C Derivations for Examples in Section 5

This appendix lists the derivations omitted in Section 5.

C.1 Derivation for [*LetRef*]

We can derive [*LetRef*] as follows. Below i is fresh.

1. $\{C\}\ M :_m \{C_0\}$	(premise)
2. $\{C_0[!x/m] \wedge x\#\tilde{e}\}\ N :_u \{C'\}$ with $x \notin \mathsf{fpn}(\tilde{e})$	(premise)
3. $\{C\}\ \mathtt{ref}(M) :_x \{\nu y.(C_0[!x/m] \wedge x\#i \wedge x = y)\}$	(1,Ref)
4. $\{C\}\ \mathtt{ref}(M) :_x \{\nu y.(C_0[!x/m] \wedge x\#\tilde{e} \wedge x = y)\}$	(Subs n-times)
5. $\{C_0[!x/m] \wedge x\#\tilde{e} \wedge x = y\}\ N :_u \{C' \wedge x = y\}$	(2, Invariance)
6. $\{C\}\ \mathtt{let}\ x = \mathtt{ref}(M)\ \mathtt{in}\ N :_u \{\nu y.(C' \wedge x = y)\}$	(4,5,LetOpen)
7. $\{C\}\ \mathtt{let}\ x = \mathtt{ref}(M)\ \mathtt{in}\ N :_u \{\nu x.C'\}$	(Conseq)

The last line uses a standard logical law (discussed below). Lines 4 and 6 use the following derived/admissible proof rules:

$$[\mathit{Subs}]\ \frac{\{C\}\ M :_u \{C'\} \quad u \notin \mathsf{fpn}(e)}{\{C[e/i]\}\ M :_u \{C'[e/i]\}} \qquad [\mathit{LetOpen}]\ \frac{\{C\}\ M :_x \{\nu\tilde{y}.C_0\} \quad \{C_0\}\ N :_u \{C'\}}{\{C\}\ \mathtt{let}\ x = M\ \mathtt{in}\ N :_u \{\nu\tilde{y}.C'\}}$$

[*LetOpen*] opens the "scope" of $\tilde{y}$ to N. The crucial step is Line 5, which turns stronger "#" into "ν" (by definition), using the consequence rule.

C.2 Derivation for `mutualParity` and `safeEven`

Let us define:

$$M_x \stackrel{\text{def}}{=} \lambda n.\mathtt{if}\ y = 0\ \mathtt{then}\ \mathtt{f}\ \mathtt{else}\ \mathtt{not}((!y)(n-1))$$
$$M_y \stackrel{\text{def}}{=} \lambda n.\mathtt{if}\ y = 0\ \mathtt{then}\ \mathtt{t}\ \mathtt{else}\ \mathtt{not}((!x)(n-1))$$

We also use:

$$\mathit{IsOdd}'(u,gh,n,xy) \ = \mathit{IsOdd}(u,gh,n,xy) \wedge !x = g \wedge !y = h$$
$$\mathit{IsEven}'(u,gh,n,xy) \ = \ \mathit{IsEven}(u,gh,n,xy) \wedge !x = g \wedge !y = h$$

We use the following derived rules and one standard structure rule appeared in [14].

$$[\mathit{Simple}]\ \frac{-}{\{C[e/u]\}e :_u \{C\}} \qquad [\mathit{IfH}]\ \frac{\{C \wedge e\}\ M_1 :_u \{C'\} \quad \{C \wedge \neg e\}\ M_2 :_u \{C'\}}{\{C\}\ \mathtt{if}\ e\ \mathtt{then}\ M_1\ \mathtt{else}\ M_2 :_u \{C'\}}$$

$$[\wedge\text{-}\mathit{Post}]\ \frac{\{C\}M :_u \{C_1\} \quad \{C\}M :_u \{C_2\}}{\{C\}M :_u \{C_1 \wedge C_2\}}$$

Figure 2 lists the derivation for `MutualParity`. In Line 4, h in the evaluation formula can be replaced by $!y$ and vice versa because of $!y = h$ and the universal quatification of h.

$$\forall h.(!y = h \wedge \{C\}h \bullet n = z\{C'\}) \quad \equiv \quad \forall h.(!y = h \wedge \{C\}(!y) \bullet n = z\{C'\})$$

In Line 5, we use the following axiom for the evaluation formula from [14]:

$$\{C \wedge A\}\ e_1 \bullet e_2 = z\{C'\} \quad \equiv \quad A \supset \{C\}e_1 \bullet e_2 = z\{C'\}$$

Fig. 2 `mutualParity` derivations

1. $\{(n \geq 1 \supset \mathit{IsEven}'(!y,gh,n-1,xy)) \ \wedge \ n=0\}\ \mathtt{f} :_z \{z = \mathit{Odd}(n) \wedge !x = g \wedge !y = h\}@\emptyset$ (Const)

2. $\{(n \geq 1 \supset \mathit{IsEven}'(!y,gh,n-1,xy)) \ \wedge \ n \geq 1\}$
   $\mathtt{not}((!y)(n-1)) :_z \{z = \mathit{Odd}(n) \wedge !x = g \wedge !y = h\}@\emptyset$ (Simple, App)

3. $\{n \geq 1 \supset \mathit{IsEven}'(!y,gh,n-1,xy)\}$
   $\mathtt{if}\ n=0\ \mathtt{then\ f\ else\ not}((!y)(n-1)) :_m \{z = \mathit{Odd}(n) \wedge !x = g \wedge !y = h\}@\emptyset$ (IfH)

4. $\{\mathsf{T}\}\ \lambda n.\mathtt{if}\ n=0\ \mathtt{then\ f\ else\ not}((!y)(n-1)) :_u$
   $\{\ \forall gh, n \geq 1.\{\mathit{IsEven}'(h,gh,n-1,xy)\}u \bullet n = z\{z = \mathit{Odd}(n) \wedge !x = g \wedge !y = h\}@\emptyset\}@\emptyset$
   (Abs, $\forall$, Conseq)

5. $\{\mathsf{T}\}\ M_x :_u \{\ \forall gh, n \geq 1.(\mathit{IsEven}(h,gh,n-1,xy) \supset \mathit{IsOdd}(u,gh,n,xy))\}@\emptyset$ (Conseq)

6. $\{\mathsf{T}\}\ x := M_x\{\ \forall gh, n \geq 1.(\mathit{IsEven}(h,gh,n-1,xy) \supset \mathit{IsOdd}(!x,gh,n,xy)) \wedge !x = g\}@x$ (Assign)

7. $\{\mathsf{T}\}\ y := M_y\{\ \forall gh, n \geq 1.(\mathit{IsOdd}(g,gh,n-1,xy) \supset \mathit{IsEven}(!y,gh,n,xy)) \wedge !y = h\}@y$

8. $\{\mathsf{T}\}\ \mathtt{mutualParity}$
   $\{\forall gh.n \geq 1.((\mathit{IsEven}(h,gh,n-1,xy) \wedge \mathit{IsOdd}(g,gh,n-1,xy)) \supset$
   $(\mathit{IsEven}(!y,gh,n,xy) \wedge \mathit{IsOdd}(!x,gh,n,xy) \wedge !x = g \wedge !y = h)\ \}@xy$ ($\wedge$-Post)

9. $\{\mathsf{T}\}\ \mathtt{mutualParity}$
   $\{\forall n \geq 1 gh.((\mathit{IsEven}(h,gh,n-1,xy) \wedge \mathit{IsOdd}(g,gh,n-1,xy) \wedge !x = g \wedge !y = h) \supset$
   $(\mathit{IsEven}(!y,gh,n,xy) \wedge \mathit{IsOdd}(!x,gh,n,xy) \wedge !x = g \wedge !y = h)\}@xy$ (Conseq)

10. $\{\mathsf{T}\}\ \mathtt{mutualParity}$
    $\{\forall n \geq 1 gh.((\mathit{IsEven}(!y,gh,n-1,xy) \wedge \mathit{IsOdd}(!x,gh,n-1,xy) \wedge !x = g \wedge !y = h) \supset$
    $(\mathit{IsEven}(!y,gh,n,xy) \wedge \mathit{IsOdd}(!x,gh,n,xy) \wedge !x = g \wedge !y = h)\}@xy$ (Conseq)

11. $\{\mathsf{T}\}\ \mathtt{mutualParity}$
    $\{\forall n \geq 1.(\exists gh.(\mathit{IsEven}(!x,gh,n-1,xy) \wedge \mathit{IsOdd}(!y,gh,n-1,xy) \wedge !x = g \wedge !y = h) \supset$
    $\exists gh.(\mathit{IsEven}(!y,gh,n,xy) \wedge \mathit{IsOdd}(!x,gh,n,xy) \wedge !x = g \wedge !y = h)\}@xy$ (Conseq)

12. $\{\mathsf{T}\}\ \mathtt{mutualParity}\{\exists gh.\mathit{IsOddEven}(gh,!x!y,xy,n)\}@xy$

where A is stateless and we set $A = \mathit{IsEven}(h,gh,n-1,xy)$. Line 9 is derived as Line 4 by replacing h and g by $!y$ and $!x$, respectively. Line 11 is the standard logical implication ($\forall x.(C_1 \supset C_2) \supset (\exists x.C_1 \supset \exists x.C_2)$). Now we derive for `safeEven`. Let us define:

$$
\begin{aligned}
\mathit{ValEven}(u) &= \forall n.\{\mathsf{T}\}u \bullet n = z\{z = \mathit{Even}(n)\}@\emptyset \\
C_0 &= !x = g \wedge !y = h \ \wedge \ \mathit{IsOdd}(g,gh,n,xy) \ \wedge \ x\#i \ \wedge \ y\#j \\
\mathit{Even}_a &= C_0 \ \wedge \ \forall n.\{C_0\}u \bullet n = z\{C_0\}@xy \\
\mathit{Even}_b &= \forall n.\{C_0\}u \bullet n = z\{z = \mathit{Even}(n)\}@xy
\end{aligned}
$$

The derivation is given as follows.

1. $\{\mathsf{T}\}\lambda n.\mathtt{t} :_m \{\mathsf{T}\}@\emptyset$

2. $\{\mathsf{T}\}\mathtt{mutualParity};\ !y :_u \{\exists gh.\mathit{IsOddEven}(gh,gu,xy,n)\}@xy$

3. $\{\mathsf{T}\}\mathtt{mutualParity};\ !y :_u \{\exists gh.(\mathit{Even}_a \ \wedge \ \mathit{Even}_b)\}@xy$

4. $\{xy\#ij\}\mathtt{mutualParity};\ !y :_u \{\exists gh.(xy\#ij \ \wedge \ \mathit{Even}_a \ \wedge \ \mathit{Even}_b)\}@xy$

5. $\{\mathsf{T}\}\mathtt{safeEven} :_u \{\nu xy.\exists gh.(xy\#ij \ \wedge \ \mathit{Even}_a \ \wedge \ \mathit{Even}_b)\}@\emptyset$

6. $\{\mathsf{T}\}m\bullet() = u\{\nu xy \exists gh.(xy\#ij \ \wedge \ \mathit{Even}_a \wedge \mathit{Even}_b)\} \supset \{\mathsf{T}\}m\bullet() = u\{\mathit{ValEven}(u)\}$ (by (AIH))

7. $\{\mathsf{T}\}\mathtt{safeEven} :_u \{\mathit{ValEven}(u)\}@\emptyset$

C.3 Derivation for `profile`

We derive:

$$\{\forall y.\{C\}\, f \bullet y = z\{C'\}@\tilde{w}\}\ \texttt{profile} :_u \{\forall y.\{C\} u \bullet y = z\{C'\}@\tilde{w}\} \tag{C.1}$$

which says: *if f satisfies the specification $\forall y.\{C\}\, f \bullet y = z\{C'\}$ and moreover if it is total, then* `profile` *satisfies the same specification*. First we derive:

$$\begin{array}{rll} E & = \forall y.\{C\}\, f \bullet y = z\{C'\}@\tilde{w} & \\ \supset E_0 & = \forall yi.\{C \wedge x\#i\}\, f \bullet y = z\{C'\}@\tilde{w}x & \text{Axiom (e8) in [14]} \\ \supset E_1 & = \forall yi.\{C \wedge x\#i\}\, f \bullet y = z\{x\#z\tilde{w}i\}@\tilde{w}x & \text{Proposition 11} \\ \supset E_2 & = \forall yi.\{C \wedge x\#i\}\, f \bullet y = z\{C' \wedge x\#i\}@\tilde{w}x & \text{Axiom (e8) in [14]} \end{array}$$

We also let $E_3 = \forall yi \neq x.\{[!x]C \wedge x\#i\}\, f \bullet y = z\{C' \wedge x\#i\}@\tilde{w}x$. The inference follows.

1. $\{\mathsf{T}\}x :=!x+1\{\mathsf{T}\}@x$	(Assign)
2. $\{[!x]C \wedge E \wedge x\#i \wedge x \neq y\}\ x :=!x+1\ \{C \wedge E \wedge x\#i \wedge x \neq y\}@x$	(Inv-#, Conseq)
3. $\{C \wedge E \wedge x\#i \wedge x \neq y\}\ fy :_z \{C' \wedge x\#i \wedge x \neq y\}@\tilde{w}x$	(App, Conseq)
4. $\{[!x]C \wedge E \wedge x\#i \wedge x \neq y\}\, x := x+1; fy :_z \{C' \wedge x\#i \wedge x \neq y\}@x\tilde{w}$	(2, 3, Seq)
5. $\{E\}\ \lambda y.(x := x+1; fy) :_u \{E_2\}@\emptyset$	(4, Abs, Inv)
6. $\{E\}\ \lambda y.(x := x+1; fy) :_u \{\mathsf{Inv}(u, x\#i, \tilde{x})\}@\emptyset$	(Abs, Inv)
7. $\{E\}\texttt{profile}\{\nu x.(\mathsf{Inv}(u, x\#i, \tilde{x}) \wedge E_3)\}@\emptyset$	(LetRef)
8. $\{E\}m \bullet () = u\{\nu x.(\mathsf{Inv}(u, x\#i, \tilde{x}) \wedge E_3)\} \supset \{E\}m \bullet () = u\{E\}$	($\star$)
9. $\{E\}\texttt{profile} :_u \{E\}@\emptyset$	(7,8,ConsEval)

Above Line 2 uses: for any C, x we have $[!x][!x]C \equiv [!x]C$. Also by $[!x]E \equiv E$ and by $[!x]x\#i \equiv x\#i$ (by Proposition 7 (3)-5), [*Inv*] becomes applicable. Line 6 is inferred by Proposition 13.

C.4 Derivation for Meyer-Sieber

For the derivation of (5.5) we use:

$$E = \forall f.(\{\mathsf{T}\}\, f \bullet ()\{\mathsf{T}\}@\emptyset \ \supset\ \{C\} g \bullet f \{C'\})$$

We use the following [*LetRef*] which is derived by [*Ref*] where C' is replaced by $[!x]C'$.

$$[\mathit{LetRef}]\ \frac{\{C\}\, M :_m \{C_0\} \quad \{[!x]C_0 \wedge !x = m \wedge x\#\tilde{e}\}\, N :_u \{C'\} \quad x \notin \mathsf{fpn}(\tilde{e})}{\{C\}\ \texttt{let}\ x = \texttt{ref}(M)\ \texttt{in}\ N :_u \{\nu x.C'\}}$$

The derivation follows. Below $M_{1,2}$ is the body of the first/second lets, respectively.

1. $\{\mathit{Even}(!x) \wedge [!x]C'\}\ \texttt{if}\ \mathit{even}(!x)\ \texttt{then}\ ()\ \texttt{else}\ \Omega()\ \{[!x]C'\}@\emptyset$	(If)
2. $\{[!x]C\}\ gf\ \{[!x]C'\}$	(cf. § 5)
3. $\{\mathit{Even}(!x) \wedge [!x]C\}\ gf\ \{\mathit{Even}(!x) \wedge [!x]C'\}$	(2, Inv)
4. $\{E \wedge [!x]C \wedge \mathit{Even}(!x) \wedge x\#gi\}\texttt{let}\ f = \ldots\ \texttt{in}\ (gf; \ldots)\{[!x]C' \wedge x\#i\}$	(3, Seq, Let)
5. $\{E \wedge C\}\ \texttt{MeyerSieber}\ \{\nu x.([!x]C' \wedge x\#i)\}$	(4, LetRef)
6. $\{E \wedge C\}\ \texttt{MeyerSieber}\ \{C'\}$	(9, Prop. 14)