2DM3 2018 — Final Theorem List — (filled, not provided in Final Exam)

Equivalence, Negation and Inequivalence

"Definition of ≡": $(p \equiv q) = (p = q)$
(3.2) "Symmetry of ≡": $p \equiv q \equiv q \equiv p$
(3.3) "Identity of ≡": $true \equiv q \equiv q$
(3.5) "Reflexivity of ≡": $p \equiv p$
(3.9) "Commutativity of ¬ with ≡" "Distributivity of ¬ over ≡": $\neg (p \equiv q) \equiv (\neg p \equiv q)$
(3.11) "¬ connection": $\neg p \equiv q \equiv p \equiv \neg q$
(3.14): $(p \not\equiv q) \equiv (\neg p \equiv q)$
(3.15): $\neg p \equiv (p \equiv false)$

Disjunction and Conjunction

(3.32): $p \vee q \equiv (p \vee \neg q \equiv p)$
(3.35) "Golden rule": $p \wedge q \equiv p \equiv q \equiv p \vee q$
(3.48): $p \wedge q \equiv (p \wedge \neg q \equiv \neg p)$
(3.49) "Semi-distributivity of ∧ over ≡": $p \wedge (q \equiv r) \equiv (p \wedge q \equiv (p \wedge r \equiv p))$
(3.50) "Strong Modus Ponens": $p \wedge (q \equiv p) \equiv p \wedge q$
(3.51) "Replacement": $(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \wedge (r \equiv q)$
(3.52) "Alternative definition of ≡": $p \equiv (q \equiv (p \wedge q) \vee (\neg p \wedge \neg q))$
(3.53) "Exclusive or" "Alternative definition of ≢": $(p \not\equiv q) \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$

Implication

(3.57) "Definition of ⇒": $p \Rightarrow q \equiv (p \vee q \equiv q)$
(3.58) "Definition of ⇐" "Consequence": $p \Leftarrow q \equiv q \Rightarrow p$
(3.59) "Definition of ⇒": $p \Rightarrow q \equiv \neg p \vee q$
(3.60) "Definition of ⇒": $p \Rightarrow q \equiv (p \wedge q \equiv p)$
(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 ⇒ over ≡": $p \Rightarrow (q \equiv r) \equiv (p \Rightarrow q \equiv p \Rightarrow r)$
(3.64) "Self-distributivity of ⇒": $p \Rightarrow (q \Rightarrow r) \equiv (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$
(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 ⇒": $p \Rightarrow p$
(3.72) "Right-zero of ⇒": $p \Rightarrow true$
(3.73) "Left-identity of ⇒": $true \Rightarrow p \equiv p$
"Definition of ¬" (3.74): $p \Rightarrow false \equiv \neg p$
(3.75) "ex falso quodlibet": $false \Rightarrow p$
(3.76a) "Weakening": $p \Rightarrow p \vee q$
(3.76a) "Weakening": $p \Rightarrow p \vee q$
(3.76b) "Weakening": $p \wedge q \Rightarrow p$
(3.76c) "Weakening": $p \wedge q \Rightarrow p \vee q$
(3.76d) "Weakening": $p \vee (q \wedge r) \Rightarrow p \vee q$
(3.76e) "Weakening": $p \wedge q \Rightarrow p \wedge (q \vee r)$
"Reflexivity of ⇒": $(p \equiv q) \Rightarrow (p \Rightarrow q)$
(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 ⇒": $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$
(3.82a) "Transitivity of ⇒": $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(3.82b) "Transitivity of ⇒": $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(3.82c) "Transitivity of ⇒": $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$
"Implication strengthening": $p \Rightarrow q \equiv p \Rightarrow p \wedge q$

Leibniz as Axiom and Substitution/Replacement Laws

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

Monotonicity with Respect to Implication

(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 ⇒": $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$

Sum Quantification: General Quantifier Material Instantiated for Sum

"Leibniz for ∑ range": $(\forall x \bullet R_1 \equiv R_2) \Rightarrow (\sum x \mid R_1 \bullet E) = (\sum x \mid R_2 \bullet E)$
"Leibniz for ∑ body": $(\forall x \bullet R \Rightarrow E_1 = E_2) \Rightarrow (\sum x \mid R \bullet E_1) = (\sum x \mid R \bullet E_2)$
(8.13) "Empty range for ∑": $(\sum x \mid false \bullet E) = 0$
(8.14) "One-point rule for ∑": $(\sum x \mid x = D \bullet E) = E[x := D]$ — provided: ¬*occurs*('x', 'D')
(8.15) "Distributivity of ∑ over +": $(\sum x \mid R \bullet E_1 + E_2) = (\sum x \mid R \bullet E_1) + (\sum x \mid R \bullet E_2)$
(8.17) "Range split": $(\sum x \mid Q \vee R \bullet E) + (\sum x \mid Q \wedge R \bullet E) = (\sum x \mid Q \bullet E) + (\sum x \mid R \bullet E)$
(8.16) "Disjoint range split for ∑": $(\forall x \bullet Q \wedge R \equiv false) \Rightarrow (\sum x \mid Q \vee R \bullet E) = (\sum x \mid Q \bullet E) + (\sum x \mid R \bullet E)$
(8.20) "Nesting for ∑": $(\sum x \mid Q \bullet (\sum y \mid R \bullet E)) = (\sum x, y \mid Q \wedge R \bullet E)$
— provided: ¬*occurs*('y', 'Q')
"Replacement in ∑": $(\sum x \mid R \wedge e = f \bullet E[y := e]) = (\sum x \mid R \wedge e = f \bullet E[y := f])$
"Dummy list permutation for ∑": $(\sum x, y \mid R \bullet E) = (\sum y, x \mid R \bullet E)$
(8.19) "Interchange of dummies": $(\sum x \mid Q \bullet (\sum y \mid R \bullet P)) = (\sum y \mid R \bullet (\sum x \mid Q \bullet P))$
— provided: ¬*occurs*('x', 'R'), ¬*occurs*('y', 'Q')
(8.21) "Dummy renaming for ∑" "α-conversion": $(\sum x \mid R \bullet E) = (\sum y \mid R[x := y] \bullet E[x := y])$
— provided: ¬*occurs*('y', 'E, R')

Specific Material for Sum Quantification

“Distributivity of $\cdot$ over $\sum$”: $a \cdot (\sum x \mid R \bullet E) = (\sum x \mid R \bullet a \cdot E)$ — provided: $\neg occurs(\text{‘x’}, \text{‘a’})$
“Zero $\sum$ body”: $(\sum x \mid R \bullet 0) = 0$

“Definition of $\le$ in terms of $<$”: $a \le b \equiv a < b \lor a = b$
“Definition of $\le$ in terms of ‘S’ and $<$”: $a \le b \equiv a < S\ b$
“Split range at top”: $m \le n \Rightarrow (m \le i < S\ n \equiv m \le i < n \lor i = n)$
“Split off term at top”: $(\sum i : \mathbb{N} \mid i < S\ n \bullet E) = (\sum i : \mathbb{N} \mid i < n \bullet E) + E[i := n]$
— provided: $\neg occurs(\text{‘i’}, \text{‘n’})$
“Split off term at top”: $m \le n \Rightarrow (\sum i \mid m \le i < S\ n \bullet E) = (\sum i \mid m \le i < n \bullet E) + E[i := n]$
— provided: $\neg occurs(\text{‘i’}, \text{‘m, n’})$
“Split off term at top using $\le$”: $(\sum i \mid i \le S\ n \bullet E) = (\sum i \mid i \le n \bullet E) + E[i := S\ n]$
— provided: $\neg occurs(\text{‘i’}, \text{‘n’})$

Universal Quantification

“Leibniz for $\forall$ body”: $(\forall x \mid R \bullet P_1 \equiv P_2) \Rightarrow ((\forall x \mid R \bullet P_1) \equiv (\forall x \mid R \bullet P_2))$
(8.18) “Range split for $\forall$”: $(\forall x \mid R \lor S \bullet P) \equiv (\forall x \mid R \bullet P) \land (\forall x \mid S \bullet P)$
(9.5) “Distributivity of $\lor$ over $\forall$”: $P \lor (\forall x \mid R \bullet Q) \equiv (\forall x \mid R \bullet P \lor Q)$
— provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.6): $P \lor (\forall x \bullet \neg R) \equiv (\forall x \mid R \bullet P)$ — provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
“Distributivity of $\Rightarrow$ over $\forall$”: $P \Rightarrow (\forall x \mid R \bullet Q) \equiv (\forall x \mid R \bullet P \Rightarrow Q)$ — prov. $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.7) “Distributivity of $\land$ over $\forall$”: $\neg (\forall x \bullet \neg R) \Rightarrow (P \land (\forall x \mid R \bullet Q) \equiv (\forall x \mid R \bullet P \land Q))$
— provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.8) “True $\forall$ body”: $(\forall x \mid R \bullet true)$
“Introducing fresh $\forall$”: $P \Rightarrow (\forall x \mid R \bullet P)$ — provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.9) “Sub-distributivity of $\forall$ over $\equiv$”: $(\forall x \mid R \bullet P \equiv Q) \Rightarrow ((\forall x \mid R \bullet P) \equiv (\forall x \mid R \bullet Q))$
(9.10) “Range weakening for $\forall$”: $(\forall x \mid Q \lor R \bullet P) \Rightarrow (\forall x \mid Q \bullet P)$
(9.11) “Body weakening for $\forall$”: $(\forall x \mid R \bullet P \land Q) \Rightarrow (\forall x \mid R \bullet P)$
(9.12) “Body monotonicity of $\forall$”: $(\forall x \mid R \bullet Q \Rightarrow P) \Rightarrow ((\forall x \mid R \bullet Q) \Rightarrow (\forall x \mid R \bullet P))$
(9.12a) “Range antitonicity of $\forall$”: $(\forall x \bullet Q \Rightarrow R) \Rightarrow ((\forall x \mid R \bullet P) \Rightarrow (\forall x \mid Q \bullet P))$
(9.12a) “Range antitonicity of $\forall$”: $(\forall x \mid \neg P \bullet Q \Rightarrow R) \Rightarrow ((\forall x \mid R \bullet P) \Rightarrow (\forall x \mid Q \bullet P))$
(9.13) “Instantiation”: $(\forall x \bullet P) \Rightarrow P[x := E]$
“Fresh $\forall$”: $P \equiv (\forall x \bullet P)$ — provided: $\neg occurs(\text{‘x’}, \text{‘P’})$

Existential Quantification

(9.21) “Distributivity of $\land$ over $\exists$”: $P \land (\exists x \mid R \bullet Q) \equiv (\exists x \mid R \bullet P \land Q)$
— provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.22): $P \land (\exists x \bullet R) \equiv (\exists x \mid R \bullet P)$ — provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
“Distributivity of $\land$ over $\forall$”: $(\exists x \bullet R) \Rightarrow (P \land (\forall x \mid R \bullet Q) \equiv (\forall x \mid R \bullet P \land Q))$
— provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.23) “Distributivity of $\lor$ over $\exists$”: $(\exists x \bullet R) \Rightarrow (P \lor (\exists x \mid R \bullet Q) \equiv (\exists x \mid R \bullet P \lor Q))$
— provided: $\neg occurs(\text{‘x’}, \text{‘P’})$
(9.24) “False $\exists$ body”: $(\exists x \mid R \bullet false) \equiv false$
(9.25) “Range weakening for $\exists$”: $(\exists x \mid R \bullet P) \Rightarrow (\exists x \mid Q \lor R \bullet P)$
“Range weakening for $\exists$”: $(\exists x \mid Q \land R \bullet P) \Rightarrow (\exists x \mid R \bullet P)$
(9.26) “Body weakening for $\exists$”: $(\exists x \mid R \bullet P) \Rightarrow (\exists x \mid R \bullet P \lor Q)$
(9.26a) “Body weakening for $\exists$”: $(\exists x \mid R \bullet P \land Q) \Rightarrow (\exists x \mid R \bullet P)$
(9.27) “Body monotonicity of $\exists$”: $(\forall x \mid R \bullet Q \Rightarrow P) \Rightarrow ((\exists x \mid R \bullet Q) \Rightarrow (\exists x \mid R \bullet P))$
“Range monotonicity of $\exists$”: $(\forall x \bullet Q \Rightarrow R) \Rightarrow ((\exists x \mid Q \bullet P) \Rightarrow (\exists x \mid R \bullet P))$
“Range monotonicity of $\exists$”: $(\forall x \mid P \bullet Q \Rightarrow R) \Rightarrow ((\exists x \mid Q \bullet P) \Rightarrow (\exists x \mid R \bullet P))$

Introduction and Interchange for $\exists$

(9.28) “$\exists$-Introduction”: $P[x := E] \Rightarrow (\exists x \bullet P)$
(9.29a) “Interchange of quantifications”: $(\exists x \bullet (\forall y \bullet P)) \Rightarrow (\forall y \bullet (\exists x \bullet P))$
(9.30a) “Witness”: $(\exists x \mid R \bullet P) \Rightarrow Q \equiv (\forall x \bullet R \land P \Rightarrow Q)$ — provided: $\neg occurs(\text{‘x’}, \text{‘Q’})$
(9.30b) “Witness”: $(\exists x \bullet P) \Rightarrow Q \equiv (\forall x \bullet P \Rightarrow Q)$ — provided: $\neg occurs(\text{‘x’}, \text{‘Q’})$

Set Theory

(11.3) “Set membership”: $F \in \{ x \mid R \bullet E \} \equiv (\exists x \mid R \bullet F = E)$ — provided: $\neg occurs(\text{‘x’}, \text{‘F’})$
(11.7s) “Simple Membership”: $e \in \{ x \mid P \} \equiv P[x := e]$
(11.7x) “Simple Membership”: $x \in \{ x \mid P \} \equiv P$
(11.7$\forall$) “Simple Membership”: $(\forall x \bullet x \in \{ x \mid P \} \equiv P)$
“Membership in two-element set enumeration”: $x \in \{x, y\}$
“Membership in set enumeration”: $x \in \{ u \mid u = x \lor R \}$ — provided: $\neg occurs(\text{‘u’}, \text{‘x’})$

Set Extensionality and Set Inclusion

(11.4) “Set extensionality” “Set equality” “Extensionality”: $S = T \equiv (\forall e \bullet e \in S \equiv e \in T)$
— provided: $\neg occurs(\text{‘e’}, \text{‘S, T’})$
(11.9) “Simple set comprehension equality”: $\{ x \mid Q \} = \{ x \mid R \} \equiv (\forall x \bullet Q \equiv R)$
(11.13) “Subset” “Definition of $\subseteq$” “Set inclusion”: $S \subseteq T \equiv (\forall e \mid e \in S \bullet e \in T)$
— provided: $\neg occurs(\text{‘e’}, \text{‘S, T’})$
“Subset” “Definition of $\subseteq$” “Set inclusion”: $S \subseteq T \equiv (\forall e \bullet e \in S \Rightarrow e \in T)$
— provided: $\neg occurs(\text{‘e’}, \text{‘S, T’})$
“Subset membership” “Casting”: $X \subseteq Y \Rightarrow (x \in X \Rightarrow x \in Y)$
(11.58) “Reflexivity of $\subseteq$”: $X \subseteq X$
“Reflexivity of $\subseteq$”: $S = T \Rightarrow S \subseteq T$
(11.59) “Transitivity of $\subseteq$”: $X \subseteq Y \Rightarrow (Y \subseteq Z \Rightarrow X \subseteq Z)$
“Flipped transitivity of $\subseteq$”: $Y \subseteq Z \Rightarrow (X \subseteq Y \Rightarrow X \subseteq Z)$
(11.57) “Antisymmetry of $\subseteq$”: $X \subseteq Y \Rightarrow (Y \subseteq X \Rightarrow X = Y)$
“Empty set”: $\{\} = \{ x \mid false \}$
“Empty set”: $x \in \{\} \equiv false$
“Empty set is least” “Bottom set”: $\{\} \subseteq X$
“Universal set”: $U = \{ x \mid true \}$
“Universal set”: $x \in U$
“Universal set is greatest” “Top set”: $X \subseteq U$
(11.56) “Simple set comprehension inclusion”: $\{ x \mid P \} \subseteq \{ x \mid Q \} \equiv (\forall x \bullet P \Rightarrow Q)$

Singleton Sets, Set Complement, Set Union and Intersection

“Singleton set membership”: $x \in \{y\} \equiv x = y$
“Singleton set inclusion”: $\{x\} \subseteq S \equiv x \in S$
“Complement”: $e \in \sim S \equiv \neg (e \in S)$
(11.19) “Self-inverse of complement”: $\sim(\sim S) = S$
“Lower $\sim$ connection for $\subseteq$”: $\sim X \subseteq Y \equiv \sim Y \subseteq X$
“Upper $\sim$ connection for $\subseteq$”: $X \subseteq \sim Y \equiv Y \subseteq \sim X$
“Union”: $e \in S \cup T \equiv e \in S \lor e \in T$
“Intersection”: $e \in S \cap T \equiv e \in S \land e \in T$
“Golden rule for $\cap$ and $\cup$”: $S \cap T = S \equiv T = S \cup T$
“Set inclusion via $\cap$”: $S \subseteq T \equiv S \cap T = S$
“Set inclusion via $\cup$”: $S \subseteq T \equiv S \cup T = T$

Proper Subset

(11.14) “Proper subset” “Definition of $\subset$”: $S \subset T \equiv S \subseteq T \land S \neq T$
(11.61): $S \subset T \equiv S \subseteq T \land \neg (T \subseteq S)$
(11.61): $S \subset T \equiv S \subseteq T \land \neg (T \subseteq S)$
(11.63) “Inclusion in terms of $\subset$”: $S \subseteq T \equiv S \subset T \lor S = T$
(11.70) “Transitivity of $\subseteq$ with $\subset$”: $X \subseteq Y \Rightarrow (Y \subset Z \Rightarrow X \subset Z)$
(11.70) “Transitivity of $\subseteq$ with $\subset$”: $X \subseteq Y \Rightarrow (Y \subset Z \Rightarrow X \subset Z)$

Set Difference and Relative Pseudo-complement

(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): $S - (T \cup U) = (S - T) \cap (S - U)$
“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 ⇨”: $A ⇨ B = \sim A \cup B$
“Pseudocomplement of union”: $(A \cup B) ⇨ C = (A ⇨ C) \cap (B ⇨ C)$
“Monotonicity of ⇨”: $B \subseteq C \Rightarrow A ⇨ B \subseteq A ⇨ C$

Cartesian Products of Sets; Relationship

(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’”: $\mathrm{snd}\ \langle x, y\rangle = y$
“Membership in $\times$”: $p \in S \times T \equiv \mathrm{fst}\ p \in S \land \mathrm{snd}\ p \in T$
(14.4) “Membership in $\times$”: $\langle x, y\rangle \in S \times T \equiv x \in S \land y \in T$
(14.5) “Membership in swapped $\times$”: $\langle x, y\rangle \in S \times T \equiv \langle y, x\rangle \in T \times S$
(14.6) “Empty factor in $\times$”: $S = \{\} \Rightarrow S \times T = \{\}$

“Definition of $\leftrightarrow$”: $A \leftrightarrow B = \mathbb{P}(A \times B)$
“Infix relationship” “Definition of ‘_⦇_⦈_’”: $a ⦇ R ⦈ b \equiv \langle a, b\rangle \in R$
“Relation extensionality”: $R = S \equiv (\forall x \bullet (\forall y \bullet x ⦇ R ⦈ y \equiv x ⦇ S ⦈ y))$ — provided: $\neg occurs$(‘x, y’, ‘R, S’)
“Relation inclusion”: $R \subseteq S \equiv (\forall x \bullet (\forall y \bullet x ⦇ R ⦈ y \Rightarrow x ⦇ S ⦈ y))$ — provided: $\neg occurs$(‘x, y’, ‘R, S’)
“Relation inclusion”: $R \subseteq S \equiv (\forall x \bullet (\forall y \mid x ⦇ R ⦈ y \bullet x ⦇ S ⦈ y))$ — provided: $\neg occurs$(‘x, y’, ‘R, S’)
“Relation inclusion”: $R \subseteq S \equiv (\forall x, y \mid x ⦇ R ⦈ y \bullet x ⦇ S ⦈ y)$ — provided: $\neg occurs$(‘x, y’, ‘R, S’)

Set Operations used as Relation Operations

“Relation union”: $a ⦇ R \cup S ⦈ b \equiv a ⦇ R ⦈ b \lor a ⦇ S ⦈ b$
“Relation intersection”: $a ⦇ R \cap S ⦈ b \equiv a ⦇ R ⦈ b \land a ⦇ S ⦈ b$
“Relation difference”: $a ⦇ R - S ⦈ b \equiv a ⦇ R ⦈ b \land \neg (a ⦇ S ⦈ b)$
“Relation pseudocomplement”: $a ⦇ R ⇨ S ⦈ b \equiv a ⦇ R ⦈ b \Rightarrow a ⦇ S ⦈ b$
“Relation complement”: $a ⦇ \sim R ⦈ b \equiv \neg (a ⦇ R ⦈ b)$
“Empty relation”: $a ⦇ \{\} ⦈ b \equiv \mathit{false}$
“Universal relation”: $(\forall A : \mathrm{Type} \bullet (\forall B : \mathrm{Type} \bullet a ⦇ A \times B ⦈ b))$
“Singleton relation”: $a_1 ⦇ \{\langle a_2, b_2\rangle\} ⦈ b_1 \equiv a_1 = a_2 \land b_1 = b_2$
“Singleton relation inclusion”: $\{\langle a, b\rangle\} \subseteq R \equiv a ⦇ R ⦈ b$

Relation-specific Operations

“Relation converse” “Relationship via $\breve{}$”: $y ⦇ R\breve{} ⦈ x \equiv x ⦇ R ⦈ y$
“Relation composition”: $a ⦇ R ⨾ S ⦈ c \equiv (\exists b \bullet a ⦇ R ⦈ b \land b ⦇ S ⦈ c)$
“Identity relation” “Relationship via ‘Id’”: $x ⦇ \mathrm{Id} ⦈ y \equiv x = y$

Sequences

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

Sequence Membership $\in$, Snoc $\triangleright$

“Membership in ϵ”: $x \in \epsilon \equiv \mathit{false}$
“Membership in $\triangleleft$”: $x \in y \triangleleft ys \equiv x = y \lor x \in ys$
(13.12) “Definition of $\triangleright$” “Definition of $\triangleright$ for ϵ”: $\epsilon \triangleright a = a \triangleleft \epsilon$
(13.13) “Definition of $\triangleright$” “Definition of $\triangleright$ for $\triangleleft$”: $(a \triangleleft s) \triangleright b = a \triangleleft (s \triangleright b)$
(13.14) “Snoc is not empty”: $xs \triangleright x \neq \epsilon$
“Snoc is not empty”: $xs \triangleright x = \epsilon \equiv \mathit{false}$
(13.15) “Cancellation of $\triangleright$”: $xs \triangleright x = ys \triangleright y \equiv xs = ys \land x = y$
(13.16) “Membership in $\triangleright$”: $x \in ys \triangleright z \equiv x \in ys \lor x = z$

Concatenation

(13.17) “Left-identity of $\frown$” “Definition of $\frown$ for ϵ”: $\epsilon \frown ys = ys$
(13.18) “Mutual associativity of $\triangleleft$ with $\frown$” “Definition of $\frown$ for $\triangleleft$”: $(x \triangleleft xs) \frown ys = x \triangleleft (xs \frown ys)$
(13.19) “Right-identity of $\frown$”: $xs \frown \epsilon = xs$
(13.20) “Associativity of $\frown$”: $(xs \frown ys) \frown zs = xs \frown (ys \frown zs)$
(13.21) “Membership in $\frown$”: $x \in ys \frown zs \equiv x \in ys \lor x \in zs$
(13.22) “Mutual associativity of $\frown$ with $\triangleright$”: $(xs \frown ys) \triangleright z = xs \frown (ys \triangleright z)$
(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”: $\neg (x \triangleleft xs \subseteq \epsilon)$
(13.27) “Subsequence anchored at head”: $x \triangleleft ys \subseteq x \triangleleft zs \equiv ys \subseteq zs$
(13.28) “Subsequence without head”: $x \neq y \Rightarrow (x \triangleleft xs \subseteq y \triangleleft ys \equiv x \triangleleft xs \subseteq ys)$
(13.29) “Proper subsequence” “Definition of $\subset$”: $xs \subset ys \equiv xs \subseteq ys \land xs \neq ys$
(13.30) “Reflexivity of $\subseteq$”: $xs \subseteq xs$
(13.31) “Cons $\subseteq$-expands”: $ys \subseteq x \triangleleft ys$
(13.33) “Subsequence of ϵ”: $xs \subseteq \epsilon \equiv xs = \epsilon$
(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”: $\mathrm{isprefix}\ (x \triangleleft xs)\ \epsilon \equiv \mathit{false}$
(13.38) “Prefix” “Cons prefix”: $\mathrm{isprefix}\ (x \triangleleft xs)\ (y \triangleleft ys) \equiv x = y \land \mathrm{isprefix}\ xs\ ys$

(13.39) “Segment” “Segment of ϵ”: $\mathrm{isseg}\ xs\ \epsilon \equiv xs = \epsilon$
(13.40) “Segment” “Segment of $\triangleleft$”: $\mathrm{isseg}\ xs\ (y \triangleleft ys) \equiv \mathrm{isprefix}\ xs\ (y \triangleleft ys) \lor \mathrm{isseg}\ xs\ ys$

Abstract Relation Algebra

"Reflexivity of ⊆": $R \subseteq R$
"Transitivity of ⊆": $Q \subseteq R \Rightarrow R \subseteq S \Rightarrow Q \subseteq S$
"Antisymmetry of ⊆": $R \subseteq S \Rightarrow S \subseteq R \Rightarrow R = S$
"Transitivity of ⊆": $Q \subseteq R \Rightarrow R \subseteq S \Rightarrow Q \subseteq S$
"Flipped Transitivity of ⊆": $R \subseteq S \Rightarrow Q \subseteq R \Rightarrow Q \subseteq S$
"Reflexivity of ⊆": $R = S \Rightarrow R \subseteq S$
"Mutual inclusion": $R = S \;\equiv\; R \subseteq S \land S \subseteq R$
"Opposite inclusion": $R \supseteq S \;\equiv\; S \subseteq R$
"Indirect Relation Equality from above": $Q = R \;\equiv\; (\forall\, S \bullet Q \subseteq S \;\equiv\; R \subseteq S\,)$
"Indirect Relation Equality from below": $Q = R \;\equiv\; (\forall\, S \bullet S \subseteq Q \;\equiv\; S \subseteq R\,)$
"Indirect Relation Inclusion from above": $Q \subseteq R \;\equiv\; (\forall\, S \bullet R \subseteq S \Rightarrow Q \subseteq S\,)$
"Indirect Relation Inclusion from below": $Q \subseteq R \;\equiv\; (\forall\, S \bullet S \subseteq Q \Rightarrow S \subseteq R\,)$

Composition

"Associativity of ⨾": $(Q ⨾ R) ⨾ S = Q ⨾ (R ⨾ S)$
"Monotonicity of ⨾": $P \subseteq Q \Rightarrow R \subseteq S \Rightarrow P ⨾ R \subseteq Q ⨾ S$
"Monotonicity of ⨾": $Q \subseteq R \Rightarrow Q ⨾ S \subseteq R ⨾ S$
"Monotonicity of ⨾": $R \subseteq S \Rightarrow Q ⨾ R \subseteq Q ⨾ S$
"Identity of ⨾": $\mathrm{Id} ⨾ R = R$
"Identity of ⨾": $R ⨾ \mathrm{Id} = R$

Converse

"Self-inverse of ˘": $(R\,\breve{}\,)\,\breve{} = R$
"Cancellation of ˘": $R\,\breve{} = S\,\breve{} \;\equiv\; R = S$
"Monotonicity of ˘": $R \subseteq S \Rightarrow R\,\breve{} \subseteq S\,\breve{}$
"Isotonicity of ˘": $R \subseteq S \;\equiv\; R\,\breve{} \subseteq S\,\breve{}$
"Converse of 'Id'": $\mathrm{Id}\,\breve{} = \mathrm{Id}$
"Converse of ⨾": $(R ⨾ S)\,\breve{} = S\,\breve{} ⨾ R\,\breve{}$

Homogeneous Relation Properties

"Definition of reflexivity": is-reflexive $R \;\equiv\; \mathrm{Id} \subseteq R$
"Definition of symmetry": is-symmetric $R \;\equiv\; R\,\breve{} \subseteq R$
"Definition of transitivity": is-transitive $R \;\equiv\; R ⨾ R \subseteq R$
"Definition of idempotency": is-idempotent $R \;\equiv\; R ⨾ R = R$
"Definition of equivalence":
is-equivalence $R \;\equiv\;$ is-reflexive $R \land$ is-symmetric $R \land$ is-transitive R
"Definition of preorder": is-preorder $R \;\equiv\;$ is-reflexive $R \land$ is-transitive R
"Definition of symmetry": is-symmetric $R \;\equiv\; R\,\breve{} = R$

Heterogeneous Relation Properties

"Definition of univalence": is-univalent $R \;\equiv\; R\,\breve{} ⨾ R \subseteq \mathrm{Id}$
"Definition of totality": is-total $R \;\equiv\; \mathrm{Id} \subseteq R ⨾ R\,\breve{}$
"Definition of injectivity": is-injective $R \;\equiv\; R ⨾ R\,\breve{} \subseteq \mathrm{Id}$
"Definition of surjectivity": is-surjective $R \;\equiv\; \mathrm{Id} \subseteq R\,\breve{} ⨾ R$
"Definition of mappings": is-mapping $R \;\equiv\;$ is-univalent $R \land$ is-total R
"Definition of bijectivity": is-bijective $R \;\equiv\;$ is-injective $R \land$ is-surjective R
"Definition of mappings": is-mapping $R \;\equiv\; R\,\breve{} ⨾ R \subseteq \mathrm{Id} \land \mathrm{Id} \subseteq R ⨾ R\,\breve{}$
"Definition of bijectivity": is-bijective $R \;\equiv\; R ⨾ R\,\breve{} \subseteq \mathrm{Id} \land \mathrm{Id} \subseteq R\,\breve{} ⨾ R$

Relation Algebra: 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 ∩": $Q \cap R = R \cap Q$
"Associativity of ∩": $(Q \cap R) \cap S = Q \cap (R \cap S)$
"Idempotency of ∩": $R \cap R = R$
"Monotonicity of ∩": $Q \subseteq R \Rightarrow Q \cap S \subseteq R \cap S$
"Inclusion via ∩": $Q \subseteq R \;\equiv\; Q \cap R = Q$
"Sub-distributivity of ⨾ over ∩": $Q ⨾ (R \cap S) \subseteq Q ⨾ R \cap Q ⨾ S$
"Sub-distributivity of ⨾ over ∩": $(Q \cap R) ⨾ S \subseteq Q ⨾ S \cap R ⨾ S$
"Converse of ∩": $(R \cap S)\,\breve{} = R\,\breve{} \cap S\,\breve{}$
"Dedekind rule": $Q ⨾ R \cap S \subseteq (Q \cap S ⨾ R\,\breve{}\,) ⨾ (R \cap Q\,\breve{} ⨾ S)$
"Modal rule": $Q ⨾ R \cap S \subseteq (Q \cap S ⨾ R\,\breve{}\,) ⨾ R$
"Modal rule": $Q ⨾ R \cap S \subseteq Q ⨾ (R \cap Q\,\breve{} ⨾ S)$
"Hesitation": $R \subseteq R ⨾ R\,\breve{} ⨾ R$

Relation Algebra: 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 ∪": $Q \subseteq R \Rightarrow Q \cup S \subseteq R \cup S$
"Inclusion via ∪": $Q \subseteq R \;\equiv\; Q \cup R = R$
"Distributivity of ⨾ over ∪": $Q ⨾ (R \cup S) = Q ⨾ R \cup Q ⨾ S$
"Distributivity of ⨾ over ∪": $(Q \cup R) ⨾ S = Q ⨾ S \cup R ⨾ S$
"Union of converses": $R\,\breve{} \cup S\,\breve{} \subseteq (R \cup S)\,\breve{}$
"Converse of ∪": $(R \cup S)\,\breve{} = R\,\breve{} \cup S\,\breve{}$
"Absorption of ∪ by ∩": $Q \cap (Q \cup R) = Q$
"Absorption of ∩ by ∪": $Q \cup (Q \cap R) = Q$
"Distributivity of ∩ over ∪": $Q \cap (R \cup S) = (Q \cap R) \cup (Q \cap S)$
"Distributivity of ∪ over ∩": $Q \cup (R \cap S) = (Q \cup R) \cap (Q \cup S)$

Least Elements in the Inclusion Order

"Least relation": $\bot \subseteq R$
"Inclusion in ⊥": $R \subseteq \bot \;\equiv\; R = \bot$
"Zero of ∩": $\bot \cap R = \bot$
"Identity of ∪": $\bot \cup R = R$
"Converse of ⊥": $\bot\,\breve{} = \bot$
"Left-zero of ⨾": $\bot ⨾ R = \bot$
"Right-zero of ⨾": $R ⨾ \bot = \bot$

Greatest Elements in the Inclusion Order

"Greatest relation": $R \subseteq \top$
"Inclusion of ⊤": $\top \subseteq R \;\equiv\; R = \top$
"Identity of ∩": $\top \cap R = R$
"Zero of ∪": $\top \cup R = \top$
"Converse of ⊤": $\top\,\breve{} = \top$

Relation Algebra: Complement

"Characterisation of ~": $S \cap R = \bot \wedge S \cup R = \top \ \equiv\ S = {\sim} R$
"Characterisation of ~": ${\sim} R \cap R = \bot \wedge {\sim} R \cup R = \top$
"Self-inverse of ~": ${\sim} ({\sim} R) = R$
"Antitonicity of ~": $Q \subseteq R \Rightarrow {\sim} R \subseteq {\sim} Q$
"Anti-isotonicity of ~": $Q \subseteq R \ \equiv\ {\sim} R \subseteq {\sim} Q$
"~ connection": ${\sim} Q \subseteq R \ \equiv\ {\sim} R \subseteq Q$
"~ connection": $Q \subseteq {\sim} R \ \equiv\ R \subseteq {\sim} Q$
"Cancellation of ~": ${\sim} Q = {\sim} R \ \equiv\ Q = R$
"Equality with ~": $Q = {\sim} R \ \equiv\ R = {\sim} Q$

"Complement of ⊤": ${\sim} \top = \bot$
"Converse of complement inclusion": $({\sim} R)^{\smile} \subseteq {\sim} R^{\smile}$
"Converse of ~" "Complement of converse" "Complement of ˘": $({\sim} R)^{\smile} = {\sim} R^{\smile}$
"De Morgan for ∩": ${\sim} (Q \cap R) = {\sim} Q \cup {\sim} R$
"De Morgan for ∪": ${\sim} (Q \cup R) = {\sim} Q \cap {\sim} R$
"Inclusion via intersection with complement" "Inclusion via ∩ ~": $R \subseteq S \ \equiv\ R \cap {\sim} S \subseteq \bot$
"Inclusion via intersection with complement" "Inclusion via ∩ ~": $R \subseteq S \ \equiv\ R \cap {\sim} S = \bot$
"Contrapositive of ⊆ with ∩": $Q \cap R \subseteq S \ \equiv\ Q \cap {\sim} S \subseteq {\sim} R$
"Schröder": $Q \mathbin{;} R \subseteq S \ \equiv\ Q^{\smile} \mathbin{;} {\sim} S \subseteq {\sim} R$
"Schröder": $Q \mathbin{;} R \subseteq S \ \equiv\ {\sim} S \mathbin{;} R^{\smile} \subseteq {\sim} Q$

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!)

These can also be used for proving theorems of shape

$$\forall\ var : Ty \bullet P$$

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`:
        ?
```

Facts that can be shown by "Evaluation"

Only where Evaluation is enabled:

Fact `6 · 7 = 42`

Assuming the Antecedent

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

```
Assuming `p` and using with ...:
    ?
  ... Assumption `p` ...
    ?
```

Case Analysis

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

Subproofs

```
    ?
  ≡⟨ Subproof for `...`:
        ⟪ proof indented as far as needed
          to avoid parse error! ⟫
    ⟩
    ?
```

Nested subproofs currently may need to be indented even further than first-level subproofs!

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`:
        ?
```

Side Proofs

```
Side proof for `P`:
  ?
Continuing with goal `?`:
    ?
  ... local property `P` ...
    ?
```

<u>Disabling Hints Producing Time-outs</u>

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 edit and command 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.

> ONLY if you are logged in via Avenue:
> `Ctrl-s` saves the notebook on the server.
> **To be safest, use in command mode, e.g. after clicking on the area of a code box where the line number would be displayed.**
> **Check the pop-up whether it is the CalcCheck-Web pop-up saying "…Notebook saved to …".**
> (Links for reloading the last three saved versions are displayed when you view the notebook again.)

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

`Esc` enters command mode

`Alt-i` ***or*** `Alt-SPACE` 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 `Shift`.

Some important symbols:

Symbol	Key sequence(s)
$\equiv$	`\equiv`, `\==`
$\not\equiv$	`\nequiv`
$\neg$	`\lnot`
$\land$	`\land`
$\lor$	`\lor`
$\Rightarrow$	`\implies`, `\=>`
$\Leftarrow$	`\follows`
$\neq$	`\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`
$\bigcup$	`\bigunion`
$\bigcap$	`\bigintersection`
$\bot$	`\bot`
$\top$	`\top`
⇨	`\pseudocompl`
$\subseteq$	`\subseteq`, `\(=`
$\supseteq$	`\supseteq`, `\)=`
$\subset$	`\subset`
$\supset$	`\supset`
$\mathbf{U}$	`\universe`

Symbol	Key sequence(s)
$\times$	`\times`
$\leftrightarrow$	`\rel`
⦇	`\lrel`, `\((`, `\([`
⦈	`\rrel`, `\))`, `\]]`
⨾	`\rcomp`, `\fcomp`, `\;;`
$\breve{}$	`\converse`, `\u{}`
$^+$	`\^+`
*	`*`
$/$	`\lres`
$\backslash$	`\rres`
ϵ	`\eps`, `\emptyseq`
$\triangleleft$	`\cons`
$\triangleright$	`\snoc`
$\frown$	`\catenate`

Contents