MODULE *GossipGlomers2*

Challenge #2: Unique *ID* Generation

Nodes receive a "generate" message and they must respond with a unique *ID*. This system must totally available, meaning it can continue to operate even in the face of network partitions.

Let's first proceed naively and imagine there's only one node running the service. The client and service node will communicate over an asynchronous channel, whose specification is based on the one found in chapter 3 of *Lamport*'s "Specifying Systems".

EXTENDS *Naturals*

CONSTANT *IDS_TO_GENERATE*

CONSTANT *MAX_VAL*

VARIABLE *rdy*, *val*, *seen*, *is_unique*, *num_ids_generated*

$vars \triangleq \langle rdy, val, seen, is\_unique, num\_ids\_generated \rangle$

$$\begin{aligned} TypeInvariant \triangleq\ & \land val \in 1 \,..\, MAX\_VAL \\ & \land rdy \in \{0, 1\} \\ & \land seen \subseteq 1 \,..\, MAX\_VAL \\ & \land is\_unique \in \{\text{TRUE}, \text{FALSE}\} \\ & \land num\_ids\_generated \in 0 \,..\, IDS\_TO\_GENERATE - 1 \end{aligned}$$

$IsUnique \triangleq is\_unique = \text{TRUE}$

$$\begin{aligned} Init \triangleq\ & \land val = 0 \\ & \land rdy = 0 \\ & \land is\_unique = \text{TRUE} \\ & \land seen = \{\} \\ & \land num\_ids\_generated = 0 \end{aligned}$$

$$\begin{aligned} RequestNewID \triangleq\ & \land num\_ids\_generated < IDS\_TO\_GENERATE \\ & \land rdy = 0 \\ & \land rdy' = 1 \\ & \land \text{UNCHANGED } val \\ & \land \text{UNCHANGED } seen \\ & \land \text{UNCHANGED } is\_unique \\ & \land \text{UNCHANGED } num\_ids\_generated \end{aligned}$$

$$\begin{aligned} HandleNewIDRequest \triangleq\ & \land num\_ids\_generated < IDS\_TO\_GENERATE \\ & \land rdy = 1 \\ & \land rdy' = 0 \\ & \land val' \in (1 \,..\, MAX\_VAL \setminus seen) \\ & \land is\_unique' = \neg(val' \in seen) \\ & \land seen' = seen \cup \{val'\} \\ & \land num\_ids\_generated' = num\_ids\_generated + 1 \end{aligned}$$

$$\begin{aligned} Finished \triangleq\ & \land num\_ids\_generated \geq IDS\_TO\_GENERATE \\ & \land \text{UNCHANGED } rdy \end{aligned}$$

```
                 $\land$ UNCHANGED $val$
                 $\land$ UNCHANGED $seen$
                 $\land$ UNCHANGED $is\_unique$
                 $\land$ UNCHANGED $num\_ids\_generated$

$Next \triangleq RequestNewID \lor HandleNewIDRequest \lor Finished$
$Spec \triangleq Init \land \Box[Next]_{vars}$
```

THEOREM $Spec \Rightarrow \Box TypeInvariant$

---

* Modification History
* Last modified Sat *Dec* 30 18:30:44 *EST* 2023 by *sca*
* Created Sat *Dec* 30 10:22:28 *EST* 2023 by *sca*