Pattern-based Abstractions for Parameterized Model Checking of Distributed Algorithms

Thanh Hai Tran, Jure Kukovec

**TLA+**
- Versatile specification language for distributed and concurrent systems
- Based on:
  - Unsorted first-order logic
  - Set theory
  - Temporal logic
- States, transitions: logical formulas
- Supporting tools:
  - TLAPS: the interactive proof system
  - TLC: the explicit-state model checker

**Automated Verification with TLC**
- Explicit-state model checker
- Used at Amazon, Microsoft...
- Bug missing with low probability
- Fixed parameters, finite domains
- Goal: automatically constructs good pattern-based abstractions to verify safety properties of TLA+ specifications

**TLA+ Patterns in Srikanth and Toueg's Asynchronous Reliable Broadcast Algorithm**

- N, T, F: parameters
- pc: program counters
- sent: message channel
- rcvd: received messages
- Proc: all processes
- Corr: correct processes
- Faulty: faulty processes
- Step: transitions (Receive, UponV1…)

**ASSUME**
\[
\land N \in \mathbb{N} \land T \in \mathbb{N} \land F \in \mathbb{N} \\
\land N > 3 \ast T \land T \geq F \land F \geq 0
\]

**Receive**
\[
\text{Receive}(self) \triangleq \\
\land \text{newMsgs}' \in \text{SUBSET} (\text{sent} \cup \text{ByzMsgs}) \\
\land \text{rcvd}' = [i \in \text{Proc} \mapsto \text{IF } i \neq \text{self} \ homosex \text{rcvd}[i] \text{ELSE } \text{rcvd}[\text{self}] \cup \text{newMsgs}']
\]

**Init**
\[
\land \text{sent} = \{\} \\
\land pc \in [\text{Proc} \rightarrow \{"V0", \ "V1"\}] \\
\land \text{rcvd} = [i \in \text{Proc} \mapsto \{\}]
\]

**UponAcceptSentBefore**
\[
\land pc[\text{self}] = "SE" \\
\land \text{Cardinality}(\text{rcvd}'[\text{self}]) \geq N - T \\
\land pc' = [pc \setminus !\text{sent}'] = "AC" \\
\land \text{sent}' = \text{sent} \\
\land \text{UNCHANGED} (\text{Corr}, \text{Faulty})
\]

**TypeOK**
\[
\land pc \in [\text{Proc} \rightarrow \{"V0", \ "V1", \ "SE", \ "AC"\}] \\
\land \text{Corr} \subseteq \text{Proc} \\
\land \text{Faulty} \subseteq \text{Proc} \\
\land \text{sent} \subseteq \text{Proc} \times M \\
\land \text{rcvd} \in [\text{Proc} \rightarrow \text{SUBSET} (\text{sent} \cup \text{ByzMsgs})]
\]

**Our toolchain**

**Challenges**
- TLA+ features: sequences, set cardinality, CHOOSE...
- Type systems
- The classification and extraction of TLA+ patterns
- Pattern-based abstractions
- Quantifier elimination

**References**