

```

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)  $\triangleq$ 
62 { eid ∈ POSSIBLE_EXPENSE_IDS :
63   ∧ recordedExpensesIn[eid] ≠ NO_EXPENSE
64   ∧ recordedExpensesIn[eid].deleted = FALSE
65   ∧ recordedExpensesIn[eid].group = gid
66   ∧  $\forall u \in \text{DOMAIN}$  recordedExpensesIn[eid].shares :
67     (recordedExpensesIn[eid].shares[u] > 0)
68      $\Rightarrow$  recordedExpensesIn[eid].acknowledged_shares[u] = TRUE}

70 IsMember(memberCounter)  $\triangleq$ 
71 memberCounter%2 = 1

73 WasEverMember(memberCounter)  $\triangleq$ 
74 memberCounter > 0

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

83 Balance(u, gid, replica)  $\triangleq$ 
84   LET groupExpenses  $\triangleq$  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)  $\triangleq$ 
93   [u ∈ USERS ↪
94     LET groupExpenses  $\triangleq$  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       ]
100
101
102   ComputeGifts(grp, balances)  $\triangleq$ 
103     LET giftingUsers  $\triangleq$ 
104       {u ∈ USERS :  $\neg$ IsMember(grp.members[u])  $\wedge$  balances[u] > 0}
105       newTotalGifted  $\triangleq$  SumFunction([u ∈ giftingUsers ↦ balances[u]))
106       newIndividualGifts  $\triangleq$  [u ∈ USERS ↢ IF u ∈ giftingUsers THEN balances[u] ELSE 0]
107     IN [grp EXCEPT !.totalGifted = newTotalGifted,
108           !.individualGiftsSent = newIndividualGifts]
109
110
111   RecalcGifts(groupsIn, recordedExpensesIn)  $\triangleq$ 
112     [gid ∈ POSSIBLE_GROUP_IDS ↢
113       IF groupsIn[gid] = NO_GROUP THEN NO_GROUP
114         ELSE LET grp  $\triangleq$  groupsIn[gid]
115           balances  $\triangleq$  ComputeBalances(grp, recordedExpensesIn)
116           IN ComputeGifts(grp, balances)
117     ]
118
119
120   _____
121   Group actions _____
122
123
124   CreateGroup  $\triangleq$ 
125      $\exists$  actor ∈ USERS :
126      $\exists$  gid ∈ POSSIBLE_GROUP_IDS :
127      $\exists$  rid ∈ POSSIBLE_REPLICA_IDS :
128        $\wedge$  ASSIGNED_REPLICA[actor] = rid
129       Ensure each gid is only used once across replicas, real app use pseudorandom functions or similar
130        $\wedge$   $\forall$  otherRid ∈ POSSIBLE_REPLICA_IDS : replicas[otherRid].groups[gid] = NO_GROUP
131        $\wedge$  LET newGroup  $\triangleq$ 
132         [id ↦ gid,
133          members ↢ [u ∈ USERS ↢ IF u = actor THEN 1 ELSE 0],
134          totalGifted ↢ 0,
135          individualGiftsSent ↢ [u ∈ USERS ↢ 0]]
136         newReplica  $\triangleq$ 
137           [replicas[rid] EXCEPT !.groups = [@(EXCEPT !.[gid] = newGroup)]]
138           IN  $\wedge$  replicas' = [replicas EXCEPT !.[rid] = newReplica]
139              $\wedge$  actionCounter' = actionCounter + 1
140
141   AddMember  $\triangleq$ 
142      $\exists$  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      $\wedge \text{LET } newReplica \triangleq$ 
150        $[replicas[rid]] \text{ EXCEPT } !.\text{groups} =$ 
151        $[@ \text{ EXCEPT } ![gid].\text{members}[newMember] = @ + 1]]$ 
152     IN  $\wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
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      $\wedge \text{LET } updatedGroups \triangleq$ 
164        $[replicas[rid].groups \text{ EXCEPT }$ 
165        $![gid].\text{members}[actor] = @ + 1]$ 
166      $newGroups \triangleq RecalcGifts(updatedGroups, replicas[rid].recordedExpenses)$ 
167      $newReplica \triangleq$ 
168        $[replicas[rid]] \text{ EXCEPT } !.\text{groups} = newGroups]$ 
169     IN  $\wedge replicas' = [replicas \text{ EXCEPT } ![rid] = newReplica]$ 
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      $\wedge \text{LET } newExpense \triangleq$ 
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  $\mapsto$  IF u = actor  $\wedge$  shares[u] > 0 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 : replicas[rid].recordedExpenses[eid].shares[u] > 0}
211    $\subseteq$  {u  $\in$  USERS : 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            $!.acknowledged\_shares = [u \in \text{USERS} \mapsto \text{IF } u = \text{actor} \wedge \text{replicas}[rid].recorded$ 
235            $\text{newExpenses} \triangleq [\text{replicas}[rid].recordedExpenses \text{ EXCEPT } ![\text{eid}] = \text{newExpense}]$ 
236            $\text{newGroups} \triangleq \text{RecalcGifts}(\text{replicas}[rid].groups, \text{newExpenses})$ 
237            $\text{newReplica} \triangleq [\text{replicas}[rid] \text{ EXCEPT } !.\text{recordedExpenses} = \text{newExpenses},$ 
238            $!.\text{groups} = \text{newGroups}]$ 
239           IN  $\wedge \text{replicas}' = [\text{replicas} \text{ EXCEPT } ![\text{rid}] = \text{newReplica}]$ 
240            $\wedge \text{actionCounter}' = \text{actionCounter} + 1$ 

242    $\text{ModifyExpenseParameters} \triangleq$ 
243    $\exists \text{actor} \in \text{USERS} :$ 
244    $\exists \text{shares} \in \text{POSSIBLE\_SHARES} :$ 
245    $\exists \text{eid} \in \text{POSSIBLE\_EXPENSE\_IDS} :$ 
246    $\exists \text{rid} \in \text{POSSIBLE\_REPLICA\_IDS} :$ 
247    $\wedge \text{ASSIGNED\_REPLICA}[\text{actor}] = \text{rid}$ 
248    $\wedge \text{replicas}[rid].recordedExpenses[\text{eid}] \neq \text{NO\_EXPENSE}$ 
249    $\wedge \text{replicas}[rid].recordedExpenses[\text{eid}].payer = \text{actor}$ 
250    $\wedge \text{SumFunction}(\text{shares}) > 0$ 
251    $\wedge \neg \text{replicas}[rid].recordedExpenses[\text{eid}].deleted$ 
252    $\wedge \text{IF } \text{replicas}[rid].recordedExpenses[\text{eid}].group \neq \text{NO\_GROUP}$ 
253    $\text{THEN } \{u \in \text{USERS} : \text{shares}[u] > 0\}$ 
254    $\subseteq \{u \in \text{USERS} : \text{IsMember}(\text{replicas}[rid].groups[\text{replicas}[rid].recordedExpenses[\text{eid}].group].m$ 
255    $\text{ELSE } \text{TRUE}$ 
256    $\wedge \text{LET } \text{newExpenses} \triangleq$ 
257    $[\text{replicas}[rid].recordedExpenses \text{ EXCEPT }$ 
258    $![\text{eid}].shares = \text{shares},$ 
259    $![\text{eid}].acknowledged\_shares = [u \in \text{USERS} \mapsto \text{IF } u = \text{actor} \wedge \text{shares}[u] > 0 \text{ THEN TRUE ELSE }$ 
260    $![\text{eid}].amount = \text{SumFunction}(\text{shares}),$ 
261    $![\text{eid}].version = @ + 1]$ 
262    $\text{newGroups} \triangleq$ 
263    $\text{IF } \text{replicas}[rid].recordedExpenses[\text{eid}].group = \text{NO\_GROUP}$ 
264    $\text{THEN } \text{replicas}[rid].groups$ 
265    $\text{ELSE } \text{RecalcGifts}(\text{replicas}[rid].groups, \text{newExpenses})$ 
266    $\text{newReplica} \triangleq$ 
267    $[\text{replicas}[rid] \text{ EXCEPT } !.\text{recordedExpenses} = \text{newExpenses},$ 
268    $!.\text{groups} = \text{newGroups}]$ 
269   IN  $\wedge \text{replicas}' = [\text{replicas} \text{ EXCEPT } ![\text{rid}] = \text{newReplica}]$ 
270    $\wedge \text{actionCounter}' = \text{actionCounter} + 1$ 

272    $\text{DeleteExpense} \triangleq$ 
273    $\exists \text{actor} \in \text{USERS} :$ 
274    $\exists \text{eid} \in \text{POSSIBLE\_EXPENSE\_IDS} :$ 
275    $\exists \text{rid} \in \text{POSSIBLE\_REPLICA\_IDS} :$ 
276    $\wedge \text{ASSIGNED\_REPLICA}[\text{actor}] = \text{rid}$ 
277    $\wedge \text{replicas}[rid].recordedExpenses[\text{eid}] \neq \text{NO\_EXPENSE}$ 
278    $\wedge \text{replicas}[rid].recordedExpenses[\text{eid}].payer = \text{actor}$ 

```

```

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

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

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

```

```

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

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       $\exists \text{inviter}, \text{rejoiner} \in \text{USERS} :$ 
359       $\exists gid \in \text{POSSIBLE\_GROUP\_IDs} :$ 
360       $\exists rid \in \text{POSSIBLE\_REPLICA\_IDs} :$ 
361       $\wedge \text{ASSIGNED\_REPLICA}[\text{inviter}] = rid$ 
362       $\wedge \text{replicas}[rid].groups[gid] \neq \text{NO\_GROUP}$ 
363       $\wedge \text{IsMember}(\text{replicas}[rid].groups[gid].members[\text{inviter}])$ 
364       $\wedge \neg \text{IsMember}(\text{replicas}[rid].groups[gid].members[\text{rejoiner}])$ 
365       $\wedge \text{WasEverMember}(\text{replicas}[rid].groups[gid].members[\text{rejoiner}])$ 
366       $\wedge \exists eid \in \text{POSSIBLE\_EXPENSE\_IDs} :$ 
367       $\wedge \text{replicas}[rid].recordedExpenses[eid] \neq \text{NO\_EXPENSE}$ 
368       $\wedge \text{replicas}[rid].recordedExpenses[eid].group = gid$ 
369       $\wedge \text{replicas}[rid].recordedExpenses[eid].shares[\text{rejoiner}] > 0$ 

```

```

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      $[@ \text{EXCEPT } ![\text{gid}].\text{members}[\text{rejoiner}] = @ + 1]$ 
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   _____
381

382  $\text{MergeExpense}(\text{expOwn}, \text{expOther}) \triangleq$ 
383   IF  $\text{expOwn} = \text{NO\_EXPENSE} \wedge \text{expOther} = \text{NO\_EXPENSE}$ 
384     THEN  $\text{NO\_EXPENSE}$ 
385   ELSE IF  $\text{expOwn} \neq \text{NO\_EXPENSE} \wedge \text{expOther} = \text{NO\_EXPENSE}$ 
386     THEN  $\text{expOwn}$ 
387   ELSE IF  $\text{expOwn} = \text{NO\_EXPENSE} \wedge \text{expOther} \neq \text{NO\_EXPENSE}$ 
388     THEN  $\text{expOther}$ 
389   ELSE IF  $\text{expOwn.version} > \text{expOther.version}$ 
390     THEN  $\text{expOwn}$ 
391   ELSE IF  $\text{expOwn.version} < \text{expOther.version}$ 
392     THEN  $\text{expOther}$ 
393   ELSE
394     LET  $\text{mergedAcknowledgedShares} \triangleq$ 
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  $\text{mergedDeleted} \triangleq \text{expOwn.deleted} \vee \text{expOther.deleted}$ 
399      $\text{useOwnVersion} \triangleq \text{expOwn.version} \geq \text{expOther.version}$ 
400      $\text{baseExp} \triangleq \text{IF } \text{useOwnVersion} \text{ THEN } \text{expOwn} \text{ ELSE } \text{expOther}$ 
401      $\text{mergedGroup} \triangleq \text{baseExp.group}$ 
402      $\text{IF } \text{expOwn.group} \neq \text{NO\_GROUP} \text{ THEN } \text{expOwn.group} \text{ ELSE } \text{expOther.group}$ 
403   IN  $[\text{baseExp} \text{ EXCEPT }$ 
404      $!.\text{deleted} = \text{mergedDeleted},$ 
405      $!.\text{group} = \text{mergedGroup},$ 
406      $!.\text{version} = \text{IF } \text{useOwnVersion} \text{ THEN } \text{expOwn.version} \text{ ELSE } \text{expOther.version}]$ 

407

408  $\text{MergeGroup}(\text{grpOwn}, \text{grpOther}, \text{mergedExpenses}, \text{gid}) \triangleq$ 
409   IF  $\text{grpOwn} = \text{NO\_GROUP} \wedge \text{grpOther} = \text{NO\_GROUP}$ 
410     THEN  $\text{NO\_GROUP}$ 
411   ELSE IF  $\text{grpOwn} \neq \text{NO\_GROUP} \wedge \text{grpOther} = \text{NO\_GROUP}$ 
412     THEN  $\text{grpOwn}$ 
413   ELSE IF  $\text{grpOwn} = \text{NO\_GROUP} \wedge \text{grpOther} \neq \text{NO\_GROUP}$ 
414     THEN  $\text{grpOther}$ 
415

```

```

416      ELSE
417          LET mergedMembers  $\triangleq$ 
418               $[u \in \text{USERS} \mapsto \text{CHOOSE } n \in \{\text{grpOwn.members}[u], \text{grpOther.members}[u]\} : n \geq \text{grpOwn.members}[u] \wedge n \geq \text{grpOther.members}[u]]$ 
419          mergedGroup  $\triangleq$   $[\text{grpOwn EXCEPT } !.\text{members} = \text{mergedMembers}]$ 
420          balances  $\triangleq$  ComputeBalances(mergedGroup, mergedExpenses)
421          IN ComputeGifts(mergedGroup, balances)
422
423      ━━━━━━
424      Merge action ━━━━━━
425
426
427      MergeReplicas  $\triangleq$ 
428           $\exists \text{ownRid}, \text{otherRid} \in \text{POSSIBLE\_REPLICA\_IDs} :$ 
429           $\wedge \text{ownRid} \neq \text{otherRid}$ 
430           $\wedge \text{LET}$ 
431              mergedExpenses  $\triangleq$ 
432                   $[eid \in \text{POSSIBLE\_EXPENSE\_IDs} \mapsto$ 
433                      MergeExpense(replicas[\text{ownRid}].recordedExpenses[eid],
434                          replicas[\text{otherRid}].recordedExpenses[eid])]
435
436              mergedGroups  $\triangleq$ 
437                   $[gid \in \text{POSSIBLE\_GROUP\_IDs} \mapsto$ 
438                      MergeGroup(replicas[\text{ownRid}].groups[gid],
439                          replicas[\text{otherRid}].groups[gid],
440                          mergedExpenses,
441                          gid)]
442
443              newReplica  $\triangleq$ 
444                   $[\text{replicas}[\text{ownRid}] \text{ EXCEPT}$ 
445                       $!.\text{groups} = \text{mergedGroups},$ 
446                       $!.\text{recordedExpenses} = \text{mergedExpenses}]$ 
447          IN replicas' = [replicas EXCEPT  $![\text{ownRid}] = \text{newReplica}$ ]
448           $\wedge \text{UNCHANGED } \text{actionCounter}$ 
449
450
451      ━━━━━━
452      Next relation ━━━━━━
453
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    $\vee \text{UNCHANGED } \langle \text{replicas}, \text{actionCounter} \rangle$ 

```

473                    

---

474     Invariants        

---

475

```

476  $TypeOK \triangleq$ 
477    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
478      $\wedge \text{replicas}[rid].recordedExpenses$ 
479        $\in [POSSIBLE\_EXPENSE\_IDs \rightarrow (\text{Expense} \cup \{NO\_EXPENSE\})]$ 
480      $\wedge \text{replicas}[rid].groups$ 
481        $\in [POSSIBLE\_GROUP\_IDs \rightarrow (\text{Group} \cup \{NO\_GROUP\})]$ 

```

```

483  $Inv\_Conservation\_of\_amount \triangleq$ 
484    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
485      $\forall eid \in POSSIBLE\_EXPENSE\_IDs :$ 
486        $\text{replicas}[rid].recordedExpenses[eid] \neq NO\_EXPENSE \Rightarrow$ 
487          $\text{LET } e \triangleq \text{replicas}[rid].recordedExpenses[eid]$ 
488          $\text{IN } e.amount = \text{SumFunction}(e.shares)$ 

```

```

490  $Inv\_ExpenseGroupExists \triangleq$ 
491    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
492      $\forall eid \in POSSIBLE\_EXPENSE\_IDs :$ 
493        $\wedge \text{replicas}[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
494          $\wedge \text{replicas}[rid].recordedExpenses[eid].deleted = \text{FALSE} \quad \text{\texttt{* remove this?}}$ 
495        $\wedge \text{replicas}[rid].recordedExpenses[eid].group \neq NO\_GROUP$ 
496      $\Rightarrow$ 
497        $\text{replicas}[rid].groups[\text{replicas}[rid].recordedExpenses[eid].group] \neq NO\_GROUP$ 

```

```

500  $Inv\_GroupBalanceZero \triangleq$ 
501    $\forall rid \in POSSIBLE\_REPLICA\_IDs :$ 
502      $\forall gid \in POSSIBLE\_GROUP\_IDs :$ 
503        $\text{replicas}[rid].groups[gid] \neq NO\_GROUP \Rightarrow$ 
504          $\text{LET } allUsers \triangleq$ 
505            $\text{include every user that was a member of the group at some part, as they always could accumulate negative bal}$ 
506            $\{u \in \text{USERS} : \text{WasEverMember}(\text{replicas}[rid].groups[gid].members[u])\}$ 
507          $total \triangleq$ 
508            $\text{SumFunction}([u \in allUsers \mapsto \text{Balance}(u, gid, \text{replicas}[rid])])$ 
509          $\text{IN } total + \text{replicas}[rid].groups[gid].totalGifted = 0$ 

```

```

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

519  $\overline{\quad}$ 
520 Liveness Helper  $\overline{\quad}$ 
521  $\overline{\quad}$ 
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  $\overline{\quad}$ 
540 Liveness  $\overline{\quad}$ 
541  $\overline{\quad}$ 
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        $\square\Diamond(replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
548          $\Rightarrow AllReplicasHaveAtLeastExpenseVersion(eid, replicas[rid].recordedExpenses[eid].version))$ 
549        $\wedge replicas[rid].recordedExpenses[eid] \neq NO\_EXPENSE$ 
550          $\Rightarrow \square\Diamond(AllReplicasHaveAtLeastExpenseVersion(eid, replicas[rid].recordedExpenses[eid].version))$ 

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

```

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     LET  $exp \triangleq replicas[rid].recordedExpenses[eid]$   
 566     IN  $\wedge exp \neq NO\_EXPENSE$   
 567      $\wedge exp.group \neq NO\_GROUP$   
 568      $\wedge \neg exp.deleted$   
 569      $\Rightarrow (\vee AllPositiveSharesAcknowledged(eid, replicas[rid])$   
 570          $\vee exp.deleted$   
 571          $\vee exp.group = NO\_GROUP$   
 572          $\vee \forall u \in USERS : \neg IsMember(replicas[rid].groups[exp.group].members[u]))$

#### 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    $\square[NoDecreaseExpenseVersion]_{\{\langle replicas, actionCounter \rangle\}}$ 
614  $Safety\_GroupMembersCounterNonDecreasing \triangleq$ 
615    $\square[NoDecreaseGroupMembersCounter]_{\{\langle replicas, actionCounter \rangle\}}$ 
617  $Safety\_AcknowledgedSharesNonDecreasingForSameVersion \triangleq$ 
618    $\square[NoDecreaseAcknowledgedSharesSameVersion]_{\{\langle replicas, actionCounter \rangle\}}$ 

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