2DM3 2018 — Midterm 2 Theorem List

Equivalence, Negation and Inequivalence

"Definition of ≡": $(p \equiv q) = (p = q)$
(3.2) "Symmetry of ≡": ?
(3.3) "Identity of ≡": ?
(3.5) "Reflexivity of ≡": $p \equiv p$
(3.9) "Commutativity of ¬ with ≡" "Distributivity of ¬ over ≡": ?
(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): $\neg p \equiv (p \equiv \text{false})$

Disjunction and Conjunction

(3.32): ?
(3.35) "Golden rule": ?
(3.48): ?
(3.49) "Semi-distributivity of ∧ over ≡": ?
(3.50) "Strong Modus Ponens": ?
(3.51) "Replacement": $(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \wedge (r \equiv q)$
(3.52) "Alternative definition of ≡": ? q) ∨ (¬ p ∧ ¬ q))
(3.53) "Exclusive or" "Alternative definition of ≢": ?

Implication

(3.57) "Definition of ⇒": ?
(3.58) "Definition of ⇐" "Consequence": ?
(3.59) "Definition of ⇒": ?
(3.60) "Definition of ⇒": ?
(3.61) "Contrapositive": ?
(3.62): $p \Rightarrow (q \equiv r) \equiv (p \wedge q \equiv p \wedge r)$
(3.63) "Distributivity of ⇒ over ≡": ?
(3.64) "Self-distributivity of ⇒": ?
(3.65) "Shunting": ?
(3.66): $p \wedge (p \Rightarrow q) \equiv p \wedge q$
(3.67): $p \wedge (q \Rightarrow p) \equiv p$
(3.68): $p \vee (p \Rightarrow q) \equiv \text{true}$
(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 ⇒": ?
(3.72) "Right-zero of ⇒": ?
(3.73) "Left-identity of ⇒": ?
"Definition of ¬" (3.74): ?
(3.75) "ex falso quodlibet": ?
(3.76a) "Weakening": ?
(3.76a) "Weakening": ?
(3.76b) "Weakening": ?
(3.76c) "Weakening": ?
(3.76d) "Weakening": ?
(3.76e) "Weakening": ?
"Reflexivity of ⇒": ?
(3.77) "Modus ponens": ?
(3.78) "Case analysis": ?
(3.79) "Case analysis": ?
(3.80) "Mutual implication": ?
(3.81) "Antisymmetry of ⇒": ?
(3.82a) "Transitivity of ⇒": ?
(3.82b) "Transitivity of ⇒": ?
(3.82c) "Transitivity of ⇒": ?
"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'": $p \Rightarrow E[z := p] \equiv p \Rightarrow E[z := \text{true}]$
(3.85b) "Replace by 'true'": $q \wedge p \Rightarrow E[z := p] \equiv q \wedge p \Rightarrow E[z := \text{true}]$
(3.85c) "Replace by 'false'": $\neg p \Rightarrow E[z := p] \equiv \neg p \Rightarrow E[z := \text{false}]$
(3.85e) "Replace by 'true'": $p \Rightarrow E[z := p] = E[z := \text{true}]$
(3.86a) "Replace by 'false'": $E[z := p] \Rightarrow p \equiv E[z := \text{false}] \Rightarrow p$
(3.86b) "Replace by 'false'": $E[z := p] \Rightarrow p \vee q \equiv E[z := \text{false}] \Rightarrow p \vee q$
(3.87) "Replace by 'true'": $p \wedge E[z := p] \equiv p \wedge E[z := \text{true}]$
(3.88) "Replace by 'false'": $p \vee E[z := p] \equiv p \vee E[z := \text{false}]$

Monotonicity with Respect to Implication

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

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 ∑": $(\sum x \mid \text{false} \bullet E) = 0$
(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 ∑": $(\forall x \bullet Q \wedge R \equiv \text{false}) \Rightarrow (\sum x \mid Q \vee R \bullet E) = (\sum x \mid Q \bullet E) + (\sum x \mid R \bullet E)$
(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: ¬*occurs*('x', 'a')
"Zero $\sum$ body": $(\sum x \mid R \bullet 0) = 0$

Manipulating Ranges over $\mathbb{N}$

"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" "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: ¬*occurs*('i', 'n')
"Split off term" "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: ¬*occurs*('i', '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: ¬*occurs*('i', '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: ¬*occurs*('x', 'P')
(9.6): $P \lor (\forall x \bullet \neg R) \equiv (\forall x \mid R \bullet P)$ — provided: ¬*occurs*('x', 'P')
"Distributivity of $\Rightarrow$ over $\forall$": $P \Rightarrow (\forall x \mid R \bullet Q) \equiv (\forall x \mid R \bullet P \Rightarrow Q)$ — provided: ¬*occurs*('x', '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: ¬*occurs*('x', 'P')
(9.8) "True $\forall$ body": $(\forall x \mid R \bullet true)$
"Introducing fresh $\forall$": $P \Rightarrow (\forall x \mid R \bullet P)$ — provided: ¬*occurs*('x', '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": ?
"Fresh $\forall$": $P \equiv (\forall x \bullet P)$ — provided: ¬*occurs*('x', '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: ¬*occurs*('x', 'P')
(9.22): $P \land (\exists x \bullet R) \equiv (\exists x \mid R \bullet P)$ — provided: ¬*occurs*('x', '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: ¬*occurs*('x', '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: ¬*occurs*('x', '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": ?
(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: ¬*occurs*('x', 'Q')
(9.30b) "Witness": $(\exists x \bullet P) \Rightarrow Q \equiv (\forall x \bullet P \Rightarrow Q)$ — provided: ¬*occurs*('x', 'Q')

Set Membership Properties

(11.3) "Set membership": ?
(11.7s) "Simple Membership": ?
(11.7x) "Simple Membership": ?
(11.7$\forall$) "Simple Membership": ?
"Membership in two-element set enumeration": ?
"Membership in set enumeration": ?

Set Extensionality and Set Inclusion

(11.4) "Set extensionality" "Set equality" "Extensionality": ?
(11.9) "Simple set comprehension equality": ?
(11.13) "Subset" "Definition of $\subseteq$" "Set inclusion": ?
"Subset" "Definition of $\subseteq$" "Set inclusion": ?
"Subset membership" "Casting": ?
(11.58) "Reflexivity of $\subseteq$": ?
"Reflexivity of $\subseteq$": ?
(11.59) "Transitivity of $\subseteq$": ?
"Flipped transitivity of $\subseteq$": ?
(11.57) "Antisymmetry of $\subseteq$": ?
"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": ?
"Singleton set inclusion": ?
"Complement": ?
(11.19) "Self-inverse of complement": ?
"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": ?
"Intersection": ?
"Golden rule for $\cap$ and $\cup$": ?
"Set inclusion via $\cap$": ?
"Set inclusion via $\cup$": ?

Proper Subset

(11.14) “Proper subset” “Definition of ⊂”: ?
(11.61): $S \subset T \equiv S \subseteq T \wedge \neg (T \subseteq S)$
(11.61): $S \subset T \equiv S \subseteq T \wedge \neg (T \subseteq S)$
(11.63) “Inclusion in terms of ⊂”: ?
(11.70) “Transitivity of ⊆ with ⊂”: ?
(11.70) “Transitivity of ⊆ with ⊂”: ?

Set Difference and Relative Pseudo-complement

(11.22) “Set difference”: ?
(11.52): $S \cap (T - S) = \{\}$
(11.54): $S - (T \cup U) = (S - T) \cap (S - U)$
“Characterisation of ⇨”: $S \subseteq A \Rightarrow B \equiv S \cap A \subseteq B$
“Membership in ⇨”: $x \in A \Rightarrow B \equiv x \in A \Rightarrow x \in B$
“Definition of ⇨”: $A \Rightarrow B = \sim A \cup B$
“Pseudocomplement of union”: $(A \cup B) \Rightarrow C = (A \Rightarrow C) \cap (B \Rightarrow C)$
“Monotonicity of ⇨”: $B \subseteq C \Rightarrow A \Rightarrow B \subseteq A \Rightarrow C$

Relations via Set Theory

“Definition of ↔”: ?

“Infix relationship” “Definition of ‘_⦇_⦈_’”: ?
“Relation extensionality”: ?
“Relation inclusion”: ?
“Relation inclusion”: ?
“Relation inclusion”: ?

Set Operations used as Relation Operations

“Relation union”: ?
“Relation intersection”: ?
“Relation difference”: ?
“Relation pseudocomplement”: $a ⦇ R ⇨ S ⦈ b \equiv a ⦇ R ⦈ b \Rightarrow a ⦇ S ⦈ b$
“Relation complement”: ?
“Empty relation”: ?
“Universal relation”: $(\forall A : \mathrm{Type} \bullet (\forall B : \mathrm{Type} \bullet a ⦇ A \times B ⦈ b))$
“Singleton relation”: ?
“Singleton relation inclusion”: ?

Relation-specific Operations

“Relation converse” “Relationship via ˘”: ?
“Relation composition”: ?
“Identity relation” “Relationship via ‘Id’”: ?

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` • 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` ...
    ?
```

```
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` ...
    ?
```

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 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.
(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)
⇒	`\implies`, `\=>`
⇐	`\follows`
≢	`\nequiv`
≠	`\neq`
∀	`\forall`
∃	`\exists`
∑	`\sum`
∏	`\product`
|	`\with`
•	`\spot`
↓	`\min`
↑	`\max`
𝔹	`\BB`, `\bool`
ℕ	`\NN`, `\nat`
ℤ	`\ZZ`, `\int`
∈	`\in`
ℙ	`\PP`, `\powerset`
∪	`\union`
∩	`\intersection`
⇨	`\pseudocompl`
⊆	`\subseteq`
⊂	`\subset`
U	`\universe`
×	`\times`
↔	`\rel`
⦇	`\lrel`, `\((`, `\([`
⦈	`\rrel`, `\))`, `\])`
⨾	`\rcomp`, `\fcomp`, `\;;`
˘	`\converse`, `\u{}`
╱	`\lres`
╲	`\rres`
ϵ	`\eps`, `\emptyseq`
◁	`\cons`
▷	`\snoc`
⌢	`\catenate`