Model Checking Op-based Counter Using TLA+

Hengfeng Wei

hfwei@nju.edu.cn

June 8, 2018

Our Goal: Model checking RDT using TLA+

(RDT: Replicated Data Types)

Our Goal: Model checking RDT using TLA+

(RDT: Replicated Data Types)

Counter, *Register*, *Set*, *Graph*, *List*, $\cdots$

Our Goal: Model checking RDT using TLA+

(RDT: Replicated Data Types)

Counter, *Register*, *Set*, *Graph*, *List*, $\cdots$

Various protocols + Various specifications

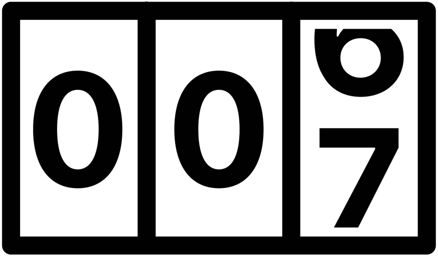
Modularity

Modularity

Communication (FIFO, Causal, $\cdots$)

Composition (`Set` $\implies$ `Graph`)

Specification (Eventual Convergence)


007

$$
\begin{aligned}
\Sigma &= \mathbb{N}_0 \times \mathbb{N}_0 \\
M &= \mathbb{N}_0 \\
\sigma_0 &= \langle 0, 0 \rangle
\end{aligned}
$$

$$
\begin{aligned}
\Sigma &= \mathbb{N}_0 \times \mathbb{N}_0 \\
M &= \mathbb{N}_0 \\
\sigma_0 &= \langle 0, 0 \rangle
\end{aligned}
$$

$\langle a, d \rangle$: $\langle$current value, # of `incs` since the last `send`$\rangle$

$$\begin{aligned} \Sigma &= \mathbb{N}_0 \times \mathbb{N}_0 \\ M &= \mathbb{N}_0 \\ \sigma_0 &= \langle 0, 0 \rangle \end{aligned}$$

$\langle a, d \rangle$: $\langle$current value, # of `incs` since the last `send`$\rangle$

$$\begin{aligned} \texttt{rd}(\langle a, d \rangle) &= \langle a, d \rangle \\ \texttt{inc}(\langle a, d \rangle) &= \langle a+1, d+1 \rangle \\ \texttt{send}(\langle a, d \rangle) &= (\langle a, 0 \rangle, d) \\ \texttt{rcv}(\langle a, d \rangle, d') &= \langle a + d', d \rangle \end{aligned}$$

EC: Eventual Consistency/Convergence

"if clients stop issuing INCs*,*
then the counters at all replicas will be eventually the same."

EC: Eventual Consistency/Convergence

"if clients stop issuing $\textsc{Inc}$*s,*
then the counters at all replicas will be eventually the same."

$$\Diamond(\forall r_i, r_j \in \mathcal{R} : c_i@r_i = c_j@r_j \land \color{red}{c_i@r_i \neq 0})$$

QC: Quiescent Consistency

"if the system is at quiescent,
then the counters at all replicas must be the same."

QC: Quiescent Consistency

"if the system is at quiescent,
then the counters at all replicas must be the same."

$$\Box\Big((\forall r_i \in \mathcal{R} : d@r_i = 0 \land incoming@r = \emptyset) \implies (\forall r_i, r_j \in \mathcal{R} : c_i@r_i = c_j@r_j) \Big)$$

SEC: Strong Eventual Consistency/Convergence

"if two replicas have processed the same set of INCS*,*
then the counters at these two replicas must be the same."

SEC: Strong Eventual Consistency/Convergence

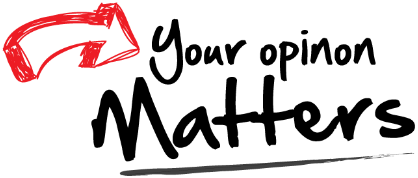
"if two replicas have processed the same set of INCS*,*
then the counters at these two replicas must be the same."

$$\Box\Big(\forall r_i, r_j \in \mathcal{R} : (\{C_i\} @r_i = \{C_j\} @r_j) \implies (c_i@r_i = c_j@r_j)\Big)$$

Cannot: loss, duplication

Can: reordering ($\{\}$ vs. $\langle\langle\rangle\rangle$)


Thank You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn