

```

1  ┌────────────────── MODULE SplitLess_replica_group_expenses ───────────────────┐
2  EXTENDS Naturals, Sequences, FiniteSets

4  CONSTANTS
5      USERS,
6      POSSIBLE_SHARES,
7      POSSIBLE_EXPENSE_IDS,
8      POSSIBLE_GROUP_IDS,
9      NO_EXPENSE,
10     NO_GROUP,
11     POSSIBLE_REPLICA_IDS,
12     ASSIGNED_REPLICA

14  VARIABLES replicas, actionCounter

16  ┌──────────────────
17  Records ┌──────────────────
18  └──────────────────

20  Expense  $\triangleq$ 
21      [id : POSSIBLE_EXPENSE_IDS,
22       group : POSSIBLE_GROUP_IDS  $\cup$  {NO_GROUP},
23       version : Nat, current version of expense, only payer can edit expense and each user only works on at most one re
24       payer : USERS,
25       amount : Nat,
26       shares : POSSIBLE_SHARES,
27       shares : [USERS  $\rightarrow$  Nat], if payer absorbs the share of a left member, their share can be higher than the max in
28       acknowledged_shares : [USERS  $\rightarrow$  BOOLEAN ],
29       deleted : BOOLEAN ]

31  Group  $\triangleq$ 
32      [id : POSSIBLE_GROUP_IDS,
33       members : [USERS  $\rightarrow$  Nat], Casul length counter for each user
34       totalGifted : Nat,
35       individualGiftsSent : [USERS  $\rightarrow$  Nat]]

37  Replica  $\triangleq$ 
38      [id : POSSIBLE_REPLICA_IDS,
39       recordedExpenses : [POSSIBLE_EXPENSE_IDS  $\rightarrow$  (Expense  $\cup$  {NO_EXPENSE})],
40       groups : [POSSIBLE_GROUP_IDS  $\rightarrow$  (Group  $\cup$  {NO_GROUP})]
41      ]

43  ┌──────────────────
44  Initialization ┌──────────────────
45  └──────────────────

46  Init  $\triangleq$ 
47       $\wedge$  replicas =

```

```

48      [rid ∈ POSSIBLE_REPLICA_IDS ↦
49      [id ↦ rid,
50      recordedExpenses ↦ [eid ∈ POSSIBLE_EXPENSE_IDS ↦ NO_EXPENSE],
51      groups ↦ [gid ∈ POSSIBLE_GROUP_IDS ↦ NO_GROUP]
52      ]
53  ]
54  ∧ actionCounter = 0

56  _____
57  Helper Functions
58  _____

60  Get expenseIds that are added to a specific group
61  GroupExpenseIds(gid, recordedExpensesIn) ≜
62  {eid ∈ POSSIBLE_EXPENSE_IDS :
63    ∧ recordedExpensesIn[eid] ≠ NO_EXPENSE
64    ∧ recordedExpensesIn[eid].deleted = FALSE
65    ∧ recordedExpensesIn[eid].group = gid
66    ∧ ∀ u ∈ DOMAIN recordedExpensesIn[eid].shares :
67      (recordedExpensesIn[eid].shares[u] > 0)
68      ⇒ recordedExpensesIn[eid].acknowledged_shares[u] = TRUE}

70  IsMember(memberCounter) ≜
71  memberCounter%2 = 1

73  WasEverMember(memberCounter) ≜
74  memberCounter > 0

76  RECURSIVE SumFunction(−)
77  SumFunction(F) ≜
78    IF DOMAIN F = {} THEN 0
79    ELSE LET d ≜ CHOOSE x ∈ DOMAIN F : TRUE
80    IN F[d] + SumFunction([y ∈ DOMAIN F \ {d} ↦ F[y]])

83  Balance(u, gid, replica) ≜
84    LET groupExpenses ≜ GroupExpenseIds(gid, replica.recordedExpenses)
85    IN SumFunction([eid ∈ groupExpenses ↦
86      IF replica.recordedExpenses[eid].payer = u
87      THEN replica.recordedExpenses[eid].amount ELSE 0])
88    − SumFunction([eid ∈ groupExpenses ↦ replica.recordedExpenses[eid].shares[u]])
89    − replica.groups[gid].individualGiftsSent[u]

92  ComputeBalances(grp, recordedExpensesIn) ≜
93  [u ∈ USERS ↦
94    LET groupExpenses ≜ GroupExpenseIds(grp.id, recordedExpensesIn)
95    IN SumFunction([eid ∈ groupExpenses ↦

```

```

96         IF recordedExpensesIn[eid].payer = u
97         THEN recordedExpensesIn[eid].amount ELSE 0))
98     - SumFunction([eid ∈ groupExpenses ↦ recordedExpensesIn[eid].shares[u]])
99 ]

```

```

102 ComputeGifts(grp, balances) ≜
103     LET giftingUsers ≜
104         {u ∈ USERS : ¬IsMember(grp.members[u]) ∧ balances[u] > 0}
105     newTotalGifted ≜ SumFunction([u ∈ giftingUsers ↦ balances[u]])
106     newIndividualGifts ≜ [u ∈ USERS ↦ IF u ∈ giftingUsers THEN balances[u] ELSE 0]
107     IN [grp EXCEPT !.totalGifted = newTotalGifted,
108         !.individualGiftsSent = newIndividualGifts]

```

```

111 RecalcGifts(groupsIn, recordedExpensesIn) ≜
112     [gid ∈ POSSIBLE_GROUP_IDS ↦
113         IF groupsIn[gid] = NO_GROUP THEN NO_GROUP
114         ELSE LET grp ≜ groupsIn[gid]
115             balances ≜ ComputeBalances(grp, recordedExpensesIn)
116             IN ComputeGifts(grp, balances)
117 ]

```

```

120
121 Group actions
122

```

```

124 CreateGroup ≜
125     ∃ actor ∈ USERS :
126     ∃ gid ∈ POSSIBLE_GROUP_IDS :
127     ∃ rid ∈ POSSIBLE_REPLICA_IDS :
128     ∧ ASSIGNED_REPLICA[actor] = rid
129     Ensure each gid is only used once across replicas, real app use pseudorandom functions or similar
130     ∧ ∀ otherRid ∈ POSSIBLE_REPLICA_IDS : replicas[otherRid].groups[gid] = NO_GROUP
131     ∧ LET newGroup ≜
132         [id ↦ gid,
133         members ↦ [u ∈ USERS ↦ IF u = actor THEN 1 ELSE 0],
134         totalGifted ↦ 0,
135         individualGiftsSent ↦ [u ∈ USERS ↦ 0]]
136     newReplica ≜
137     [replicas[rid] EXCEPT !.groups = [⊙ EXCEPT ![gid] = newGroup]]
138     IN ∧ replicas' = [replicas EXCEPT ![rid] = newReplica]
139     ∧ actionCounter' = actionCounter + 1

```

```

141 AddMember ≜
142     ∃ actor, newMember ∈ USERS :

```

```

143    $\exists gid \in POSSIBLE\_GROUP\_IDs :$ 
144    $\exists rid \in POSSIBLE\_REPLICA\_IDs :$ 
145        $\wedge ASSIGNED\_REPLICA[actor] = rid$ 
146        $\wedge replicas[rid].groups[gid] \neq NO\_GROUP$ 
147        $\wedge IsMember(replicas[rid].groups[gid].members[actor])$ 
148        $\wedge \neg IsMember(replicas[rid].groups[gid].members[newMember])$ 
149        $\wedge LET newReplica \triangleq$ 
150            $[replicas[rid] \text{ EXCEPT } !.groups =$ 
151                $[@ \text{ EXCEPT } ![gid].members[newMember] = @ + 1]]$ 
152        $IN \quad \wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
153        $\wedge actionCounter' = actionCounter + 1$ 




```

```

155   LeaveGroup  $\triangleq$ 
156        $\exists actor \in USERS :$ 
157        $\exists gid \in POSSIBLE\_GROUP\_IDs :$ 
158        $\exists rid \in POSSIBLE\_REPLICA\_IDs :$ 
159            $\wedge ASSIGNED\_REPLICA[actor] = rid$ 
160            $\wedge replicas[rid].groups[gid] \neq NO\_GROUP$ 
161            $\wedge IsMember(replicas[rid].groups[gid].members[actor])$ 
162            $\wedge Balance(actor, gid, replicas[rid]) \geq 0$ 
163            $\wedge LET updatedGroups \triangleq$ 
164                $[replicas[rid].groups \text{ EXCEPT }$ 
165                    $![gid].members[actor] = @ + 1]$ 
166                $newGroups \triangleq RecalcGifts(updatedGroups, replicas[rid].recordedExpenses)$ 
167                $newReplica \triangleq$ 
168                    $[replicas[rid] \text{ EXCEPT } !.groups = newGroups]$ 
169            $IN \quad \wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
170            $\wedge actionCounter' = actionCounter + 1$ 

```

```

173   
174   Expense actions 
175   

```

```

177   CreateExpense  $\triangleq$ 
178        $\exists actor \in USERS :$ 
179        $\exists shares \in POSSIBLE\_SHARES :$ 
180        $\exists eid \in POSSIBLE\_EXPENSE\_IDs :$ 
181        $\exists rid \in POSSIBLE\_REPLICA\_IDs :$ 
182            $\wedge ASSIGNED\_REPLICA[actor] = rid$ 
183            $\wedge SumFunction(shares) > 0$ 
184            $\wedge \forall otherRid \in POSSIBLE\_REPLICA\_IDs : replicas[otherRid].recordedExpenses[eid] = NO\_EXPENSE$ 
185            $\wedge LET newExpense \triangleq$ 
186                $[id \mapsto eid,$ 
187                    $group \mapsto NO\_GROUP,$ 
188                    $version \mapsto 0,$ 

```

```

189      payer  $\mapsto$  actor,
190      amount  $\mapsto$  SumFunction(shares),
191      shares  $\mapsto$  shares,
192      acknowledged_shares  $\mapsto$   $[u \in USERS \mapsto \text{IF } u = \text{actor} \wedge \text{shares}[u] > 0 \text{ THEN TRUE ELSE FALSE}]$ ,
193      deleted  $\mapsto$  FALSE]
194    newReplica  $\triangleq$ 
195      [replicas[rid] EXCEPT !.recordedExpenses = [ @ EXCEPT ![eid] = newExpense]]
196    IN     $\wedge$  replicas' = [replicas EXCEPT ![rid] = newReplica]
197           $\wedge$  actionCounter' = actionCounter + 1

199  AddExpenseToGroup  $\triangleq$ 
200     $\exists$  actor  $\in$  USERS :
201     $\exists$  eid  $\in$  POSSIBLE_EXPENSE_IDS :
202     $\exists$  gid  $\in$  POSSIBLE_GROUP_IDS :
203     $\exists$  rid  $\in$  POSSIBLE_REPLICA_IDS :
204       $\wedge$  ASSIGNED_REPLICA[actor] = rid
205       $\wedge$  replicas[rid].groups[gid]  $\neq$  NO_GROUP
206       $\wedge$  replicas[rid].recordedExpenses[eid]  $\neq$  NO_EXPENSE
207       $\wedge$  IsMember(replicas[rid].groups[gid].members[actor])
208       $\wedge$  replicas[rid].recordedExpenses[eid].payer = actor
209       $\wedge$  replicas[rid].recordedExpenses[eid].group = NO_GROUP
210       $\wedge$   $\{u \in USERS : \text{replicas[rid].recordedExpenses[eid].shares}[u] > 0\}$ 
211         $\subseteq$   $\{u \in USERS : \text{IsMember(replicas[rid].groups[gid].members}[u])\}$ 
212       $\wedge$  LET newExpense  $\triangleq$ 
213        [replicas[rid].recordedExpenses[eid] EXCEPT !.group = gid, !.version = @ + 1]
214        newExpenses  $\triangleq$ 
215        [replicas[rid].recordedExpenses EXCEPT ![eid] = newExpense]
216        newReplica  $\triangleq$ 
217        [replicas[rid] EXCEPT !.recordedExpenses = newExpenses]
218      IN     $\wedge$  replicas' = [replicas EXCEPT ![rid] = newReplica]
219             $\wedge$  actionCounter' = actionCounter + 1

221  RemoveExpenseFromGroup  $\triangleq$ 
222     $\exists$  actor  $\in$  USERS :
223     $\exists$  eid  $\in$  POSSIBLE_EXPENSE_IDS :
224     $\exists$  gid  $\in$  POSSIBLE_GROUP_IDS :
225     $\exists$  rid  $\in$  POSSIBLE_REPLICA_IDS :
226       $\wedge$  ASSIGNED_REPLICA[actor] = rid
227       $\wedge$  replicas[rid].groups[gid]  $\neq$  NO_GROUP
228       $\wedge$  replicas[rid].recordedExpenses[eid]  $\neq$  NO_EXPENSE
229       $\wedge$  IsMember(replicas[rid].groups[gid].members[actor])
230       $\wedge$  replicas[rid].recordedExpenses[eid].group = gid
231       $\wedge$  replicas[rid].recordedExpenses[eid].payer = actor
232       $\wedge$  LET newExpense  $\triangleq$  [replicas[rid].recordedExpenses[eid] EXCEPT !.group = NO_GROUP,
233        !.version = @ + 1,
```

```

234      !.acknowledged_shares = [u ∈ USERS ↦ IF u = actor ∧ replicas[rid].recorded
235      newExpenses ≜ [replicas[rid].recordedExpenses EXCEPT ![eid] = newExpense]
236      newGroups ≜ RecalcGifts(replicas[rid].groups, newExpenses)
237      newReplica ≜ [replicas[rid] EXCEPT !.recordedExpenses = newExpenses,
238      !.groups = newGroups]
239  IN    ∧ replicas' = [replicas EXCEPT ![rid] = newReplica]
240      ∧ actionCounter' = actionCounter + 1

242  ModifyExpenseParameters ≜
243    ∃ actor ∈ USERS :
244    ∃ shares ∈ POSSIBLE_SHARES :
245    ∃ eid ∈ POSSIBLE_EXPENSE_IDS :
246    ∃ rid ∈ POSSIBLE_REPLICA_IDS :
247      ∧ ASSIGNED_REPLICA[actor] = rid
248      ∧ replicas[rid].recordedExpenses[eid] ≠ NO_EXPENSE
249      ∧ replicas[rid].recordedExpenses[eid].payer = actor
250      ∧ SumFunction(shares) > 0
251      ∧ ¬replicas[rid].recordedExpenses[eid].deleted
252      ∧ IF replicas[rid].recordedExpenses[eid].group ≠ NO_GROUP
253      THEN {u ∈ USERS : shares[u] > 0}
254      ⊆ {u ∈ USERS : IsMember(replicas[rid].groups[replicas[rid].recordedExpenses[eid].group].m
255      ELSE TRUE
256      ∧ LET newExpenses ≜
257        [replicas[rid].recordedExpenses EXCEPT
258        ![eid].shares = shares,
259        ![eid].acknowledged_shares = [u ∈ USERS ↦ IF u = actor ∧ shares[u] > 0 THEN TRUE ELSE
260        ![eid].amount = SumFunction(shares),
261        ![eid].version = @ + 1]
262      newGroups ≜
263      IF replicas[rid].recordedExpenses[eid].group = NO_GROUP
264      THEN replicas[rid].groups
265      ELSE RecalcGifts(replicas[rid].groups, newExpenses)
266      newReplica ≜
267      [replicas[rid] EXCEPT !.recordedExpenses = newExpenses,
268      !.groups = newGroups]
269  IN    ∧ replicas' = [replicas EXCEPT ![rid] = newReplica]
270      ∧ actionCounter' = actionCounter + 1

272  DeleteExpense ≜
273    ∃ actor ∈ USERS :
274    ∃ eid ∈ POSSIBLE_EXPENSE_IDS :
275    ∃ rid ∈ POSSIBLE_REPLICA_IDS :
276      ∧ ASSIGNED_REPLICA[actor] = rid
277      ∧ replicas[rid].recordedExpenses[eid] ≠ NO_EXPENSE
278      ∧ replicas[rid].recordedExpenses[eid].payer = actor

```

```

279       $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{deleted} = \text{FALSE}$ 
280       $\wedge \text{IF } \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group} \neq \text{NO\_GROUP}$ 
281          THEN  $\wedge \text{IsMember}(\text{replicas}[\text{rid}].\text{groups}[\text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group}].\text{members}[\text{actor}])$ 
282          ELSE TRUE
283       $\wedge \text{LET } \text{newExpenses} \triangleq$ 
284           $[\text{replicas}[\text{rid}].\text{recordedExpenses} \text{ EXCEPT } ![\text{eid}].\text{deleted} = \text{TRUE}, ![\text{eid}].\text{version} = @ + 1]$ 
285           $\text{newGroups} \triangleq$ 
286           $\text{RecalcGifts}(\text{replicas}[\text{rid}].\text{groups}, \text{newExpenses})$ 
287           $\text{newReplica} \triangleq$ 
288           $[\text{replicas}[\text{rid}] \text{ EXCEPT } !.\text{recordedExpenses} = \text{newExpenses},$ 
289               $!.groups = \text{newGroups}]$ 
290      IN  $\wedge \text{replicas}' = [\text{replicas} \text{ EXCEPT } ![\text{rid}] = \text{newReplica}]$ 
291           $\wedge \text{actionCounter}' = \text{actionCounter} + 1$ 

293 AcknowledgeShare  $\triangleq$ 
294      $\exists \text{actor} \in \text{USERS} :$ 
295      $\exists \text{eid} \in \text{POSSIBLE\_EXPENSE\_IDS} :$ 
296      $\exists \text{rid} \in \text{POSSIBLE\_REPLICA\_IDS} :$ 
297          $\wedge \text{ASSIGNED\_REPLICA}[\text{actor}] = \text{rid}$ 
298          $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}] \neq \text{NO\_EXPENSE}$ 
299          $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{deleted} = \text{FALSE}$ 
300          $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group} \neq \text{NO\_GROUP}$ 
301          $\wedge \text{IsMember}(\text{replicas}[\text{rid}].\text{groups}[\text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group}].\text{members}[\text{actor}])$ 
302          $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{shares}[\text{actor}] > 0$ 
303          $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{acknowledged\_shares}[\text{actor}] = \text{FALSE}$ 
304      $\wedge \text{LET } \text{newExpenses} \triangleq$ 
305          $[\text{replicas}[\text{rid}].\text{recordedExpenses} \text{ EXCEPT } ![\text{eid}].\text{acknowledged\_shares}[\text{actor}] = \text{TRUE}]$ 
306          $\text{newGroups} \triangleq$ 
307          $\text{RecalcGifts}(\text{replicas}[\text{rid}].\text{groups}, \text{newExpenses})$ 
308          $\text{newReplica} \triangleq$ 
309          $[\text{replicas}[\text{rid}] \text{ EXCEPT } !.\text{recordedExpenses} = \text{newExpenses},$ 
310              $!.groups = \text{newGroups}]$ 
311     IN  $\wedge \text{replicas}' = [\text{replicas} \text{ EXCEPT } ![\text{rid}] = \text{newReplica}]$ 
312          $\wedge \text{actionCounter}' = \text{actionCounter} + 1$ 
313      $\wedge \text{UNCHANGED } \text{actionCounter}$ 

316 Payer absorbs share of a member who left and never acknowledged
317 PayerAbsorbsLeftMemberShare  $\triangleq$ 
318      $\exists \text{actor} \in \text{USERS} :$ 
319      $\exists \text{eid} \in \text{POSSIBLE\_EXPENSE\_IDS} :$ 
320      $\exists \text{leftMember} \in \text{USERS} :$ 
321      $\exists \text{rid} \in \text{POSSIBLE\_REPLICA\_IDS} :$ 
322          $\wedge \text{ASSIGNED\_REPLICA}[\text{actor}] = \text{rid}$ 
323          $\wedge \text{actor} \neq \text{leftMember}$ 
324          $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}] \neq \text{NO\_EXPENSE}$ 

```

```

325  $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{deleted} = \text{FALSE}$ 
326  $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{payer} = \text{actor}$ 
327  $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{shares}[\text{leftMember}] > 0$ 
328  $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{acknowledged\_shares}[\text{leftMember}] = \text{FALSE}$ 
329  $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group} \neq \text{NO\_GROUP}$ 
330  $\wedge \text{LET } \text{gid} \triangleq \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group}$ 
331  $\text{IN } \wedge \text{replicas}[\text{rid}].\text{groups}[\text{gid}] \neq \text{NO\_GROUP}$ 
332  $\wedge \text{IsMember}(\text{replicas}[\text{rid}].\text{groups}[\text{gid}].\text{members}[\text{actor}])$ 
333  $\wedge \neg \text{IsMember}(\text{replicas}[\text{rid}].\text{groups}[\text{gid}].\text{members}[\text{leftMember}])$ 
334  $\wedge \text{WasEverMember}(\text{replicas}[\text{rid}].\text{groups}[\text{gid}].\text{members}[\text{leftMember}])$ 
335  $\wedge \text{LET } \text{oldShares} \triangleq \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{shares}$ 
336  $\text{leftShare} \triangleq \text{oldShares}[\text{leftMember}]$ 
337  $\text{newShares} \triangleq [u \in \text{USERS} \mapsto$ 
338  $\quad \text{IF } u = \text{actor} \text{ THEN } \text{oldShares}[u] + \text{leftShare}$ 
339  $\quad \text{ELSE IF } u = \text{leftMember} \text{ THEN } 0$ 
340  $\quad \text{ELSE } \text{oldShares}[u]]$ 
341  $\text{newExpenses} \triangleq$ 
342  $\quad [\text{replicas}[\text{rid}].\text{recordedExpenses} \text{ EXCEPT}$ 
343  $\quad \quad ![\text{eid}].\text{shares} = \text{newShares},$ 
344  $\quad \quad ![\text{eid}].\text{acknowledged\_shares} = [u \in \text{USERS} \mapsto$ 
345  $\quad \quad \quad \text{IF } u = \text{leftMember} \text{ THEN FALSE}$ 
346  $\quad \quad \quad \text{ELSE } \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{acknowledged\_shares}[u]],$ 
347  $\quad \quad ![\text{eid}].\text{version} = @ + 1]$ 
348  $\text{newGroups} \triangleq \text{RecalcGifts}(\text{replicas}[\text{rid}].\text{groups}, \text{newExpenses})$ 
349  $\text{newReplica} \triangleq$ 
350  $\quad [\text{replicas}[\text{rid}] \text{ EXCEPT } !.\text{recordedExpenses} = \text{newExpenses},$ 
351  $\quad \quad !.\text{groups} = \text{newGroups}]$ 
352  $\text{IN } \wedge \text{replicas}' = [\text{replicas} \text{ EXCEPT } ![\text{rid}] = \text{newReplica}]$ 
353  $\wedge \text{UNCHANGED } \text{actionCounter}$ 

355 Alternative conflict resolution: member rejoins to acknowledge
356 Follows the add member protocol by having a group member reentering the rejoining one
357  $\text{RejoinToAcknowledge} \triangleq$ 
358  $\quad \exists \text{inviter}, \text{rejoiner} \in \text{USERS} :$ 
359  $\quad \exists \text{gid} \in \text{POSSIBLE\_GROUP\_IDS} :$ 
360  $\quad \exists \text{rid} \in \text{POSSIBLE\_REPLICA\_IDS} :$ 
361  $\quad \wedge \text{ASSIGNED\_REPLICA}[\text{inviter}] = \text{rid}$ 
362  $\quad \wedge \text{replicas}[\text{rid}].\text{groups}[\text{gid}] \neq \text{NO\_GROUP}$ 
363  $\quad \wedge \text{IsMember}(\text{replicas}[\text{rid}].\text{groups}[\text{gid}].\text{members}[\text{inviter}])$ 
364  $\quad \wedge \neg \text{IsMember}(\text{replicas}[\text{rid}].\text{groups}[\text{gid}].\text{members}[\text{rejoiner}])$ 
365  $\quad \wedge \text{WasEverMember}(\text{replicas}[\text{rid}].\text{groups}[\text{gid}].\text{members}[\text{rejoiner}])$ 
366  $\quad \wedge \exists \text{eid} \in \text{POSSIBLE\_EXPENSE\_IDS} :$ 
367  $\quad \wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}] \neq \text{NO\_EXPENSE}$ 
368  $\quad \wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{group} = \text{gid}$ 
369  $\quad \wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{shares}[\text{rejoiner}] > 0$ 

```



```

370       $\wedge \text{replicas}[\text{rid}].\text{recordedExpenses}[\text{eid}].\text{acknowledged\_shares}[\text{rejoiner}] = \text{FALSE}$ 
371       $\wedge \text{LET } \text{newReplica} \triangleq$ 
372           $[\text{replicas}[\text{rid}] \text{ EXCEPT } !.\text{groups} =$ 
373               $[\text{@} \text{ EXCEPT } ![\text{gid}].\text{members}[\text{rejoiner}] = \text{@} + 1]]$ 
374      IN       $\wedge \text{replicas}' = [\text{replicas} \text{ EXCEPT } ![\text{rid}] = \text{newReplica}]$ 
375       $\wedge \text{UNCHANGED } \text{actionCounter}$ 

```

```

378
379 Merge action helpers
380

```

```

382 MergeExpense(expOwn, expOther)  $\triangleq$ 
383     IF expOwn = NO_EXPENSE  $\wedge$  expOther = NO_EXPENSE
384     THEN NO_EXPENSE
385     ELSE IF expOwn  $\neq$  NO_EXPENSE  $\wedge$  expOther = NO_EXPENSE
386     THEN expOwn
387     ELSE IF expOwn = NO_EXPENSE  $\wedge$  expOther  $\neq$  NO_EXPENSE
388     THEN expOther
389     ELSE IF expOwn.version > expOther.version
390     THEN expOwn
391     ELSE IF expOwn.version < expOther.version
392     THEN expOther
393     ELSE
394         LET mergedAcknowledgedShares  $\triangleq$ 
395              $[u \in \text{USERS} \mapsto$ 
396                  $\text{expOwn.acknowledged\_shares}[u] \vee \text{expOther.acknowledged\_shares}[u]]$ 
397         IN       $[\text{expOwn} \text{ EXCEPT } !.\text{acknowledged\_shares} = \text{mergedAcknowledgedShares}]$ 
398         LET mergedDeleted  $\triangleq$   $\text{expOwn.deleted} \vee \text{expOther.deleted}$ 
399         useOwnVersion  $\triangleq$   $\text{expOwn.version} \geq \text{expOther.version}$ 
400         baseExp  $\triangleq$  IF useOwnVersion THEN expOwn ELSE expOther
401         mergedGroup  $\triangleq$  baseExp.group
402         IF expOwn.group  $\neq$  NO_GROUP THEN expOwn.group ELSE expOther.group
403     IN       $[ \text{baseExp} \text{ EXCEPT } !.$ 
404          $\text{deleted} = \text{mergedDeleted},$ 
405          $!.group = \text{mergedGroup},$ 
406          $!.version = \text{IF useOwnVersion THEN expOwn.version ELSE expOther.version} ]$ 

```

```

409 MergeGroup(grpOwn, grpOther, mergedExpenses, gid)  $\triangleq$ 
410     IF grpOwn = NO_GROUP  $\wedge$  grpOther = NO_GROUP
411     THEN NO_GROUP
412     ELSE IF grpOwn  $\neq$  NO_GROUP  $\wedge$  grpOther = NO_GROUP
413     THEN grpOwn
414     ELSE IF grpOwn = NO_GROUP  $\wedge$  grpOther  $\neq$  NO_GROUP
415     THEN grpOther

```

```

416     ELSE
417         LET  $mergedMembers \triangleq$ 
418              $[u \in USERS \mapsto \text{CHOOSE } n \in \{grpOwn.members[u], grpOther.members[u]\} :$ 
419                  $n \geq grpOwn.members[u] \wedge n \geq grpOther.members[u]]$ 
420              $mergedGroup \triangleq [grpOwn \text{ EXCEPT } !.members = mergedMembers]$ 
421              $balances \triangleq \text{ComputeBalances}(mergedGroup, mergedExpenses)$ 
422         IN  $\text{ComputeGifts}(mergedGroup, balances)$ 

424
425 Merge action
426

428  $MergeReplicas \triangleq$ 
429      $\exists ownRid, otherRid \in POSSIBLE\_REPLICA\_IDs :$ 
430      $\wedge ownRid \neq otherRid$ 
431      $\wedge$  LET
432          $mergedExpenses \triangleq$ 
433          $[eid \in POSSIBLE\_EXPENSE\_IDs \mapsto$ 
434              $\text{MergeExpense}(replicas[ownRid].recordedExpenses[eid],$ 
435                  $replicas[otherRid].recordedExpenses[eid])]$ 

437          $mergedGroups \triangleq$ 
438          $[gid \in POSSIBLE\_GROUP\_IDs \mapsto$ 
439              $\text{MergeGroup}(replicas[ownRid].groups[gid],$ 
440                  $replicas[otherRid].groups[gid],$ 
441                  $mergedExpenses,$ 
442                  $gid)]$ 

444          $newReplica \triangleq$ 
445          $[replicas[ownRid] \text{ EXCEPT}$ 
446              $!.groups = mergedGroups,$ 
447              $!.recordedExpenses = mergedExpenses]$ 
448     IN  $replicas' = [replicas \text{ EXCEPT } ![ownRid] = newReplica]$ 
449      $\wedge \text{UNCHANGED } actionCounter$ 

452
453 Next relation
454

455  $Next \triangleq$ 
456      $\vee \text{CreateGroup}$ 
457      $\vee \text{AddMember}$ 
458      $\vee \text{LeaveGroup}$ 
459      $\vee \text{CreateExpense}$ 
460      $\vee \text{AddExpenseToGroup}$ 
461      $\vee \text{RemoveExpenseFromGroup}$ 
462      $\vee \text{ModifyExpenseParameters}$ 

```

```

463     $\vee DeleteExpense$ 
464     $\vee AcknowledgeShare$ 
465     $\vee PayerAbsorbsLeftMemberShare$ 
466     $\vee RejoinToAcknowledge$ 
467     $\vee MergeReplicas$ 
468     $\vee UNCHANGED \langle replicas, actionCounter \rangle$ 

```

```

473
474 Invariants
475
476  $TypeOK \triangleq$ 
477    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
478      $\wedge replicas[rid].recordedExpenses$ 
479        $\in [POSSIBLE\_EXPENSE\_IDs \rightarrow (Expense \cup \{NO\_EXPENSE\})]$ 
480      $\wedge replicas[rid].groups$ 
481        $\in [POSSIBLE\_GROUP\_IDs \rightarrow (Group \cup \{NO\_GROUP\})]$ 
482
483  $Inv\_Conservation\_of\_amount \triangleq$ 
484    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
485      $\forall eid \in POSSIBLE\_EXPENSE\_IDs :$ 
486        $replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE \Rightarrow$ 
487         LET  $e \triangleq replicas[rid].recordedExpenses[eid]$ 
488         IN  $e.amount = SumFunction(e.shares)$ 
489
490  $Inv\_ExpenseGroupExists \triangleq$ 
491    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
492      $\forall eid \in POSSIBLE\_EXPENSE\_IDs :$ 
493        $\wedge replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
494        $\wedge replicas[rid].recordedExpenses[eid].deleted = FALSE$  \ * remove this?
495        $\wedge replicas[rid].recordedExpenses[eid].group \neq NO\_GROUP$ 
496        $\Rightarrow$ 
497        $replicas[rid].groups[replicas[rid].recordedExpenses[eid].group] \neq NO\_GROUP$ 
498
499
500  $Inv\_GroupBalanceZero \triangleq$ 
501    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
502      $\forall gid \in POSSIBLE\_GROUP\_IDs :$ 
503        $replicas[rid].groups[gid] \neq NO\_GROUP \Rightarrow$ 
504       LET  $allUsers \triangleq$ 
505         include every user that was a member of the group at some part, as they always could accumulate negative bal
506          $\{u \in USERS : WasEverMember(replicas[rid].groups[gid].members[u])\}$ 
507        $total \triangleq$ 
508        $SumFunction([u \in allUsers \mapsto Balance(u, gid, replicas[rid])])$ 
509       IN  $total + replicas[rid].groups[gid].totalGifted = 0$ 

```

```

512  $Inv \triangleq$ 
513    $\wedge TypeOK$ 
514    $\wedge Inv\_Conservation\_of\_amount$ 
515    $\wedge Inv\_ExpenseGroupExists$ 
516    $\wedge Inv\_GroupBalanceZero$ 

519
520 Liveness Helper
521
522  $AllReplicasHaveAtLeastExpenseVersion(eid, version) \triangleq$ 
523    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
524      $\wedge replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
525      $\wedge replicas[rid].recordedExpenses[eid].version \geq version$ 

527  $AllReplicasHaveAtLeastGroupMemberCounter(gid, user, counter) \triangleq$ 
528    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
529      $\wedge replicas[rid].groups[gid] \neq NO\_GROUP$ 
530      $\wedge replicas[rid].groups[gid].members[user] \geq counter$ 

532  $AllPositiveSharesAcknowledged(eid, replica) \triangleq$ 
533    $replica.recordedExpenses[eid] = NO\_EXPENSE$ 
534    $\vee$ 
535    $\forall u \in USERS :$ 
536      $replica.recordedExpenses[eid].shares[u] > 0$ 
537      $\Rightarrow replica.recordedExpenses[eid].acknowledged\_shares[u] = TRUE$ 

539
540 Liveness
541

543 Expense version captures modifications and group membership
544  $Liveness\_ExpensePropagates \triangleq$ 
545    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
546      $\forall eid \in POSSIBLE\_EXPENSE\_IDs :$ 
547        $\Box \Diamond (replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
548          $\Rightarrow AllReplicasHaveAtLeastExpenseVersion(eid, replicas[rid].recordedExpenses[eid].version))$ 
549        $\wedge replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
550        $\Rightarrow \Box \Diamond (AllReplicasHaveAtLeastExpenseVersion(eid, replicas[rid].recordedExpenses[eid].version))$ 

552  $Liveness\_GroupMemberShipPropagates \triangleq$ 
553    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
554      $\forall gid \in POSSIBLE\_GROUP\_IDs :$ 
555      $\forall user \in USERS :$ 
556        $\Box \Diamond (replicas[rid].groups[gid] \neq NO\_GROUP$ 
557          $\Rightarrow AllReplicasHaveAtLeastGroupMemberCounter(gid, user, replicas[rid].groups[gid].memb$ 

```

559 Expenses in groups eventually resolve acknowledgment status
 560 Either all shares are acknowledged or the expense is deleted/removed, or all members leave
 561 $Liveness_ExpenseSharesEventuallyAcknowledged \triangleq$
 562 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 563 $\forall eid \in POSSIBLE_EXPENSE_IDs :$
 564 $\square \diamond ($
 565 $\quad LET \ exp \triangleq \ replicas[rid].recordedExpenses[eid]$
 566 $\quad IN \quad \wedge \ exp \neq NO_EXPENSE$
 567 $\quad \wedge \ exp.group \neq NO_GROUP$
 568 $\quad \wedge \neg exp.deleted$
 569 $\quad \Rightarrow (\vee AllPositiveSharesAcknowledged(eid, replicas[rid])$
 570 $\quad \vee exp.deleted$
 571 $\quad \vee exp.group = NO_GROUP$
 572 $\quad \vee \forall u \in USERS : \neg IsMember(replicas[rid].groups[exp.group].members[u]))$

Safety Helper

578 $NoDecreaseExpenseVersion \triangleq$
 579 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 580 $\forall eid \in POSSIBLE_EXPENSE_IDs :$
 581 $(replicas[rid].recordedExpenses[eid] \neq NO_EXPENSE)$
 582 \Rightarrow
 583 $\wedge replicas'[rid].recordedExpenses[eid] \neq NO_EXPENSE$
 584 $\wedge replicas'[rid].recordedExpenses[eid].version$
 585 $\geq replicas[rid].recordedExpenses[eid].version$

 587 $NoDecreaseGroupMembersCounter \triangleq$
 588 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 589 $\forall gid \in POSSIBLE_GROUP_IDs :$
 590 $\forall u \in USERS :$
 591 $(replicas[rid].groups[gid] \neq NO_GROUP)$
 592 \Rightarrow
 593 $\wedge replicas'[rid].groups[gid] \neq NO_GROUP$
 594 $\wedge replicas'[rid].groups[gid].members[u]$
 595 $\geq replicas[rid].groups[gid].members[u]$

 597 $NoDecreaseAcknowledgedSharesSameVersion \triangleq$
 598 $\forall rid \in POSSIBLE_REPLICA_IDs :$
 599 $\forall eid \in POSSIBLE_EXPENSE_IDs :$
 600 $\forall u \in USERS :$
 601 $\wedge replicas[rid].recordedExpenses[eid] \neq NO_EXPENSE$
 602 $\wedge replicas'[rid].recordedExpenses[eid] \neq NO_EXPENSE$ this always exists by *NoDecreaseExpenseVersion* property
 603 $\wedge replicas[rid].recordedExpenses[eid].version = replicas'[rid].recordedExpenses[eid].version$
 604 $\wedge replicas[rid].recordedExpenses[eid].acknowledged_shares[u] = TRUE$
 605 \Rightarrow
 606 $replicas'[rid].recordedExpenses[eid].acknowledged_shares[u] = TRUE$

```

Safety
611 Safety_ExpenseVersionsNonDecreasing  $\triangleq$ 
612  $\Box[NoDecreaseExpenseVersion]_{\{\langle replicas, actionCounter \rangle\}}$ 

614 Safety_GroupMembersCounterNonDecreasing  $\triangleq$ 
615  $\Box[NoDecreaseGroupMembersCounter]_{\{\langle replicas, actionCounter \rangle\}}$ 

617 Safety_AcknowledgedSharesNonDecreasingForSameVersion  $\triangleq$ 
618  $\Box[NoDecreaseAcknowledgedSharesSameVersion]_{\{\langle replicas, actionCounter \rangle\}}$ 


621 
622 Specification
623 
624 Spec  $\triangleq$  Init  $\wedge \Box[Next]_{\langle replicas, actionCounter \rangle}$ 

626 FairSpec  $\triangleq$ 
627  $\wedge Spec$ 
628  $\wedge WF_{\langle replicas, actionCounter \rangle}(MergeReplicas)$ 
629  $\wedge WF_{\langle replicas, actionCounter \rangle}(AcknowledgeShare)$ 
630  $\wedge WF_{\langle replicas, actionCounter \rangle}(PayerAbsorbsLeftMemberShare)$ 
631  $\wedge WF_{\langle replicas, actionCounter \rangle}(RejoinToAcknowledge)$ 

633 |
    \ * LaTeX: \usepackage[landscape, margin = 0.5in]{geometry}
    \ * Modification History
    \ * Last modified Wed Jan 14 10:10:09 CET 2026 by floyd
    \ * Created Fri Oct 24 11:14:17 CEST 2025 by floyd

```