The Complexity of Verifying Observation Population Protocols

Chana Weil-Kennedy

joint work with Javier Esparza and Mikhail Raskin

European Research Council

Established by the European Commission

The project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 787367

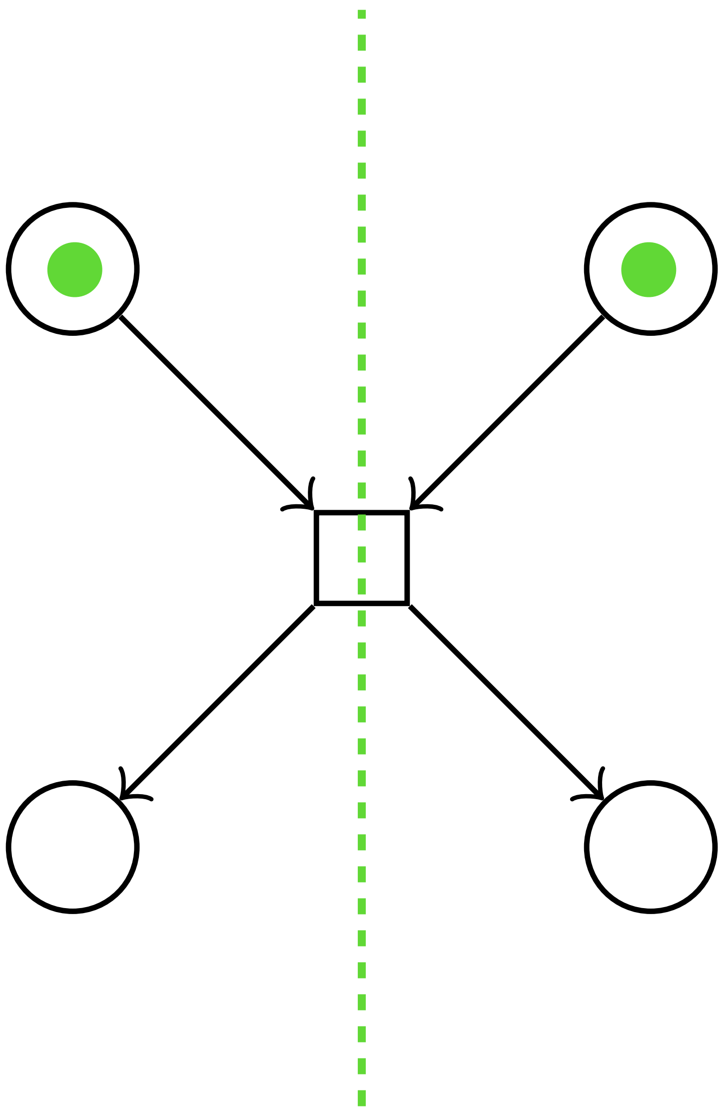
Population protocols

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

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

- Agents communicate through *rendez-vous*.

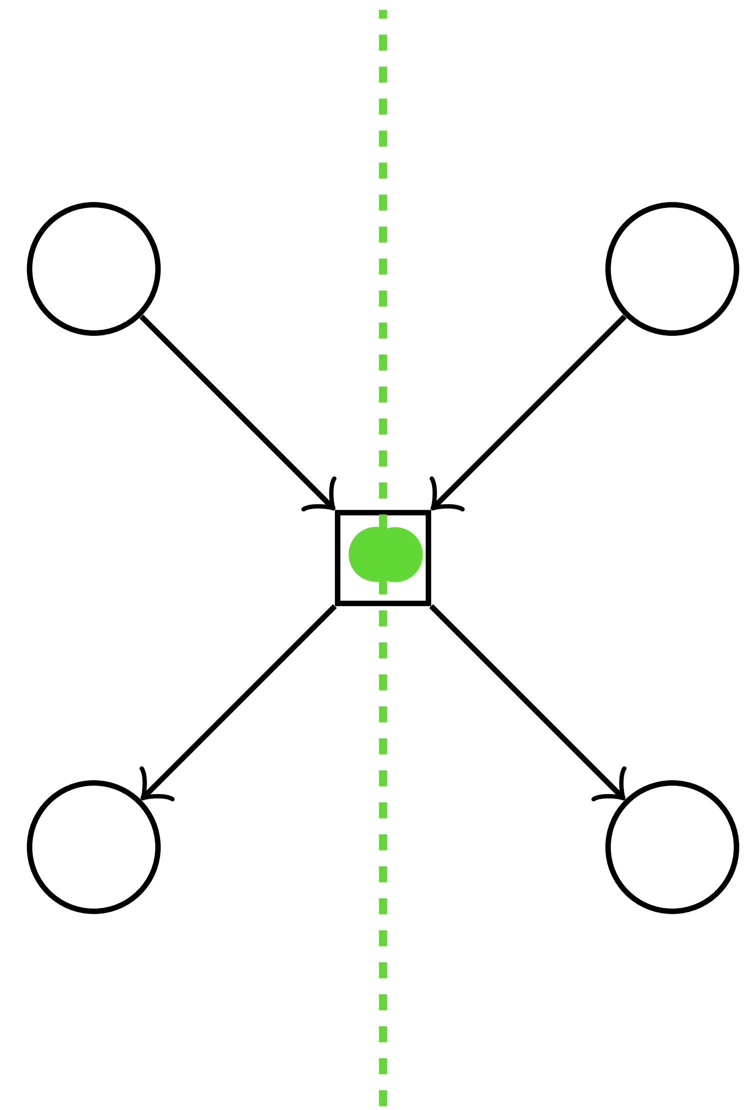
- Motivating scenarios : networks of passively mobile sensors, propagation of trust, chemical reactions networks



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*.

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

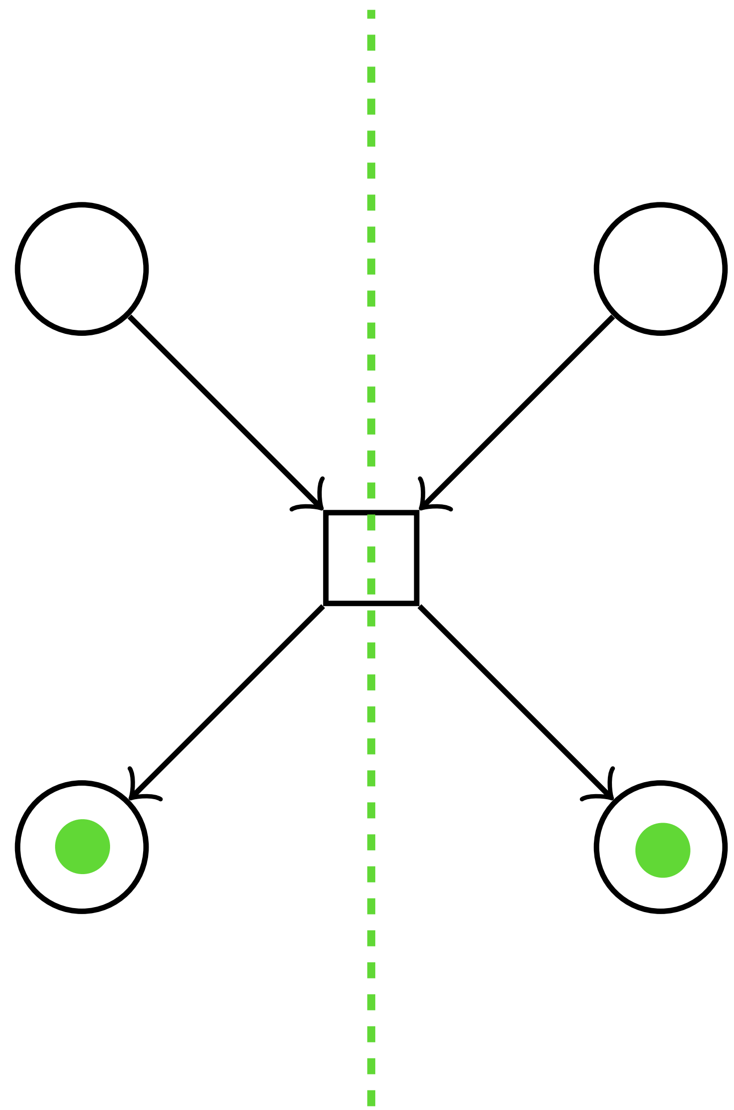
Population protocols

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

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

- Agents communicate through *rendez-vous*.

- 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 $\qquad$ Π_2^p-complete

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

Π_2^p-complete

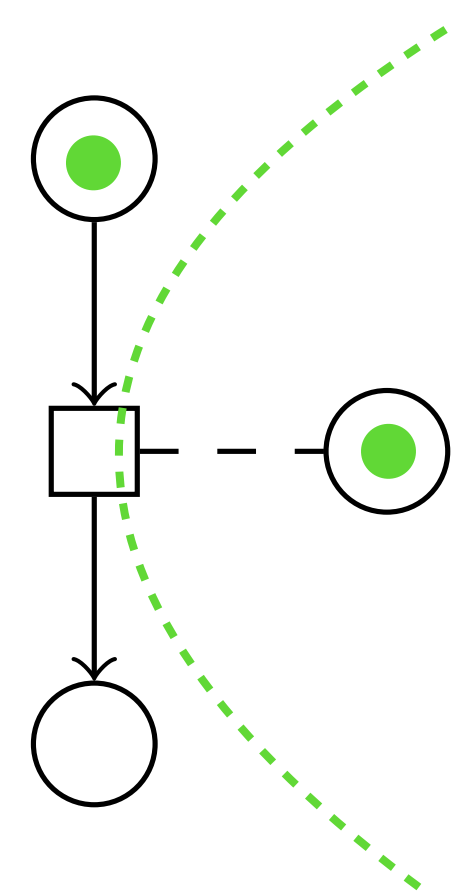
Immediate Observation Population Protocols

[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



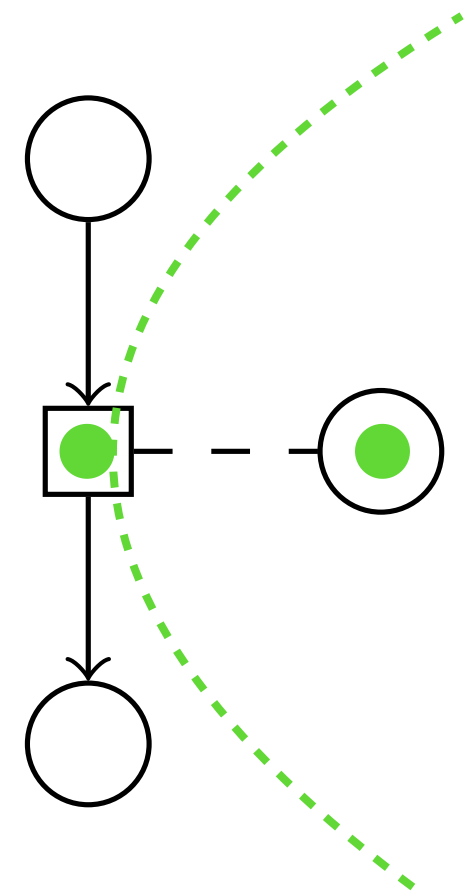
Immediate Observation Population Protocols

[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



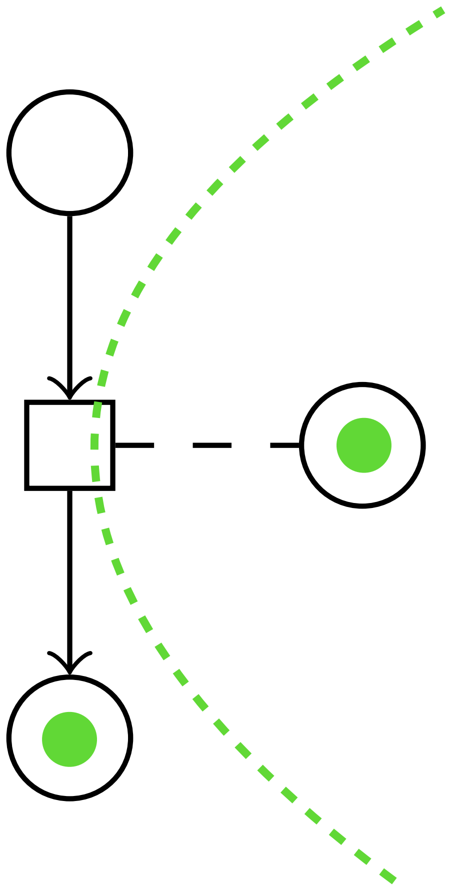
Immediate Observation Population Protocols

[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.

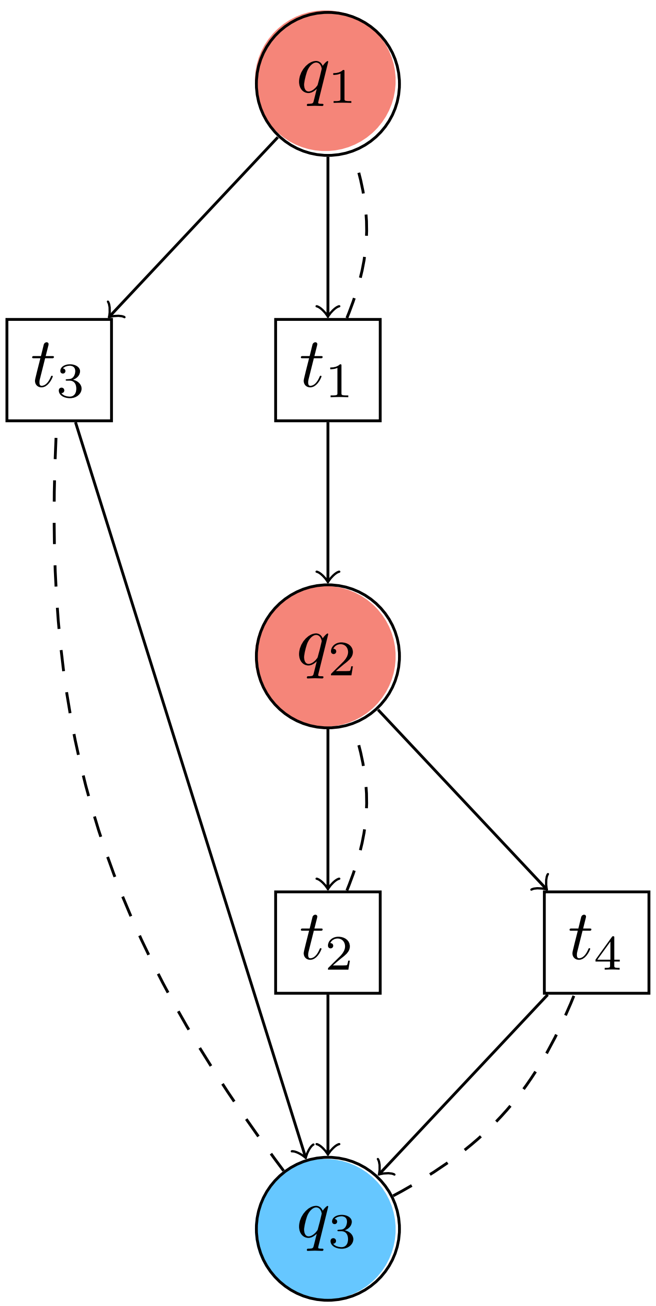
- Motivating scenarios : sensor networks, enzymatic chemical reactions networks



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**

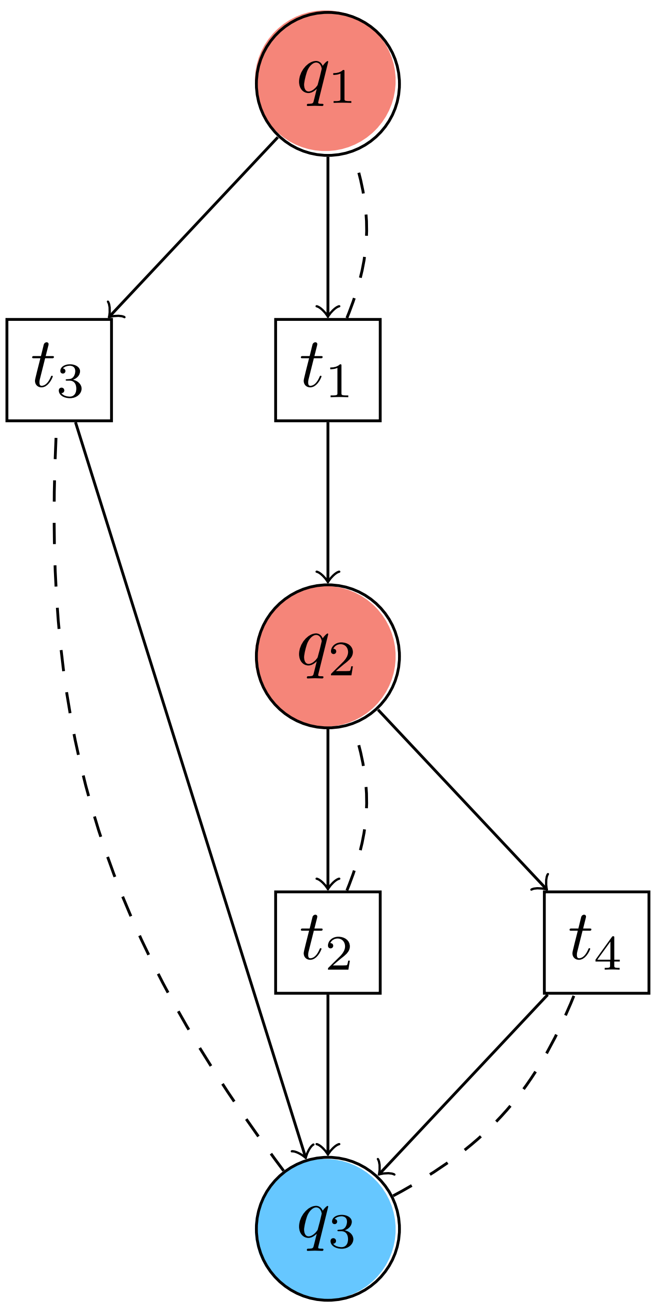
Correctness - an example



Protocol for $(n,0,0)$
such that $n \geq 3$

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

Correctness - an example



Protocol for $(n,0,0)$
such that $n \geq 3$

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

Initial configurations: $C_0^{(n)} = (\ n,\ 0,\ 0\ )$

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.

A good representation - counting constraints

We consider infinite sets of configurations defined by counting constraints.

number of agents in q_2

lower bound

upper bound

- 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.

e.g. in a protocol with two states q_1 and q_2

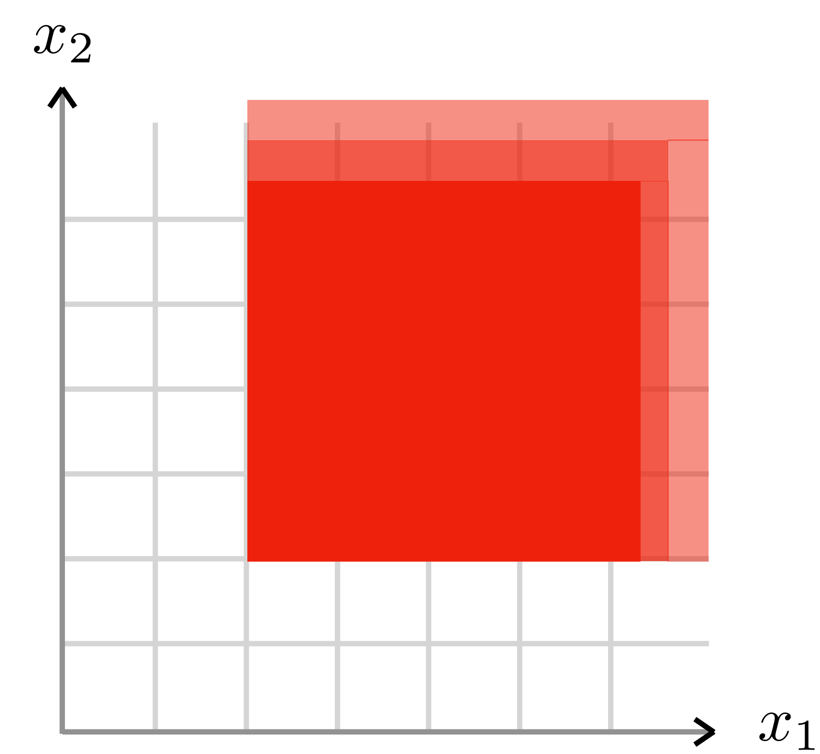
number of agents in q_2

lower bound

upper bound

- An expression $2 \leq x_2 \leq 5$ is an *atomic bound.*

- *Counting constraints* are boolean combinations of atomic bounds.



$$2 \leq x_1 \leq \infty \wedge$$
$$2 \leq x_2 \leq \infty$$

Main Theorem

Theorem

For *P* an IO protocol with *n* states, for Γ 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 Γ a counting constraint describing a set S,

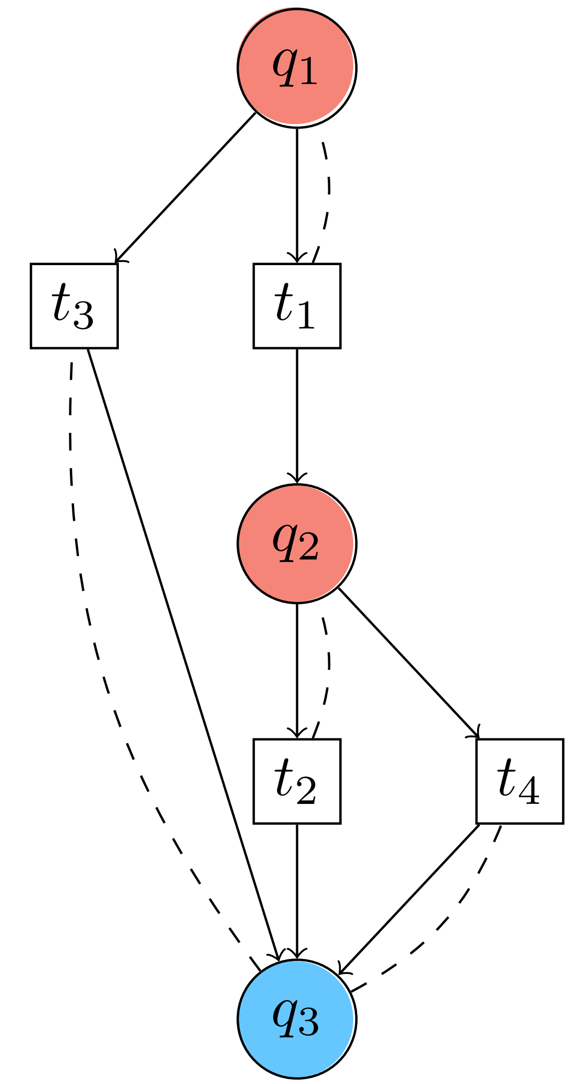
1. there exist counting constraints for *pre*(S)* and *post*(S)*
2. the size of these counting constraints is $\leq size(\Gamma) + n^3$

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.

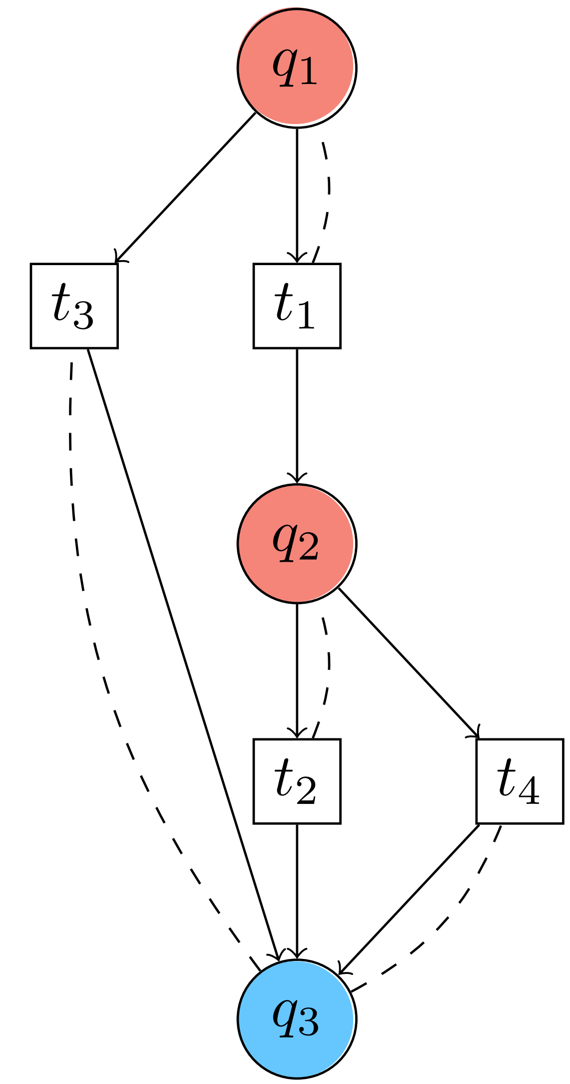


$$post^*\begin{pmatrix} 3 \leq q_1 \leq \infty \wedge \\ 0 \leq q_2 \leq 0 \wedge \\ 0 \leq q_3 \leq 0 \end{pmatrix} \subseteq pre^*\begin{pmatrix} 0 \leq q_1 \leq 0 \wedge \\ 0 \leq q_2 \leq 0 \wedge \\ 3 \leq q_3 \leq \infty \end{pmatrix}$$

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.



$$post^*\begin{pmatrix} 3 \leq q_1 \leq \infty \wedge \\ 0 \leq q_2 \leq 0 \wedge \\ 0 \leq q_3 \leq 0 \end{pmatrix} \quad \cap \quad \overline{pre^*\begin{pmatrix} 0 \leq q_1 \leq 0 \wedge \\ 0 \leq q_2 \leq 0 \wedge \\ 3 \leq q_3 \leq \infty \end{pmatrix}} \quad = \quad \emptyset$$

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**.

PSPACE-complete $\qquad\qquad$ Π_2^p-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]*

Conclusion

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

PSPACE-complete Π_2^p-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 !