5. Theorems about Fundamental Concepts (ch. 3)

Review of key properties (Proof Logic handout)

Unless properties—sample proofs

Conjunction

p58 $$\frac{p \textbf{ unless } q \text{ , } p' \textbf{ unless } q'}{(p \wedge p') \textbf{ unless } (p \wedge q') \vee (p' \wedge q) \vee (q \wedge q')}$$

$\{p \wedge \neg q\}$ s $\{p \vee q\}$ definition
$\{p' \wedge \neg q'\}$ s $\{p' \vee q'\}$ definition

combining the two above we get

$\{(p \wedge \neg q) \wedge (p' \wedge \neg q')\}$ LHS1
s
$\{(p \vee q) \wedge (p' \vee q')\}$ RHS1

but we must prove

$\{(p \wedge p') \wedge \neg((p \wedge q') \vee (p' \wedge q) \vee (q \wedge q'))\}$ LHS
s
$\{(p \wedge p') \vee ((p \wedge q') \vee (p' \wedge q) \vee (q \wedge q'))\}$ RHS

and we notice that

LHS $\Rightarrow$ LHS1
$(p \wedge p') \wedge \neg((p \wedge q') \vee (p' \wedge q) \vee (q \wedge q')) \Rightarrow (p \wedge \neg q) \wedge (p' \wedge \neg q')$
$(p \wedge p') \wedge \neg(p \wedge q') \wedge \neg(p' \wedge q) \wedge \neg(q \wedge q') \Rightarrow (p \wedge \neg q) \wedge (p' \wedge \neg q')$ clearly true

RHS1 $\Rightarrow$ RHS
$(p \vee q) \wedge (p' \vee q') \Rightarrow (p \wedge p') \vee ((p \wedge q') \vee (p' \wedge q) \vee (q \wedge q'))$ distributivity

Ensures properties—sample proofs

Assuming

p64 $$\frac{p \vee q \textbf{ ensures } r}{p \textbf{ ensures } q \vee r}$$

prove

p64 $$\frac{p \textbf{ ensures } q \vee r}{p \wedge \neg q \textbf{ ensures } q \vee r}$$

p **ensures** $q \vee r$	given
$(p \wedge q) \vee (p \wedge \neg q)$ **ensures** $q \vee r$	calculus
$(p \wedge \neg q)$ **ensures** $q \vee r \vee (p \wedge q)$	due to assumed property above
$(p \wedge \neg q)$ **ensures** $q \vee r$	$q \vee (p \wedge q) \equiv q$

Leads-to properties—sample proofs

Induction

p72 $$\frac{\langle \forall m : m \in W :: p \wedge M = m \rightarrow (p \wedge M < m) \vee q \rangle}{p \rightarrow q}$$

where W is a <u>well-founded set</u> under < (no infinitely decreasing sequence)
M is a <u>metric</u> or <u>variant function</u>: M : state → W

1. Principle of complete mathematical induction

$$\frac{\langle \forall m :: \frac{\langle \forall n : n<m :: A(n) \rangle}{A(m)} \rangle}{\langle \forall m :: A(m) \rangle}$$

2. Let
`A(m) ≡ p(m) → q where p(m) ≡ p ∧ (M=m)`

3. We know that

$$\frac{\langle \forall m :: \frac{\langle \forall n : n<m :: p(n) \rightarrow q \rangle}{p(m) \rightarrow q} \rangle}{\langle \forall m :: p(m) \rightarrow q \rangle}$$

4. For any value of m, establish the conclusion part of the premise
`p(m) → q`

$\langle \forall n : n<m :: p(n) \rightarrow q \rangle$	premise	(1)
$\langle \exists n : n<m :: p(n) \rangle \rightarrow q$	disjunction	(2)
$q \rightarrow q$	implication	(3)
$\langle \exists n : n<m :: p(n) \rangle \vee q \rightarrow q$	finite disjunction on (2,3)	(4)
$p(m) \rightarrow \langle \exists n : n<m :: p(n) \rangle \vee q$	replace M<m by n<m in inductive premise	(5)

$\langle \forall m : m \in W :: p \wedge M = m \rightarrow (p \wedge M < m) \vee q \rangle$
$\langle \forall m : m \in W :: p(m) \rightarrow (p \wedge M < m) \vee q \rangle$
$p(m) \rightarrow (p \wedge M < m) \vee q$
$p(m) \rightarrow \langle \exists n : n{=}M :: p \wedge n < m \rangle \vee q$
$p(m) \rightarrow \langle \exists n : n < m :: p \wedge n{=}M \rangle \vee q$
$p(m) \rightarrow \langle \exists n : n < m :: p(n) \rangle \vee q$

$p(m) \rightarrow q$	transitivity (5,4)	(6)

- The premise of the mathematical induction holds.

5. Show that the conclusion of the mathematical induction gives us the desired result
$p \rightarrow q$

$\langle \forall m :: p(m) \rightarrow q \rangle$	the conclusion of the induction in 3	(1)
$\langle \exists m :: p(m) \rangle \rightarrow q$	disjunction	(2)
$\langle \exists m :: p \wedge (M{=}m) \rangle \rightarrow q$	definition of p(m)	(3)
$p \wedge \langle \exists m :: (M{=}m) \rangle \rightarrow q$	m not present in p	(4)
$p \rightarrow q$	M always assumes some value	(5)

Progress-Safety-Progress (PSP)

p65 $$\frac{p \rightarrow q,\ r\ \textbf{unless}\ b}{p \wedge r \rightarrow (q \wedge r) \vee b}$$

Proof method

- Induction on the structure of the proof, e.g., <u>length</u>.
- We consider the number of inference rules applied in proving $p \rightarrow q$

  <u>Base case</u>: length 1 $\equiv$ prove for p **ensures** q

  <u>Inductive step</u>: length greater than 1

  $\equiv$ last step requires us to apply transitivity

  $\equiv$ last step requires us to apply disjunction
- When several $\rightarrow$ appear in the premise we need to combine the lengths!

Base case

p **ensures** q	premise	(1)
r **unless** b	premise	(2)
$p \wedge r$ **ensures** $(p \wedge b) \vee (r \wedge q) \vee (q \wedge b)$	conjunction on ensures	(3)
$p \wedge r$ **ensures** $(r \wedge q) \vee (b \wedge (q \vee p))$	calculus	(4)
$p \wedge r$ **ensures** $(r \wedge q) \vee b$	consequence weakening	(5)

Inductive step [transitivity]

$p \rightarrow q'$ and $q' \rightarrow q$ and r **unless** b	assume	(1)
$p \wedge r \rightarrow (q' \wedge r) \vee \mathbf{b}$	inductive assumption	(2)
$q' \wedge r \rightarrow \underline{(q \wedge r) \vee b}$	inductive assumption	(3)
$p \wedge r \rightarrow \underline{((q \wedge r) \vee b)} \vee \mathbf{b}$	cancellation theorem on (2) and (3)	(4)

Inductive step [disjunction]

$\langle \forall m : m \in W :: p'(m) \rightarrow q \rangle$	assume	(1)
$p = \langle \exists m : m \in W :: p'(m) \rangle$	assume	(2)
r **unless** b	premise	(3)
$\langle \forall m : m \in W :: p'(m) \wedge r \rightarrow (q \wedge r) \vee b \rangle$	assume	(4)
$\langle \exists m : m \in W :: p'(m) \wedge r \rangle \rightarrow (q \wedge r) \vee b$	disjunction on (4)	(5)
$\langle \exists m : m \in W :: p'(m) \rangle \wedge r \rightarrow (q \wedge r) \vee b$	m does not appear in r	(6)
$p \wedge r \rightarrow (q \wedge r) \vee b$	definition of p	(7)

Proving bounds on progress

Proof method

- Do not count statements being executed.
- Show that $p \rightarrow q$ in at most n state changes
  - introduce a display function M : states – {0..n}
  - show that each step either establishes q or preserves p and decreases M