McMaster University — COMPSCI&SFWRENG 2DM3
Dept. of Computing and Software — Theorem List 4
Dr. W. Kahl — 2017-12-09

The names listed here are precisely the names used in the preloaded material you are already familiar with. In the final exam, each question will specify which theorems are available. **If a theorem name is not found by theorem name completion, then that theorem is not available.**

Basic Propositional Logic

Equivalence

“Definition of $\equiv$”: $(p \equiv q) = (p = q)$
(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 $\equiv$”: $\mathsf{true} \equiv q \equiv q$
(3.4): true
(3.5) “Reflexivity of $\equiv$”: $p \equiv p$

Negation and Inequivalence

(3.8) “Definition of ‘false’”: $\mathsf{false} \equiv \neg\, \mathsf{true}$
(3.9) “Distributivity of $\neg$ over $\equiv$” “Mutual associativity of $\neg$ with $\equiv$”: $\neg\,(p \equiv q) \equiv (\neg\, p \equiv q)$
(3.10) “Definition of $\not\equiv$”: $(p \not\equiv q) \equiv \neg\,(p \equiv q)$
(3.11) “$\neg$ connection”: $\neg\, p \equiv q \equiv p \equiv \neg\, q$
(3.12) “Double negation”: $\neg\,(\neg\, p) \equiv p$
(3.13) “Negation of ‘false’”: $\neg\, \mathsf{false} \equiv \mathsf{true}$
(3.14): $(p \not\equiv q) \equiv (\neg\, p \equiv q)$
(3.15): $\neg\, p \equiv p \equiv \mathsf{false}$
“Identity of $\not\equiv$”: $(p \not\equiv \mathsf{false}) \equiv p$
(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 of $\equiv$ with $\not\equiv$”: $((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$
(3.19) “Mutual interchangeability of $\equiv$ with $\not\equiv$”: $(p \not\equiv (q \equiv r)) \equiv (p \equiv (q \not\equiv r))$

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” “LEM”: $p \vee \neg\, p$
(3.29) “Zero of $\vee$”: $p \vee \mathsf{true} \equiv \mathsf{true}$
(3.30) “Identity of $\vee$”: $p \vee \mathsf{false} \equiv p$
(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 $\wedge$”: $p \wedge \mathsf{true} \equiv p$
(3.40) “Zero of $\wedge$”: $p \wedge \mathsf{false} \equiv \mathsf{false}$
(3.41) “Distributivity of $\wedge$ over $\wedge$”: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$
(3.42) “Contradiction”: $p \wedge \neg\, p \equiv \mathsf{false}$
(3.43) (3.43a) “Absorption”: $p \wedge (p \vee q) \equiv p$
(3.43) (3.43b) “Absorption”: $p \vee (p \wedge q) \equiv p$
(3.44) (3.44a) “Absorption”: $p \wedge (\neg\, p \vee q) \equiv p \wedge q$
(3.44) (3.44b) “Absorption”: $p \vee (\neg\, p \wedge q) \equiv p \vee q$
(3.44) (3.44c) “Absorption”: $\neg\, p \wedge (p \vee q) \equiv \neg\, p \wedge q$
(3.44) (3.44d) “Absorption”: $\neg\, p \vee (p \wedge q) \equiv \neg\, p \vee q$
(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) (3.47a) “De Morgan”: $\neg\,(p \wedge q) \equiv \neg\, p \vee \neg\, q$
(3.47) (3.47b) “De Morgan”: $\neg\,(p \vee q) \equiv \neg\, p \wedge \neg\, q$
(3.48): $p \wedge q \equiv p \wedge \neg\, q \equiv \neg\, p$
(3.49) “Semi-distributivity of $\wedge$ over $\equiv$”: $p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$
(3.50) “Strong Modus Ponens”: $p \wedge (q \equiv p) \equiv p \wedge q$
(3.51) “Replacement”: $(p \equiv q) \wedge (r \equiv p) \quad \equiv \quad (p \equiv q) \wedge (r \equiv q)$
(3.52) “Alternative definition of $\equiv$”: $p \equiv q \equiv (p \wedge q) \vee (\neg\, p \wedge \neg\, q)$
(3.53) “Exclusive or” “Alternative definition of $\not\equiv$”: $(p \not\equiv q) \equiv (\neg\, p \wedge q) \vee (p \wedge \neg\, q)$

Implication

(3.57) “Definition of $\Rightarrow$” “Definition of Implication”: $p \Rightarrow q \equiv (p \vee q \equiv q)$
(3.58) “Definition of $\Leftarrow$” “Consequence”: $p \Leftarrow q \equiv q \Rightarrow p$
(3.59) “Definition of $\Rightarrow$” “Definition of Implication”: $p \Rightarrow q \equiv \neg\, p \vee q$
(3.60) “Definition of $\Rightarrow$” “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): $p \vee (p \Rightarrow q) \equiv \mathsf{true}$
(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 $\Rightarrow$”: $p \Rightarrow p$
(3.72) “Right-zero of $\Rightarrow$”: $p \Rightarrow \mathsf{true}$
(3.73) “Left-identity of $\Rightarrow$”: $\mathsf{true} \Rightarrow p \quad \equiv \quad p$
(3.74): $p \Rightarrow \mathsf{false} \quad \equiv \quad \neg\, p$
(3.75) “ex falso quodlibet”: $\mathsf{false} \Rightarrow p$
(3.76) (3.76a) “Weakening” “Strengthening”: $p \Rightarrow p \vee q$
(3.76) (3.76a) “Weakening” “Strengthening”: $p \Rightarrow p \vee q$
(3.76) (3.76b) “Weakening” “Strengthening”: $p \wedge q \Rightarrow p$
(3.76) (3.76c) “Weakening” “Strengthening”: $p \wedge q \Rightarrow p \vee q$
(3.76) (3.76d) “Weakening” “Strengthening”: $p \vee (q \wedge r) \Rightarrow p \vee q$
(3.76) (3.76e) “Weakening” “Strengthening”: $p \wedge q \Rightarrow p \wedge (q \vee r)$
(3.77) “Modus ponens”: $p \wedge (p \Rightarrow q) \Rightarrow q$
(3.78) “Case analysis”: $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv p \vee q \Rightarrow r$
(3.79) “Case analysis”: $(p \Rightarrow r) \wedge (\neg\, p \Rightarrow r) \equiv r$
(3.80) “Mutual implication”: $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$
(3.81) “Antisymmetry of $\Rightarrow$”: $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$
(3.82) (3.82a) “Transitivity of $\Rightarrow$”: $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(3.82) (3.82b) “Transitivity of $\Rightarrow$”: $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(3.82) (3.82c) “Transitivity of $\Rightarrow$”: $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

Inductive Theory of the Natural Numbers

“Definition of $+$” “Left-identity of $+$” “Definition of $+$ for 0”: $0 + n = n$
“Definition of $+$” “Definition of $+$ for ‘S’”: $S\, m + n = S\,(m + n)$
“Right-identity of $+$”: $m + 0 = m$
“Adding the successor”: $m + S\, n = S\,(m + n)$
“Symmetry of $+$”: $m + n = n + m$
“Associativity of $+$”: $(a + b) + c = a + (b + c)$
“Identity of $+$”: $0 + a = a$
“Definition of 1”: $1 = S\, 0$
“Successor”: $S\, n = n + 1$
“Definition of $\cdot$” “Left-zero of $\cdot$”: $0 \cdot n = 0$
“Definition of $\cdot$”: $S\, m \cdot n = n + m \cdot n$
“Left-identity of $\cdot$”: $1 \cdot n = n$
“Right-zero of $\cdot$”: $m \cdot 0 = 0$
“Multiplying the successor”: $m \cdot S\, n = m \cdot n + m$
“Symmetry of $\cdot$”: $m \cdot n = n \cdot m$
“Zero of $\cdot$”: $m \cdot 0 = 0$
“Identity of $\cdot$”: $1 \cdot m = m$
“Distributivity of $\cdot$ over $+$”: $k \cdot (m + n) = k \cdot m + k \cdot n$
“Associativity of $\cdot$”: $(k \cdot m) \cdot n = k \cdot (m \cdot n)$
“Subtraction from zero”: $0 - n = 0$
“Subtraction of zero from successor”: $S\, m - 0 = S\, m$

“Subtraction of successor from successor”: $\mathrm{S}\ m - \mathrm{S}\ n = m - n$
“Right-identity of subtraction”: $m - 0 = m$
“Self-cancellation of subtraction”: $m - m = 0$
“Subtraction after addition”: $(m + n) - n = m$
“Subtraction from multiplication with successor”: $m \cdot \mathrm{S}\ n - m = m \cdot n$
“Subtraction of sum”: $k - (m + n) = (k - m) - n$
“Distributivity of · over subtraction”: $k \cdot (m - n) = k \cdot m - k \cdot n$
“Monus exchange”: $m + (n - m) = n + (m - n)$

Order in the Ind. Th. of the <u>Natural Numbers</u>

“Cancellation of ‘S’”: $\mathrm{S}\ m = \mathrm{S}\ n \equiv m = n$
“Zero is not suc”: $0 = \mathrm{S}\ n \equiv \mathrm{false}$
“Cancellation of +”: $k + m = k + n \equiv m = n$
“Predecessor of zero”: $\mathrm{pred}\ 0 = 0$
“Predecessor of successor”: $\mathrm{pred}\ (\mathrm{S}\ n) = n$
“Zero is least element”: $0 \le a$
“Isotony of successor”: $\mathrm{S}\ a \le \mathrm{S}\ b \equiv a \le b$
“Successor is not at most zero”: $\mathrm{S}\ a \le 0 \equiv \mathrm{false}$
“Zero is unique least element”: $a \le 0 \equiv a = 0$
“Reflexivity of ≤”: $a \le a$
“Antisymmetry of ≤”: $a \le b \Rightarrow b \le a \Rightarrow a = b$
“Transitivity of ≤”: $a \le b \Rightarrow b \le c \Rightarrow a \le c$
“Isotony of +”: $a + b \le a + c \equiv b \le c$
“Monotony of +”: $a \le b \Rightarrow c \le d \Rightarrow a + c \le b + d$
“Monotony of predecessor”: $a \le b \Rightarrow \mathrm{pred}\ a \le \mathrm{pred}\ b$
“Monotony of -”: $a \le b \Rightarrow a - c \le b - c$
“Monotony of ·”: $b \le c \Rightarrow a \cdot b \le a \cdot c$
“Successor is non-decreasing”: $a \le \mathrm{S}\ a$
“Subtraction is non-increasing”: $a - b \le a$
“Antitony of -”: $b \le c \Rightarrow a - c \le a - b$
“Zero is less than successor”: $0 < \mathrm{S}\ a$
“Isotony of successor”: $\mathrm{S}\ a < \mathrm{S}\ b \equiv a < b$
“Nothing is less than zero”: $a < 0 \equiv \mathrm{false}$
“Irreflexivity of <”: $a < a \equiv \mathrm{false}$
“Zero is <-least element”: $0 < a \lor 0 = a$
“Less than successor”: $a < \mathrm{S}\ b \equiv a < b \lor a = b$
“Less than successor”: $a < \mathrm{S}\ a$
“Only zero is less than one”: $a < 1 \equiv a = 0$
“Definition of ≤ in terms of ‘S‘ and <”: $a \le b \equiv a < \mathrm{S}\ b$
“Definition of ≤ in terms of <”: $a \le b \equiv a < b \lor a = b$
“Split range at top”: $m \le n \Rightarrow (m \le i < \mathrm{S}\ n \equiv m \le i < n \lor i = n)$

Basic Theory of <u>Integers</u>

(15.1) (15.1a) “Associativity of +”: $(a + b) + c = a + (b + c)$
(15.1) (15.1b) “Associativity of ·”: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(15.2) (15.2a) “Symmetry of +”: $a + b = b + a$
(15.2) (15.2b) “Symmetry of ·”: $a \cdot b = b \cdot a$
(15.3) “Additive identity” “Identity of +”: $0 + a = a$
(15.4) “Multiplicative identity” “Identity of ·”: $1 \cdot a = a$
(15.5) “Distributivity” “Distributivity of · over +”: $a \cdot (b + c) = a \cdot b + a \cdot c$
(15.7) “Cancellation of ·”: $c \neq 0 \Rightarrow (c \cdot a = c \cdot b \equiv a = b)$
(15.8) “Cancellation of +”: $a + b = a + c \equiv b = c$
“Non-zero multiplication”: $a \neq 0 \Rightarrow b \neq 0 \Rightarrow a \cdot b \neq 0$
(15.9) “Zero of ·”: $a \cdot 0 = 0$
(15.13) “Unary minus”: $a + -a = 0$
(15.14) “Subtraction”: $a - b = a + -b$
(15.17) “Self-inverse of unary minus”: $-(-a) = a$
(15.18) “Fixpoint of unary minus”: $-0 = 0$
(15.20): $-a = -1 \cdot a$
(15.19) “Distributivity of unary minus over +”: $-(a + b) = -a + -b$
(15.21): $-a \cdot b = a \cdot -b$
(15.22): $a \cdot -b = -(a \cdot b)$
(15.23): $-a \cdot -b = a \cdot b$
(15.24) “Right-identity of –”: $a - 0 = a$
(15.25): $(a - b) + (c - d) = (a + c) - (b + d)$
“Mutual associativity of + and –”: $a + (b - c) = (a + b) - c$
“Subtraction of addition”: $a - (b + c) = (a - b) - c$
(15.25c): $(a - b) + (b - c) = a - c$
(15.26): $(a - b) - (c - d) = (a + d) - (b + c)$
(15.27): $(a - b) \cdot (c - d) = (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c)$
(15.29) “Distributivity of · over –”: $(a - b) \cdot c = a \cdot c - b \cdot c$

Positivity of <u>Integers</u>

(15.30) “Positivity under +”: $\mathrm{pos}\ a \land \mathrm{pos}\ b \Rightarrow \mathrm{pos}\ (a + b)$
(15.30a) “Positivity under +”: $\mathrm{pos}\ a \Rightarrow (\mathrm{pos}\ b \Rightarrow \mathrm{pos}\ (a + b))$
(15.31) “Positivity under ·”: $\mathrm{pos}\ a \land \mathrm{pos}\ b \Rightarrow \mathrm{pos}\ (a \cdot b)$
(15.31a) “Positivity under ·”: $\mathrm{pos}\ a \Rightarrow (\mathrm{pos}\ b \Rightarrow \mathrm{pos}\ (a \cdot b))$
(15.32) “Non-positivity of 0”: $\neg\ \mathrm{pos}\ 0$
(15.33) “Positivity under unary minus”: $b \neq 0 \Rightarrow (\mathrm{pos}\ b \equiv \neg\ \mathrm{pos}\ (-b))$
(15.33a) “Positivity under unary minus”: $b \neq 0 \Rightarrow (\mathrm{pos}\ b \not\equiv \mathrm{pos}\ (-b))$
(15.33b) “Positivity under unary minus”: $b \neq 0 \Rightarrow (\mathrm{pos}\ (-b) \equiv \neg\ \mathrm{pos}\ b)$
(15.33c) “Positivity under unary minus”: $(\mathrm{pos}\ (-b) \equiv \mathrm{pos}\ b) \Rightarrow b = 0$
“Positive implies non-zero”: $\mathrm{pos}\ a \Rightarrow a \neq 0$
(15.34) “Positivity of squares”: $b \neq 0 \Rightarrow \mathrm{pos}\ (b \cdot b)$
“Positivity of 1”: $\mathrm{pos}\ 1$
“Positivity”: $\mathrm{pos}\ a \equiv a \neq 0 \land \neg\ \mathrm{pos}\ (-a)$
(15.35) “Positivity under ·”: $\mathrm{pos}\ a \Rightarrow (\mathrm{pos}\ b \equiv \mathrm{pos}\ (a \cdot b))$

Order on <u>Integers</u>

(15.36) “Less” “Definition of <”: $a < b \equiv \mathrm{pos}\ (b - a)$
(15.37) “Greater” “Definition of >”: $a > b \equiv \mathrm{pos}\ (a - b)$
(15.38) “At most” “Definition of ≤”: $a \le b \equiv a < b \lor a = b$
(15.39) “At least” “Definition of ≥”: $a \ge b \equiv a > b \lor a = b$
“Irreflexivity of <”: $\neg\ (a < a)$
“Irreflexivity of <”: $a = b \Rightarrow \neg\ (a < b)$
“Irreflexivity of <”: $a < b \Rightarrow \neg\ (a = b)$
“Irreflexivity of <”: $\neg\ (a < b \land a = b)$
“Converse of <”: $a > b \equiv b < a$
“Converse of ≤”: $a \ge b \equiv b \le a$
“Irreflexivity of >”: $\neg\ (a > a)$
“Irreflexivity of >”: $a = b \Rightarrow \neg\ (a > b)$
“Irreflexivity of >”: $a > b \Rightarrow \neg\ (a = b)$
“Irreflexivity of >”: $\neg\ (a > b \land a = b)$
(15.40) “Positive elements”: $\mathrm{pos}\ b \equiv 0 < b$
(15.41) (15.41a) “Transitivity” “Transitivity of <”: $a < b \land b < c \Rightarrow a < c$
(15.41) (15.41b) “Transitivity” “Transitivity of ≤ with <”: $a \le b \land b < c \Rightarrow a < c$
(15.41) (15.41c) “Transitivity” “Transitivity of < with ≤”: $a < b \land b \le c \Rightarrow a < c$
(15.41) (15.41d) “Transitivity” “Transitivity of ≤”: $a \le b \land b \le c \Rightarrow a \le c$
“Transitivity of ≤”: $a \le b \Rightarrow (b \le c \Rightarrow a \le c)$
(15.42) “Monotonicity of +” “Isotonicity of +” “<-Isotony of +”: $a < b \equiv a + d < b + d$
“Monotonicity of +” “<-Monotony of +”: $a < b \Rightarrow a + d < b + d$
“<-Monotonicity of +” “<-Monotony of +”: $a < b \Rightarrow (c < d \Rightarrow a + c < b + d)$
“<-Monotonicity of +” “<-Monotony of +”: $a < b \land c < d \Rightarrow a + c < b + d$
“Monotonicity of +” “Isotonicity of +” “≤-Isotony of +”: $a \le b \equiv a + d \le b + d$
(15.42) “Monotonicity of ·”: $0 < d \Rightarrow (a < b \equiv a \cdot d < b \cdot d)$
(15.42) “Monotonicity of ·” “<-Monotony of ·”: $0 < d \Rightarrow (a < b \equiv a \cdot d < b \cdot d)$
“Monotonicity of ·” “≤-Monotony of ·”: $0 < d \Rightarrow (a \le b \equiv a \cdot d \le b \cdot d)$
“Asymmetry of <”: $\neg\ (a < b \land b < a)$
(15.44A) “Trichotomy — A”: $a < b \equiv (a = b \equiv a > b)$
(15.44B) “Trichotomy — B”: $\neg\ (a < b \land (a = b \land a > b))$
(15.44) “Trichotomy”: $(a < b \equiv (a = b \equiv a > b)) \land \neg\ (a < b \land (a = b \land a > b))$
“Complement of <”: $a < b \not\equiv a \ge b$
“Complement of >”: $a > b \not\equiv a \le b$
“Trichotomy” “Trichotomy — ∨”: $a < b \lor (a = b \lor a > b)$
(15.45) “Antisymmetry of ≤”: $a \le b \land b \le a \equiv a = b$
(15.46) “Reflexivity of ≤”: $a \le a$

Integrality

“Least positive”: $\mathrm{pos}\ a \equiv 1 \le a$
“Least greater element”: $a < b \equiv a + 1 \le b$
“At least successor”: $a > b \equiv a \ge b + 1$
“Less than successor”: $a < b + 1 \equiv a \le b$
“Successor greater”: $a + 1 > b \equiv a \ge b$
“Split-off top”: $m \le n \Rightarrow (m \le i < n + 1 \equiv m \le i < n \lor i = n)$
“Split-off bottom”: $m \le n \Rightarrow (m \le i < n + 1 \equiv m + 1 \le i < n + 1 \lor i = m)$

Abstract Relation Algebra

Starting from Inclusion, Composition, and Converse

“Reflexivity of ⊆”: $R \subseteq R$
“Reflexivity of ⊆”: $R = S \Rightarrow R \subseteq S$
“Transitivity of ⊆”: $Q \subseteq R \Rightarrow R \subseteq S \Rightarrow Q \subseteq S$
“Antisymmetry of ⊆”: $R \subseteq S \Rightarrow S \subseteq R \Rightarrow R = S$
“Mutual inclusion”: $R = S \equiv R \subseteq S \land S \subseteq R$
“Associativity of ⨾”: $(Q \mathbin{;} R) \mathbin{;} S = Q \mathbin{;} (R \mathbin{;} S)$
“Monotonicity of ⨾”: $P \subseteq Q \Rightarrow R \subseteq S \Rightarrow P \mathbin{;} R \subseteq Q \mathbin{;} S$
“Monotonicity of ⨾”: $Q \subseteq R \Rightarrow Q \mathbin{;} S \subseteq R \mathbin{;} S$
“Monotonicity of ⨾”: $R \subseteq S \Rightarrow Q \mathbin{;} R \subseteq Q \mathbin{;} S$
“Identity of ⨾”: $\mathrm{Id} \mathbin{;} R = R$
“Identity of ⨾”: $R \mathbin{;} \mathrm{Id} = R$
“Self-inverse of ˘”: $(R^{\smile})^{\smile} = R$
“Injectivity of converse”: $R^{\smile} = S^{\smile} \equiv R = S$
“Monotonicity of ˘”: $R \subseteq S \Rightarrow R^{\smile} \subseteq S^{\smile}$
“Isotonicity of ˘”: $R \subseteq S \equiv R^{\smile} \subseteq S^{\smile}$
“Converse of ‘Id’”: $\mathrm{Id}^{\smile} = \mathrm{Id}$
“Converse of ⨾”: $(R \mathbin{;} S)^{\smile} = S^{\smile} \mathbin{;} R^{\smile}$
“Indirect Relation Equality” “Indirect Relation Equality from above”: $Q = R \equiv (\forall\, S \bullet Q \subseteq S \equiv R \subseteq S\,)$
“Indirect Relation Inclusion” “Indirect Relation Inclusion from above”: $Q \subseteq R \equiv (\forall\, S \bullet R \subseteq S \Rightarrow Q \subseteq S\,)$

Continuing with Intersection

“Characterisation of ∩”: $Q \subseteq R \cap S \equiv Q \subseteq R \land Q \subseteq S$
“Weakening for ∩”: $Q \cap R \subseteq Q \land Q \cap R \subseteq R$
“Symmetry of ∩”: $Q \cap R \subseteq R \cap Q$
“Symmetry of ∩”: $Q \cap R = R \cap Q$
“Associativity of ∩”: $(Q \cap R) \cap S \subseteq Q \cap (R \cap S)$
“Associativity of ∩”: $(Q \cap R) \cap S = Q \cap (R \cap S)$
“Idempotency of ∩”: $R \cap R = R$
“Monotonicity of ∩”: $Q \subseteq R \Rightarrow Q \cap S \subseteq R \cap S$
“Sub-distributivity of ⨾ over ∩”: $Q \mathbin{;} (R \cap S) \subseteq Q \mathbin{;} R \cap Q \mathbin{;} S$
“Sub-distributivity of ⨾ over ∩”: $(Q \cap R) \mathbin{;} S \subseteq Q \mathbin{;} S \cap R \mathbin{;} S$
“Converse of ∩”: $(R \cap S)^{\smile} \subseteq R^{\smile} \cap S^{\smile}$
“Converse of ∩”: $(R \cap S)^{\smile} = R^{\smile} \cap S^{\smile}$
“Dedekind rule”: $Q \mathbin{;} R \cap S \subseteq (Q \cap S \mathbin{;} R^{\smile}) \mathbin{;} (R \cap Q^{\smile} \mathbin{;} S)$
“Modal rule”: $Q \mathbin{;} R \cap S \subseteq (Q \cap S \mathbin{;} R^{\smile}) \mathbin{;} R$
“Modal rule”: $Q \mathbin{;} R \cap S \subseteq Q \mathbin{;} (R \cap Q^{\smile} \mathbin{;} S)$

Continuing with Union

“Characterisation of ∪”: $Q \cup R \subseteq S \equiv Q \subseteq S \land R \subseteq S$
“Weakening for ∪”: $Q \subseteq Q \cup R \land R \subseteq Q \cup R$
“Symmetry of ∪”: $Q \cup R = R \cup Q$
“Associativity of ∪”: $(Q \cup R) \cup S = Q \cup (R \cup S)$
“Idempotency of ∪”: $R \cup R = R$
“Monotonicity of ∪”: $Q \subseteq R \Rightarrow Q \cup S \subseteq R \cup S$
“Distributivity of ⨾ over ∪”: $Q \mathbin{;} (R \cup S) = Q \mathbin{;} R \cup Q \mathbin{;} S$
“Converse of ∪”: $(R \cup S)^{\smile} = R^{\smile} \cup S^{\smile}$
“Distributivity of ∩ over ∪”: $Q \cap (R \cup S) = (Q \cap R) \cup (Q \cap S)$
“Absorption of ∪ by ∩”: $Q \cap (Q \cup R) = Q$
“Absorption of ∩ by ∪”: $Q \cup (Q \cap R) = Q$
“Distributivity of ∪ over ∩”: $Q \cup (R \cap S) = (Q \cup R) \cap (Q \cup S)$

Homogeneous Relation Properties 1

“Definition of reflexivity”: $\text{is-reflexive } R \equiv \mathrm{Id} \subseteq R$
“Definition of symmetry”: $\text{is-symmetric } R \equiv R^{\smile} \subseteq R$
“Definition of transitivity”: $\text{is-transitive } R \equiv R \mathbin{;} R \subseteq R$
“Definition of idempotency”: $\text{is-idempotent } R \equiv R \mathbin{;} R = R$
“Definition of equivalence”: $\text{is-equivalence } R \equiv \text{is-reflexive } R \land \text{is-symmetric } R \land \text{is-transitive } R$
“Definition of symmetry”: $\text{is-symmetric } R \equiv R^{\smile} = R$

“Reflexivity of converse”: $\text{is-reflexive } R \equiv \text{is-reflexive } (R^{\smile})$
“Symmetry of converse”: $\text{is-symmetric } R \equiv \text{is-symmetric } (R^{\smile})$
“Transitivity of converse”: $\text{is-transitive } R \equiv \text{is-transitive } (R^{\smile})$
“Idempotency of converse”: $\text{is-idempotent } R \equiv \text{is-idempotent } (R^{\smile})$
“Converse of an equivalence”: $\text{is-equivalence } R \equiv \text{is-equivalence } (R^{\smile})$
“Idempotency from reflexive and transitive”: $\text{is-reflexive } R \Rightarrow \text{is-transitive } R \Rightarrow \text{is-idempotent } R$

Heterogeneous Relation Properties

“Definition of univalence”: $\text{is-univalent } R \equiv R^{\smile} \mathbin{;} R \subseteq \mathrm{Id}$
“Definition of totality”: $\text{is-total } R \equiv \mathrm{Id} \subseteq R \mathbin{;} R^{\smile}$
“Definition of injectivity”: $\text{is-injective } R \equiv R \mathbin{;} R^{\smile} \subseteq \mathrm{Id}$
“Definition of surjectivity”: $\text{is-surjective } R \equiv \mathrm{Id} \subseteq R^{\smile} \mathbin{;} R$

“Definition of mappings”: $\text{is-mapping } R \equiv \text{is-univalent } R \land \text{is-total } R$
“Definition of mappings”: $\text{is-mapping } R \equiv R^{\smile} \mathbin{;} R \subseteq \mathrm{Id} \land \mathrm{Id} \subseteq R \mathbin{;} R^{\smile}$

“Definition of bijectivity”: $\text{is-bijective } R \equiv \text{is-injective } R \land \text{is-surjective } R$
“Definition of bijectivity”: $\text{is-bijective } R \equiv R \mathbin{;} R^{\smile} \subseteq \mathrm{Id} \land \mathrm{Id} \subseteq R^{\smile} \mathbin{;} R$

“total in univalent”: $\text{is-total } R \Rightarrow \text{is-univalent } S \Rightarrow R \subseteq S \Rightarrow S \subseteq R$
“total in univalent”: $\text{is-total } R \Rightarrow \text{is-univalent } S \Rightarrow R \subseteq S \Rightarrow S = R$

“Definition of inverse”: $R \text{ is-inverse-of } S \equiv R \mathbin{;} S = \mathrm{Id} \land S \mathbin{;} R = \mathrm{Id}$

“Inverse of mapping”: $\text{is-mapping } f \Rightarrow g \text{ is-inverse-of } f \Rightarrow g = f^{\smile}$

Homogeneous Relation Properties 2

“Definition of antisymmetry”: $\text{is-antisymmetric } R \equiv R \cap R^{\smile} \subseteq \mathrm{Id}$
“Definition of ordering”: $\text{is-order } R \equiv \text{is-reflexive } R \land \text{is-antisymmetric } R \land \text{is-transitive } R$

“Antisymmetry of converse”: $\text{is-antisymmetric } R \equiv \text{is-antisymmetric } (R^{\smile})$
“Converse of an order”: $\text{is-order } E \equiv \text{is-order } (E^{\smile})$
“Hesitation”: $R \subseteq R \mathbin{;} R^{\smile} \mathbin{;} R$
“Idempotency from symmetric and transitive”: $\text{is-symmetric } R \Rightarrow \text{is-transitive } R \Rightarrow \text{is-idempotent } R$

Leibniz as Axiom and Replacement Laws

(3.83) "Leibniz": $e = f \Rightarrow E[z := e] = E[z := f]$
(3.84) (3.84a) "Substitution" "Replacement": $e = f \wedge E[z := e] \equiv e = f \wedge E[z := f]$
(3.84) (3.84b) "Substitution" "Replacement": $e = f \Rightarrow E[z := e] \equiv e = f \Rightarrow E[z := f]$
(3.84) (3.84c) "Substitution" "Replacement":
$q \wedge e = f \Rightarrow E[z := e] \equiv q \wedge e = f \Rightarrow E[z := f]$
(3.85) (3.85a) "Replace by 'true'": $p \Rightarrow E[z := p] \equiv p \Rightarrow E[z := \mathrm{true}]$
(3.85) (3.85b) "Replace by 'true'": $q \wedge p \Rightarrow E[z := p] \equiv q \wedge p \Rightarrow E[z := \mathrm{true}]$
(3.85c) "Replace by 'false'": $\neg p \Rightarrow E[z := p] \equiv \neg p \Rightarrow E[z := \mathrm{false}]$
(3.86) (3.86a) "Replace by 'false'": $E[z := p] \Rightarrow p \equiv E[z := \mathrm{false}] \Rightarrow p$
(3.86) (3.86b) "Replace by 'false'": $E[z := p] \Rightarrow p \vee q \equiv E[z := \mathrm{false}] \Rightarrow p \vee q$
(3.87) "Replace by 'true'": $p \wedge E[z := p] \equiv p \wedge E[z := \mathrm{true}]$
(3.88) "Replace by 'false'": $p \vee E[z := p] \equiv p \vee E[z := \mathrm{false}]$
(3.89) "Shannon": $E[z := p] \equiv (p \wedge E[z := \mathrm{true}]) \vee (\neg p \wedge E[z := \mathrm{false}])$

Monotonicity with Respect to Implication

"Left-monotonicity of ∨" "Monotonicity of ∨": $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$
(4.2) "Left-monotonicity of ∨" "Monotonicity of ∨": $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$
"Monotonicity of ∨": $(p \Rightarrow q) \Rightarrow (r \Rightarrow s) \Rightarrow (p \vee r \Rightarrow q \vee s)$
(4.3) "Left-monotonicity of ∧" "Monotonicity of ∧": $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$
"Monotonicity of ∧": $(p \Rightarrow p') \Rightarrow (q \Rightarrow q') \Rightarrow (p \wedge q \Rightarrow p' \wedge q')$
"Antitonicity of ¬": $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$
"Monotonicity of ⇒" "Right-monotonicity of ⇒": $(p \Rightarrow q) \Rightarrow ((r \Rightarrow p) \Rightarrow (r \Rightarrow q))$
"Antitonicity of ⇒" "Left-antitonicity of ⇒": $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$

General Quantification

"Leibniz for ⋆ range": $(\forall x \bullet R_1 \equiv R_2\ ) \Rightarrow (\star x \mid R_1 \bullet E\ ) = (\star x \mid R_2 \bullet E\ )$
"Leibniz for ⋆ body": $(\forall x \bullet E_1 = E_2\ ) \Rightarrow (\star x \mid R \bullet E_1\ ) = (\star x \mid R \bullet E_2\ )$
(8.11) "Substitution" "Substitution into ⋆", provided: ¬*occurs*('x', 'F'):
$(\star x \mid R \bullet P\ )[y := F] \equiv (\star x \mid R[y := F] \bullet P[y := F]\ )$
(8.13) "Empty range" "Empty range for ⋆": $(\star x \mid \mathrm{false} \bullet P\ ) \equiv u$
— provided 'u' is the identity of '⋆'
(8.14) "One-point rule" "One-point rule for ⋆":
$(\star x \mid x = E \bullet P\ ) \equiv P[x := E]$ — provided: ¬*occurs*('x', 'E')
(8.15) "Distributivity" "Distributivity of ⋆ over ∧":
$(\star x \mid R \bullet P\ ) \star (\star x \mid R \bullet Q\ ) \equiv (\star x \mid R \bullet P \star Q\ )$
(8.17) "Range split": $(\star x \mid R \bullet P\ ) \star (\star x \mid S \bullet P\ )$
$\equiv (\star x \mid R \vee S \bullet P\ ) \star (\star x \mid R \wedge S \bullet P\ )$
(8.20) "Nesting": — provided: ¬*occurs*('y', 'R')
$(\star x, y \mid R \wedge S \bullet P\ ) \equiv (\star x \mid R \bullet (\star y \mid S \bullet P\ )\ )$

(8.20a) "Nesting": $(\star x, y \mid S \bullet P\ ) \equiv (\star x \bullet (\star y \mid S \bullet P\ )\ )$
"Context": $(\star y \mid R \wedge e = f \bullet P[x := e]\ ) \equiv (\star y \mid R \wedge e = f \bullet P[x := f]\ )$
(8.20a) "Dummy list permutation": $(\star x, y \mid R \bullet P\ ) \equiv (\star y, x \mid R \bullet P\ )$
(8.19) "Interchange of dummies" provided: ¬*occurs*('y', 'R'), ¬*occurs*('x','S'):
$(\star x \mid R \bullet (\star y \mid S \bullet P\ )\ ) \equiv (\star y \mid S \bullet (\star x \mid R \bullet P\ )\ )$
(8.21) "Dummy renaming" "α-conversion", provided: ¬*occurs*('y', 'P, R'):
$(\star x \mid R \bullet P\ ) \equiv (\star y \mid R[x := y] \bullet P[x := y]\ )$

"Split off term" "Split off term at top": $(\star i : \mathbb{N} \mid i < S\ n \bullet E\ )$
$= (\star i : \mathbb{N} \mid i < n \bullet E\ ) \star E[i := n]$

"Split off term" "Split off term at top": $m \le n \Rightarrow$
$(\star i : \mathbb{N} \mid m \le i < S\ n \bullet E\ ) = (\star i : \mathbb{N} \mid m \le i < n \bullet E\ ) \star E[i := n]$

"Split off term at top using ≤":
$(\star i : \mathbb{N} \mid i \le S\ n \bullet E\ ) = (\star i : \mathbb{N} \mid i \le n \bullet E\ ) \star E[i := S\ n]$

Universal Quantification

"Trading" "Trading for ∀": $(\forall x \mid R \bullet P\ ) \equiv (\forall x \bullet R \Rightarrow P\ )$
(9.8) "True ∀ body": $(\forall x \mid R \bullet \mathrm{true}\ )$
(9.9) "Sub-distributivity of ∀ over ≡":
$(\forall x \mid R \bullet P \equiv Q\ ) \Rightarrow ((\forall x \mid R \bullet P\ ) \equiv (\forall x \mid R \bullet Q\ ))$
(9.10) "Range weakening for ∀" "Range strengthening for ∀":
$(\forall x \mid Q \vee R \bullet P\ ) \Rightarrow (\forall x \mid Q \bullet P\ )$
(9.11) "Body weakening for ∀" "Body strengthening for ∀":
$(\forall x \mid R \bullet P \wedge Q\ ) \Rightarrow (\forall x \mid R \bullet P\ )$
(9.12) "Monotonicity of ∀" "Body monotonicity of ∀":
$(\forall x \mid R \bullet Q \Rightarrow P\ ) \Rightarrow ((\forall x \mid R \bullet Q\ ) \Rightarrow (\forall x \mid R \bullet P\ ))$
(9.12a) "Range antitonicity of ∀":
$(\forall x \bullet Q \Rightarrow R\ ) \Rightarrow ((\forall x \mid R \bullet P\ ) \Rightarrow (\forall x \mid Q \bullet P\ ))$
(9.13) "Instantiation": $(\forall x \bullet P\ ) \Rightarrow P[x := E]$
(9.13a) "Instantiation": $(\forall x \bullet P\ ) \Rightarrow P[x := x]$
(9.13b) "Instantiation": $(\forall x \mid R \bullet P\ ) \Rightarrow (R \Rightarrow P)[x := E]$

Existential Quantification

(9.17) "Generalised De Morgan": $(\exists x \mid R \bullet P\ ) \equiv \neg (\forall x \mid R \bullet \neg P\ )$
(9.18) (9.18a) "Generalised De Morgan": $\neg (\exists x \mid R \bullet \neg P\ ) \equiv (\forall x \mid R \bullet P\ )$
(9.18) (9.18b) "Generalised De Morgan": $\neg (\exists x \mid R \bullet P\ ) \equiv (\forall x \mid R \bullet \neg P\ )$
(9.18) (9.18c) "Generalised De Morgan": $(\exists x \mid R \bullet \neg P\ ) \equiv \neg (\forall x \mid R \bullet P\ )$
"Trading" "Trading for ∃": $(\exists x \mid R \bullet P\ ) \equiv (\exists x \bullet R \wedge P\ )$
(9.21) "Distributivity of ∧ over ∃", provided: ¬*occurs*('x', 'P'):
$P \wedge (\exists x \mid R \bullet Q\ ) \equiv (\exists x \mid R \bullet P \wedge Q\ )$
(9.22), provided: ¬*occurs*('x', 'P'): $P \wedge (\exists x \bullet R\ ) \equiv (\exists x \mid R \bullet P\ )$
(9.24) "False ∃ body": $(\exists x \mid R \bullet \mathrm{false}\ ) \equiv \mathrm{false}$

(9.25) “Range weakening for ∃” “Range strengthening for ∃”:
$(\exists\, x \mid R \bullet P\,) \Rightarrow (\exists\, x \mid Q \lor R \bullet P\,)$

(9.26) “Body weakening for ∃” “Body strengthening for ∃”:
$(\exists\, x \mid R \bullet P\,) \Rightarrow (\exists\, x \mid R \bullet P \lor Q\,)$

(9.26a) “Body weakening for ∃” “Body strengthening for ∃”:
$(\exists\, x \mid R \bullet P \land Q\,) \Rightarrow (\exists\, x \mid R \bullet P\,)$

(9.27) “Monotonicity of ∃” “Body monotonicity of ∃”:
$(\forall\, x \mid R \bullet Q \Rightarrow P\,) \Rightarrow ((\exists\, x \mid R \bullet Q\,) \Rightarrow (\exists\, x \mid R \bullet P\,))$

(9.27a) “Range monotonicity of ∃”:
$(\forall\, x \bullet Q \Rightarrow R\,) \Rightarrow ((\exists\, x \mid Q \bullet P\,) \Rightarrow (\exists\, x \mid R \bullet P\,))$

(9.28) “∃-Introduction”: $P[x := E] \Rightarrow (\exists\, x \bullet P\,)$

Relations via Set Theory

(14.2) “Pair equality”: $\langle b, c\rangle = \langle b', c'\rangle \equiv b = b' \land c = c'$
“Definition of ‘fst‘”: $\mathrm{fst}\ \langle x, y\rangle = x$
“Definition of ‘snd‘”: $\mathrm{snd}\ \langle x, y\rangle = y$
“Definition of ↔”: $A \leftrightarrow B = \mathbb{P}\,(A \times B)$
“Infix relationship” “Definition of ‘_⦇_⦈_‘”: $a \llparenthesis R \rrparenthesis b \equiv \langle a, b\rangle \in R$

“Relation extensionality”: $R = S \equiv (\forall\, x \bullet (\forall\, y \bullet x \llparenthesis R \rrparenthesis y \equiv x \llparenthesis S \rrparenthesis y\,))$
— provided: ¬*occurs*(‘x, y‘, ‘R, S‘)
“Relation inclusion”: $R \subseteq S \equiv (\forall\, x \bullet (\forall\, y \bullet x \llparenthesis R \rrparenthesis y \Rightarrow x \llparenthesis S \rrparenthesis y\,))$
— provided: ¬*occurs*(‘x, y‘, ‘R, S‘)
“Relation inclusion”: $R \subseteq S \equiv (\forall\, x, y \mid x \llparenthesis R \rrparenthesis y \bullet x \llparenthesis S \rrparenthesis y\,)$
— provided: ¬*occurs*(‘x, y‘, ‘R, S‘)

“Empty relation”: $a \llparenthesis \{\} \rrparenthesis b \equiv \mathrm{false}$
“Universal relation”: $(\forall\, A : \mathrm{Type} \bullet (\forall\, B : \mathrm{Type} \bullet a \llparenthesis A \times B \rrparenthesis b\,)\,)$
“Singleton relation”: $a_1 \llparenthesis \{\langle a_2, b_2\rangle\} \rrparenthesis b_1 \equiv a_1 = a_2 \land b_1 = b_2$
“Singleton relation inclusion”: $\{\langle a, b\rangle\} \subseteq R \equiv a \llparenthesis R \rrparenthesis b$
“Relation union”: $a \llparenthesis R \cup S \rrparenthesis b \equiv a \llparenthesis R \rrparenthesis b \lor a \llparenthesis S \rrparenthesis b$
“Relation intersection”: $a \llparenthesis R \cap S \rrparenthesis b \equiv a \llparenthesis R \rrparenthesis b \land a \llparenthesis S \rrparenthesis b$
“Relation difference”: $a \llparenthesis R - S \rrparenthesis b \equiv a \llparenthesis R \rrparenthesis b \land \neg\,(a \llparenthesis S \rrparenthesis b)$
“Relation pseudocomplement”: $a \llparenthesis R \mathbin{\Rightarrow} S \rrparenthesis b \equiv a \llparenthesis R \rrparenthesis b \Rightarrow a \llparenthesis S \rrparenthesis b$
“Relation complement”: $a \llparenthesis \sim R \rrparenthesis b \equiv \neg\,(a \llparenthesis R \rrparenthesis b)$
“Empty relation”: $a \llparenthesis \{\} \rrparenthesis b \equiv \mathrm{false}$
“Universal relation”: $(\forall\, A : \mathrm{Type} \bullet (\forall\, B : \mathrm{Type} \bullet a \llparenthesis A \times B \rrparenthesis b\,)\,)$
“Relation composition”: $a \llparenthesis R \mathbin{;} S \rrparenthesis c \equiv (\exists\, b \bullet a \llparenthesis R \rrparenthesis b \land b \llparenthesis S \rrparenthesis c\,)$
— provided: ¬*occurs*(‘b‘, ‘a, c, R, S‘)
“Identity relation” “Relationship via ‘Id‘”: $x \llparenthesis \mathrm{Id} \rrparenthesis y \equiv x = y$
“Relation converse” “Relationship via ˘”: $y \llparenthesis R^{\smile} \rrparenthesis x \equiv x \llparenthesis R \rrparenthesis y$
“Relationship via right residual”: $b \llparenthesis R \setminus S \rrparenthesis c \equiv (\forall\, a \bullet a \llparenthesis R \rrparenthesis b \Rightarrow a \llparenthesis S \rrparenthesis c\,)$
— provided: ¬*occurs*(‘a‘, ‘b, c, R, S‘)
“Relationship via left residual”: $a \llparenthesis S / R \rrparenthesis b \equiv (\forall\, c \bullet b \llparenthesis R \rrparenthesis c \Rightarrow a \llparenthesis S \rrparenthesis c\,)$
— provided: ¬*occurs*(‘c‘, ‘a, b, R, S‘)

Sequences

(13.3) “Cons is not empty”: $x \lhd xs \neq \epsilon$
“Cons is not empty”: $x \lhd xs = \epsilon \equiv \mathrm{false}$
(13.4) “Injectivity of ◁”: $x \lhd xs = y \lhd ys \equiv x = y \land xs = ys$
(13.6) “Cons decomposition”: $xs = \epsilon \lor (\exists\, y \bullet (\exists\, ys \bullet xs = y \lhd ys))$
(13.7) “Tail is different”: $x \lhd xs \neq xs$

Sequence Membership ∈, Snoc ▷

“Membership in ϵ”: $x \in \epsilon \equiv \mathrm{false}$
“Membership in ◁”: $x \in y \lhd ys \equiv x = y \lor x \in ys$
(13.12) “Definition of ▷” “Definition of ▷ for ϵ”: $\epsilon \rhd a = a \lhd \epsilon$
(13.13) “Definition of ▷” “Definition of ▷ for ◁”: $(a \lhd s) \rhd b = a \lhd (s \rhd b)$
(13.14) “Snoc is not empty”: $xs \rhd x \neq \epsilon$
“Snoc is not empty”: $xs \rhd x = \epsilon \equiv \mathrm{false}$
(13.15) “Injectivity of ▷”: $xs \rhd x = ys \rhd y \equiv xs = ys \land x = y$
(13.16) “Membership in ▷”: $x \in ys \rhd z \equiv x \in ys \lor x = z$

Concatenation

(13.17) “Left-identity of ⌢” “Definition of ⌢ for ϵ”: $\epsilon \frown ys = ys$
(13.18) “Mutual associativity of ◁ with ⌢” “Definition of ⌢ for ◁”:
$(x \lhd xs) \frown ys = x \lhd (xs \frown ys)$
(13.19) “Right-identity of ⌢”: $xs \frown \epsilon = xs$
(13.20) “Associativity of ⌢”: $(xs \frown ys) \frown zs = xs \frown (ys \frown zs)$
(13.21) “Membership in ⌢”: $x \in ys \frown zs \equiv x \in ys \lor x \in zs$
(13.22) “Mutual associativity of ⌢ with ▷”: $(xs \frown ys) \rhd z = xs \frown (ys \rhd z)$
(13.23) “Empty concatenation”: $xs \frown ys = \epsilon \equiv xs = \epsilon \land ys = \epsilon$

Subsequences, Prefix, Segments

(13.25) “Empty subsequence”: $\epsilon \subseteq ys$
(13.26) “Subsequence” “Cons is not a subsequence of ϵ”: $\neg\,(x \lhd xs \subseteq \epsilon)$
Corollary “Cons is not a subsequence of ϵ”: $x \lhd xs \subseteq \epsilon \equiv \mathrm{false}$
(13.27) “Subsequence anchored at head”: $x \lhd ys \subseteq x \lhd zs \equiv ys \subseteq zs$
“Subsequence anchored at head”: $y = z \Rightarrow (y \lhd ys \subseteq z \lhd zs \equiv ys \subseteq zs)$
(13.28) “Subsequence without head”: $x \neq y \Rightarrow (x \lhd xs \subseteq y \lhd ys \equiv x \lhd xs \subseteq ys)$
(13.29) “Proper subsequence” “Definition of ⊂”: $xs \subset ys \equiv xs \subseteq ys \land xs \neq ys$
(13.30) “Reflexivity of ⊆”: $xs \subseteq xs$
(13.31) “Cons ⊆-expands”: $ys \subseteq x \lhd ys$
(13.33) “Subsequence of ϵ”: $xs \subseteq \epsilon \equiv xs = \epsilon$
“Non-empty subsequences”:
$y \lhd ys \subseteq z \lhd zs \equiv (y = z \Rightarrow ys \subseteq zs) \land (y \neq z \Rightarrow y \lhd ys \subseteq zs)$
(13.34) “Membership of subsequence”: $ys \subseteq zs \Rightarrow x \in ys \Rightarrow x \in zs$
(13.36) “Empty prefix”: $\mathrm{isprefix}\ \epsilon\ xs$
(13.37) “Not Prefix” “Cons is not prefix of ϵ”: $\mathrm{isprefix}\ (x \lhd xs)\ \epsilon \equiv \mathrm{false}$

(13.38) “Prefix” “Cons prefix”: $\text{isprefix}\ (x \lhd xs)\ (y \lhd ys) \equiv x = y \land \text{isprefix}\ xs\ ys$
(13.39) “Segment” “Segment of ϵ”: $\text{isseg}\ xs\ \epsilon \equiv xs = \epsilon$
(13.40) “Segment” “Segment of $\lhd$”:
$\text{isseg}\ xs\ (y \lhd ys) \equiv \text{isprefix}\ xs\ (y \lhd ys) \lor \text{isseg}\ xs\ ys$

Reverse

“Definition of ‘rev’ for ϵ”: $\text{rev}\ \epsilon = \epsilon$
“Definition of ‘rev’ for $\lhd$”: $\text{rev}\ (x \lhd xs) = \text{rev}\ xs \rhd x$
“Reverse of snoc”: $\text{rev}\ (xs \rhd y) = y \lhd \text{rev}\ xs$
“Reverse of $\frown$”: $\text{rev}\ (xs \frown ys) = \text{rev}\ ys \frown \text{rev}\ xs$
“Self-inverse of reverse”: $\text{rev}\ (\text{rev}\ xs) = xs$
“Cancellation of reverse”: $\text{rev}\ xs = \text{rev}\ ys \equiv xs = ys$
“Membership in reverse”: $y \in \text{rev}\ xs \equiv y \in xs$

Sets

(11.3) “Set membership”, provided: $\neg$*occurs*(‘x’, ‘F’):
$F \in \{ x \mid R \bullet E \} \equiv (\exists x \mid R \bullet F = E)$
“Set Abbreviation”: $\{ x \mid P \} = \{ x \mid P \bullet x \}$

(11.7) (11.7s) “Simple Membership”: $e \in \{ x \mid P \} \equiv P[x := e]$
(11.7) (11.7∀) “Simple Membership”: $(\forall x \bullet x \in \{ x \mid P \} \equiv P)$

(11.4) “Set Equality” “Extensionality”, provided: $\neg$*occurs*(‘e’, ‘S, T’):
$S = T \equiv (\forall e \bullet e \in S \equiv e \in T)$
(11.6) “Mathematical Formulation of Set Comprehension”, provided: $\neg$*occurs*(‘y’, ‘E, P’):
$\{ x \mid P \bullet E \} = \{ y \mid (\exists x \mid P \bullet y = E) \}$
(11.9) “Simple set comprehension equality”: $\{ x \mid Q \} = \{ x \mid R \} \equiv (\forall x \bullet Q \equiv R)$

(11.13) “Subset” “Inclusion”, provided: $\neg$*occurs*(‘x’, ‘S, T’):
$S \subseteq T \equiv (\forall x \mid x \in S \bullet x \in T)$
“Subset” “Inclusion”, provided: $\neg$*occurs*(‘x’, ‘S, T’): $S \subseteq T \equiv (\forall x \bullet x \in S \Rightarrow x \in T)$

(11.14) “Proper subset” “Definition of $\subset$”: $S \subset T \equiv S \subseteq T \land S \neq T$

(11.56) “Simple set comprehension inclusion”: $\{ x \mid P \} \subseteq \{ x \mid Q \} \equiv (\forall x \bullet P \Rightarrow Q)$
(11.63) “Inclusion in terms of $\subset$”: $S \subseteq T \equiv S \subset T \lor S = T$
(11.70) “Transitivity of $\subseteq$ with $\subset$”: $X \subseteq Y \Rightarrow (Y \subset Z \Rightarrow X \subset Z)$
“Indirect set equality from below”, provided: $\neg$*occurs*(‘S’, ‘A, B’):
$A = B \equiv (\forall S : \text{set}\ X \bullet S \subseteq A \equiv S \subseteq B)$
“Indirect set equality from above”, provided: $\neg$*occurs*(‘S’, ‘A, B’):
$A = B \equiv (\forall S : \text{set}\ X \bullet A \subseteq S \equiv B \subseteq S)$

Set Inclusion (ctd.); Empty and Universal Sets

“Casting”: $X \subseteq Y \Rightarrow (x \in X \Rightarrow x \in Y)$
(11.58) “Reflexivity of $\subseteq$”: $X \subseteq X$
(11.59) “Transitivity of $\subseteq$”: $X \subseteq Y \Rightarrow Y \subseteq Z \Rightarrow X \subseteq Z$
“Antisymmetry of $\subseteq$”: $X \subseteq Y \Rightarrow Y \subseteq X \Rightarrow X = Y$
“Empty set”: $\{\} = \{ x \mid \text{false} \}$
“Empty set”: $x \in \{\} \equiv \text{false}$
“Empty set is least” “Bottom set”: $\{\} \subseteq X$
“Inclusion in empty set”: $S \subseteq \{\} \equiv S = \{\}$
“Universal set”: $\mathbf{U} = \{ x \mid \text{true} \}$
“Universal set”: $x \in \mathbf{U}$
“Universal set is greatest” “Top set”: $X \subseteq \mathbf{U}$
“Inclusion of universe”: $\mathbf{U} \subseteq S \equiv \mathbf{U} = S$
“Singleton set”: $x \in \{y\} \equiv x = y$
“Singleton set inclusion”: $\{x\} \subseteq S \equiv x \in S$
(11.61): $S \subset T \equiv S \subseteq T \land \neg (T \subseteq S)$

Set Complement

“Complement”: $e \in \sim S \equiv \neg (e \in S)$
(11.19) “Self-inverse of complement”: $\sim (\sim S) = S$
“Inclusion of complement”: $\sim X \subseteq Y \equiv \sim Y \subseteq X$
“Inclusion in complement”: $X \subseteq \sim Y \equiv Y \subseteq \sim X$

Set Union and Intersection

“Union”: $e \in S \cup T \equiv e \in S \lor e \in T$
“Intersection”: $e \in S \cap T \equiv e \in S \land e \in T$
(11.26) “Symmetry of $\cup$”: $S \cup T = T \cup S$
(11.27) “Associativity of $\cup$”: $S \cup (T \cup W) = (S \cup T) \cup W$
(11.28) “Idempotency of $\cup$”: $S \cup S = S$
(11.30) “Zero of $\cup$”: $S \cup \mathbf{U} = \mathbf{U}$
(11.30) “Identity of $\cup$”: $S \cup \{\} = S$
(11.31) “Weakening of $\cup$”: $S \subseteq S \cup T$
(11.32) “LEM of $\cup$”: $S \cup \sim S = \mathbf{U}$
(11.33) “Symmetry of $\cap$”: $S \cap T = T \cap S$
(11.34) “Associativity of $\cap$”: $S \cap (T \cap W) = (S \cap T) \cap W$
(11.35) “Idempotency of $\cap$”: $S \cap S = S$
(11.36) “Zero of $\cap$”: $S \cap \{\} = \{\}$
(11.37) “Identity of $\cap$”: $S \cap \mathbf{U} = S$
(11.38) “Weakening of $\cap$”: $S \cap T \subseteq S$
(11.39) “Contradiction of $\cap$”: $S \cap \sim S = \{\}$
“Golden Rule”: $S \cap T = S \equiv T = S \cup T$
“Monotonicity of $\cap$”: $S \subseteq T \Rightarrow S \cap U \subseteq T \cap U$
“Monotonicity of $\cap$”: $S \subseteq T \Rightarrow (U \subseteq V \Rightarrow S \cap U \subseteq T \cap V)$

Set Difference and Relative Pseudocomplement

(11.22) “Set difference”: $v \in S - T \equiv v \in S \land \neg (v \in T)$
(11.52): $S \cap (T - S) = \{\}$
(11.54): $S - (T \cup U) = (S - T) \cap (S - U)$
“Complement as set difference”: $\sim A = \mathbf{U} - A$
“Characterisation of ⇨”: $S \subseteq A ⇨ B \equiv S \cap A \subseteq B$
“Membership in ⇨”: $x \in A ⇨ B \equiv x \in A \Rightarrow x \in B$
“Definition of ⇨”: $A ⇨ B = \sim A \cup B$
“Complement as pseudocomplement”: $\sim A = A ⇨ \{\}$
“Pseudocomplement of union”: $(A \cup B) ⇨ C = (A ⇨ C) \cap (B ⇨ C)$
“Monotonicity of ⇨”: $B \subseteq C \Rightarrow A ⇨ B \subseteq A ⇨ C$
“Antitonicity of ⇨”: $A \subseteq B \Rightarrow B ⇨ C \subseteq A ⇨ C$

CalcCheck Structured Proofs

Simple Induction

```
By induction on `var : Ty`:
  Base case:
    ?
  Induction step:
      ?
    ... Induction hypothesis ...
      ?
```

Making base case, induction step, and induction hypothesis explicit:

```
By induction on `var : Ty`:
  Base case `?`:
    ?
  Induction step `?`:
      ?
    ... Induction hypothesis `?` ...
      ?
```

(Remember that in nested inductions, induction hypotheses always need to be made explicit!)

Induction pattern for sequences (choose x wisely!):

```
Theorem: P
Proof:
  By induction on `xs : Seq A`:
    Base case `P[xs ≔ ϵ]`:
        ?
    Induction step `∀ x : A • P[xs ≔ x ◃ xs]`:
      For any `x`:
          ?
```

These can also be used for proving theorems of shape

$$\forall\ \texttt{var : Ty} \bullet P$$

by induction on precisely that universally-quantified variable, that is, "on `var : Ty`:".
The induction hypothesis is then P.
Example for sequences:

```
Theorem: ∀ xs : Seq A • P
Proof:
  By induction on `xs : Seq A`:
    Base case `P[xs ≔ ϵ]`:
        ?
    Induction step `∀ x : A • P[xs ≔ x ◃ xs]`:
      For any `x`:
          ?
```

Assuming the Antecedent

```
Assuming `p`, `q`:
    ?
  ... Assumption `p` ...
    ?
```

Case Analysis

```
By cases: `p`, `q`, `r`
  Completeness:
    ?
  Case `p`:
      ?
    ... Assumption `p` ...
      ?
  ...
```

Proving Universal Quantifications

```
For any `var : Ty`:
    ?
```

```
For any `var : Ty` satisfying `p`:
      ?
    ... Assumption `p` ...
      ?
```

Theorems Used as Proof Methods (Examples)

```
Using "Mutual implication":
  Subproof for `... ⇒ ...`:
      ?
  Subproof for `... ⇒ ...`:
      ?
```

```
Using "Extensionality":
  Subproof for `∀ x • ...`:
    For any `x`:
        ?
```

Disabling Hints Producing Time-outs

Add "?, " at the beginning of the hint:

```
    ≡⟨ ?, "Golden rule" ⟩
```

Selected CalcCheck$_{\text{Web}}$ Key Bindings

(See Getting Started with CalcCheck$_{\text{Web}}$ for the complete listing.)

The following key bindings work the same in **both modes**:

`Ctrl-Enter` performs a syntax check on the contents of all code cells before and up to the current cell.

`Ctrl-Alt-Enter` performs proof checks (if enabled) on the contents of all code cells before and up to the current cell.

`Shift-Alt-RightArrow` enlarges the width of the current code cell entry area by a small amount

`Ctrl-Shift-Alt-RightArrow` enlarges the width of the current code cell entry area by a large amount

`Shift-Alt-LeftArrow` reduces the width of the current code cell entry area by a small amount

`Ctrl-Shift-Alt-LeftArrow` reduces the width of the current code cell entry area by a large amount

`Ctrl-Shift-v` (for visible spaces) toggles display of initial spaces on each line as "␣" characters.

`Ctrl-Shift-L` toggles display of line numbers. — **Always untoggle before further editing!**

ONLY if you are logged in via Avenue:

`Ctrl-s` saves the notebook on the server.
(Links for reloading the last three saved versions are displayed when you the notebook again later.)

In **edit mode**, you have the following **key bindings**:

`Esc` enters command mode

`Alt-SPACE` ***or*** `Alt-i` inserts one space in the current line and in all non-empty lines below it, until a line is encountered that is not indented more than to the cursor position.

`Alt-BACKSPACE` deletes **only a space character** to the left of the current cursor position, and also from lines below it, until a line is encountered that is not indented at least to the cursor position.

`Alt-DELETE` deletes **only a space character** to the right of the current cursor position, and also from lines below it, until a line is encountered that is not indented more than to the cursor position.

The last three bindings also work with the `Shift` *key pressed.*

Some important symbols:

Symbol	Key sequence(s)
$\Rightarrow$	`\implies`, `\=>`
$\Leftarrow$	`\follows`
$\not\equiv$	`\nequiv`
$\neq$	`\neq`
$\forall$	`\forall`
$\exists$	`\exists`
$\sum$	`\sum`
$\prod$	`\product`
$\mid$	`\with`
$\bullet$	`\spot`
$\downarrow$	`\min`
$\uparrow$	`\max`
$\mathbb{B}$	`\BB`, `\bool`
$\mathbb{N}$	`\NN`, `\nat`
$\mathbb{Z}$	`\ZZ`, `\int`
$\in$	`\in`
$\mathbb{P}$	`\PP`, `\powerset`
$\cup$	`\union`
$\cap$	`\intersection`
⇨	`\pseudocompl`
$\subseteq$	`\subseteq`
$\subset$	`\subset`
$\mathbf{U}$	`\universe`
$\times$	`\times`
$\leftrightarrow$	`\rel`
⦇	`\lrel`, `\((`, `\([`
⦈	`\rrel`, `\))`, `\])`
$⨾$	`\rcomp`, `\fcomp`, `\;;`
$\smile$	`\converse`, `\u{}`
$/$	`\lres`
$\backslash$	`\rres`
ϵ	`\eps`, `\emptyseq`
$\triangleleft$	`\cons`
$\triangleright$	`\snoc`
$\frown$	`\catenate`

Contents