Programming Languages: Imperative Program Construction Midterm

Shin-Cheng Mu

Autumn Term, 2022

Notes regarding proofs.

- Proofs in this course are supposed to be carried out via equational reasoning — not by, for example, truth table.
- Proofs need not be too detailed. For example, properties such as symmetry associativity, zero, identity of logical operators (e.g. (3.24), (3.25), (3.36), (3.37), (3.29), (3.30)) are too ubiquitous and can be used without explicit mentioning.
- Questions 1 and 2 are about logic and their proofs out to be carried out in finer details. For other questions, you can skip many steps as long as you can convince me that each step is from an established property. Arithmetic properties (e.g. those regarding $+, -, \times, \leqslant, \geqslant$, etc) are supposed to be known.

1. (10 points) Prove that $\neg\ p \Rightarrow (q \equiv p \vee q)$.

Solution:

$$
\begin{array}{ll}
 & \neg\ p \Rightarrow (q \equiv p \vee q) \\
= & \quad \{\ (3.59)\ \text{defn. of implication, (3.12) double negation}\ \} \\
 & p \vee (q \equiv p \vee q) \\
= & \quad \{\ (3.27)\ \text{distributivity}\ \} \\
 & p \vee q \equiv p \vee p \vee q \\
= & \quad \{\ (3.26)\ \text{idempotency of } (\vee)\ \} \\
 & p \vee q \equiv p \vee q \\
= & \quad \{\ (3.3)\ \} \\
 & \mathit{True}\ .
\end{array}
$$

Alternatively,

$$
\begin{array}{ll}
 & \neg\ p \Rightarrow (q \equiv p \vee q) \\
= & \quad \{\ (3.62)\ \} \\
 & \neg\ p \wedge q \equiv \neg\ p \wedge (p \vee q) \\
= & \quad \{\ (3.44)\ \text{absorption}\ \} \\
 & \neg\ p \wedge q \equiv \neg\ p \wedge q \\
= & \quad \{\ (3.3)\ \} \\
 & \mathit{True}\ .
\end{array}
$$

2. (a) (10 points) Prove (3.78): $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q) \Rightarrow r$.

Solution:

$$
\begin{array}{ll}
 & (p \Rightarrow r) \wedge (q \Rightarrow r) \\
= & \quad \{ \text{ (3.59) defn. of implication } \} \\
 & (\neg\, p \vee r) \wedge (\neg\, q \vee r) \\
= & \quad \{ \text{ (3.45) distributivity } \} \\
 & (\neg\, p \wedge \neg\, q) \vee r \\
= & \quad \{ \text{ (3.47) de Morgan } \} \\
 & \neg\, (p \vee q) \vee r \\
= & \quad \{ \text{ (3.59) defn. of implication } \} \\
 & p \vee q \Rightarrow r \ .
\end{array}
$$

(b) (10 points) Prove that $\{P\}\, S\, \{R\} \wedge \{Q\}\, S\, \{R\} \equiv \{P \vee Q\}\, S\, \{R\}$.

Solution:

$$
\begin{array}{ll}
 & \{P\}\, S\, \{R\} \wedge \{Q\}\, S\, \{R\} \\
= & \quad \{ \text{ definition of Hoare triple } \} \\
 & (P \Rightarrow wp\ S\ R) \wedge (Q \Rightarrow wp\ S\ R) \\
= & \quad \{ \text{ (3.78) } \} \\
 & (P \vee Q) \Rightarrow wp\ S\ R \\
= & \quad \{ \text{ definition of Hoare triple } \} \\
 & \{P \vee Q\}\, S\, \{R\} \ .
\end{array}
$$

3. Given an array X of integers having N elements (with index $0 \mathinner{..} N-1$), where $N \geqslant 0$. Express the following formally:

   (a) (10 points) the maximum of X occurs only once in X;

   (b) (10 points) X is a permutation of $0 \mathinner{..} N-1$.

   Note: The element of X with index i is denoted by $X[i]$. In case you don't know what a permutation is, $[3, 1, 2, 0]$ and $[1, 3, 0, 2]$ are both permutations of $0 \mathinner{..} 3$.

Solution: There are many possible answers. For example

(a) $\langle \#i : 0 \leqslant i < N : X[i] = \langle \uparrow j : 0 \leqslant j < N : X[j] \rangle \rangle = 1$,

(b) $\langle \forall i : 0 \leqslant i < N : 0 \leqslant X[i] < N \wedge \langle \forall j : i < j < N : X[i] \neq X[j] \rangle \rangle$.
Or, $\langle \forall n : 0 \leqslant n < N : \langle \exists i : 0 \leqslant i < N : X[i] = n \rangle \rangle$.

4. (20 points) Denote the following program by *PROG*:

$$
\begin{array}{l}
n_0 := n \\
\textbf{if}\ d > 0 \rightarrow n := n - d \,/\, 2 \\
\ \ \mid\ d < 0 \rightarrow n := n - 1 \\
\textbf{fi}\ ,
\end{array}
$$

where all variables has type *Int* and division is integral division. Calculate $wp\ PROG\ (n < n_0)$. You may assume that all the usual arithmetic properties about integers are known.

Solution: Denote **if** $d > 0 \to n := n - d \,/\, 2 \mid d < 0 \to n := n - 1$ **fi** by IF.

$$
\begin{array}{ll}
 & wp\ (n_0 := n; \mathsf{IF})\ (n < n_0) \\
= & \quad \{\ \text{definition of } wp \text{ (case of sequencing)}\ \} \\
 & wp\ (n_0 := n)\ (wp\ \mathsf{IF}\ (n < n_0)) \\
= & \quad \{\ \text{definition of } wp \text{ (case of } \textbf{if}\text{)}\ \} \\
 & wp\ (n_0 := n)\ ((d > 0 \Rightarrow wp\ (n := n - d \,/\, 2)\ (n < n_0)) \wedge \\
 & \qquad\qquad (d < 0 \Rightarrow wp\ (n := n - 1)\ (n < n_0)) \wedge (d > 0 \vee d < 0)) \\
= & \quad \{\ \text{definition of } wp \text{ (case of assignments), substitution}\ \} \\
 & \\
 & wp\ (n_0 := n)\ ((d > 0 \Rightarrow n - d \,/\, 2 < n_0) \wedge \\
 & \qquad\qquad (d < 0 \Rightarrow n - 1 < n_0) \wedge (d > 0 \vee d < 0)) \\
= & \quad \{\ \text{definition of } wp \text{ (case of assignments), substitution}\ \} \\
 & (d > 0 \Rightarrow n - d \,/\, 2 < n) \wedge \\
 & (d < 0 \Rightarrow n - 1 < n) \wedge (d > 0 \vee d < 0) \\
= & \quad \{\ \text{arithmetics: } n - x < n \equiv x > 0;\ n - 1 < n \equiv \mathit{True}\ \} \\
 & (d > 0 \Rightarrow d \,/\, 2 > 0) \wedge \\
 & (d < 0 \Rightarrow \mathit{True}) \wedge (d > 0 \vee d < 0) \\
= & \quad \{\ \text{integer division: } d \,/\, 2 > 0 \equiv d > 1\ \} \\
 & (d > 0 \Rightarrow d > 1) \wedge \\
 & (d < 0 \Rightarrow \mathit{True}) \wedge (d > 0 \vee d < 0) \\
= & \quad \{\ \text{(3.72) zero of implication; (3.39) identity of } (\wedge)\ \} \\
 & (d > 0 \Rightarrow d > 1) \wedge (d > 0 \vee d < 0) \\
= & \quad \{\ \text{(3.59) defn. of implication}\ \} \\
 & (d \leqslant 0 \vee d > 1) \wedge (d > 0 \vee d < 0) \\
= & \quad \{\ \text{distributivity}\ \} \\
 & (d \leqslant 0 \wedge d > 0) \vee (d \leqslant 0 \wedge d < 0) \vee (d > 1 \wedge d > 0) \vee (d > 1 \wedge d < 0) \\
= & \quad \{\ \text{arithmetics, identity of } (\vee)\ \} \\
 & d < 0 \vee d > 1\ .
\end{array}
$$

5. (a) (20 points) Prove the correctness of the following program:

$$
\begin{array}{l}
\textbf{con}\ N : \mathit{Int}\ \{N \geqslant 0\};\ F : \textbf{array}\ [0..N)\ \textbf{of}\ \mathit{Int} \\
\textbf{var}\ b : \mathit{Bool} \\
\textbf{var}\ n : \mathit{Int} \\
b, n := \mathit{False}, 0 \\
\textbf{do}\ n \neq N \to b := b \vee F[n] = 0 \\
\qquad\qquad\quad n := n + 1 \\
\textbf{od} \\
\{b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle\}
\end{array}
$$

Notes and Hints:

- $F : \textbf{array}\ [0..N)\ \textbf{of}\ \mathit{Int}$ denotes that F is an array having N elements, all of them being Int, with index $0..N-1$.
- You need to have enough properties about n in the invariant to show that the program terminates.
- When dealing with the quantification, you will need the splitting theorem (8.23):

$$\langle \star i : 0 \leqslant i < n + 1 : P \rangle = \langle \star i : 0 \leqslant i < n : P \rangle \star P[i \backslash n]\ ,$$

provided that $0 \leqslant n$.

Solution: We abbreviate $b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle$ to P. The annotated program is:

con $N : Int\ \{N \geqslant 0\}; F :$ **array** $[0..N)$ **of** Int
var $b : Bool$
var $n : Int$

$b, n := False, 0$ -- Pf_0
$\{(b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N, bnd : N - n\}$ -- Pf_2
do $n \neq N \rightarrow \{P \wedge 0 \leqslant n \leqslant N \wedge n \neq N\}$
$b := b \vee F[n] = 0$
$n := n + 1$
$\{P \wedge 0 \leqslant n \leqslant N\}$ -- Pf_3
od
$\{b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle\}$ -- Pf_1

Pf_0.

$$
\begin{array}{ll}
 & ((b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N)[b, n \backslash False, 0] \\
= & (False \equiv \langle \exists i : 0 \leqslant i < 0 : F[i] = 0 \rangle) \wedge 0 \leqslant 0 \leqslant N \\
= & \quad \{ \text{ empty range } \} \\
 & (False \equiv False) \wedge 0 \leqslant N \\
= & 0 \leqslant N \ .
\end{array}
$$

Pf_1. It is immediate that

$$
\begin{array}{l}
(b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge \neg\, (n \neq N) \\
\quad \Rightarrow (b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle) \ .
\end{array}
$$

Pf_2. We certainly have

$$P \wedge 0 \leqslant n \leqslant N \wedge n \neq N \ \ \Rightarrow \ \ N - n \geqslant 0 \ .$$

Furthermore,

$$
\begin{array}{ll}
 & ((N - n < C)[n \backslash n + 1])[b \backslash b \vee F[n] = 0] \\
= & N - (n + 1) < C \\
\Leftarrow & P \wedge 0 \leqslant n \leqslant N \wedge n \neq N \wedge N - n = C \ .
\end{array}
$$

Pf_3.

$$
\begin{array}{ll}
 & ((P \wedge 0 \leqslant n \leqslant N)[n \backslash n + 1])[b \backslash b \vee F[n] = 0] \\
= & (b \vee F[n] = 0 \ \equiv \ \langle \exists i : 0 \leqslant i < n + 1 : F[i] = 0 \rangle) \wedge 0 \leqslant n + 1 \leqslant N \\
\Leftarrow & \quad \{ \ 0 \leqslant n + 1 \Leftarrow 0 \leqslant n \ \} \\
 & (b \vee F[n] = 0 \ \equiv \ \langle \exists i : 0 \leqslant i < n + 1 : F[i] = 0 \rangle) \wedge 0 \leqslant n < N \\
\Leftarrow & \quad \{ \text{ (8.23) split off } i = n \ \} \\
 & (b \vee F[n] = 0 \ \equiv \ \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle \vee F[n] = 0) \wedge 0 \leqslant n < N \\
\Leftarrow & (b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge n \neq N \ .
\end{array}
$$

(b) (10 points) Prove the correctness of the following program:

con $N : Int\ \{N \geqslant 0\}; F : \mathbf{array}\ [0..N)\ \mathbf{of}\ Int$
var $b : Bool$
var $n : Int$

$b, n := False, 0$
do $n \neq N \wedge \neg\, b \rightarrow b := F[n] = 0$
$\qquad\qquad\qquad\qquad\quad n := n + 1$
od
$\{b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle\}$

Notes and Hints:

- Proofs of termination is similar to that proved in Problem 5(a). To save your time, you *do not* need to prove the termination of the loop.
- You might find the property proved in Problem 1 useful.

Solution: We abbreviate $b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle$ to P. It turns out that we may use the same invariant as that in Problem 5(a). The annotated program is:

con $N : Int\ \{N \geqslant 0\}; F : \mathbf{array}\ [0..N)\ \mathbf{of}\ Int$
var $b : Bool$
var $n : Int$

$b, n := False, 0$ -- Pf_0
$\{(b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N, bnd : N - n\}$
do $n \neq N \wedge \neg\, b \rightarrow \{P \wedge 0 \leqslant n \leqslant N \wedge n \neq N \wedge \neg\, b\}$
$\qquad\qquad\qquad\quad b := F[n] = 0$
$\qquad\qquad\qquad\quad n := n + 1$
$\qquad\qquad\qquad\quad \{P \wedge 0 \leqslant n \leqslant N\}$ -- Pf_1
od
$\{b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle\}$ -- Pf_2

Pf_0: similar to Pf_0 in 5(a).
Pf_1:

$$
\begin{array}{ll}
 & ((P \wedge 0 \leqslant n \leqslant N)[n \backslash n+1])[b \backslash F[n] = 0] \\
= & (F[n] = 0 \ \equiv\ \langle \exists i : 0 \leqslant i < n+1 : F[i] = 0 \rangle) \wedge 0 \leqslant n+1 \leqslant N \\
\Leftarrow & \quad \{\ 0 \leqslant n+1 \Leftarrow 0 \leqslant n\ \} \\
 & (F[n] = 0 \ \equiv\ \langle \exists i : 0 \leqslant i < n+1 : F[i] = 0 \rangle) \wedge 0 \leqslant n < N \\
\Leftarrow & \quad \{\ (8.23)\ \text{split off}\ i = n\ \} \\
 & (F[n] = 0 \ \equiv\ \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle \vee F[n] = 0) \wedge 0 \leqslant n < N \\
\Leftarrow & \quad \{\ \text{Problem 1}\ \} \\
 & \neg \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle \wedge 0 \leqslant n < N \\
\Leftarrow & \quad \{\ \text{Leibniz}\ \} \\
 & (b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge \neg\, b \wedge 0 \leqslant n \leqslant N \wedge n \neq N\ .
\end{array}
$$

Pf_2:

$$
\begin{array}{ll}
 & (b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge \neg\, (n \neq N \wedge \neg\, b) \\
= & \quad \{\ \text{de Morgan}\ \} \\
 & (b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge (n = N \vee b) \\
= & \quad \{\ \text{distributivity}\ \} \\
 & ((b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge n = n) \vee \\
 & ((b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge b) \\
= & \quad \{\ (3.84)\text{, weakening}\ \} \\
 & (b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle) \vee \\
 & ((b \equiv \langle \exists i : 0 \leqslant i < n : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge b) \\
\Rightarrow & \quad \{\ \text{range weakening}\ \} \\
 & (b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle) \vee \\
 & ((b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle) \wedge 0 \leqslant n \leqslant N \wedge b) \\
= & \quad \{\ \text{weakening}\ \} \\
 & b \equiv \langle \exists i : 0 \leqslant i < N : F[i] = 0 \rangle\ .
\end{array}
$$