; f\,x = f\,y$	transparency	**if** a **then** x **else** y **fi** $=$ **if** $\neg a$ **then** y **else** x **fi**	
$x{\ne}y \;=\; \neg(x{=}y)$	unequality		case reversal

The operators $<$ $\le$ $>$ $\ge$ apply to numbers, characters, strings, and lists, with the laws

$x{\le}x$	reflexivity	$\neg\, x{<}x$	irreflexivity
$\neg(x{<}y \land x{=}y)$	exclusivity	$\neg(x{>}y \land x{=}y)$	exclusivity
$\neg(x{<}y \land x{>}y)$	exclusivity	$x{\le}y \;=\; x{<}y \lor x{=}y$	inclusivity
$x{\le}y \land y{\le}z \Rightarrow x{\le}z$	transitivity	$x{<}y \land y{\le}z \Rightarrow x{<}z$	transitivity
$x{<}y \land y{<}z \Rightarrow x{<}z$	transitivity	$x{\le}y \land y{<}z \Rightarrow x{<}z$	transitivity
$x{>}y \;=\; y{<}x$	mirror	$x{\ge}y \;=\; y{\le}x$	mirror
$\neg\, x{<}y \;=\; x{\ge}y$	totality	$\neg\, x{\le}y \;=\; x{>}y$	totality
$x{\le}y \land y{\le}x = x{=}y$	antisymmetry	$x{<}y \lor x{=}y \lor x{>}y$	totality, trichotomy

End of Generic

11.4.2 Numbers

Let d be a sequence of (zero or more) digits, and let x , y , and z be numbers.

$d0{+}1 = d1$	counting
$d1{+}1 = d2$	counting
$d2{+}1 = d3$	counting
$d3{+}1 = d4$	counting
$d4{+}1 = d5$	counting
$d5{+}1 = d6$	counting
$d6{+}1 = d7$	counting
$d7{+}1 = d8$	counting
$d8{+}1 = d9$	counting
$d9{+}1 = (d{+}1)0$	counting (see Exercise 32)
$x{+}0 = x$	identity
$x{+}y = y{+}x$	symmetry
$x{+}(y{+}z) \;=\; (x{+}y){+}z$	associativity
$-\infty{<}x{<}\infty \Rightarrow (x{+}y = x{+}z \;=\; y{=}z)$	cancellation
$-\infty{<}x \Rightarrow\; \infty{+}x = \infty$	absorption
$x{<}\infty \;\Rightarrow\; -\infty + x = -\infty$	absorption
$-x \;=\; 0 - x$	negation
$-\,-x = x$	self-inverse
$-(x{+}y) = -x + -y$	distributivity
$-(x{-}y) = y{-}x$	antisymmetry
$-(x{\times}y) = -x \times y$	semi-distributivity
$-(x/y) = -x\,/\,y$	semi-distributivity
$x{-}0 = x$	identity
$x{-}y \;=\; x + -y$	subtraction
$x + (y - z) \;=\; (x + y) - z$	associativity
$-\infty{<}x{<}\infty \;\Rightarrow\; (x{-}y = x{-}z \;=\; y{=}z)$	cancellation

$-\infty<x<\infty \;\Rightarrow\; x-x=0$	inverse
$x<\infty \;\Rightarrow\; \infty-x=\infty$	absorption
$-\infty<x \;\Rightarrow\; -\infty-x=-\infty$	absorption
$-\infty<x<\infty \;\Rightarrow\; x\times0=0$	base
$x\times1=x$	identity
$x\times y=y\times x$	symmetry
$x\times(y+z)=x\times y+x\times z$	distributivity
$x\times(y\times z)=(x\times y)\times z$	associativity
$-\infty<x<\infty \land x\neq0 \;\Rightarrow\; (x\times y=x\times z \;=\; y=z)$	cancellation
$0<x \;\Rightarrow\; x\times\infty=\infty$	absorption
$0<x \;\Rightarrow\; x\times-\infty \;=\; -\infty$	absorption
$x/1=x$	identity
$-\infty<x<\infty \land x\neq0 \;\Rightarrow\; x/x=1$	inverse
$x\times(y/z)=(x\times y)/z=x/(z/y)$	multiplication-division
$y\neq0 \;\Rightarrow\; (x/y)/z=x/(y\times z)$	multiplication-division
$-\infty<x<\infty \;\Rightarrow\; x/\infty=0=x/-\infty$	annihilation
$-\infty<x<\infty \;\Rightarrow\; x^0=1$	base
$x^1=x$	identity
$x^{y+z}=x^y\times x^z$	exponents
$x^{y\times z}=(x^y)^z$	exponents
$-\infty<0<1<\infty$	direction
$x<y \;=\; -y<-x$	reflection
$-\infty<x<\infty \;\Rightarrow\; (x+y<x+z \;=\; y<z)$	cancellation, translation
$0<x<\infty \;\Rightarrow\; (x\times y<x\times z \;=\; y<z)$	cancellation, scale
$x<y \lor x=y \lor x>y$	trichotomy
$-\infty \le x \le \infty$	extremes

End of Numbers

11.4.3 Bunches

Let x and y be elements (binaries, numbers, characters, sets, strings and lists of elements).

$x\colon y \;=\; x=y$	elementary law
$x\colon A,B \;=\; x\colon A \;\lor\; x\colon B$	compound law
$A,A=A$	idempotence
$A,B=B,A$	symmetry
$A,(B,C)=(A,B),C$	associativity
$A`A=A$	idempotence
$A`B=B`A$	symmetry
$A`(B`C)=(A`B)`C$	associativity
$A,B\colon C \;=\; A\colon C \;\land\; B\colon C$	antidistributivity
$A\colon B`C \;=\; A\colon B \;\land\; A\colon C$	distributivity
$A\colon A,B$	generalization
$A`B\colon A$	specialization
$A\colon A$	reflexivity
$A\colon B \;\land\; B\colon A \;=\; A=B$	antisymmetry
$A\colon B \;\land\; B\colon C \;\Rightarrow\; A\colon C$	transitivity
$¢\,null \;=\; 0$	size
$¢\,x \;=\; 1$	size
$¢\,nat \;=\; \infty$	size
$¢(A,B)+¢(A`B) \;=\; ¢A+¢B$	size

$\neg\, x\colon A \;\Rightarrow\; \text{¢}(A\text{‘}x) = 0$	size
$A\colon B \;\Rightarrow\; \text{¢}A \le \text{¢}B$	size
$A,(A\text{‘}B) \;=\; A$	absorption
$A\text{‘}(A,B) \;=\; A$	absorption
$A\colon B \;\boldsymbol{=}\; A,B = B \;\boldsymbol{=}\; A = A\text{‘}B$	inclusion
$A,(B,C) \;=\; (A,B),(A,C)$	distributivity
$A,(B\text{‘}C) \;=\; (A,B)\text{‘}(A,C)$	distributivity
$A\text{‘}(B,C) \;=\; (A\text{‘}B), (A\text{‘}C)$	distributivity
$A\text{‘}(B\text{‘}C) \;=\; (A\text{‘}B)\text{‘}(A\text{‘}C)$	distributivity
$A\colon B \;\wedge\; C\colon D \;\Rightarrow\; A,C\colon B,D$	conflation, monotonicity
$A\colon B \;\wedge\; C\colon D \;\Rightarrow\; A\text{‘}C\colon B\text{‘}D$	conflation, monotonicity
$null\colon A$	induction
$A, null = A$	identity
$A \text{ ‘ } null = null$	base
$\text{¢}A = 0 \;\boldsymbol{=}\; A = null$	size
$x\colon int \;\wedge\; y\colon xint \;\wedge\; x{\le}y \;\Rightarrow\; (i\colon x,..y \;\boldsymbol{=}\; i\colon int \;\wedge\; x{\le}i{<}y)$	
$x\colon int \;\wedge\; y\colon xint \;\wedge\; x{\le}y \;\Rightarrow\; \text{¢}(x,..y) \;=\; y{-}x$	
$-null \;=\; null$	distribution
$-(A, B) \;=\; -A, -B$	distribution
$A{+}null \;=\; null{+}A \;=\; null$	distribution
$(A, B){+}(C, D) \;=\; A{+}C, A{+}D, B{+}C, B{+}D$	distribution

and similarly for many other operators (see the final page of the book)

End of Bunches

11.4.4 Sets

Let S be a set, and let A and B be anything.

$\{{\sim}S\} \;=\; S$

${\sim}\{A\} \;=\; A$

$\{A\} \;\ne\; A$

$A \in \{B\} \;\boldsymbol{=}\; A\colon B$

$\{A\} \subseteq \{B\} \;\boldsymbol{=}\; A\colon B$

$\{A\}\colon \text{ϟ}B \;\boldsymbol{=}\; A\colon B$

$\$\{A\} = \text{¢}A$

$\{A\} \cup \{B\} \;=\; \{A, B\}$

$\{A\} \cap \{B\} \;=\; \{A \text{ ‘ } B\}$

$\{A\} = \{B\} \;\boldsymbol{=}\; A = B$

$\{A\} \ne \{B\} \;\boldsymbol{=}\; A \ne B$

End of Sets

11.4.5 Strings

Let S, T, and U be strings; let i and j be items (binary values, numbers, characters, sets, lists, functions); let n be extended natural; let x, y, and z be integers such that $x{\le}y{\le}z$.

$nil; S \;=\; S; nil \;=\; S$

$S; (T; U) \;=\; (S; T); U$

$\leftrightarrow nil \;=\; 0$

$\leftrightarrow i \;=\; 1$

$\leftrightarrow(S; T) \;=\; \leftrightarrow S + \leftrightarrow T$

$S_{nil} \;=\; nil$

$\leftrightarrow S{<}\infty \;\Rightarrow\; (S; i; T)_{\leftrightarrow S} \;=\; i$

$\leftrightarrow S{<}\infty \;\Rightarrow\; S;i;T \triangleleft \leftrightarrow S \triangleright j \;=\; S;j;T$

$S_{(T_U)} \;=\; (S_T)_U$

$S_{T;\,U} \;=\; S_T; S_U$

$S_{\{A\}} \;=\; \{S_A\}$

$\leftrightarrow S{<}\infty \;\Rightarrow\; nil \;\le\; S \;<\; S; i; T$

$\leftrightarrow S{<}\infty \;\Rightarrow\; (i{<}j \;\Rightarrow\; S; i; T \;<\; S; j; U)$

$\leftrightarrow S{<}\infty \;\Rightarrow\; (i{=}j \;\boldsymbol{=}\; S; i; T \;=\; S; j; T)$

$0{*}S \;=\; nil$

$(n{+}1){*}S \;=\; n{*}S; S$

${*}S \;=\; {*}{*}S \;=\; nat{*}S$

$x;..x \;=\; nil$

$x;..x{+}1 \;=\; x$

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

$\leftrightarrow(x;..y) \;=\; y{-}x$

End of Strings

11.4.6 Lists

Let S and T be strings; let i and j be items (binary values, numbers, characters, sets, lists, functions); let L, M, and N be lists.

$$[S] \ne S$$
$$\sim[S] = S$$
$$[\sim L] = L$$
$$[S]\ T = S_T$$
$$[S];;[T] = [S;\ T]$$
$$[S] = [T] \;\;=\;\; S = T$$
$$[S] < [T] \;\;=\;\; S < T$$
$$nil \rightarrow i \mid L = i$$
$$n \rightarrow i \mid [S] = [S \triangleleft n \triangleright i]$$
$$(S;T) \rightarrow i \mid L = S \rightarrow (T \rightarrow i \mid L@S) \mid L$$
$$\#[S] = \leftrightarrow S$$
$$S_{[T]} = [S_T]$$
$$[S]\ [T] = [S_T]$$
$$L\ \{A\} = \{L\ A\}$$
$$L\ [S] = [L\ S]$$
$$(L\ M)\ N = L\ (M\ N)$$
$$L@nil = L$$
$$L@i = L\ i$$
$$L@(S;\ T) = L@S@T$$

End of Lists

11.4.7 Functions

Renaming Law — if v and w do not appear in D and w does not appear in b

$$\langle v{:}\ D \rightarrow b\rangle = \langle w{:}\ D \rightarrow \langle v{:}\ D \rightarrow b\rangle w\rangle$$

Application Law: if element $x{:}\ D$

$$\langle v{:}\ D \rightarrow b\rangle x = (\text{substitute } x \text{ for } v \text{ in } b\,)$$

Domain Law

$$\square\langle v{:}\ D \rightarrow b\rangle = D$$

Law of Extension

$$f = \langle v{:}\ \square f \rightarrow f\ v\rangle$$

Function Inclusion Law

$$f{:}\ g \;\;=\;\; \square g{:}\ \square f \ \wedge\ \forall x{:}\ \square g\cdot f\ x{:}\ g\ x$$

Function Equality Law

$$f = g \;\;=\;\; \square f = \square g \ \wedge\ \forall x{:}\ \square f\cdot f\ x = g\ x$$

Laws of Functional Union

$$\square(f, g) = \square f\ \text{‘}\ \square g$$
$$(f, g)\ x = f\ x, g\ x$$

Distributive Laws

$$f\ null = null$$
$$f\ (A, B) = f\ A, f\ B$$
$$f\ (\S g) = \S y{:}\ f\ (\square g)\cdot \exists x{:}\ \square g\cdot f\ x = y \ \wedge\ g\ x$$
$$f\ \textbf{if}\ b\ \textbf{then}\ x\ \textbf{else}\ y\ \textbf{fi} = \textbf{if}\ b\ \textbf{then}\ f\ x\ \textbf{else}\ f\ y\ \textbf{fi}$$
$$\textbf{if}\ b\ \textbf{then}\ f\ \textbf{else}\ g\ \textbf{fi}\ x = \textbf{if}\ b\ \textbf{then}\ f\ x\ \textbf{else}\ g\ x\ \textbf{fi}$$

Function Composition Laws: If $\neg\ f{:}\ \square g$

$$\square(g\ f) = \S x{:}\ \square f\cdot f\ x{:}\ \square g$$
$$(g\ f)\ x = g\ (f\ x)$$
$$f\ (g\ h) = (f\ g)\ h$$

Laws of Functional Intersection

$$\square(f\ \text{‘}\ g) = \square f, \square g$$
$$(f\ \text{‘}\ g)x = (f \mid g)x\ \text{‘}\ (g \mid f)x$$

Laws of Selective Union

$$\square(f \mid g) = \square f, \square g$$
$$(f \mid g)x = \textbf{if}\ x{:}\ \square f\ \textbf{then}\ f\ x\ \textbf{else}\ g\ x\ \textbf{fi}$$
$$f \mid f = f$$
$$f \mid (g \mid h) = (f \mid g) \mid h$$
$$(g \mid h)\ f = g\ f \mid h\ f$$

Arrow Laws

$$f{:}\ null \rightarrow A$$
$$A \rightarrow B{:}\ (A\text{‘}C) \rightarrow (B, D)$$
$$(A, B) \rightarrow C = A \rightarrow C \mid B \rightarrow C$$
$$f{:}\ A \rightarrow B \;\;=\;\; A{:}\ \square f \ \wedge\ \forall a{:}\ A\cdot f\ a{:}\ B$$

End of Functions

11.4.8 Quantifiers

Let x be an element, let a, b and c be binary, let n and m be numeric, let f and g be functions, and let p be a predicate.

$\forall v\colon null\cdot\ b \;=\; \top$

$\forall v\colon x\cdot\ b \;=\; \langle v\colon x \to b\rangle\ x$

$\forall v\colon A,B\cdot\ b \;=\; (\forall v\colon A\cdot\ b) \land (\forall v\colon B\cdot\ b)$

$\forall v\colon (\S v\colon D\cdot\ b)\cdot\ c \;=\; \forall v\colon D\cdot\ b \Rightarrow c$

$\exists v\colon null\cdot\ b \;=\; \bot$

$\exists v\colon x\cdot\ b \;=\; \langle v\colon x \to b\rangle\ x$

$\exists v\colon A,B\cdot\ b \;=\; (\exists v\colon A\cdot\ b) \lor (\exists v\colon B\cdot\ b)$

$\exists v\colon (\S v\colon D\cdot\ b)\cdot\ c \;=\; \exists v\colon D\cdot\ b \land c$

$\Sigma v\colon null\cdot\ n \;=\; 0$

$\Sigma v\colon x\cdot\ n \;=\; \langle v\colon x \to n\rangle\ x$

$(\Sigma v\colon A,B\cdot\ n) + (\Sigma v\colon A\text{‘}B\cdot\ n) \;=\; (\Sigma v\colon A\cdot\ n) + (\Sigma v\colon B\cdot\ n)$

$\Sigma v\colon (\S v\colon D\cdot\ b)\cdot\ n \;=\; \Sigma v\colon D\cdot\ \mathbf{if}\ b\ \mathbf{then}\ n\ \mathbf{else}\ 0\ \mathbf{fi}$

$\Pi v\colon null\cdot\ n \;=\; 1$

$\Pi v\colon x\cdot\ n \;=\; \langle v\colon x \to n\rangle\ x$

$(\Pi v\colon A,B\cdot\ n) \times (\Pi v\colon A\text{‘}B\cdot\ n) \;=\; (\Pi v\colon A\cdot\ n) \times (\Pi v\colon B\cdot\ n)$

$\Pi v\colon (\S v\colon D\cdot\ b)\cdot\ n \;=\; \Pi v\colon D\cdot\ \mathbf{if}\ b\ \mathbf{then}\ n\ \mathbf{else}\ 1\ \mathbf{fi}$

$MIN\ v\colon null\cdot\ n \;=\; \infty$

$MIN\ v\colon x\cdot\ n \;=\; \langle v\colon x \to n\rangle\ x$

$MIN\ v\colon A,B\cdot\ n \;=\; min\ (MIN\ v\colon A\cdot\ n)\ (MIN\ v\colon B\cdot\ n)$

$MIN\ v\colon (\S v\colon D\cdot\ b)\cdot\ n \;=\; MIN\ v\colon D\cdot\ \mathbf{if}\ b\ \mathbf{then}\ n\ \mathbf{else}\ \infty\ \mathbf{fi}$

$MAX\ v\colon null\cdot\ n \;=\; -\infty$

$MAX\ v\colon x\cdot\ n \;=\; \langle v\colon x \to n\rangle\ x$

$MAX\ v\colon A,B\cdot\ n \;=\; max\ (MAX\ v\colon A\cdot\ n)\ (MAX\ v\colon B\cdot\ n)$

$MAX\ v\colon (\S v\colon D\cdot\ b)\cdot\ n \;=\; MAX\ v\colon D\cdot\ \mathbf{if}\ b\ \mathbf{then}\ n\ \mathbf{else}\ -\infty\ \mathbf{fi}$

$\S v\colon null\cdot\ b \;=\; null$

$\S v\colon x\cdot\ b \;=\; \mathbf{if}\ \langle v\colon x \to b\rangle\ x\ \mathbf{then}\ x\ \mathbf{else}\ null\ \mathbf{fi}$

$\S v\colon A,B\cdot\ b \;=\; (\S v\colon A\cdot\ b), (\S v\colon B\cdot\ b)$

$\S v\colon A\text{‘}B\cdot\ b \;=\; (\S v\colon A\cdot\ b)\ \text{‘}\ (\S v\colon B\cdot\ b)$

$\S v\colon (\S v\colon D\cdot\ b)\cdot\ c \;=\; \S v\colon D\cdot\ b \land c$

Change of Variable Laws — if d does not appear in b

$\forall r\colon f\,D\cdot\ b \;=\; \forall d\colon D\cdot\ \langle r\colon f\,D \to b\rangle\ (f\,d)$

$\exists r\colon f\,D\cdot\ b \;=\; \exists d\colon D\cdot\ \langle r\colon f\,D \to b\rangle\ (f\,d)$

$MIN\ r\colon f\,D\cdot\ n \;=\; MIN\ d\colon D\cdot\ \langle r\colon f\,D \to n\rangle\ (f\,d)$

$MAX\ r\colon f\,D\cdot\ n \;=\; MAX\ d\colon D\cdot\ \langle r\colon f\,D \to n\rangle\ (f\,d)$

Bunch-Element Conversion Laws

$A\colon B \;=\; \forall a\colon A\cdot\ \exists b\colon B\cdot\ a=b$

$fA\colon gB \;=\; \forall a\colon A\cdot\ \exists b\colon B\cdot\ fa=gb$

Idempotent Laws — if $D \ne null$ and v does not appear in b

$\forall v\colon D\cdot\ b \;=\; b$

$\exists v\colon D\cdot\ b \;=\; b$

Absorption Laws — if $x\colon D$

$\langle v\colon D \to b\rangle x \land \exists v\colon D\cdot\ b \;=\; \langle v\colon D \to b\rangle x$

$\langle v\colon D \to b\rangle x \lor \forall v\colon D\cdot\ b \;=\; \langle v\colon D \to b\rangle x$

$\langle v\colon D \to b\rangle x \land \forall v\colon D\cdot\ b \;=\; \forall v\colon D\cdot\ b$

$\langle v\colon D \to b\rangle x \lor \exists v\colon D\cdot\ b \;=\; \exists v\colon D\cdot\ b$

Inclusion Law

$A\colon B \;=\; \forall x\colon A\cdot\ x\colon B$

Cardinality Law

$¢A \;=\; \Sigma\,(A \to 1)$

Identity Laws

$\forall v\cdot\ \top$

$\lnot \exists v\cdot\ \bot$

Distributive Laws — if $D \ne null$ and v does not appear in a

$a \land \forall v\colon D\cdot\ b \;=\; \forall v\colon D\cdot\ a \land b$

$a \land \exists v\colon D\cdot\ b \;=\; \exists v\colon D\cdot\ a \land b$

$a \lor \forall v\colon D\cdot\ b \;=\; \forall v\colon D\cdot\ a \lor b$

$a \lor \exists v\colon D\cdot\ b \;=\; \exists v\colon D\cdot\ a \lor b$

$a \Rightarrow \forall v\colon D\cdot\ b \;=\; \forall v\colon D\cdot\ a \Rightarrow b$

$a \Rightarrow \exists v\colon D\cdot\ b \;=\; \exists v\colon D\cdot\ a \Rightarrow b$

Antidistributive Laws — if $D \ne null$ and v does not appear in a

$a \Leftarrow \exists v\colon D\cdot\ b \;=\; \forall v\colon D\cdot\ a \Leftarrow b$

$a \Leftarrow \forall v\colon D\cdot\ b \;=\; \exists v\colon D\cdot\ a \Leftarrow b$

Specialization Law — if $x: D$

$\forall v: D\cdot b \quad \Longrightarrow \quad \langle v: D \to b\rangle\, x$

One-Point Laws — if $x: D$

and v does not appear in x

$\forall v: D\cdot v{=}x \Rightarrow b \quad = \quad \langle v: D \to b\rangle\, x$

$\exists v: D\cdot v{=}x \wedge b \quad = \quad \langle v: D \to b\rangle\, x$

Duality Laws

$\neg\forall v\cdot b \quad = \quad \exists v\cdot \neg b$ (deMorgan)

$\neg\exists v\cdot b \quad = \quad \forall v\cdot \neg b$ (deMorgan)

$-\,MAX\ v\cdot n \quad = \quad MIN\ v\cdot -n$

$-\,MIN\ v\cdot n \quad = \quad MAX\ v\cdot -n$

Solution Laws

$\S v: D\cdot \top \ = \ D$

$(\S v: D\cdot b)\!:\ D$

$\S v: D\cdot \bot \ = \ null$

$(\S v\cdot b)\!: (\S v\cdot c) \quad = \quad \forall v\cdot b \Rightarrow c$

$(\S v\cdot b), (\S v\cdot c) \quad = \quad \S v\cdot b \vee c$

$(\S v\cdot b)$ ‘ $(\S v\cdot c) \quad = \quad \S v\cdot b \wedge c$

$x: \S p \quad = \quad x: \Box p \ \wedge\ p\ x$

$\forall f \ = \ (\S f){=}(\Box f)$

$\exists f \ = \ (\S f){\ne}null$

Bounding Laws

if v does not appear in n

$n > (MAX\ v: D\cdot m) \ \Rightarrow\ (\forall v: D\cdot n{>}m)$

$n < (MIN\ v: D\cdot m) \ \Rightarrow\ (\forall v: D\cdot n{<}m)$

$n \ge (MAX\ v: D\cdot m) \ = \ (\forall v: D\cdot n{\ge}m)$

$n \le (MIN\ v: D\cdot m) \ = \ (\forall v: D\cdot n{\le}m)$

$n \ge (MIN\ v: D\cdot m) \ \Leftarrow\ (\exists v: D\cdot n{\ge}m)$

$n \le (MAX\ v: D\cdot m) \ \Leftarrow\ (\exists v: D\cdot n{\le}m)$

$n > (MIN\ v: D\cdot m) \ = \ (\exists v: D\cdot n{>}m)$

$n < (MAX\ v: D\cdot m) \ = \ (\exists v: D\cdot n{<}m)$

Generalization Law — if $x: D$

$\langle v: D \to b\rangle\, x \quad \Longrightarrow \quad \exists v: D\cdot b$

Splitting Laws — for any fixed domain

$\forall v\cdot a \wedge b \quad = \quad (\forall v\cdot a)\ \wedge\ (\forall v\cdot b)$

$\exists v\cdot a \wedge b \quad \Longrightarrow \quad (\exists v\cdot a)\ \wedge\ (\exists v\cdot b)$

$\forall v\cdot a \vee b \quad \Longleftarrow \quad (\forall v\cdot a)\ \vee\ (\forall v\cdot b)$

$\exists v\cdot a \vee b \quad = \quad (\exists v\cdot a)\ \vee\ (\exists v\cdot b)$

$\forall v\cdot a \Rightarrow b \quad \Longrightarrow \quad (\forall v\cdot a)\ \Rightarrow\ (\forall v\cdot b)$

$\forall v\cdot a \Rightarrow b \quad \Longrightarrow \quad (\exists v\cdot a)\ \Rightarrow\ (\exists v\cdot b)$

$\forall v\cdot a = b \quad \Longrightarrow \quad (\forall v\cdot a)\ =\ (\forall v\cdot b)$

$\forall v\cdot a = b \quad \Longrightarrow \quad (\exists v\cdot a)\ =\ (\exists v\cdot b)$

Commutative Laws

$\forall v\cdot \forall w\cdot b \quad = \quad \forall w\cdot \forall v\cdot b$

$\exists v\cdot \exists w\cdot b \quad = \quad \exists w\cdot \exists v\cdot b$

Semicommutative Laws (Skolem)

$\exists v\cdot \forall w\cdot b \quad \Longrightarrow \quad \forall w\cdot \exists v\cdot b$

$\forall x\cdot \exists y\cdot p\ x\ y \quad = \quad \exists f\cdot \forall x\cdot p\ x\ (f\ x)$

Domain Change Laws

$A: B \ \Longrightarrow\ (\forall v: A\cdot b)\ \Leftarrow\ (\forall v: B\cdot b)$

$A: B \ \Longrightarrow\ (\exists v: A\cdot b)\ \Rightarrow\ (\exists v: B\cdot b)$

$\forall v: A\cdot v: B \Rightarrow p \ = \ \forall v: A$‘$B\cdot p$

$\exists v: A\cdot v: B \wedge p \ = \ \exists v: A$‘$B\cdot p$

Extreme Laws

$(MIN\ n: int\cdot n) = (MIN\ n: real\cdot n) = -\infty$

$(MAX\ n: int\cdot n) = (MAX\ n: real\cdot n) = \infty$

Connection Laws (Galois)

$n{\le}m \quad = \quad \forall k\cdot\ k{\le}n \Rightarrow k{\le}m$

$n{\le}m \quad = \quad \forall k\cdot\ k{<}n \Rightarrow k{<}m$

$n{\le}m \quad = \quad \forall k\cdot\ m{\le}k \Rightarrow n{\le}k$

$n{\le}m \quad = \quad \forall k\cdot\ m{<}k \Rightarrow n{<}k$

Distributive Laws — if $D{\ne}null$ and v does not appear in n

$max\ n\ (MAX\ v: D\cdot m) \ = \ (MAX\ v: D\cdot max\ n\ m)$

$max\ n\ (MIN\ v: D\cdot m) \ = \ (MIN\ v: D\cdot max\ n\ m)$

$min\ n\ (MAX\ v: D\cdot m) \ = \ (MAX\ v: D\cdot min\ n\ m)$

$min\ n\ (MIN\ v: D\cdot m) \ = \ (MIN\ v: D\cdot min\ n\ m)$

$n + (MAX\ v: D\cdot m) \ = \ (MAX\ v: D\cdot n{+}m)$

$n + (MIN\ v: D\cdot m) \ = \ (MIN\ v: D\cdot n{+}m)$

$n - (MAX\ v: D\cdot m) \ = \ (MIN\ v: D\cdot n{-}m)$

$n - (MIN\ v: D\cdot m) \ = \ (MAX\ v: D\cdot n{-}m)$

$(MAX\ v: D\cdot m) - n \ = \ (MAX\ v: D\cdot m{-}n)$

$(MIN\ v: D\cdot m) - n \ = \ (MIN\ v: D\cdot m{-}n)$

$n{\ge}0 \ \Rightarrow\ n \times (MAX\ v: D\cdot m) \ = \ (MAX\ v: D\cdot n{\times}m)$

$n{\ge}0 \ \Rightarrow\ n \times (MIN\ v: D\cdot m) \ = \ (MIN\ v: D\cdot n{\times}m)$

$n{\le}0 \ \Rightarrow\ n \times (MAX\ v: D\cdot m) \ = \ (MIN\ v: D\cdot n{\times}m)$

$n{\le}0 \ \Rightarrow\ n \times (MIN\ v: D\cdot m) \ = \ (MAX\ v: D\cdot n{\times}m)$

$n \times (\Sigma v: D\cdot m) \ = \ (\Sigma v: D\cdot n{\times}m)$

$(\Pi v: D\cdot m)^n \ = \ (\Pi v: D\cdot m^n)$

End of Quantifiers

11.4.9 Limits

$(MAX\ m\cdot\ MIN\ n\cdot\ f(m+n))\ \le\ (LIM\ f)\ \le\ (MIN\ m\cdot\ MAX\ n\cdot\ f(m+n))$
$\exists m\cdot\ \forall n\cdot\ p(m+n)\ \ \Longrightarrow\ \ LIM\ p\ \ \Longrightarrow\ \ \forall m\cdot\ \exists n\cdot\ p(m+n)$
$(LIM\ n\cdot\ n) = \infty$

End of Limits

11.4.10 Specifications and Programs

For specifications P , Q , R , and S , and binary b ,

$ok\ \ =\ \ x'=x\ \wedge\ y'=y\ \wedge\ ...$
$x{:=}\ e\ \ =\ \ x'=e\ \wedge\ y'=y\ \wedge\ ...$
$P.\ Q\ \ =\ \ \exists x'', y'', ...\cdot\ \langle x', y', ...\rightarrow P\rangle\ x''\ y''\ ...\ \wedge\ \langle x, y, ...\rightarrow Q\rangle\ x''\ y''\ ...$
$P\|Q\ \ =\ \ \exists t_P, t_Q\cdot\ \langle t'\rightarrow P\rangle t_P\ \wedge\ \langle t'\rightarrow Q\rangle t_Q\ \wedge\ t' = max\ t_P\ t_Q$
$\textbf{if } b \textbf{ then } P \textbf{ else } Q \textbf{ fi}\ \ =\ \ b \wedge P \vee \neg b \wedge Q$
$\textbf{var } x{:}\ T\cdot\ P\ \ =\ \ \exists x, x'{:}\ T\cdot\ P$
$\textbf{frame } x\cdot\ P\ \ =\ \ P\ \wedge\ y'=y\ \wedge\ ...$
$\textbf{while } b \textbf{ do } P \textbf{ od}\ \ =\ \ t'\ge t \wedge \textbf{if } b \textbf{ then } P.\ \ t{:=}\ t+1.\ \ \textbf{while } b \textbf{ do } P \textbf{ od else } ok \textbf{ fi}$
$\forall\sigma, \sigma'\cdot\ \textbf{if } b \textbf{ then } P.\ \ W \textbf{ else } ok \textbf{ fi}\ \Leftarrow\ W\ \ \Longrightarrow\ \ \forall\sigma, \sigma'\cdot\ \textbf{while } b \textbf{ do } P \textbf{ od}\ \Leftarrow\ W$
$\qquad (Fmn\ \ \Leftarrow\ \ m=n \wedge ok) \wedge (Fik\ \ \Leftarrow\ \ m\le i<j<k\le n \wedge (Fij.\ Fjk))$
$\Longrightarrow\qquad Fmn\ \ \Leftarrow\ \ \textbf{for } i{:=}\ m;..n \textbf{ do } m\le i<n \Rightarrow Fi(i+1) \textbf{ od}$
$Im\Rightarrow I'n\ \ \Longleftarrow\ \ \textbf{for } i{:=}\ m;..n \textbf{ do } m\le i<n \wedge Ii \Rightarrow I'(i+1) \textbf{ od}$
$\textbf{wait until } w\ \ =\ \ t{:=}\ max\ t\ w$
$\textbf{assert } b\ \ =\ \ \textbf{if } b \textbf{ then } ok \textbf{ else } screen!\ \text{“error”}.\ \ \textbf{wait until } \infty \textbf{ fi}$
$\textbf{ensure } b\ \ =\ \ b \wedge ok$
$P.\ \ (P \textbf{ result } e)=e$ but do not double-prime or substitute in $(P \textbf{ result } e)$
$c?\ \ =\ \ \boldsymbol{r}{:=}\ \boldsymbol{r}+1$
$c\ \ =\ \ \mathcal{M}c_{\boldsymbol{r}c-1}$
$c!\ e\ \ =\ \ \mathcal{M}c_{\boldsymbol{w}c} = e\ \wedge\ \mathcal{T}c_{\boldsymbol{w}c} = t\ \wedge\ (wc{:=}\ wc+1)$
$\surd c\ \ =\ \ \mathcal{T}c_{\boldsymbol{r}c} + (\text{transit time}) \le t$
$\textbf{ivar } x{:}\ T\cdot\ S\ \ =\ \ \exists x{:}\ time\rightarrow T\cdot\ S$
$\textbf{chan } c{:}\ T\cdot\ P\ \ =\ \ \exists \mathcal{M}c{:}\ \infty{*}T\cdot\ \exists \mathcal{T}c{:}\ \infty{*}xreal\cdot\ \exists \boldsymbol{r}c, \boldsymbol{r}c', \boldsymbol{w}c, \boldsymbol{w}c'{:}\ xnat\cdot$
$\qquad\qquad (\forall i, j{:}\ nat\cdot\ i\le j\ \Rightarrow\ t \le \mathcal{T}c_i \le \mathcal{T}c_j \le t') \wedge \boldsymbol{r}c=\boldsymbol{w}c=0 \wedge P$
$ok.\ P\ \ =\ \ P.\ ok\ \ =\ \ P$ identity
$P.\ (Q.\ R)\ \ =\ \ (P.\ Q).\ R$ associativity
$P\vee Q.\ R\vee S\ \ =\ \ (P.\ R) \vee (P.\ S) \vee (Q.\ R) \vee (Q.\ \mathrm{S})$ distributivity
$\textbf{if } b \textbf{ then } P \textbf{ else } Q \textbf{ fi}.\ R\ \ =\ \ \textbf{if } b \textbf{ then } P.\ R \textbf{ else } Q.\ R \textbf{ fi}$ distributivity (unprimed b)
$P.\ \ \textbf{if } b \textbf{ then } Q \textbf{ else } R \textbf{ fi}\ \ =\ \ \textbf{if } P.\ b \textbf{ then } P.\ Q \textbf{ else } P.\ R \textbf{ fi}$ distributivity (unprimed b)
$P \| Q\ \ =\ \ Q \| P$ symmetry
$P \| (Q \| R)\ \ =\ \ (P \| Q) \| R$ associativity
$P \| t'=t\ \ =\ \ P\ \ =\ \ t'=t \| P$ identity
$P \| Q\vee R\ \ =\ \ (P \| Q) \vee (P \| R)$ distributivity
$P \| \textbf{if } b \textbf{ then } Q \textbf{ else } R \textbf{ fi}\ \ =\ \ \textbf{if } b \textbf{ then } P \| Q \textbf{ else } P \| R \textbf{ fi}$ distributivity
$\textbf{if } b \textbf{ then } P\|Q \textbf{ else } R\|S \textbf{ fi}\ \ =\ \ \textbf{if } b \textbf{ then } P \textbf{ else } R \textbf{ fi} \| \textbf{if } b \textbf{ then } Q \textbf{ else } S \textbf{ fi}$ distributivity
$x{:=}\ \textbf{if } b \textbf{ then } e \textbf{ else } f \textbf{ fi}\ \ =\ \ \textbf{if } b \textbf{ then } x{:=}\ e \textbf{ else } x{:=}\ f \textbf{ fi}$ functional-imperative

End of Specifications and Programs

11.4.11 Substitution

Let x and y be different boundary state variables, let e and f be expressions of the prestate, and let P be a specification.

$x{:=}\,e.\,P \;=\;$ (for x substitute e in P)

$(x{:=}\,e \,\|\, y{:=}\,f).\; P \;=\;$ (for x substitute e and independently for y substitute f in P)

End of Substitution

11.4.12 Conditions

Let P and Q be any specifications, and let C be a precondition, and let C' be the corresponding postcondition (in other words, C' is the same as C but with primes on all the state variables).

$C \land (P.\,Q) \;\Leftarrow\; C{\land}P.\,Q$

$C \Rightarrow (P.Q) \;\Leftarrow\; C{\Rightarrow}P.\,Q$

$(P.Q) \land C' \;\Leftarrow\; P.\,Q{\land}C'$

$(P.Q) \Leftarrow C' \;\Leftarrow\; P.\,Q{\Leftarrow}C'$

$P.\,C{\land}Q \;\Leftarrow\; P{\land}C'.\,Q$

$P.\,Q \;\Leftarrow\; P{\land}C'.\;C{\Rightarrow}Q$

C is a sufficient precondition for P to be refined by S
  if and only if $C{\Rightarrow}P$ is refined by S.

C' is a sufficient postcondition for P to be refined by S
  if and only if $C'{\Rightarrow}P$ is refined by S.

End of Conditions

11.4.13 Refinement

Refinement by Steps (Stepwise Refinement) (monotonicity, transitivity)

If $A \Leftarrow$ **if** b **then** C **else** D **fi** and $C \Leftarrow E$ and $D \Leftarrow F$ are theorems,
  then $A \Leftarrow$ **if** b **then** E **else** F **fi** is a theorem.

If $A \Leftarrow B.C$ and $B \Leftarrow D$ and $C \Leftarrow E$ are theorems, then $A \Leftarrow D.E$ is a theorem.

If $A \Leftarrow B\|C$ and $B \Leftarrow D$ and $C \Leftarrow E$ are theorems, then $A \Leftarrow D\|E$ is a theorem.

If $A \Leftarrow B$ and $B \Leftarrow C$ are theorems, then $A \Leftarrow C$ is a theorem.

Refinement by Parts (monotonicity, conflation)

If $A \Leftarrow$ **if** b **then** C **else** D **fi** and $E \Leftarrow$ **if** b **then** F **else** G **fi** are theorems,
  then $A{\land}E \Leftarrow$ **if** b **then** $C{\land}F$ **else** $D{\land}G$ **fi** is a theorem.

If $A \Leftarrow B.C$ and $D \Leftarrow E.F$ are theorems, then $A{\land}D \Leftarrow B{\land}E.\,C{\land}F$ is a theorem.

If $A \Leftarrow B\|C$ and $D \Leftarrow E\|F$ are theorems, then $A{\land}D \Leftarrow B{\land}E \,\|\, C{\land}F$ is a theorem.

If $A \Leftarrow B$ and $C \Leftarrow D$ are theorems, then $A{\land}C \Leftarrow B{\land}D$ is a theorem.

Refinement by Cases

$P \Leftarrow$ **if** b **then** Q **else** R **fi** is a theorem if and only if
$P \Leftarrow b \land Q$ and $P \Leftarrow \lnot b \land R$ are theorems.

End of Refinement

End of Laws

11.5 Names

abs: $xreal \to \S r: xreal \cdot r \ge 0$	$abs\ r = \textbf{if } r \ge 0 \textbf{ then } r \textbf{ else } -r \textbf{ fi}$
bin (the binary values)	$bin = \top, \bot$
$ceil$: $real \to int$	$r \le ceil\ r < r+1$
$char$ (the characters)	$char = ..., \text{“a”}, \text{“A”}, ...$
div: $real \to (\S r: real \cdot r>0) \to int$	$div\ x\ y = floor\ (x/y)$
$divides$: $(nat+1) \to int \to bin$	$divides\ n\ i = i/n: int$
$entro$: $prob \to \S r: xreal \cdot r \ge 0$	$entro\ p = p \times info\ p + (1-p) \times info\ (1-p)$
$even$: $int \to bin$	$even\ i = i/2: int$
	$even = divides\ 2$
$floor$: $real \to int$	$floor\ r \le r < floor\ r + 1$
$info$: $prob \to \S r: xreal \cdot r \ge 0$	$info\ p = -\ log\ p$
int (the integers)	$int = nat, -nat$
LIM (limit quantifier)	see Laws
log: $(\S r: xreal \cdot r \ge 0) \to xreal$	$log\ (2^x) = x$
	$log\ (x \times y) = log\ x + log\ y$
max: $xrat \to xrat \to xrat$	$max\ x\ y = \textbf{if } x \ge y \textbf{ then } x \textbf{ else } y \textbf{ fi}$
	$-\ max\ a\ b = min\ (-a)\ (-b)$
MAX (maximum quantifier)	see Laws
min: $xrat \to xrat \to xrat$	$min\ x\ y = \textbf{if } x \le y \textbf{ then } x \textbf{ else } y \textbf{ fi}$
	$-\ min\ a\ b = max\ (-a)\ (-b)$
MIN (minimum quantifier)	see Laws
mod: $real \to (\S r: real \cdot r>0) \to real$	$0 \le mod\ a\ d < d$
	$a = div\ a\ d \times d + mod\ a\ d$
nat (the naturals)	$0, nat+1: nat$
	$0, B+1: B \Rightarrow nat: B$
nil (the empty string)	$\leftrightarrow nil = 0$
	$nil; S = S = S; nil$
	$nil \le S$
$null$ (the empty bunch)	$¢null = 0$
	$null, A = A = A, null$
	$null: A$
odd: $int \to bin$	$odd\ i = \neg\ i/2: int$
	$odd = \neg even$
ok (the empty program)	$ok = \sigma' = \sigma$
	$ok.P = P = P.ok$
$prob$ (probability)	$prob = \S r: real \cdot 0 \le r \le 1$
$rand$ (random number)	$rand\ n: 0,..n$
rat (the rationals)	$rat = int/(nat+1)$
$real$ (the reals)	$r: real = r: xreal \wedge -\infty < r < \infty$
suc: $nat \to (nat+1)$	$suc\ n = n+1$
$xint$ (the extended integers)	$xint = -\infty, int, \infty$
$xnat$ (the extended naturals)	$xnat = nat, \infty$
$xrat$ (the extended rationals)	$xrat = -\infty, rat, \infty$
$xreal$ (the extended reals)	$x: xreal = \exists f: nat \to rat \cdot x = LIM\ f$

End of Names

11.6 Symbols

End of Symbols

11.7 Precedence

0	$\top$ $\bot$ ( ) { } [ ] $\langle\ \rangle$ **if fi** **do od** number text name superscript subscript
1	@ juxtaposition
2	prefix– ¢ \$ $\leftrightarrow$ # * ~ ⚡ □ $\rightarrow$ $\surd$
3	$\times$ / $\cap$
4	+ infix– $\cup$
5	; ;.. ;; ‘
6	, ,.. | $\triangleleft\triangleright$
7	= $\ne$ < > $\le$ $\ge$: :: $\in$ $\subseteq$
8	$\neg$
9	$\wedge$
10	$\vee$
11	$\Rightarrow$ $\Leftarrow$
12	:= ! ?
13	**exit when** **go to** **wait until** **assert** **ensure** **or**
14	. $\Vert$ **result**
15	$\forall\cdot$ $\exists\cdot$ $\Sigma\cdot$ $\Pi\cdot$ §· *LIM*· *MAX*· *MIN*· **var**· **ivar**· **chan**· **frame**·
16	$\pmb{=}$ $\pmb{\Longrightarrow}$ $\pmb{\Longleftarrow}$

Superscripting and subscripting serve to bracket all operations within them.

Juxtaposition associates from left to right, so $a\ b\ c$ means the same as $(a\ b)\ c$. The infix operators @ / – associate from left to right. The infix operators * $\rightarrow$ associate from right to left. The infix operators $\times$ $\cap$ + $\cup$; ;; ‘ , | $\wedge$ $\vee$. $\Vert$ are associative (they associate in both directions).

On levels 7, 11, and 16 the operators are continuing. For example, $a=b=c$ neither associates to the left nor associates to the right, but means the same as $a=b \wedge b=c$. On any one of these levels, a mixture of continuing operators can be used. For example, $a\le b<c$ means the same as $a\le b \wedge b<c$.

The operators $\pmb{=}$ $\pmb{\Longrightarrow}$ $\pmb{\Longleftarrow}$ are identical to = $\Rightarrow$ $\Leftarrow$ except for precedence.

End of Precedence

11.8 Distribution

The operators in the following expressions distribute over bunch union in any operand:

$[A]$ $A@B$ $A\ B$ $-A$ $\$A$ $\leftrightarrow A$ $\#A$ $\sim A$
A^B A_B $A\times B$ A/B $A\cap B$ $A+B$ $A-B$ $A;;B$ $A\cup B$ $A;B$ $A‘B$
$\neg A$ $A\wedge B$ $A\vee B$

The operator in $A*B$ distributes over bunch union in its left operand only.

End of Distribution

End of Reference

End of a Practical Theory of Programming