TLA+ specification of Causal Consistency variants, including CC, CM, and CCv.

See the paper "On Verifying Causal Consistency" ($POPL'2017$).

10 EXTENDS TLC, $Sequences$, $FiniteSets$, $FunctionUtils$

12 CONSTANTS $Keys$, $Vals$
13 $InitVal \triangleq$ CHOOSE $v : v \notin (Keys \cup Vals)$

15 $Operation \triangleq [op : \{\text{"read"}, \text{"write"}\}, key : Keys, val : Vals]$
16 $R(k, v) \triangleq [op \mapsto \text{"read"}, key \mapsto k, val \mapsto v]$
17 $W(k, v) \triangleq [op \mapsto \text{"write"}, key \mapsto k, val \mapsto v]$

19 $Session \triangleq Seq(Operation)$ A session $s \in Session$ is a sequence of operations.
20 $History \triangleq$ SUBSET $Session$ A history $h \in History$ is a set of sessions.

Test case: The following histories are from Figure 2 of the $POPL'2017$ paper.

Naming:

$- ha$: history of Figure 2(a)
$- hasa$: session a of history ha

30 $hasa \triangleq \langle W(\text{"x"}, 1), R(\text{"x"}, 2) \rangle$
31 $hasb \triangleq \langle W(\text{"x"}, 2), R(\text{"x"}, 1) \rangle$
32 $ha \triangleq \{hasa, hasb\}$ CM but not CCv

34 $hbsa \triangleq \langle W(\text{"z"}, 1), W(\text{"x"}, 1), W(\text{"y"}, 1) \rangle$
35 $hbsb \triangleq \langle W(\text{"x"}, 2), R(\text{"z"}, 0), R(\text{"y"}, 1), R(\text{"x"}, 2) \rangle$
36 $hb \triangleq \{hbsa, hbsb\}$ CCv but not CM

38 $hcsa \triangleq \langle W(\text{"x"}, 1) \rangle$
39 $hcsb \triangleq \langle W(\text{"x"}, 2), R(\text{"x"}, 1), R(\text{"x"}, 2) \rangle$
40 $hc \triangleq \{hcsa, hcsb\}$ CC but not CM nor CCv

42 $hdsa \triangleq \langle W(\text{"x"}, 1), R(\text{"y"}, 0), W(\text{"y"}, 1), R(\text{"x"}, 1) \rangle$
43 $hdsb \triangleq \langle W(\text{"x"}, 2), R(\text{"y"}, 0), W(\text{"y"}, 2), R(\text{"x"}, 2) \rangle$
44 $hd \triangleq \{hdsa, hdsb\}$ CC, CM, and CCv but no SC

46 $hesa \triangleq \langle W(\text{"x"}, 1), W(\text{"y"}, 1) \rangle$
47 $hesb \triangleq \langle R(\text{"y"}, 1), W(\text{"x"}, 2) \rangle$
48 $hesc \triangleq \langle R(\text{"x"}, 2), R(\text{"x"}, 1) \rangle$
49 $he \triangleq \{hesa, hesb, hesc\}$ not CC (nor CM, nor CCv)
50 ├──

Program order: a union of total orders among operations in the same session.

54 $ProgramOrder(h) \triangleq$
55   LET RECURSIVE $SessionProgramOrder(\_)$
56        $SessionProgramOrder(s) \triangleq$
57   IF $s = \langle \rangle$ THEN $\{\}$

```
58          ELSE  LET  sh  ≜  Head(s)
59                     st  ≜  Tail(s)
60               IN    {⟨sh, t⟩ : t ∈ Range(st)} ∪ SessionProgramOrder(st)
61     IN    UNION {SessionProgramOrder(s) : s ∈ h}
```

Test case: *TODO*: *Cardinality* testing

```
66   CardOfProgramOrderOf(h) ≜
67   THEOREM  CardOfProgramOrderTheorem ≜
68    ∀ h ∈ {ha, hb, hc, hd, he}:
69      Cardinality(ProgramOrder(h)) = CardOfProgramOrderOf(h)
70 ├─────────────────────────────────────────────────────────────────┤
```

Sequential semantics of read-write registers.

```
74 ├─────────────────────────────────────────────────────────────────┤
```

Utilities.

FIXME: there may be multiple same operations in one and more sessions.

```
80   Ops(h) ≜    Return the set of all operations in history h ∈ History.
81     UNION {Range(s) : s ∈ h}
82 ├─────────────────────────────────────────────────────────────────┤
```

Specification of Causal Consistency: *CC*, *CCv*, and *CM*

```
86   CCv(h) ≜    Check whether h ∈ History satisfies CCv (Causal Convergence)
87    ∧ LET  ops ≜ Ops(h)
88       IN    ∧ ∃ co ∈ SUBSET (ops × ops) :
89                 ∃ arb ∈ SUBSET (ops × ops) :
90                   ∀ op ∈ ops : TRUE
91       ∧ FALSE
92 └─────────────────────────────────────────────────────────────────┘
```