Programming Languages: Imperative Program Construction Midterm

Shin-Cheng Mu

Autumn Term, 2021

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. In the proof of the famous Fundamental Invariance Theorem the following property was used:

$$P \wedge X \Rightarrow Q \vee (P \wedge R) \;\equiv\; P \wedge X \Rightarrow Q \vee R \;. \tag{1}$$

Our aim is to prove (1), in three steps.

(a) (10 points) Prove that for all W and Z, $W \Rightarrow (Q \vee Z) \;\equiv\; (W \Rightarrow Q) \vee (W \Rightarrow Z)$.

Solution:

$$\begin{array}{ll} & (W \Rightarrow Q) \vee (W \Rightarrow Z) \\ = & \quad \{\ (3.59)\ X \Rightarrow Y \equiv \neg\, X \vee Y\ \} \\ & (\neg\, W \vee Q) \vee (\neg\, W \vee Z) \\ = & \quad \{\ (3.36), (3.38)\ \} \\ & \neg\, W \vee Q \vee Z \\ = & \quad \{\ (3.59)\ \} \\ & W \Rightarrow (Q \vee Z)\ . \end{array}$$

(b) (10 points) Prove that for all P, X, and R, $P \wedge X \Rightarrow P \wedge R \;\equiv\; P \wedge X \Rightarrow R$.

Solution:

$$\begin{array}{ll} & P \wedge X \Rightarrow P \wedge R \\ = & \quad \{\ (3.60)\ \text{definition of implication}\ \} \\ & P \wedge X \wedge P \wedge R \equiv P \wedge X \\ = & \quad \{\ (3.38)\ \text{idempotency}\ \} \\ & P \wedge X \wedge R \equiv P \wedge X \\ = & \quad \{\ (3.60)\ \text{definition of implication}\ \} \\ & P \wedge X \Rightarrow R\ . \end{array}$$

(c) (10 points) Prove (1) using (a) and (b).

Solution:

$$
\begin{array}{ll}
 & P \wedge X \Rightarrow Q \vee (P \wedge R) \\
\equiv & \quad \{ \text{(a)} \} \\
 & (P \wedge X \Rightarrow Q) \vee (P \wedge X \Rightarrow (P \wedge R)) \\
\equiv & \quad \{ \text{(b)} \} \\
 & (P \wedge X \Rightarrow Q) \vee (P \wedge X \Rightarrow R) \\
\equiv & \quad \{ \text{(a)} \} \\
 & P \wedge X \Rightarrow Q \vee R \ .
\end{array}
$$

2. (15 points) Recall the weakest precondition of **if**: $wp\ (\textbf{if}\ B_0 \to S_0 \mid B_1 \to S_1\ \textbf{fi})\ Q\ =\ (B_0 \Rightarrow wp\ S_0\ Q) \wedge (B_1 \Rightarrow wp\ S_1\ Q) \wedge (B_0 \vee B_1)$. In particular,

$$wp\ (\textbf{if}\ B \to S_0 \mid \neg\ B \to S_1\ \textbf{fi})\ Q\ =\ (B \Rightarrow wp\ S_0\ Q) \wedge (\neg\ B \Rightarrow wp\ S_1\ Q)\ .$$

We sometimes also see this alternative formulation:

$$wp\ (\textbf{if}\ B \to S_0 \mid \neg\ B \to S_1\ \textbf{fi})\ Q\ =\ (B \wedge wp\ S_0\ Q) \vee (\neg\ B \wedge wp\ S_1\ Q)\ .$$

Prove that the two definitions are equivalent by showing that

$$(B \Rightarrow P) \wedge (\neg\ B \Rightarrow R)\ =\ (B \wedge P) \vee (\neg\ B \wedge R)\ .$$

Hint: conjunct the lefthand side with $(B \vee \neg\ B)$.

Solution: We reason:

$$
\begin{array}{ll}
 & (B \Rightarrow P) \wedge (\neg\ B \Rightarrow R) \\
= & \quad \{ \text{since } B \vee \neg\ B \equiv \mathit{True}, (3.29) \} \\
 & (B \vee \neg\ B) \wedge (B \Rightarrow P) \wedge (\neg\ B \Rightarrow R) \\
= & \quad \{ (3.46) \text{ distributivity} \} \\
 & (B \wedge (B \Rightarrow P) \wedge (\neg\ B \Rightarrow R)) \vee \\
 & (\neg\ B \wedge (B \Rightarrow P) \wedge (\neg\ B \Rightarrow R)) \\
= & \quad \{ (3.66)\ X \wedge (X \Rightarrow Y) \equiv X \wedge Y \} \\
 & (B \wedge P \wedge (\neg\ B \Rightarrow R)) \vee (\neg\ B \wedge (B \Rightarrow P) \wedge R) \\
= & \quad \{ (3.59)\ X \Rightarrow Y \equiv \neg\ X \vee Y \} \\
 & (B \wedge P \wedge (B \vee R)) \vee (\neg\ B \wedge (\neg\ B \vee P) \wedge R) \\
= & \quad \{ (3.43) \text{ absorption: } X \wedge (X \vee Y) \equiv X \} \\
 & (B \wedge P) \vee (\neg\ B \wedge R)\ .
\end{array}
$$

3. (10 points) A consecutive segment of an array of *Int* is called "steep" (陡 in Chinese) if each of its elements is larger than the sum of all elements to its lefthand side. For example, in the array below,

$$6, 3, 4, 8, 10, 19, 38, 2, 7,$$

the segment $3, 4, 8$ is steep (since $0 < 3$, $3 < 4$ and $3 + 4 < 8$), the segments $8, 10, 19, 38$ and $2, 7$ are also steep (since $8 < 10$, $8 + 10 < 19$, $8 + 10 + 19 < 38$, etc). An empty segment is steep. A singleton segment containing one negative element, for example, -1, is *not* steep, since -1 is not larger than the sum of all elements to its lefthand side, which is 0.

Given an array A : **array** $[0..N)$ **of** *Int*, write down an expression stating that "r is the length of the longest steep segment of A."

It might be easier if you construct the expression in stages. For example, try to define *sum i j* denoting sum of a segment of an array, *steep i j* denoting whether a segment is steep, etc, and use them in the final expression.

Solution: Define

$$sum\ \ i\ j = \langle \Sigma k : i \leqslant k < j : A\ [k] \rangle\ ,$$
$$steep\ i\ j = \langle \forall k : i \leqslant k < j : sum\ i\ k < A\ [k] \rangle\ .$$

The expression is

$$r = \langle \uparrow\ p\ q : 0 \leqslant p \leqslant q \leqslant N \wedge steep\ p\ q : q - p \rangle\ .$$

4. (25 points) Verify the following program.

con N : *Int* $\{1 \leqslant N\}$
con F : **array** $[0..N)$ **of** *Int*
var x, y : *Int*
$x, y := 0, N - 1$
do $x \neq y \wedge F\ [x] \leqslant F\ [y] \rightarrow x := x + 1$
$\mid\ \ x \neq y \wedge F\ [x] \geqslant F\ [y] \rightarrow y := y - 1$
od
$\{F\ [x] = \langle \uparrow\ i : 0 \leqslant i < N : F\ [i] \rangle\}$

Hint: it might help using the property that $x \uparrow y \uparrow z = x \uparrow z$, if $x \geqslant y$.

Solution: Let P denote

$$\langle \uparrow\ i : x \leqslant i < y + 1 : F\ [i] \rangle = \langle \uparrow\ i : 0 \leqslant i < N : F\ [i] \rangle\ .$$

The annotated program is:

con N : *Int* $\{1 \leqslant N\}$
con F : **array** $[0..N)$ **of** *Int*
var x, y : *Int*
$x, y := 0, N - 1$ -- Pf0
$\{P \wedge 0 \leqslant x \leqslant y < N, bnd : y - x\}$ -- Pf1
do $x \neq y \wedge F\ [x] \leqslant F\ [y] \rightarrow x := x + 1$ -- Pf2
$\mid\ \ x \neq y \wedge F\ [x] \geqslant F\ [y] \rightarrow y := y - 1$ -- Pf3
od
$\{F\ [x] = \langle \uparrow\ i : 0 \leqslant i < N : F\ [i] \rangle\}$ -- Pf4

Pf0. We reason:

$$\begin{array}{ll} & (P \wedge 0 \leqslant x \leqslant y < N)[x, y \backslash 0, N - 1] \\ \equiv & \langle \uparrow\ i : 0 \leqslant i < N : F\ [i] \rangle = \langle \uparrow\ i : 0 \leqslant i < N : F\ [i] \rangle \wedge 0 \leqslant 0 \leqslant N - 1 < N \\ \Leftarrow & 1 \leqslant N\ . \end{array}$$

Pf1. That $0 \leqslant x \leqslant y < N$ implies that $y - x \geqslant 0$. To show that $y - x$ decrements in the first branch, we reason:

$$
\begin{array}{ll}
& (y - x < C)[x \backslash x + 1] \\
\equiv & y - (x + 1) < C \\
\Leftarrow & y - x = C \wedge P \wedge 0 \leqslant x \leqslant y < N \ .
\end{array}
$$

The other branch is dealt with similarly.

Pf2. The assumption that $0 \leqslant x \leqslant y < N$ and $x \neq y$ equivales $0 \leqslant x < y < N$. We reason:

$$
\begin{array}{ll}
& \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle [x \backslash x + 1] \\
= & \langle \uparrow i : x + 1 \leqslant i < y + 1 : F\ [i] \rangle \\
= & \quad \{ \text{ assumption: } 0 \leqslant x < y < N, \text{ split off } i = y \ \} \\
& \langle \uparrow i : x + 1 \leqslant i < y : F\ [i] \rangle \uparrow F\ [y] \\
= & \quad \{ \text{ assumption: } F\ [x] \leqslant F\ [y] \ \} \\
& \langle \uparrow i : x + 1 \leqslant i < y : F\ [i] \rangle \uparrow F\ [x] \uparrow F\ [y] \\
= & \langle \uparrow i : x \leqslant i < y : F\ [i] \rangle \uparrow F\ [y] \\
= & \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle \ .
\end{array}
$$

Therefore,

$$
\begin{array}{ll}
& (P \wedge 0 \leqslant x \leqslant y < N)[x \backslash x + 1] \\
\equiv & \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle [x \backslash x + 1] = \langle \uparrow i : 0 \leqslant i < N : F\ [i] \rangle \wedge 0 \leqslant x + 1 \leqslant y < N \\
\Leftarrow & \quad \{ \text{ reasoning above } \} \\
& \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle = \langle \uparrow i : 0 \leqslant i < N : F\ [i] \rangle \wedge \\
& \quad 0 \leqslant x \leqslant y < N \wedge x \neq y \wedge F\ [x] \leqslant F\ [y] \ .
\end{array}
$$

Pf3. We reason:

$$
\begin{array}{ll}
& \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle [y \backslash y - 1] \\
= & \langle \uparrow i : x \leqslant i < y : F\ [i] \rangle \\
= & \quad \{ \text{ assumption: } 0 \leqslant x < y < N, \text{ split off } i = x \ \} \\
& F\ [x] \uparrow \langle \uparrow i : x + 1 \leqslant i < y : F\ [i] \rangle \\
= & \quad \{ \text{ assumption: } F\ [x] \geqslant F\ [y] \ \} \\
& F\ [x] \uparrow F\ [y] \uparrow \langle \uparrow i : x + 1 \leqslant i < y : F\ [i] \rangle \\
= & F\ [x] \uparrow \langle \uparrow i : x + 1 \leqslant i < y + 1 : F\ [i] \rangle \\
= & \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle \ .
\end{array}
$$

Therefore,

$$
\begin{array}{ll}
& (P \wedge 0 \leqslant x \leqslant y < N)[y \backslash y - 1] \\
\equiv & \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle [y \backslash y - 1] = \langle \uparrow i : 0 \leqslant i < N : F\ [i] \rangle \wedge 0 \leqslant x \leqslant y - 1 < N \\
\Leftarrow & \quad \{ \text{ reasoning above } \} \\
& \langle \uparrow i : x \leqslant i < y + 1 : F\ [i] \rangle = \langle \uparrow i : 0 \leqslant i < N : F\ [i] \rangle \wedge \\
& \quad 0 \leqslant x \leqslant y < N \wedge x \neq y \wedge F\ [x] \geqslant F\ [y] \ .
\end{array}
$$

Pf4. Consider:

$$
\begin{array}{ll}
& \neg \left((x \neq y \wedge F\ [x] \leqslant F\ [y]) \vee (x \neq y \wedge F\ [x] \geqslant F\ [y]) \right) \\
\equiv & \quad \{ \text{ distributivity } \} \\
& \neg \left(x \neq y \wedge (F\ [x] \leqslant F\ [y] \vee F\ [x] \geqslant F\ [y]) \right) \\
\equiv & \quad \{ \ A \leqslant B \vee A \geqslant B = \mathit{True} \ \} \\
& \neg (x \neq y) \\
\equiv & \ x = y \ .
\end{array}
$$

Therefore,

$$
\begin{array}{ll}
& P \wedge \neg\, ((x \neq y \wedge F\,[x] \leqslant F\,[y]) \vee (x \neq y \wedge F\,[x] \geqslant F\,[y])) \\
\equiv & P \wedge x = y \\
\equiv & \langle \uparrow i : x \leqslant i < x+1 : F\,[i] \rangle = \langle \uparrow i : 0 \leqslant i < N : F\,[i] \rangle \\
\equiv & \langle \uparrow i : x = i : F\,[i] \rangle = \langle \uparrow i : 0 \leqslant i < N : F\,[i] \rangle \\
\equiv & \quad \{ \text{ one-point rule } \} \\
& F\,[x] = \langle \uparrow i : 0 \leqslant i < N : F\,[i] \rangle \ .
\end{array}
$$

5. (20 points) Let $(\oplus) : \mathit{Int} \to \mathit{Int} \to \mathit{Int}$ be an associative, commutative binary operator with identity element e, and let f be some function of type $\mathit{Int} \to \mathit{Int} \to \mathit{Int}$. The following incomplete program attempts to compute $\langle \oplus i\ j : 0 \leqslant i < M \wedge 0 \leqslant j < N : f\ i\ j \rangle$.

   Missing parts of the program are marked by $???$. Complete the program and prove its correctness. The missing parts are supposed to be discovered while trying to prove the program, but you need *not* tell me how the proof and program evolve. You only need to present the final program and its proof.

   con $M, N : \mathit{Int}\ \{0 < M \wedge 0 \leqslant N\}$
   var $x, y, s : \mathit{Int}$

   $x, y, s := 0, N, e$
   $\{P \wedge Q \wedge ???, \mathit{bnd}: ???\}$
   do $y \neq 0 \quad \wedge\ x \neq ??? \ \to s := ???$
   $\qquad\qquad\qquad\qquad\qquad\quad y := y - 1$
   $\mid \quad y = ??? \ \wedge\ x \neq M \quad \to x, y := x + 1, N$
   od
   $\{s = \langle \oplus i\ j : 0 \leqslant i < M \wedge 0 \leqslant j < N : f\ i\ j \rangle\}$

   To make the task easier, P in the invariant denotes:

$$
\begin{array}{l}
s = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \\
\qquad \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle \ ,
\end{array}
$$

   while Q denotes $x = M \Rightarrow y = N$.

   Note: you might wonder why we bother with such an awkward program when the task can be done by two nested loops. The program was originally a more complex one that allows us to exploit other properties of f (e.g monotonicity) and skip some of the computation. For this exam I decided to make it easier.

Solution:

con $M, N : \mathit{Int}\ \{0 < M \wedge 0 \leqslant N\}$
var $x, y, s : \mathit{Int}$

$x, y, s := 0, N, e$ -- Pf0
$\{P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N, \mathit{bnd} : y + (N+1) \times (M - x)\}$ -- Pf1
do $y \neq 0 \wedge x \neq M \to s := s \oplus f\ x\ (y-1)$ -- Pf2
$\qquad\qquad\qquad\quad y := y - 1$
$\mid \quad y = 0 \wedge x \neq M \to x, y := x + 1, N$ -- Pf3
od
$\{s = \langle \oplus i\ j : 0 \leqslant i < M \wedge 0 \leqslant j < N : f\ i\ j \rangle\}$ -- Pf4

Recall

$$
\begin{array}{l}
P \equiv\ s = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle \ , \\
Q \equiv x = M \Rightarrow y = N \ .
\end{array}
$$

Pf0. We reason

$$
\begin{array}{ll}
& (P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N)[x, y, s \backslash 0, N, e] \\
\equiv & s = \langle \oplus i\ j : 0 \leqslant i < 0 \wedge 0 \leqslant j < 0 : f\ i\ j \rangle \oplus \langle \oplus j : N \leqslant j < N : f\ 0\ j \rangle \wedge \\
& (0 = M \Rightarrow N = N) \wedge 0 \leqslant 0 \leqslant M \wedge 0 \leqslant N \leqslant N \\
\Leftarrow & e = e \oplus e \wedge 0 < M \wedge 0 \leqslant N \\
\equiv & 0 < M \wedge 0 \leqslant N \ .
\end{array}
$$

Pf1. Under the condition that $0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N$, the bound $y + (N + 1) \times (M - x)$ is always a non-negative number.

It is apparent that the first branch decreases the bound. Consider the second branch:

$$
\begin{array}{ll}
& (y + (N + 1) \times (M - x) < C)[x, y \backslash x + 1, N] \\
\equiv & N + (N + 1) \times (M - (x + 1)) < C \\
\equiv & N + (N + 1) \times (M - x) - (N + 1) < C \\
\equiv & (-1) + (N + 1) \times (M - x) < C \\
\Leftarrow & y + (N + 1) \times (M - x) = C \wedge y = 0 \ .
\end{array}
$$

Pf2. Consider

$$
\begin{array}{ll}
& (\langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle)[y \backslash y - 1] \\
= & \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y - 1 \leqslant j < N : f\ x\ j \rangle \\
= & \quad \{ \text{ assuming } 0 \leqslant y - 1 < N, \text{ split off } j = y - 1 \ \} \\
& \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle \oplus f\ x\ (y - 1) \ .
\end{array}
$$

Therefore,

$$
\begin{array}{ll}
& (P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N)[y \backslash y - 1] \\
\Leftarrow & \quad \{ \text{ calculation above } \} \\
& s = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle \oplus f\ x\ (y - 1) \wedge \\
& (x = M \Rightarrow y - 1 = N) \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y - 1 < N \\
\Leftarrow & s = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle \oplus f\ x\ (y - 1) \wedge \\
& Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N \wedge \\
& y \neq 0 \wedge x \neq M \ .
\end{array}
$$

Note that, since we do not have $y - 1 = N$, we let $x \neq M$ such that $x = M \Rightarrow y - 1 = N$ holds. That is how we discover the missing guard.

With another substitution $[s \backslash s \oplus f\ x\ (y - 1)]$ we restore the invariant:

$$
\begin{array}{ll}
& ((P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N)[y \backslash y - 1])[s \backslash s \oplus f\ x\ (y - 1)] \\
\Leftarrow & \quad \{ \text{ calculation above } \} \\
& s \oplus f\ x\ (y - 1) = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle \oplus f\ x\ (y - 1) \wedge \\
& Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N \wedge y \neq 0 \wedge x \neq M \\
\Leftarrow & P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N \wedge y \neq 0 \wedge x \neq M \ .
\end{array}
$$

Pf3. Consider:

$$
\begin{array}{ll}
& (\langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : y \leqslant j < N : f\ x\ j \rangle)[x, y \backslash x + 1, N] \\
= & \langle \oplus i\ j : 0 \leqslant i < x + 1 \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : N \leqslant j < N : f\ (x + 1)\ j \rangle \\
= & \langle \oplus i\ j : 0 \leqslant i < x + 1 \wedge 0 \leqslant j < N : f\ i\ j \rangle \\
= & \quad \{ \text{ assuming } 0 \leqslant x, \text{ split off } i = x \ \} \\
& \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : 0 \leqslant j < N : f\ x\ j \rangle \ .
\end{array}
$$

Therefore,

$$
\begin{array}{ll}
& (P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N)[x, y \backslash x+1, N] \\
\equiv & P[x, y \backslash x+1, N] \wedge Q[x, y \backslash x+1, N] \wedge 0 \leqslant x+1 \leqslant M \wedge 0 \leqslant N \leqslant N \\
\Leftarrow & s = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : 0 \leqslant j < N : f\ x\ j \rangle \wedge \\
& (x+1 = M \Rightarrow N = N) \wedge 0 \leqslant x+1 \leqslant M \wedge 0 \leqslant N \leqslant N \\
\Leftarrow & P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N \wedge \\
& y = 0 \wedge x \neq M \ .
\end{array}
$$

Also note how we let $y = 0$, such that P matches $s = \langle \oplus i\ j : 0 \leqslant i < x \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : 0 \leqslant j < N : f\ x\ j \rangle$. That is how we discover the missing guard of this branch.

Pf4. Consider

$$
\begin{array}{ll}
& \neg\ ((y \neq 0 \wedge x \neq M) \vee (y = 0 \wedge x \neq M)) \\
\equiv & \quad \{\ \text{distributivity}\ \} \\
& \neg\ ((y \neq 0 \vee y = 0) \wedge x \neq M) \\
\equiv & \quad \{\ P \vee \neg\ P\ \} \\
& \neg\ (x \neq M) \\
\equiv & x = M \ .
\end{array}
$$

We have

$$
\begin{array}{ll}
& P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N \wedge \neg\ ((y \neq 0 \wedge x \neq M) \vee (y = 0 \wedge x \neq M)) \\
\equiv & \quad \{\ \text{calculation above}\ \} \\
& P \wedge Q \wedge 0 \leqslant x \leqslant M \wedge 0 \leqslant y \leqslant N \wedge x = M \\
\Rightarrow & P \wedge x = M \wedge y = N \\
\equiv & s = \langle \oplus i\ j : 0 \leqslant i < M \wedge 0 \leqslant j < N : f\ i\ j \rangle \oplus \langle \oplus j : N \leqslant j < N : f\ x\ j \rangle \\
\equiv & s = \langle \oplus i\ j : 0 \leqslant i < M \wedge 0 \leqslant j < N : f\ i\ j \rangle \ .
\end{array}
$$