The Complexity of Verifying Observation Population Protocols

Chana Weil-Kennedy
joint work with Javier Esparza and Mikhail Raskin
Population protocols

[Angluin, Aspnes, Diamadi, Fischer, Peralta, ’04]

• Distributed computing model where anonymous finite-state mobile agents jointly compute a function.

• Agents communicate through rendez-vous.

• Motivating scenarios: networks of passively mobile sensors, propagation of trust, chemical reactions networks
Population protocols

[Angluin, Aspnes, Diamadi, Fischer, Peralta, ’04]

- Distributed computing model where anonymous finite-state mobile agents jointly compute a function.

- Agents communicate through rendez-vous.

Population protocols

[Angluin, Aspnes, Diamadi, Fischer, Peralta, ’04]

- Distributed computing model where anonymous finite-state mobile agents jointly compute a function.

- Agents communicate through *rendez-vous*.

- Motivating scenarios: networks of passively mobile sensors, propagation of trust, chemical reactions networks
Verifying correctness - results

- Verifying whether a protocol is correct is TOWER-hard for general population protocols. [Esparza, Ganty, Leroux, Majumdar, ’15]

- We investigate the correctness problem for two subclasses: immediate observation and delayed observation population protocols. PSPACE-complete \( \Pi^p_2 \)-complete
Verifying correctness - results

• Verifying whether a protocol is correct is TOWER-hard for general population protocols.  
  \[\text{Esparza, Ganty, Leroux, Majumdar, '15}\]

• We investigate the correctness problem for two subclasses: immediate observation and delayed observation population protocols.

  - PSPACE-complete
  - $\Pi^p_2$-complete
Immediate Observation Population Protocols

[Angluin, Aspnes, Eisenstat, Ruppert, ’07]

- Subclass introduced to model one-way communication.

- An agent *observes* another agent’s state and *immediately* updates its own based on this information.

- Motivating scenarios: sensor networks, enzymatic chemical reactions networks
Immediate Observation Population Protocols

[Angluin, Aspnes, Eisenstat, Ruppert, ’07]

• Subclass introduced to model one-way communication.

• An agent *observes* another agent’s state and *immediately* updates its own based on this information.

• Motivating scenarios: sensor networks, enzymatic chemical reactions networks
Immediate Observation Population Protocols

[Angluin, Aspnes, Eisenstat, Ruppert, ’07]

- Subclass introduced to model one-way communication.

- An agent *observes* another agent’s state and *immediately* updates its own based on this information.

- Motivating scenarios: sensor networks, enzymatic chemical reactions networks
Approach to the PSPACE algorithm

- **Express correctness** as a boolean formula over sets of agent configurations with $pre^*$ and $post^*$

- Find a **good representation** for sets of configurations

- Show that we only need to verify the formula for **small configurations**
Correctness - an example

- Goal of a protocol: compute a function $f : \mathbb{N}^k \rightarrow \{ \text{true, false} \}$
- Configurations are number of agents in each state
- Correctness: for every initial configuration $C_0$, the protocol “computes” $f(C_0)$

Protocol for $(n,0,0)$ such that $n \geq 3$
Correctness - an example

- Goal of a protocol: compute a function $f : \mathbb{N}^k \to \{\text{true}, \text{false}\}$
- Configurations are number of agents in each state
- Correctness: for every initial configuration $C_0$, the protocol “computes” $f(C_0)$

Initial configurations: $C^{(n)}_0 = (n, 0, 0)$

This protocol is correct if and only if for every initial configuration $C^{(n)}_0$:

- $n \geq 3 \Rightarrow$ all configurations reachable from $C^{(n)}_0$ can reach the configuration with all agents in $q_3$.
- $n < 3 \Rightarrow$ there is no reachable configuration with an agent in $q_3$. 

Protocol for $(n,0,0)$ such that $n \geq 3$
A good representation - counting constraints

We consider infinite sets of configurations defined by counting constraints.

- An expression $2 \leq x_2 \leq 5$ is an atomic bound.
A good representation - counting constraints

We consider infinite sets of configurations defined by counting constraints.

- An expression $2 \leq x_2 \leq 5$ is an atomic bound.
- Counting constraints are boolean combinations of atomic bounds.

E.g. in a protocol with two states $q_1$ and $q_2$:

\[
\begin{align*}
2 \leq x_1 \leq \infty \land \\
2 \leq x_2 \leq \infty
\end{align*}
\]
Main Theorem

**Theorem**

For $P$ an IO protocol with $n$ states, for $\Gamma$ a counting constraint describing a set $S$,

1. there exist counting constraints for $pre^*(S)$ and $post^*(S)$
2. the size of these counting constraints is $\leq size(\Gamma) + n^3$
Main Theorem

Theorem

For $P$ an IO protocol with $n$ states, for $\Gamma$ a counting constraint describing a set $S$,

1. there exist counting constraints for $\text{pre}^*(S)$ and $\text{post}^*(S)$
2. the size of these counting constraints is $\leq \text{size}(\Gamma) + n^3$

essentially the largest number of agents in a minimal configuration
Applying the Main Theorem

This protocol is correct if and only if for every initial configuration $C_0^{(n)}$:

- $n \geq 3 \Rightarrow$ all configurations reachable from $C_0^{(n)}$ can reach the configuration with all agents in $q_3$.
- $n < 3 \Rightarrow$ there is no reachable configuration with an agent in $q_3$.

$$post^* \left( \begin{array}{c} 3 \leq q_1 \leq \infty \land \\ 0 \leq q_2 \leq 0 \land \\ 0 \leq q_3 \leq 0 \end{array} \right) \subseteq pre^* \left( \begin{array}{c} 0 \leq q_1 \leq 0 \land \\ 0 \leq q_2 \leq 0 \land \\ 3 \leq q_3 \leq \infty \end{array} \right)$$
Applying the Main Theorem

This protocol is correct if and only if for every initial configuration $C_0^{(n)}$:

- $n \geq 3 \Rightarrow$ all configurations reachable from $C_0^{(n)}$ can reach the configuration with all agents in $q_3$.
- $n < 3 \Rightarrow$ there is no reachable configuration with an agent in $q_3$.

\[
\text{post}^* \left( \begin{array}{l}
3 \leq q_1 \leq \infty \\
0 \leq q_2 \leq 0 \\
0 \leq q_3 \leq 0
\end{array} \right) \cap
\text{pre}^* \left( \begin{array}{l}
0 \leq q_1 \leq 0 \\
0 \leq q_2 \leq 0 \\
3 \leq q_3 \leq \infty
\end{array} \right) = \emptyset
\]

By the Main Theorem, if the intersection is not empty then it contains a “small” configuration.
Conclusion

• We solved the correctness problem for subclasses of population protocols: immediate observation and delayed observation.

  \[ \text{PSPACE-complete} \quad \text{and} \quad \Pi_2^P \text{-complete} \]

• **Future work**: solve the correctness problem for the remaining three subclasses introduced in seminal paper of Angluin et al.

  \[\text{[The Computational Power of Population Protocols, Angluin et al., '07]}\]
Conclusion

• We solved the correctness problem for subclasses of population protocols: immediate observation and delayed observation.

  \[
  \text{PSPACE-complete} \quad \text{and} \quad \Pi_2^p\text{-complete}
  \]

• Future work: solve the correctness problem for the remaining three subclasses introduced in seminal paper of Angluin et al.

  [The Computational Power of Population Protocols, Angluin et al., ’07]

Thank you!