```
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, FiniteSets, Functions, 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 ----------

   Sequential semantics of read-write registers.
40 ----------

   Auxiliary definitions for the axioms used in the definitions of causal consistency
44  The program order of h ∈ History is a union of total orders among operations in the same session
45 ProgramOrder(h) ≜ UNION {Seq2Rel(s) : s ∈ h}

47  The set of operations that preceed o ∈ Operation in program order in history h ∈ History
48 POPast(h, o) ≜ InverseImage(ProgramOrder(h), o)

50  The set of operations that preceed o ∈ Operation in causal order co
51 CausalPast(co, o) ≜ InverseImage(co, o)

53  The restriction of arbitration arb to the operations in the causal past of operation o ∈ Operation
54 CausalArb(co, arb, o) ≜ arb | CausalPast(co, o)
55 ----------

   Axioms used in the defintions of causal consistency
59  AxCausalArb ≜
60 ----------
```

```
    Specification of Causal Consistency: CC, CCv, and CM
64  CCv(h) ≜  Check whether h ∈ History satisfies CCv (Causal Convergence)
65    ∧ WellFormed(h)
66    ∧ LET ops ≜ Ops(h)
67      IN    ∧ ∃ co ∈ SUBSET (ops × ops) :   FIXME: efficiency!!!
68                ∃ arb ∈ SUBSET (ops × ops) :
69                  ∧ IsStrictPartialOrder(co, ops)
70                  ∧ IsStrictTotalOrder(arb, ops)
71                  ∧ Respect(co, ProgramOrder(h))   AxCausal
72                  ∧ Respect(arb, co)               AxArb
73                  ∧ ∀ op ∈ ops : TRUE              TODO: AxCausalArb
74    ∧ FALSE
75
    \* Modification History
    \* Last modified Fri Apr 09 12:46:47 CST 2021 by hengxin
    \* Created Tue Apr 01 10:24:07 CST 2021 by hengxin
```