

```

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   replicas = [rid  $\in$  POSSIBLE_REPLICA_IDS
33      $\mapsto$  [id  $\mapsto$  rid,
34       group  $\mapsto$  INITIAL_GROUP] ]
35    $\wedge$  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   
$$\boxed{\quad}$$

51   
$$InviteMember \triangleq$$

52   
$$\exists actor, newMember \in USERS :$$

53   
$$\exists rid \in POSSIBLE\_REPLICA\_IDs :$$

54   
$$\quad \wedge ASSIGNED\_REPLICA[actor] = rid$$

55   
$$\quad \wedge IsMember(replicas[rid].group.members[actor])$$

56   
$$\quad \wedge \neg IsMember(replicas[rid].group.members[newMember])$$

57   
$$\quad \wedge \neg IsMemberContender(replicas[rid].group.invited_members[newMember])$$

58   
$$\quad \wedge \text{LET } newReplica \triangleq$$

59   
$$\quad \quad [replicas[rid] \text{ EXCEPT } !.group.invited_members[newMember] = @ + 1]$$

60   
$$\quad \quad \text{IN}$$

61   
$$\quad \quad \wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$$

62   
$$\quad \quad \wedge actionCounter' = actionCounter + 1$$


64   
$$AcceptInvitation \triangleq$$

65   
$$\exists actor \in USERS :$$

66   
$$\exists rid \in POSSIBLE\_REPLICA\_IDs :$$

67   
$$\quad \wedge ASSIGNED\_REPLICA[actor] = rid$$

68   
$$\quad \wedge IsMemberContender(replicas[rid].group.invited_members[actor])$$

69   
$$\quad \wedge \text{LET } newReplica \triangleq$$

70   
$$\quad \quad [replicas[rid] \text{ EXCEPT }$$

71   
$$\quad \quad \quad !.group.invited_members[actor] = @ + 1,$$

72   
$$\quad \quad \quad !.group.members[actor] = @ + 1]$$

73   
$$\quad \quad \text{IN}$$

74   
$$\quad \quad \wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$$

75   
$$\quad \quad \wedge actionCounter' = actionCounter + 1$$


77   
$$LeaveGroup \triangleq$$

78   
$$\exists actor \in USERS :$$

79   
$$\exists rid \in POSSIBLE\_REPLICA\_IDs :$$

80   
$$\quad \wedge ASSIGNED\_REPLICA[actor] = rid$$

81   
$$\quad \wedge IsMember(replicas[rid].group.members[actor])$$

82   
$$\quad \wedge \text{LET } newReplica \triangleq$$

83   
$$\quad \quad [replicas[rid] \text{ EXCEPT } !.group.members[actor] = @ + 1]$$

84   
$$\quad \quad \text{IN}$$

85   
$$\quad \quad \wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$$

86   
$$\quad \quad \wedge actionCounter' = actionCounter + 1$$


89   
$$\boxed{\quad}$$

90   Merge action 
$$\boxed{\quad}$$

91   
$$\boxed{\quad}$$

92   
$$MergeReplicas \triangleq$$

93   
$$\exists ownRid, otherRid \in POSSIBLE\_REPLICA\_IDs :$$

94   
$$\quad \wedge ownRid \neq otherRid$$

95   
$$\quad \wedge \text{LET }$$


```

```

96      merged_members  $\triangleq$ 
97          [u  $\in$  USERS  $\mapsto$ 
98              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                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 EXCEPT !.members = merged_members,
106                !.invited_members = merged_persumed_membrs]
107            IN  $\wedge$  replicas' = [replicas EXCEPT ![ownRid].group = merged_group]
108             $\wedge$  UNCHANGED actionCounter

111      _____
112  Next relation _____
113
114  Next  $\triangleq$ 
115       $\vee$  InviteMember
116       $\vee$  AcceptInvitation
117       $\vee$  LeaveGroup
118       $\vee$  MergeReplicas
119       $\vee$  UNCHANGED (replicas, actionCounter)

122      _____
123  Invariants _____
124
125  TypeOK  $\triangleq$ 
126       $\forall$  rid  $\in$  POSSIBLE_REPLICA_IDS :
127           $\wedge$  replicas[rid].group
128               $\in$  Group

130      _____
131  Liveness Helper _____
132
133  AllReplicasHaveAtLeastGroupMemberCounter(user, member_counter)  $\triangleq$ 
134       $\forall$  rid  $\in$  POSSIBLE_REPLICA_IDS :
135           $\wedge$  replicas[rid].group.members[user]  $\geq$  member_counter

137  AllReplicasHaveAtLeastGroupPersumedMemberCounter(user, persumend_member_counter)  $\triangleq$ 
138       $\forall$  rid  $\in$  POSSIBLE_REPLICA_IDS :
139           $\wedge$  replicas[rid].group.invited_members[user]  $\geq$  persumend_member_counter

141      _____
142  Liveness

```

```

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

```

#### 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    $\square[MemberOnlyAfterInvitation]_{\langle replicas, actionCounter \rangle}$ 
181  $Safety\_NoDecreaseMembershipCounters \triangleq$ 
182    $\square[NoDecreaseMembershipCounters]_{\langle replicas, actionCounter \rangle}$ 

```

185 \_\_\_\_\_

186 Specification

187 \_\_\_\_\_

```

188  $Spec \triangleq Init \wedge \square[Next]_{\langle replicas, actionCounter \rangle}$ 
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*