```
┌──────────────────────────── MODULE Record ────────────────────────────┐
It is necessary to use type invariant when reasoning about EXCEPT expressions. See step ⟨4⟩2 in
the proof for Spec ⇒ SV!Spec.

See https://groups.google.com/d/msg/tlaplus/rmmH9vFwH_0/rY18YWMGDQAJ.
EXTENDS Naturals, TLAPS
├──────────────────────────────────────────────────────────────────────┤
CONSTANTS Participant   the set of partipants

VARIABLES state   state[p][q]: the state of q ∈ Participant from the view of p ∈ Participant

State ≜ [maxBal : Nat, maxVBal : Nat]

TypeOK ≜ state ∈ [Participant → [Participant → State]]
├──────────────────────────────────────────────────────────────────────┤
InitState ≜ [maxBal ↦ 0, maxVBal ↦ 0]

Init ≜ state = [p ∈ Participant ↦ [q ∈ Participant ↦ InitState]]

Prepare(p, b) ≜
    ∧ state[p][p].maxBal < b
    ∧ state′ = [state EXCEPT ![p][p].maxBal = b]
├──────────────────────────────────────────────────────────────────────┤
Next ≜ ∃ p ∈ Participant, b ∈ Nat : Prepare(p, b)

Spec ≜ Init ∧ □[Next]_state
├──────────────────────────────────────────────────────────────────────┤
Record refines SimpleVoting
maxBal ≜ [p ∈ Participant ↦ state[p][p].maxBal]

SV ≜ INSTANCE SimpleVoting

THEOREM Invariant ≜ Spec ⇒ □TypeOK
  OMITTED

THEOREM Spec ⇒ SV!Spec
  ⟨1⟩1. Init      ⇒ SV!Init
    BY DEF Init, SV!Init, maxBal, InitState
  ⟨1⟩2. TypeOK ∧ [Next]_state ⇒ [SV!Next]_maxBal
    ⟨2⟩1. UNCHANGED state ⇒ UNCHANGED maxBal
      BY DEF maxBal
    ⟨2⟩2. TypeOK ∧ Next ⇒ SV!Next
      ⟨3⟩ SUFFICES ASSUME NEW p ∈ Participant, NEW b ∈ Nat,
                          TypeOK,
                          Prepare(p, b)
                   PROVE  SV!IncreaseMaxBal(p, b)
        BY DEF Next, SV!Next
      ⟨3⟩1. maxBal[p] < b
      BY  DEF Prepare, maxBal
    ⟨3⟩2. maxBal′ = [maxBal EXCEPT ![p] = b]
      BY  DEF Prepare, maxBal, TypeOK, State
    ⟨3⟩3. QED
      BY ⟨3⟩1, ⟨3⟩2  DEF SV!IncreaseMaxBal
  ⟨2⟩3. QED
    BY ⟨2⟩1, ⟨2⟩2
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, Invariant, PTL DEF SV!Spec, Spec
```

* Modification History

* Last modified *Mon Aug* 19 22:26:16 *CST* 2019 by *hengxin*

* Created *Thu Aug* 15 10:52:49 *CST* 2019 by *hengxin*