```
1  ---------- MODULE CC ----------
   TLA+ specification of Causal Consistency variants, including CC, CM, and CCv.
   See the paper "On Verifying Causal Consistency" (POPL'2017).
8  EXTENDS Naturals, Sequences, Functions, FiniteSets, FiniteSetsExt, RelationUtils, TLC

10 CONSTANTS Keys, Vals
11 InitVal ≜ CHOOSE v : v ∉ (Keys ∪ Vals)

13  oid: unique operation identifier
14 Operation ≜ [op : {"read", "write"}, key : Keys, val : Vals, oid : Nat]
15 R(k, v, oid) ≜ [op ↦ "read", key ↦ k, val ↦ v, oid ↦ oid]
16 W(k, v, oid) ≜ [op ↦ "write", key ↦ k, val ↦ v, oid ↦ oid]

18 Session ≜ Seq(Operation)  A session s ∈ Session is a sequence of operations.
19 History ≜ SUBSET Session  A history h ∈ History is a set of sessions.
20 ----------

   Utilities.
24 Ops(h) ≜  Return the set of all operations in history h ∈ History.
25   UNION {Range(s) : s ∈ h}
26 ----------

   Well-formedness of history h ∈ History:
   – TODO: type invariants
   - uniqueness of oids
33 WellFormed(h) ≜
34  ∧ h ∈ History
35   ∧ Cardinality(Ops(h)) = ReduceSet(LAMBDA s, x : Len(s) + x, h, 0)
36 ----------

   Program order: a union of total orders among operations in the same session.
40 ProgramOrder(h) ≜ UNION {Seq2Rel(s) : s ∈ h}
41 ----------

   Sequential semantics of read-write registers.
45 ----------

   Specification of Causal Consistency: CC, CCv, and CM
49 CCv(h) ≜  Check whether h ∈ History satisfies CCv (Causal Convergence)
50   ∧ WellFormed(h)
51   ∧ LET ops ≜ Ops(h)
52     IN   ∧ ∃ co ∈ SUBSET (ops × ops) :
53             ∃ arb ∈ SUBSET (ops × ops) :
54               ∧ IsStrictPartialOrder(co, ops)
55               ∧ IsStrictTotalOrder(arb, ops)
56               ∧ Respect(co, ProgramOrder(h))   AxCausal
57               ∧ Respect(arb, co)               AxArb
58               ∧ ∀ op ∈ ops : TRUE              TODO: AxCausalArb
59   ∧ FALSE
```

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

Naming Conventions:

– *ha*: history of Figure 2(*a*)
– *hasa*: session a of history ha

TODO: to automatically generate histories

$hasa \triangleq \langle W(\text{“x”}, 1, 1),\ R(\text{“x”}, 2, 2)\rangle$
$hasb \triangleq \langle W(\text{“x”}, 2, 3),\ R(\text{“x”}, 1, 4)\rangle$
$ha \triangleq \{hasa, hasb\}$ *CM* but not *CCv*

$hbsa \triangleq \langle W(\text{“z”}, 1, 1),\ W(\text{“x”}, 1, 2),\ W(\text{“y”}, 1, 3)\rangle$
$hbsb \triangleq \langle W(\text{“x”}, 2, 4),\ R(\text{“z”}, 0, 5),\ R(\text{“y”}, 1, 6),\ R(\text{“x”}, 2, 7)\rangle$
$hb \triangleq \{hbsa, hbsb\}$ *CCv* but not *CM*

$hcsa \triangleq \langle W(\text{“x”}, 1, 1)\rangle$
$hcsb \triangleq \langle W(\text{“x”}, 2, 2),\ R(\text{“x”}, 1, 3),\ R(\text{“x”}, 2, 4)\rangle$
$hc \triangleq \{hcsa, hcsb\}$ *CC* but not *CM* nor *CCv*

$hdsa \triangleq \langle W(\text{“x”}, 1, 1),\ R(\text{“y”}, 0, 2),\ W(\text{“y”}, 1, 3),\ R(\text{“x”}, 1, 4)\rangle$
$hdsb \triangleq \langle W(\text{“x”}, 2, 5),\ R(\text{“y”}, 0, 6),\ W(\text{“y”}, 2, 7),\ R(\text{“x”}, 2, 8)\rangle$
$hd \triangleq \{hdsa, hdsb\}$ *CC*, *CM*, and *CCv* but no *SC*

$hesa \triangleq \langle W(\text{“x”}, 1, 1),\ W(\text{“y”}, 1, 2)\rangle$
$hesb \triangleq \langle R(\text{“y”}, 1, 3),\ W(\text{“x”}, 2, 4)\rangle$
$hesc \triangleq \langle R(\text{“x”}, 2, 5),\ R(\text{“x”}, 1, 6)\rangle$
$he \triangleq \{hesa, hesb, hesc\}$ not *CC* (nor *CM*, nor *CCv*)

THEOREM $WellFormedTheorem \triangleq$
  $\forall\, h \in \{ha, hb, hc, hd, he\} : WellFormed(h)$

$CardOfProgramOrderOfHistory(h) \triangleq$
  LET $CardOfProgramOrderOfSession(s) \triangleq$
    IF $Len(s) \leq 1$ THEN 0 ELSE $Sum(1\,..\,Len(s)-1)$
  IN $ReduceSet(\text{LAMBDA } s, x : CardOfProgramOrderOfSession(s) + x,\ h,\ 0)$

THEOREM $ProgramOrderCardinalityTheorem \triangleq$
  $\forall\, h \in \{ha, hb, hc, hd, he\} :$
    $Cardinality(ProgramOrder(h)) = CardOfProgramOrderOfHistory(h)$

* Modification *History*
* Last modified *Mon Apr* 05 15:27:39 *CST* 2021 by *hengxin*
* Created *Tue Apr* 01 10:24:07 *CST* 2021 by *hengxin*