11.4公理和定律

11.4.0布尔

令 a, b, c, d 和 e 为布尔。

布尔公理

$\top$

$\neg\bot$

双重否定定律

$\neg\neg a \quad = \quad a$

排中定律(Tertium non Datur)

$a \vee \neg a$

对偶定律 (德・摩根定律)

$\neg(a \wedge b) \quad = \quad \neg a \vee \neg b$

$\neg(a \vee b) \quad = \quad \neg a \wedge \neg b$

非矛盾定律

$\neg(a \wedge \neg a)$

互斥定律

$a \Rightarrow \neg b \quad = \quad b \Rightarrow \neg a$

$a = \neg b \quad = \quad b = \neg a$

基定律

$\neg(a \wedge \bot)$

$a \vee \top$

$a \Rightarrow \top$

$\bot \Rightarrow a$

包含定律

$a \Rightarrow b \quad = \quad \neg a \vee b$ (实质蕴涵)

$a \Rightarrow b \quad = \quad (a \wedge b \quad = \quad a)$

$a \Rightarrow b \quad = \quad (a \vee b \quad = \quad b)$

同一定律

$\top \wedge a \quad = \quad a$

$\bot \vee a \quad = \quad a$

$\top \Rightarrow a \quad = \quad a$

$\top = a \quad = \quad a$

吸收定律

$a \wedge (a \vee b) \quad = \quad a$

$a \vee (a \wedge b) \quad = \quad a$

幂等定律

$a \wedge a \quad = \quad a$

$a \vee a \quad = \quad a$

直接证明定律

$(a \Rightarrow b) \wedge a \Rightarrow b$

$(a \Rightarrow b) \wedge \neg b \Rightarrow \neg a$

$(a \vee b) \wedge \neg a \Rightarrow b$

自反定律

$a \Rightarrow a$

$a = a$

传递定律

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

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

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

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

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

间接证明定律

$\neg a \Rightarrow \perp \quad = \quad a$

$\neg a \Rightarrow a \quad = \quad a$

特定化定律

$a \wedge b \Rightarrow a$

结合定律

$a \wedge (b \wedge c) \quad = \quad (a \wedge b) \wedge c$

$a \vee (b \vee c) \quad = \quad (a \vee b) \vee c$

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

$a \neq (b \neq c) \quad = \quad (a \neq b) \neq c$

$a = (b \neq c) \quad = \quad (a = b) \neq c$

分配定律

$a \wedge (b \wedge c) \quad = \quad (a \wedge b) \wedge (a \wedge c)$

$a \wedge (b \vee c) \quad = \quad (a \wedge b) \vee (a \wedge c)$

$a \vee (b \wedge c) \quad = \quad (a \vee b) \wedge (a \vee c)$

$a \vee (b \vee c) \quad = \quad (a \vee b) \vee (a \vee c)$

$a \vee (b \Rightarrow c) \quad = \quad (a \vee b) \Rightarrow (a \vee c)$

$a \vee (b = c) \quad = \quad (a \vee b) = (a \vee c)$

$a \Rightarrow (b \wedge c) \quad = \quad (a \Rightarrow b) \wedge (a \Rightarrow c)$

$a \Rightarrow (b \vee c) \quad = \quad (a \Rightarrow b) \vee (a \Rightarrow c)$

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

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

对称定律(可交换定律)

$a \wedge b \quad = \quad b \wedge a$

$a \vee b \quad = \quad b \vee a$

$a = b \quad = \quad b = a$

$a \neq b \quad = \quad b \neq a$

普遍化定律

$a \Rightarrow a \vee b$

反分配定律

$a \wedge b \Rightarrow c \quad = \quad (a \Rightarrow c) \vee (b \Rightarrow c)$

$a \vee b \Rightarrow c \quad = \quad (a \Rightarrow c) \wedge (b \Rightarrow c)$

反对称定律(双重蕴涵)

$(a \Rightarrow b) \wedge (b \Rightarrow a) \quad = \quad a = b$

移动定律

$a \wedge b \Rightarrow c \quad = \quad a \Rightarrow (b \Rightarrow c)$

$a \wedge b \Rightarrow c \quad = \quad a \Rightarrow \neg b \vee c$

抛弃定律

$a \wedge (a \Rightarrow b) \quad = \quad a \wedge b$

$a \Rightarrow (a \wedge b) \quad = \quad a \Rightarrow b$

归并定律

$(a \Rightarrow b) \wedge (c \Rightarrow d) \quad \Rightarrow \quad a \wedge c \Rightarrow b \wedge d$

$(a \Rightarrow b) \wedge (c \Rightarrow d) \quad \Rightarrow \quad a \vee c \Rightarrow b \vee d$

反单调定律

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

单调定律

$a \Rightarrow b \quad \Rightarrow \quad c \wedge a \Rightarrow c \wedge b$

$a \Rightarrow b \quad \Rightarrow \quad c \vee a \Rightarrow c \vee b$

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

换位定律

$a \Rightarrow b \quad = \quad \neg b \Rightarrow \neg a$

分解定律

$a \wedge c \quad \Rightarrow \quad (a \vee b) \wedge (\neg b \vee c) = (a \wedge \neg b) \vee (b \wedge c) \quad \Rightarrow \quad a \vee c$

情况基定律

if $\top$ **then** a **else** $b \quad = \quad a$

if $\bot$ **then** a **else** $b \quad = \quad b$

情况分析定律

if a **then** b **else** $c \quad = \quad (a \wedge b) \vee (\neg a \wedge c)$

if a **then** b **else** $c = (a \Rightarrow b) \wedge (\neg a \Rightarrow c)$

单一情况定律

if a **then** b **else** $\top \quad = \quad a \Rightarrow b$

if a **then** b **else** $\bot \quad = \quad a \wedge b$

情况创建定律

$a \quad = \quad$ **if** b **then** $b \Rightarrow a$ **else** $\neg b \Rightarrow a$

$a \quad = \quad$ **if** b **then** $b \wedge a$ **else** $\neg b \wedge a$

$a \quad = \quad$ **if** b **then** $b = a$ **else** $b \neq a$

情况反向定律

if a **then** b **else** $c \quad = \quad$ **if** $\neg a$ **then** c **else** b

情况幂等定律

if a **then** b **else** $b \quad = \quad b$

情况吸收定律

if a **then** b **else** $c \quad = \quad$ **if** a **then** $a \wedge b$ **else** c

if a **then** b **else** $c \quad = \quad$ **if** a **then** $a \Rightarrow b$ **else** c

if a **then** b **else** $c \quad = \quad$ **if** a **then** $a = b$ **else** c

if a **then** b **else** $c \quad = \quad$ **if** a **then** b **else** $\neg a \wedge c$

if a **then** b **else** c $=$ **if** a **then** b **else** $a \vee c$

if a **then** b **else** c $=$ **if** a **then** b **else** $a \neq c$

情况分配定律

$\neg$ **if** a **then** b **else** c $=$ **if** a **then** $\neg b$ **else** $\neg c$

(**if** a **then** b **else** c) $\wedge d$ $=$ **if** a **then** $b \wedge d$ **else** $c \wedge d$

并且类似地所有的操作符可分配于**if**的第二和第三操作数

if a **then** $b \wedge c$ **else** $d \wedge e$ $=$ (**if** a **then** b **else** d) $\wedge$ (**if** a **then** c **else** e)

并且类似地可替换 $\wedge$ 为任何其他的操作符。

————————————————————————————————————布尔结束

11.4.1通用符号

操作符 $= +$ **if then else** 适用于任何类型的表达式，并有如下公理成立：

$x = x$ 自反性

$x{=}y$ $=$ $y{=}x$ 对称性

$x{=}y \wedge y{=}z$ $\Rightarrow$ $x{=}z$ 传递性

$x{=}y$ $\Rightarrow$ $(\cdots x \cdots) = (\cdots y \cdots)$ 透明性

$x \neq y$ $=$ $\neg(x = y)$ 不等性

if $\top$ **then** x **else** y $=$ x 基情况

if $\perp$ **then** x **else** y $=$ y 基情况

注意：在透明性公理中 x 的上下文（由x周围的省略号表示）必须与y 的上下文（由 y 周围的省略号表示)一样。

操作符 $<$ $\leq$ $>$ $\geq$ 可适用于数字，字符，字符串和表，有如下公理成立：

$\neg\, x < x$ 反自反性

$\neg(x < y \wedge x > y)$ 排他性

$\neg(x < y \wedge x = y)$ 排他性

$x \leq y \wedge y \leq x$ $=$ $x = y$ 反对称性

$x{<}y \wedge y{<}z \Rightarrow x{<}z$ 传递性

$x \leq y$ $=$ $x{<}y \vee x{=}y$ 包含性

$x > y$ $=$ $y < x$ 镜像

$x \geq y$ $=$ $y \leq x$ 镜像

$x{<}y \vee x{=}y \vee x{>}y$ 完全性，三分法

————————————————————————————————————通用符号结束

11.4.2数

令 d 为一个数字序列(零个或多个数字)，令 x， y，和 z 为数字。

$d0{+}1 = d1$ 计数

$d1{+}1 = d2$ 计数

$d2{+}1 = d3$ 计数

$d3{+}1 = d4$ 计数

$d4{+}1 = d5$ 计数

$d5+1 = d6$	计数
$d6+1 = d7$	计数
$d7+1 = d8$	计数
$d8+1 = d9$	计数
$d9+1 = (d+1)0$	计数 (参见练习22)
$+x = x$	恒等性
$x+0 = x$	恒等元
$x+y = y+x$	对称性
$x+(y+z) = (x+y)+z$	结合性
$-\infty < x < \infty \Rightarrow (x+y = x+z = y=z)$	消去性
$-\infty < x \Rightarrow \infty + x = \infty$	吸收律
$x < \infty \Rightarrow -\infty + x = -\infty$	吸收律
$-x = 0 - x$	负数
$- -x = x$	自反
$-(x+y) = -x + -y$	分配性
$-(x \times y) = -x \times y$	半分配性
$-(x/y) = (-x)/y$	结合性
$x - y = -(y - x)$	反对称性
$x-y = x + -y$	减法
$x + (y - z) = (x + y) - z$	结合性
$-\infty < x < \infty \Rightarrow (x - y = x - z = y = z)$	消去性
$-\infty<x<\infty \Rightarrow x-x = 0$	逆转
$x < \infty \Rightarrow \infty - x = \infty$	吸收律
$-\infty < x \Rightarrow -\infty - x = -\infty$	吸收律
$-\infty<x<\infty \Rightarrow x\times 0 = 0$	基
$x\times 1 = x$	恒等元
$x\times y = y\times x$	对称性
$x\times(y+z) = x\times y + x\times z$	分配性
$x\times(y\times z) = (x\times y) \times z$	结合性
$-\infty<x<\infty \wedge x\neq 0 \Rightarrow (x\times y = x\times z = y=z)$	消去性
$0 < x \Rightarrow x \times \infty = \infty$	吸收律
$0 < x \Rightarrow x \times -\infty = -\infty$	吸收律
$x/1 = x$	恒等元
$-\infty<y<\infty \wedge y\neq 0 \Rightarrow x/y\times y = x$	逆转
$x \times (y/z) = (x \times y)/z$	结合性
$-\infty < x < \infty \Rightarrow x/\infty = 0 = x/-\infty$	湮没性
$-\infty<x<\infty \Rightarrow x^0 = 1$	基
$x^1 = x$	恒等性
$x^{y+z} = x^y \times x^z$	指数
$x^{y\times z} = (x^y)^z$	指数
$-\infty < 0<1<\infty$	方向性
$x < y = -y < -x$	反射性
$-\infty<x<\infty \Rightarrow (x+y < x+z = y<z)$	消去性，转换
$0<x<\infty \Rightarrow (x\times y < x\times z = y<z)$	消去性，比例

$x < y \vee x = y \vee x > y$ 三分法

$-\infty \le x \le \infty$ 极值

---数结束

11.4.3 束

令x和 y为元素（布尔，数字，字符，集合，串和元素的表）。

x: y = x=y	初等公理
x: A,B = x: A ∨ x: B	复合公理
A,A = A	幂等性
A,B = B,A	对称性
A,(B,C) = (A,B),C	结合性
A'A = A	幂等性
A'B = B'A	对称性
A'(B'C) = (A'B)'C	结合性
A,B: C = A: C ∧ B: C	反分配性
A: B'C = A: B ∧ A: C	分配性
A: A,B	普遍化
A'B: A	特定化
A: A	自反性
A: B ∧ B: A = A=B	反对称性
A: B ∧ B: C ⇒ A: C	传递性
$\not\subset null = 0$	大小
$\not\subset x = 1$	大小
⊄(A, B) + ⊄(A'B) = ⊄A + ⊄B	大小
¬ x: A ⇒ ⊄(A'x) = 0	大小
A: B ⇒ ⊄A ≤ ⊄B	大小
A,(A'B) = A	吸收律
A'(A,B) = A	吸收律
A: B = A,B = B = A = A'B	包含性
A,(B,C) = (A,B),(A,C)	分配性
A,(B'C) = (A,B)'(A,C)	分配性
A'(B,C) = (A'B), (A'C)	分配性
A'(B'C) = (A'B)'(A'C)	分配性
A: B ∧ C: D ⇒ A,C: B,D	inflation，单调性
A: B ∧ C: D ⇒ A'C: B'D	inflation，单调性
null: A	归纳
A, null = A	恒等性
A ' null = null	基
⊄A = 0 = A = null	大小
i: x,..y = $x \le$ i<y	(对广义整数i , x , y , $x \le y$)
⊄(x,..y) = y–x	(对广义整数i , x , y , $x \le y$)
–null = null	分配性

$-(A, B) \quad = \quad -A, -B$ 分配性

$A + null = null + A = null$ 分配性

$(A, B)+(C, D) \quad = \quad A+C, A+D, B+C, B+D$ 分配性

对许多其它运算符也类似（见本书最后页）

--束结束

11.4.4集合

$\{\sim S\} = S$

$\sim \{A\} = A$

$\{A\} \neq A$

$A \in \{B\} = A : B$

$\{A\} \subseteq \{B\} = A : B$

$\{A\} \in_{2} \{B\} = A : B$

$\$ \{A\} = ¢\ A$

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

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

$\{A\} = \{B\} \quad = \quad A = B$

$\{A\} \neq \{B\} \quad = \quad A \neq B$

--集合结束

11.4.5 串

令S， T ,和U是串；令i和j是项（布尔，数，字符，项束，集合，表，函数）；令 n为自然数；令x， y，和 z 为整数。

$nil; S = S; nil = S$

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

$\#nil = 0$

$\#\ i = 1$

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

$S_{nil} = nil$

$(S; i; T)_{\#S} = i$

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

$S_{(TU)} = (S_T)_U$

$0*S = nil$

$(n+1)*S = n*S; S$

$i{=}j = S; i; T = S; j; T$

$i<j \Rightarrow S; i; T < S; j; U$

$nil \le S < S; i; T$

$x;..x = nil$

$x;..x+1 = x$

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

$\#(x;..y) = y-x$

---串结束

11.4.6 表

令S和T为串；令n为自然数；令 i和 j 为项（布尔，数，字符，项束，集合，表，函数）；令 L , M , 和N为表。

$[S]\ n = S_n$

$\#[S] = S$

$(\# S) \rightarrow i \mid [S; j; T] = [S; i; T]$

$[S]+[T] = [S; T]$

$[S] = [T] \quad = \quad S = T$

$[S]\ [T] = [S_T]$

$[S] < [T] \quad = \quad S < T$

$(L\ M)\ n = L\ (M\ n)$

$L\ null = null$

$(L\ M)\ N = L\ (M\ N)$

$L\ (A, B) = L\ A, L\ B$

$L@nil = L$

$L\ \{A\} = \{L\ A\}$

$L@i = L\ i$

$L\ nil = nil$

$L@(S; T) = L@S@T$

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

$nil \rightarrow i \mid L = i$

$L\ [S] = [L\ S]$

$(S;T) \rightarrow i \mid L = S \rightarrow (T \rightarrow i \mid L@S) \mid L$

$L\ (M+N) = L\ M + L\ N$

$[S]\ S = [S] = [\ S]$

--表结束

11.4.7 函数

换名公理 — 若 v和w不出现在D中，且w不出现在b中

$\lambda v: D\cdot\ b \quad = \quad \lambda w: D\cdot$ (在b中以w置换v)

应用公理：若元素$x: D$

$(\lambda v: D\cdot\ b)\ x =$ (在b中以x置换v)

扩展定律

$f \quad = \quad \lambda v: \Delta f\cdot\ f\ v$

定义域公理

$\Delta\ \lambda v: D\cdot\ b \quad = \quad D$

函数组合公理：若 $\neg\ f: \Delta g$

$\Delta(g\ f) = \S x: \Delta f\cdot\ fx: \Delta g$

$(g\ f)\ x = g\ (f\ x)$

$f\ (g\ h) = (f\ g)\ h$

函数包含定律

$f: g = \Delta g: \Delta f \wedge \forall x: \Delta g \cdot fx: gx$

基数公理

$¢A = \Sigma A \to 1$

函数相等定律

$f = g = \Delta f = \Delta g \wedge \forall x: \Delta f \cdot fx = gx$

函数交公理

$\Delta(f ‘ g) = \Delta f, \Delta g$

$(f ‘ g)\ x = f\,x ‘ g\,x$

函数并公理

$\Delta(f, g) = \Delta f ‘ \Delta g$

$(f, g)\ x = f\,x, g\,x$

选择合并定律

$f \mid f = f$

$(g \mid h)\ f = g\,f \mid h\,f$

$(\lambda v: A \cdot x) \mid (\lambda v: B \cdot y) = \lambda v: A, B \cdot \textbf{if } v: A \textbf{ then } x \textbf{ else } y$

选择合并公理与定律

$\Delta(f \mid g) = \Delta f, \Delta g$

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

$f \mid (g \mid h) = (f \mid g) \mid h$

分配公理

$f\ null = null$

$f\,(A, B) = f\,A, f\,B$

$f\,(\S g) = \S y: f\,(\Delta g) \cdot \exists x: \Delta g \cdot fx{=}y \wedge gx$

$f\,(\textbf{if } b \textbf{ then } x \textbf{ else } y) = \textbf{if } b \textbf{ then } f\,x \textbf{ else } f\,y$

$(\textbf{if } b \textbf{ then } f \textbf{ else } g)\ x = \textbf{if } b \textbf{ then } f\,x \textbf{ else } g\,x$

箭头定律

$f: null \to A$

$A \to B: (A ‘ C) \to (B, D)$

$f: A \to B = A: \Delta f \wedge \forall a: A \cdot fa: B$

---函数结束

11.4.8 量词

令 x为元素，令 a , b和 c为布尔变量，令 n和m为数，令 f和g为函数，令P为谓词。

$\forall v: null \cdot b = \top$

$\forall v: A,B \cdot b = (\forall v: A \cdot b) \wedge (\forall v: B \cdot b)$

$\forall v: x\cdot b = (\lambda v: x\cdot b)\ x$

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

$\exists v: null\cdot b = \bot$

$\exists v: A,B\cdot b = (\exists v: A\cdot b) \vee (\exists v: B\cdot b)$

$\exists v: x\cdot b = (\lambda v: x\cdot b)\ x$

$\exists v: (\S v: D\cdot b)\cdot c = \exists v: D\cdot b \wedge c$

$\Sigma v: null\cdot n = 0$

$(\Sigma v: A,B\cdot n) + (\Sigma v: A`B\cdot n) = (\Sigma v: A\cdot n) + (\Sigma v: B\cdot n)$

$\Sigma v: x\cdot n = (\lambda v: x\cdot n)\ x$

$\Sigma v: (\S v: D\cdot b)\cdot n = \Sigma v: D\cdot \textbf{if } b \textbf{ then } n \textbf{ else } 0$

$\Pi v: null\cdot n = 1$

$(\Pi v: A,B\cdot n) \times (\Pi v: A`B\cdot n) = (\Pi v: A\cdot n) \times (\Pi v: B\cdot n)$

$\Pi v: x\cdot n = (\lambda v: x\cdot n)\ x$

$\Pi v: (\S v: D\cdot b)\cdot n = \Pi v: D\cdot \textbf{if } b \textbf{ then } n \textbf{ else } 1$

$MIN\ v: null\cdot n = \infty$

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

$MIN\ v: x\cdot n = (\lambda v: x\cdot n)\ x$

$MIN\ v: (\S v: D\cdot b)\cdot n = MIN\ v: D\cdot \textbf{if } b \textbf{ then } n \textbf{ else } \infty$

$MAX\ v: null\cdot n = -\infty$

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

$MAX\ v: x\cdot n = (\lambda v: x\cdot n)\ x$

$MAX\ v: (\S v: D\cdot b)\cdot n = MAX\ v: D\cdot \textbf{if } b \textbf{ then } n \textbf{ else } -\infty$

$\S v: null\cdot b = null$

$\S v: x\cdot b = \textbf{if } (\lambda v: x\cdot b)\ x \textbf{ then } x \textbf{ else } null$

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

$\S v: A`B\cdot b = (\S v: A\cdot b)\ `\ (\S v: B\cdot b)$

$\S v: (\S v: D\cdot b)\cdot c = \S v: D\cdot b \wedge c$

变量改变定律 — 若 d不出现在b中

$\forall r: fD\cdot b = \forall d: D\cdot$ (在b中以fd置换r)

$\exists r\colon fD\cdot\ b = \exists d\colon D\cdot$ (在b中以 fd置换r)

$\Sigma r\colon fD\cdot\ n = \Sigma d\colon D\cdot$ (在n中以fd置换r)

$\Pi r\colon fD\cdot\ n = \Pi d\colon D\cdot$ (在n中以fd置换r)

$MIN\ r\colon fD\cdot\ n = MIN\ d\colon D\cdot$ (在n中以fd置换r)

$MAX\ r\colon fD\cdot\ n = MAX\ d\colon D\cdot$ (在n中以fd置换r)

束-元素转换定律

$V\colon W = \forall v\colon V\cdot \exists w\colon W\cdot\ v{=}w$

$fV\colon gW = \forall v\colon V\cdot \exists w\colon W\cdot\ fv{=}gw$

恒等公理

$\forall v\cdot\top$

$\neg\exists v\cdot\bot$

幂等定律 — 若 $D\neq\ null$且v不出现在b 中

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

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

吸收定律 — 若f $x\colon D$

$(\lambda v\colon D\cdot\ b)\ x \wedge \exists v\colon D\cdot\ b = (\lambda v\colon D\cdot\ b)\ x$

$(\lambda v\colon D\cdot\ b)\ x \vee \forall v\colon D\cdot\ b = (\lambda v\colon D\cdot\ b)\ x$

$(\lambda v\colon D\cdot\ b)\ x \wedge \forall v\colon D\cdot\ b = \forall v\colon D\cdot\ b$

$(\lambda v\colon D\cdot\ b)\ x \vee \exists v\colon D\cdot\ b = \exists v\colon D\cdot\ b$

分配公理和定律 — 若 $D\neq\ null$且v不出现在a 中

$a \wedge \forall v\colon D\cdot\ b = \forall v\colon D\cdot\ a \wedge b$

$a \wedge \exists v\colon D\cdot\ b = \exists v\colon D\cdot\ a \wedge b$

$a \vee \forall v\colon D\cdot\ b = \forall v\colon D\cdot\ a \vee b$

$a \vee \exists v\colon D\cdot\ b = \exists v\colon D\cdot\ a \vee b$

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

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

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

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

特定化定律 — 若 $x\colon D$

$\forall v\colon D\cdot\ b \Longrightarrow (\lambda v\colon D\cdot\ b)\ x$

普遍化定律 — 若 $x\colon D$

$(\lambda v: D \cdot b)\, x \Longrightarrow \exists v: D \cdot b$

单点定律 — 若 $x: D$且v不出现在x中

$\forall v: D \cdot v{=}x \Rightarrow b = (\lambda v: D \cdot b)\, x$

$\exists v: D \cdot v{=}x \wedge b = (\lambda v: D \cdot b)\, x$

分裂定律 — 对任何固定定义域

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

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

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

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

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

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

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

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

二元定律

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

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

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

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

交换定律

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

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

解定律

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

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

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

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

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

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

$x: \S p = x: \Delta p \wedge px$

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

$\exists f = (\S f)\ null$

半交换定律(Skolem)

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

$\forall x \cdot \exists y \cdot Pxy = \exists f \cdot \forall x \cdot Px(fx)$

定义域改变定律

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

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

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

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

约束公理和定律

若 v不出现在 n中

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

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

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

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

$n \geq (MIN\ v: D \cdot m) \Leftarrow (\exists v: D \cdot n\geq m)$

$n \leq (MAX\ v: D \cdot m) \Leftarrow (\exists v: D \cdot n\leq m)$

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

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

极值定律

$\forall v \cdot (MIN\ v \cdot n) \leq n \leq (MAX\ v \cdot n)$

连接定律(Galois)

$n\leq m = \forall k \cdot k\leq n \Rightarrow k\leq m$

$n\leq m = \forall k \cdot k<n \Rightarrow k<m$

$n\leq m = \forall k \cdot m\leq k \Rightarrow n\leq k$

$n\leq m = \forall k \cdot m<k \Rightarrow n<k$

分配定律— if $D \neq null$ 且 v不出现在 n中

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

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

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

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

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

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

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

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

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

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

$n\geq 0 \Rightarrow n \times (MAX\ v: D \cdot m) = (MAX\ v: D \cdot n\times m)$

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

--量词结束

11.4.9 极限

$(MAX\ m{\cdot}\ MIN\ n{\cdot}\ f(m+n)) \le (LIM\ f) \le (MIN\ m{\cdot}\ MAX\ n{\cdot}\ f(m+n))$

$\exists m{\cdot}\ \forall n{\cdot}\ p(m+n) \Longrightarrow LIM\ p \Longrightarrow \forall m{\cdot}\ \exists n{\cdot}\ p(m+n)$

--极限结束

11.4.10 规约与程序

对于规范P，Q，R 和 S，以及布尔变量b，

$ok = x'{=}x \wedge y'{=}y \wedge \ldots$

$x{:=}\ e = x'{=}e \wedge y'{=}y \wedge \ldots$

$P.\ Q = \exists x'', y'', \ldots{\cdot}$ (在P中以x'' 置换 x'，y'' 置换 y')
∧ (在Q中以x'' 置换x，y'' 置换y)

$P||Q = \exists t_P, t_Q{\cdot}$ (在P中以t_P置换t')
∧ (在Q中以t_Q置换t')
$\wedge\ t' = max\ t_P\ t_Q$

if b **then** P **else** $Q = b \wedge P \vee \neg b \wedge Q$

var $x{:}\ T{\cdot}\ P = \exists x, x'{:}\ T{\cdot}\ P$

while b **do** $P = t'{\ge}t \wedge$ (**if** b **then** ($P.\ t{:=}\ t{+}inc.$ **while** b **do** P) **else** ok)

$(Fmn \Longleftarrow m{=}n \wedge ok) \wedge (Fik \Longleftarrow m{\le}i{<}j{<}k{\le}n \wedge (Fij.\ Fjk))$

$\Rightarrow (Fmn \Longleftarrow$ **for** $i{:=}\ m;..n$ **do** $m{\le}i{<}n \Rightarrow Fi(i{+}1))$

$Im{\Rightarrow}I'n \Longleftarrow$ **for** $i{:=}\ m;..n$ **do** $m{\le}i{<}n \wedge Ii \Rightarrow I'(i{+}1)$

wait until $w = t{:=}\ max\ t\ w$

assert $b =$ **if** b **then** ok **else** ($print$ "error". **wait until** ∞)

ensure $b = b \wedge ok$

$x' = (P$ **result** $e) = P.\ x' = e$

$c? = r{:=}\ r{+}1$

$c = M\ (r{-}1)$

$c!\ e = M\ w = e \wedge T\ w = t \wedge (w{:=}\ w{+}1)$

$\surd c = T\ r$ + (transit time) $\le t$

ivar $x{:}\ T{\cdot}\ S = \exists x{:}\ time{\rightarrow}T{\cdot}\ S$

chan $c{:}\ T{\cdot}\ P = \exists M_c{:}\ [\infty{*}T]{\cdot}\ \exists T_c{:}\ [\infty{*}xreal]{\cdot}$ **var** $r_c, w_c{:}\ xnat := 0{\cdot}\ P$

$ok.\ P = P.\ ok = P$ 恒等性

$P.\ (Q.\ R) = (P.\ Q).\ R$ 结合性

$\textbf{if } b \textbf{ then } P \textbf{ else } P = P$ 幂等性

$\textbf{if } b \textbf{ then } P \textbf{ else } Q = \textbf{if } \neg b \textbf{ then } Q \textbf{ else } P$ 情况逆转

$P = \textbf{if } b \textbf{ then } b \Rightarrow P \textbf{ else } \neg b \Rightarrow P$ 情况创建

$P \vee Q.\ R \vee S = (P.\ R) \vee (P.\ S) \vee (Q.\ R) \vee (Q.\ \mathrm{S})$ 分配性

$(\textbf{if } b \textbf{ then } P \textbf{ else } Q).\ R = \textbf{if } b \textbf{ then } (P.\ R) \textbf{ else } (Q.\ R)$ 分配性 (unprimed b)

$ok \parallel P = P \parallel ok = P$ 恒等性

$P \parallel Q = Q \parallel P$ 对称性

$P \parallel (Q \parallel R) = (P \parallel Q) \parallel R$ 结合性

$P \parallel Q \vee R = (P \parallel Q) \vee (P \parallel R)$ 分配性

$P \parallel \textbf{if } b \textbf{ then } Q \textbf{ else } R = \textbf{if } b \textbf{ then } (P \parallel Q) \textbf{ else } (P \parallel R)$ 分配性

$\textbf{if } b \textbf{ then } (P \| Q) \textbf{ else } (R \| S) = \textbf{if } b \textbf{ then } P \textbf{ else } R \parallel \textbf{if } b \textbf{ then } Q \textbf{ else } S$ 分配性

$x := \textbf{if } b \textbf{ then } e \textbf{ else } f = \textbf{if } b \textbf{ then } x := e \textbf{ else } x := f$ 函数-命令

$\forall \sigma, \sigma' \cdot (\textbf{if } b \textbf{ then } (P.\ W) \textbf{ else } ok \Longleftarrow W) \Longrightarrow \forall \sigma, \sigma' \cdot (\textbf{while } b \textbf{ do } P \Longleftarrow W)$

--规范与函数结束

11.4.11 置换

令x和 y为不同的边界状态变量，令e和f为前置状态表达式，令P为一个规范。.

$x := e.\ P =$ (在P中置换x为e)

$(x := e \parallel y := f).\ P =$ (在P中置换x为e，且独立地置换y为 f)

--置换结束

11.4.12 条件

令 P和Q为任意规范，令C为一个前置条件，令C'为相应的后置条件（换句话说，除了在所有状态变量上加撇外，C'与C相同）。

$C \wedge (P.\ Q) \Longleftarrow C \wedge P.\ Q$

$C \Rightarrow (P.Q) \Longleftarrow C \Rightarrow P.\ Q$

$(P.Q) \wedge C' \Longleftarrow P.\ Q \wedge C'$

$(P.Q) \Leftarrow C' \Longleftarrow P.\ Q \Leftarrow C'$

$P.\ C \wedge Q \Longleftarrow P \wedge C'.\ Q$

$P.\ Q \Longleftarrow P \wedge C'.\ C \Rightarrow Q$

C是P被S精化的充分前置条件当且仅当$C \Rightarrow P$被S精化。

C' 是P被S精化的充分前置条件当且仅当$C' \Rightarrow P$被S精化。

--条件结束

11.4.13 精化

逐步精化法(逐步精化)(单调性,传递性)

若 $A \Leftarrow$ **if** b **then** C **else** D 和$C \Leftarrow E$ 和$D \Leftarrow F$ 为定理，

则 $A \Leftarrow$ **if** b **then** E **else** F 为定理。

若 $A \Leftarrow B.C$ 和 $B \Leftarrow D$ 和 $C \Leftarrow E$ 为定理，则 $A \Leftarrow D.E$ 为定理。

若 $A \Leftarrow B||C$ 和 $B \Leftarrow D$ 和 $C \Leftarrow E$ 为定理，则 $A \Leftarrow D||E$ 为定理。

若 $A \Leftarrow B$ 和 $B \Leftarrow C$ 为定理，则 $A \Leftarrow C$ 为定理。

部分精化法（单调性，归并）

若 $A \Leftarrow$ **if** b **then** C **else** D 和 $E \Leftarrow$ **if** b **then** F **else** G 为定理，

则 $A \wedge E \Leftarrow$ **if** b **then** $C \wedge F$ **else** $D \wedge G$ 为定理。

若 $A \Leftarrow B.C$ 和 $D \Leftarrow E.F$ 为定理，则 $A \wedge D \Leftarrow B \wedge E.\ C \wedge F$ 为定理。

若 $A \Leftarrow B||C$ 和 $D \Leftarrow E||F$ 为定理，则$A \wedge D \Leftarrow B \wedge E\ ||\ C \wedge F$ 为定理。

若 $A \Leftarrow B$ 和$C \Leftarrow D$ 为定理，则$A \wedge C \Leftarrow B \wedge D$ 为定理。

情况精化法

$P \Leftarrow$ **if** b **then** Q **else** R 为定理当且仅当

$P \Leftarrow b \wedge Q$ 和 $P \Leftarrow \neg b \wedge R$ 为定理。

--精化结束

--公理和定律结束

11.5 名字

abs: *xreal*→§*r*: *xreal*· *r*≥0	*abs r* = **if** *r*≥0 **then** *r* **else** –*r*
bool (布尔)	*bool* = ⊤ , ⊥
ceil: *real*→*int*	*r* ≤ *ceil r* < *r*+1
char (字符)	*char* = ..., \`a, \`A, ...
div: *real*→(§*r*: *real*· *r*>0)→*int*	*div x y* = *floor* (*x*/*y*)
divides: (*nat*+1)→*int*→*bool*	*divides n i* = *i*/*n*: *int*
entro: *prob*→§*r*: *xreal*· *r*≥0	*entro p* = *p* × *info p* + (1–*p*) × *info* (1–*p*)
even: *int*→*bool*	*even i* = *i*/2: *int* *even* = *divides* 2
floor: *real*→*int*	*floor r* ≤ *r* < *floor r* + 1
info: *prob*→§*r*: *xreal*· *r*≥0	*info p* = – *log p*
int (整数)	*int* = *nat*, –*nat*
LIM (极限量词)	见公理和定律
log: (§*r*: *xreal*· *r*≥0)→*xreal*	*log* (2^x) = *x* *log* (*x*×*y*) = *log x* + *log y*
max: *xrat*→*xrat*→*xrat*	*max x y* = **if** *x*≥*y* **then** *x* **else** *y* – *max a b* = *min* (–*a*) (–*b*)
MAX (最大量词)	见公理与定律

min: *xrat*→*xrat*→*xrat*	*min x y* = **if** *x*≤*y* **then** *x* **else** *y*
	– *min a b* = *max* (–*a*) (–*b*)
MIN (最小量词)	见公理与定律
mod: *real*→(§*r*: *real*· *r*>0)→*real*	0 ≤ *mod a d* < *d*
	a = *div a d* × *d* + *mod a d*
nat (自然数)	0, *nat*+1: *nat*
	0, *B*+1: *B* ⇒ *nat*: *B*
nil (空串)	*nil* = 0
	nil; *S* = *S* = *S*; *nil*
	nil ≤ *S*
null (空束)	¢*null* = 0
	null, *A* = *A* = *A*, *null*
	null: *A*
odd: *int*→*bool*	*odd i* ＝ ¬ *i*/2: *int*
	odd = ¬*even*
ok (空程序)	*ok* ＝ σ′=σ
	ok.*P* ＝ *P*.*ok* ＝ *ok* ‖ *P* ＝ *P* ‖ *ok* ＝ *P*
prob (概率)	*prob* = §*r*: *real*· 0≤*r*≤1
rand (随机数)	*rand n*: 0,..*n*
rat (有理数)	*rat* = *int*/(*nat*+1)
real (实数)	*r*: *real* ＝ *r*: *xreal* ∧ –∞<*r*<∞
suc: *nat*→(*nat*+1)	*suc n* = *n*+1
xint (广义整数)	*xint* = –∞, *int*, ∞
xnat (广义自然数)	*xnat* = *nat*, ∞
xrat (广义有理数)	*xrat* = –∞, *rat*, ∞
xreal (广义实数)	*x*: *xreal* ＝ ∃*f*: *nat*→*rat*· *x* = *LIM f*

--名字结束

11.6 符号

⊤	真值	( )	括号
⊥	假值	{ }	集合括号
¬	非	[ ]	表括号
∧	与	2	幂集
∨	或	¢	束的大小，基数
⇒	蕴含，等于或强于	$	集合大小，基数
⟹	蕴含，等于或强于		串大小，长度
⇐	被蕴含，由…导出，弱于或等于	#	表大小，长度
⟸	被蕴含，由…导出，弱于或等于	|	选择合并，否则
=	等于，当且仅当	‖	独立（并行）组合
＝	等于，当且仅当	~	集合内容
≠	不同于，不等于，异或，布尔加	~	表内容
<	小于	*	串的重复
>	大于	Δ	函数的定义域

≤	小于或等于	→	函数箭头
≥	大于或等于	∈	集合的元素
+	加	⊆	子集
+	表连接	∪	集合并
–	减	∩	集合交
×	倍数，相乘	@	指针索引
/	除	λ	函数，变量引入
,	束的并	∀	对所有，全称量词
,..	从(incl) 到(excl)	∃	存在，存在量词
‘	束的交	Σ	和，累加量词
;	串连接	Π	乘积，累乘量词
;..	从 (incl)到(excl)	§	那些，解量词
:	在里面，束包含	′	x'是状态变量x的终结值
::	包含	`	`A是一个字符
:=	赋值	"	"hello"是一个字符表的文本
.	相关（顺序）组合	a^b	指数
·	变量引入	a_b	串索引
!	输出	$a\ b$	索引，应用，组合
?	输入	√	输入检查
		∞	无限

assert	**ivar**
chan	**loop end**
ensure	**or**
exit when	**result**
for do	**var**
frame	**wait until**
go to	**while do**
if then else	

——————————————————————————————————————符号结束

11.7 优先级

0. ⊤ ⊥ ( ) { } [ ] **loop end** 数 字符 文本 名字
1. @ 并置
2. +前缀 –前缀 ¢ $ # * ~ $_2$ Δ → √ 上标 下标
3. × / ∩
4. + – + ∪
5. ; ;.. ‘
6. , ,.. |
7. = ≠ < > ≤ ≥ : :: ∈ ⊆
8. ¬
9. ∧
10. ∨
11. ⇒ ⇐
12. := ! ?
13. **if then else** **while do** **exit when** **for do** **go to**

wait until **assert** **ensure** **or**
14. . ‖ **result**
15. λ· ∀· ∃· Σ· Π· §· *LIM*· *MAX*· *MIN*· **var**· **ivar**·
chan· **frame**·
16. ＝ ⟹ ⟸

在第2级，上标和下标中的运算相当于加了括号的运算，例如2^{3+4}相当于$2^{(3+4)}$，$(3;5;7;9)_{1+1}$相当于$(3;5;7;9)_{(1+1)}$。

并置从左向右结合，因此*a b c*等同于(*a b*) *c*。中缀运算符 @ / – 从左向右结合。中缀运算符 * → 从右向左结合。中缀运算符 × ∩ + + ∪ ; ‘ , | ∧ ∨ . ‖ 是可结合的（可从两个方向结合）。

在第 7, 11, 和16级，运算符是连续的。例如，$a = b = c$ 既不向左也不向右结合，但等同于$a = b \wedge b = c$。在任意级别的连续运算符可以混合使用，例如 $a \le b < c$ 等同于 $a \le b \wedge b < c$。

在第13和15级，优先顺序应用于最后一个操作数（**or**的第一个操作数），而不是被运算符包围的操作数。

运算符＝ ⟹ ⟸除优先级别外与 = ⇒ ⇐ 等同。
———————————————————————————————————————优先级结束

11.8 分配性

下面运算符在束的并上是可分配的：
[ ] @ 并置 +前缀 –前缀 *$* # *(仅左操作数)
~ 上标 下标 × / ∩ + – + ∪ ; ‘ ¬ ∧ ∨
———————————————————————————————————————分配性结束
———————————————————————————————————————参考结束
———————————————————————————————————一种实用的程序设计理论结束