

```

1 |----- MODULE Record -----|
2 | EXTENDS Naturals, TLAPS |
3 |-----|
4 | CONSTANTS Participant  the set of partipants
5 |
6 | VARIABLES state  state[p][q]: the state of q ∈ Participant from the view of p ∈ Participant
7 |
8 | State ≜ [maxBal : Nat, maxVBal : Nat]
9 |
10 | TypeOK ≜ state ∈ [Participant → [Participant → State]]
11 |-----|
12 | InitState ≜ [maxBal ↦ 0, maxVBal ↦ 0]
13 |
14 | Init ≜ state = [p ∈ Participant ↦ [q ∈ Participant ↦ InitState]]
15 |
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)
21 |
22 | Spec ≜ Init ∧ □[Next]state
23 |-----|
24 | Record refines SimpleVoting
25 |-----|
26 |
27 | maxBal ≜ [p ∈ Participant ↦ state[p][p].maxBal]
28 |
29 | SV ≜ INSTANCE SimpleVoting
30 |
31 | THEOREM Invariant ≜ Spec ⇒ □TypeOK
32 | OMITTED
33 |
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⟩ SUFFICES ASSUME NEW p ∈ Participant, NEW b ∈ Nat,
42 |     Prepare(p, b)
43 |     PROVE SV!IncreaseMaxBal(p, b)
44 |     BY DEF Next, SV!Next
45 |     ⟨3⟩1. maxBal[p] < b
46 |     BY DEF Prepare, maxBal
47 |     ⟨3⟩2. maxBal' = [maxBal EXCEPT ![p] = b] failed here!
48 |     BY DEF Prepare, maxBal
49 |     ⟨3⟩3. QED
50 |     BY ⟨3⟩1, ⟨3⟩2 DEF SV!IncreaseMaxBal

```

```

51       $\langle 2 \rangle 3$ . QED
52      BY  $\langle 2 \rangle 1$ ,  $\langle 2 \rangle 2$ 
53       $\langle 1 \rangle 3$ . QED
54      BY  $\langle 1 \rangle 1$ ,  $\langle 1 \rangle 2$ , PTL DEF SV!Spec, Spec
55  ┌──────────────────────────────────────────────────────────────────────────────────┐
    \ * Modification History
    \ * Last modified Sat Aug 17 14:43:49 CST 2019 by hengxin
    \ * Created Thu Aug 15 10:52:49 CST 2019 by hengxin

```