MODULE *library*

EXTENDS *Naturals*, *Integers*, *TLC*, *Sequences*

$PT \triangleq$ INSTANCE PT

CONSTANTS *Books*, *People*, *NumCopies*

ASSUME $NumCopies \subseteq Nat$ The number of copies you can checkout is a natural number

some shorthand functions to add and remove from a set

$set +\!+ x \triangleq set \cup \{x\}$

$set --\ x \triangleq set \setminus \{x\}$

--algorithm *library*

variables

$library \in [Books \to NumCopies]$, The library is a set of books, each with a number of > 0 copies.

$reserves = [b \in Books \mapsto \langle\rangle]$; Initially,the library has no active reservations

People can only checkout 1 book at a time

define

$AvailableBooks \triangleq \{b \in Books : library[b] > 0\}$ a book is available if it's in the library and it's count is greater than

$BorrowableBooks(p) \triangleq \{b \in AvailableBooks :$

$\lor\ reserves[b] = \langle\rangle$

$\lor\ p = Head(reserves[b])\}$

a book is borrowable if it is not reserved, OR if it is your reserved

end define ;

fair process $person \in People$

variables

$books = \{\}$, The books they have? *TODO JLW*, Why is this not *my_private*

$wants \in$ SUBSET $Books$;

begin

Person:

while TRUE **do**

either

Checkout

with $b \in (BorrowableBooks(self) \cap wants) \setminus books$ **do**

$library[b] := library[b] - 1$; decrement the count in the library

$books := books +\!+ b$;

$wants := wants --\ b$;

if $reserves[b] \neq \langle\rangle \land self = Head(reserves[b])$ **then**

$reserves[b] := Tail(reserves[b])$;

end if ;

```
            end with ;
        or
            Return
            with b ∈ books do
                library[b] := library[b] + 1 ;   put it back in the library
                books := books −− b ;
            end with ;
        or
            Reserve
            with b ∈ {b ∈ Books : self ∉ PT!Range(reserves[b])} do
                reserves[b] := Append(reserves[b], self) ;   Find a book I want to reserve
            end with ;
        or
            Want
            with b ∈ Books \ wants do
                wants := wants ++ b ;
            end with ;
        end either ;
    end while ;
    goto Person ;
end process



end algorithm ;
```

BEGIN TRANSLATION ($chksum(pcal) =$ "c051bee3" $\land\ chksum(tla) =$ "493425c7")

VARIABLES $library$, $reserves$, pc

define statement

$AvailableBooks \triangleq \{b \in Books : library[b] > 0\}$

$BorrowableBooks(p) \triangleq \{b \in AvailableBooks :$
$\quad \lor\ reserves[b] = \langle\rangle$
$\quad \lor\ p = Head(reserves[b])\}$

VARIABLES $books$, $wants$

$vars \triangleq \langle library, reserves, pc, books, wants\rangle$

$ProcSet \triangleq (People)$

$Init \triangleq$ Global variables
$\land\ library \in [Books \to NumCopies]$
$\land\ reserves = [b \in Books \mapsto \langle\rangle]$
Process person
$\land\ books = [self \in People \mapsto \{\}]$
$\land\ wants \in [People \to \text{SUBSET } Books]$
$\land\ pc = [self \in ProcSet \mapsto$ "Person"$]$

$$
\begin{array}{l}
Person(self) \triangleq \ \land\ pc[self] = \text{“Person”} \\
\qquad \land\ \lor\ \land\ \exists\, b \in (BorrowableBooks(self) \cap wants[self]) \setminus books[self] : \\
\qquad\qquad\qquad \land\ library' = [library \text{ EXCEPT } ![b] = library[b] - 1] \\
\qquad\qquad\qquad \land\ books' \ = [books \text{ EXCEPT } ![self] \ = books[self] \ ++\ b] \\
\qquad\qquad\qquad \land\ wants' = [wants \text{ EXCEPT } ![self] = wants[self] -\!\!- b] \\
\qquad\qquad\qquad \land \text{ IF } reserves[b] \neq \langle\rangle \land self \quad\ = Head(reserves[b]) \\
\qquad\qquad\qquad\qquad \text{THEN } \land\ reserves' = [reserves \text{ EXCEPT } ![b] = Tail(reserves[b])] \\
\qquad\qquad\qquad\qquad \text{ELSE } \land \text{ TRUE} \\
\qquad\qquad\qquad\qquad\qquad\ \land \text{ UNCHANGED } reserves \\
\qquad\quad \lor\ \land\ \exists\, b \in books[self] : \\
\qquad\qquad\qquad \land\ library' = [library \text{ EXCEPT } ![b] = library[b] + 1] \\
\qquad\qquad\qquad \land\ books' = [books \text{ EXCEPT } ![self] = books[self] -\!\!- b] \\
\qquad\qquad \land \text{ UNCHANGED } \langle reserves,\ wants\rangle \\
\qquad\quad \lor\ \land\ \exists\, b \in \{b \quad \in Books : self \notin \ PT!Range(reserves[b])\} : \\
\qquad\qquad\qquad reserves' = [reserves \text{ EXCEPT } ![b] = Append(reserves[b],\ self)] \\
\qquad\qquad \land \text{ UNCHANGED } \langle library,\ books,\ wants\rangle \\
\qquad\quad \lor\ \land\ \exists\, b \in Books \setminus wants[self] : \\
\qquad\qquad\qquad wants' = [wants \text{ EXCEPT } ![self] = wants[self] \ ++\ b] \\
\qquad\qquad \land \text{ UNCHANGED } \langle library,\ reserves,\ books\rangle \\
\qquad \land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“Person”}]
\end{array}
$$

$$person(self) \ \triangleq \ Person(self)$$

Allow infinite stuttering to prevent deadlock on termination.

$$
\begin{array}{l}
Terminating \ \triangleq \ \land\ \forall\, self \in ProcSet : pc[self] = \text{“Done”} \\
\qquad\qquad\qquad\quad \land \text{ UNCHANGED } vars
\end{array}
$$

$$
\begin{array}{l}
Next \ \triangleq \ (\exists\, self \in People : person(self)) \\
\qquad\qquad\ \lor\ Terminating
\end{array}
$$

$$
\begin{array}{l}
Spec \ \triangleq \ \land\ Init \land \Box[Next]_{vars} \\
\qquad\qquad\ \land\ \forall\, self \in People : \mathrm{WF}_{vars}(person(self))
\end{array}
$$

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

END TRANSLATION

$$
\begin{array}{l}
NoDuplicateReservations \ \triangleq \\
\quad \forall\, b \in Books : \\
\qquad \forall\, i,\, j \in 1 \,..\, Len(reserves[b]) : \\
\qquad\quad i \neq j \Rightarrow reserves[b][i] \neq reserves[b][j]
\end{array}
$$

$$
\begin{array}{l}
TypeInvariant \ \triangleq \\
\quad \land\ library \in [Books \to NumCopies \ ++\ 0] \quad \text{library is always a map of books to number of copies or 0} \\
\quad \land\ books \ \in [People \to \text{SUBSET } Books] \quad \text{people never have books that aren't from the library} \\
\quad \land\ wants \in [People \to \text{SUBSET } Books] \quad \text{People can only want books we have} \\
\quad \land\ reserves \in [Books \to Seq(People)]
\end{array}
$$

$\land\ NoDuplicateReservations$

$Liveness \triangleq$
$\quad \forall\, p \in People :$
$\quad\quad \forall\, b \in Books :$
$\quad\quad\quad b \in wants[p] \leadsto b \notin wants[p]$

$\land \Diamond(\forall\, p \in People : wants[p] = \{\})$ * Eventually you always get what you want.

* Modification History
* Last modified *Wed Feb* 17 17:06:05 *MST* 2021 by *jeremy*
* Created *Wed Feb* 17 09:26:49 *MST* 2021 by *jeremy*