MODULE *Data*

This module contains basic operators shared by the specifications of the deconstructed and the distributed Bakery algorithms.

EXTENDS *Integers*, *TLAPS*

Lexicographic ordering on pairs of integers.

$$q \ll r \triangleq \lor\ q[1] < r[1] \\ \quad \lor\ \land\ q[1] = r[1] \\ \quad\quad \land\ q[2] < r[2]$$

$Max(i, j) \triangleq$ IF $i \geq j$ THEN i ELSE j

pseudo-value represented as an inverted question mark in the paper

$qm \triangleq$ CHOOSE $v : v \notin Nat$

CONSTANT N

ASSUME $NAssump \triangleq N \in Nat \setminus \{0\}$

Processes and their identities.

$Procs \triangleq 1 \,..\, N$

$OtherProcs(i) \triangleq Procs \setminus \{i\}$

$ProcIds \triangleq \{\langle i \rangle : i \in Procs\}$

$SubProcs \triangleq \{p \in Procs \times Procs : p[1] \neq p[2]\}$

$SubProcsOf(i) \triangleq \{p \in SubProcs : p[1] = i\}$

$WrProcs \triangleq \{w \in Procs \times Procs \times \{\text{“wr”}\} : w[1] \neq w[2]\}$

$MsgProcs \triangleq \{w \in Procs \times Procs \times \{\text{“msg”}\} : w[1] \neq w[2]\}$

Utility lemmas used in the *TLAPS* proofs.

LEMMA $qmNotNat \triangleq qm \notin Nat$

BY *NoSetContainsEverything* DEF qm

LEMMA $TotalOrder \triangleq$

  ASSUME NEW $i \in Procs$, NEW $wi \in Nat$,

    NEW $j \in Procs \setminus \{i\}$, NEW $wj \in Nat$

  PROVE $\langle wi, i \rangle \ll \langle wj, j \rangle \lor \langle wj, j \rangle \ll \langle wi, i \rangle$

BY DEF $\ll$, *Procs*

LEMMA $AsymmetricOrder \triangleq$

  ASSUME NEW $i \in Procs$, NEW $wi \in Nat$,

    NEW $j \in Procs$, NEW $wj \in Nat$

  PROVE $\neg(\langle wi, i \rangle \ll \langle wj, j \rangle \land \langle wj, j \rangle \ll \langle wi, i \rangle)$

BY DEF $\ll$, *Procs*

The provers have a hard time with the process identifiers, and we help them by proving utility lemmas.

LEMMA $DisjointIds \triangleq$

  $\land\ ProcIds \cap SubProcs = \{\}$

$\land$ *ProcIds* $\cap$ *WrProcs* $= \{\}$
$\land$ *ProcIds* $\cap$ *MsgProcs* $= \{\}$
$\land$ *SubProcs* $\cap$ *WrProcs* $= \{\}$
$\land$ *SubProcs* $\cap$ *MsgProcs* $= \{\}$
$\land$ *WrProcs* $\cap$ *MsgProcs* $= \{\}$
BY DEF *ProcIds*, *SubProcs*, *WrProcs*, *MsgProcs*

LEMMA *ProcId* $\triangleq$
ASSUME NEW $i \in Procs$
PROVE $\land \langle i \rangle \in ProcIds$
$\land \langle i \rangle \notin SubProcs$
$\land \langle i \rangle \notin WrProcs$
$\land \langle i \rangle \notin MsgProcs$
BY DEF *ProcIds*, *SubProcs*, *WrProcs*, *MsgProcs*

LEMMA *SubProcId* $\triangleq$
ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $\land \langle i, j \rangle \in SubProcs$
$\land \langle i, j \rangle \notin ProcIds$
$\land \langle i, j \rangle \notin WrProcs$
$\land \langle i, j \rangle \notin MsgProcs$
$\land \langle i, j, \text{"wr"} \rangle \in WrProcs$
$\land \langle i, j, \text{"wr"} \rangle \notin ProcIds$
$\land \langle i, j, \text{"wr"} \rangle \notin SubProcs$
$\land \langle i, j, \text{"wr"} \rangle \notin MsgProcs$
$\land \langle i, j, \text{"msg"} \rangle \in MsgProcs$
$\land \langle i, j, \text{"msg"} \rangle \notin ProcIds$
$\land \langle i, j, \text{"msg"} \rangle \notin SubProcs$
$\land \langle i, j, \text{"msg"} \rangle \notin WrProcs$
BY DEF *ProcIds*, *SubProcs*, *WrProcs*, *MsgProcs*, *OtherProcs*

LEMMA *SubProcsOfEquality* $\triangleq$
ASSUME NEW $p \in Procs$
PROVE $SubProcsOf(p) = \{\langle p, q \rangle : q \in OtherProcs(p)\}$
BY DEF *SubProcsOf*, *SubProcs*, *OtherProcs*

Several variables represent functions of the (informal) type

$[\ i \in Procs \rightarrow\ [\ OtherProcs(i) \rightarrow S\ ]\ ]$

We write this as $POP(S)$ and provide some utility lemmas below.

$PFunc(X, Y) \triangleq$
partial functions from X to Y
UNION $\{[XX \rightarrow Y] : XX \in$ SUBSET $X\}$

$POP(S) \triangleq$
set of functions $[i \in Procs \rightarrow\ [OtherProcs(i) \rightarrow S]]$
$\{f \in [Procs \rightarrow PFunc(Procs, S)] :$

$\quad \forall\, i \in \mathit{Procs} : \text{DOMAIN } f[i] = \mathit{OtherProcs}(i)\}$

LEMMA $\mathit{POP\_construct} \triangleq$
ASSUME NEW S, NEW $s(\_, \_)$,
$\qquad \forall\, p \in \mathit{Procs} : \forall\, q \in \mathit{OtherProcs}(p) : s(p, q) \in S$
PROVE $[p \in \mathit{Procs} \mapsto [q \in \mathit{OtherProcs}(p) \mapsto s(p, q)]] \in \mathit{POP}(S)$
$\langle 1 \rangle$.DEFINE $f(p) \triangleq [q \in \mathit{OtherProcs}(p) \mapsto s(p, q)]$
$\langle 1 \rangle 1.$ ASSUME NEW $p \in \mathit{Procs}$
$\quad$ PROVE $\land\, f(p) \in \mathit{PFunc}(\mathit{Procs}, S)$
$\qquad\qquad \land$ DOMAIN $f(p) = \mathit{OtherProcs}(p)$
$\quad \langle 2 \rangle.\mathit{OtherProcs}(p) \in$ SUBSET Procs
$\qquad$ BY DEF $\mathit{OtherProcs}$
$\quad \langle 2 \rangle$.QED BY DEF PFunc
$\langle 1 \rangle$.QED BY $\langle 1 \rangle 1$, Zenon DEF POP

LEMMA $\mathit{POP\_access} \triangleq$
ASSUME NEW S, NEW $f \in \mathit{POP}(S)$,
$\qquad$ NEW $p \in \mathit{Procs}$, NEW $q \in \mathit{OtherProcs}(p)$
PROVE $f[p][q] \in S$
BY DEF POP, PFunc

LEMMA $\mathit{POP\_except} \triangleq$
ASSUME NEW S, NEW $f \in \mathit{POP}(S)$,
$\qquad$ NEW $p \in \mathit{Procs}$, NEW $q \in \mathit{OtherProcs}(p)$, NEW $s \in S$
PROVE $\land\, [f \text{ EXCEPT } ![p][q] = s] \in \mathit{POP}(S)$
$\qquad \land\, [f \text{ EXCEPT } ![p][q] = s][p][q] = s$
$\qquad \land\, \forall\, pp \in \mathit{Procs} : \forall\, qq \in \mathit{OtherProcs}(pp) :$
$\qquad\quad pp \neq p \lor qq \neq q \Rightarrow [f \text{ EXCEPT } ![p][q] = s][pp][qq] = f[pp][qq]$
BY DEF POP, PFunc, $\mathit{OtherProcs}$

NB: Combining the two following lemmas breaks proofs.
LEMMA $\mathit{POP\_except\_fun\_type} \triangleq$
ASSUME NEW S, NEW $f \in \mathit{POP}(S)$, NEW $p \in \mathit{Procs}$,
$\qquad$ NEW $g(\_, \_)$, $\forall\, q \in \mathit{OtherProcs}(p) : g(p, q) \in S$
PROVE $[f \text{ EXCEPT } ![p] = [q \in \mathit{OtherProcs}(p) \mapsto g(p, q)]] \in \mathit{POP}(S)$
BY DEF POP, PFunc, $\mathit{OtherProcs}$

LEMMA $\mathit{POP\_except\_fun\_value} \triangleq$
ASSUME NEW S, NEW $f \in \mathit{POP}(S)$, NEW $p \in \mathit{Procs}$,
$\qquad$ NEW $g(\_, \_)$, $\forall\, q \in \mathit{OtherProcs}(p) : g(p, q) \in S$
PROVE LET $\mathit{ff} \triangleq [f \text{ EXCEPT } ![p] = [q \in \mathit{OtherProcs}(p) \mapsto g(p, q)]]$
$\qquad$ IN $\land\, \forall\, q \in \mathit{OtherProcs}(p) : \mathit{ff}[p][q] = g(p, q)$
$\qquad\quad \land\, \forall\, pp \in \mathit{Procs} \setminus \{p\} : \forall\, qq \in \mathit{OtherProcs}(pp) : \mathit{ff}[pp][qq] = f[pp][qq]$
BY DEF POP, PFunc, $\mathit{OtherProcs}$

LEMMA $\mathit{POP\_except\_equal} \triangleq$
ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$,

$\quad\quad$ NEW S, NEW $f \in POP(S)$, NEW $g \in POP(S)$, NEW $x \in S$,
$\quad\quad$ $\forall\, k \in Procs : \forall\, l \in OtherProcs(k) :$
$\quad\quad\quad$ $g[k][l] = \text{IF } k = i \land l = j \text{ THEN } x \text{ ELSE } f[k][l]$
$\quad$ PROVE $\;g = [f \text{ EXCEPT } ![i][j] = x]$
BY DEF POP, $PFunc$

* Modification History
* Last modified *Tue Nov* 16 19:50:05 *CET* 2021 by *merz*
* Created *Mon Sep* 06 18:41:47 *CEST* 2021 by *merz*