Equivalence and true

*(3.1) associativity of $\equiv$: $((p \equiv q) \equiv r) \;\equiv\; (p \equiv (q \equiv r))$
*(3.2) symmetry of $\equiv$: $p \equiv q \equiv q \equiv p$
*(3.3) identity of $\equiv$: $true \equiv q \equiv q$
(3.4) $true$
(3.5) reflexivity of $\equiv$: $p \equiv p$

Negation, inequivalence, and false

*(3.8) definition of $false$: $false \equiv \neg true$
*(3.9) distributivity of $\neg$ over $\equiv$: $\neg(p \equiv q) \;\equiv\; \neg p \equiv q$
*(3.10) definition of $\not\equiv$: $(p \not\equiv q) \;\equiv\; \neg(p \equiv q)$
(3.11) $\neg p \equiv q \equiv p \equiv \neg q$
(3.12) double negation $\neg\neg p \equiv p$
(3.13) negation of $false$: $\neg false \equiv true$
(3.14) $(p \not\equiv q) \;\equiv\; \neg p \equiv q$
(3.15) $\neg p \equiv p \equiv false$
(3.16) symmetry of $\not\equiv$: $(p \not\equiv q) \;\equiv\; (q \not\equiv p)$
(3.17) associativity of $\not\equiv$: $((p \not\equiv q) \not\equiv r) \;\equiv\; (p \not\equiv (q \not\equiv r))$
(3.18) mutual associativity: $((p \not\equiv q) \equiv r) \;\equiv\; (p \not\equiv (q \equiv r))$
(3.19) mutual interchangeability: $p \not\equiv q \equiv r \;\equiv\; p \equiv q \not\equiv r$

Disjunction

*(3.24) symmetry of $\vee$: $p \vee q \equiv q \vee p$
*(3.25) associativity of $\vee$: $(p \vee q) \vee r \equiv p \vee (q \vee r)$
*(3.26) idempotency of $\vee$: $p \vee p \equiv p$
*(3.27) distributivity of $\vee$ over $\equiv$: $p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$
*(3.28) excluded middle: $p \vee \neg p$
(3.29) zero of $\vee$: $p \vee true \equiv true$
(3.30) identity of $\vee$: $p \vee false \equiv p$
(3.31) distributivity of $\vee$ over $\vee$: $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$
(3.32) $p \vee q \equiv p \vee \neg q \equiv p$

Conjunction

*(3.35) golden rule: $p \wedge q \equiv p \equiv q \equiv p \vee q$
(3.36) symmetry of $\wedge$: $p \wedge q \equiv q \wedge p$
(3.37) associativity of $\wedge$: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
(3.38) idempotency of $\wedge$: $p \wedge p \equiv p$
(3.39) identity of $\wedge$: $p \wedge true \equiv p$
(3.40) zero of $\wedge$: $p \wedge false \equiv false$
(3.41) distributivity of $\wedge$ over $\wedge$: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$
(3.42) contradiction: $p \wedge \neg p \equiv false$
(3.43) absorption:
  (a) $p \wedge (p \vee q) \equiv p$
  (b) $p \vee (p \wedge q) \equiv p$
(3.44) absorption:
  (a) $p \wedge (\neg p \vee q) \equiv p \wedge q$
  (b) $p \vee (\neg p \wedge q) \equiv p \vee q$
(3.45) distributivity of $\vee$ over $\wedge$: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
(3.46) distributivity of $\wedge$ over $\vee$: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
(3.47) De Morgan:
  (a) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
  (b) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
(3.48) $p \wedge q \equiv p \wedge \neg q \equiv \neg p$
(3.49) $p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$
(3.50) $p \wedge (q \equiv p) \equiv p \wedge q$
(3.51) replacement: $(p \equiv q) \wedge (r \equiv p) \;\equiv\; (p \equiv q) \wedge (r \equiv q)$
(3.52) definition of $\equiv$: $p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
(3.53) exclusive or: $p \not\equiv q \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$
(3.55)
$(p \wedge q) \wedge r \;\equiv\; p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r$

Implication

*(3.57) definition of implication: $p \Rightarrow q \equiv p \vee q \equiv q$
*(3.58) consequence: $p \Leftarrow q \equiv q \Rightarrow p$
(3.59) definition of implication: $p \Rightarrow q \equiv \neg p \vee q$
(3.60) definition of implication: $p \Rightarrow q \equiv p \wedge q \equiv p$
(3.61) contrapositive: $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
(3.62) $p \Rightarrow (q \equiv r) \equiv p \wedge q \equiv p \wedge r$
(3.63) distributivity of $\Rightarrow$ over $\equiv$:
  $p \Rightarrow (q \equiv r) \equiv p \Rightarrow q \equiv p \Rightarrow r$
(3.64) $p \Rightarrow (q \Rightarrow r) \equiv (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$
(3.65) shunting: $p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$
(3.66) $p \wedge (p \Rightarrow q) \equiv p \wedge q$
(3.67) $p \wedge (q \Rightarrow p) \equiv p$
(3.68) $p \vee (p \Rightarrow q) \equiv true$
(3.69) $p \vee (q \Rightarrow p) \equiv q \Rightarrow p$
(3.70) $p \vee q \Rightarrow p \wedge q \equiv p \equiv q$
(3.71) reflexivity of $\Rightarrow$: $p \Rightarrow p \equiv true$
(3.72) right zero of $\Rightarrow$: $p \Rightarrow true \equiv true$
(3.73) left identity of $\Rightarrow$: $true \Rightarrow p \equiv p$
(3.74) $p \Rightarrow false \equiv \neg p$
(3.75) $false \Rightarrow p \equiv true$
(3.76) weakening/strengthening:
  (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) $p \wedge q \Rightarrow p \wedge (q \vee r)$
(3.77) Modus ponens: $p \wedge (p \Rightarrow q) \Rightarrow q$
(3.78) $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$
(3.79) $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv r$
(3.80) mutual implication: $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$
(3.81) antisymmetry: $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$
(3.82) transitivity:
  (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) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

Proof techniques

(4.4) deduction:
  To prove $P \Rightarrow Q$, assume P and prove Q.
(4.5) case analysis:
  If E^z_{true}, E^z_{false} are theorems, then so is E^z_P.
(4.6) case analysis:
  $(p \vee q \vee r) \wedge (p \Rightarrow s) \wedge (q \Rightarrow s) \wedge (r \Rightarrow s) \Rightarrow s$
(4.7) mutual implication:
  To prove $P \equiv Q$, prove $P \Rightarrow Q$ and $Q \Rightarrow P$.
(4.9) proof by contradiction:
  To prove P, prove $\neg P \Rightarrow false$.
(4.12) proof by contrapositive:
  To prove $P \Rightarrow Q$, prove $\neg Q \Rightarrow \neg P$.

Quantification

For symmetric & associative binary operator $\star$ with identity u.
*(8.13) empty range: $(\star x \mid false : P) = u$
*(8.14) one-point rule: provided $\neg occurs(`x', `E')$,
  $(\star x \mid x = E : P) = P[x := E]$
*(8.15) distributivity: provided each quantification is defined,
  $(\star x \mid R : P) \star (\star x \mid R : Q) = (\star x \mid R : P \star Q)$
*(8.16) range split: provided $R \wedge S \equiv false$ and each quantification is defined,
  $(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
*(8.17) range split: provided each quantification is defined,
  $(\star x \mid R \vee S : P) \star (\star x \mid R \wedge S : P)$
  $= (\star x \mid R : P) \star (\star x \mid S : P)$
*(8.18) range split for idempotent $\star$: provided each quantification is defined,
  $(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
*(8.19) interchange of dummies: provided each quantification is defined, $\neg occurs(`y', `R')$, and $\neg occurs(`x', `Q')$,
  $(\star x \mid R : (\star y \mid Q : P)) = (\star y \mid Q : (\star x \mid R : P))$
*(8.20) nesting: provided $\neg occurs(`y', `R')$,
  $(\star x, y \mid R \wedge Q : P) = (\star x \mid R : (\star y \mid Q : P))$
*(8.21) dummy renaming: provided $\neg occurs(`y', `R, P')$,
  $(\star x \mid R : P) = (\star y \mid R[x := y] : P[x := y])$
(8.22) change of dummy: provided $\neg occurs(`y', `R, P')$ and f has an inverse,
  $(\star x \mid R : P) = (\star y \mid R[x := f.y] : P[x := f.y])$
(8.23) split off term:
  $(\star i \mid 0 \le i < n+1 : P) = (\star i \mid 0 \le i < n : P) \star P^i_n$
  $(\star i \mid 0 \le i < n+1 : P) = P^i_0 \star (\star i \mid 0 < i < n+1 : P)$

Universal quantification

*(9.2) trading: $(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$
(9.3) trading
  (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) $(\forall x \mid R : P) \equiv (\forall x \mid : R \vee P \equiv P)$
(9.4) trading:
  (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) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \vee P \equiv P)$
*(9.5) distributivity of $\vee$ over $\forall$: provided $\neg occurs(`x', `P')$,
  $P \vee (\forall x \mid R : Q) \equiv (\forall x \mid R : P \vee Q)$
(9.6) provided $\neg occurs(`x', `P')$,
  $(\forall x \mid R : P) \equiv P \vee (\forall x \mid : \neg R)$
(9.7) distributivity of $\wedge$ over $\forall$: provided $\neg occurs(`x', `P')$,
  $\neg(\forall x \mid : \neg R) \Rightarrow ((\forall x \mid R : P \wedge Q) \equiv P \wedge (\forall x \mid R : Q))$
(9.8) $(\forall x \mid R : true) \equiv true$
(9.9) $(\forall x \mid R : P \equiv Q) \Rightarrow ((\forall x \mid R : P) \equiv (\forall x \mid R : Q))$
(9.10) range weakening/strengthening:
  $(\forall x \mid Q \vee R : P) \Rightarrow (\forall x \mid Q : P)$
(9.11) body weakening/strengthening:
  $(\forall x \mid R : P \wedge Q) \Rightarrow (\forall x \mid R : P)$
(9.12) monotonicity of $\forall$:
  $(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P))$
(9.13) instantiation: $(\forall x \mid : P) \Rightarrow P[x := e]$
(9.16) P is a theorem iff $(\forall x \mid : P)$ is a theorem.

Existential quantification

*(9.17) generalized De Morgan: $(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$
(9.18) generalized 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) $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$
(9.19) trading: $(\exists x \mid R : P) \equiv (\exists x \mid : R \wedge P)$
(9.20) trading: $(\exists x \mid Q \wedge R : P) \equiv (\exists x \mid Q : R \wedge P)$
(9.21) distributivity of $\wedge$ over $\exists$: provided $\neg occurs(`x', `P')$,
  $P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$
(9.22) provided $\neg occurs(`x', `P')$,
  $(\exists x \mid R : P) \equiv P \wedge (\exists x \mid : R)$
(9.23) distributivity of $\vee$ over $\exists$: provided $\neg occurs(`x', `P')$,
  $(\exists x \mid : R) \Rightarrow ((\exists x \mid R : P \vee Q) \equiv P \vee (\exists x \mid R : Q))$
(9.24) $(\exists x \mid R : false) \equiv false$
(9.25) range weakening/strengthening:
  $(\exists x \mid R : P) \Rightarrow (\exists x \mid Q \vee R : P)$
(9.26) body weakening/strengthening:
  $(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$
(9.27) monotonicity of $\exists$:
  $(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P))$
(9.28) $\exists$-introduction: $P[x := E] \Rightarrow (\exists x \mid : P)$
(9.29) interchange of quantifications: provided $\neg occurs(`y', `R')$, and $\neg occurs(`x', `Q')$,
  $(\exists x \mid R : (\forall y \mid Q : P)) \Rightarrow (\forall y \mid Q : (\exists x \mid R : P))$
(9.30) provided $\neg occurs(`\hat{x}', `Q')$,
  $(\exists x \mid R : P) \Rightarrow Q$ is a theorem iff $(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem

Sets

*(11.3) set membership: $F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$
*(11.4) extensionality: $S = T \equiv (\forall x \mid : x \in S \equiv x \in T)$
(11.5): $S = \{x \mid x \in S : x\}$
(11.6): $\{x \mid R : E\} = \{y \mid (\exists x \mid R : y = E) : y\}$
(11.7): $x \in \{x \mid R\} \equiv R$
(11.9): $\{x \mid Q\} = \{x \mid R\} \equiv (\forall x \mid : Q \equiv R)$
*(11.12) size: $\#S = (+x \mid x \in S : 1)$

*(11.13) subset: $S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$
*(11.14) proper subset: $S \subset T \equiv S \subseteq T \wedge S \neq T$
*(11.17) complement: $v \in \sim S \equiv v \in \mathbf{U} \wedge v \notin S$
*(11.20) union: $v \in S \cup T \equiv v \in S \vee v \in T$
*(11.21) intersection: $v \in S \cap T \equiv v \in S \wedge v \in T$
*(11.22) difference: $v \in S - T \equiv v \in S \wedge v \notin T$
*(11.23) power set: $v \in \mathcal{P}S \equiv v \subseteq S$
(11.24) all propositional and predicate logic axioms and theorems E_p can be transferred to sets E_s where you interchange $\emptyset$ with $false$, $\mathbf{U}$ with $true$, $\cup$ with $\vee$, $\cap$ with $\wedge$, and $\sim$ with $\neg$.
(11.25) metatheorem: for any set expressions E_s and F_s:
(a) $E_s = F_s$ is valid iff $E_p \equiv F_p$ is valid.
(b) $E_s \subseteq F_s$ is valid iff $E_p \Rightarrow F_p$ is valid.
(c) $E_s = \mathbf{U}$ is valid iff E_p is valid.
(11.43) $S \subseteq T \wedge U \subseteq V \Rightarrow (S \cup U) \subseteq (T \cup V)$
(11.44) $S \subseteq T \wedge U \subseteq V \Rightarrow (S \cap U) \subseteq (T \cap V)$
(11.49) $S - T = S \cap \sim T$
(11.50) $S - T \subseteq S$
(11.51) $S - \emptyset = S$
(11.52) $S \cap (T - S) = \emptyset$
(11.53) $S \cup (T - S) = S \cup T$
(11.54) $S - (T \cup U) = (S - T) \cap (S - U)$
(11.55) $S - (T \cap U) = (S - T) \cup (S - U)$
(11.56) $(\forall x \mid: P \Rightarrow Q) \equiv \{x \mid P\} \subseteq \{x \mid Q\}$
(11.57) antisymmetry: $S \subseteq T \wedge T \subseteq S \equiv S = T$
(11.58) reflexivity: $S \subseteq S$
(11.59) transitivity: $S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$
(11.60) $\emptyset \subseteq S$
(11.61) $S \subset T \equiv S \subseteq T \wedge \neg(T \subseteq S)$

Tuples and Cross Products

(14.1) ordered pair: $\langle b, c\rangle = \{\{b\}, \{b, c\}\}$
*(14.2) pair equality: $\langle b, c\rangle = \langle b', c'\rangle \equiv b = b' \wedge c = c'$
(14.4) membership: $\langle x, y\rangle \in S \times T \equiv x \in S \wedge y \in T$
(14.5) $\langle x, y\rangle \in S \times T \equiv \langle y, x\rangle \in T \times S$
(14.6) $S = \emptyset \Rightarrow S \times T = T \times S = \emptyset$
(14.7) $S \times T = T \times S \equiv S = \emptyset \vee T = \emptyset \vee S = T$
(14.8) distributivity of $\times$ over $\cup$:
$S \times (T \cup U) = (S \times T) \cup (S \times U)$
$(S \cup T) \times U = (S \times U) \cup (T \times U)$
(14.9) distributivity of $\times$ over $\cap$:
$S \times (T \cap U) = (S \times T) \cap (S \times U)$
$(S \cap T) \times U = (S \times U) \cap (T \times U)$
(14.10) distributivity of $\times$ over $-$: $S \times (T - U) = (S \times T) - (S \times U)$
(14.11) monotonicity: $T \subseteq U \Rightarrow S \times T \subseteq S \times U$
(14.12) $S \subseteq U \wedge T \subseteq V \Rightarrow S \times T \subseteq U \times V$
(14.13) $S \times T \subseteq S \times U \wedge S \neq \emptyset \Rightarrow T \subseteq U$
(14.14) $(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$
(14.15) for finite S and T, $\#(S \times T) = \#S \cdot \#T$

Relations

(14.16) domain: $Dom.\rho = \{b : B \mid (\exists c : b\rho c)\}$
(14.17) range: $Ran.\rho = \{c : C \mid (\exists b : b\rho c)\}$
(14.20) composition: if $\rho : B \times C$ and $\sigma : C \times D$,
$\langle b, d\rangle \in \rho \circ \sigma \equiv (\exists c \mid c \in C : \langle b, c\rangle \in \rho \wedge \langle c, d\rangle \in \sigma)$
(14.22) associativity of $\circ$: $\rho \circ (\sigma \circ \theta) = (\rho \circ \sigma) \circ \theta$
(14.23) distributivity of $\circ$ over $\cup$:
$\rho \circ (\sigma \cup \theta) = \rho \circ \sigma \cup \rho \circ \theta$
$(\sigma \cup \theta) \circ \rho = \sigma \circ \rho \cup \theta \circ \rho$
(14.24) distributivity of $\circ$ over $\cap$:
$\rho \circ (\sigma \cap \theta) \subseteq \rho \circ \sigma \cap \rho \circ \theta$
$(\sigma \cap \theta) \circ \rho \subseteq \sigma \circ \rho \cap \theta \circ \rho$
(14.26) $\rho^m \circ \rho^n = \rho^{m+n}$, $m \geq 0, n \geq 0$
(14.27) $(\rho^m)^n = \rho^{m \cdot n}$, $m \geq 0, n \geq 0$

Group theory

(18.18): $b = (b^{-1})^{-1}$
(18.19) cancellation: $b \circ d = c \circ d = b = c$, $d \circ b = d \circ c = b = c$
(18.20) unique solution:
$b \circ x = c \equiv x = b^{-1} \circ c$
$x \circ b = c \equiv x = c \circ b^{-1}$
(18.21) one-to-one: $b \neq c \equiv d \circ b \neq d \circ c$, $b \neq c \equiv b \circ d \neq c \circ d$
(18.22) onto: $(\exists x \mid: b \circ x = c)$, $(\exists x \mid: x \circ b = c)$
$\langle S, \oplus, \otimes, \sim, 0, 1\rangle$ where $\oplus$ and $\otimes$ are associative, symmetric, binary operators; 0 and 1 are the identities of $\oplus$ and $\otimes$;
unary operator $\sim$ satisfies $b \oplus (\sim b) = 1$ and $b \otimes (\sim b) = 0$ for all b ($\sim b$ is the complement of b);
$\otimes$ distributes over $\oplus$: $b \otimes (c \oplus d) = (b \otimes c) \oplus (b \otimes d)$;
and $\oplus$ distributes over $\otimes$: $b \oplus (c \otimes d) = (b \oplus c) \otimes (b \oplus d)$.
(18.49) idempotency: $b \oplus b = b$, $b \otimes b = b$
(18.50) zero: $b \oplus 1 = 1$, $b \otimes 0 = 0$
(18.51) absorption: $b \oplus (b \otimes c) = b$, $b \otimes (b \oplus c) = b$
(18.52) cancellation:
$(b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \equiv c = d$
$(b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \equiv c = d$
(18.53) unique complement: $b \oplus c = 1 \wedge b \otimes c = 0 \equiv c = \sim b$
(18.54) double complement: $\sim(\sim b) = b$
(18.55) constant complement: $\sim 0 = 1$, $\sim 1 = 0$
(18.56) De Morgan:
$\sim(b \oplus c) = (\sim b) \otimes (\sim c)$
$\sim(b \otimes c) = (\sim b) \oplus (\sim c)$
(18.57): $b \oplus (\sim c) = 1 \equiv b \oplus c = b$, $b \otimes (\sim c) = 0 \equiv b \otimes c = b$
*(18.59): $b \leq c \equiv b \otimes c = b$
*(18.60): $b < c \equiv b \leq c \wedge b \neq c$
(18.61): $\leq$ is a partial order

Definitions

To prove $\{Q\}$ **if** B **then** $S1$ **else** $S2$ $\{R\}$, prove $\{Q \wedge B\}$ $S1$ $\{R\}$ and $\{Q \wedge \neg B\}$ $S2$ $\{R\}$.
To show $x := E$ is an implementation of $\{Q\}$ $x :=?$ $\{R\}$, prove $Q \Rightarrow R[x := E]$.
To prove a loop $\{Q\}$ *initialization*; $\{P\}$ **do** $B \rightarrow S$ **od** $\{R\}$ is correct, prove P is $true$ before execution of the loop, P is a loop invariant ($\{P \wedge B\}$ S $\{P\}$), execution of the loop terminates, and R holds upon termination ($P \wedge \neg B \Rightarrow R$).
Dual: interchange $true$ with $false$, $\wedge$ with $\vee$, $\equiv$ with $\not\equiv$, $\Rightarrow$ with $\not\Leftarrow$, and $\Leftarrow$ with $\not\Rightarrow$.
Metatheorem duality: P is valid iff $\neg P_D$ is valid. $P \equiv Q$ is valid iff $P_D \equiv Q_D$ is valid.
Valid Hoare triple: $\{R[x := E]\}$ $x := E$ $\{R\}$.
Satisfiable: a state exists in which it's satisfied; at least one interpretation of a logic maps a formula to true.
Satisfied: true for a given state.
Valid: satisfied for all states; every interpretation of a logic maps a formula to true.
Formal logic: a set of symbols, a set of formulas constructed from the symbols, a set of distinguished formulas called axioms, and a set of inference rules.
Consistent: at least one of its formulas is a theorem and at least one isn't; otherwise, inconsistent.
Sound: both valid in form and its premises are true; every theorem is valid.
Complete: every valid formula is a theorem.
Model: every theorem is mapped to true by the interpretation.
Sequent: $A_0, \ldots, A_n \vdash Q$ means "Q is provable from $A_0, \ldots, A_n$".
Witness: for $(\exists x \mid R : P)$ if $(R \wedge P)[x := \hat{x}]$ is valid, then $\hat{x}$ is a witness for x.
Minimal element: if y is a minimal element and $y \in S$: $(\forall x \mid x \prec y : x \notin S)$.
Well founded: every nonempty subset of U has a minimal element. $\langle U, \prec\rangle$ is well founded iff it admits induction.
Noetherian of $\langle U, \prec\rangle$: every decreasing chain beginning with any $x \in U$ is finite.
Function: a relation $f : B \times C$ where it's determinate: $(\forall b, c, c' \mid bfc \wedge bfc' : c = c')$.
Total: a function $f : B \times C$ where $B = Dom.f$; otherwise, partial.
Black composition: $f \bullet g = g \circ f$.
Algebra: a pair of a set of elements, called the *carrier* of the algebra, and a set of operators defined on the carrier. Each operator is a total function of type $S^m \rightarrow S$ for some m where m is the *arity* of the operator. The algebra is *finite* if the carrier is finite, otherwise, infinite.
Subalgebra: $\langle T, \circ\rangle$ is a subalgebra of $\langle S, \circ\rangle$ if T is a nonempty subset of S and T is closed under every operator in $\circ$. **Closed**: a subset T of a set S is closed under an operator if applying the operator to elements in T always produces an element in T.
Signature: the name of an algebra's carrier and the list of types of its operators. Same signature if same number of operators and corresponding operators have the same types.
One-to-one: for $f : B \rightarrow C$, $(\forall b, c \mid b, c \in B : f(b) = f(c) \Rightarrow b = c)$.
Onto: for $f : B \rightarrow C$, $(\forall c \mid c \in C : (\exists b \mid b \in B : f(b) = c))$.
Isomorphism: for two algebras, a function $h : S \rightarrow \hat{S}$ where h is one-to-one and onto, $h(c) = \hat{c}$, $h(\sim b) = \hat{\sim} h(b)$, and $h(b \circ c) = h(b) \hat{\circ} h(c)$.
Homomorphism: an isomorphism that doesn't need to be one-to-one or onto.
Automorphism: an isomorphism from A to A.
Semigroup: $\langle S, \circ\rangle$ where $\circ$ is a binary associative operator.
Monoid: $\langle S, \circ, 1\rangle$, a semigroup with an identity 1.
Abelian: a monoid where $\circ$ is also symmetric.
Submonoid: a subalgebra of a monoid that contains the identity of the monoid.
Group: a monoid where every element $b \in S$ has an inverse b^{-1}.
Equivalence relation: a relation that's reflexive, symmetric, and transitive.
Equivalence class: a subset of elements that are equivalent under an equivalence relation: $[b]_R, b \in B$, then $x \in [b]_R \equiv xRb$.
Partial order: a binary relation that's reflexive, antisymmetric, and transitive.
Quasi/sharp/strict order: a binary relation that's irreflexive and transitive.
Total/linear order: a partial order $\preceq$ over B where $(\forall b, c \mid: b \preceq c \vee c \preceq b)$ or $\preceq \cup \preceq^{-1} = B \times B$.
Incomparability: $b \frown_{\preceq} c \equiv b \not\preceq c \wedge c \not\preceq b$.
Stratified/weak: $\frown_{\preceq}$ is an equivalence relation.
Least element: $b \in S \wedge (\forall c \mid c \in S : b \preceq c)$.
Lower bound: $(\forall c \mid c \in S : b \preceq c)$.
Greatest lower bound: b is a lower bound and every lower bound c satisfies $c \preceq b$.
Greatest element: $b \in S \wedge (\forall c \mid c \in S : c \preceq b)$.
Upper bound: $(\forall c \mid c \in S : c \preceq b)$.
Lowest upper bound: b is an upper bound and every upper bound c satisfies $b \preceq c$.
Monotone: a function $f : X \rightarrow Y$ where $x \preceq y \equiv f(x) \preceq f(y)$.
Fixed point: can solve for $x = F(x)$ when the domain of x is a complete lattice and the function $F(x)$ is monotone.
Interval: a partial order $(X, \prec)$ where for all $a, b, c, d \in X$, $a \prec c$ and $b \prec d$ implies $a \prec d$ or $b \prec c$. Or there exists a total order $(Y, \lhd)$ and two mappings $f, g : X \rightarrow Y$ such that for all $a, b \in X$: $f(a) \lhd g(a)$ and $a \prec b \equiv g(a) \prec f(b)$.
If $R \subseteq B \times B$:
Reflexive closure $r(R)$: $R \cup \imath_B$
Symmetric closure $s(R)$: $R \cup R^{-1}$
Transitive closure R^+: $(\cup i \mid 0 < i : R^i) = \bigcup_{i=1}^{\infty} R^i$ or $bR^+c \equiv (\exists i \mid 0 < i : bR^ic)$
Reflexive transitive closure R^*
$R^+ \cup \imath_B = (\cup i \mid 0 \leq i : R^i) = \bigcup_{i=0}^{\infty} R^i$ or $bR^*c \equiv (\exists i \mid 0 \leq i : bR^ic)$ where $R^0 = \imath_B$
Reflexive: $(\forall b \mid: bRb)$ or $\imath_B \subseteq R$
Irreflexive: $(\forall b \mid: \neg(bRb))$ or $\imath_B \cap R = \emptyset$
Symmetric: $(\forall b, c \mid: bRc \equiv cRb)$ or $R^{-1} = R$
Antisymmetric: $(\forall b, c \mid: bRc \wedge cRb \Rightarrow b = c)$ or $R \cap R^{-1} \subseteq \imath_B$
Asymmetric: $(\forall b, c \mid: bRc \Rightarrow \neg(cRb))$ or $R \cap R^{-1} = \emptyset$
Transitive: $(\forall b, c, d \mid: bRc \wedge cRd \Rightarrow bRd)$ or $R = (\cup i \mid i > 0 : \rho^i)$
`S1;S2` $= R_1 \circ R_2$
`if T then S1 else S2` $= (I_T \circ R_1) \cup (\overline{I_T} \circ R_2)$
`while T do S` $= (I_T \circ R)^* \circ \overline{I_T}$