

```

1  ┌────────────────────────── MODULE SplitLess_group_join_leave ───────────────────────────┐
2  └────────────────────────── EXTENDS Naturals ───────────────────────────┘

4  CONSTANTS
5      USERS,
6      POSSIBLE_REPLICA_IDS,
7      ASSIGNED_REPLICA,
8      INITIAL_MEMBER

10 VARIABLES
11     replicas, actionCounter

13     ┌──────────────────────────
14     │ Records ┌──────────────────────────
15     │ └──────────────────────────
16     Group  $\triangleq$  [ members : [USERS  $\rightarrow$  Nat],
17                     invited_members : [USERS  $\rightarrow$  Nat]]

19     Replica  $\triangleq$  [id : POSSIBLE_REPLICA_IDS,
20                     group : Group]

23     ┌──────────────────────────
24     │ Initialization ┌──────────────────────────
25     │ └──────────────────────────
26     Init  $\triangleq$ 
27          $\wedge$  LET InitialGroup  $\triangleq$ 
28             [members  $\mapsto$  [u  $\in$  USERS  $\mapsto$  0],
29             invited_members  $\mapsto$  [u  $\in$  USERS  $\mapsto$  IF u = INITIAL_MEMBER THEN 1 ELSE 0]]
30         IN  $\wedge$  replicas = [rid  $\in$  POSSIBLE_REPLICA_IDS  $\mapsto$  [group  $\mapsto$  InitialGroup]]

32         ┌──────────────────────────
33         │ replicas = [rid  $\in$  POSSIBLE_REPLICA_IDS
34         │      $\mapsto$  [id  $\mapsto$  rid,
35         │     group  $\mapsto$  INITIAL_GROUP] ]
36         └──────────────────────────
37          $\wedge$  actionCounter = 0

38     ┌──────────────────────────
39     │ Helper Actions ┌──────────────────────────
40     │ └──────────────────────────
41     IsMember(memberCounter)  $\triangleq$ 
42         memberCounter%2 = 1

44     IsMemberContender(memberCounter)  $\triangleq$ 
45         memberCounter%2 = 1

48     ┌──────────────────────────
49     │ Group Actions ┌──────────────────────────

```

```

50       
51 InviteMember  $\triangleq$ 
52    $\exists actor, newMember \in USERS :$ 
53    $\exists rid \in POSSIBLE\_REPLICA\_IDs :$ 
54      $\wedge ASSIGNED\_REPLICA[actor] = rid$ 
55      $\wedge IsMember(replicas[rid].group.members[actor])$ 
56      $\wedge \neg IsMember(replicas[rid].group.members[newMember])$ 
57      $\wedge \neg IsMemberContender(replicas[rid].group.invited\_members[newMember])$ 
58      $\wedge LET newReplica \triangleq$ 
59        $[replicas[rid] \text{ EXCEPT } !.group.invited\_members[newMember] = @ + 1]$ 
60     IN
61        $\wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
62        $\wedge actionCounter' = actionCounter + 1$ 

64 AcceptInvitation  $\triangleq$ 
65    $\exists actor \in USERS :$ 
66    $\exists rid \in POSSIBLE\_REPLICA\_IDs :$ 
67      $\wedge ASSIGNED\_REPLICA[actor] = rid$ 
68      $\wedge IsMemberContender(replicas[rid].group.invited\_members[actor])$ 
69      $\wedge LET newReplica \triangleq$ 
70        $[replicas[rid] \text{ EXCEPT }$ 
71          $!.group.invited\_members[actor] = @ + 1,$ 
72          $!.group.members[actor] = @ + 1]$ 
73     IN
74        $\wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
75        $\wedge actionCounter' = actionCounter + 1$ 

77 LeaveGroup  $\triangleq$ 
78    $\exists actor \in USERS :$ 
79    $\exists rid \in POSSIBLE\_REPLICA\_IDs :$ 
80      $\wedge ASSIGNED\_REPLICA[actor] = rid$ 
81      $\wedge IsMember(replicas[rid].group.members[actor])$ 
82      $\wedge LET newReplica \triangleq$ 
83        $[replicas[rid] \text{ EXCEPT } !.group.members[actor] = @ + 1]$ 
84     IN
85        $\wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
86        $\wedge actionCounter' = actionCounter + 1$ 

89       
90 Merge action
91       
92 MergeReplicas  $\triangleq$ 
93    $\exists ownRid, otherRid \in POSSIBLE\_REPLICA\_IDs :$ 
94      $\wedge ownRid \neq otherRid$ 
95      $\wedge LET$ 

```

96 $merged_members \triangleq$
 97 $[u \in USERS \mapsto$
 98 $\text{CHOOSE } n \in \{replicas[ownRid].group.members[u], replicas[otherRid].group.members[u]\} :$
 99 $n \geq replicas[ownRid].group.members[u] \wedge n \geq replicas[otherRid].group.members[u]]$
 100 $merged_persumed_membrs \triangleq$
 101 $[u \in USERS \mapsto$
 102 $\text{CHOOSE } n \in \{replicas[ownRid].group.invited_members[u], replicas[otherRid].group.invited_members[u]\} :$
 103 $n \geq replicas[ownRid].group.invited_members[u] \wedge n \geq replicas[otherRid].group.invited_members[u]]$
 104 $merged_group \triangleq$
 105 $[replicas[ownRid].group \text{ EXCEPT } !.members = merged_members,$
 106 $!.invited_members = merged_persumed_membrs]$
 107 IN $\wedge replicas' = [replicas \text{ EXCEPT } ![ownRid].group = merged_group]$
 108 $\wedge \text{UNCHANGED } actionCounter$

111 $Next \triangleq$
 112 $\vee InviteMember$
 113 $\vee AcceptInvitation$
 114 $\vee LeaveGroup$
 115 $\vee MergeReplicas$
 116 $\vee \text{UNCHANGED } \langle replicas, actionCounter \rangle$

122 $TypeOK \triangleq$
 123 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 124 $\wedge replicas[rid].group$
 125 $\in Group$

130 $Liveness \text{ Helper} \triangleq$
 131 $AllReplicasHaveAtLeastGroupMemberCounter(user, member_counter) \triangleq$
 132 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 133 $\wedge replicas[rid].group.members[user] \geq member_counter$
 134 $AllReplicasHaveAtLeastGroupPersumedMemberCounter(user, persumend_member_counter) \triangleq$
 135 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 136 $\wedge replicas[rid].group.invited_members[user] \geq persumend_member_counter$

141 $Liveness$
 142

```

143 _____
144 Liveness_GroupMemberShipPropagates  $\triangleq$ 
145    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
146      $\forall user \in USERS :$ 
147        $\Box \Diamond AllReplicasHaveAtLeastGroupMemberCounter(user, replicas[rid].group.members[user])$ 
149 Liveness_PersumedGroupMemberShipPropagates  $\triangleq$ 
150    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
151      $\forall user \in USERS :$ 
152        $\Box \Diamond AllReplicasHaveAtLeastGroupPersumedMemberCounter(user, replicas[rid].group.invited\_mem$ 

```

Safety Helper

```

158 MemberOnlyAfterInvitation  $\triangleq$ 
159    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
160      $\forall u \in USERS :$ 
161        $\wedge ASSIGNED\_REPLICA[u] = rid$ 
162        $\wedge \neg IsMember(replicas[rid].group.members[u])$ 
163        $\wedge IsMember(replicas'[rid].group.members[u])$ 
164        $\Rightarrow$ 
165        $\wedge IsMemberContender(replicas[rid].group.invited\_members[u])$ 
167 NoDecreaseMembershipCounters  $\triangleq$ 
168    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
169      $\forall u \in USERS :$ 
170        $replicas'[rid].group.members[u]$ 
171        $\geq replicas[rid].group.members[u]$ 
172        $\wedge replicas'[rid].group.invited\_members[u]$ 
173        $\geq replicas[rid].group.invited\_members[u]$ 

```

Safety

```

178 Safety_MemberOnlyAfterInvitation  $\triangleq$ 
179    $\Box [MemberOnlyAfterInvitation]_{\langle replicas, actionCounter \rangle}$ 
181 Safety_NoDecreaseMembershipCounters  $\triangleq$ 
182    $\Box [NoDecreaseMembershipCounters]_{\langle replicas, actionCounter \rangle}$ 

```

```

185 _____

```

Specification

```

186 _____
187 _____
188 Spec  $\triangleq Init \wedge \Box [Next]_{\langle replicas, actionCounter \rangle}$ 
189 FairSpec  $\triangleq Spec \wedge WF_{\langle replicas, actionCounter \rangle}(MergeReplicas)$ 

```

```

191 

```

```

\ * Modification History
\ * Last modified Thu Jan 15 10:42:22 CET 2026 by floyd

```

* Created *Mon Nov 24 10:30:46 CET 2025* by *floyd*