```
1  ---------- MODULE Record ----------
2  EXTENDS Naturals, TLAPS
3  ----------------------------------
4  CONSTANTS Participant   the set of partipants
6  VARIABLES state   state[p][q]: the state of q ∈ Participant from the view of p ∈ Participant
8  State ≜ [maxBal : Nat, maxVBal : Nat]
10 TypeOK ≜ state ∈ [Participant → [Participant → State]]
11 ----------------------------------
12 InitState ≜ [maxBal ↦ 0, maxVBal ↦ 0]
14 Init ≜ state = [p ∈ Participant ↦ [q ∈ Participant ↦ InitState]]
16 Prepare(p, b) ≜
17     ∧ state[p][p].maxBal < b
18     ∧ state' = [state EXCEPT ![p][p].maxBal = b]
19 ----------------------------------
20 Next ≜ ∃ p ∈ Participant, b ∈ Nat : Prepare(p, b)
22 Spec ≜ Init ∧ □[Next]_state
23 ----------------------------------
   Record refines SimpleVoting
27 maxBal ≜ [p ∈ Participant ↦ state[p][p].maxBal]
29 SV ≜ INSTANCE SimpleVoting
31 THEOREM Invariant ≜ Spec ⇒ □TypeOK
32   OMITTED
34 THEOREM Spec ⇒ SV!Spec
35   ⟨1⟩1. Init       ⇒ SV!Init
36     BY DEF Init, SV!Init, maxBal, InitState
37   ⟨1⟩2. [Next]_state ⇒ [SV!Next]_maxBal
38     ⟨2⟩1. UNCHANGED state ⇒ UNCHANGED maxBal
39       BY DEF maxBal
40     ⟨2⟩2. Next ⇒ SV!Next
41       ⟨3⟩ ASSUME NEW p ∈ Participant, NEW b ∈ Nat,
42                  Prepare(p, b)
43           PROVE  SV!IncreaseMaxBal(p, b)  SV!Next
44         ⟨4⟩1. maxBal[p] < b  Wrong decomposition: maxBal[p]SV! < b
45           BY DEF Prepare, maxBal
46         ⟨4⟩2. maxBal' = [maxBal EXCEPT ![p] = b]
47           BY DEF Prepare, maxBal
48         ⟨4⟩3. QED
49           BY ⟨4⟩1, ⟨4⟩2 DEF SV!IncreaseMaxBal
50       ⟨3⟩1. QED
```

```
        BY  DEF Next, SV!Next
  ⟨2⟩3. QED
    BY ⟨2⟩1, ⟨2⟩2
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, PTL DEF SV!Spec, Spec
```

\ * Modification History

\ * Last modified *Thu Aug* 15 11:51:11 *CST* 2019 by *hengxin*

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