```
┌──────────────────────────── MODULE bank_account ────────────────────────────┐
  Copyright (c) 2017, Gene Cooperman. May be freely distributed
  and modified as long as this copyright notice remains.

  Joint bank account by husband and wife; C statements are assumed atomic.

EXTENDS Naturals, Sequences, TLC   Sequences required for “procedure” stmt
CONSTANT N   N is number of iterations. Assign to it in model overview.

--algorithm bank{
  variables account = 100, cash = [i ∈ {“husband”, “wife”} ↦ 10],
            iterations = [i ∈  {“husband”, “wife”} ↦ N] ;
     Note that we need to define iterations[“husband”] and iterations[“wife”].
      We do _not_ want a single global variable, iterations, that is
      shared between “husband” and “wife”.
     In model, replace defaultInitValue by value for iterations

  procedure withdraw( amount1 ) {
    withdraw_start: account := account − amount1 ;
     w1:            cash[self] := cash[self] + amount1 ;
     w2:            return ;
   }

  procedure deposit( amount2 ) {
    deposit_start: account := account + amount2 ;
    d1:            cash[self] := cash[self] − amount2 ;
    d2:            return ;
   }

  process ( spouse ∈ {“husband”, “wife”} )
    variable total ;
  { start: while ( iterations[self] > 0 ) {
       We hard-wire the max amount below, but this could have been a CONSTANT .
      s1: with ( amount ∈ 1 . . 2 )
             call withdraw(amount) ;
      s2: with ( amount ∈ 1 . . 2 )
             call deposit(amount) ;
      s3: iterations[self] := iterations[self] − 1 ;
          total := account + cash[“husband”] + cash[“wife”] ;
       } ;
      assert iterations[self] = 0 ;

      if ( iterations[“husband”] = 0 ∧ iterations[“wife”] = 0 ) {
        total := account + cash[“husband”] + cash[“wife”] ;
        print total ;
        assert total = 120 ;
       }
```

    } end process block

} * end algorithm

BEGIN TRANSLATION

$\text{CONSTANT } \mathit{defaultInitValue}$

$\text{VARIABLES } \mathit{account}, \mathit{cash}, \mathit{iterations}, \mathit{pc}, \mathit{stack}, \mathit{amount}1, \mathit{amount}2, \mathit{total}$

$$\mathit{vars} \triangleq \langle \mathit{account}, \mathit{cash}, \mathit{iterations}, \mathit{pc}, \mathit{stack}, \mathit{amount}1, \mathit{amount}2, \mathit{total} \rangle$$

$$\mathit{ProcSet} \triangleq (\{\text{“husband”}, \text{“wife”}\})$$

$$\begin{aligned}
\mathit{Init} \triangleq\ & \text{Global variables} \\
& \land \mathit{account} = 100 \\
& \land \mathit{cash} = [i \in \{\text{“husband”}, \text{“wife”}\} \mapsto 10] \\
& \land \mathit{iterations} = [i \in \{\text{“husband”}, \text{“wife”}\} \mapsto N] \\
& \text{Procedure withdraw} \\
& \land \mathit{amount}1 = [\mathit{self} \in \mathit{ProcSet} \mapsto \mathit{defaultInitValue}] \\
& \text{Procedure deposit} \\
& \land \mathit{amount}2 = [\mathit{self} \in \mathit{ProcSet} \mapsto \mathit{defaultInitValue}] \\
& \text{Process spouse} \\
& \land \mathit{total} = [\mathit{self} \in \{\text{“husband”}, \text{“wife”}\} \mapsto \mathit{defaultInitValue}] \\
& \land \mathit{stack} = [\mathit{self} \in \mathit{ProcSet} \mapsto \langle\rangle] \\
& \land \mathit{pc} = [\mathit{self} \in \mathit{ProcSet} \mapsto \text{“start”}]
\end{aligned}$$

$$\begin{aligned}
\mathit{withdraw\_start}(\mathit{self}) \triangleq\ & \land \mathit{pc}[\mathit{self}] = \text{“withdraw\_start”} \\
& \land \mathit{account}' = \mathit{account} - \mathit{amount}1[\mathit{self}] \\
& \land \mathit{pc}' = [\mathit{pc} \text{ EXCEPT } ![\mathit{self}] = \text{“w1”}] \\
& \land \text{UNCHANGED } \langle \mathit{cash}, \mathit{iterations}, \mathit{stack}, \mathit{amount}1, \\
& \qquad \mathit{amount}2, \mathit{total} \rangle
\end{aligned}$$

$$\begin{aligned}
w1(\mathit{self}) \triangleq\ & \land \mathit{pc}[\mathit{self}] = \text{“w1”} \\
& \land \mathit{cash}' = [\mathit{cash} \text{ EXCEPT } ![\mathit{self}] = \mathit{cash}[\mathit{self}] + \mathit{amount}1[\mathit{self}]] \\
& \land \mathit{pc}' = [\mathit{pc} \text{ EXCEPT } ![\mathit{self}] = \text{“w2”}] \\
& \land \text{UNCHANGED } \langle \mathit{account}, \mathit{iterations}, \mathit{stack}, \mathit{amount}1, \mathit{amount}2, \\
& \qquad \mathit{total} \rangle
\end{aligned}$$

$$\begin{aligned}
w2(\mathit{self}) \triangleq\ & \land \mathit{pc}[\mathit{self}] = \text{“w2”} \\
& \land \mathit{pc}' = [\mathit{pc} \text{ EXCEPT } ![\mathit{self}] = \mathit{Head}(\mathit{stack}[\mathit{self}]).\mathit{pc}] \\
& \land \mathit{amount}1' = [\mathit{amount}1 \text{ EXCEPT } ![\mathit{self}] = \mathit{Head}(\mathit{stack}[\mathit{self}]).\mathit{amount}1] \\
& \land \mathit{stack}' = [\mathit{stack} \text{ EXCEPT } ![\mathit{self}] = \mathit{Tail}(\mathit{stack}[\mathit{self}])] \\
& \land \text{UNCHANGED } \langle \mathit{account}, \mathit{cash}, \mathit{iterations}, \mathit{amount}2, \mathit{total} \rangle
\end{aligned}$$

$$\mathit{withdraw}(\mathit{self}) \triangleq \mathit{withdraw\_start}(\mathit{self}) \lor w1(\mathit{self}) \lor w2(\mathit{self})$$

$$\begin{aligned}
\mathit{deposit\_start}(\mathit{self}) \triangleq\ & \land \mathit{pc}[\mathit{self}] = \text{“deposit\_start”} \\
& \land \mathit{account}' = \mathit{account} + \mathit{amount}2[\mathit{self}] \\
& \land \mathit{pc}' = [\mathit{pc} \text{ EXCEPT } ![\mathit{self}] = \text{“d1”}] \\
& \land \text{UNCHANGED } \langle \mathit{cash}, \mathit{iterations}, \mathit{stack}, \mathit{amount}1,
\end{aligned}$$

```
                              $amount2,\ total\rangle$

$d1(self) \triangleq$ $\land\ pc[self] = $ “d1”
                      $\land\ cash' = [cash\ \textsc{except}\ ![self] = cash[self] - amount2[self]]$
                      $\land\ pc' = [pc\ \textsc{except}\ ![self] = $ “d2”$]$
                      $\land\ \textsc{unchanged}\ \langle account,\ iterations,\ stack,\ amount1,\ amount2,$
                                          $total\rangle$

$d2(self) \triangleq$ $\land\ pc[self] = $ “d2”
                      $\land\ pc' = [pc\ \textsc{except}\ ![self] = Head(stack[self]).pc]$
                      $\land\ amount2' = [amount2\ \textsc{except}\ ![self] = Head(stack[self]).amount2]$
                      $\land\ stack' = [stack\ \textsc{except}\ ![self] = Tail(stack[self])]$
                      $\land\ \textsc{unchanged}\ \langle account,\ cash,\ iterations,\ amount1,\ total\rangle$

$deposit(self) \triangleq deposit\_start(self) \lor d1(self) \lor d2(self)$

$start(self) \triangleq$ $\land\ pc[self] = $ “start”
                         $\land\ \textsc{if}\ iterations[self] > 0$
                              $\textsc{then}$ $\land\ pc' = [pc\ \textsc{except}\ ![self] = $ “s1”$]$
                                              $\land\ total' = total$
                              $\textsc{else}$ $\land\ Assert(iterations[self] = 0,$
                                                        “Failure of assertion at line 42, column 7.”$)$
                                              $\land\ \textsc{if}\ iterations[$“husband”$] = 0 \land iterations[$“wife”$] = 0$
                                                    $\textsc{then}$ $\land\ total' = [total\ \textsc{except}\ ![self] = account + cash[$“husband”$] + cash[$“
                                                                    $\land\ PrintT(total'[self])$
                                                                    $\land\ Assert(total'[self] = 120,$
                                                                              “Failure of assertion at line 47, column 9.”$)$
                                                    $\textsc{else}$ $\land\ \textsc{true}$
                                                                    $\land\ total' = total$
                                              $\land\ pc' = [pc\ \textsc{except}\ ![self] = $ “Done”$]$
                         $\land\ \textsc{unchanged}\ \langle account,\ cash,\ iterations,\ stack,\ amount1,$
                                             $amount2\rangle$

$s1(self) \triangleq$ $\land\ pc[self] = $ “s1”
                      $\land\ \exists\ amount \in 1\ ..\ 2 :$
                           $\land\ \land\ amount1' = [amount1\ \textsc{except}\ ![self] = amount]$
                              $\land\ stack' = [stack\ \textsc{except}\ ![self] = \langle[procedure \mapsto$ “withdraw”,
                                                                       $pc \mapsto$ “s2”,
                                                                       $amount1 \mapsto amount1[self]]\rangle$
                                                                       $\circ\ stack[self]]$
                           $\land\ pc' = [pc\ \textsc{except}\ ![self] = $ “withdraw_start”$]$
                      $\land\ \textsc{unchanged}\ \langle account,\ cash,\ iterations,\ amount2,\ total\rangle$

$s2(self) \triangleq$ $\land\ pc[self] = $ “s2”
                      $\land\ \exists\ amount \in 1\ ..\ 2 :$
                           $\land\ \land\ amount2' = [amount2\ \textsc{except}\ ![self] = amount]$
                              $\land\ stack' = [stack\ \textsc{except}\ ![self] = \langle[procedure \mapsto$ “deposit”,
```

$$\begin{array}{l}
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad pc \qquad\quad \mapsto \text{"s3"}, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad amount2 \mapsto \; amount2[self]]\rangle \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \circ\, stack[self]] \\
\qquad\qquad\quad \land\, pc' = [pc \text{ EXCEPT } ![self] = \text{"deposit\_start"}] \\
\qquad\qquad \land\, \text{UNCHANGED } \langle account, cash, iterations, amount1, total \rangle
\end{array}$$

$$\begin{array}{lcl}
s3(self) & \triangleq & \land\, pc[self] = \text{"s3"} \\
 & & \land\, iterations' = [iterations \text{ EXCEPT } ![self] = iterations[self] - 1] \\
 & & \land\, total' = [total \text{ EXCEPT } ![self] = account + cash[\text{"husband"}] + cash[\text{"wife"}]] \\
 & & \land\, pc' = [pc \text{ EXCEPT } ![self] = \text{"start"}] \\
 & & \land\, \text{UNCHANGED } \langle account, cash, stack, amount1, amount2 \rangle
\end{array}$$

$$spouse(self) \triangleq start(self) \lor s1(self) \lor s2(self) \lor s3(self)$$

$$\begin{array}{lcl}
Next & \triangleq & (\exists\, self \in ProcSet : withdraw(self) \lor deposit(self)) \\
 & & \quad \lor (\exists\, self \in \{\text{"husband"}, \text{"wife"}\} : spouse(self)) \\
 & & \quad \lor \;\; \text{Disjunct to prevent deadlock on termination} \\
 & & \qquad ((\forall\, self \in ProcSet : pc[self] = \text{"Done"}) \land \text{UNCHANGED } vars)
\end{array}$$

$$Spec \triangleq Init \land \Box[Next]_{vars}$$

$$Termination \triangleq \Diamond(\forall\, self \in ProcSet : pc[self] = \text{"Done"})$$

END TRANSLATION