FSTTCS'14 | New Delhi, India

Verification of Dynamic Register Automata

Parosh Aziz Abdulla

Mohammed Faouzi Atig

Ahmet Kara

Othmane Rezine

UPPSALA UNIVERSITET

technische universität dortmund

Communication Protocols Analysis

Verification of a class of protocols:

- **Dynamic creation** of processes
  - **Unique** ID for each process
- Finite number of **registers** per process
  - Used to store the ID of others
- **Point-to-point** communication
- **Rendez-vous** communication

Dynamic Register Automata

[Bollig et al. 2010, 2013]

Dynamic Register Automata

Applications

- Leader Election Protocol
- Peer To Peer Protocol
- Ad-Hoc Networks

Dynamic Register Automata

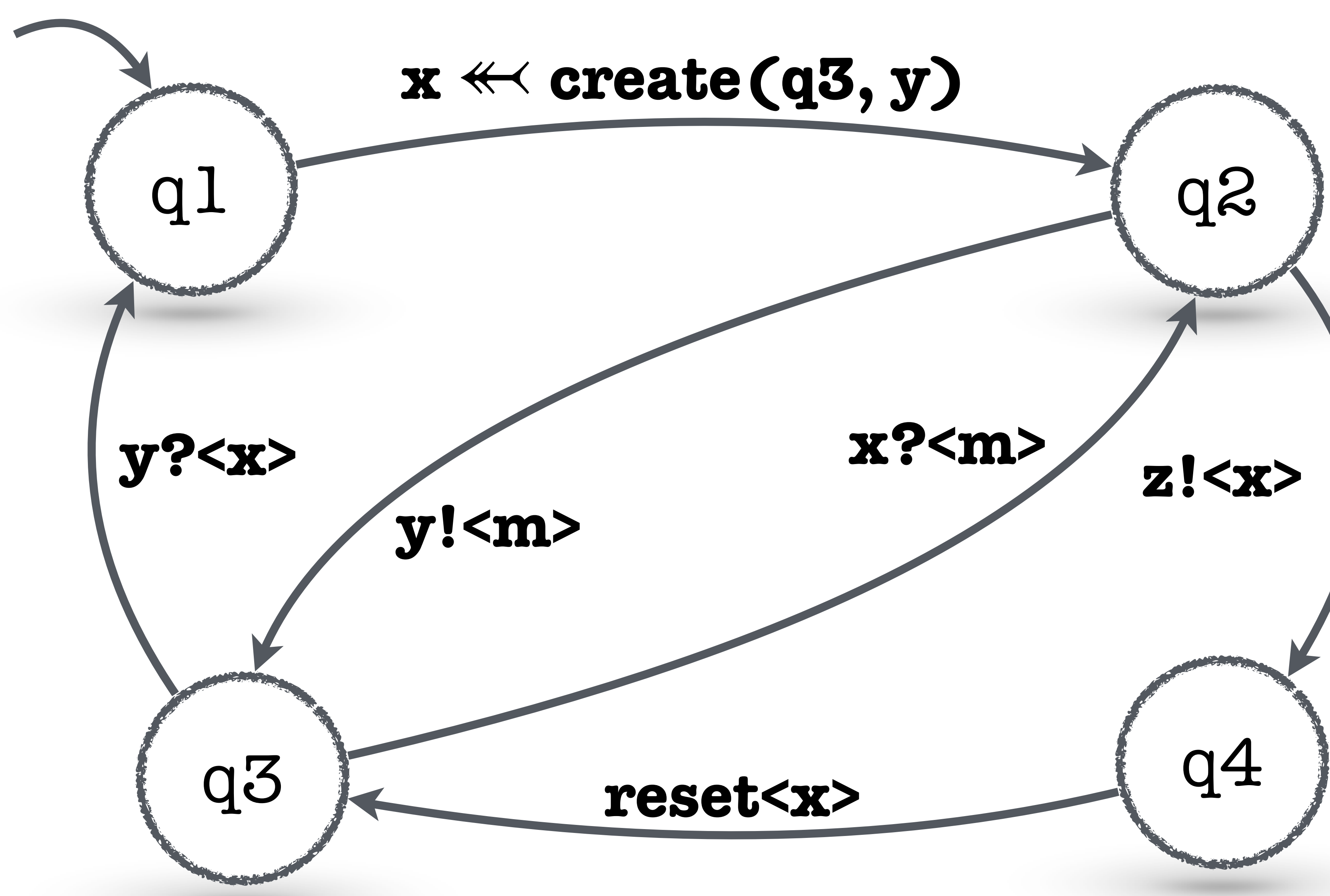
Applications

Formal Model

Dynamic Register Automata

Formal Model

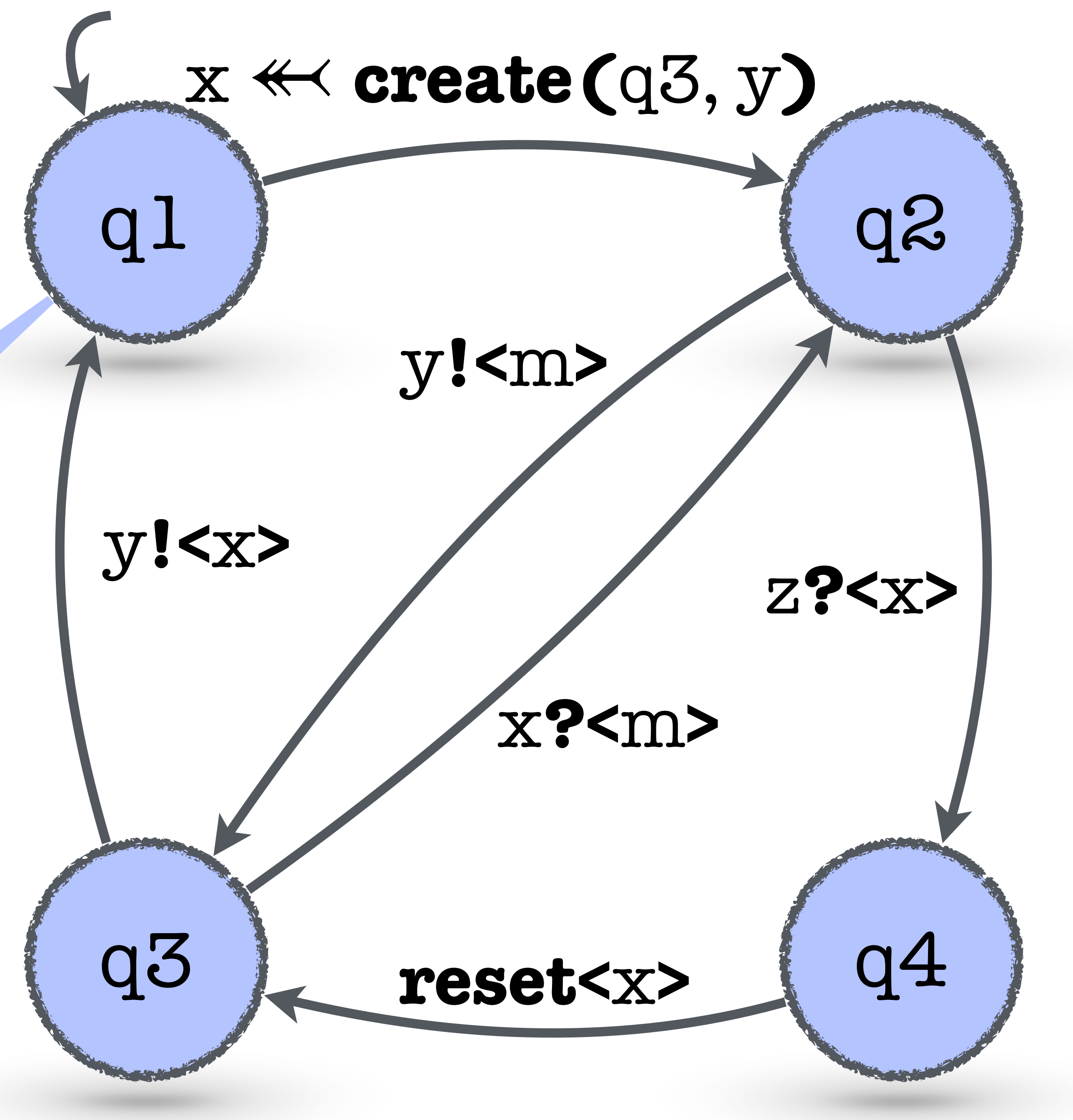
Process Model



Dynamic Register Automata

Formal Model | **Process Model**

Finite number of States

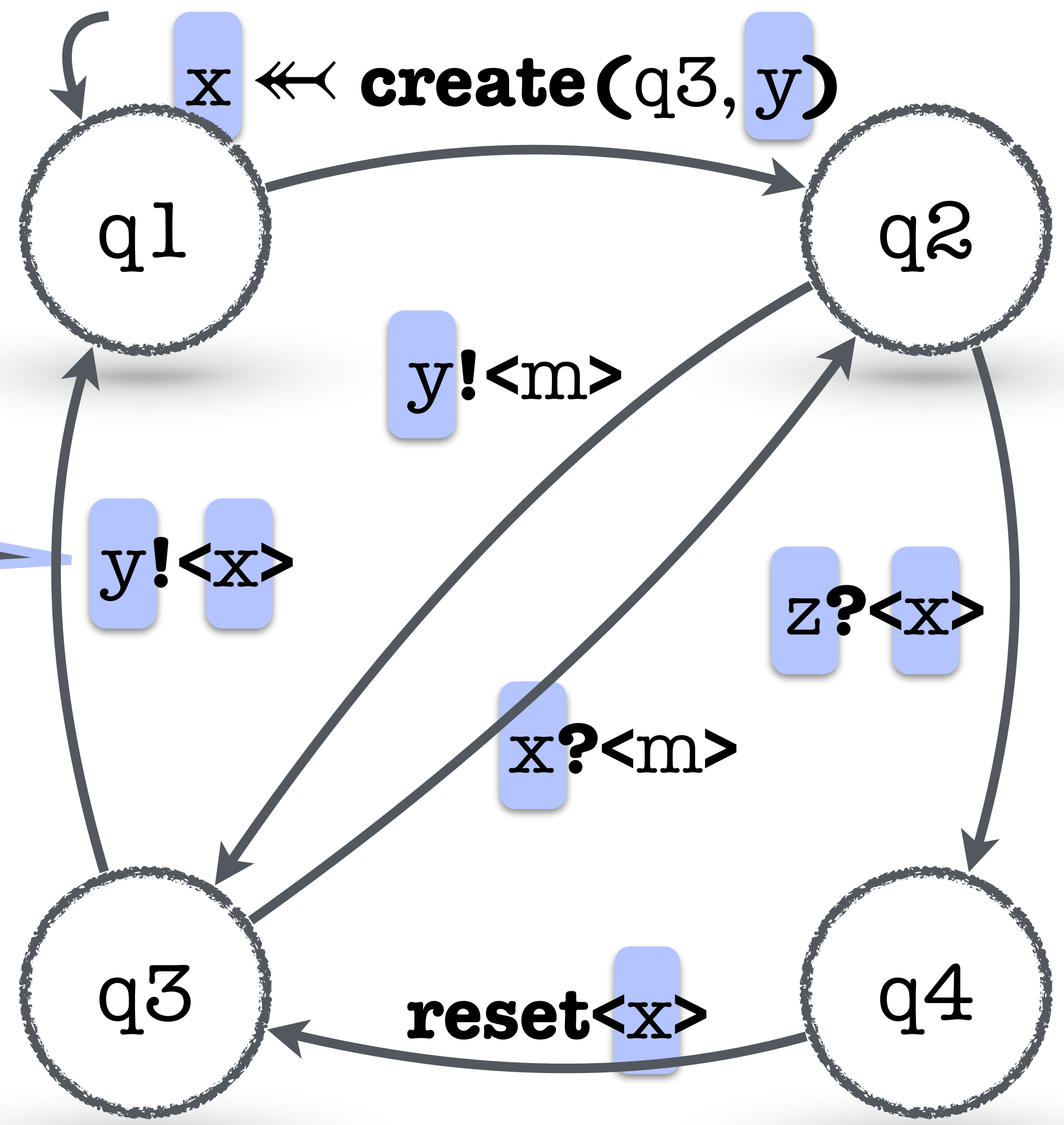


Dynamic Register Automata

Formal Model | **Process Model**

Finite number of States

Finite number of Registers



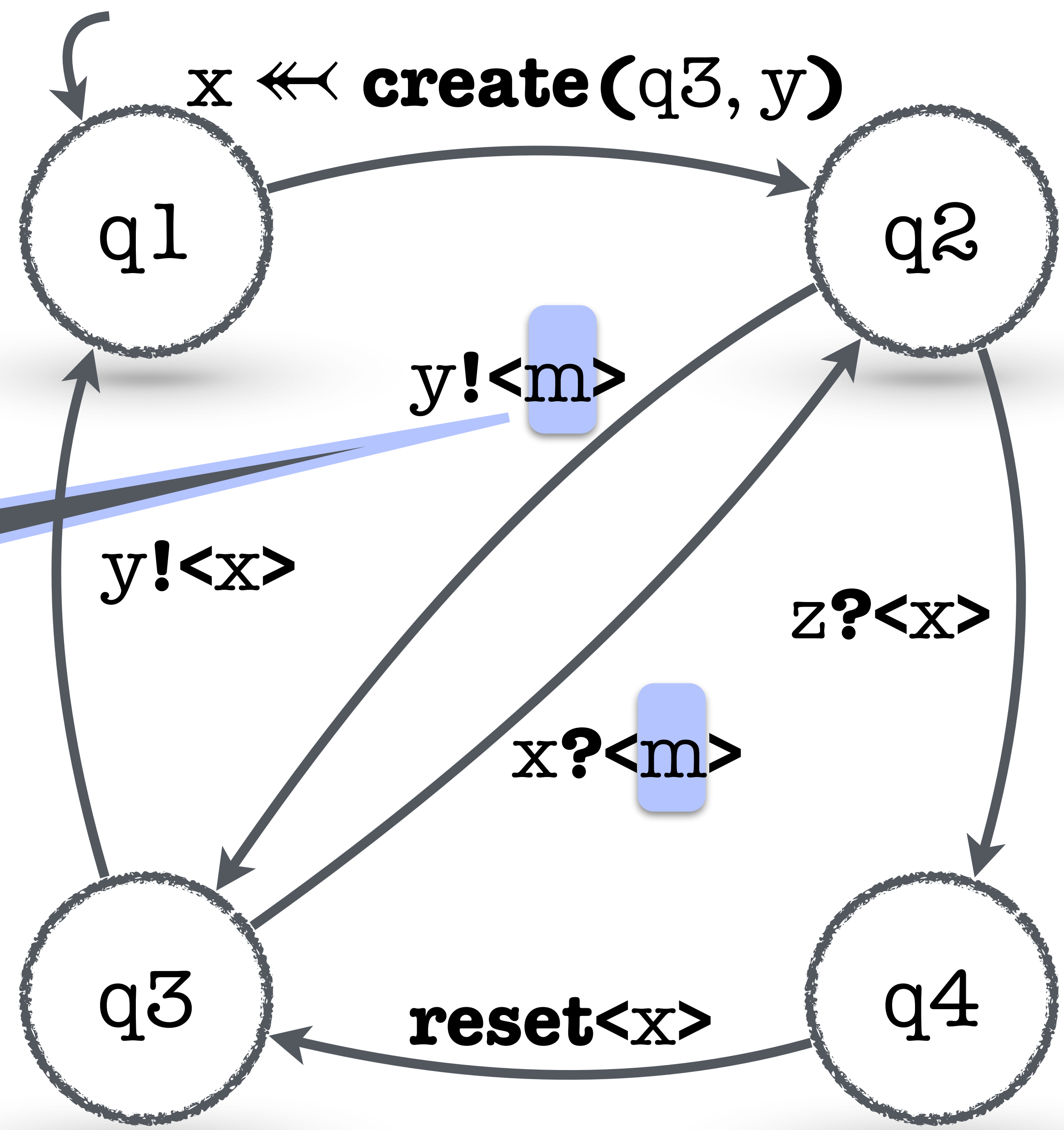
Dynamic Register Automata

Formal Model | **Process Model**

Finite number of States

Finite number of Registers

Finite message alphabet



Dynamic Register Automata

Formal Model | **Process Model**

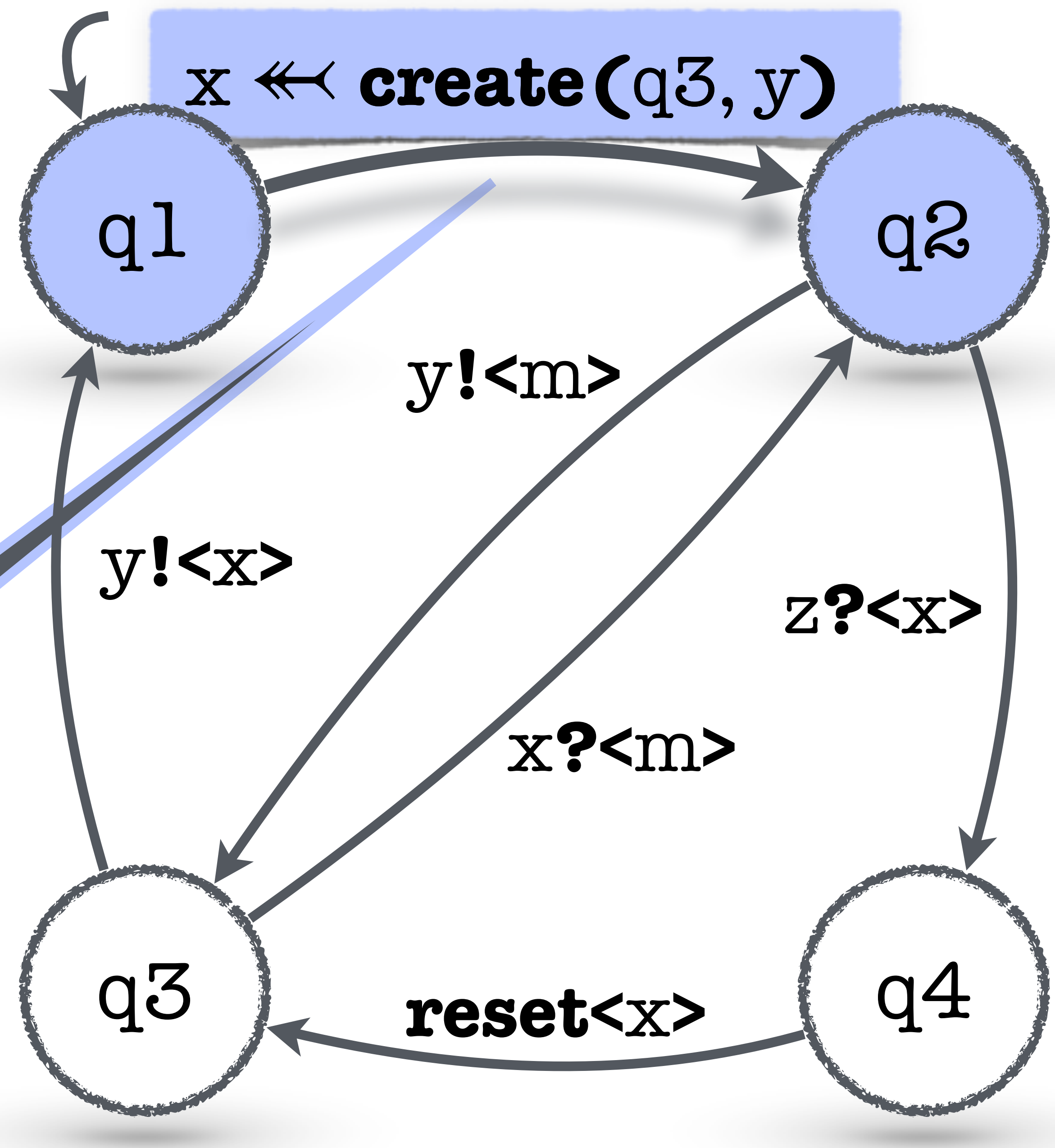
Finite number of States

Finite number of Registers

Finite message alphabet

Transitions:

Create Process



Dynamic Register Automata

Formal Model | **Process Model**

Finite number of States

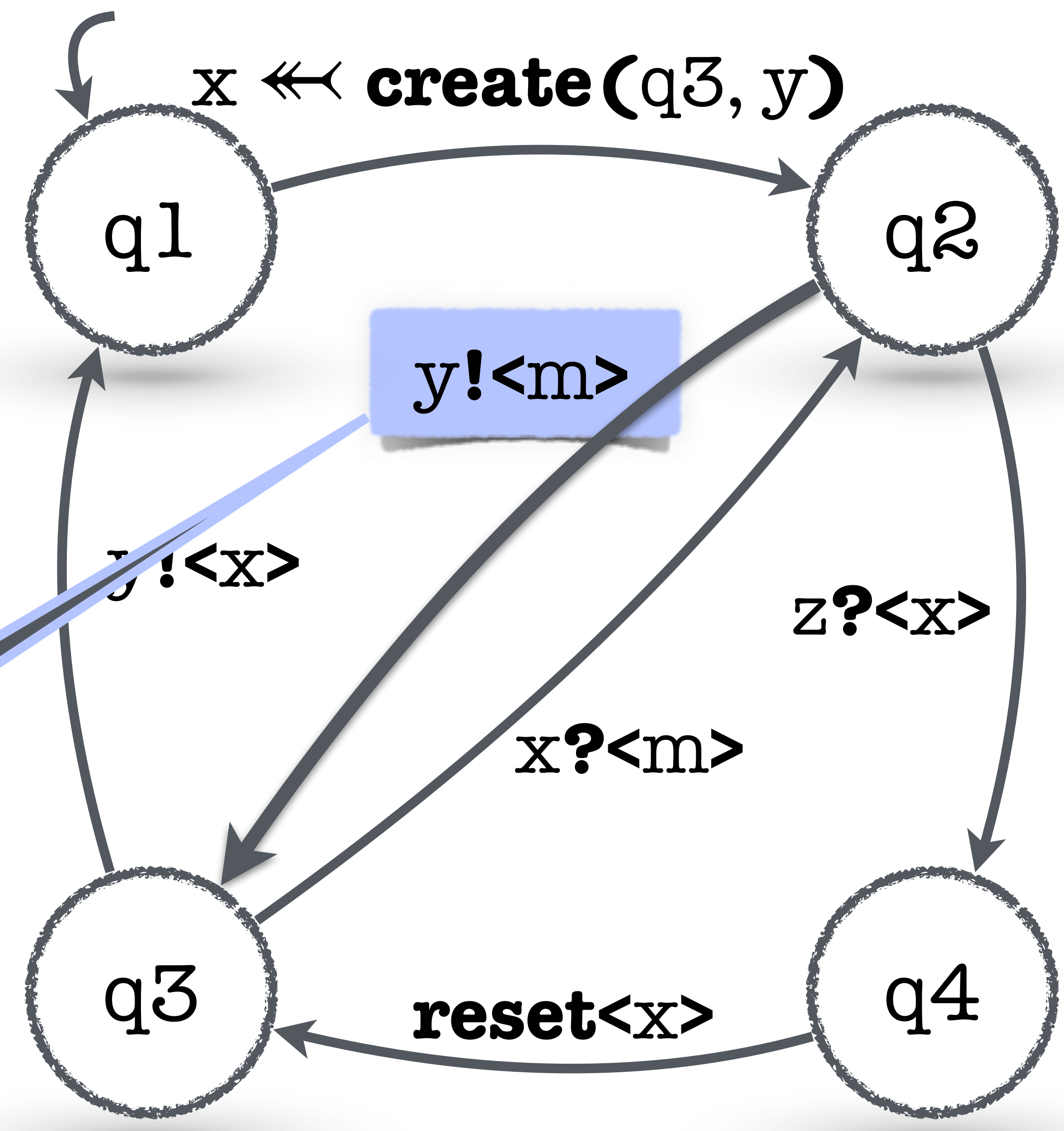
Finite number of Registers

Finite message alphabet

Transitions:

Create Process

Send Message



Dynamic Register Automata

Formal Model | **Process Model**

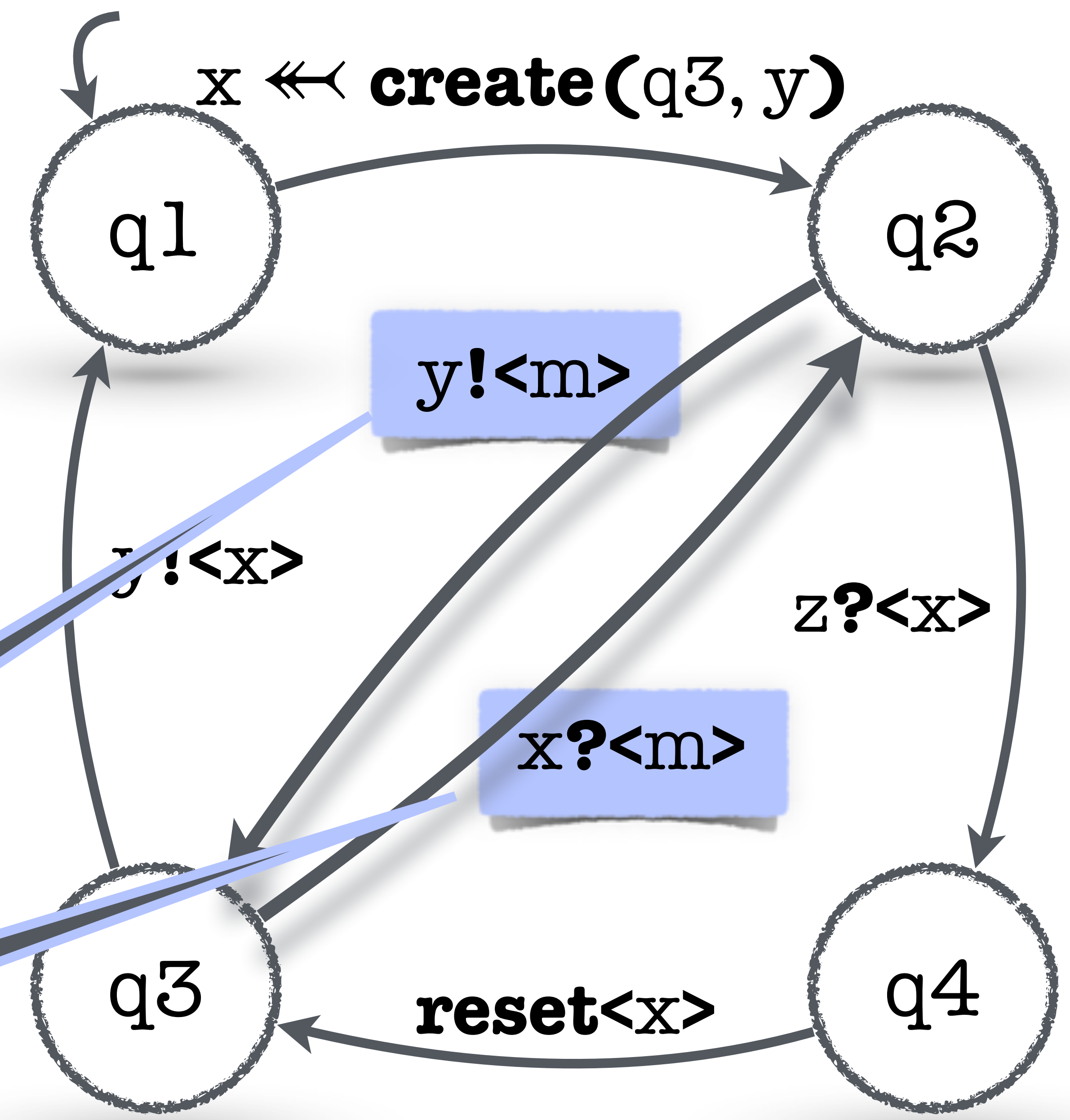
Finite number of States

Finite number of Registers

Finite message alphabet

Transitions:

- Create Process
- Send Message
- Receive Message



Dynamic Register Automata

Formal Model | **Process Model**

Finite number of States

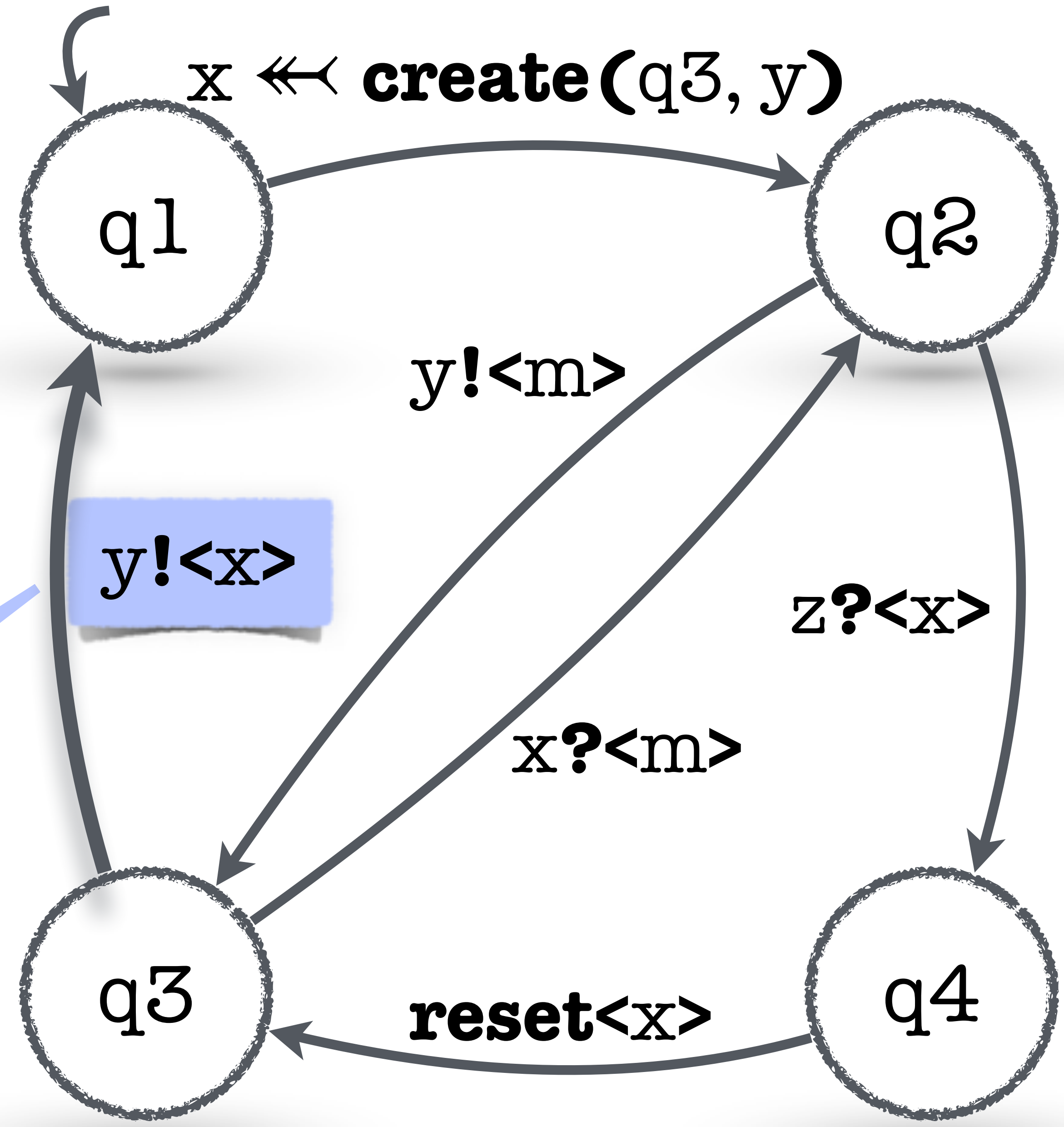
Finite number of Registers

Finite message alphabet

Transitions:

Create Process

Send ID



Dynamic Register Automata

Formal Model | **Process Model**

Finite number of States

Finite number of Registers

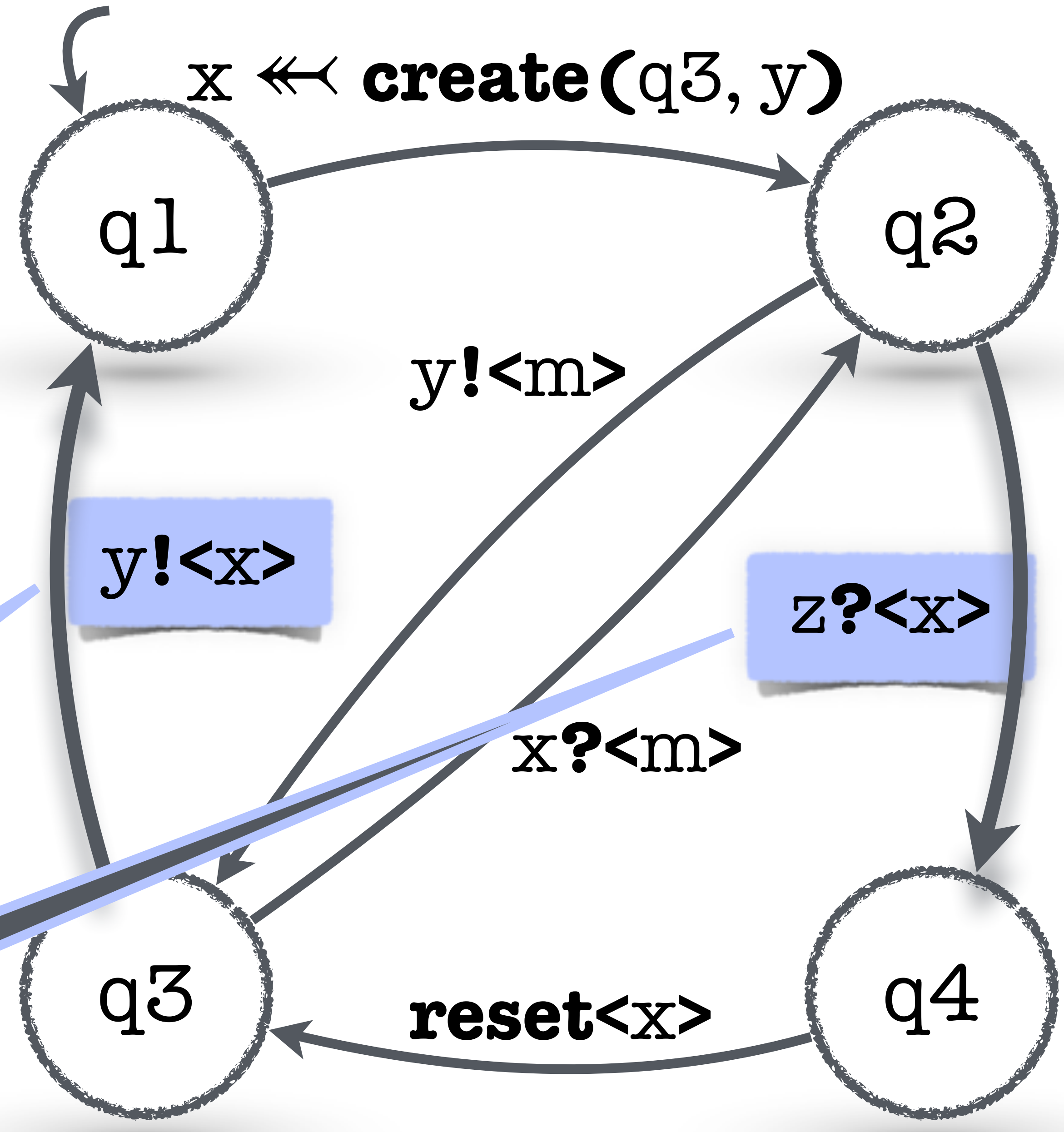
Finite message alphabet

Transitions:

Create Process

Send ID

Receive ID



Dynamic Register Automata

Verification of Dynamic Register Automata

Formal Model

Finite number of States

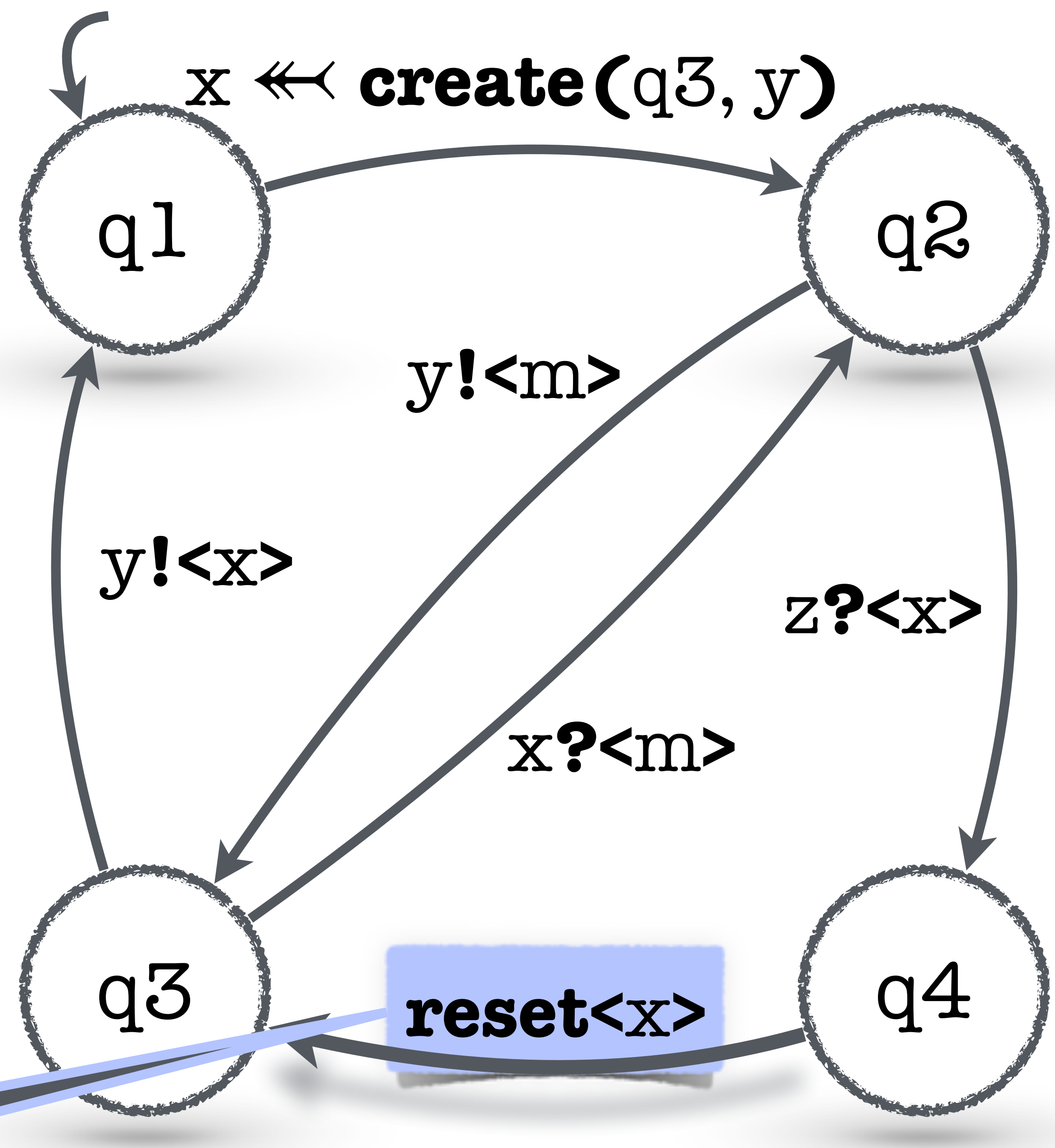
Finite number of Registers

Finite message alphabet

Transitions:

- Create Process
- Send Msg / ID
- Receive Msg / ID
- Register Reset

Process Model



Dynamic Register Automata

Formal Model | **Process Model**

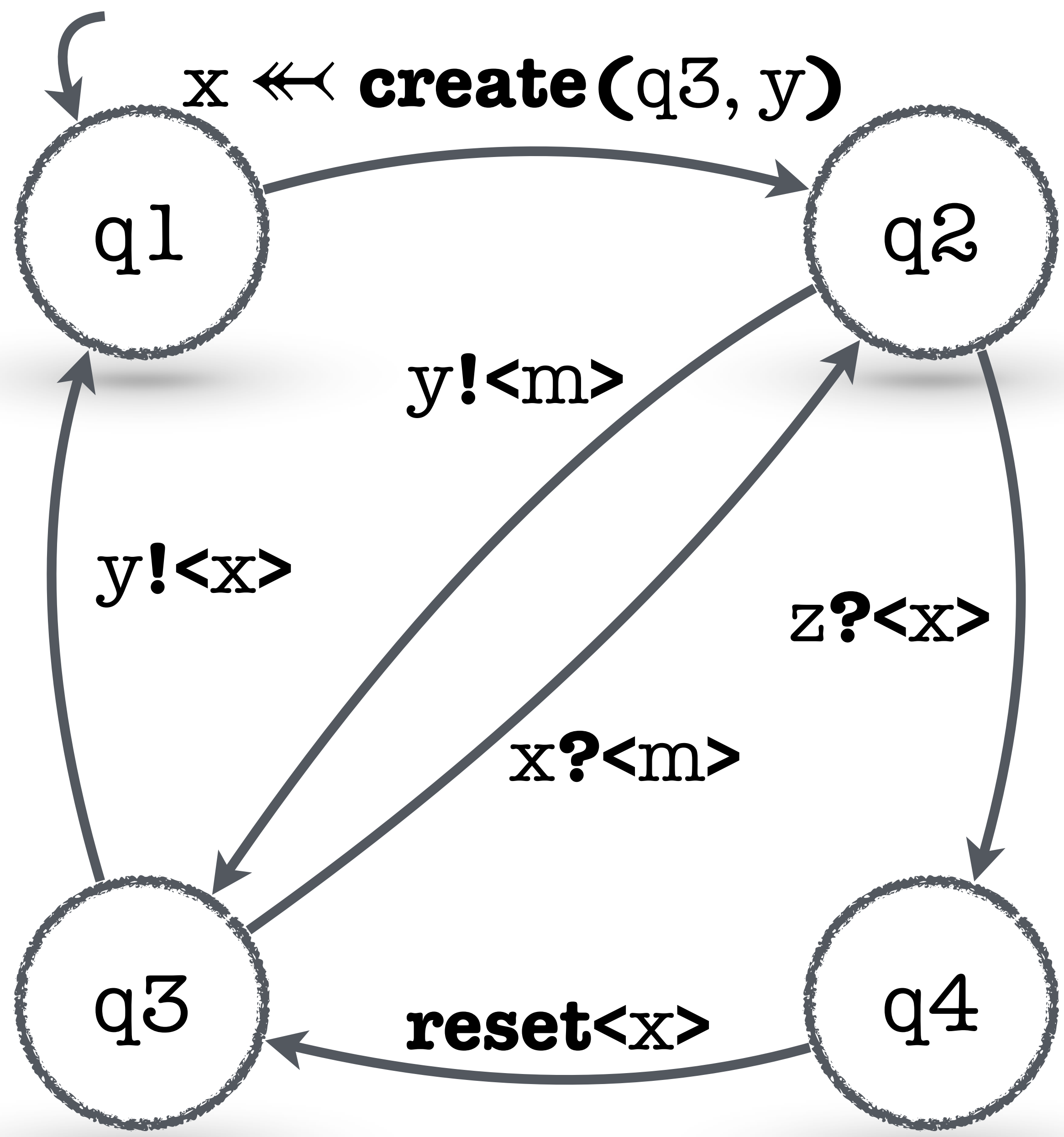
Finite number of States

Finite number of Registers

Finite message alphabet

Transitions:

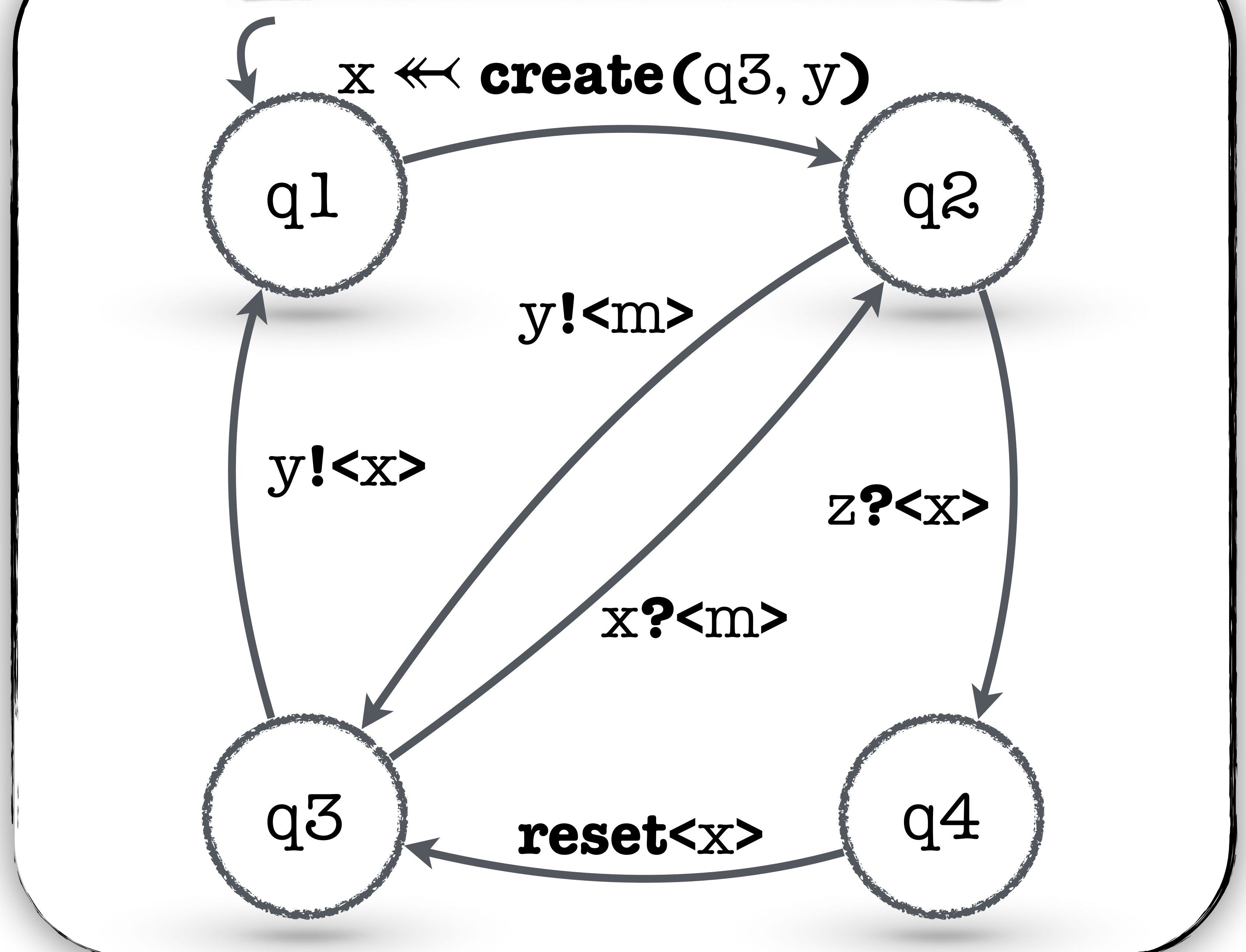
- Create Process
- Send Msg / ID
- Receive Msg / ID
- Register Reset



Dynamic Register Automata

Formal Model

Process Model

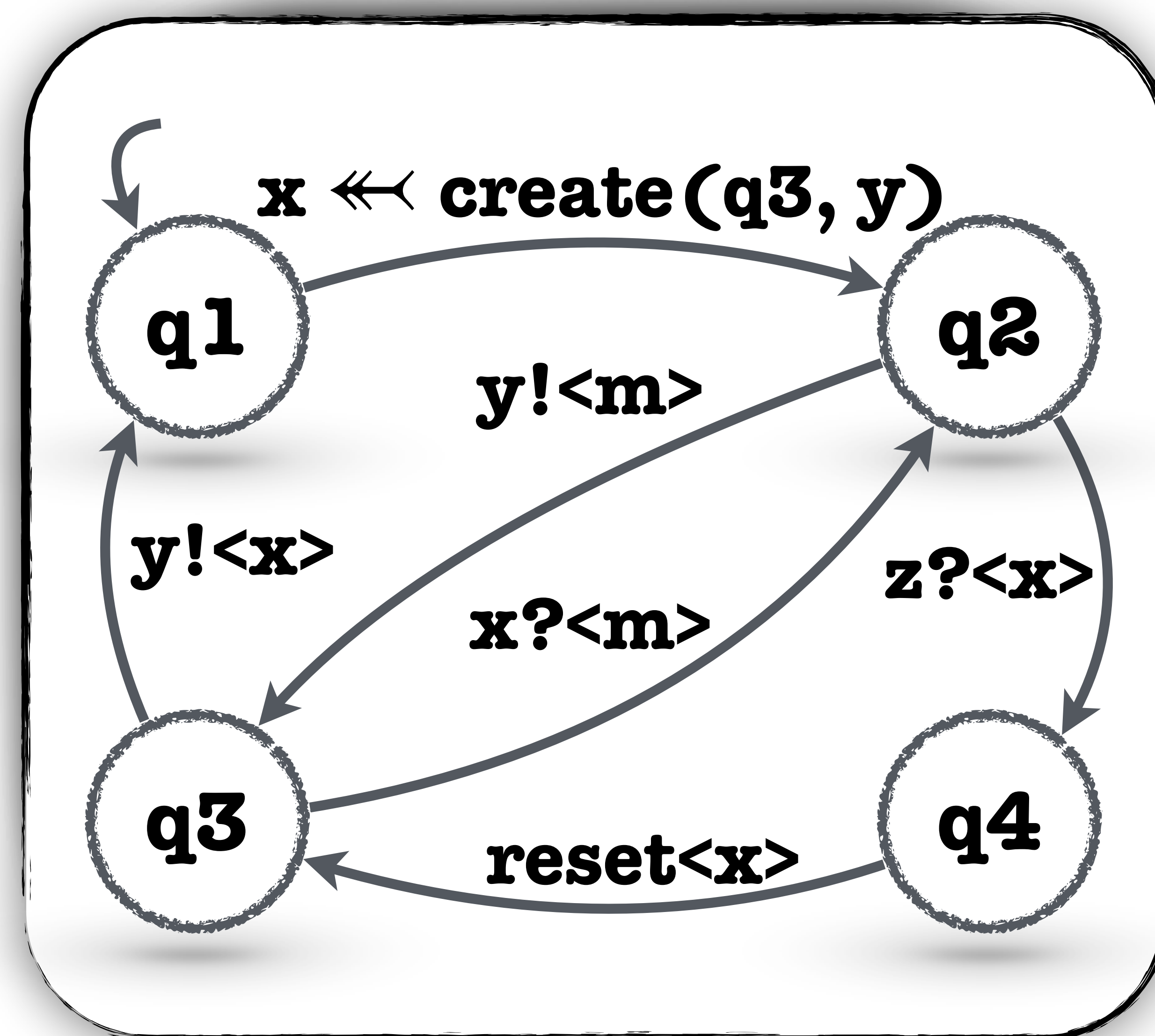


Dynamic Register Automata

Formal Model

Process Model

Finite State System



Dynamic Register Automata

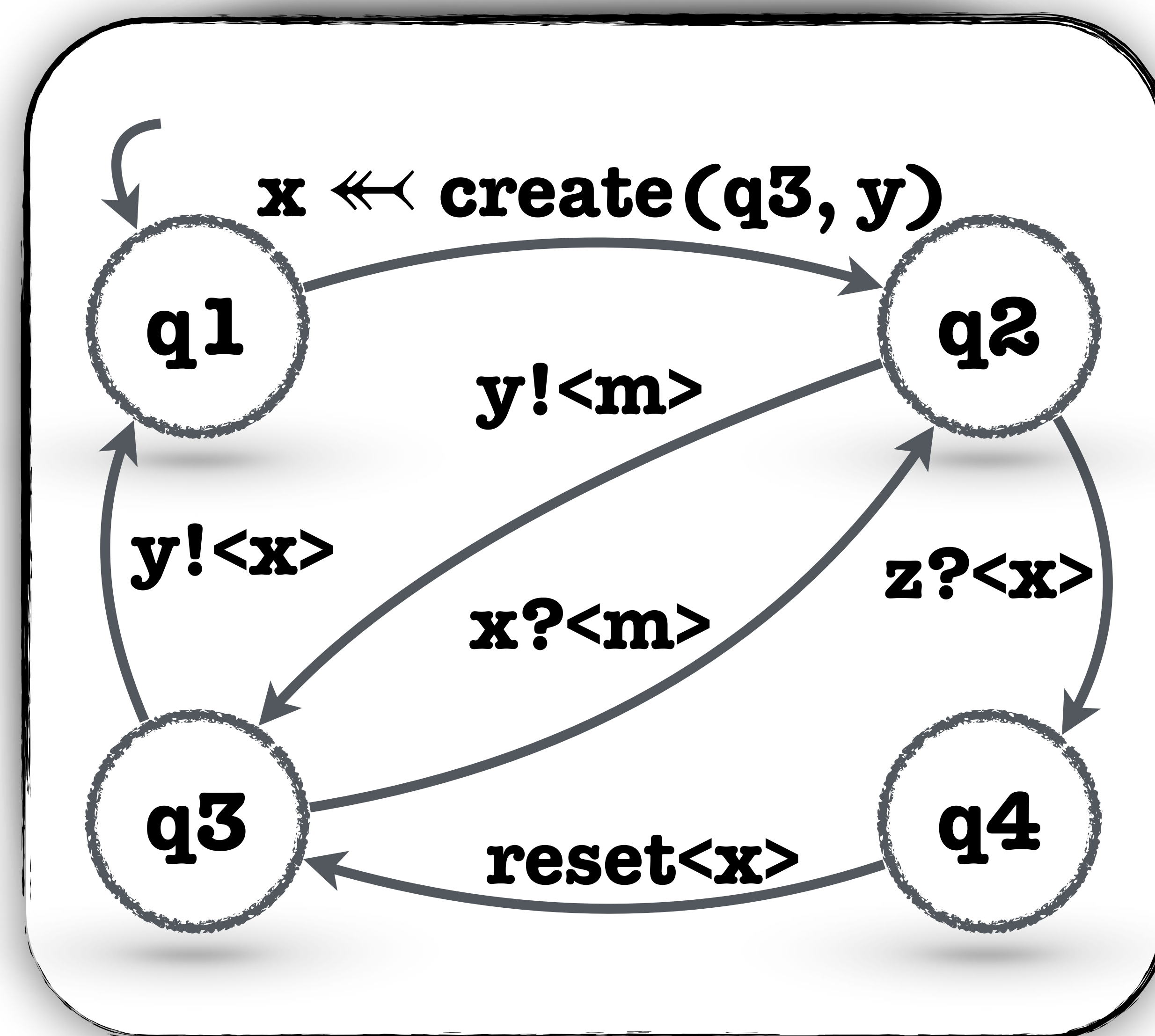
Formal Model

Configuration

Network of Processes

Process Model

Finite State System

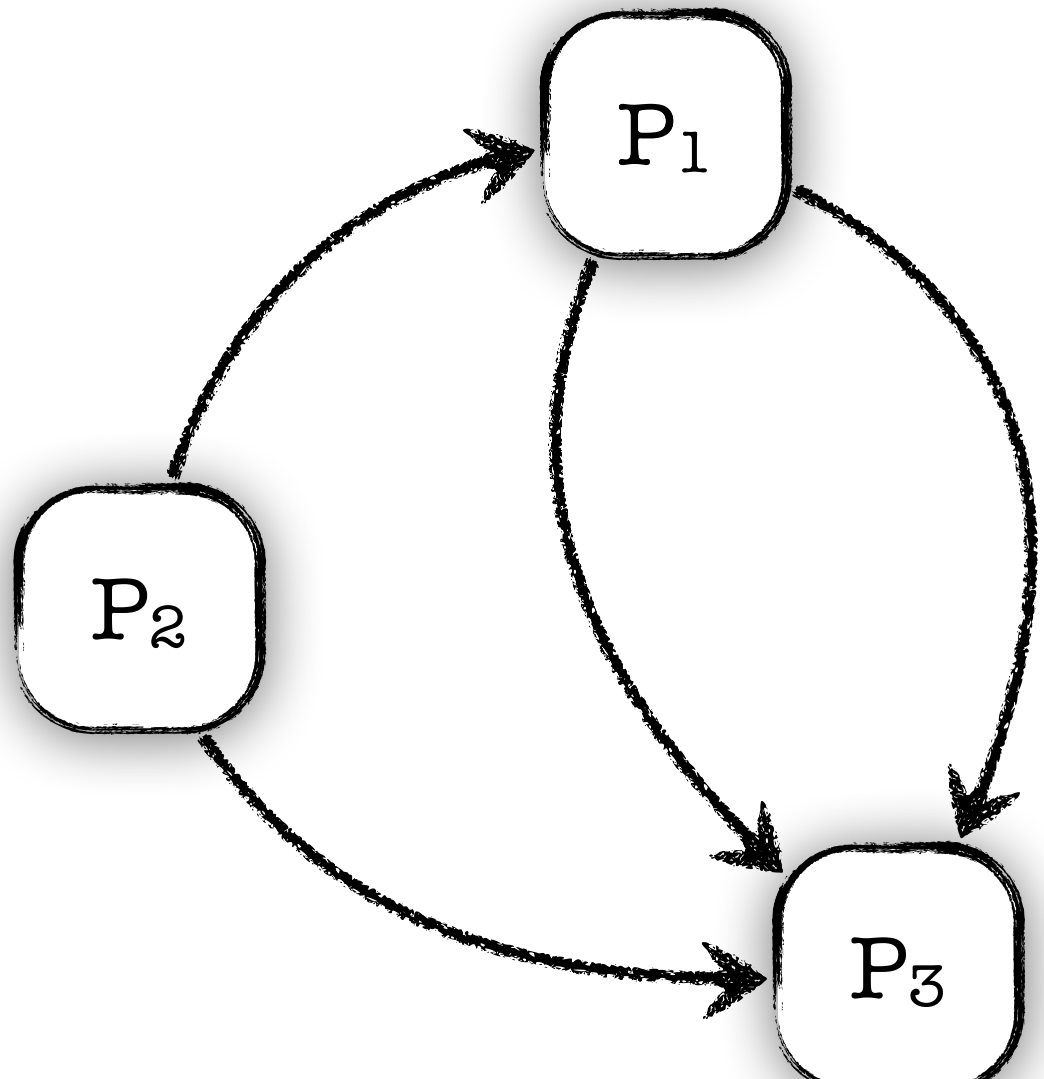


Dynamic Register Automata

Formal Model

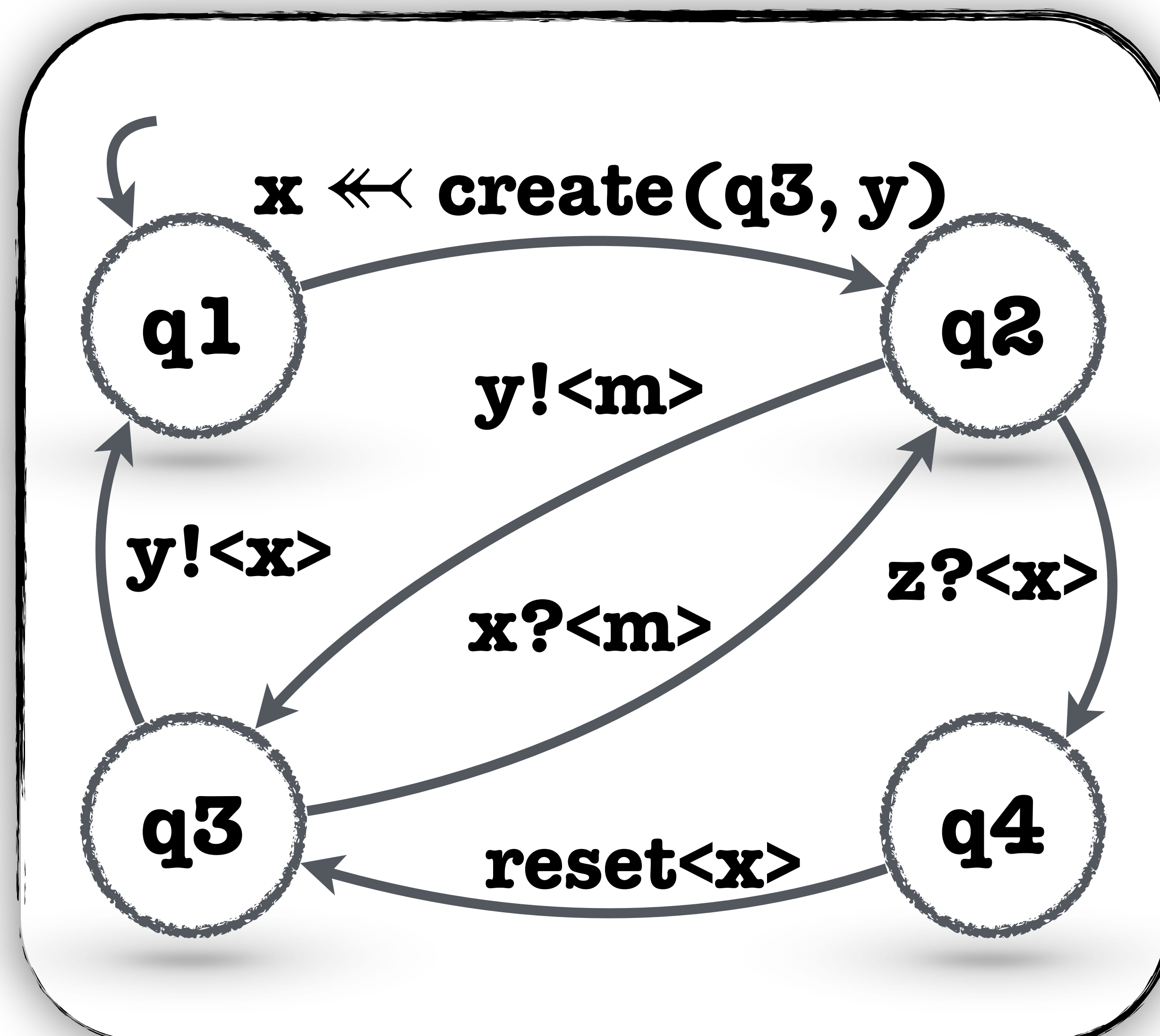
Configuration

Network of Processes



Process Model

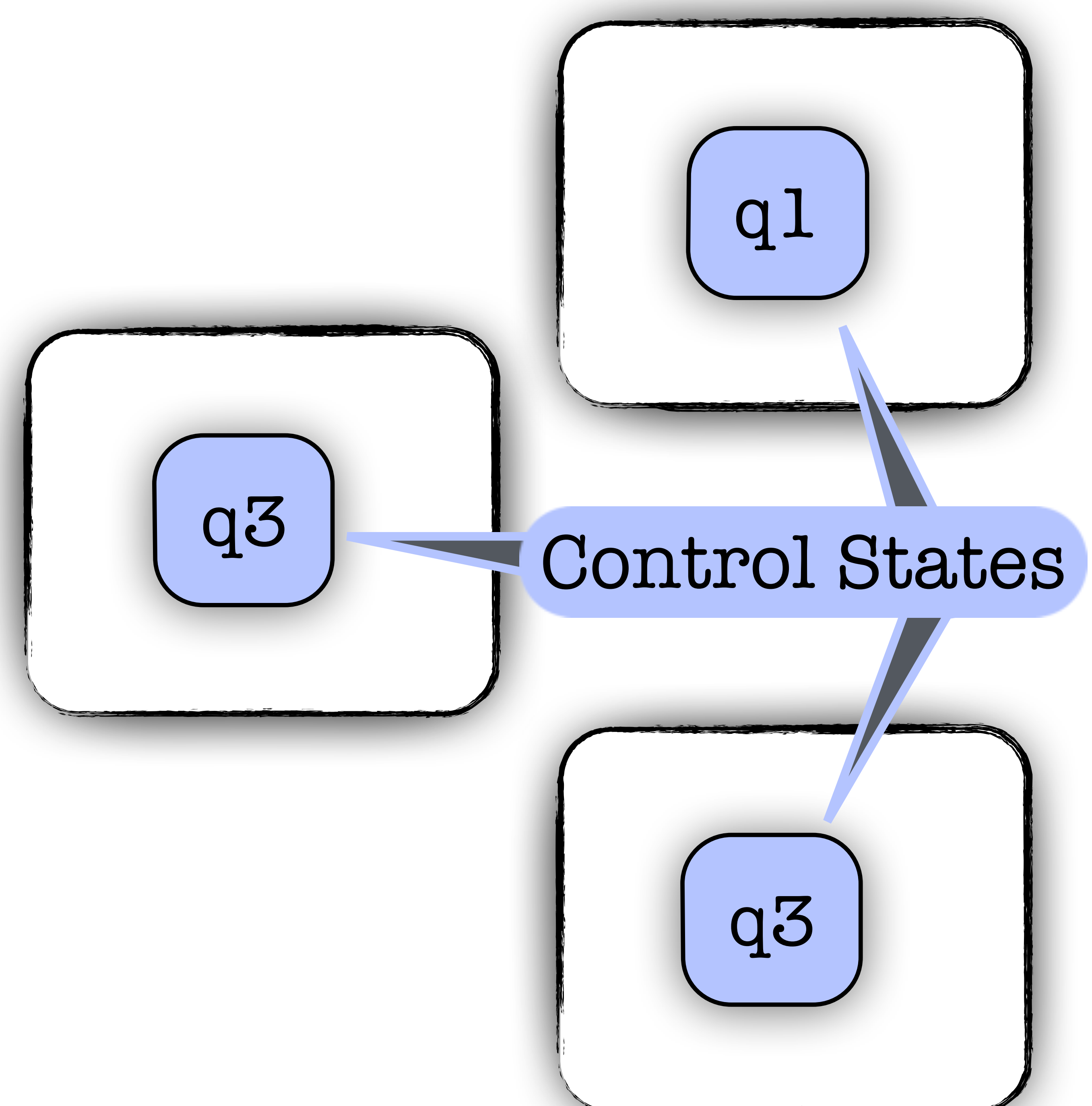
Finite State System



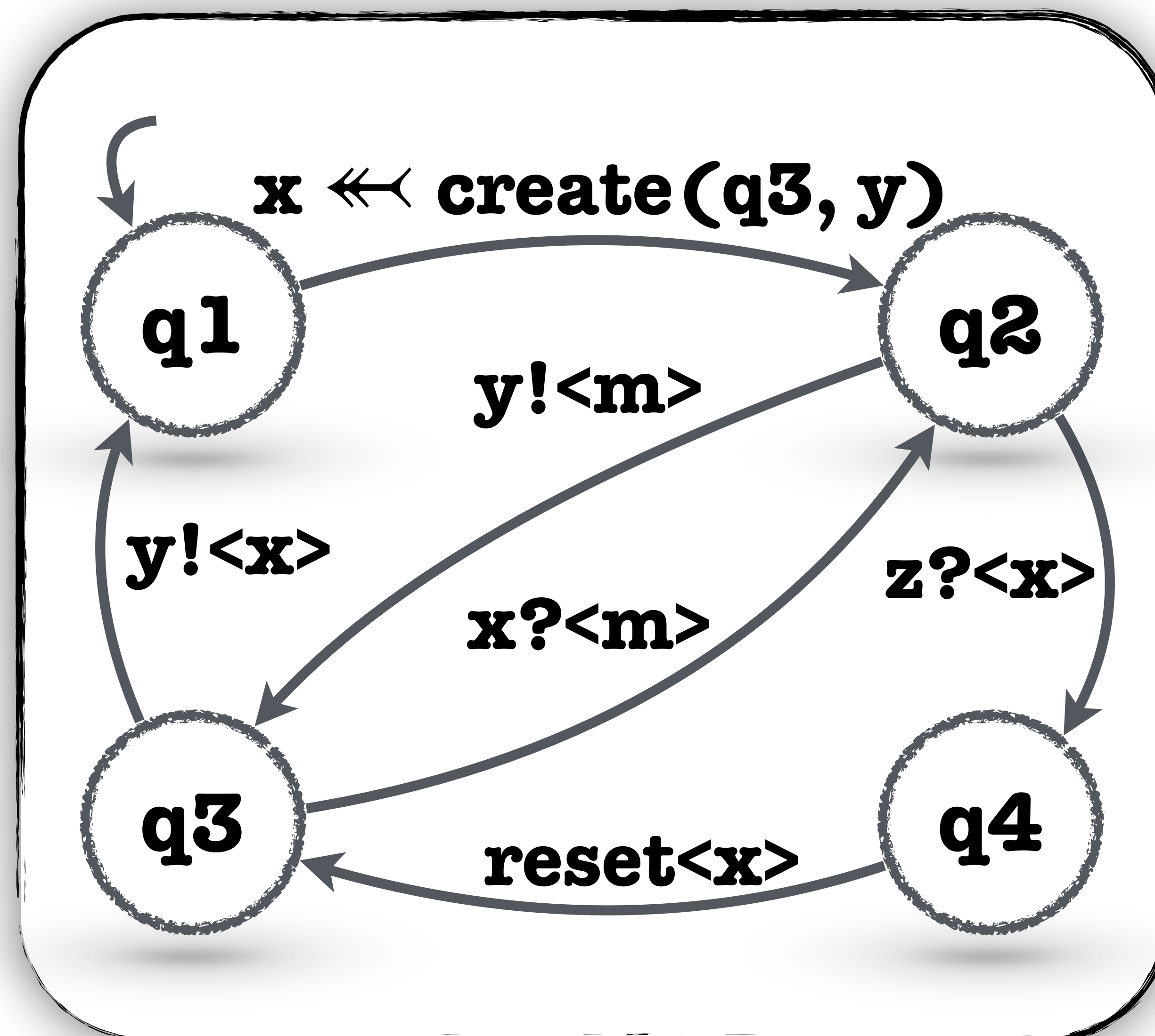
Dynamic Register Automata

Formal Model

Configuration



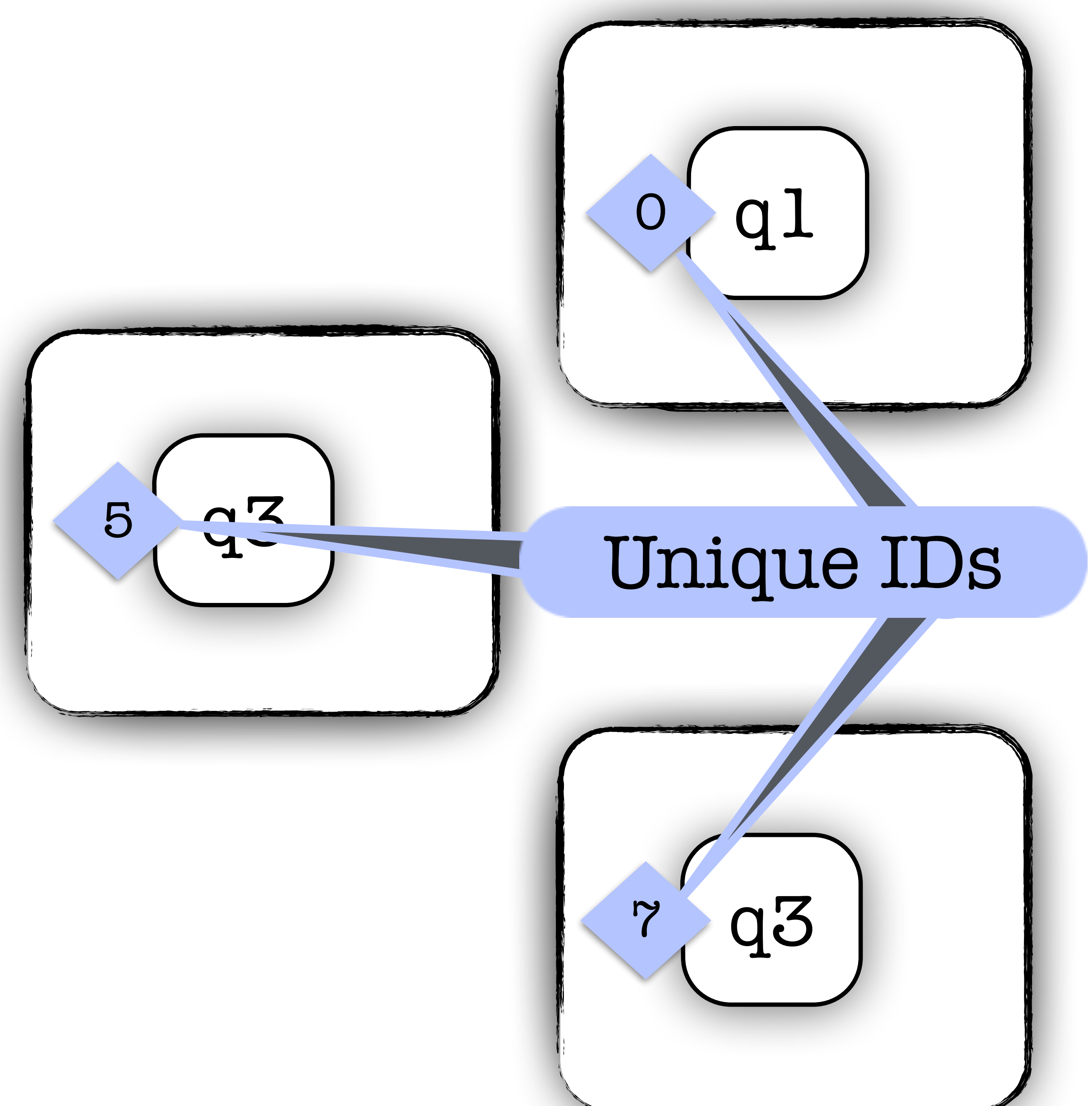
Process Model



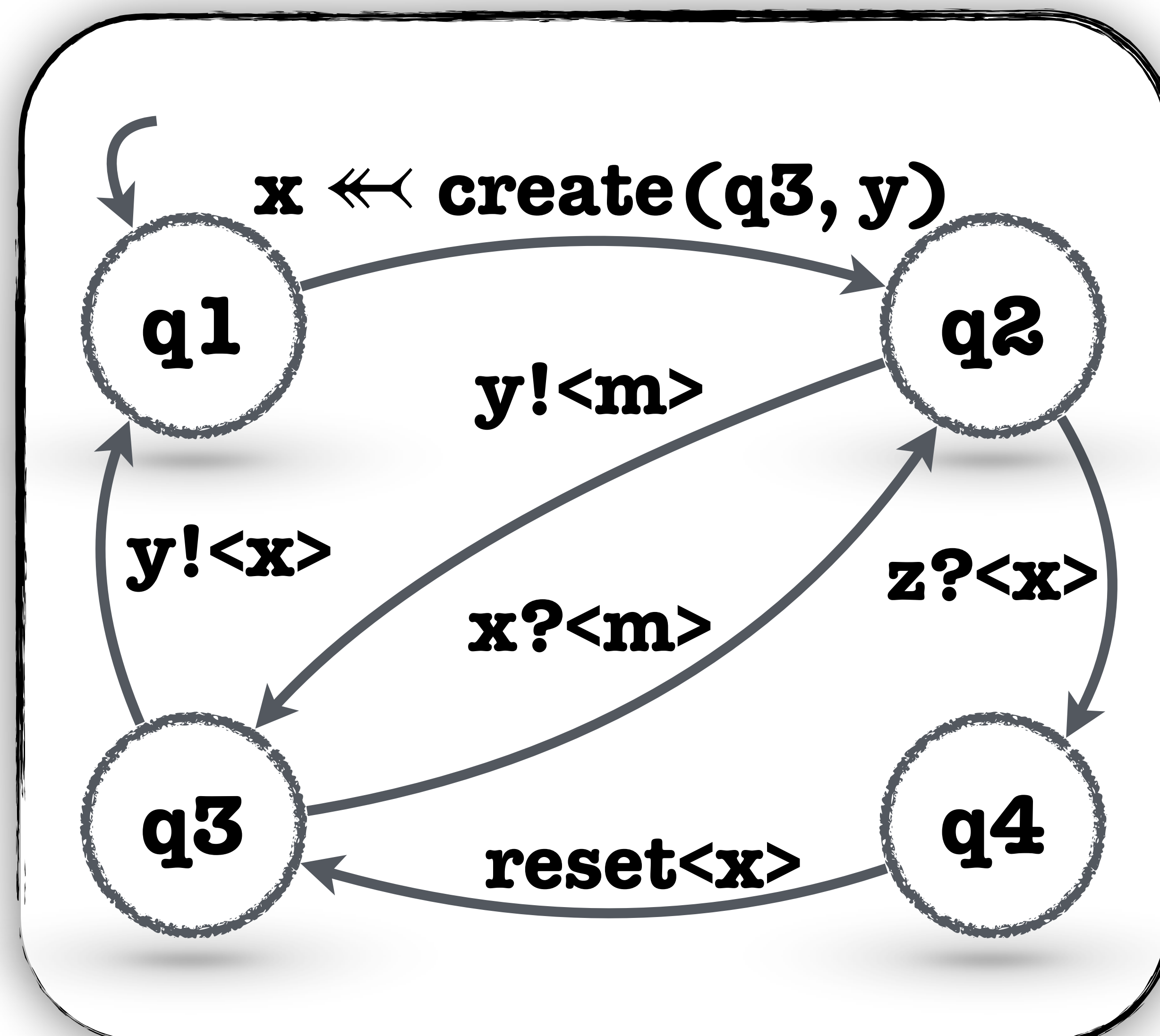
Dynamic Register Automata

Formal Model

Configuration



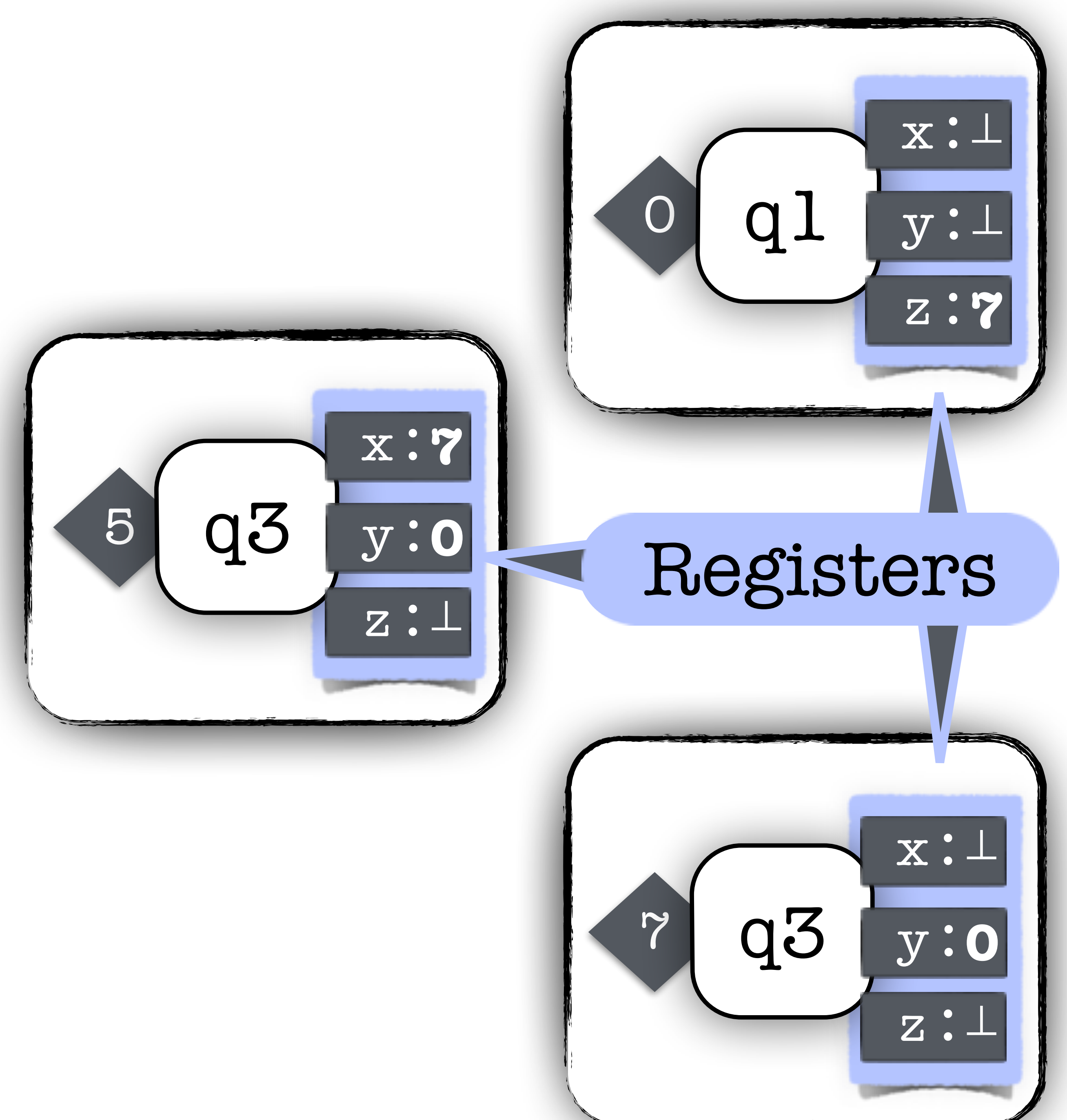
Process Model



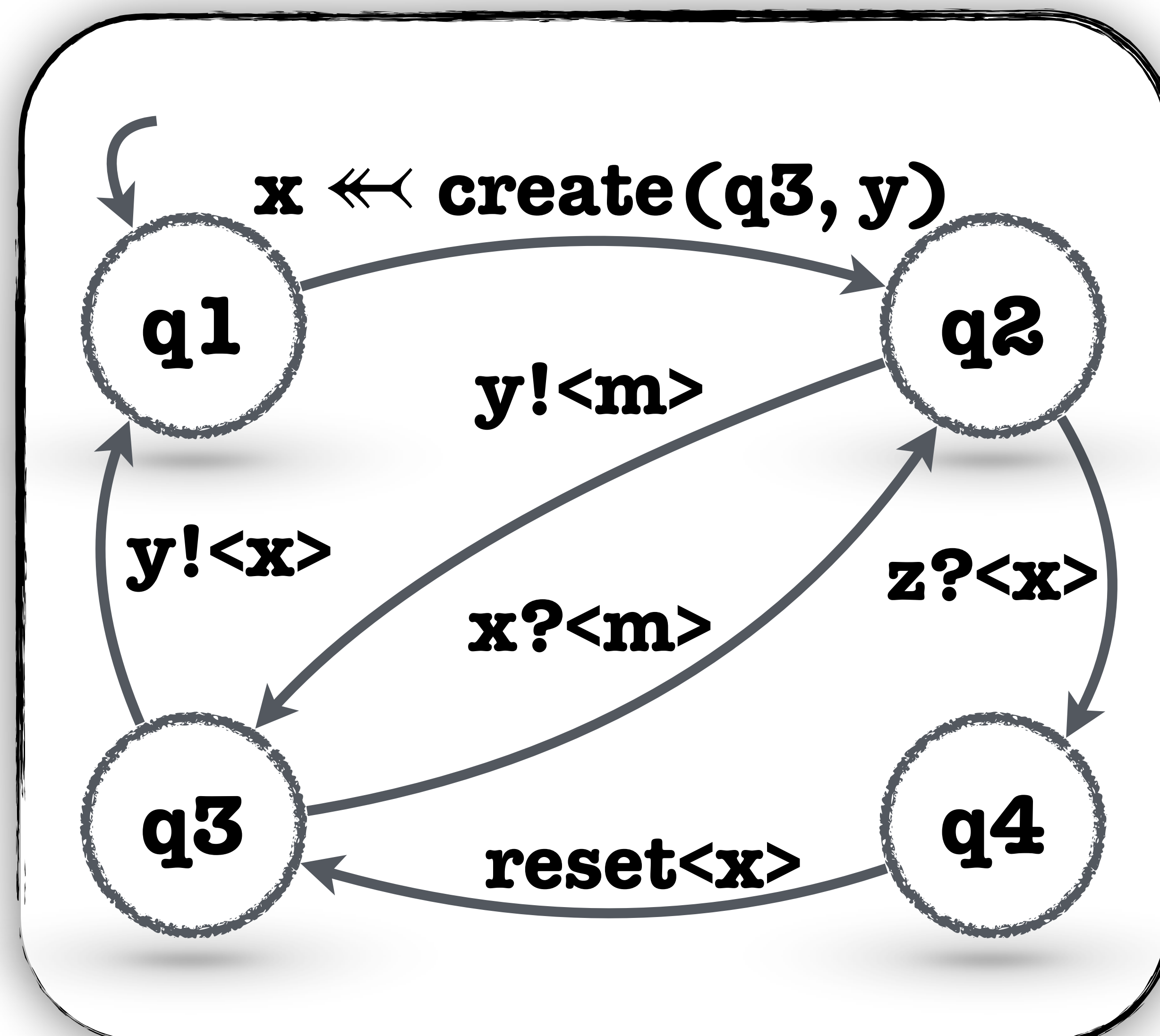
Dynamic Register Automata

Formal Model

Configuration



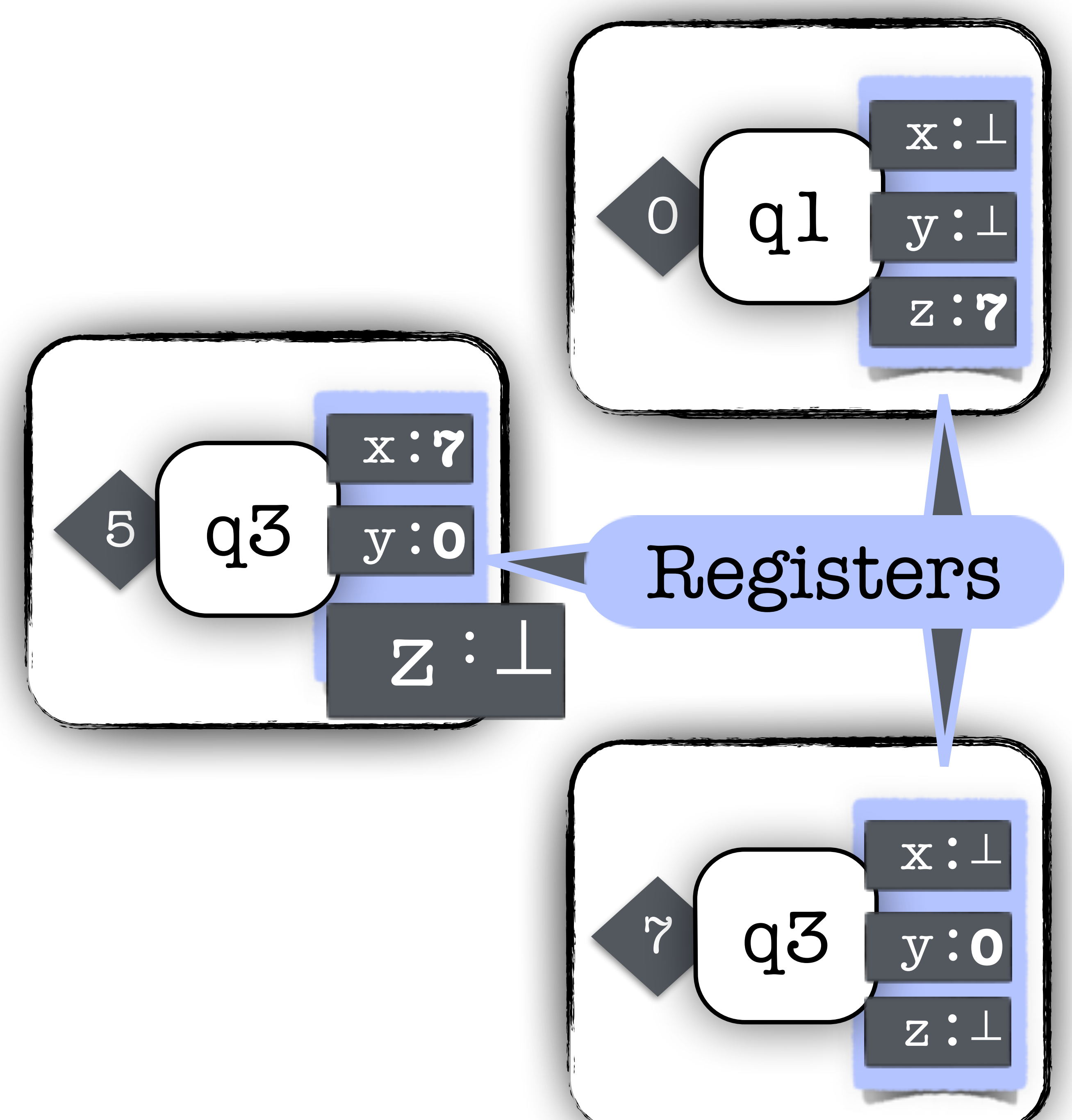
Process Model



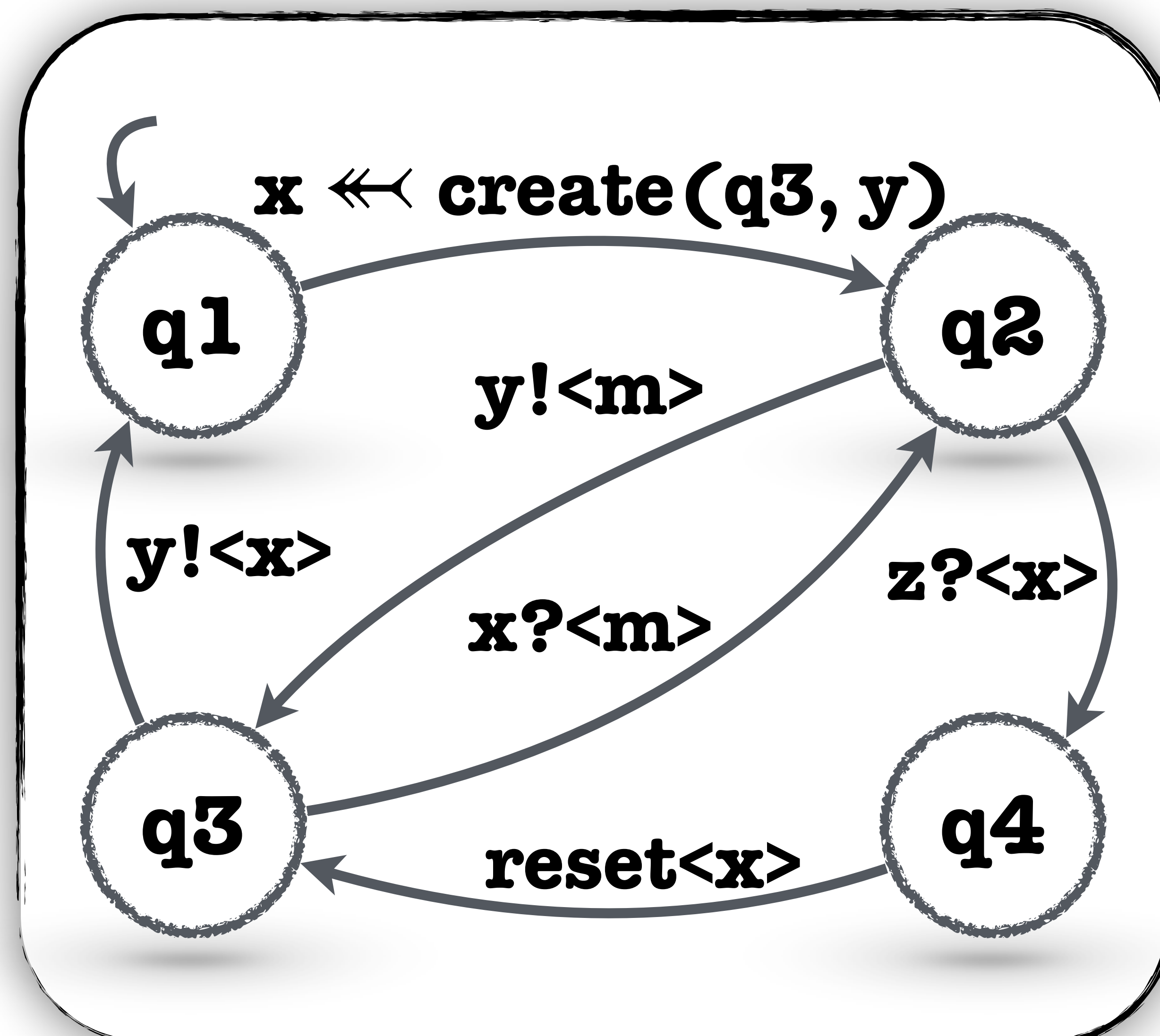
Dynamic Register Automata

Formal Model

Configuration



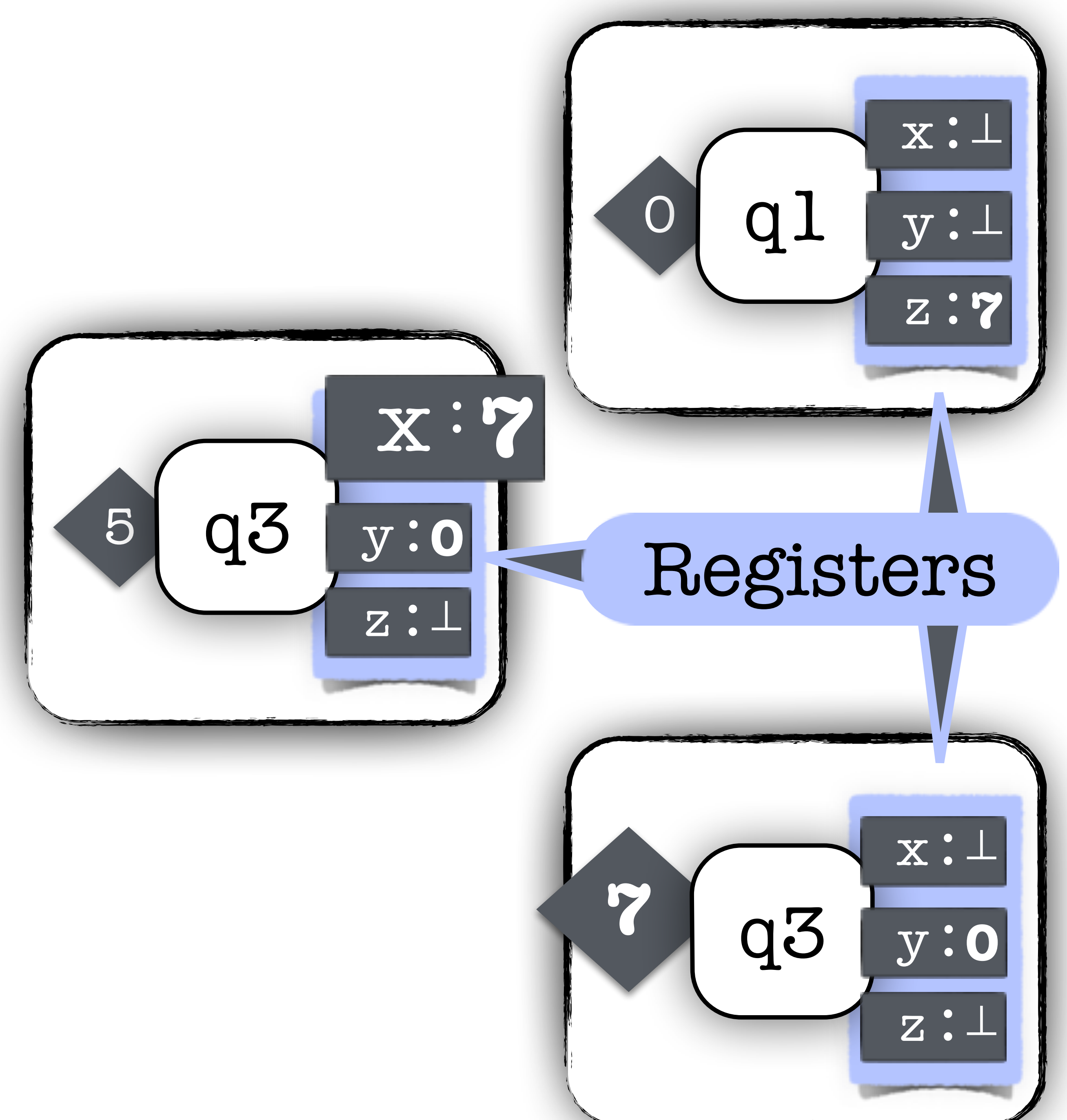
Process Model



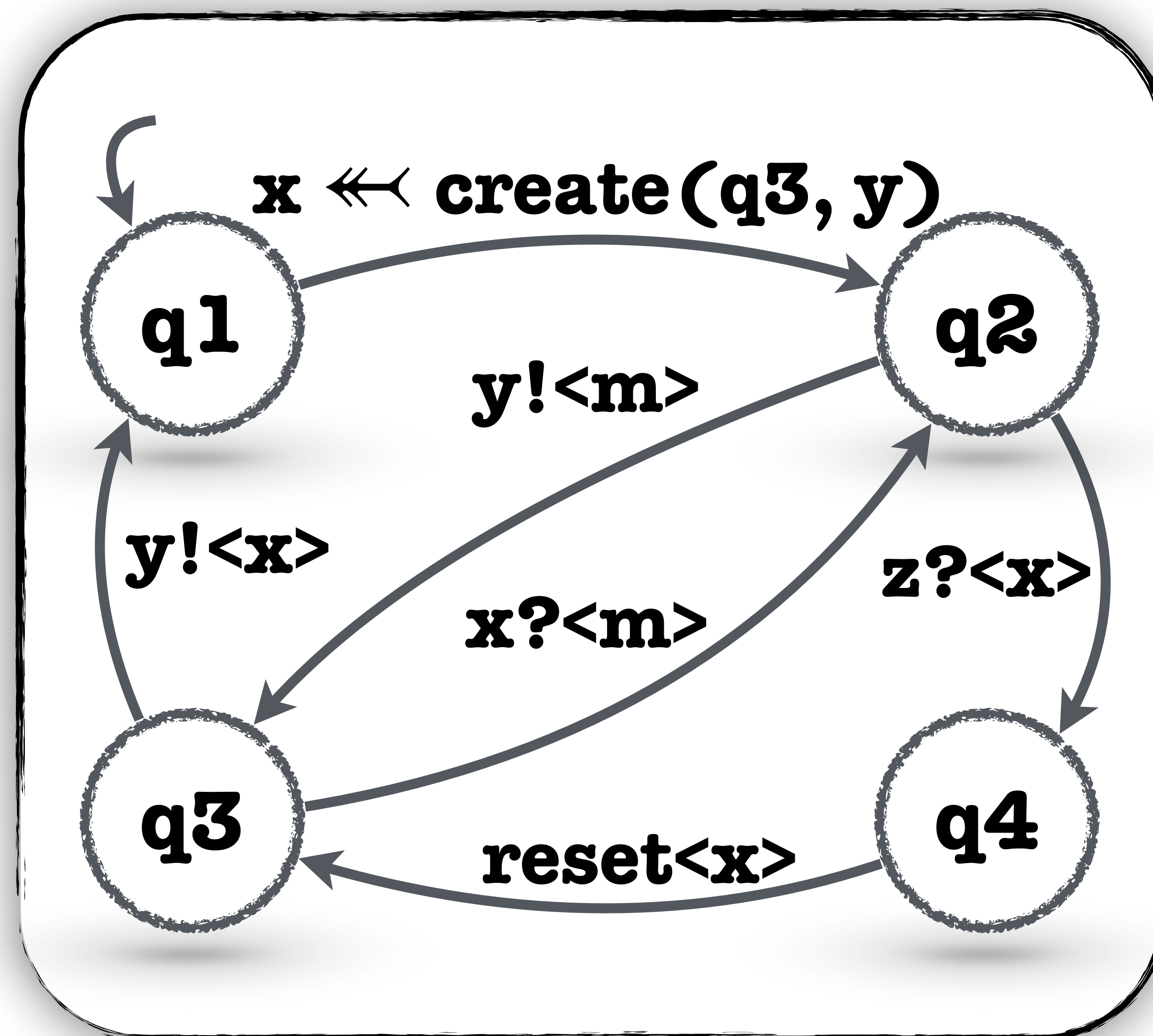
Dynamic Register Automata

Formal Model

Configuration



Process Model

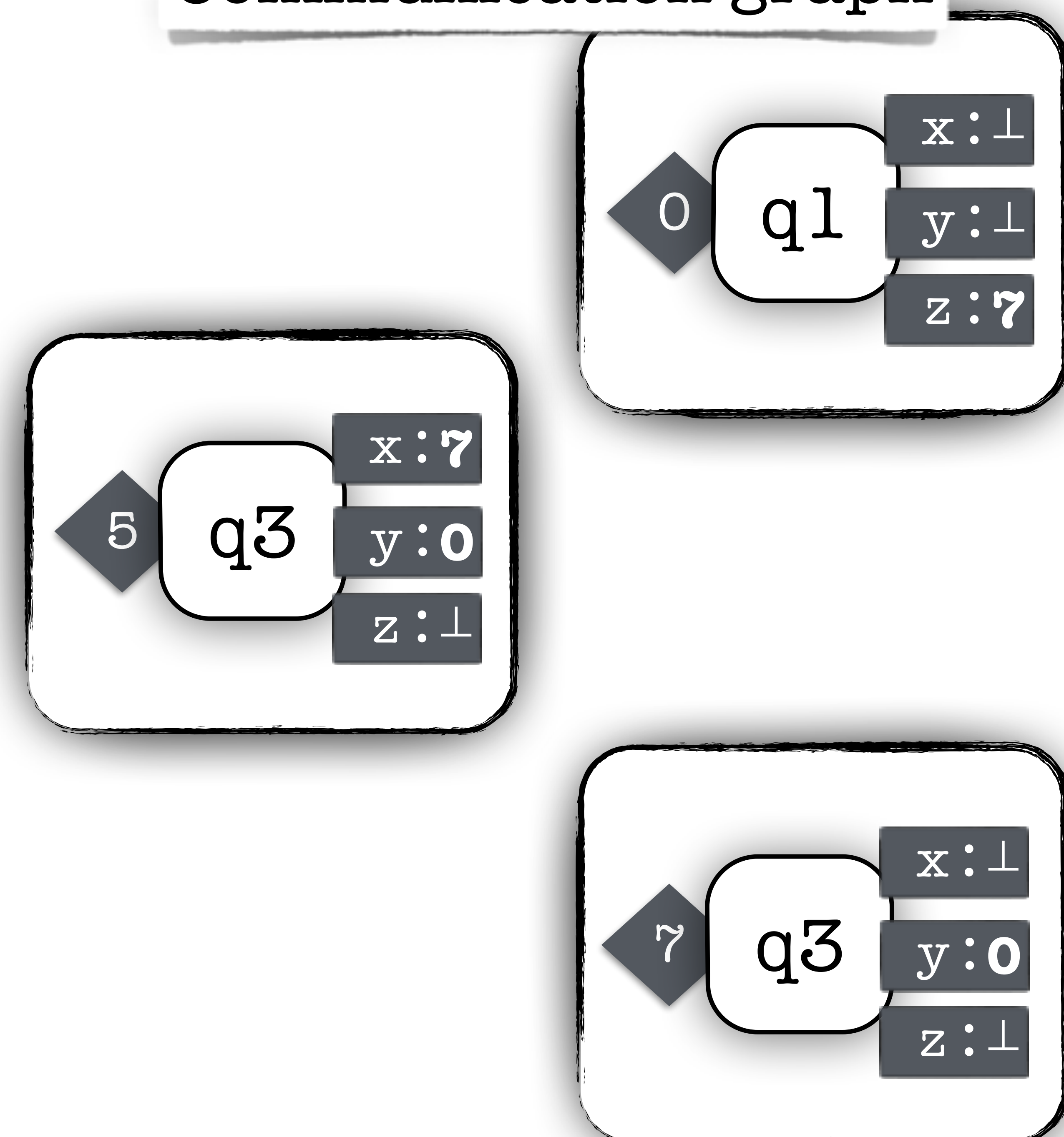


Dynamic Register Automata

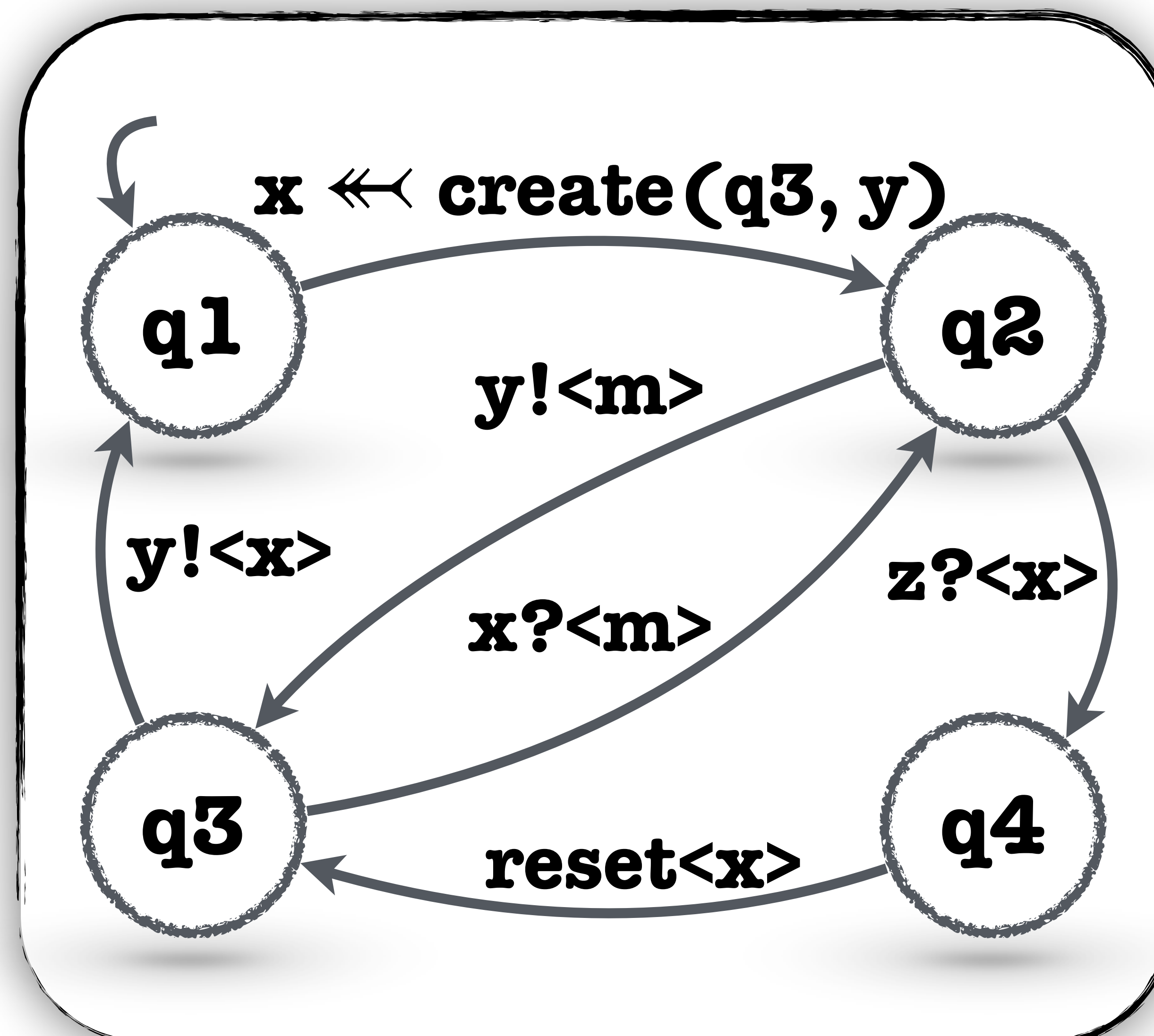
Formal Model

Configuration

Communication graph



Process Model

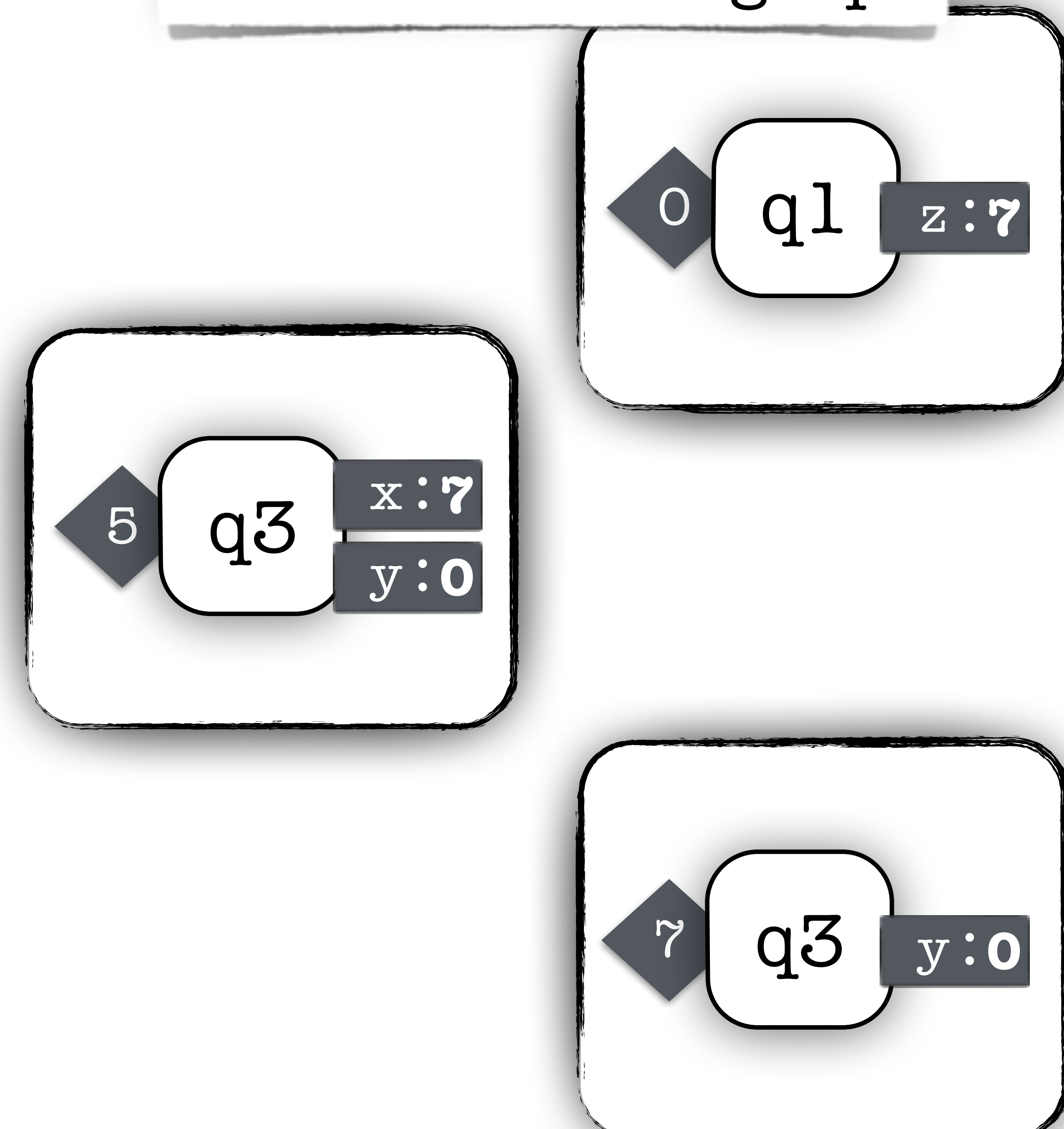


Dynamic Register Automata

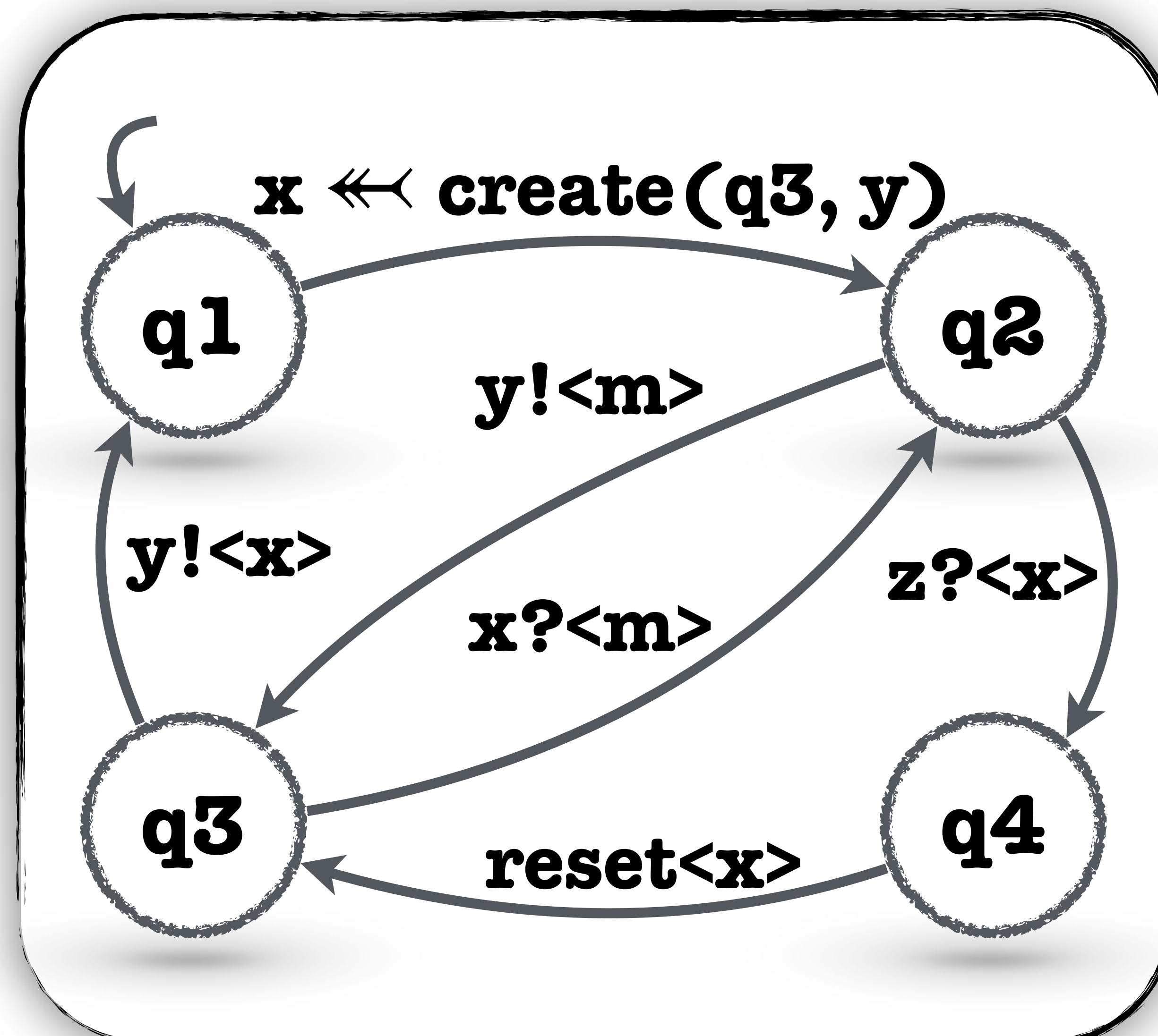
Formal Model

Configuration

Communication graph



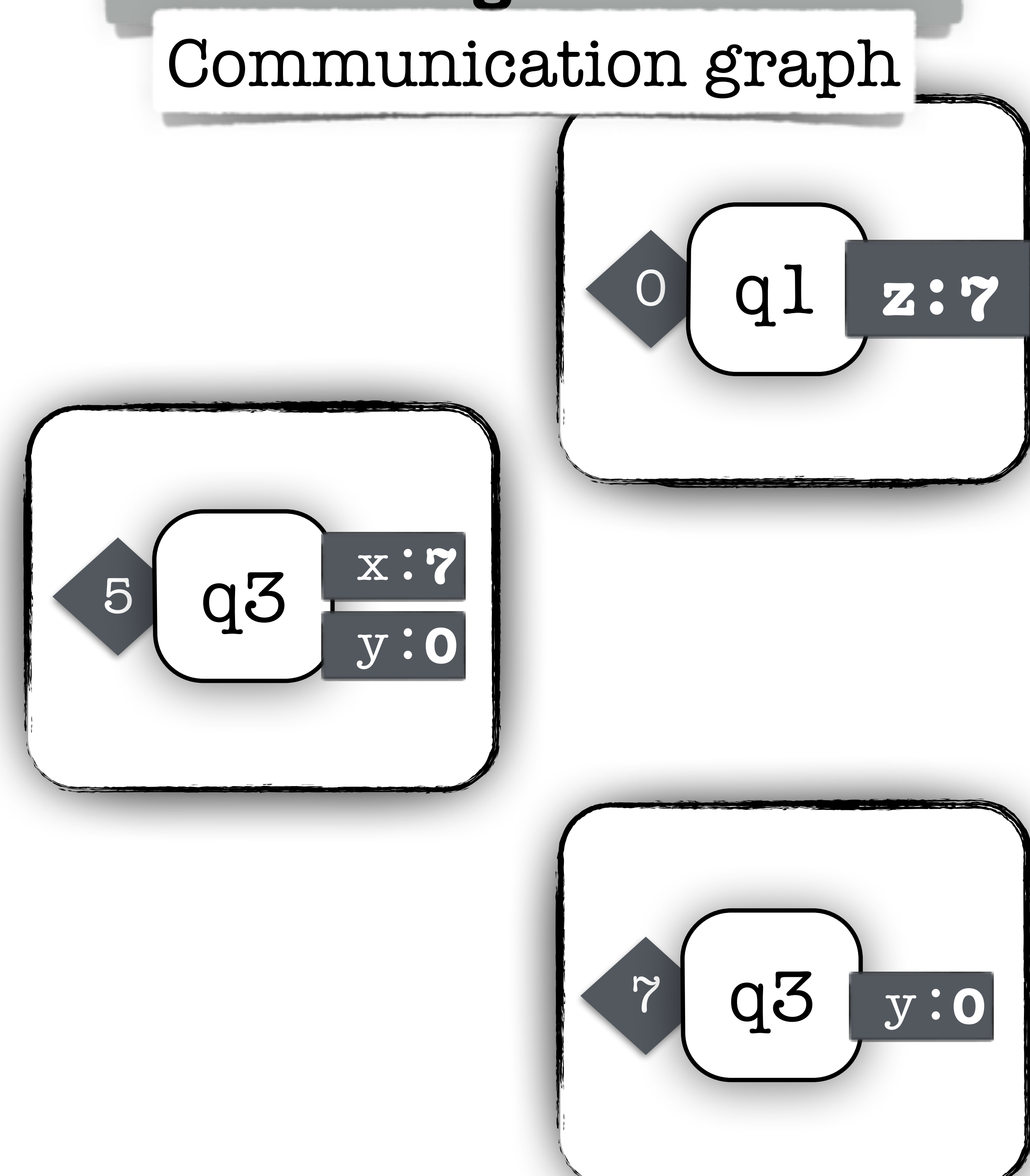
Process Model



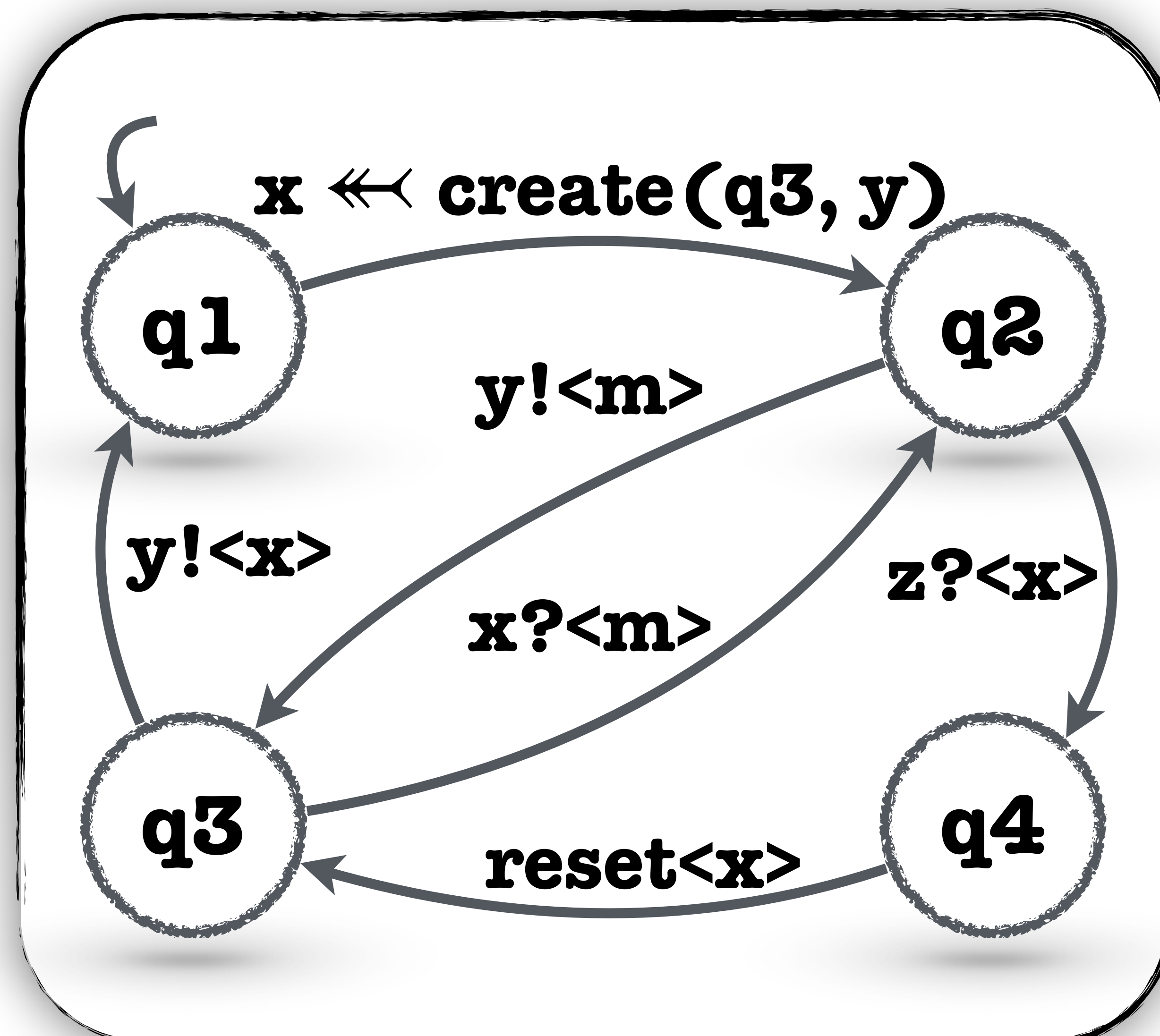
Dynamic Register Automata

Formal Model

Configuration



Process Model

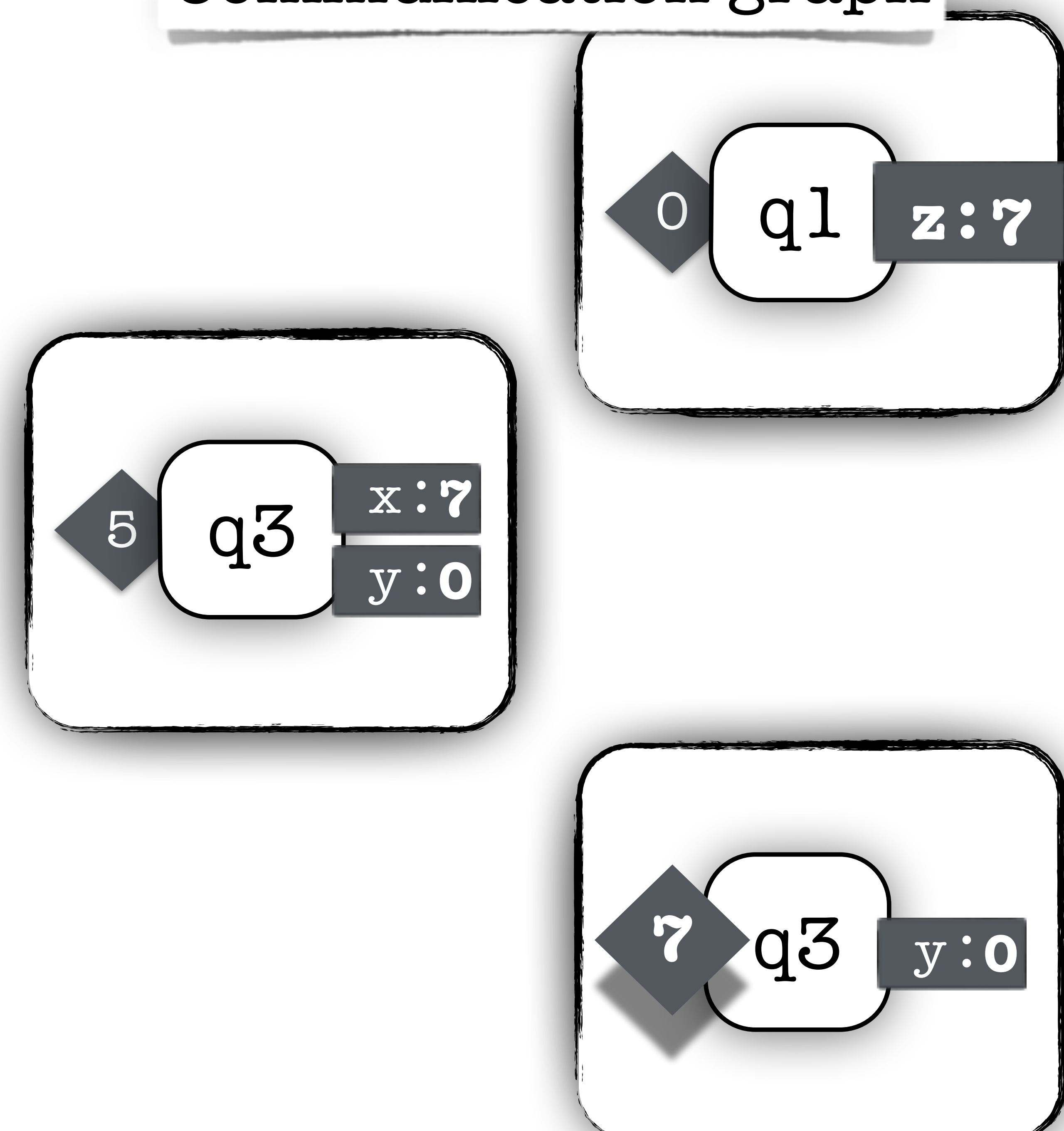


Dynamic Register Automata

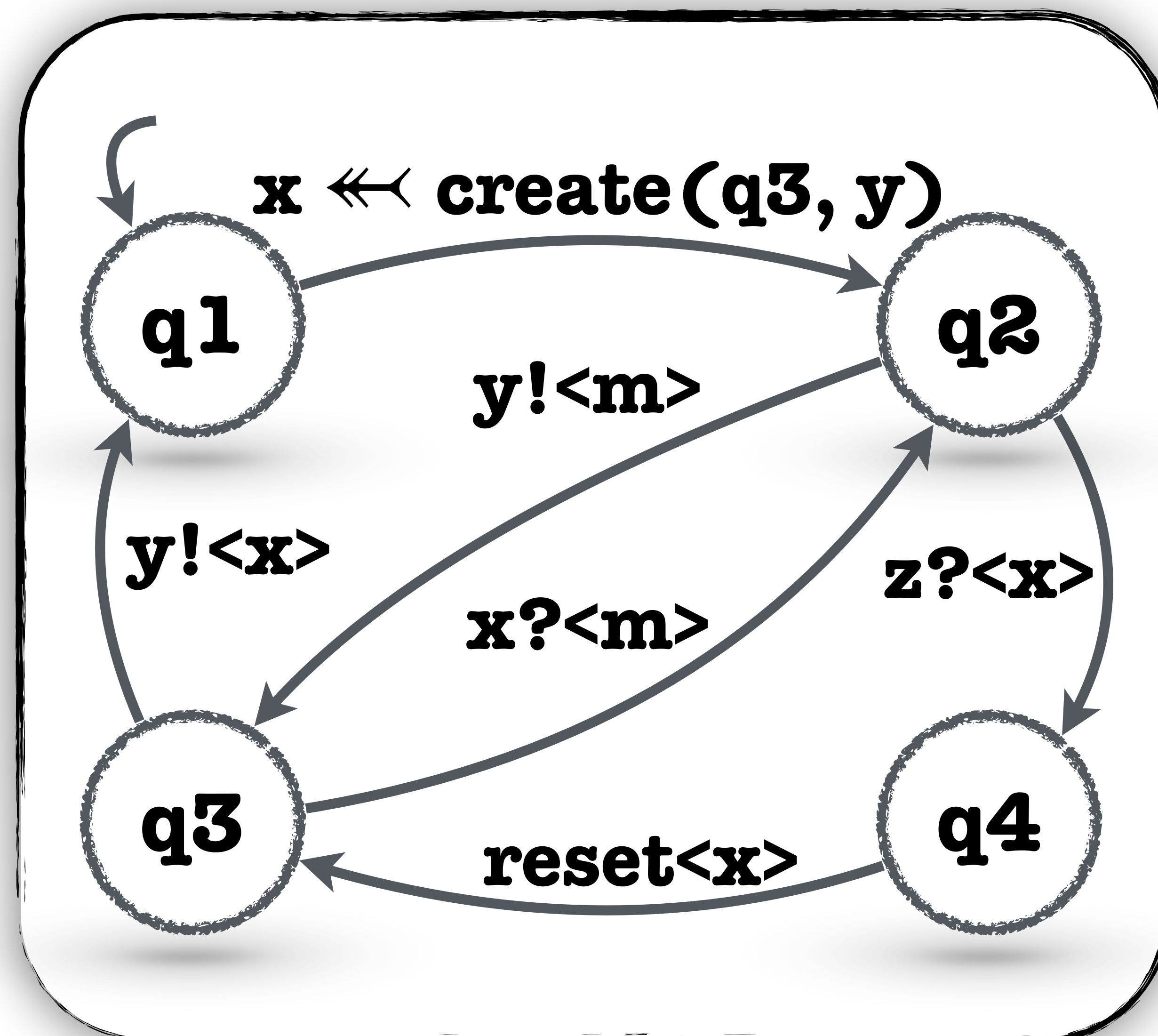
Formal Model

Configuration

Communication graph



Process Model

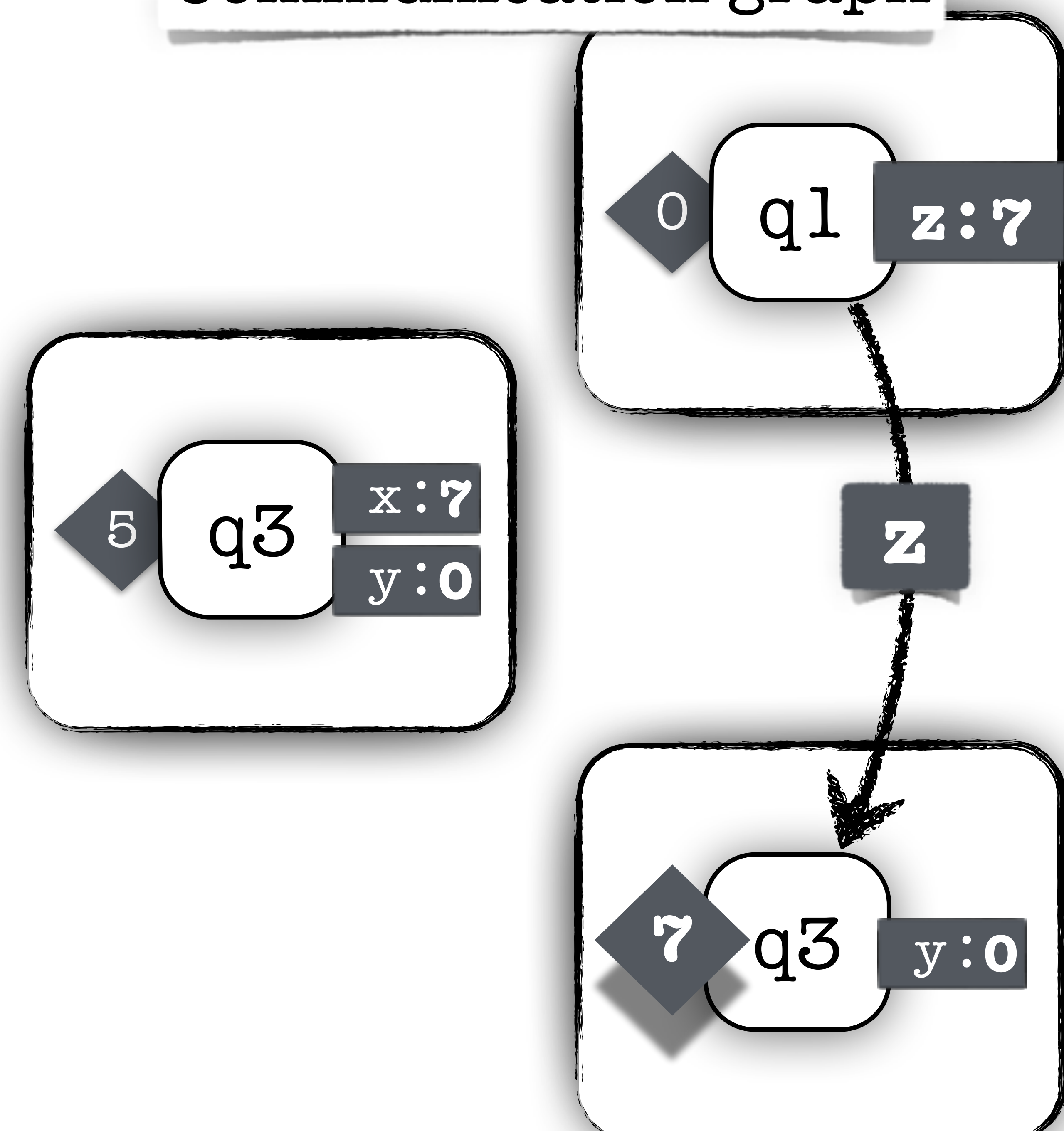


Dynamic Register Automata

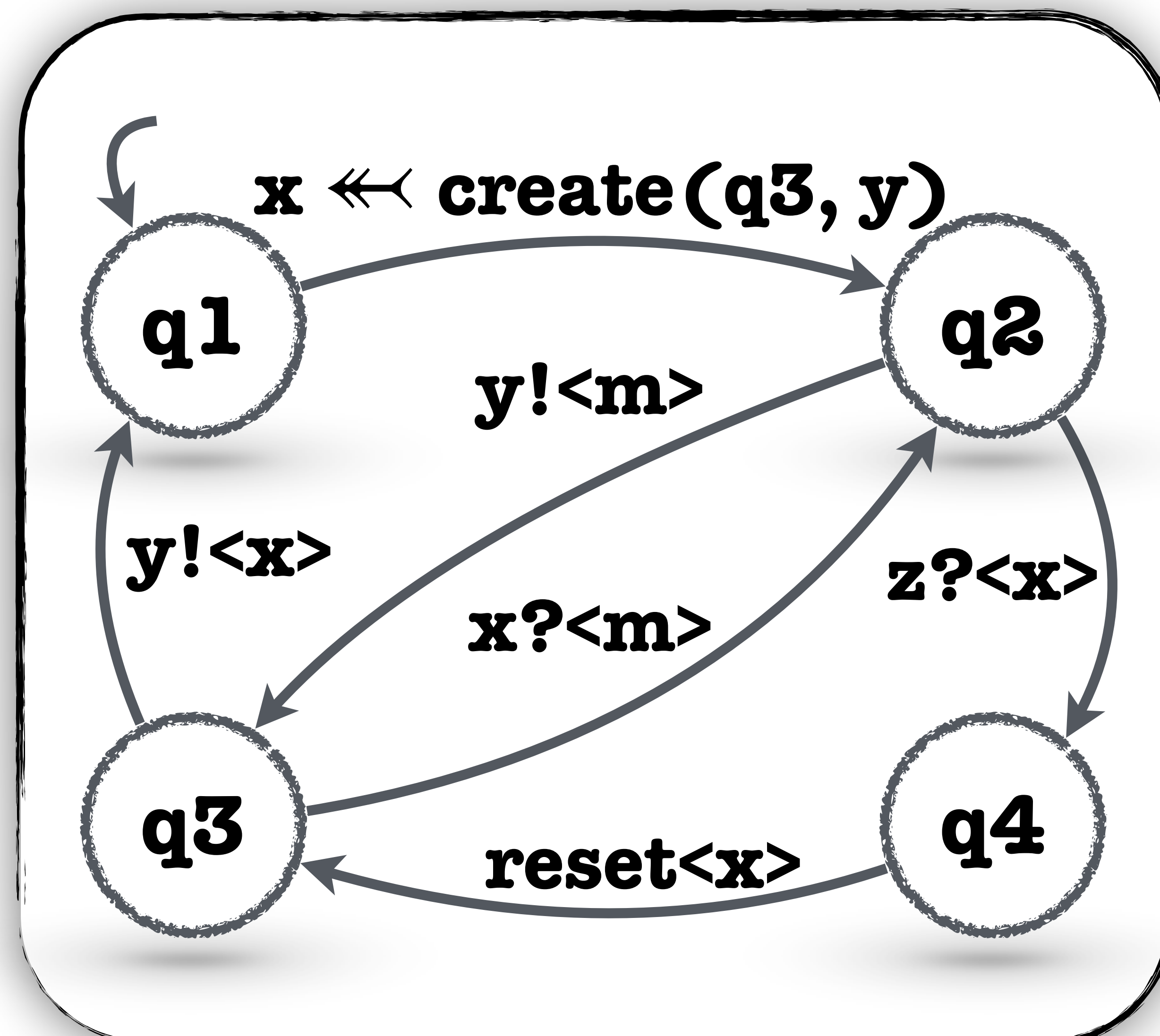
Formal Model

Configuration

Communication graph



Process Model

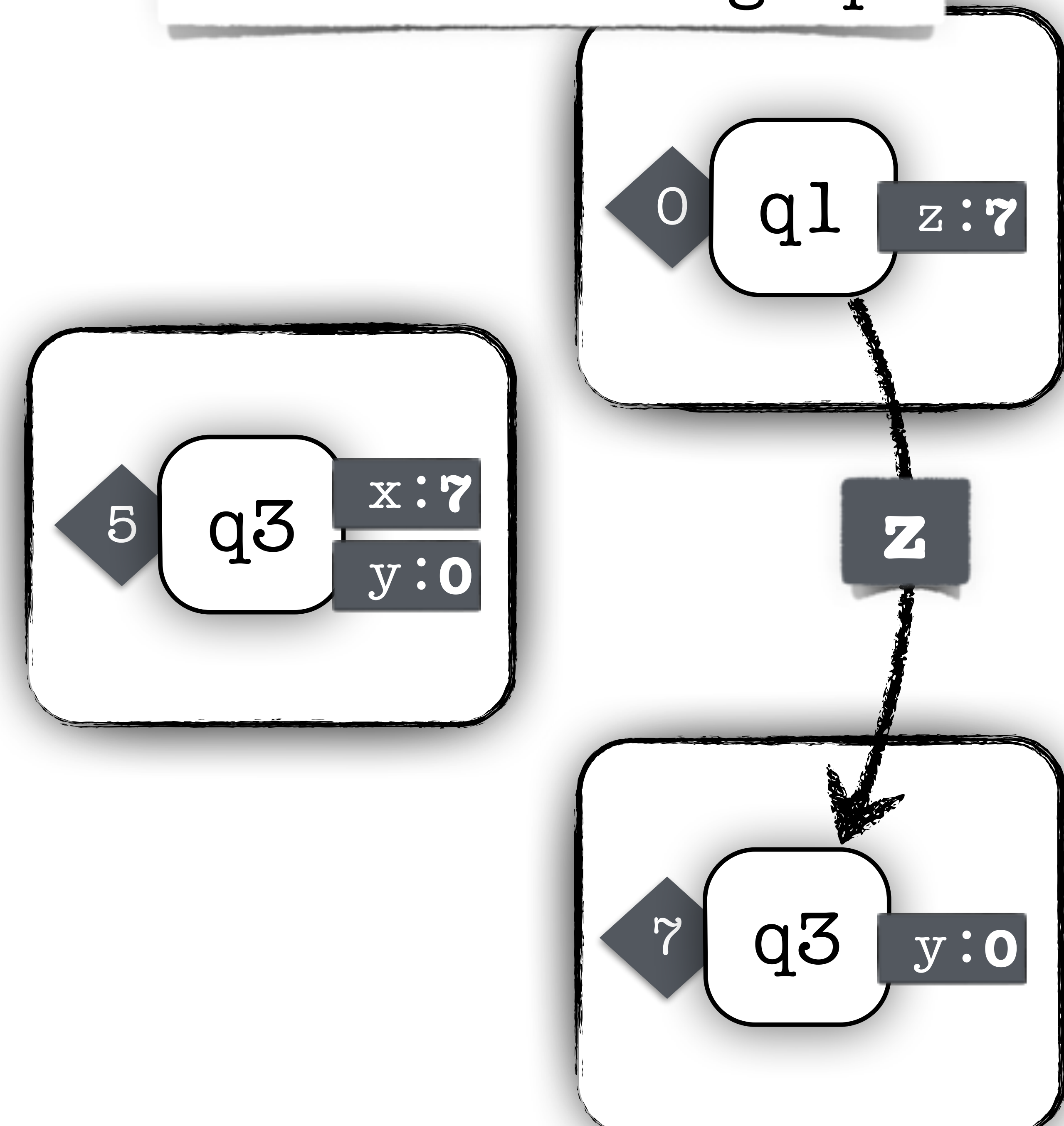


Dynamic Register Automata

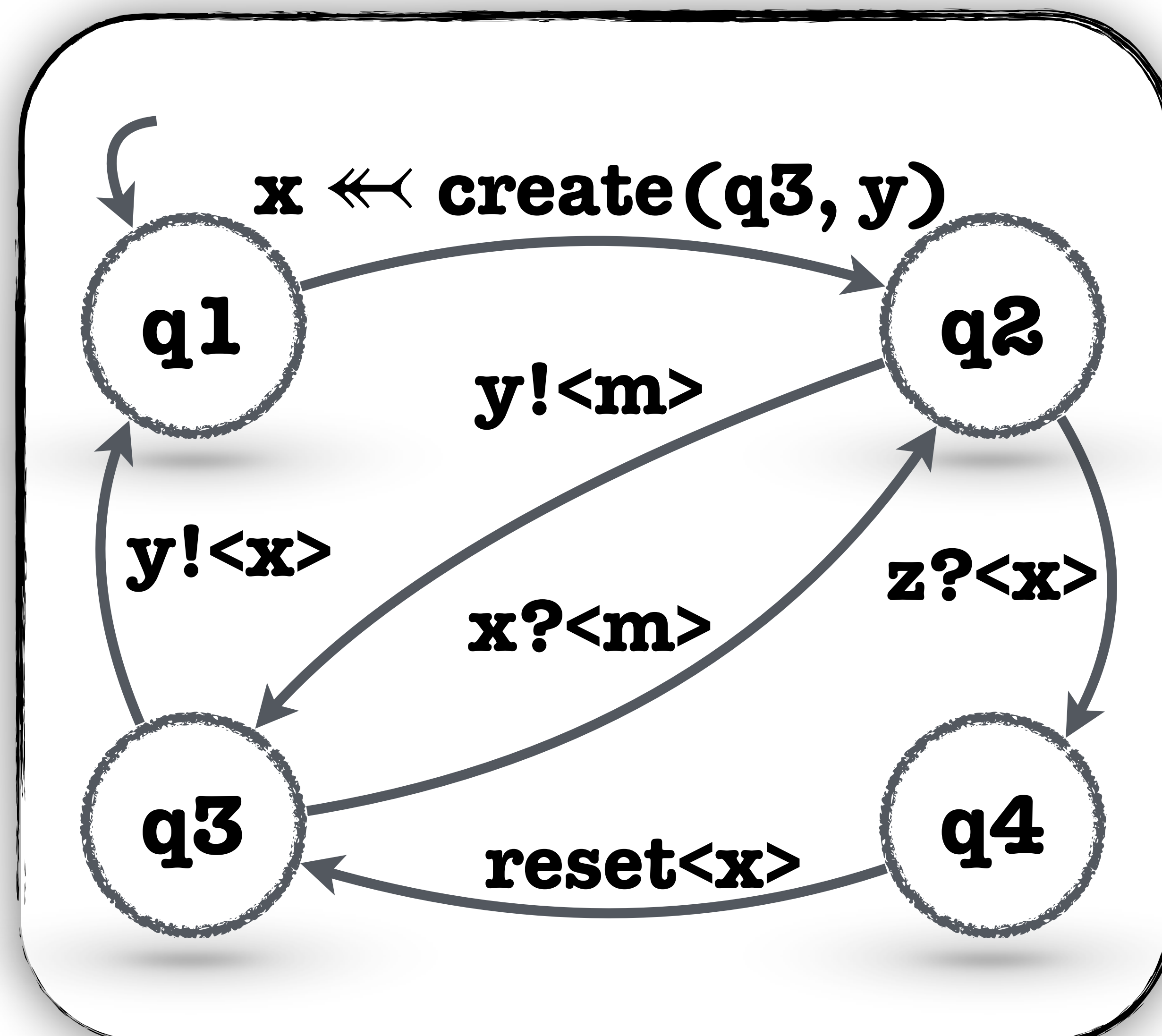
Formal Model

Configuration

Communication graph



Process Model

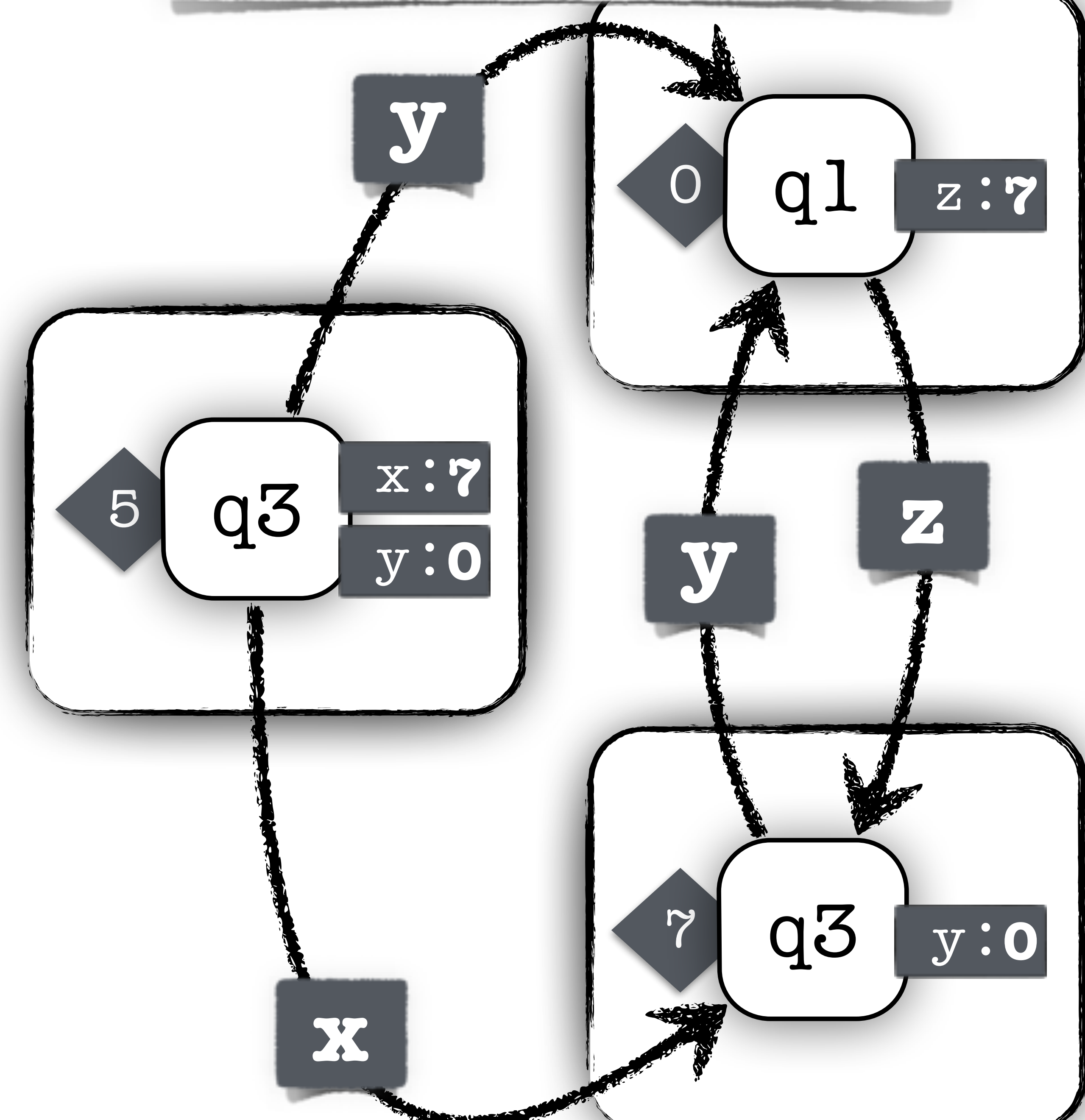


Dynamic Register Automata

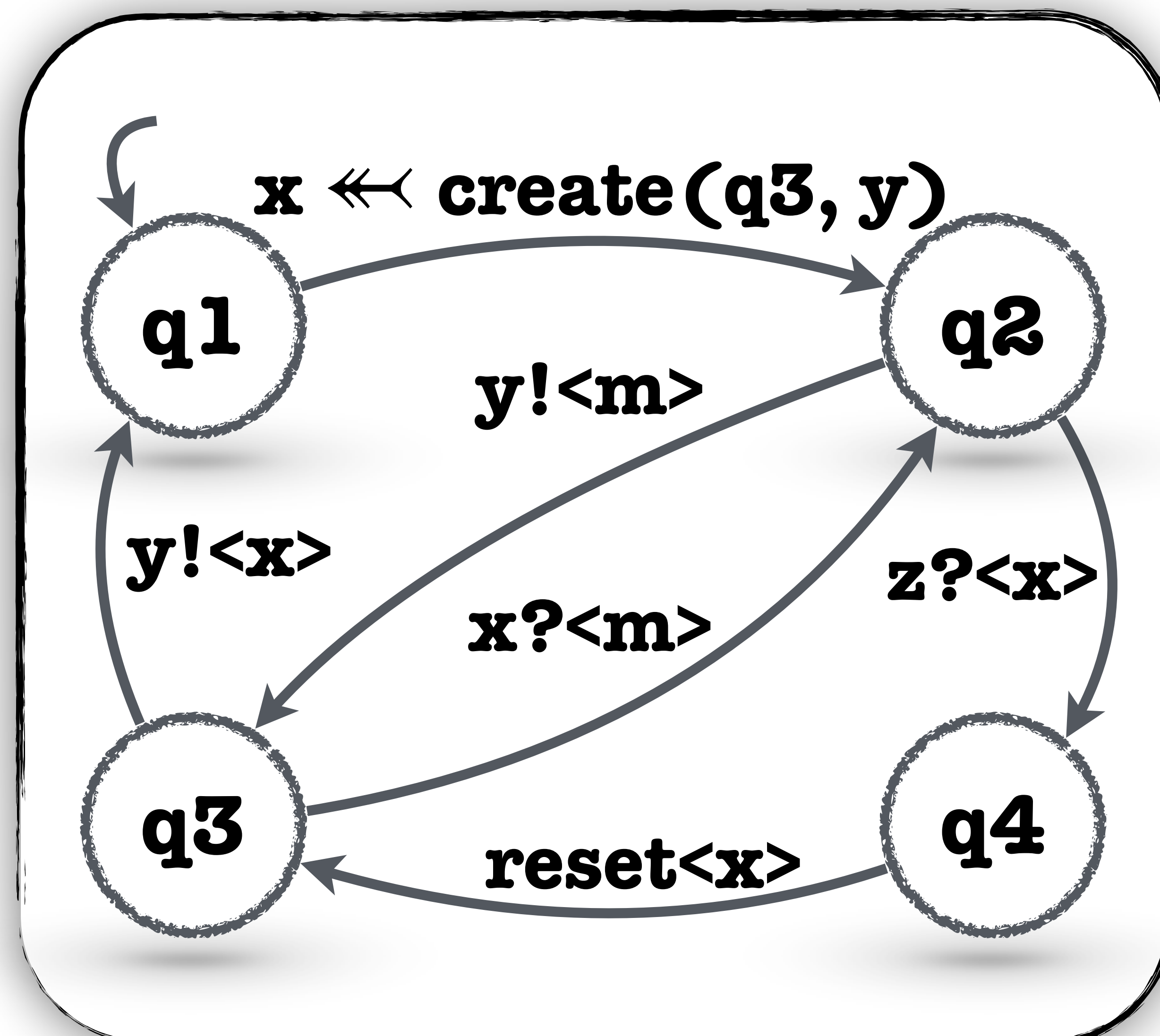
Formal Model

Configuration

Communication graph



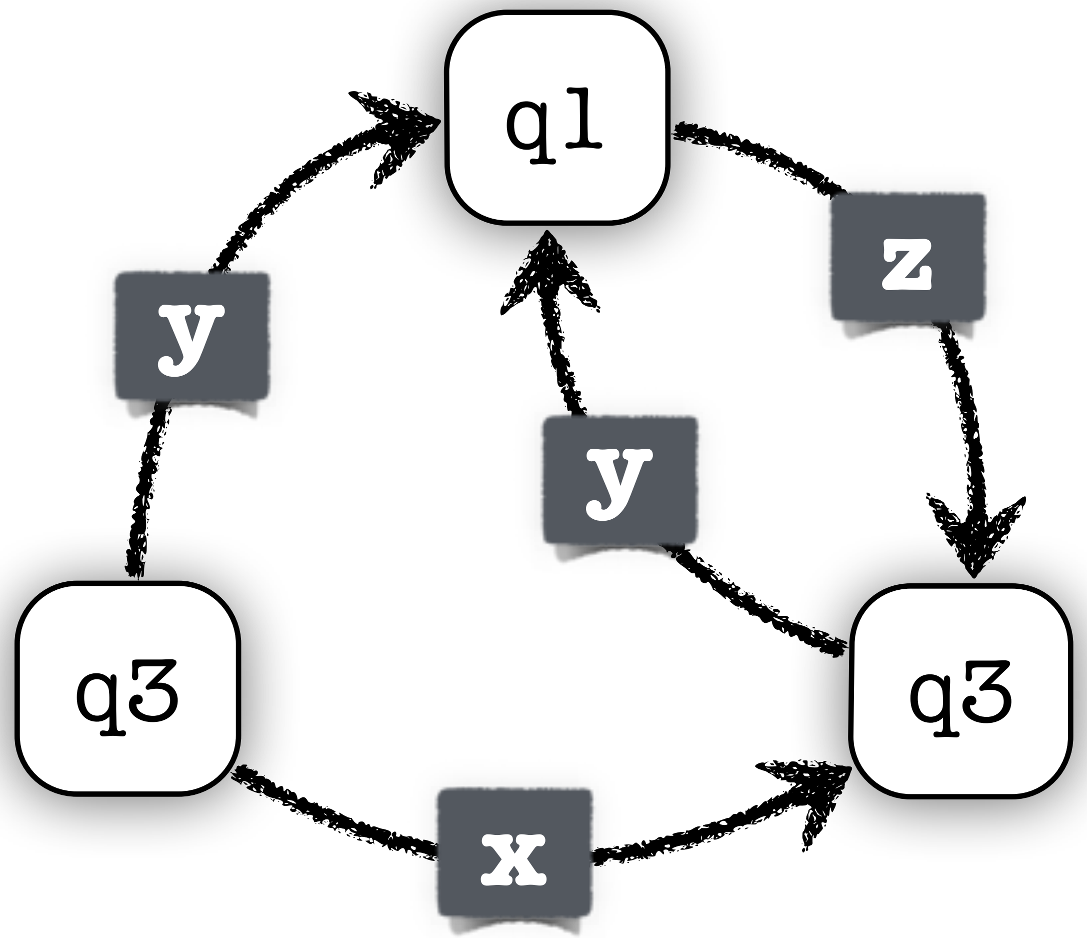
Process Model



Dynamic Register Automata

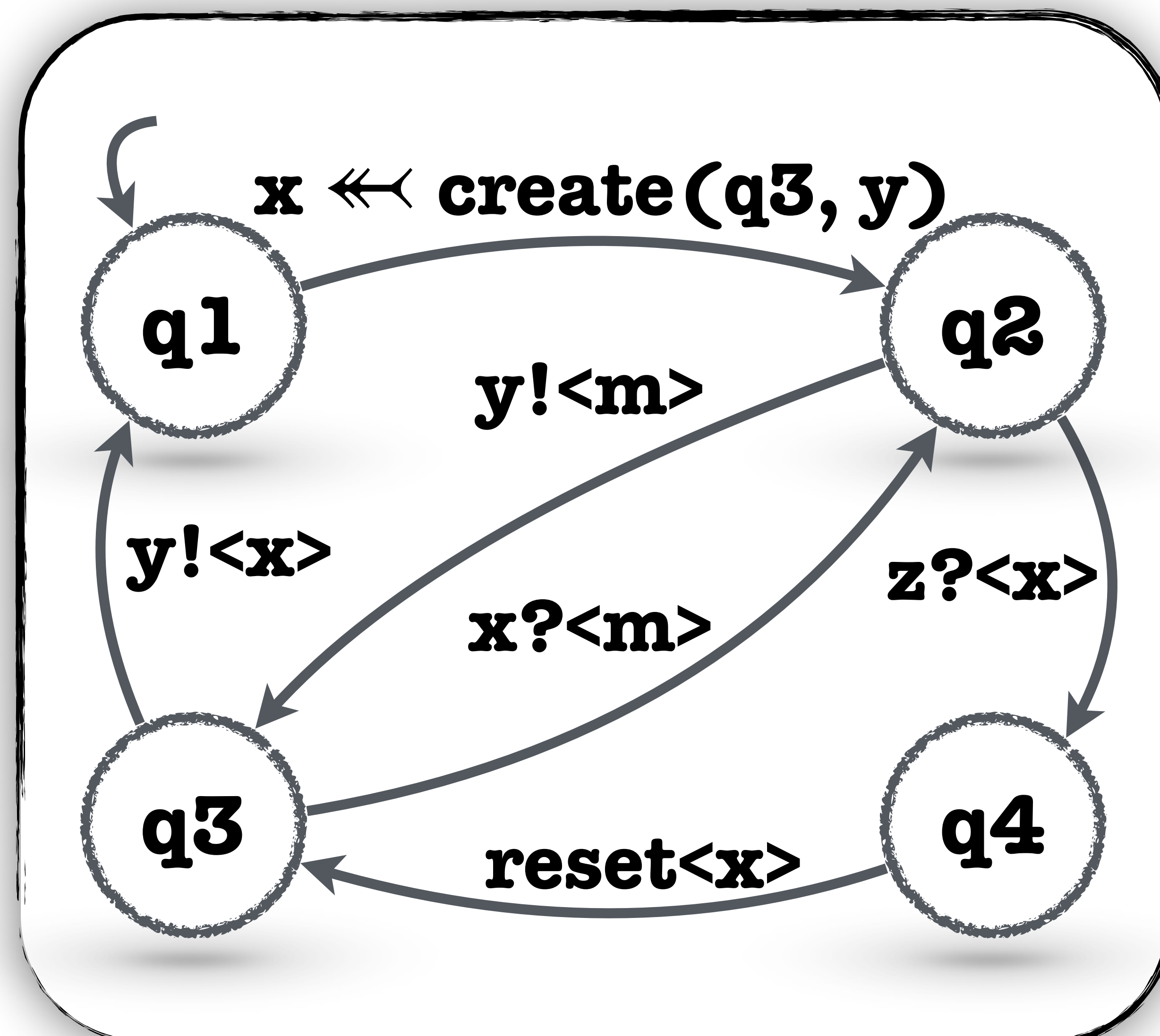
Formal Model

Configuration



Communication graph

Process Model

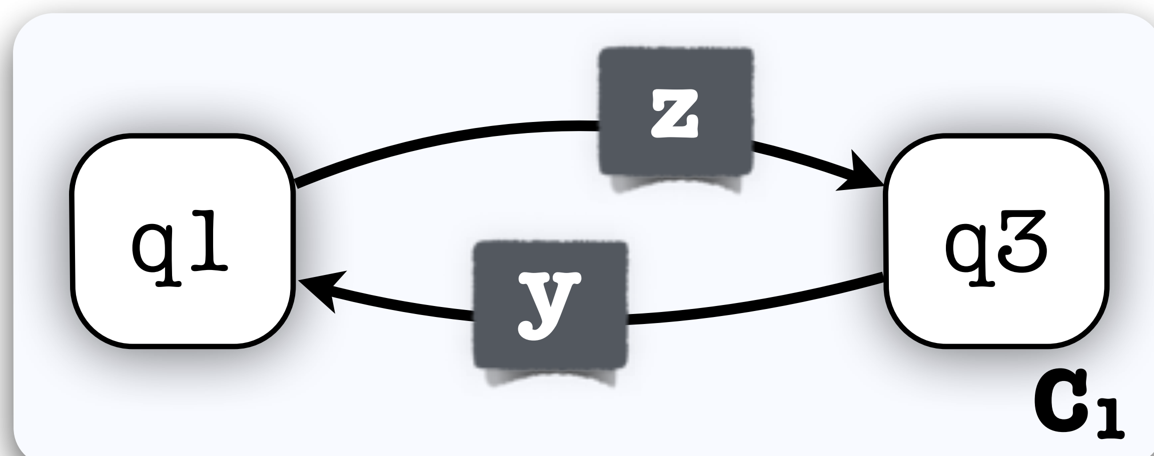


Dynamic Register Automata

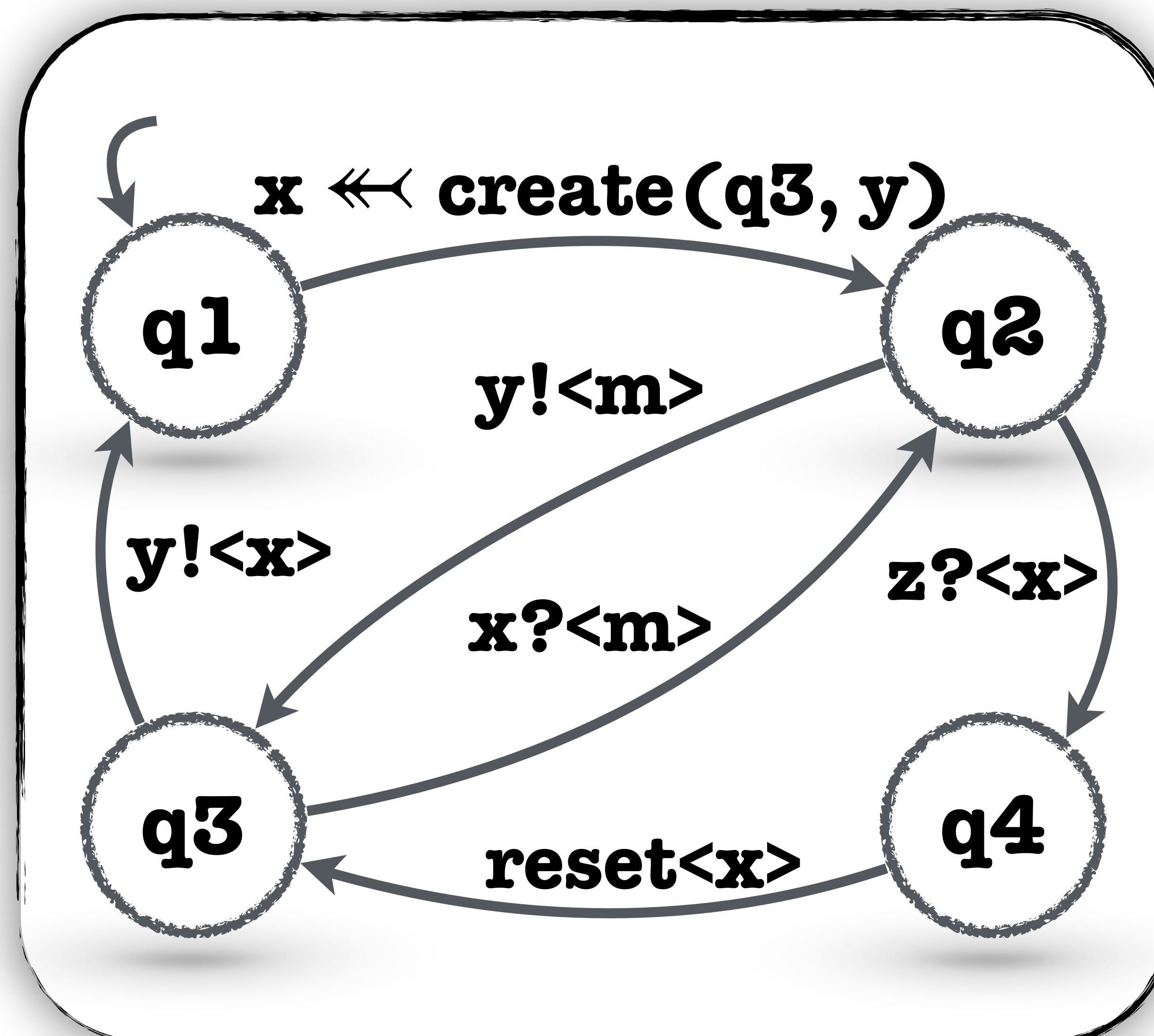
Formal Model

Configuration

Transition Relation



Process Model



Dynamic Register Automata

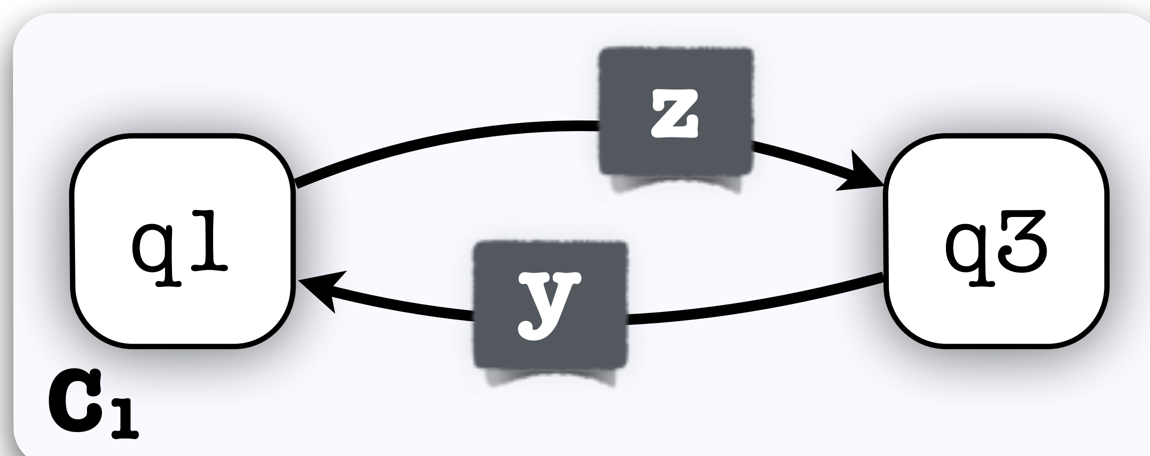
Formal Model

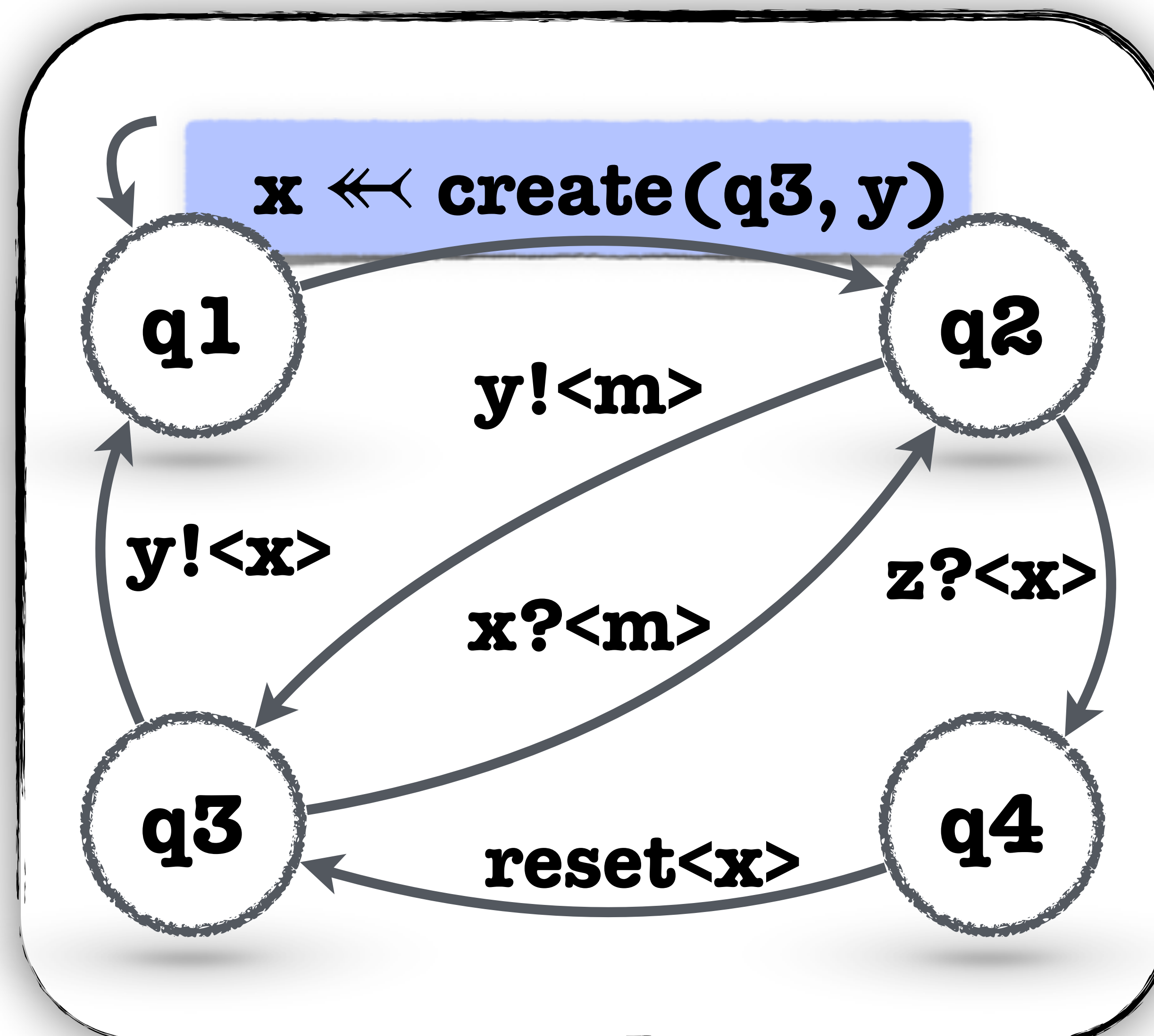
Configuration

Transition Relation

Process Creation

Process Model





Dynamic Register Automata

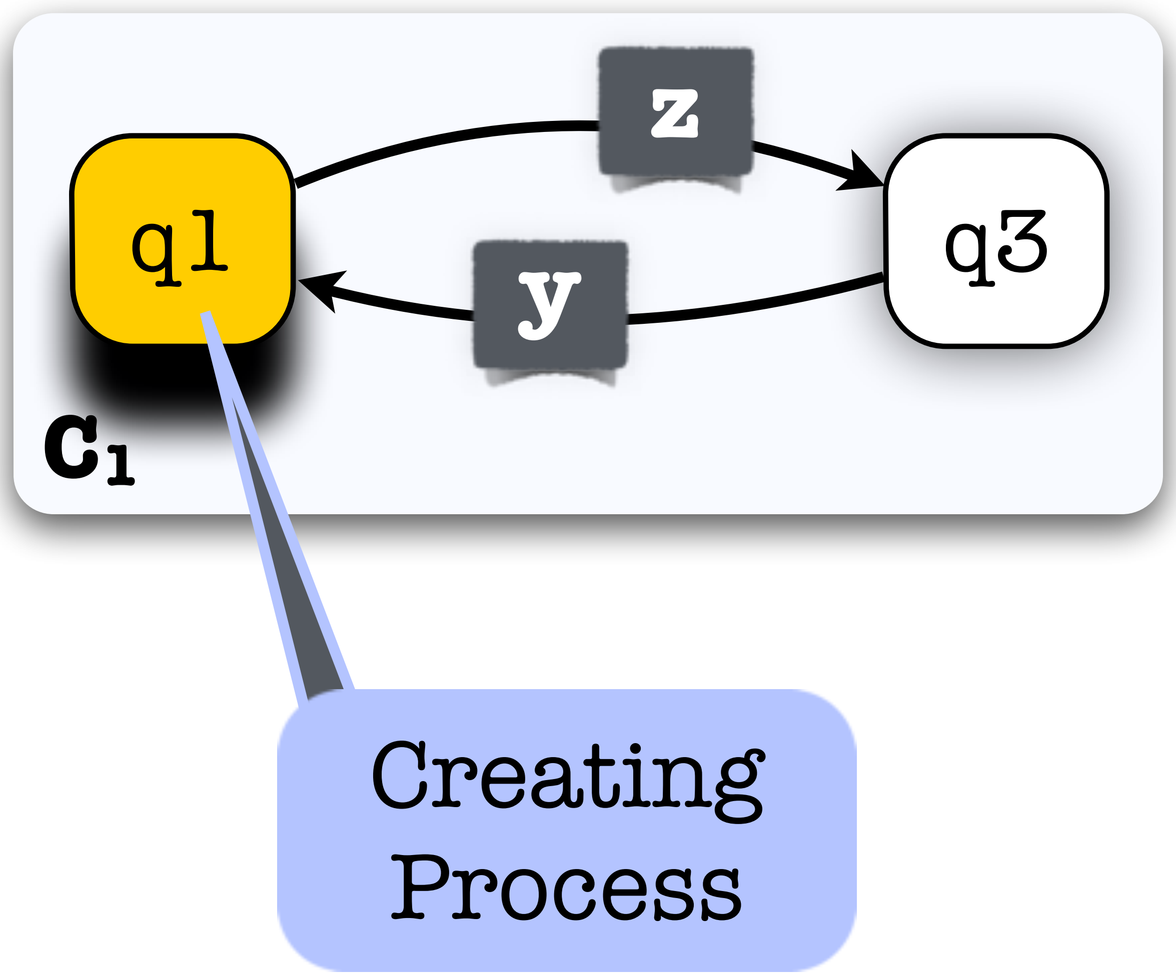
Formal Model

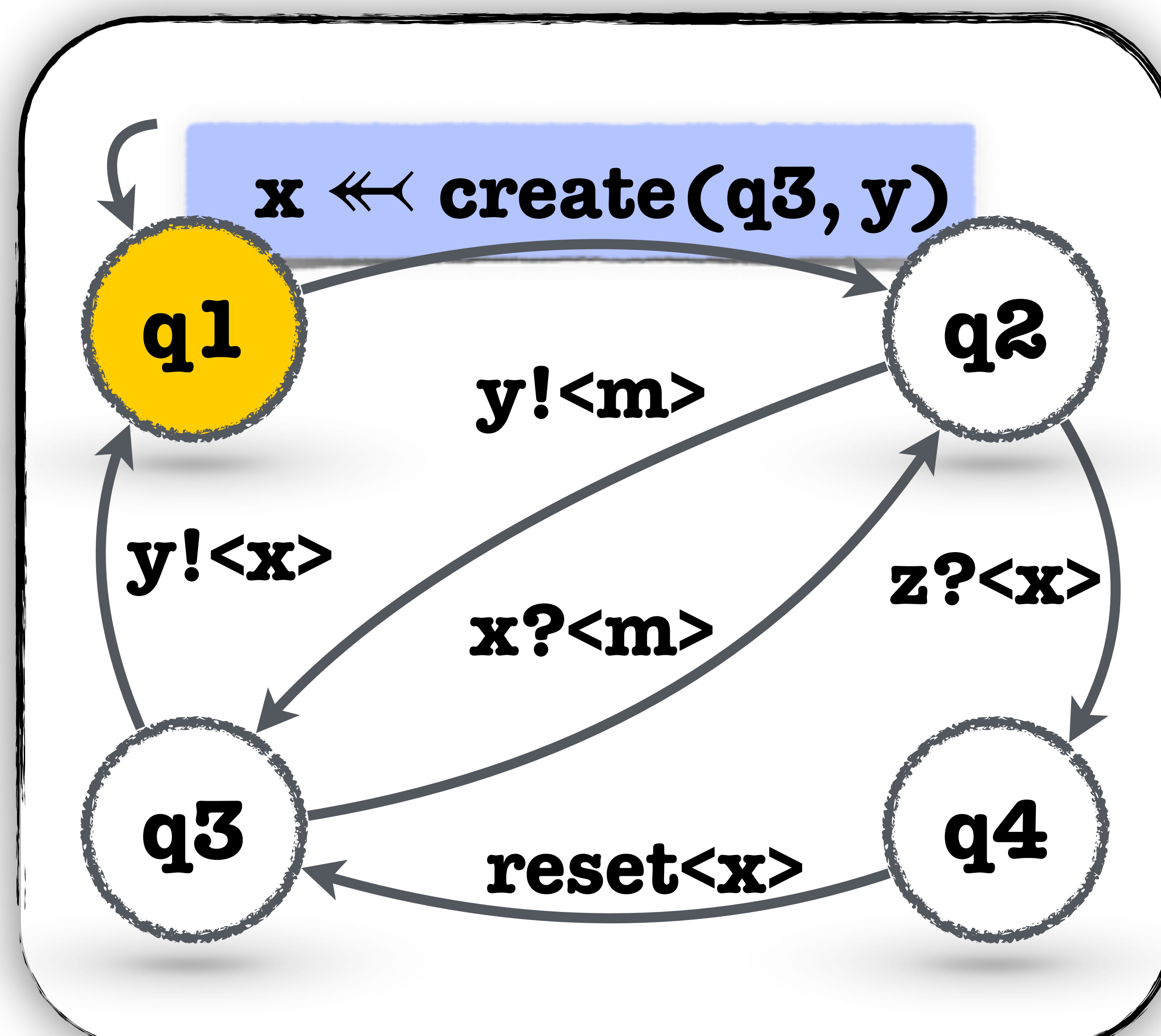
Configuration

Transition Relation

Process Creation

Process Model





Dynamic Register Automata

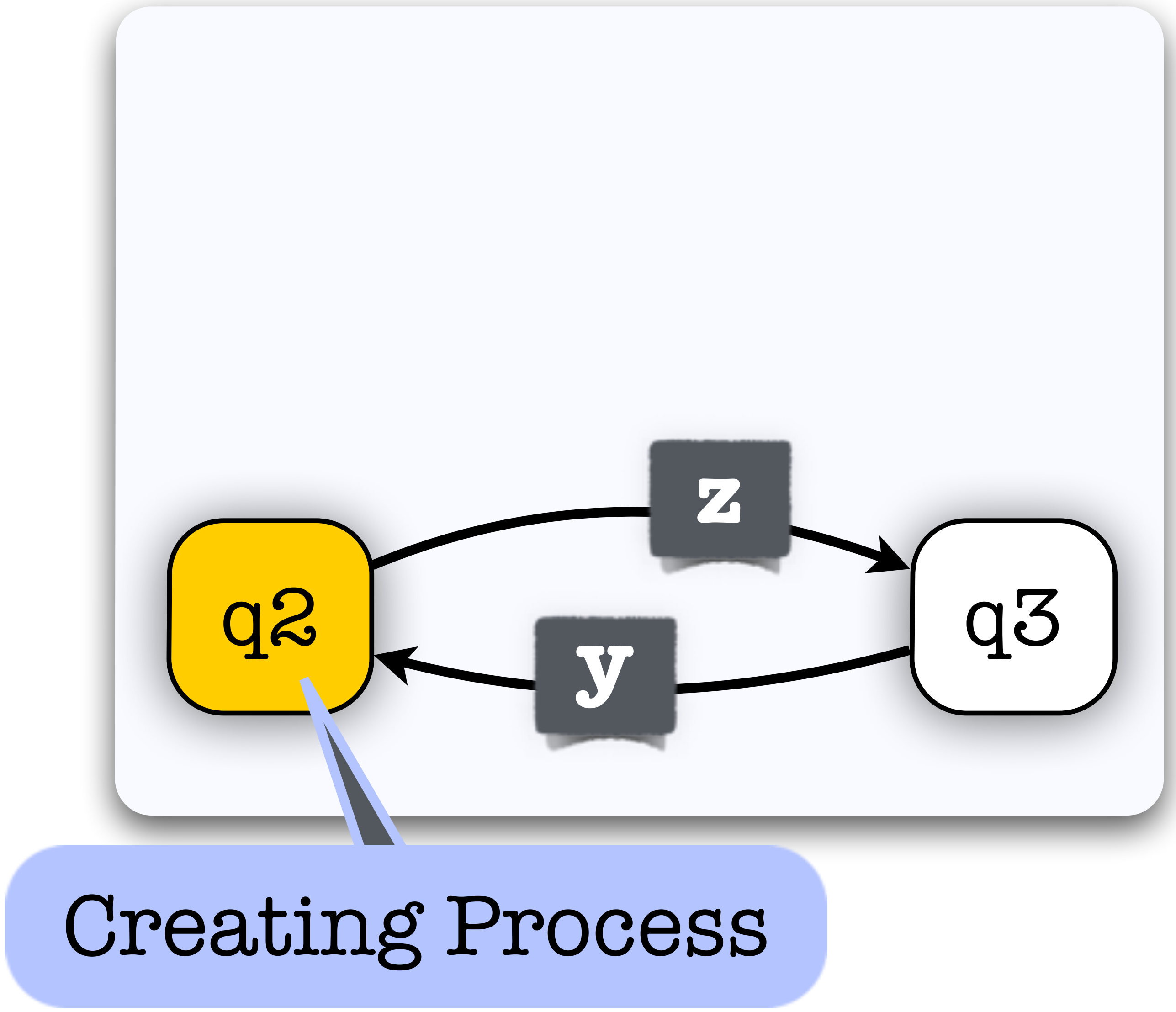
Formal Model

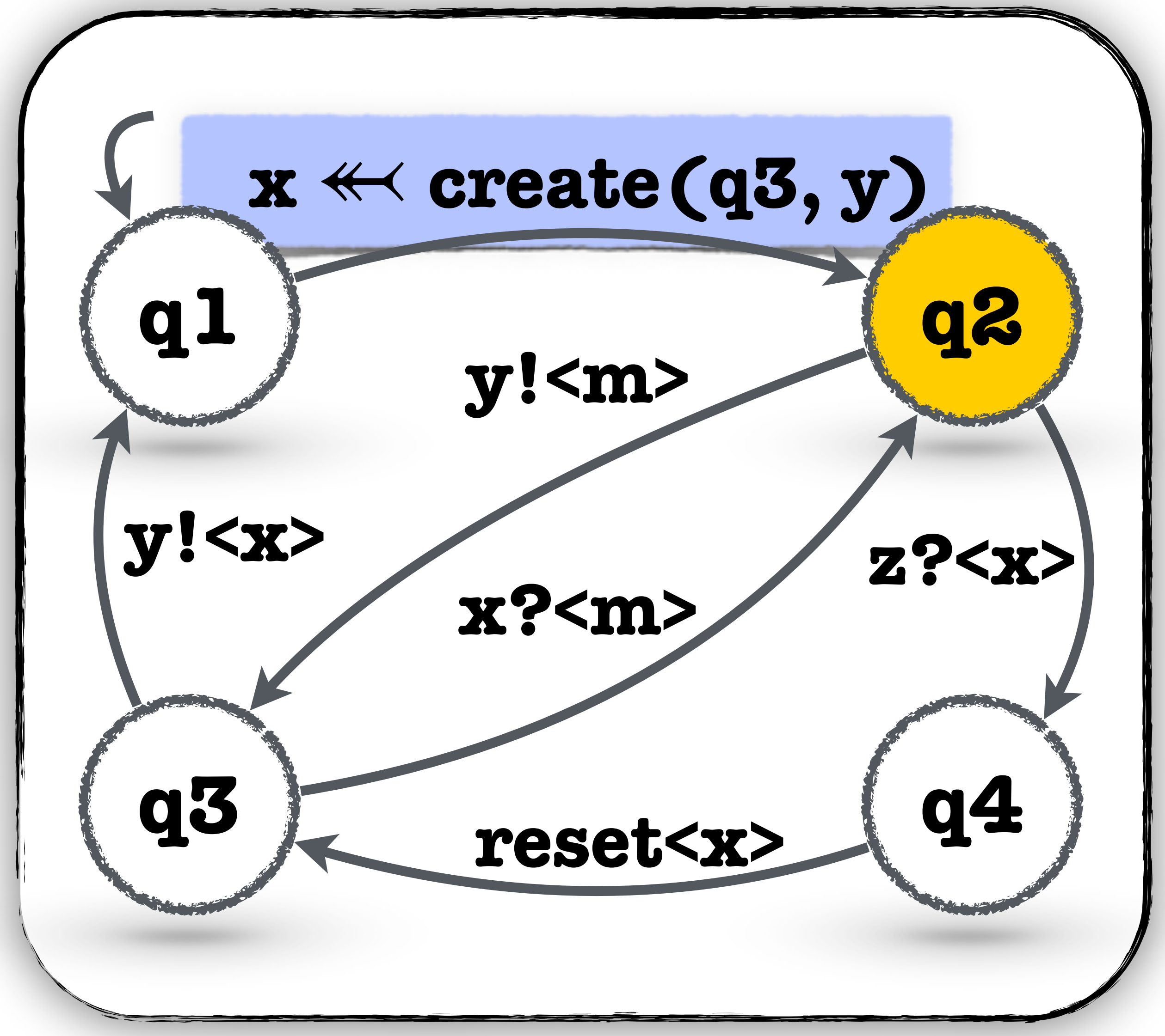
Configuration

Transition Relation

Process Model

Process Creation





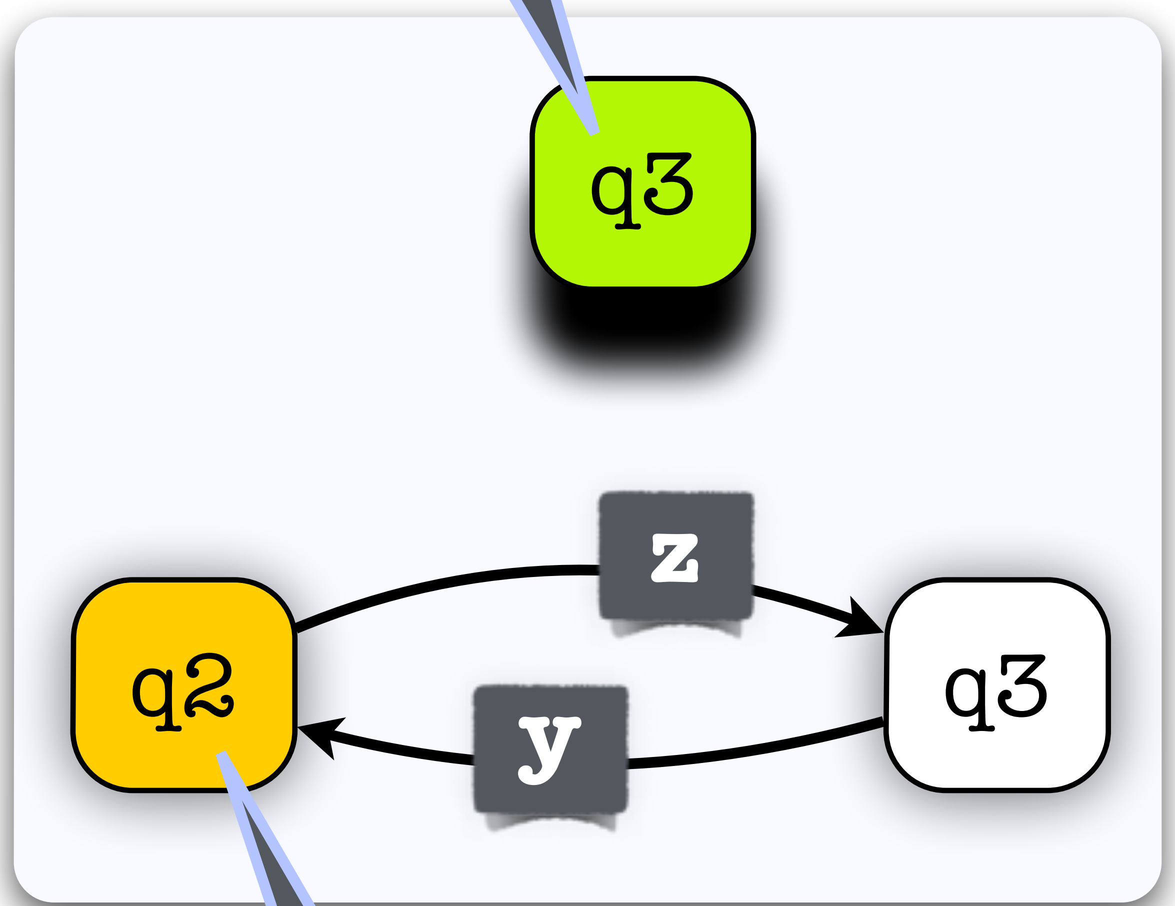
Dynamic Register Automata

Formal Model

Configuration

Transition Relation

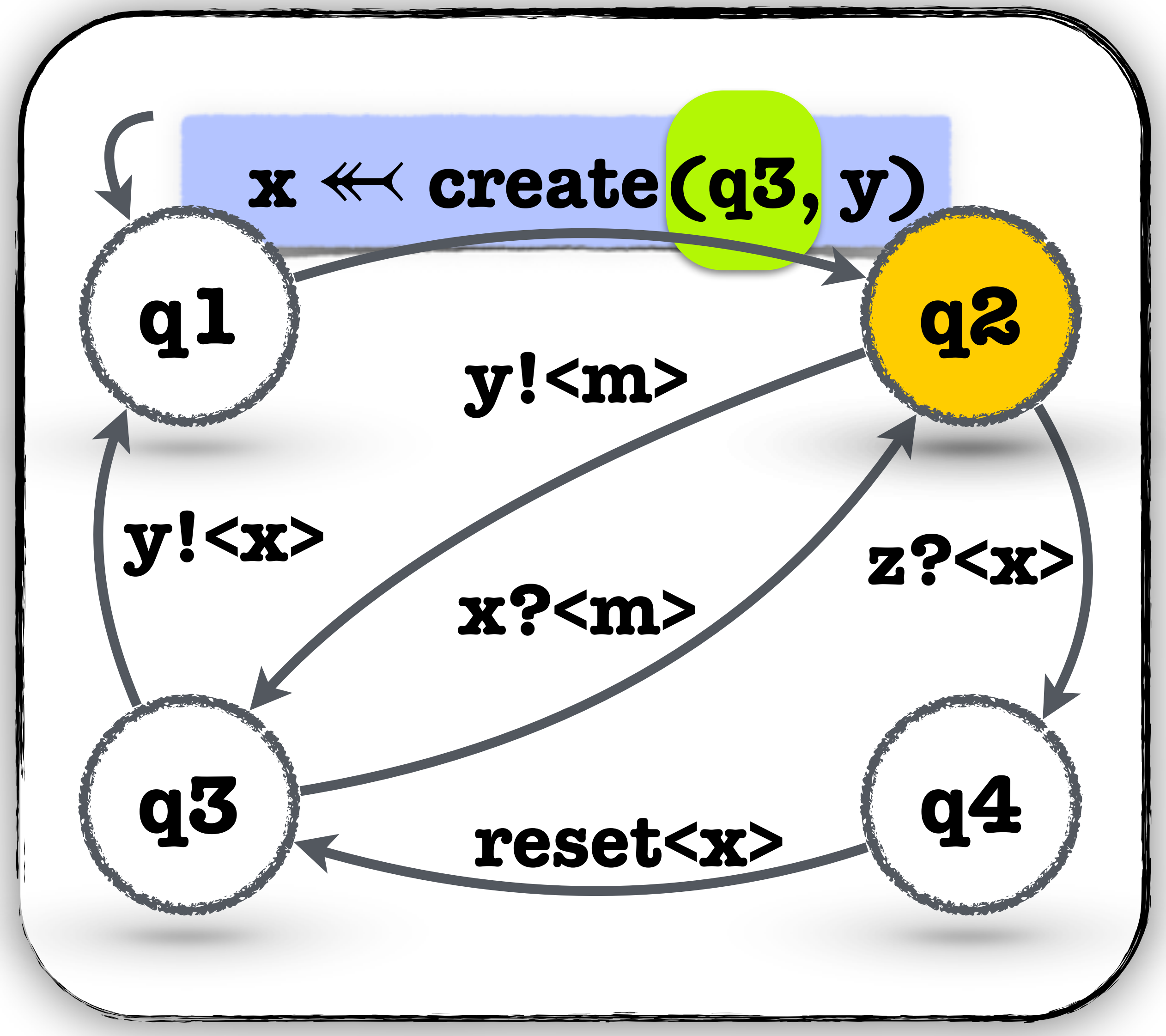
Created Process



Creating Process

Process Model

Process Creation



Dynamic Register Automata

Formal Model

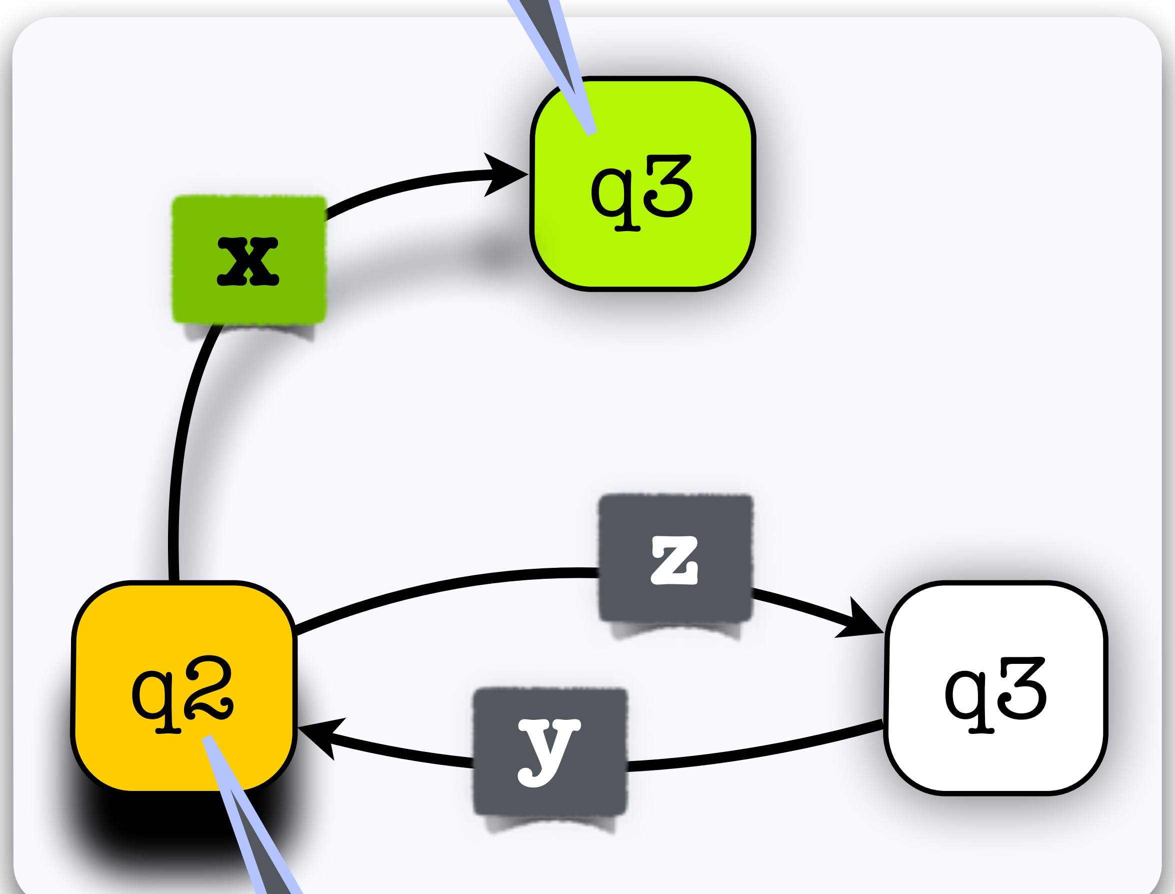
Configuration

Transition Relation

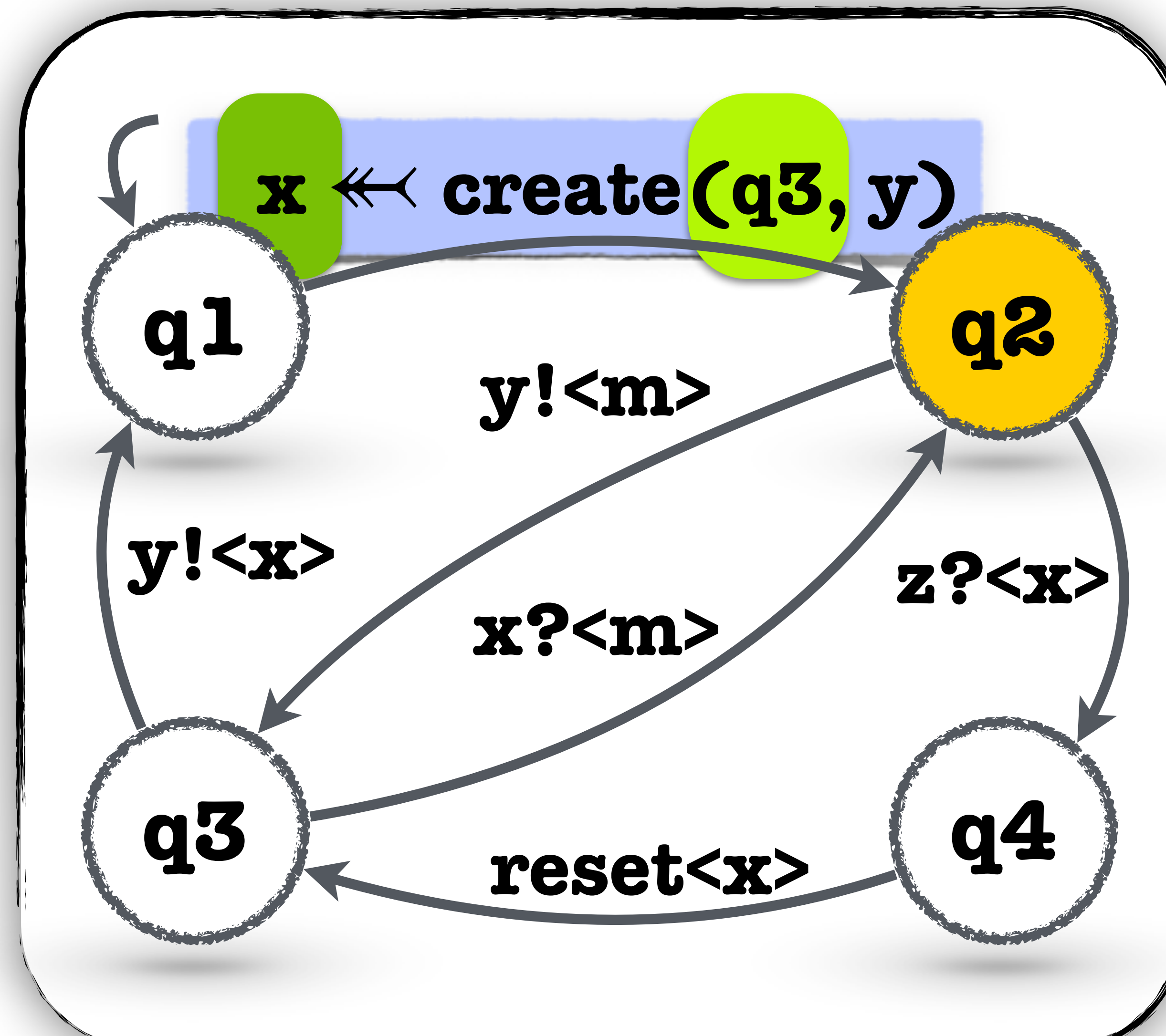
Process Model

Process Creation

Created Process



Creating Process

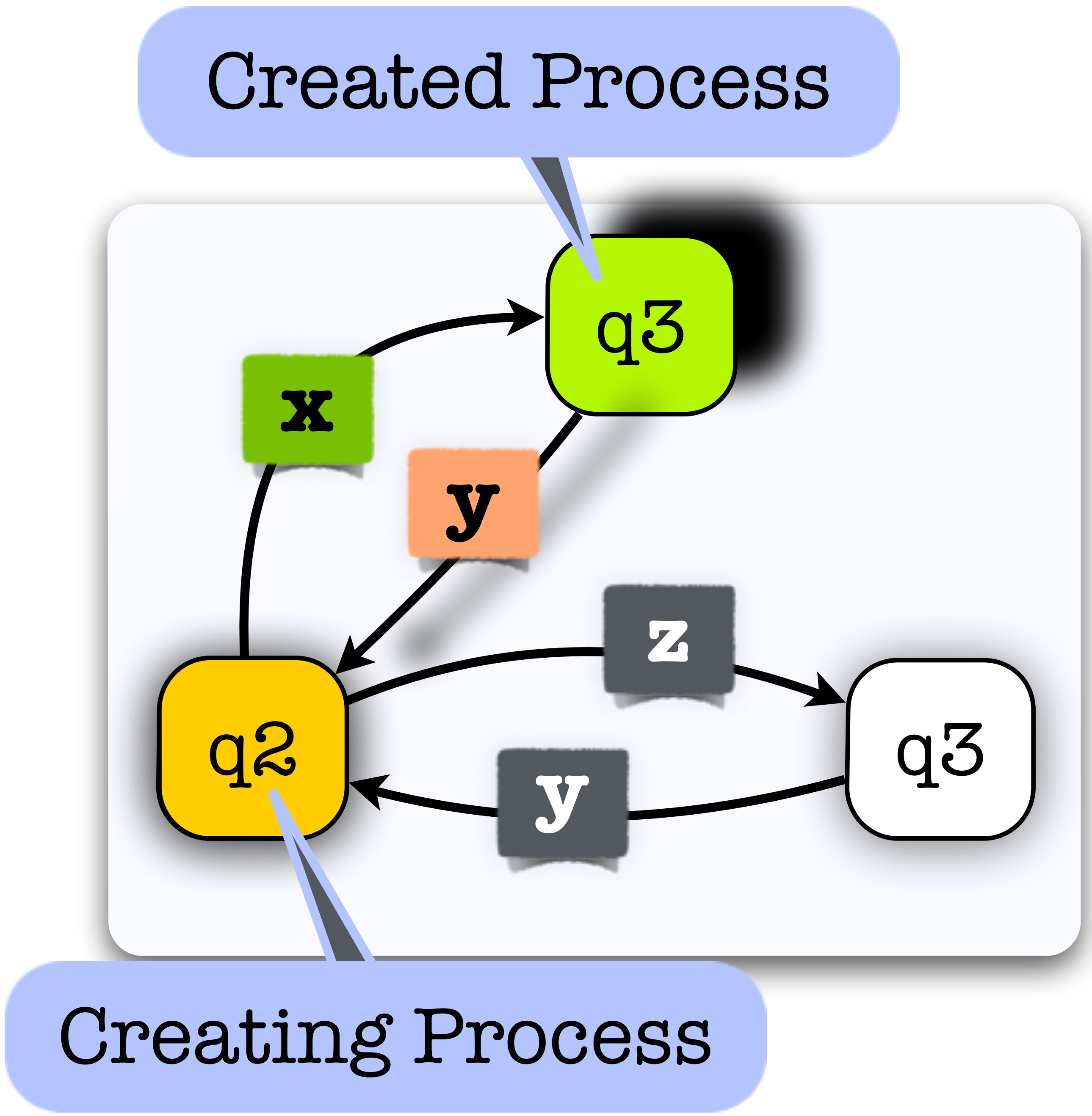


Dynamic Register Automata

Formal Model

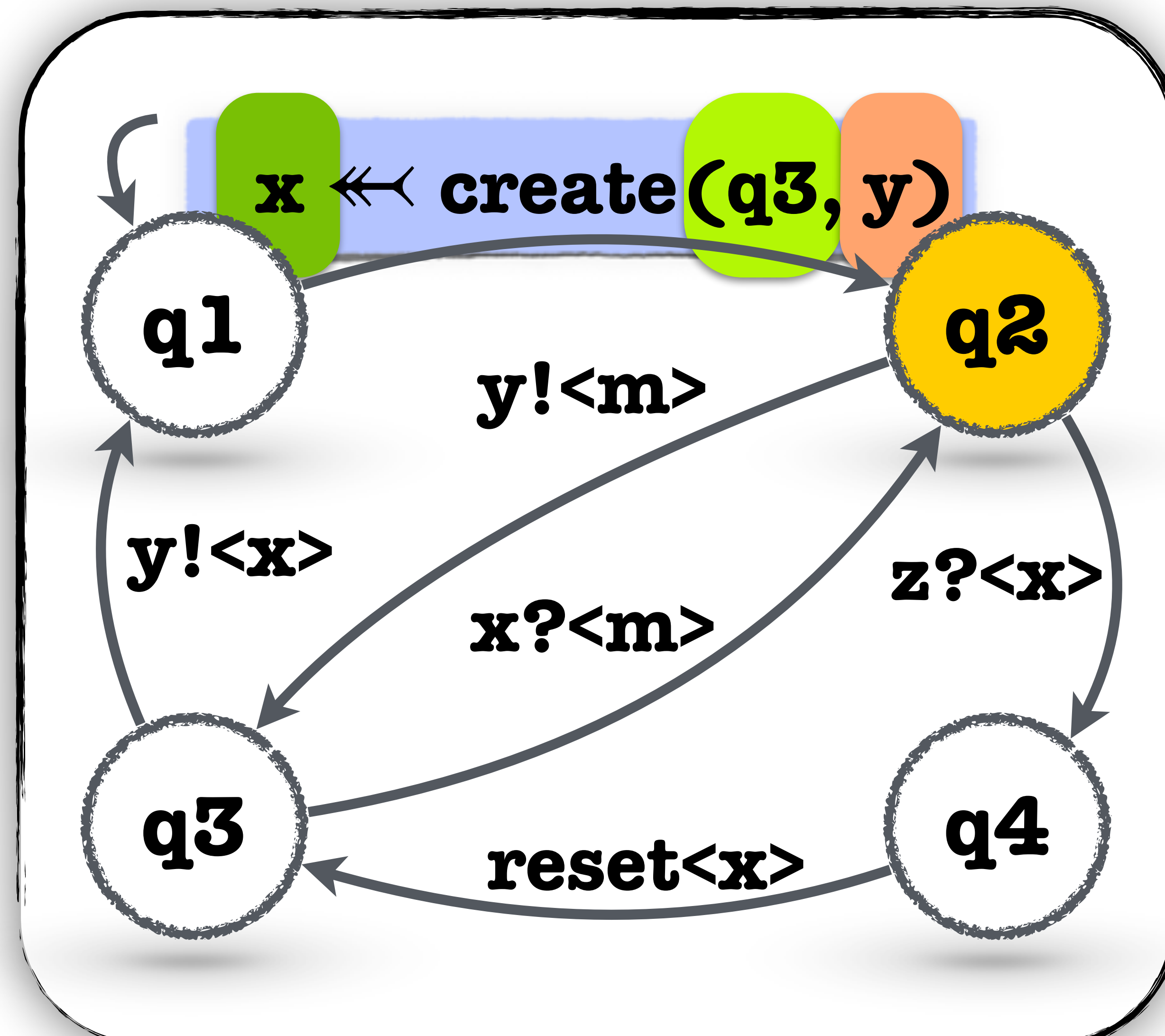
Configuration

Transition Relation



Process Model

Process Creation

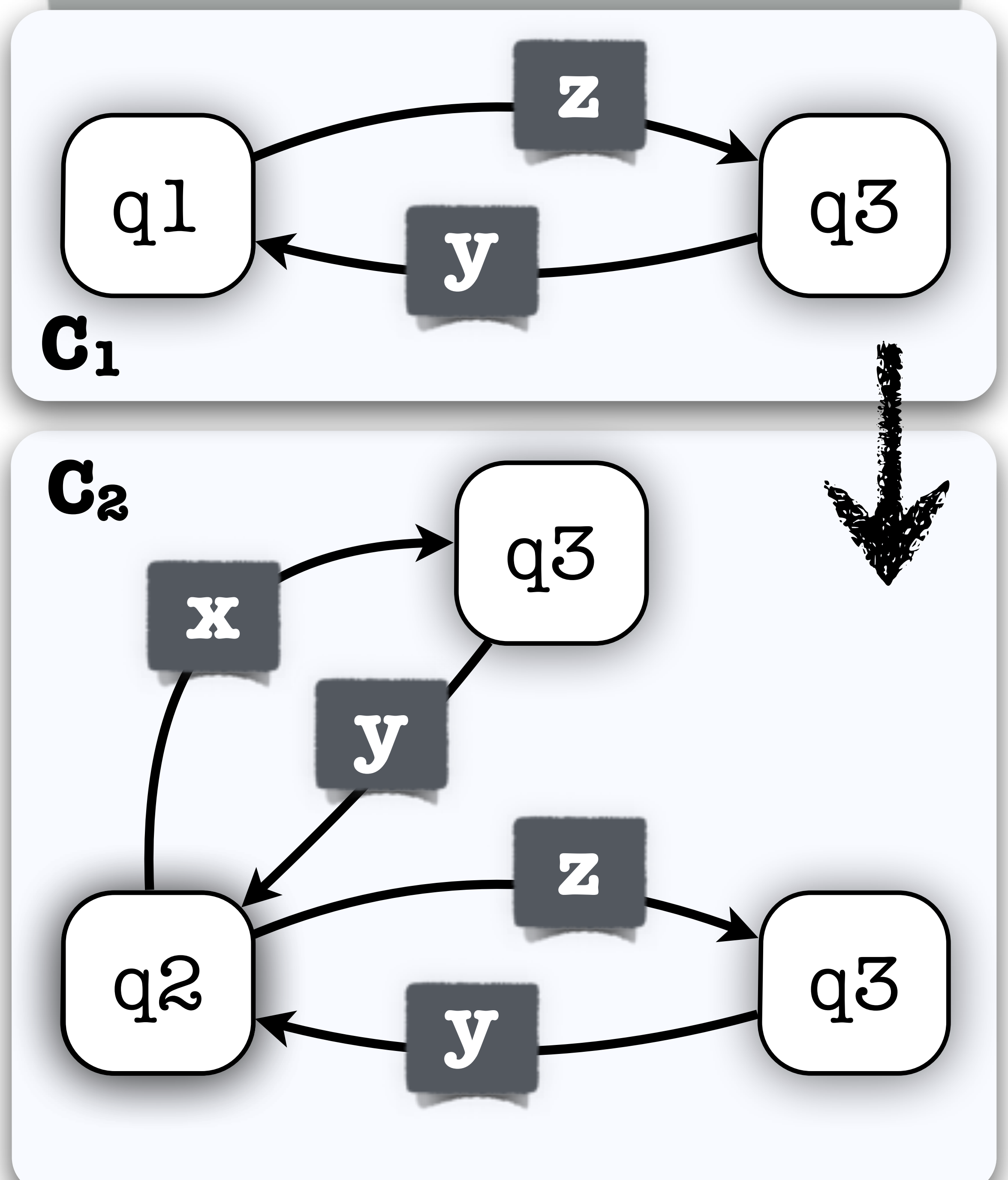


Dynamic Register Automata

Formal Model

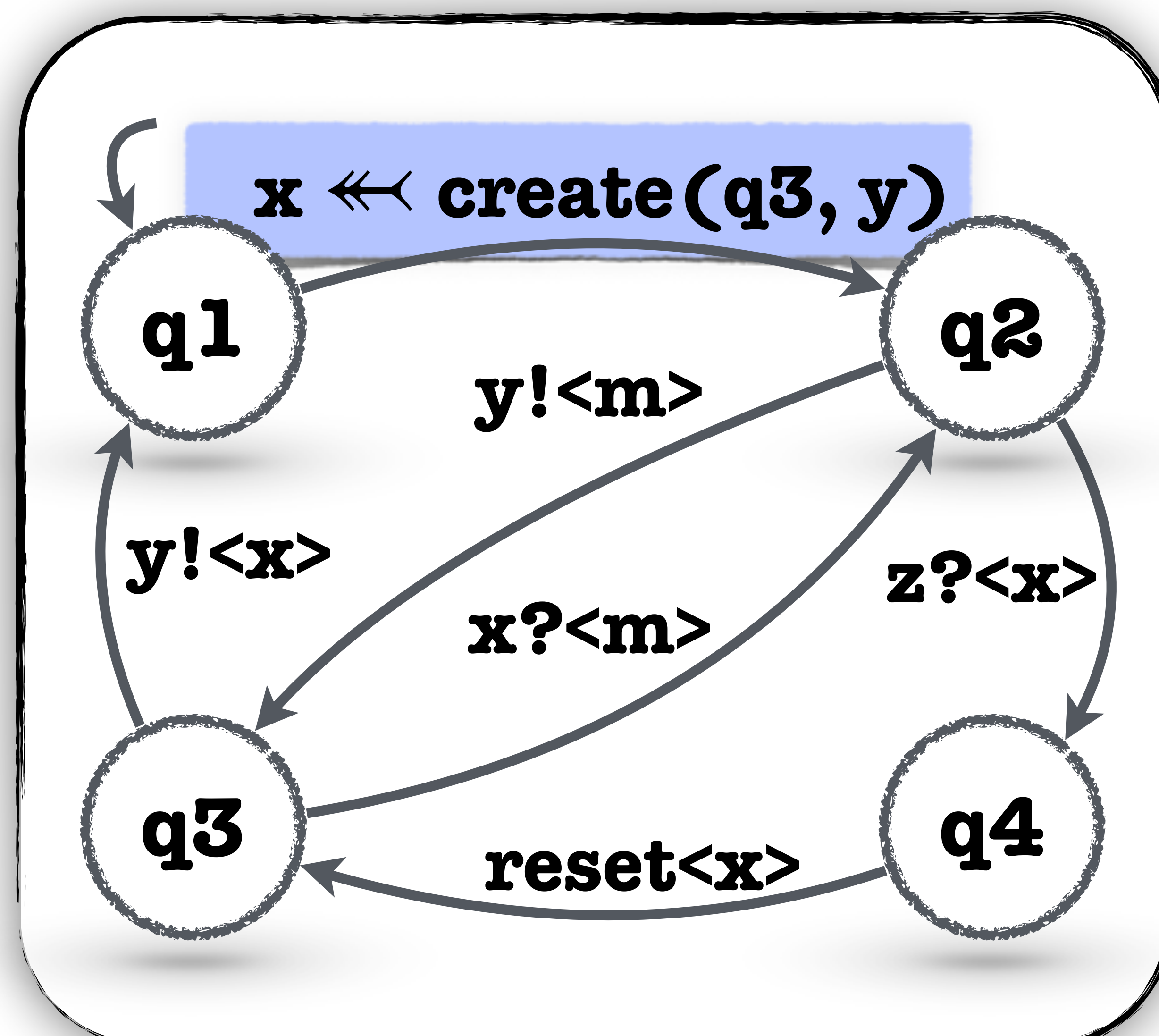
Configuration

Transition Relation



Process Model

Process Creation



Dynamic Register Automata

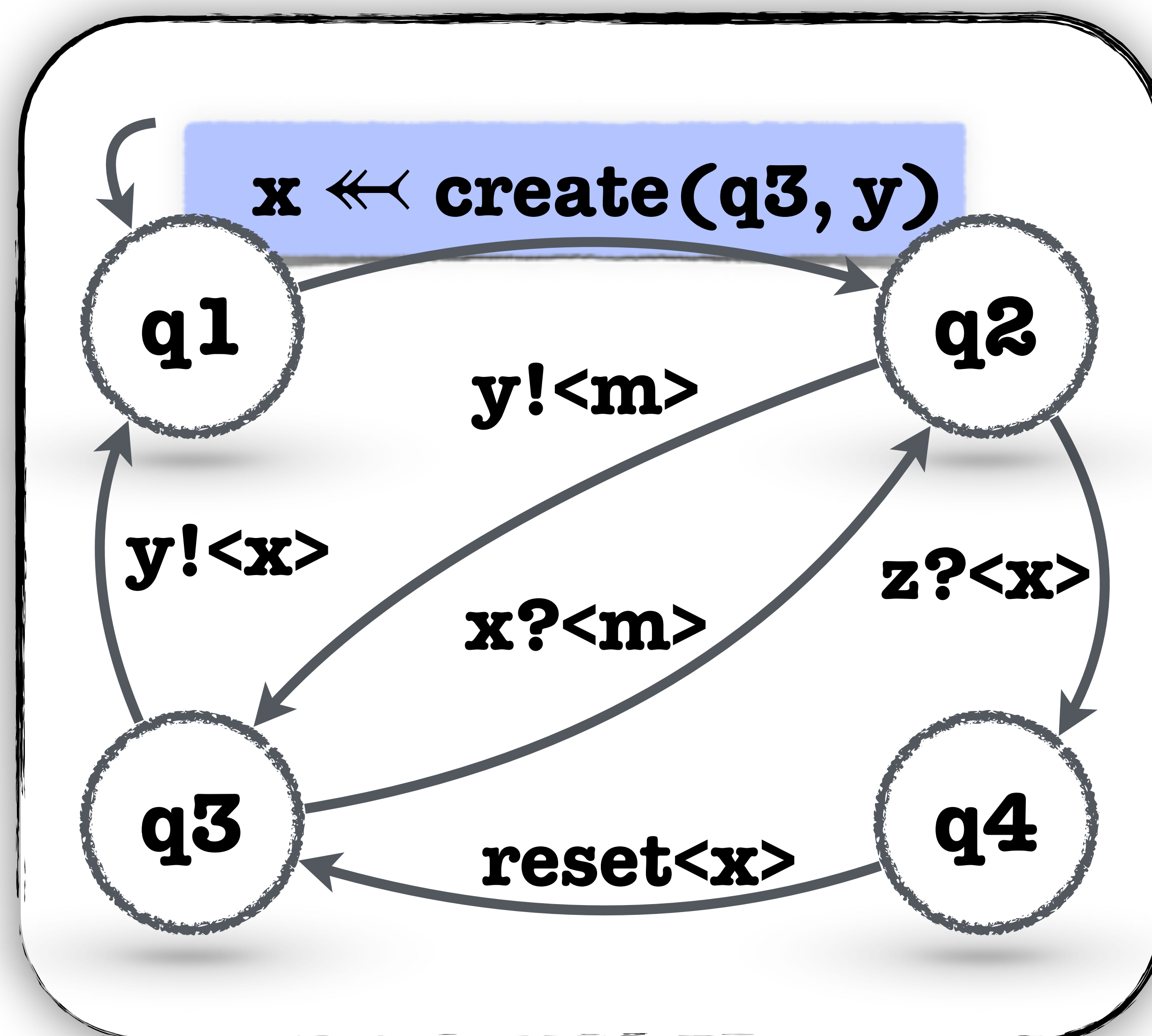
Formal Model

Configuration

Process Model

Transition Relation

Process Creation



Dynamic Register Automata

Formal Model

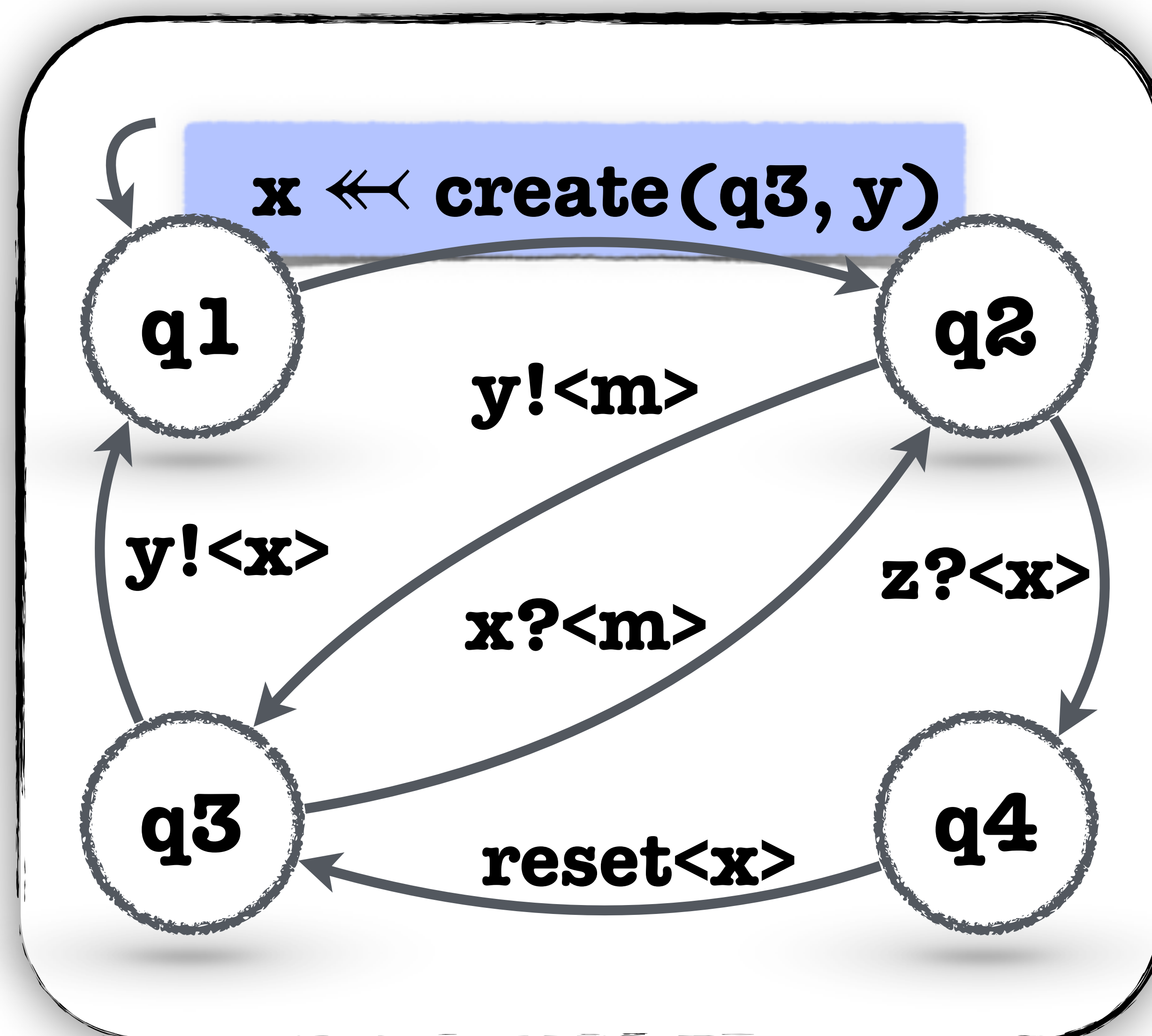
Configuration

Process Model

Transition Relation

Process Creation

Send & Receive ID



Dynamic Register Automata

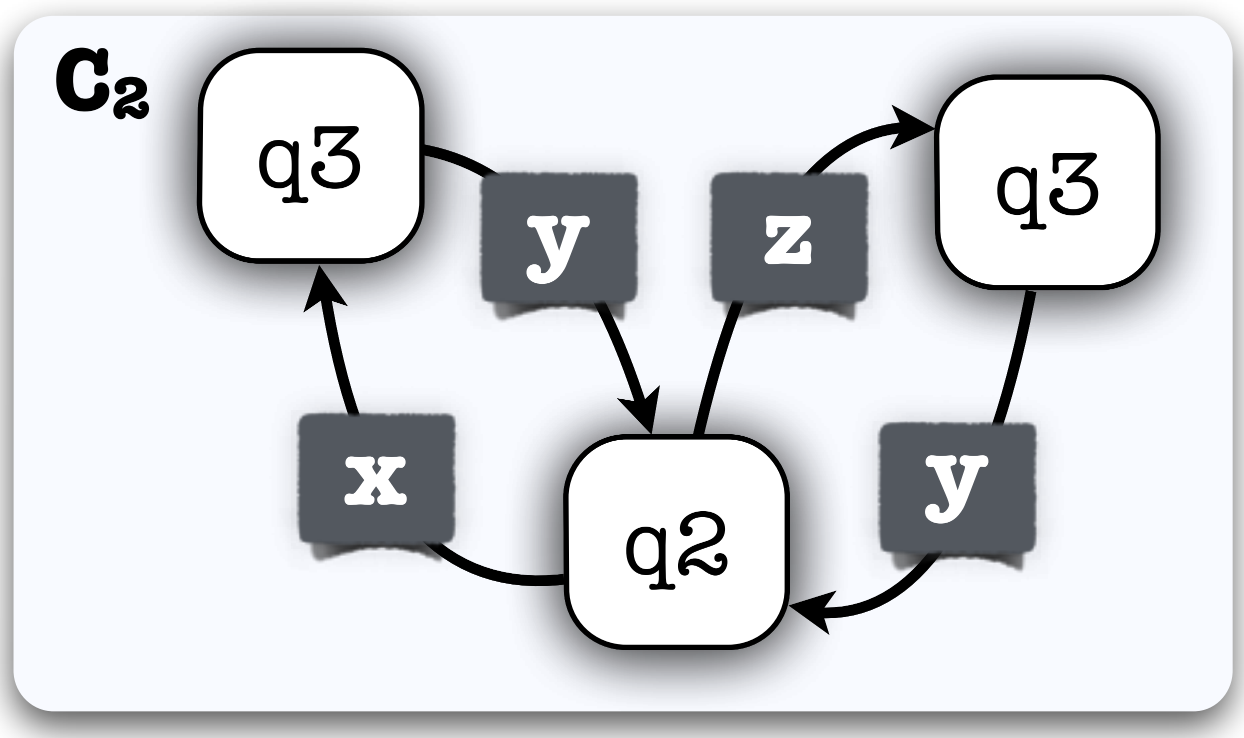
Formal Model

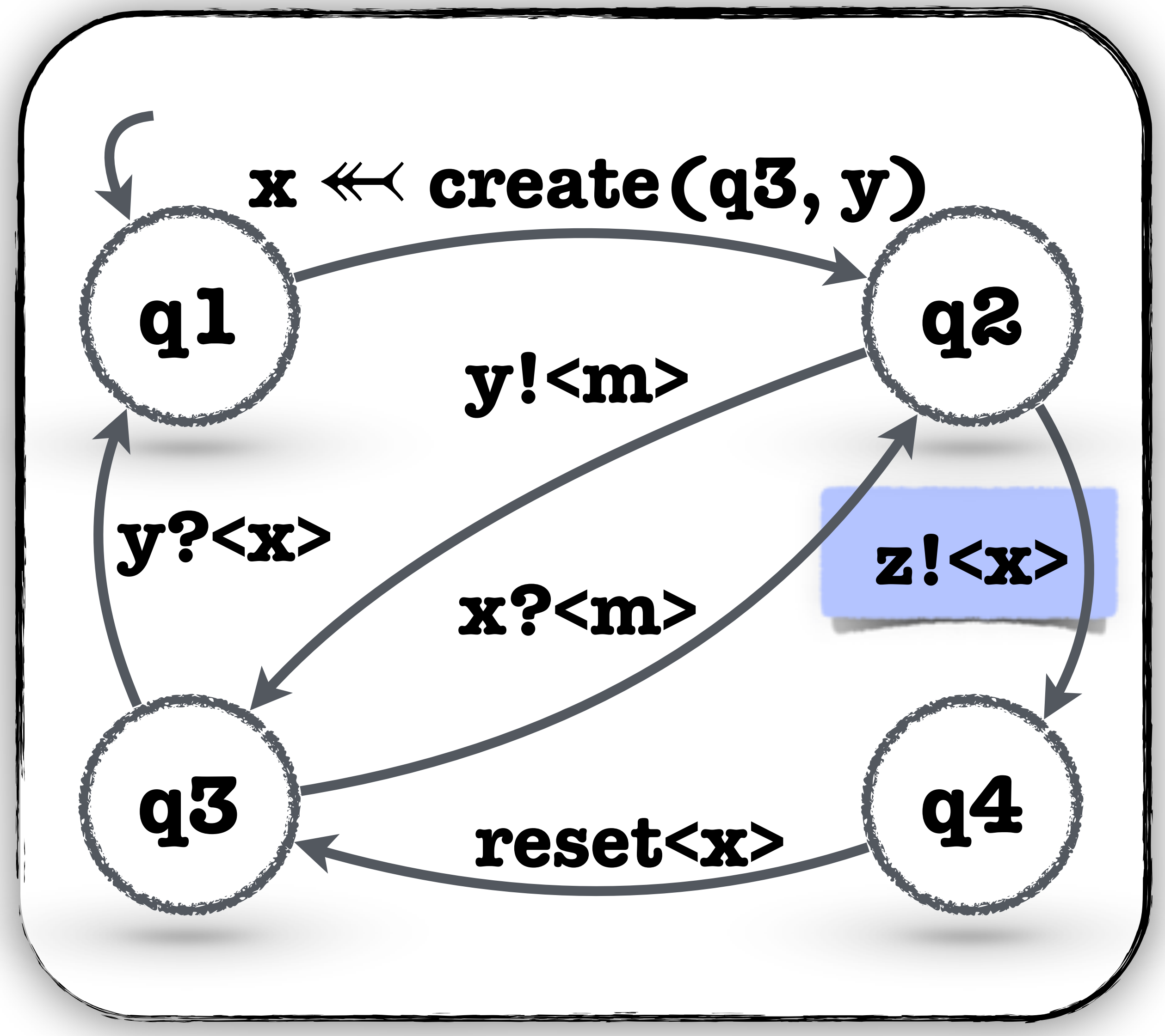
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

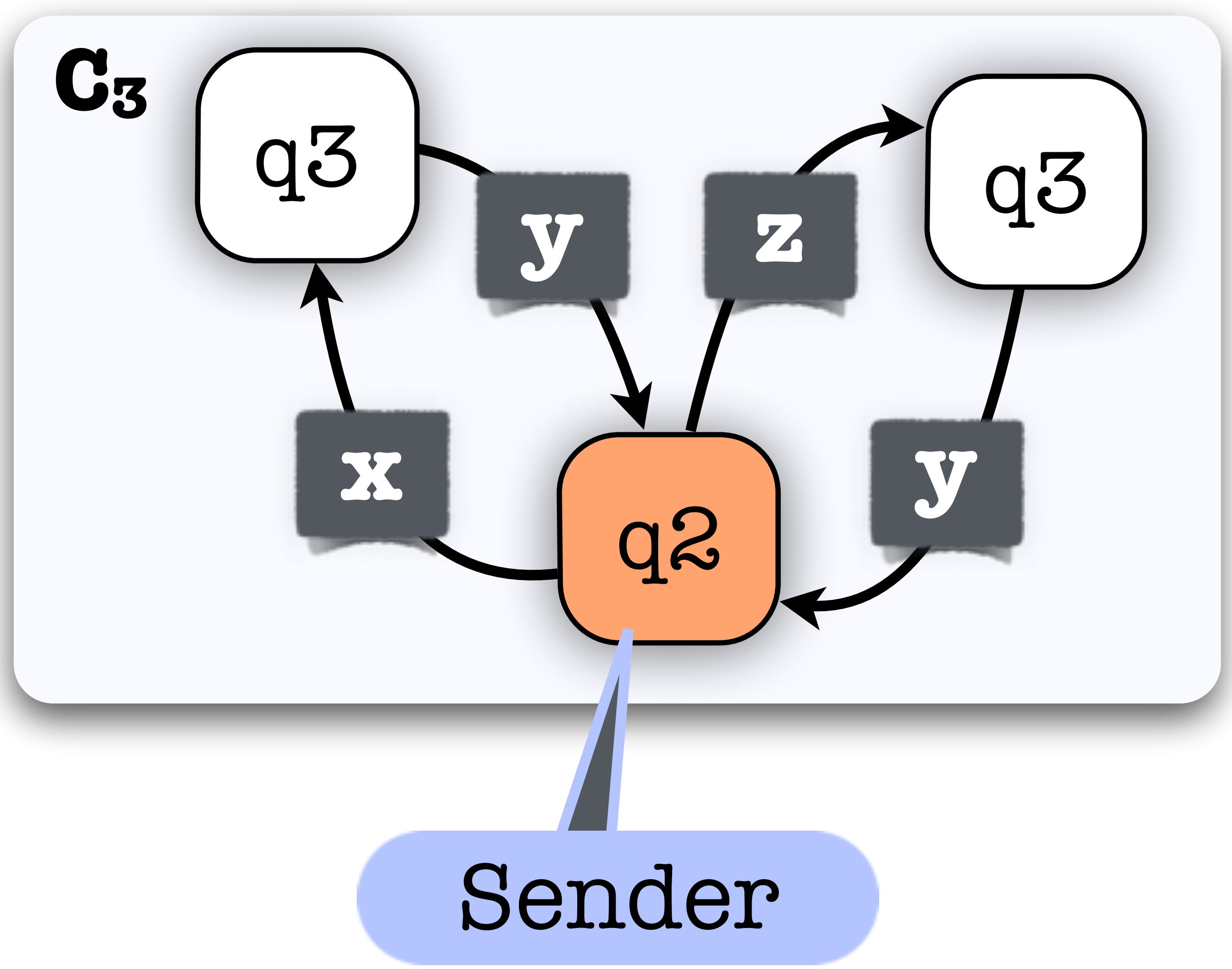
Formal Model

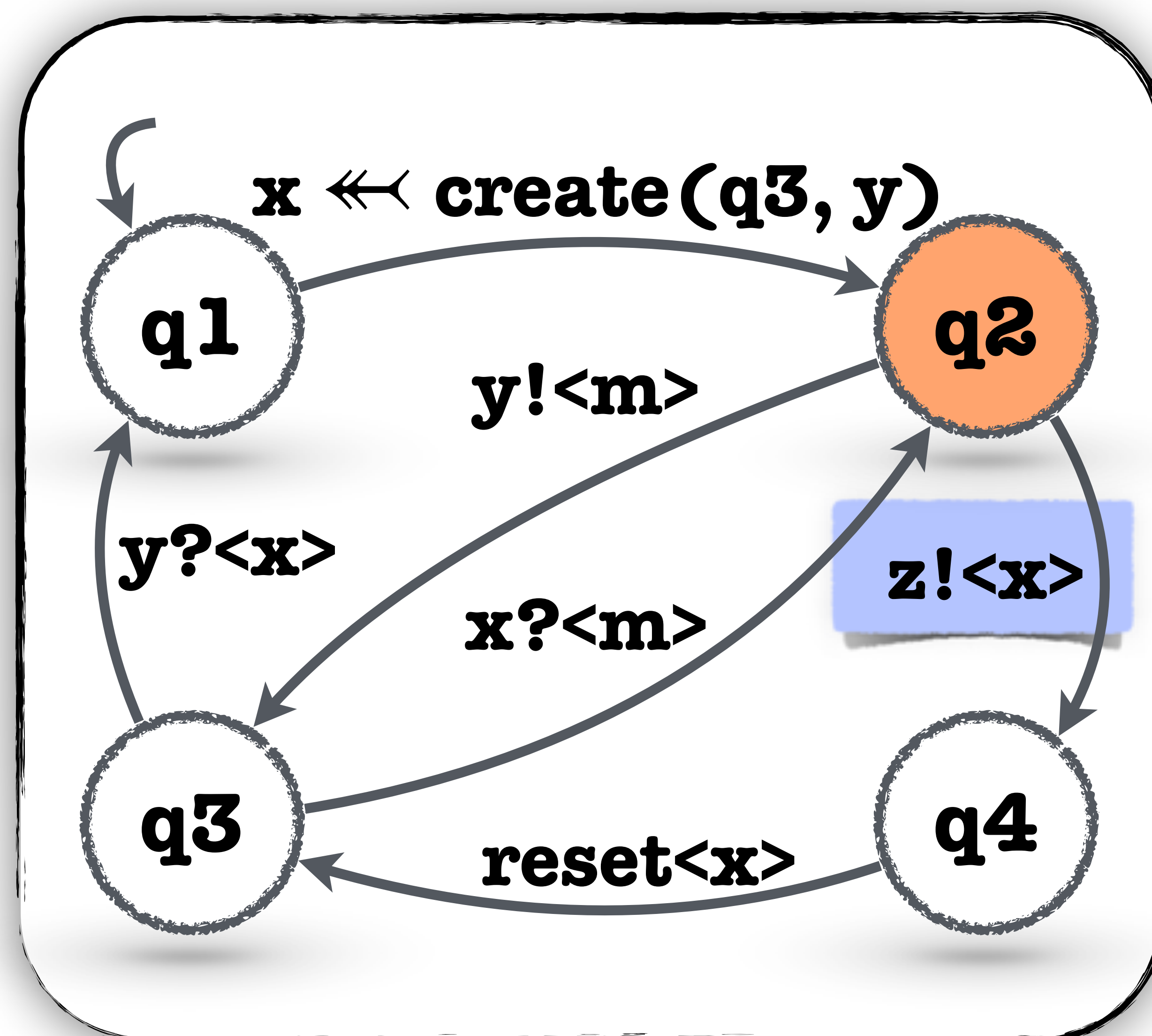
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

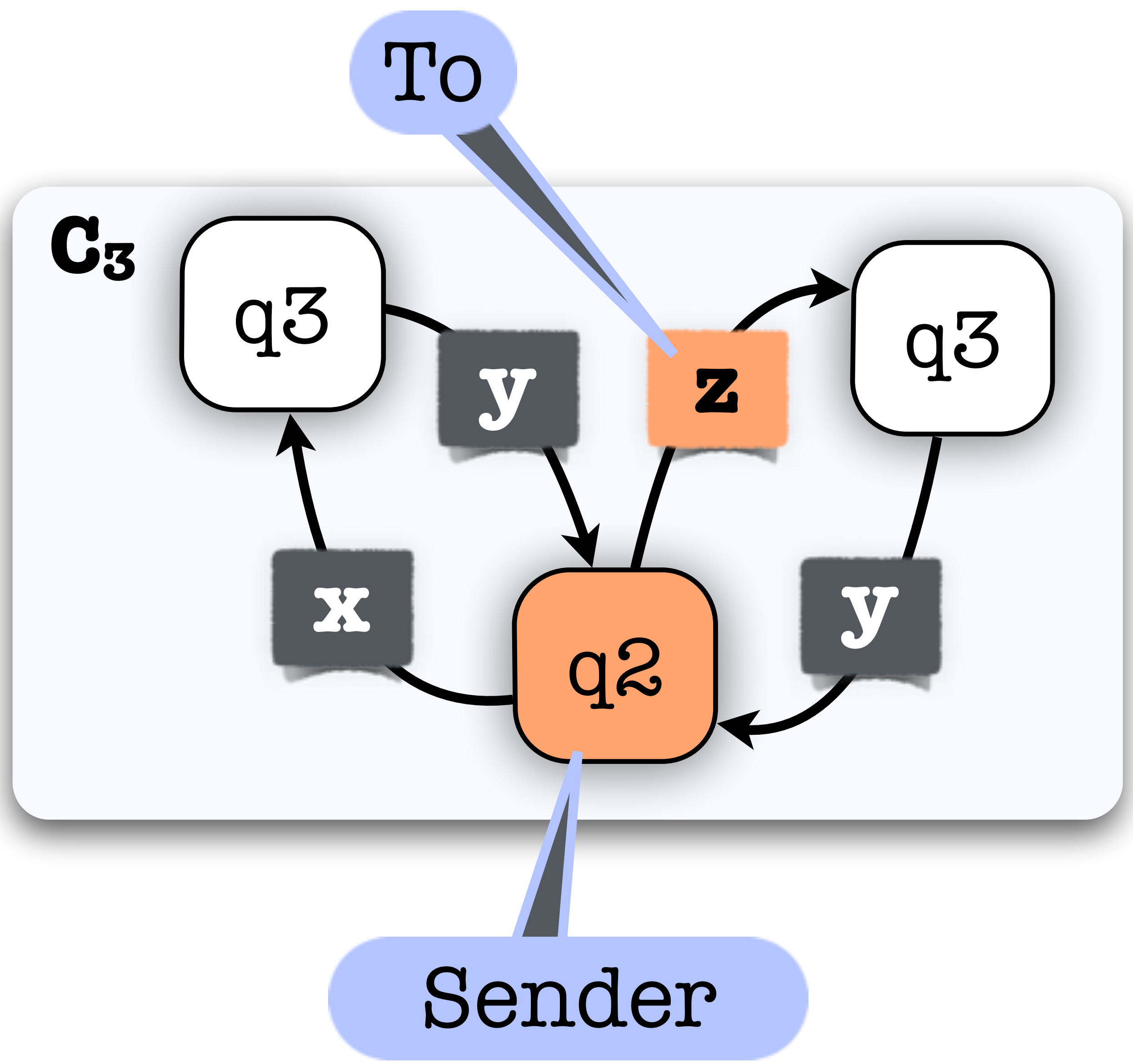
Formal Model

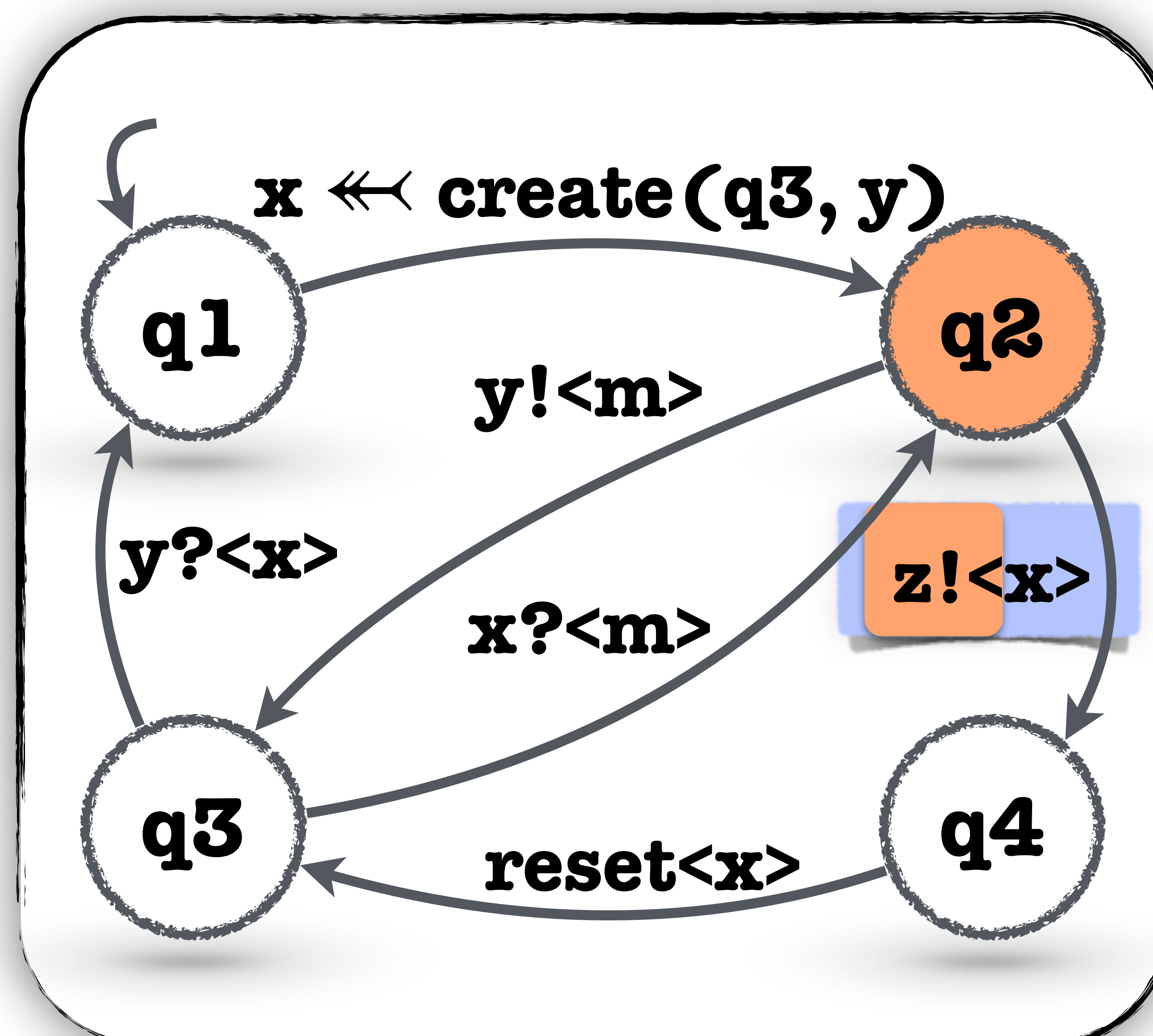
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

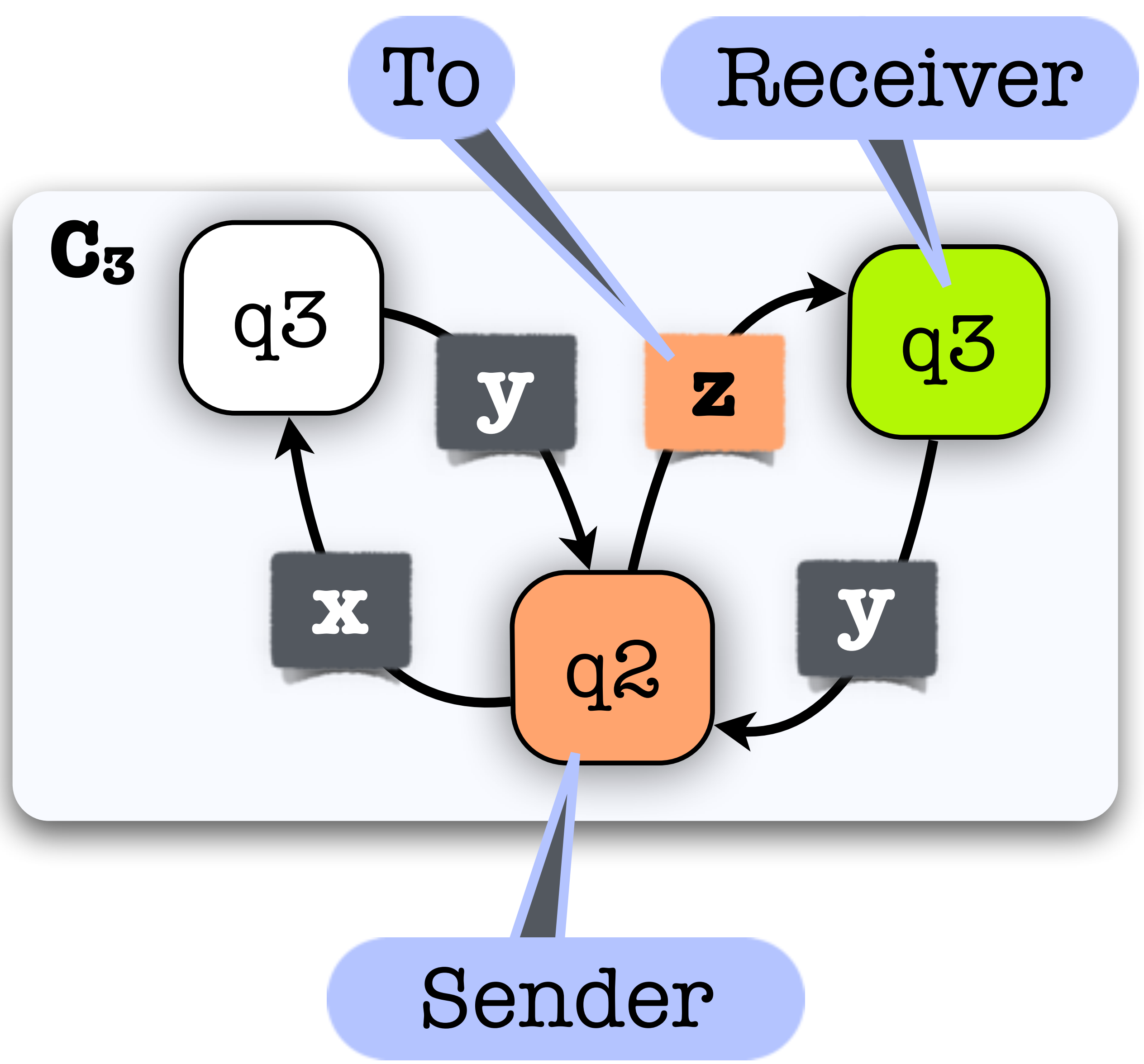
Formal Model

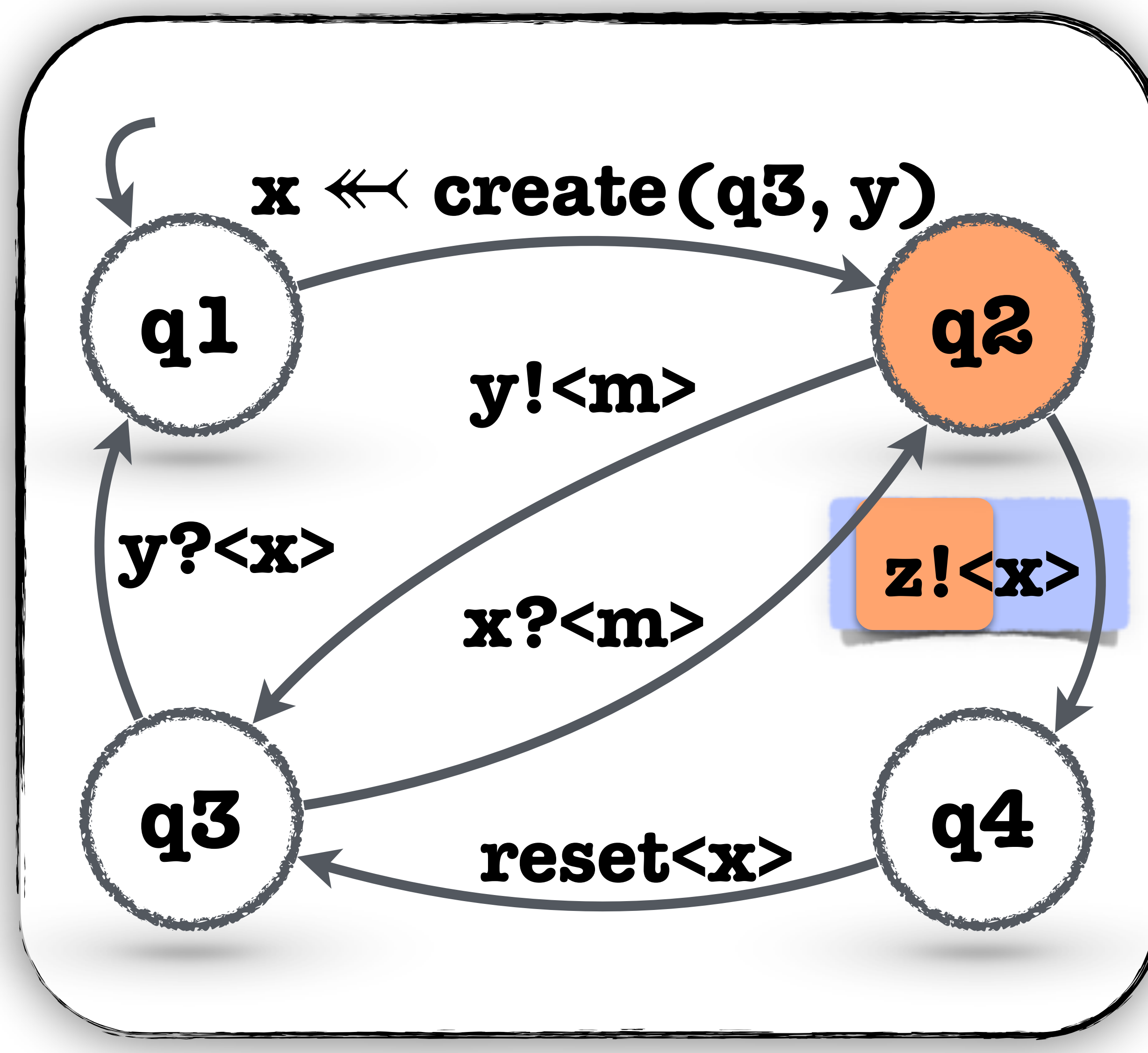
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

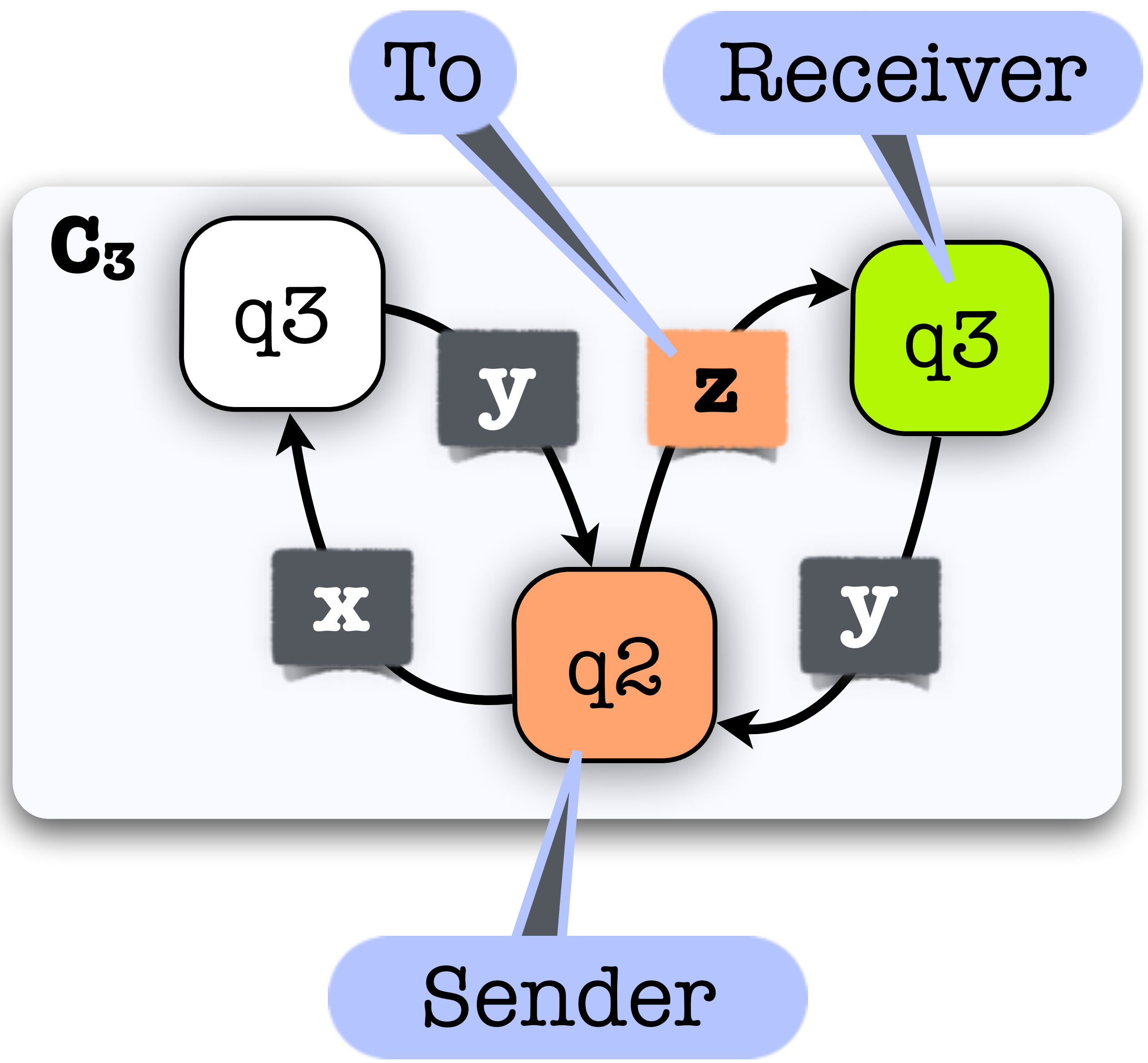
Formal Model

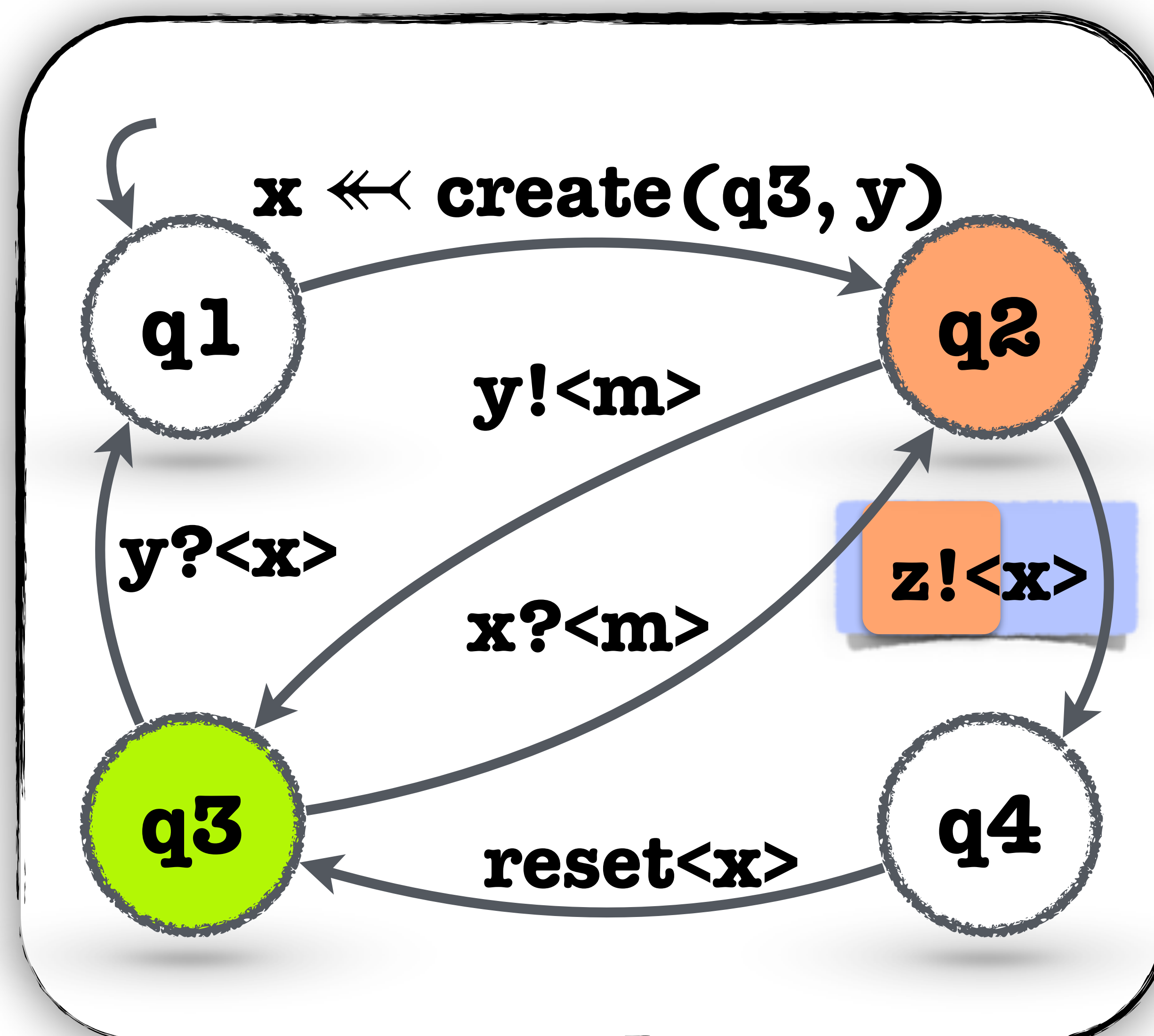
Configuration

Transition Relation

Process Model

Send & Receive ID





Dynamic Register Automata

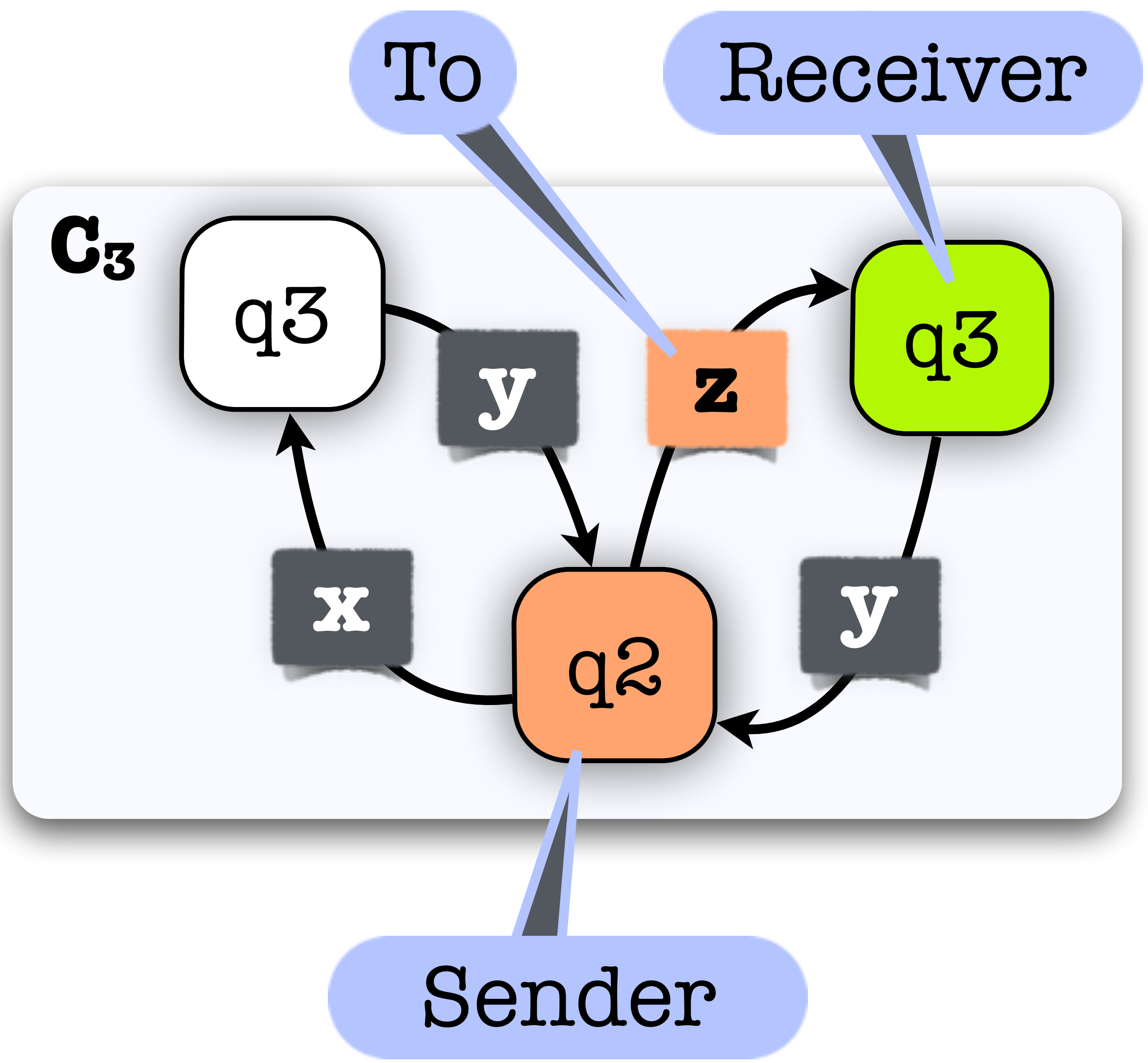
Formal Model

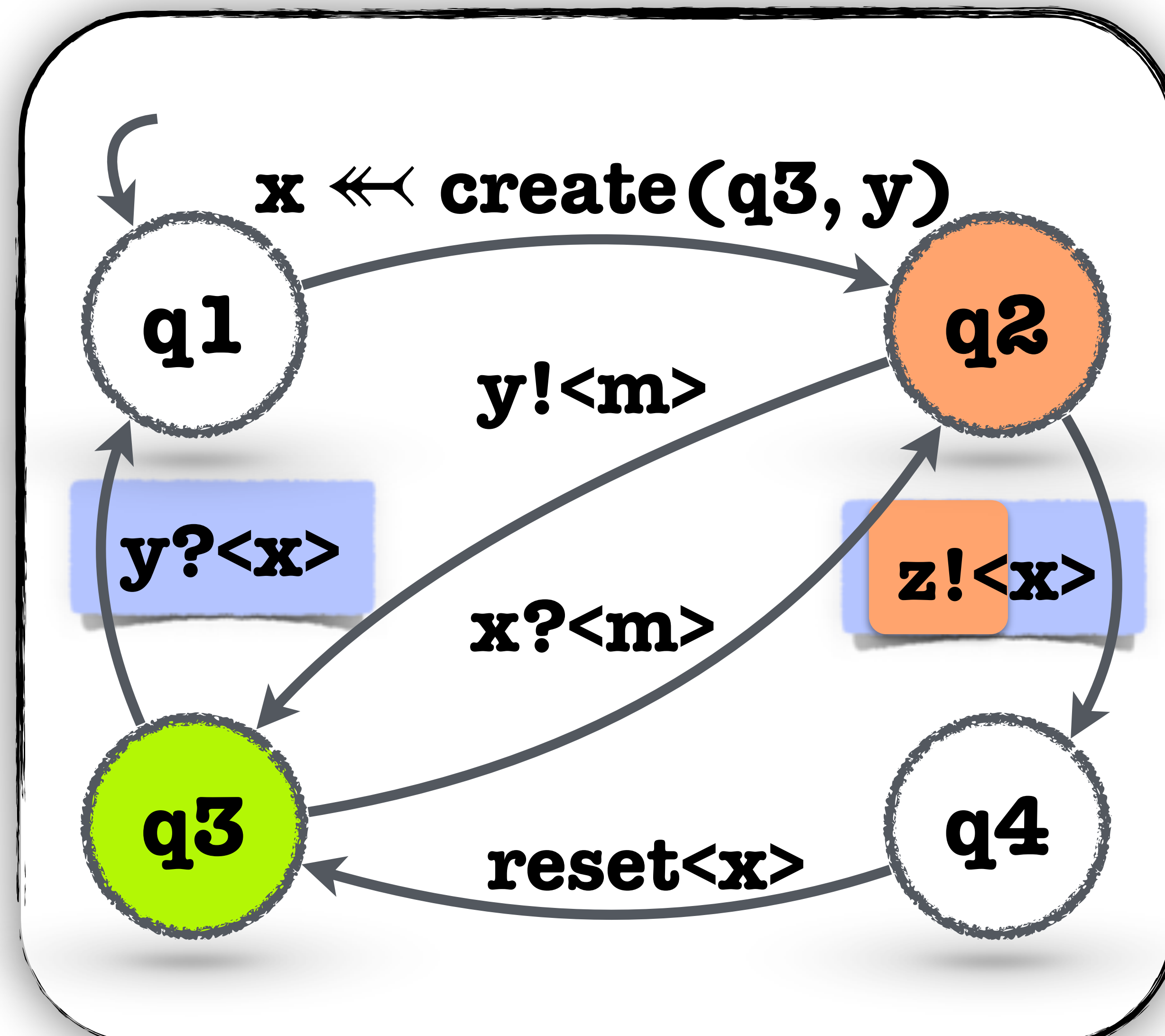
Configuration

Transition Relation

Process Model

Send & Receive ID





Dynamic Register Automata

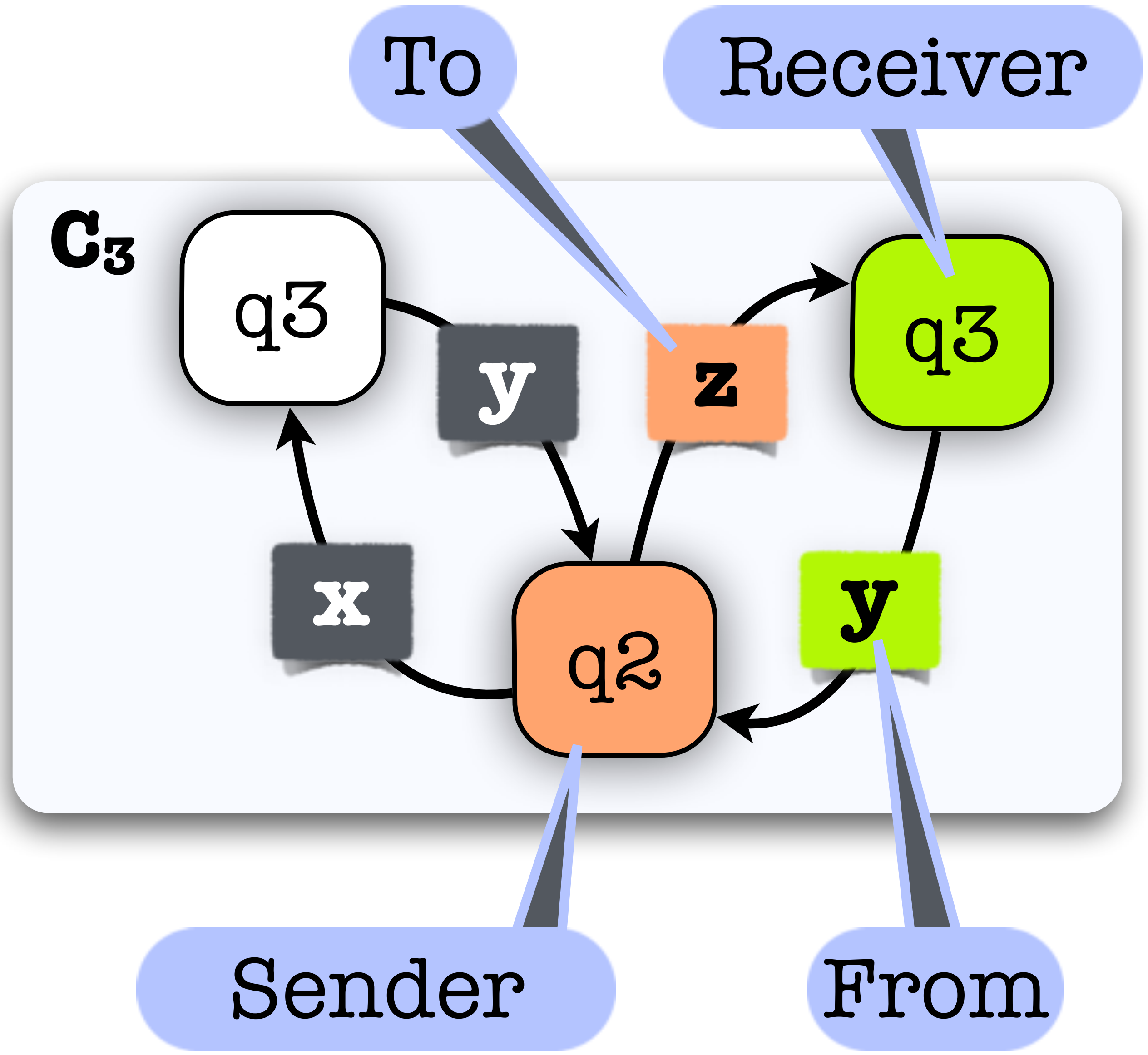
Formal Model

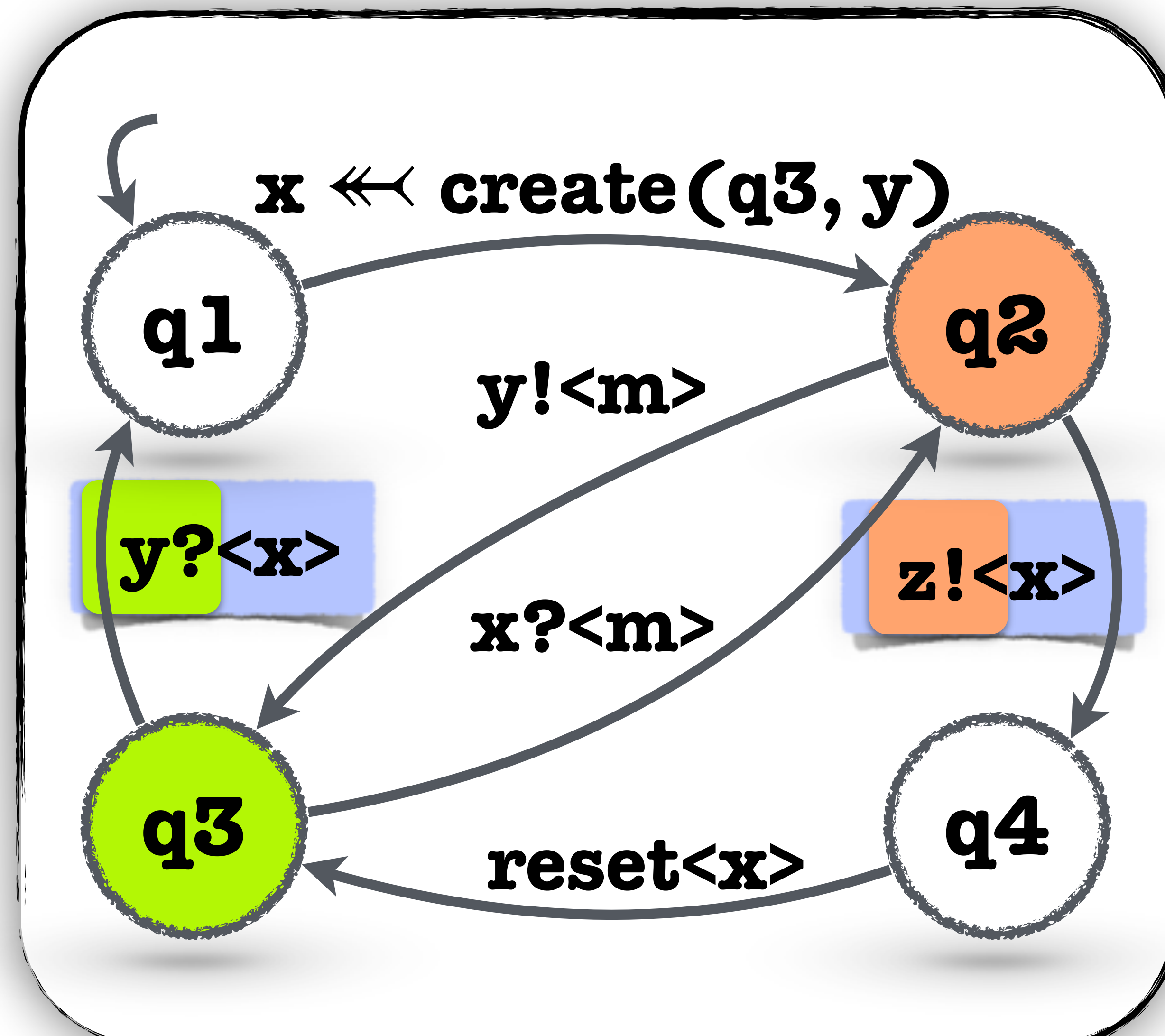
Configuration

Transition Relation

Process Model

Send & Receive ID





Dynamic Register Automata

Formal Model

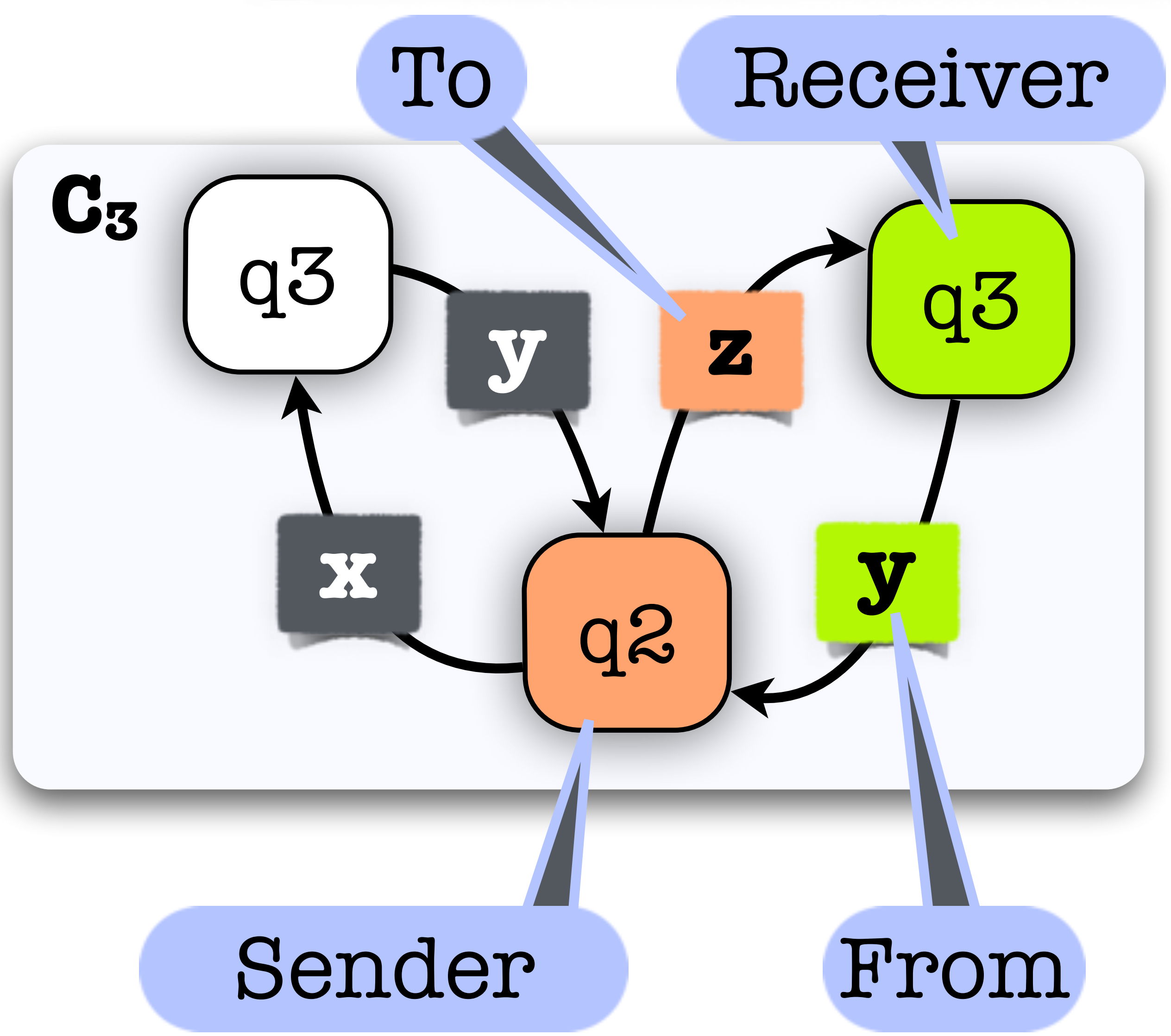
Configuration

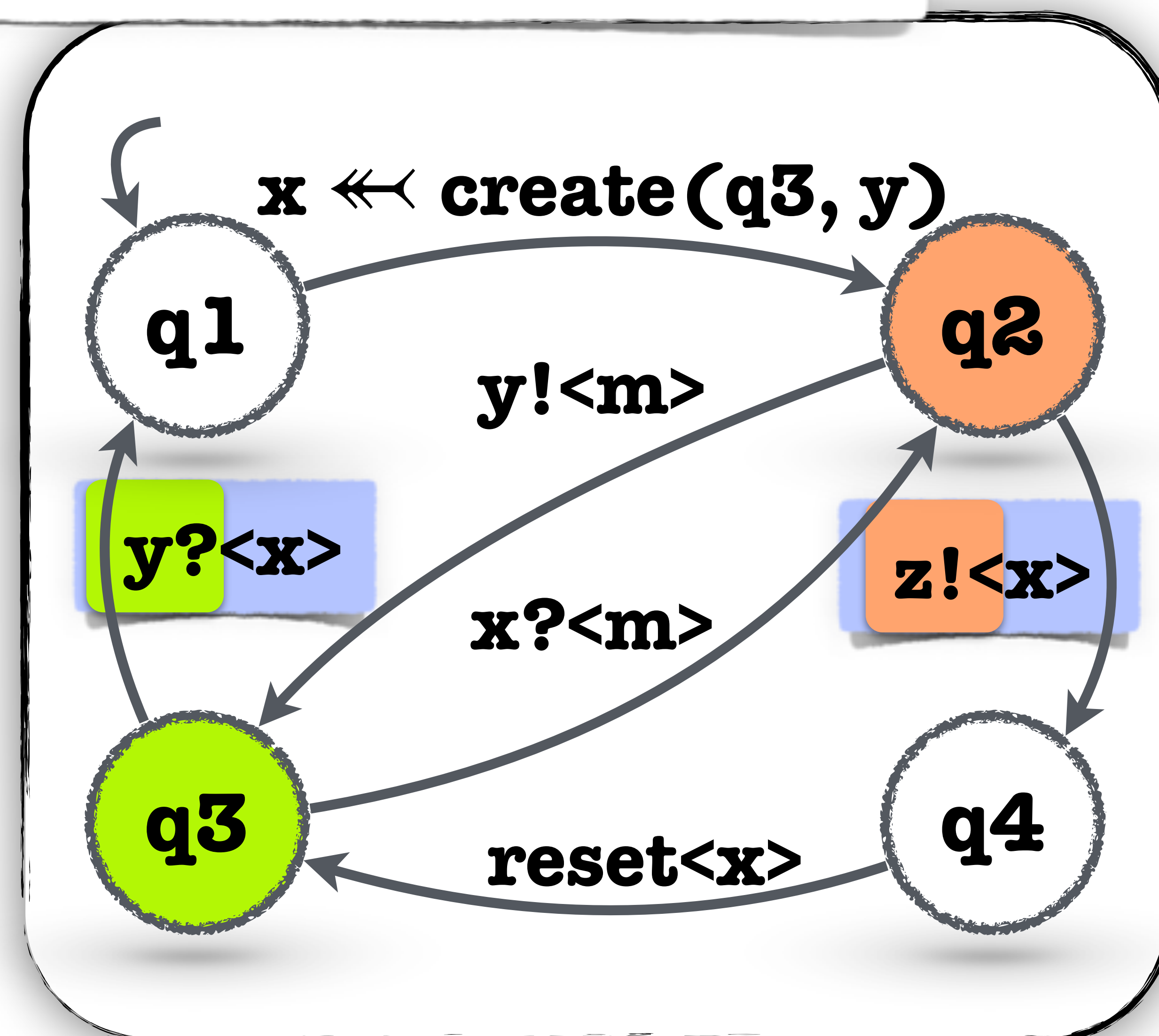
Transition Relation

Process Model

Send & Receive ID

Point-To-Point, Rendez-Vous communication





Dynamic Register Automata

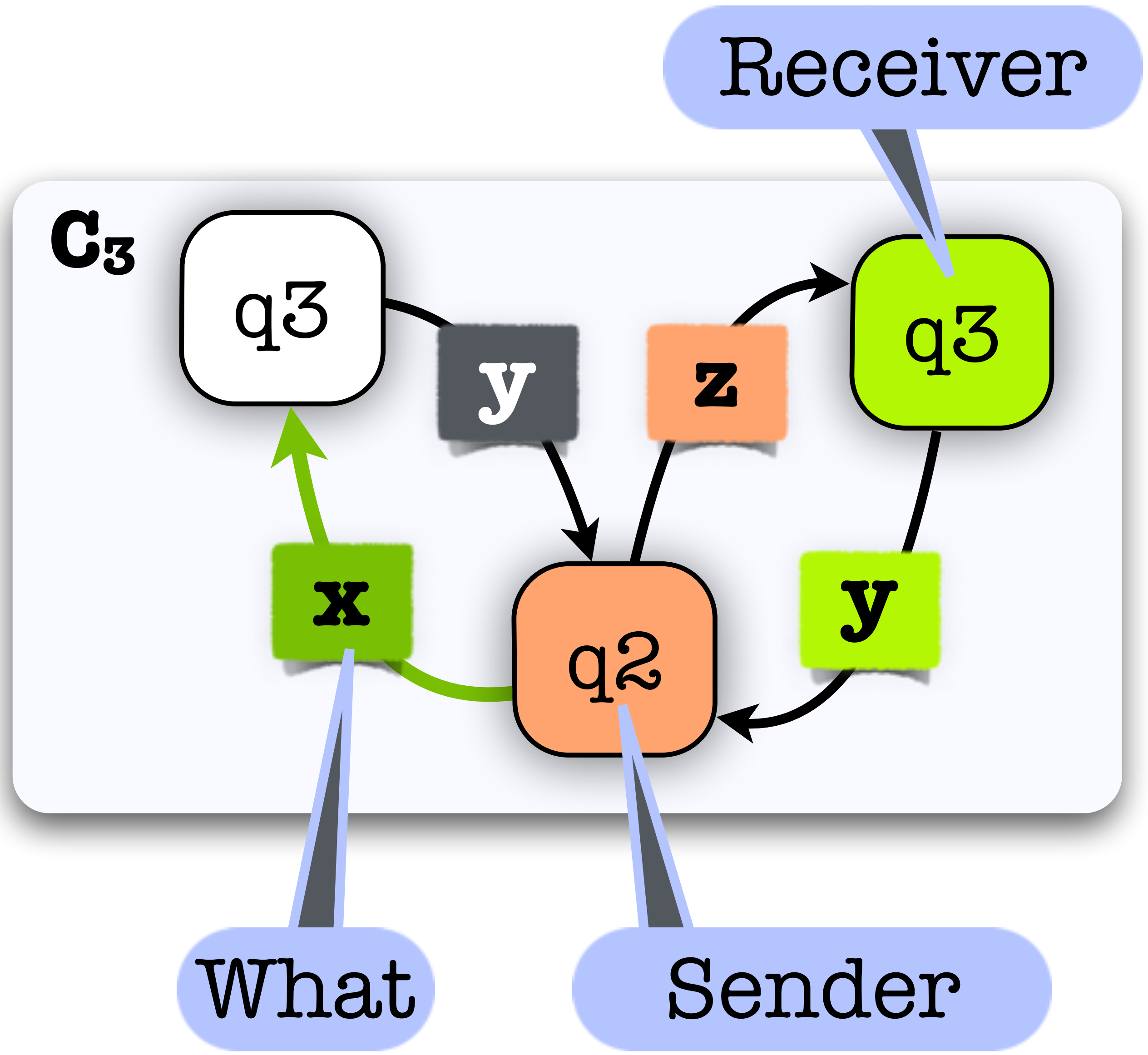
Formal Model

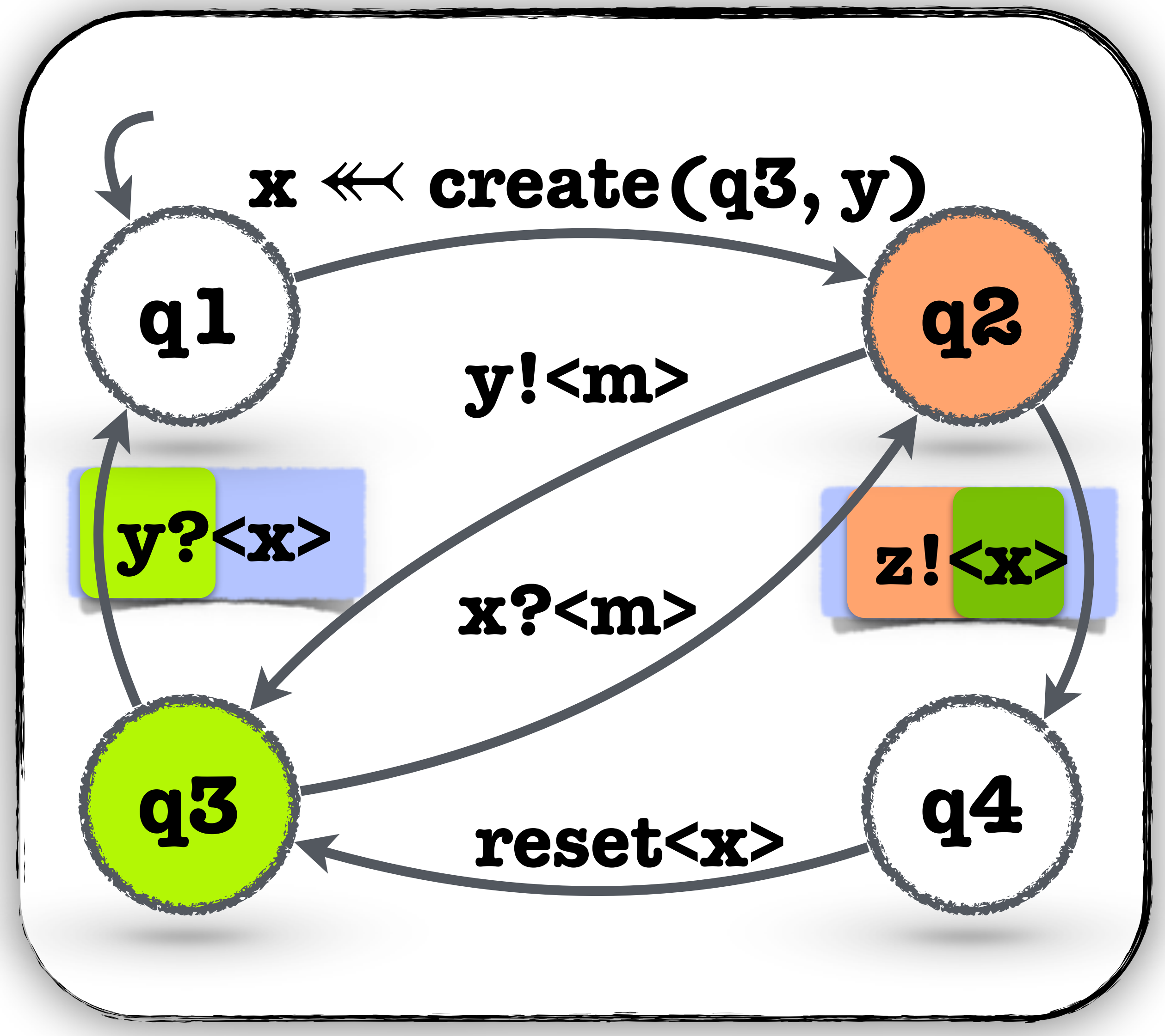
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

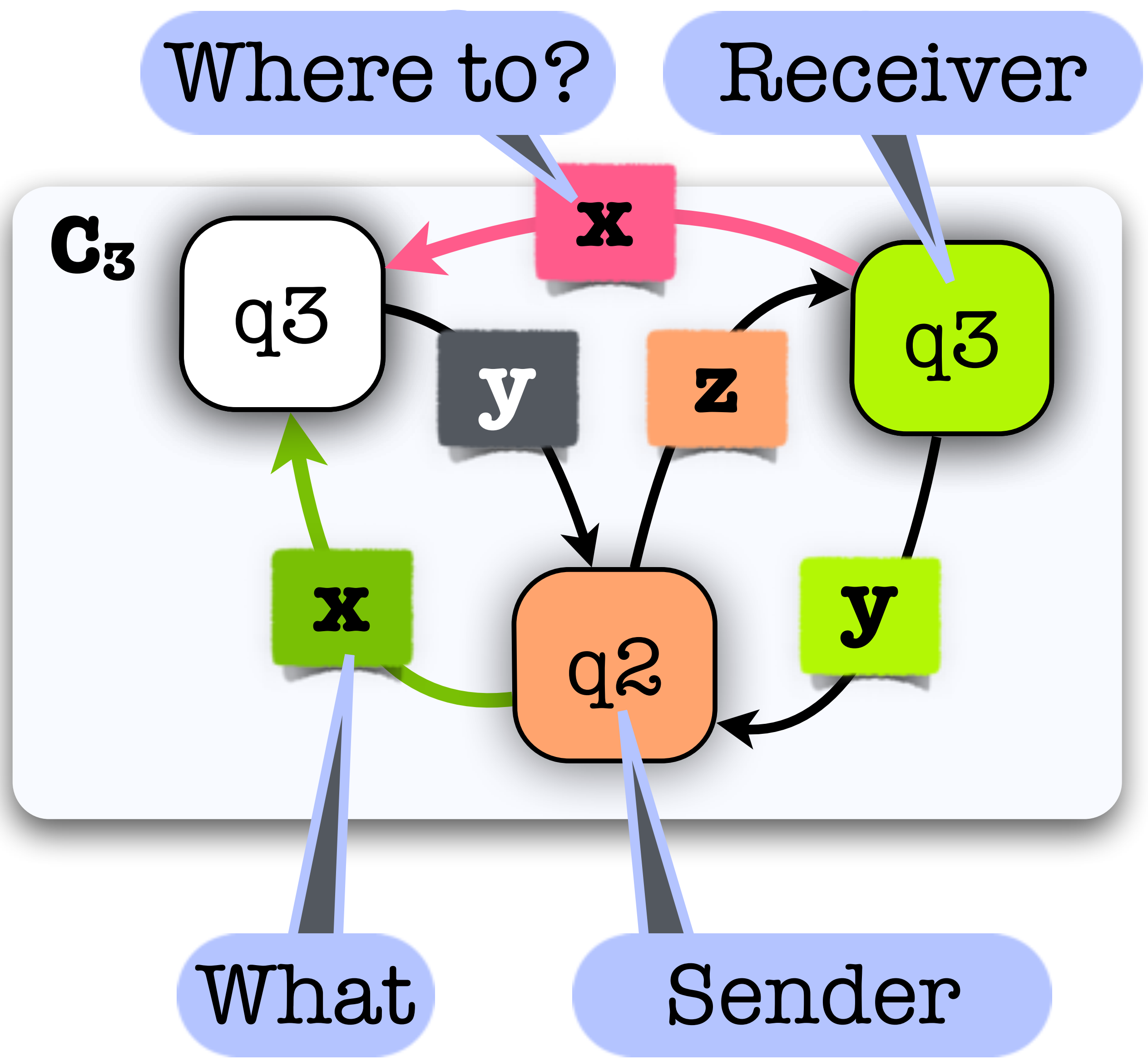
Formal Model

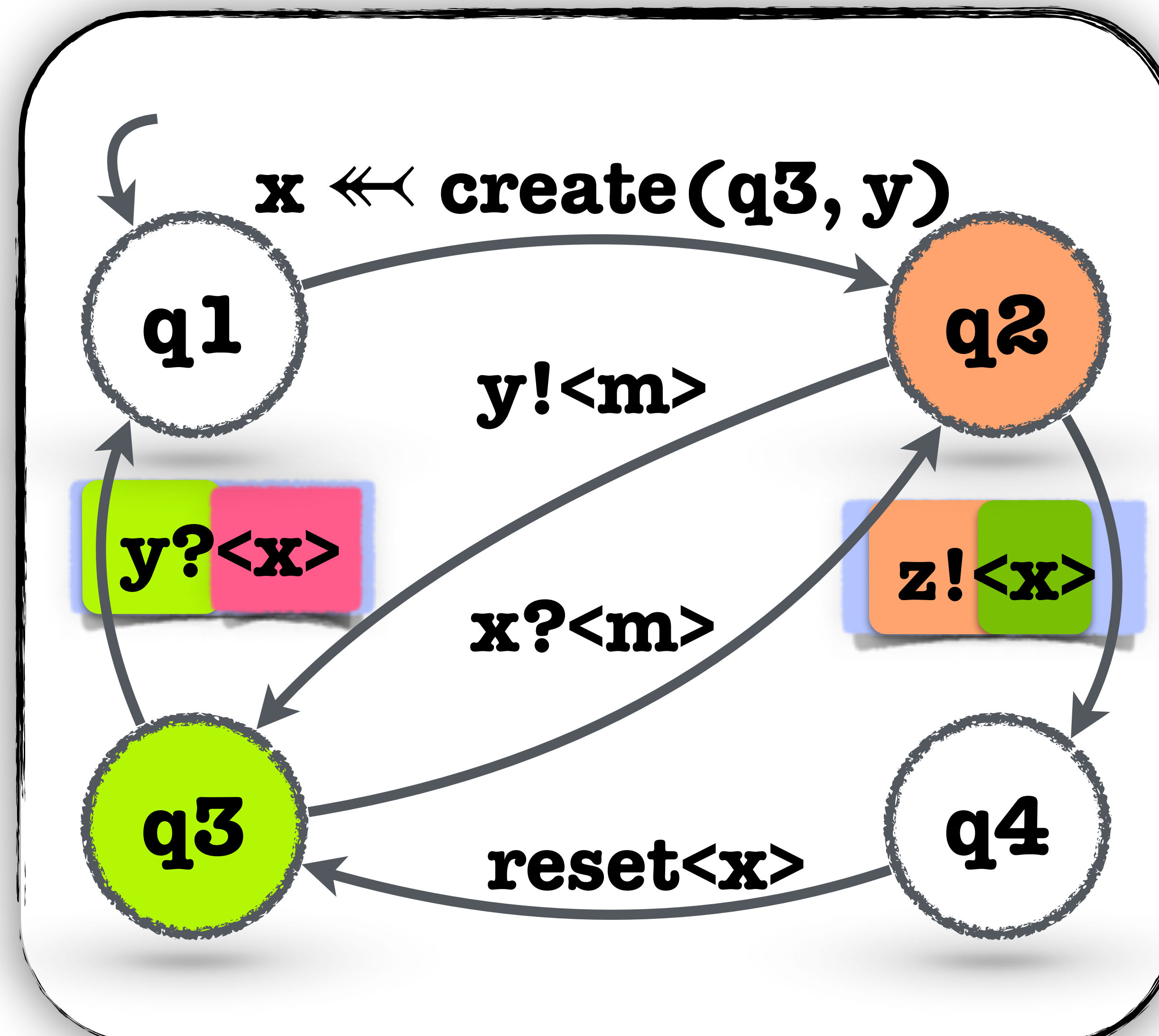
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

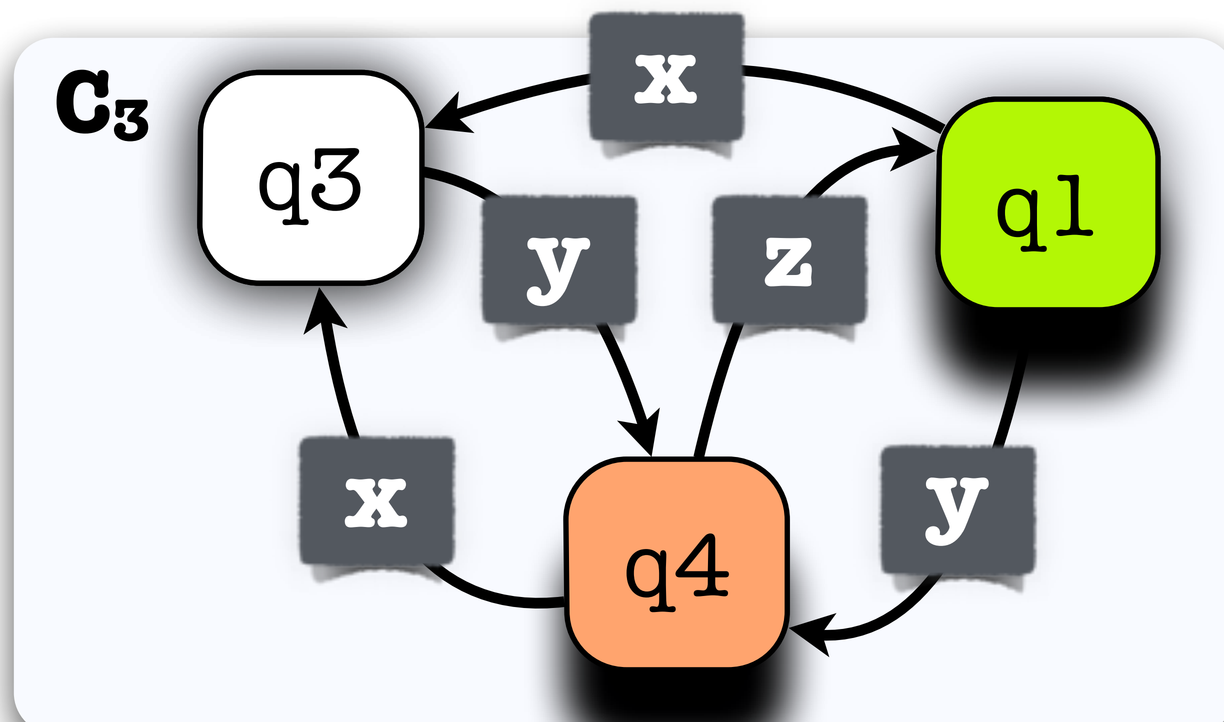
Formal Model

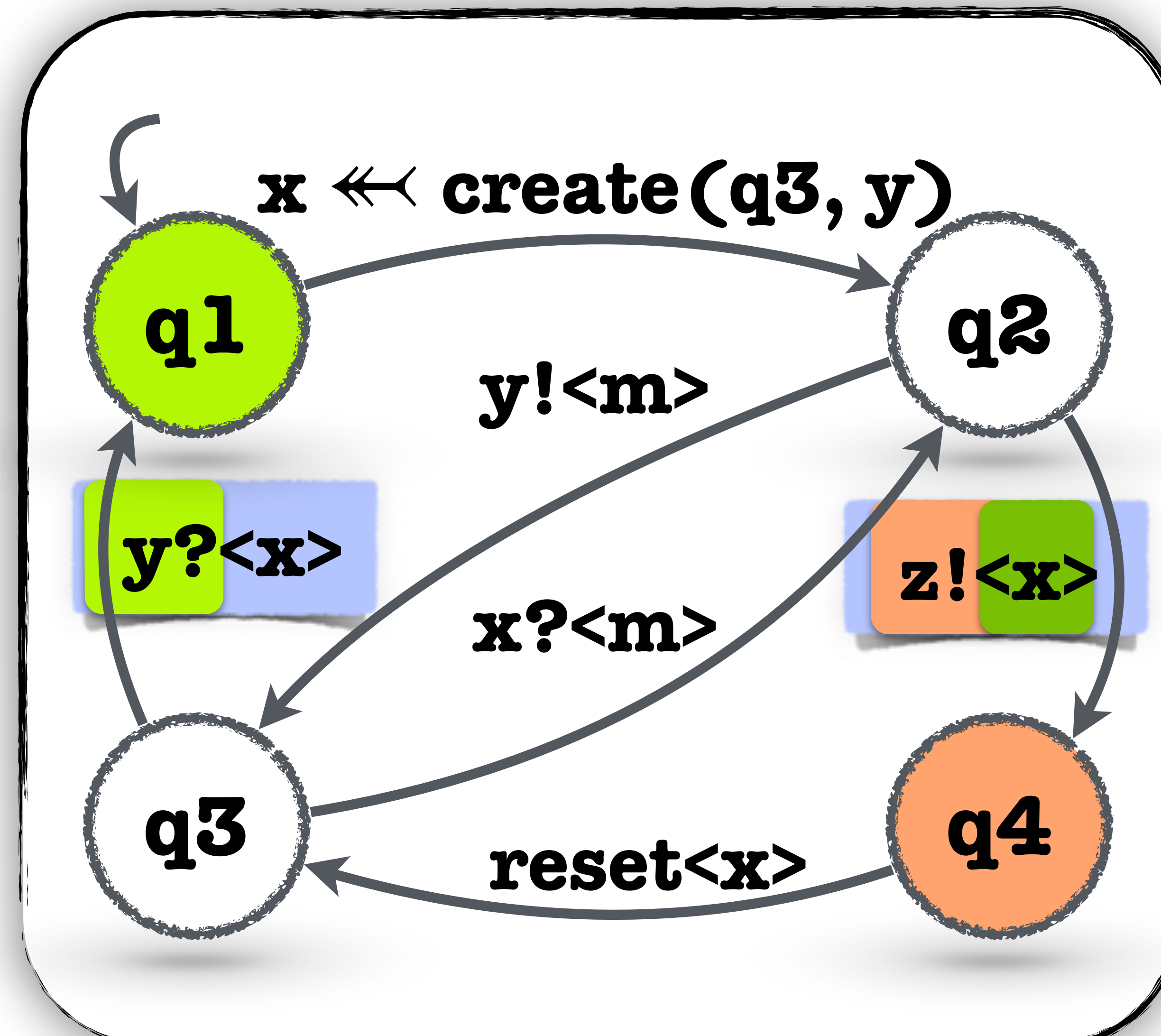
Configuration

Transition Relation

Send & Receive ID

Process Model





Dynamic Register Automata

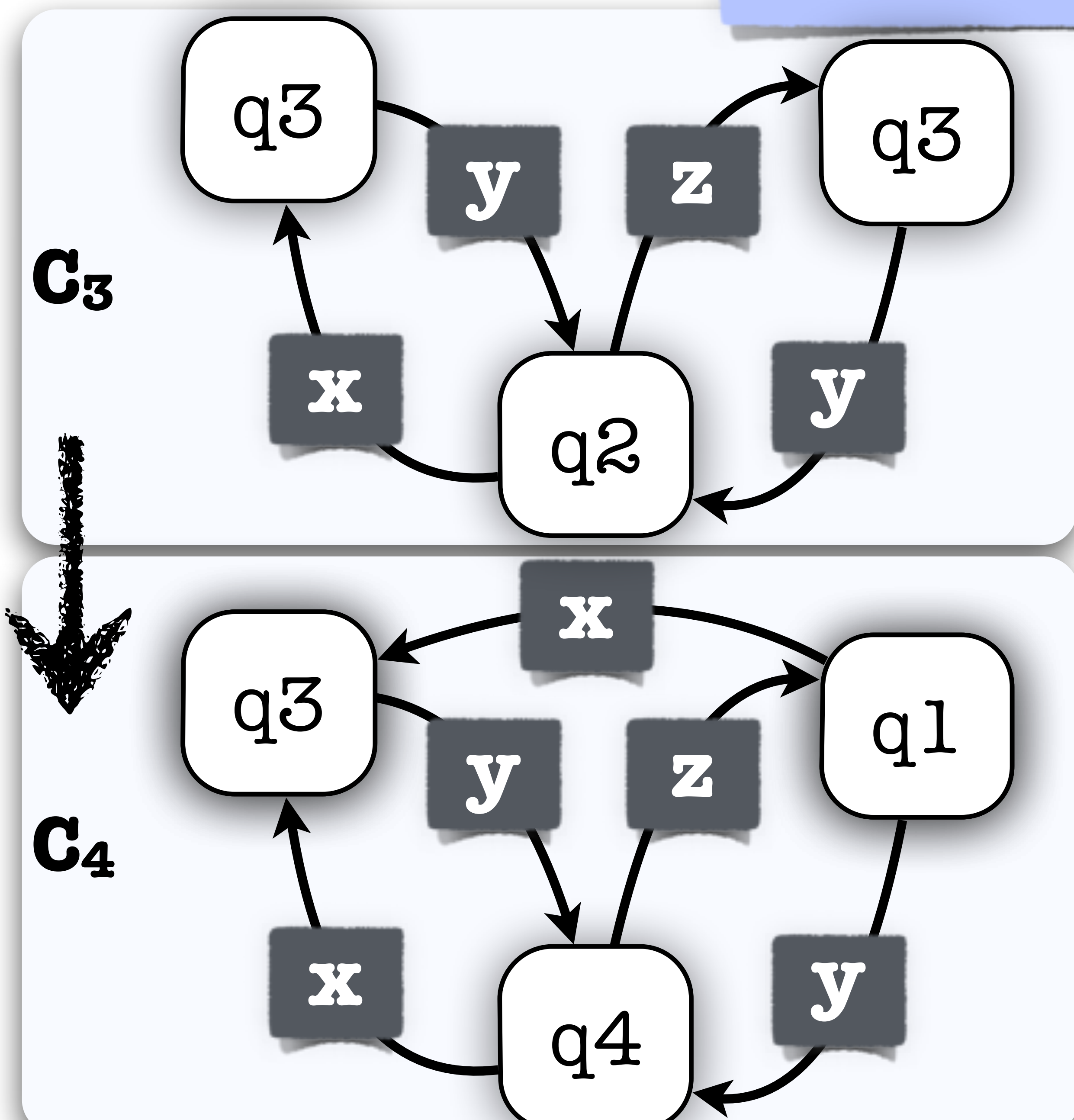
Formal Model

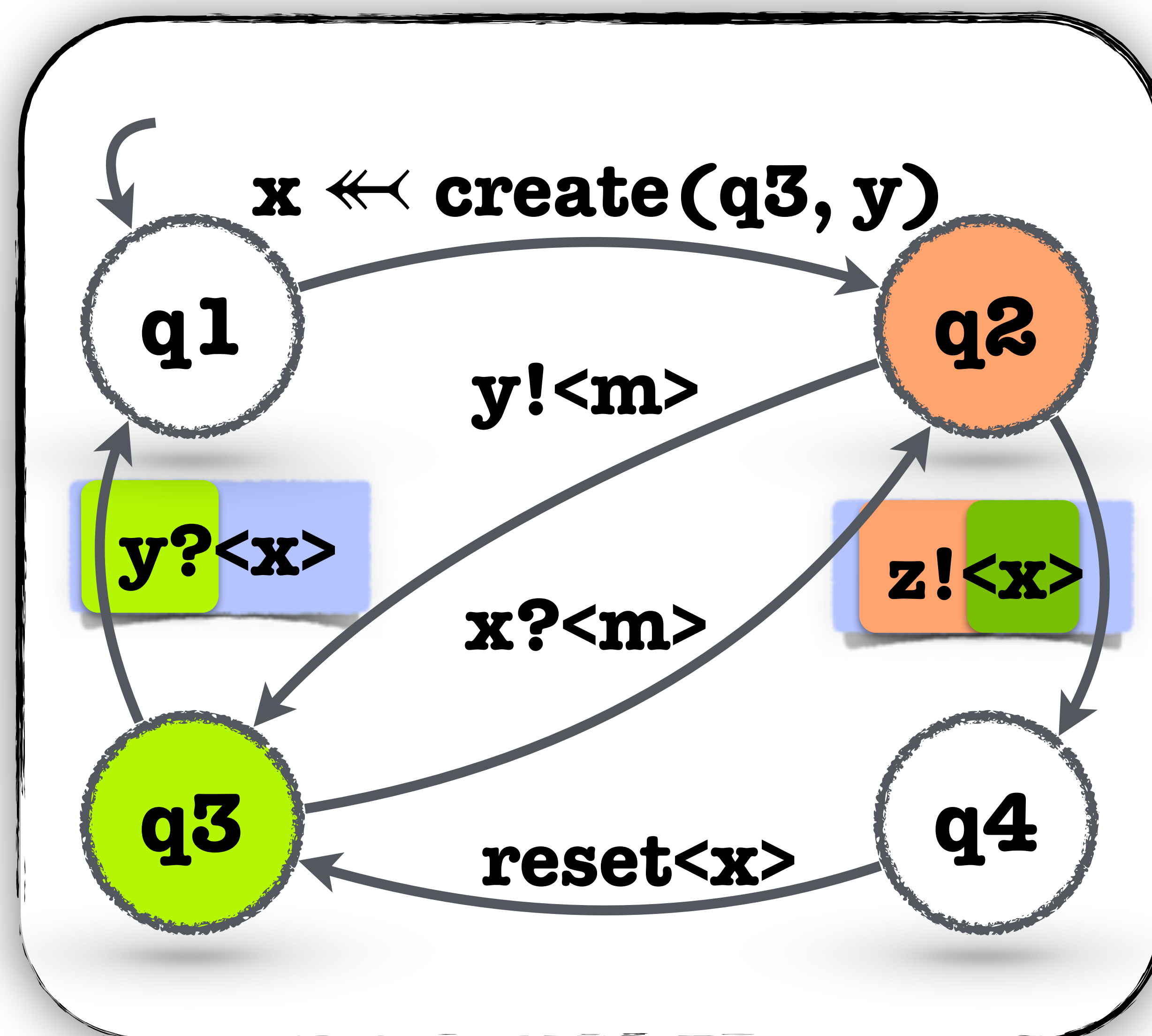
Configuration

Transition Relation

Process Model

Send & Receive ID





Dynamic Register Automata

Formal Model

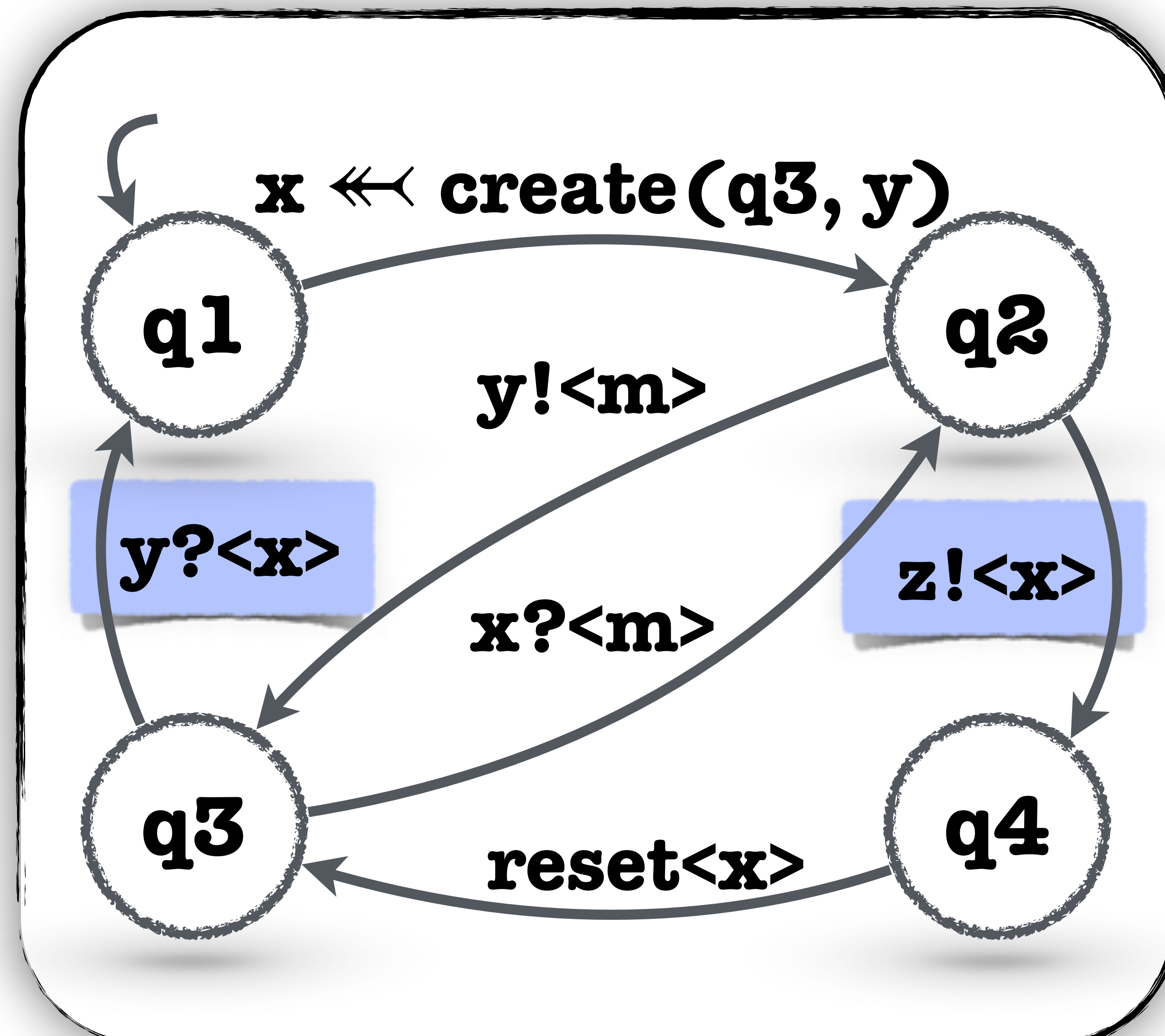
Configuration

Process Model

Transition Relation

Process Creation

Send & Receive ID



Dynamic Register Automata

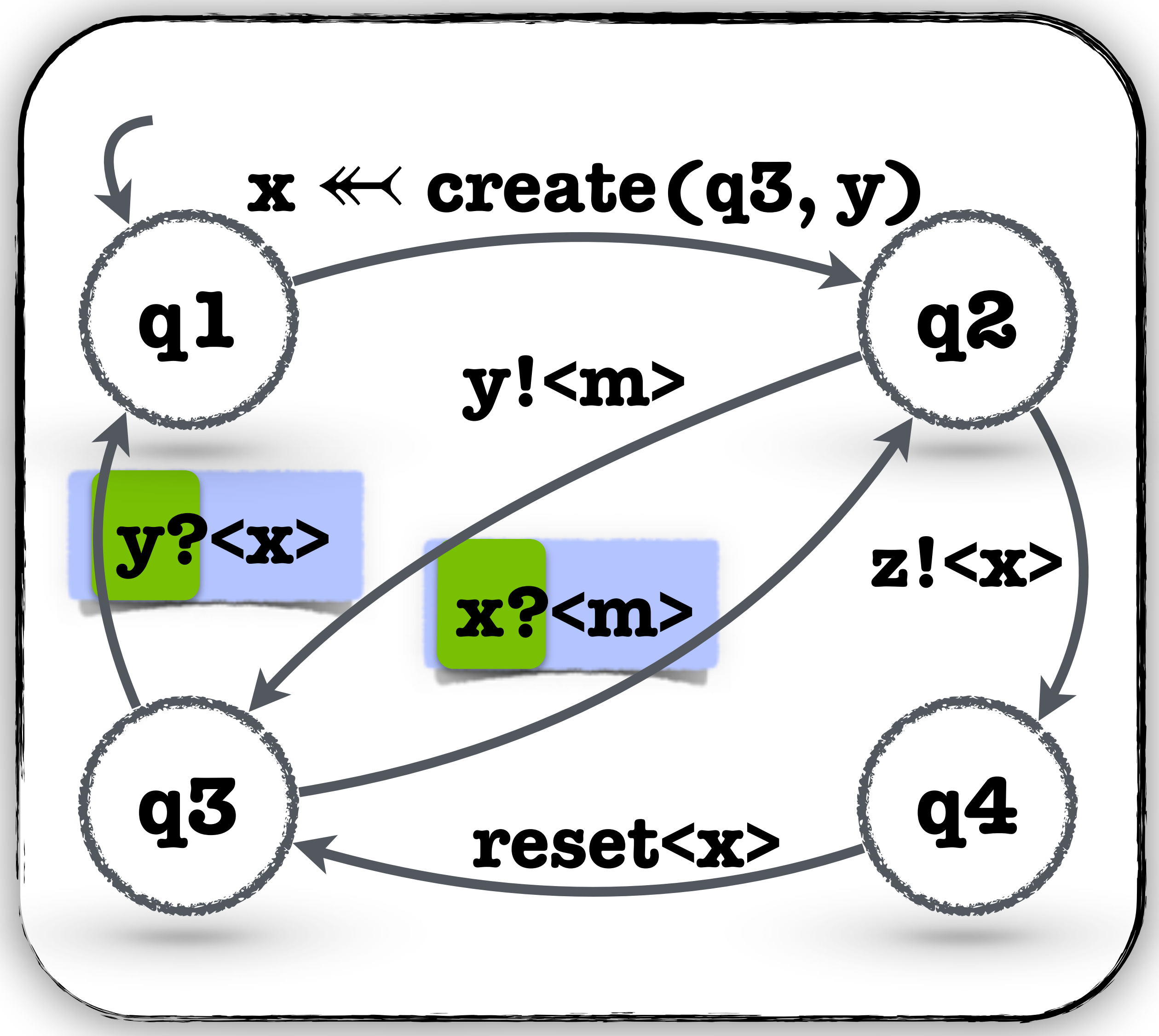
Formal Model

Configuration

Process Model

Transition Relation

- Process Creation
- Send & Receive ID



Dynamic Register Automata

Formal Model

Configuration

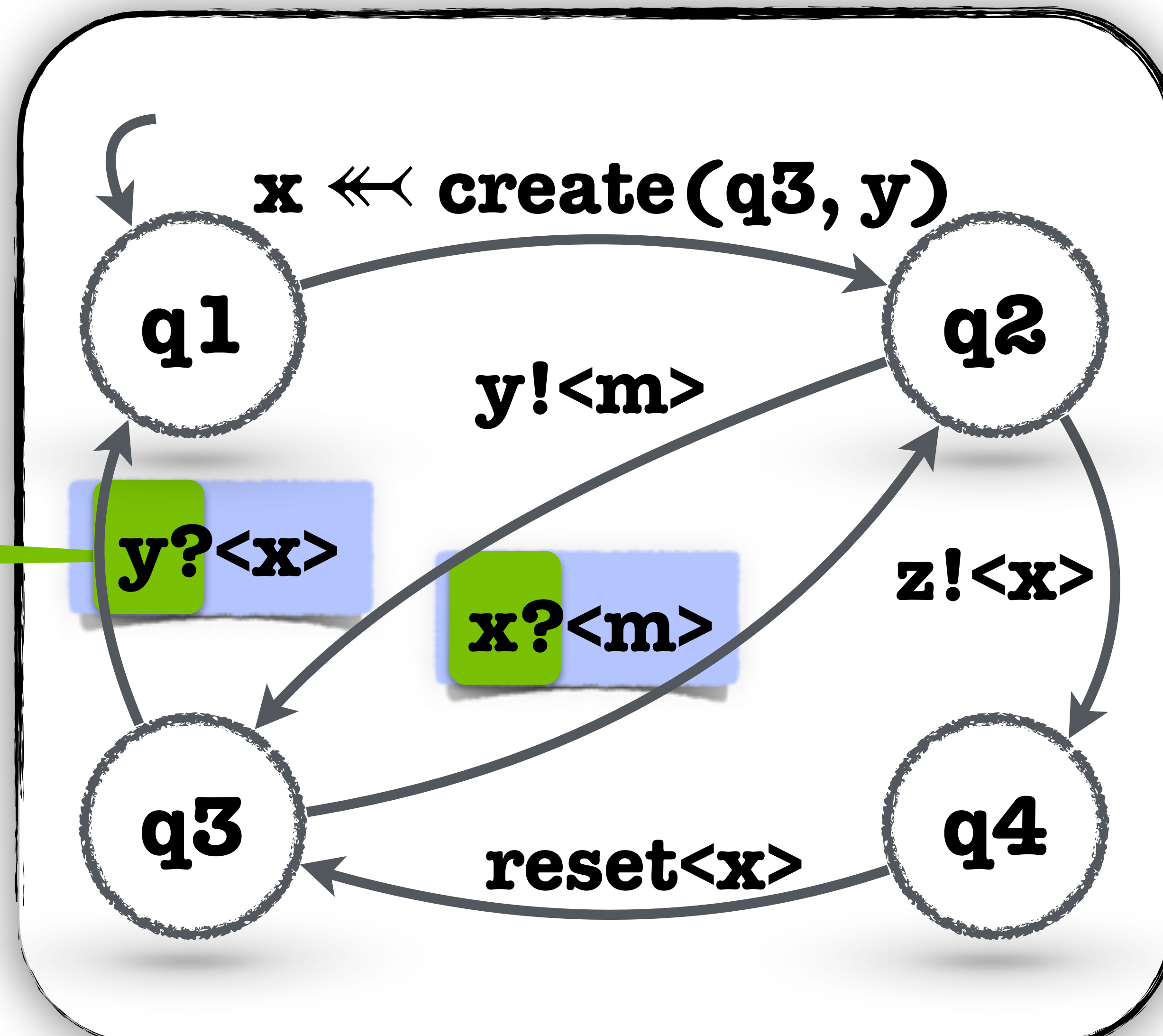
Process Model

Transition Relation

Process Creation

Send & Receive ID

Selective Receive



Dynamic Register Automata

Formal Model

Configuration

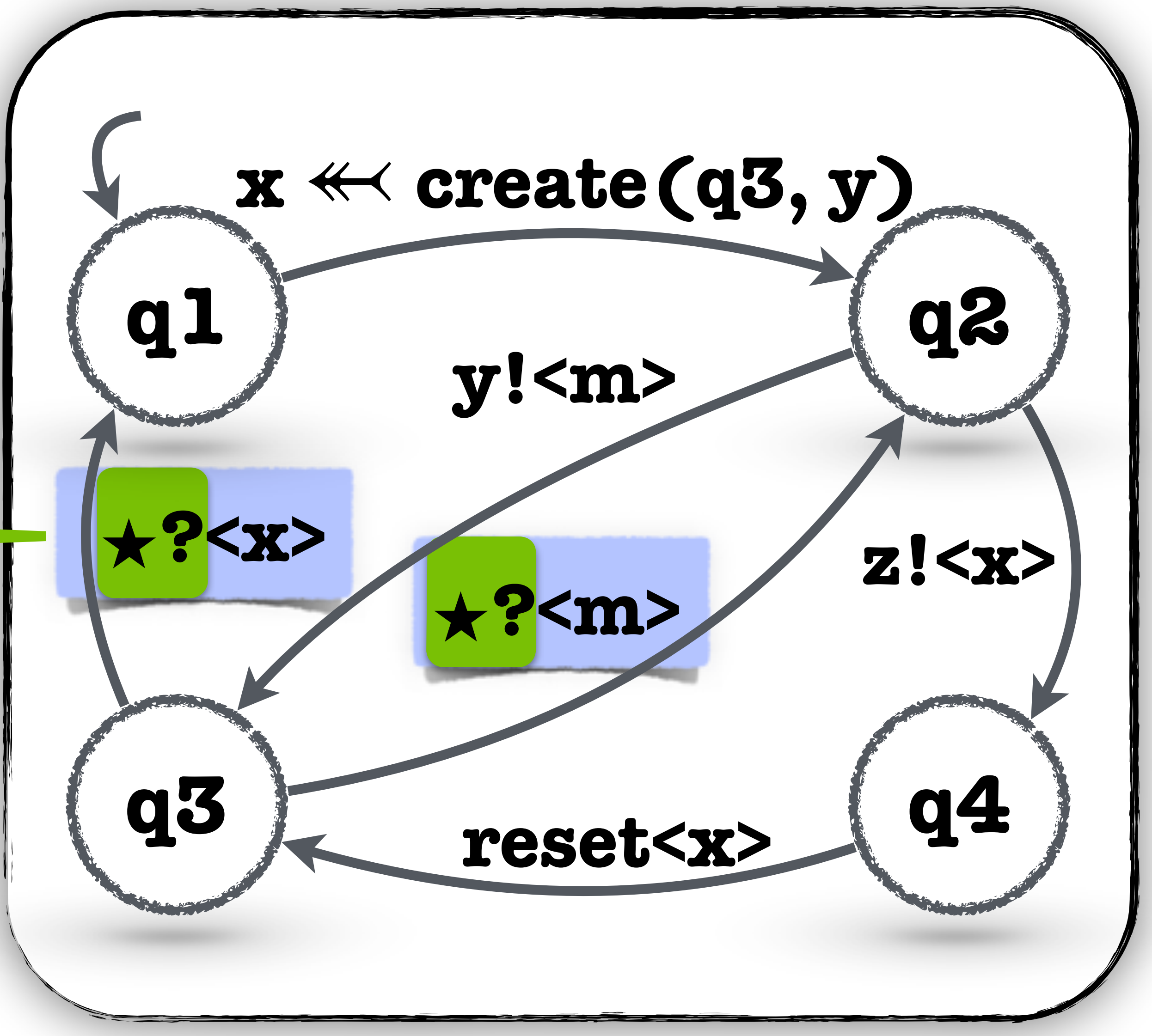
Process Model

Transition Relation

Process Creation

Send & Receive ID

Non Selective Receive



Dynamic Register Automata

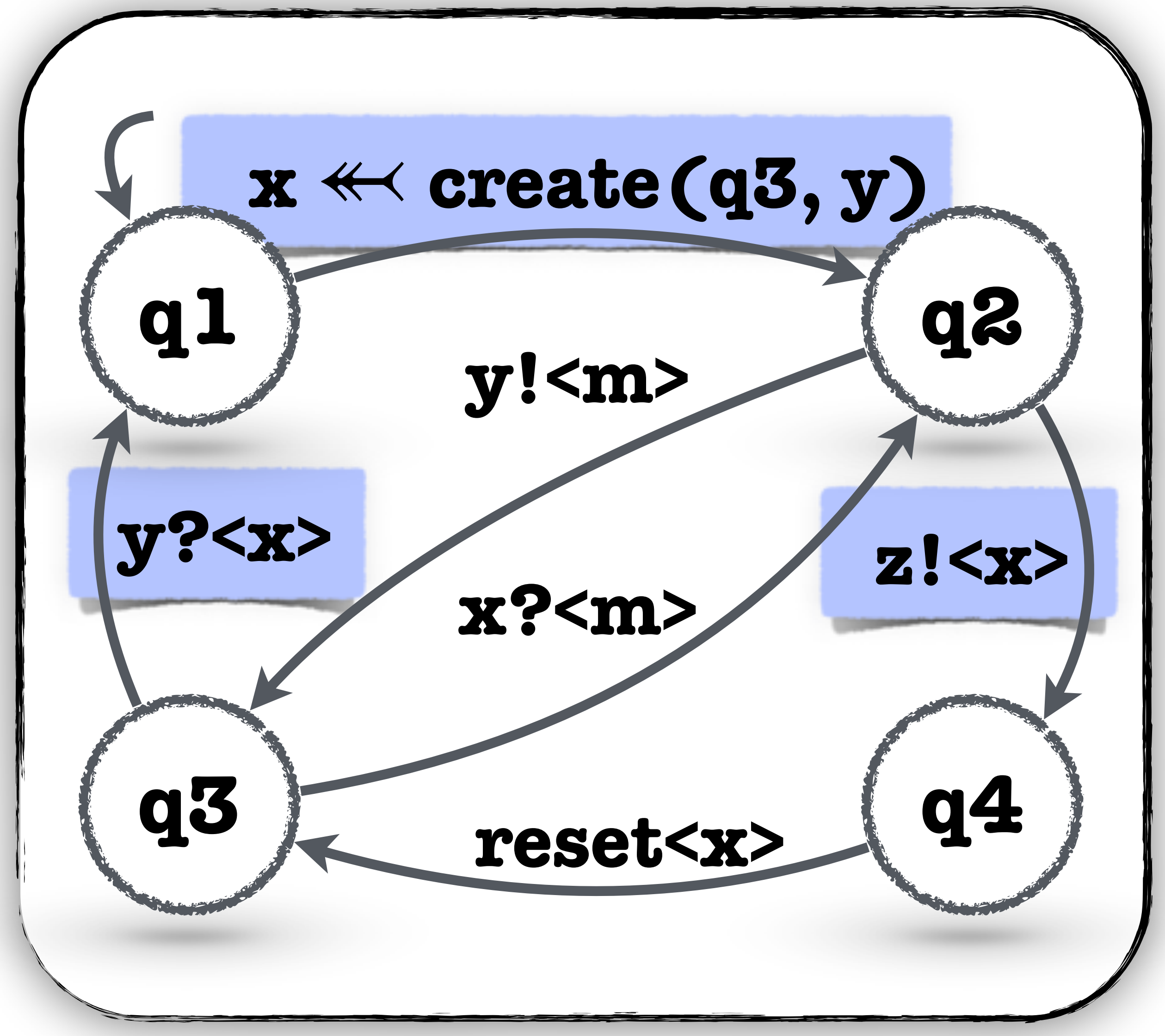
Formal Model

Configuration

Process Model

Transition Relation

- Process Creation
- Send & Receive ID



Dynamic Register Automata

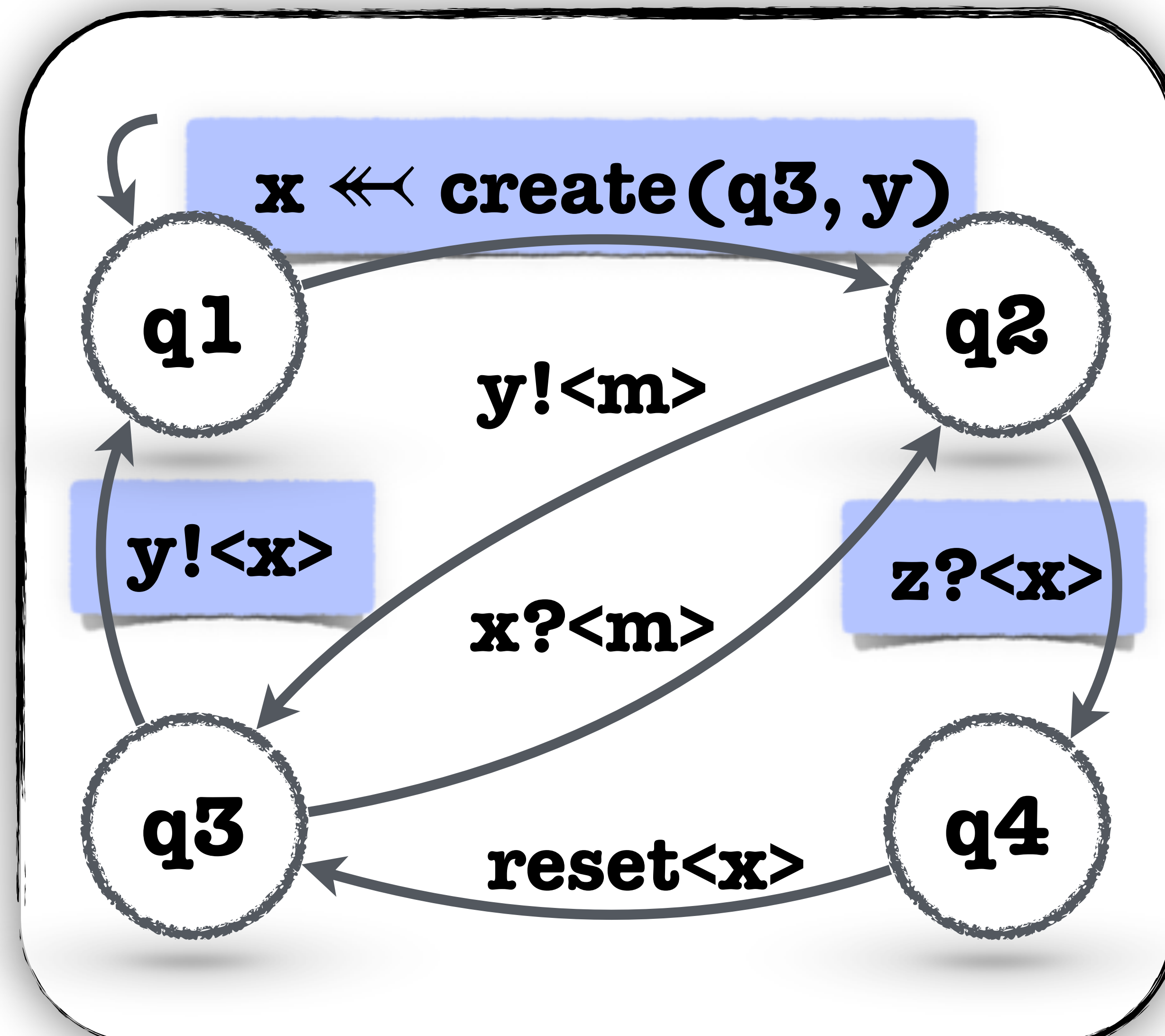
Formal Model

Configuration

Process Model

Transition Relation

- Process Creation
- Send & Receive ID
- Register Reset



Dynamic Register Automata

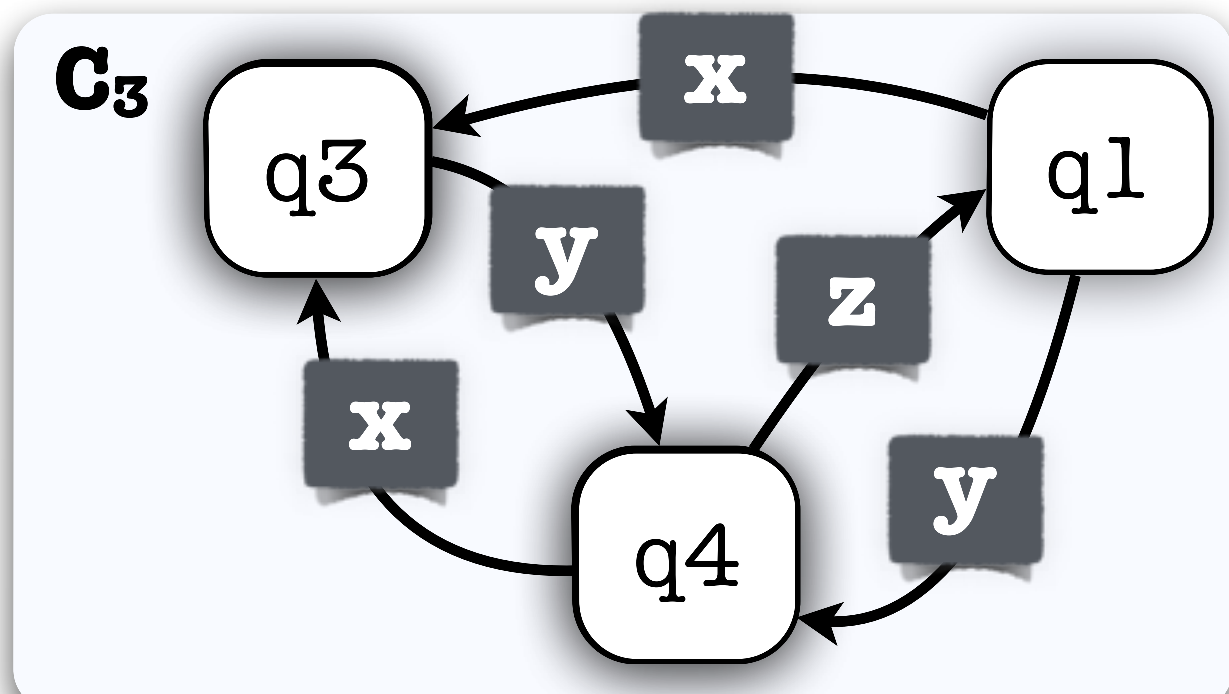
Formal Model

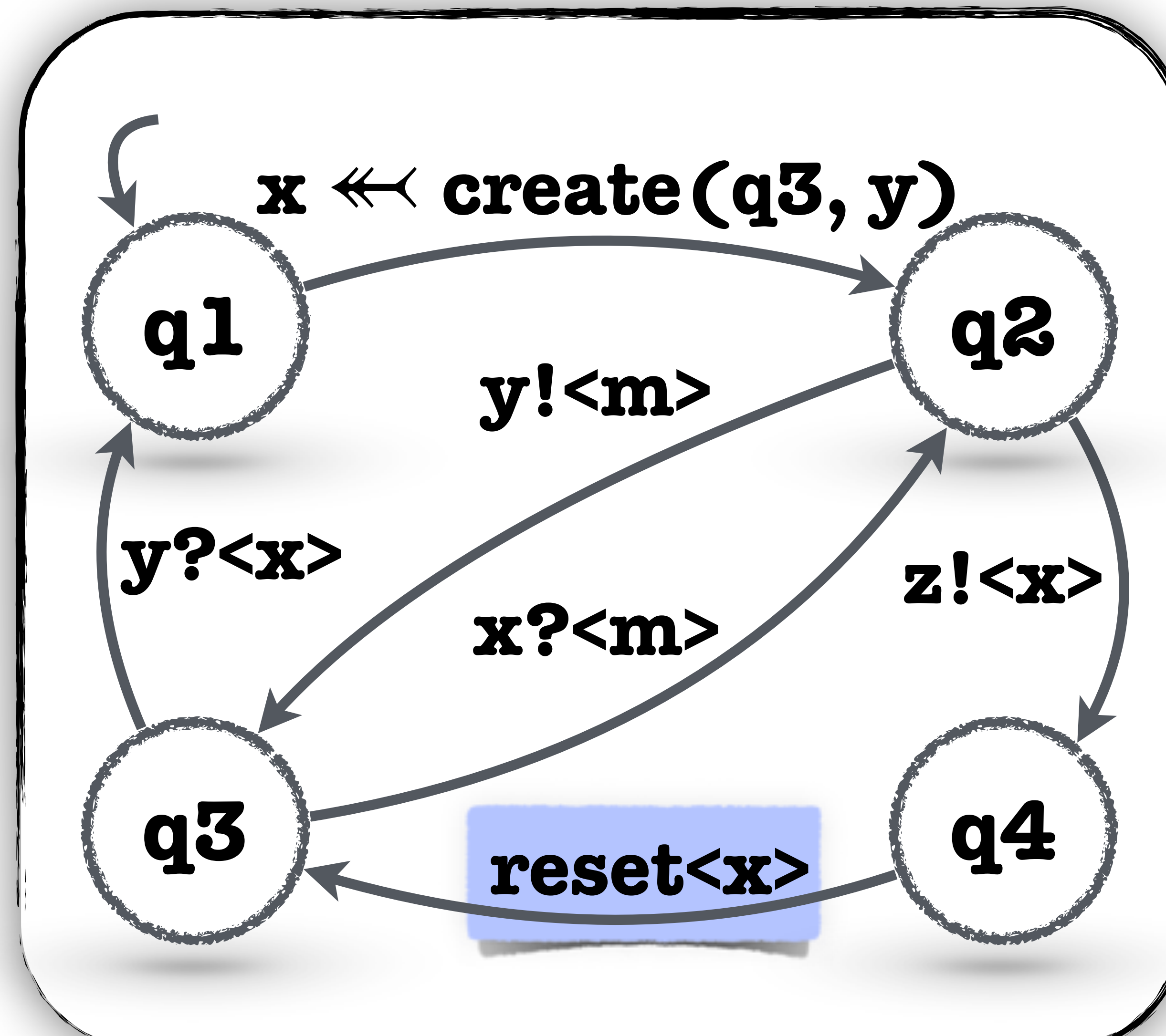
Configuration

Transition Relation

Register Reset

Process Model





Dynamic Register Automata

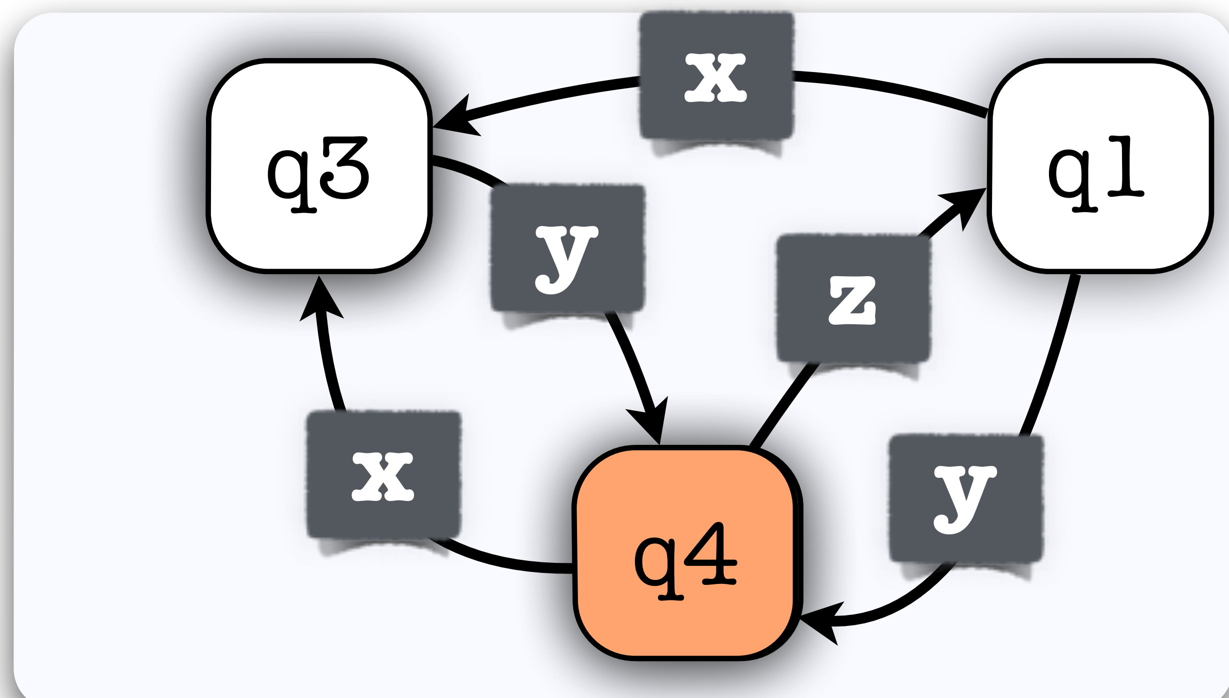
Formal Model

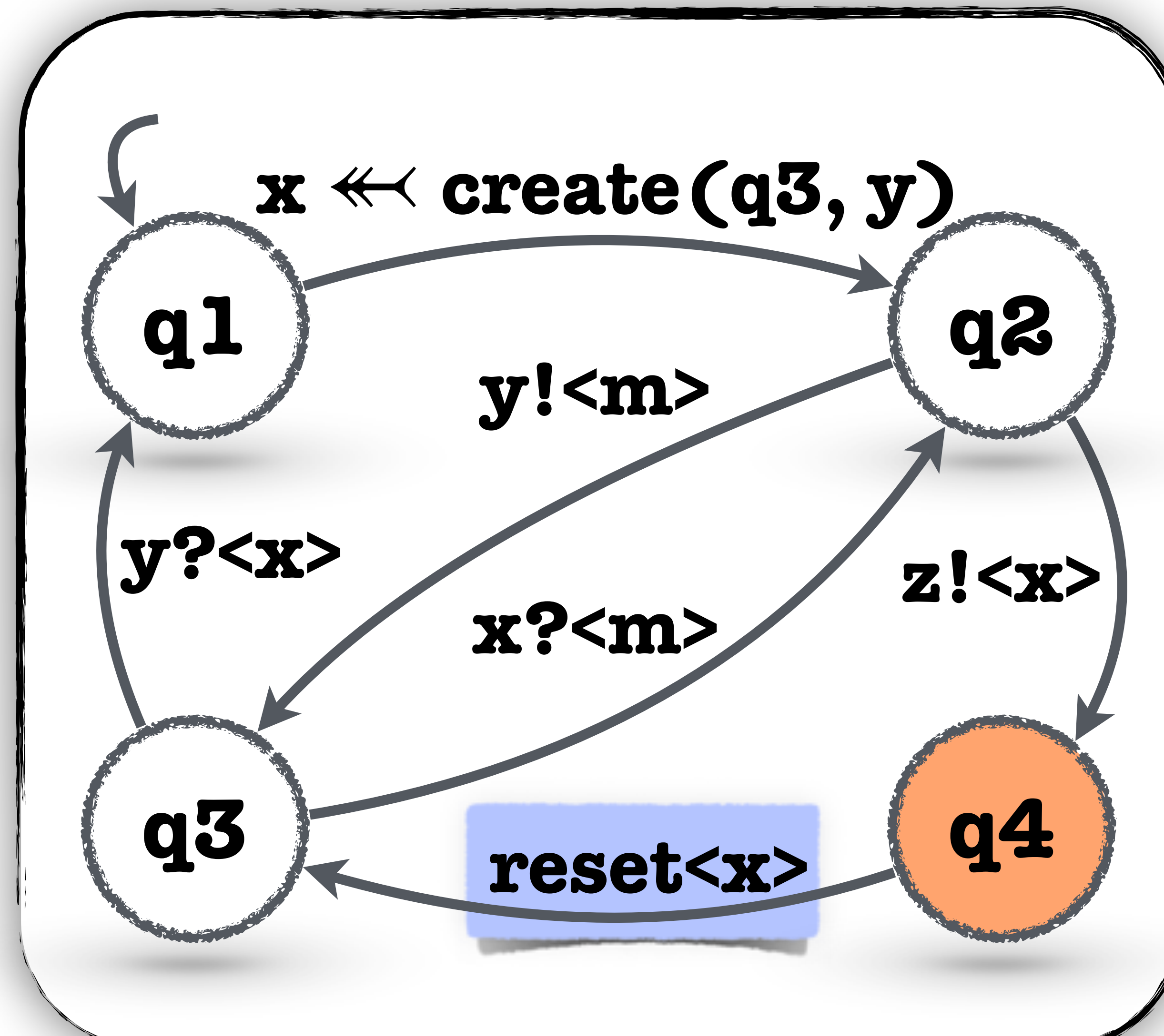
Configuration

Process Model

Transition Relation

Register Reset





Dynamic Register Automata

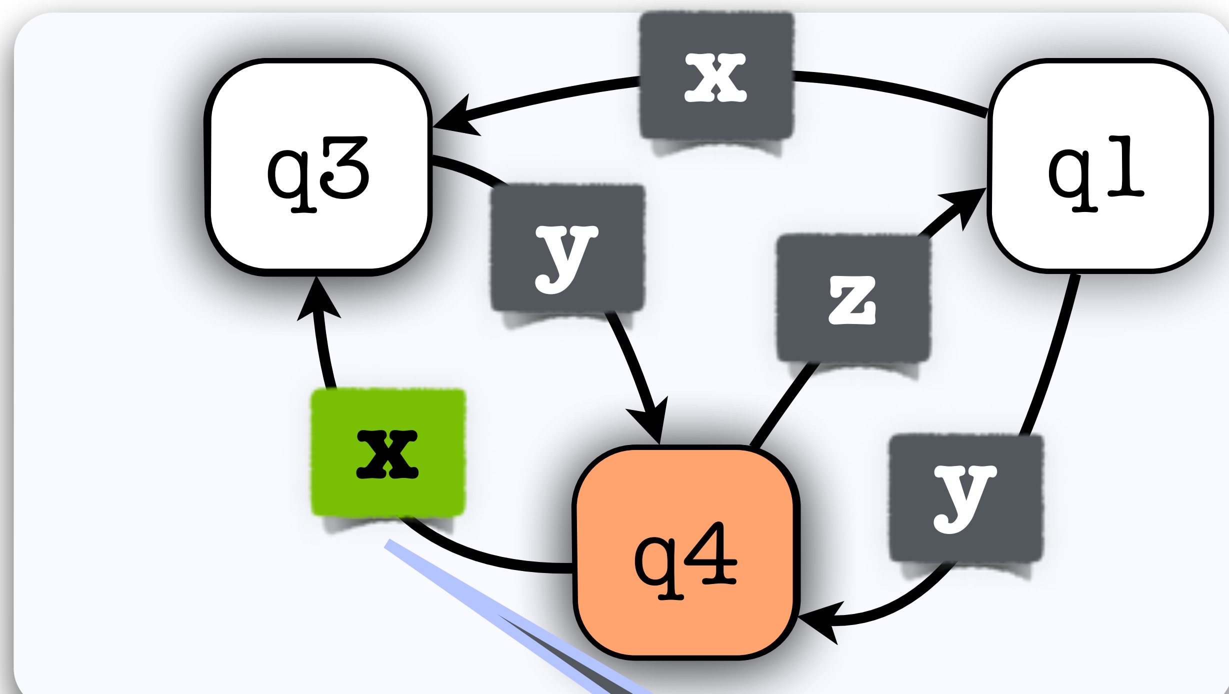
Formal Model

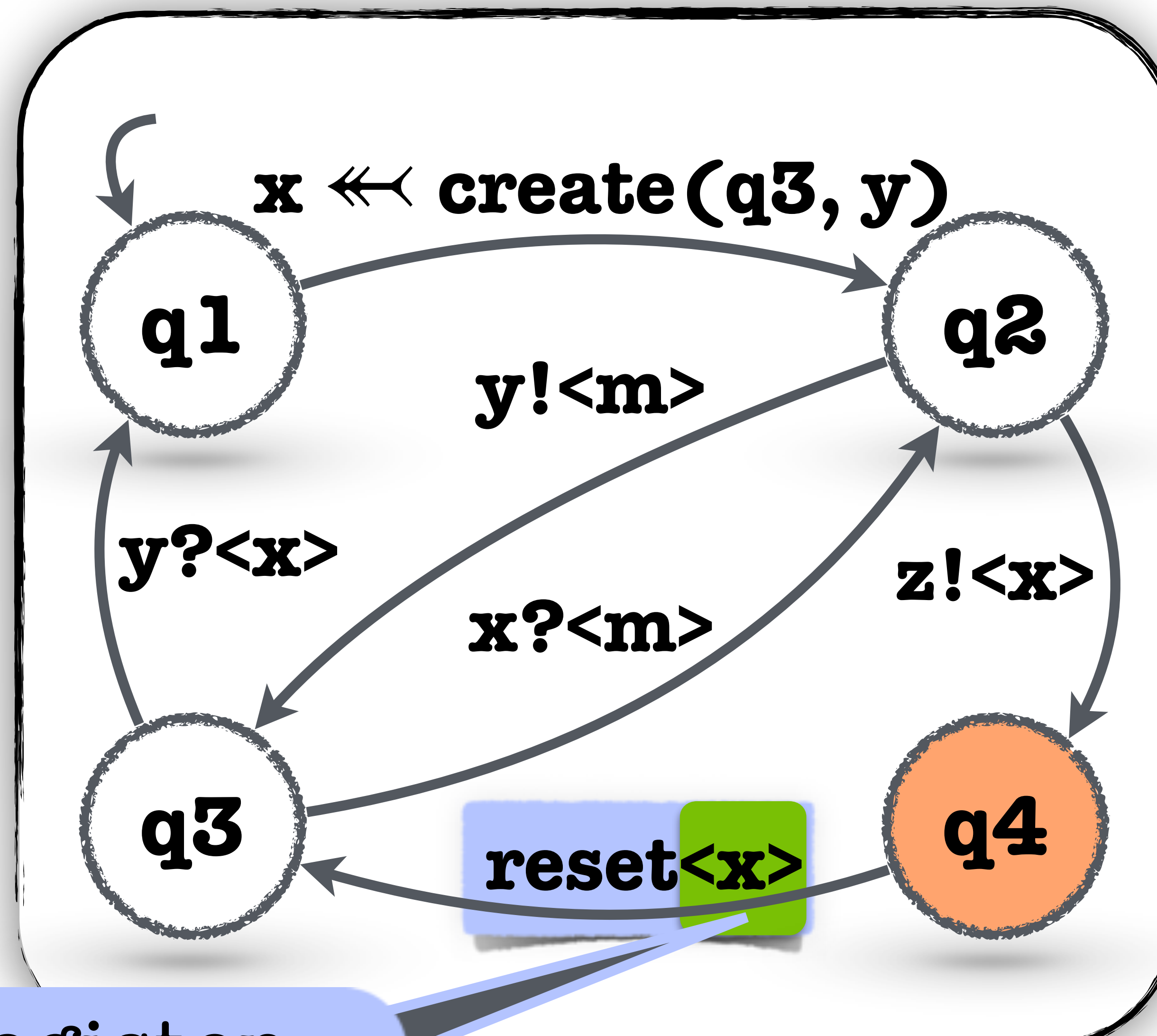
Configuration

Transition Relation

Process Model

Register Reset





Which register

Dynamic Register Automata

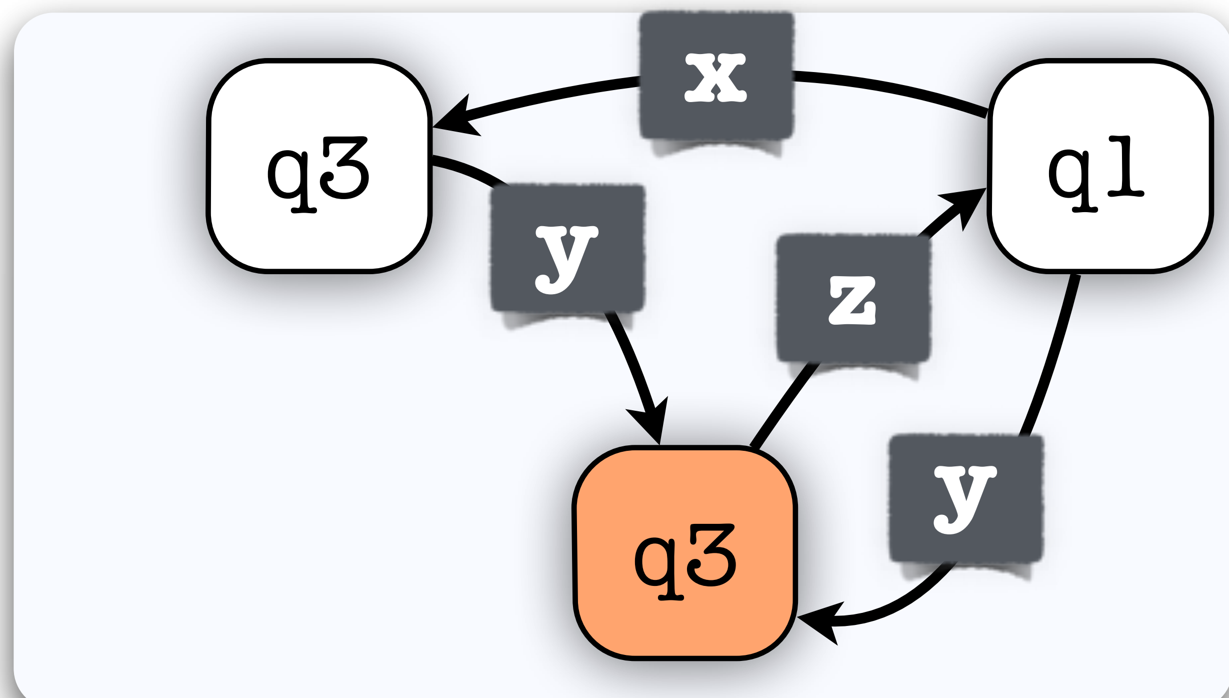
Formal Model

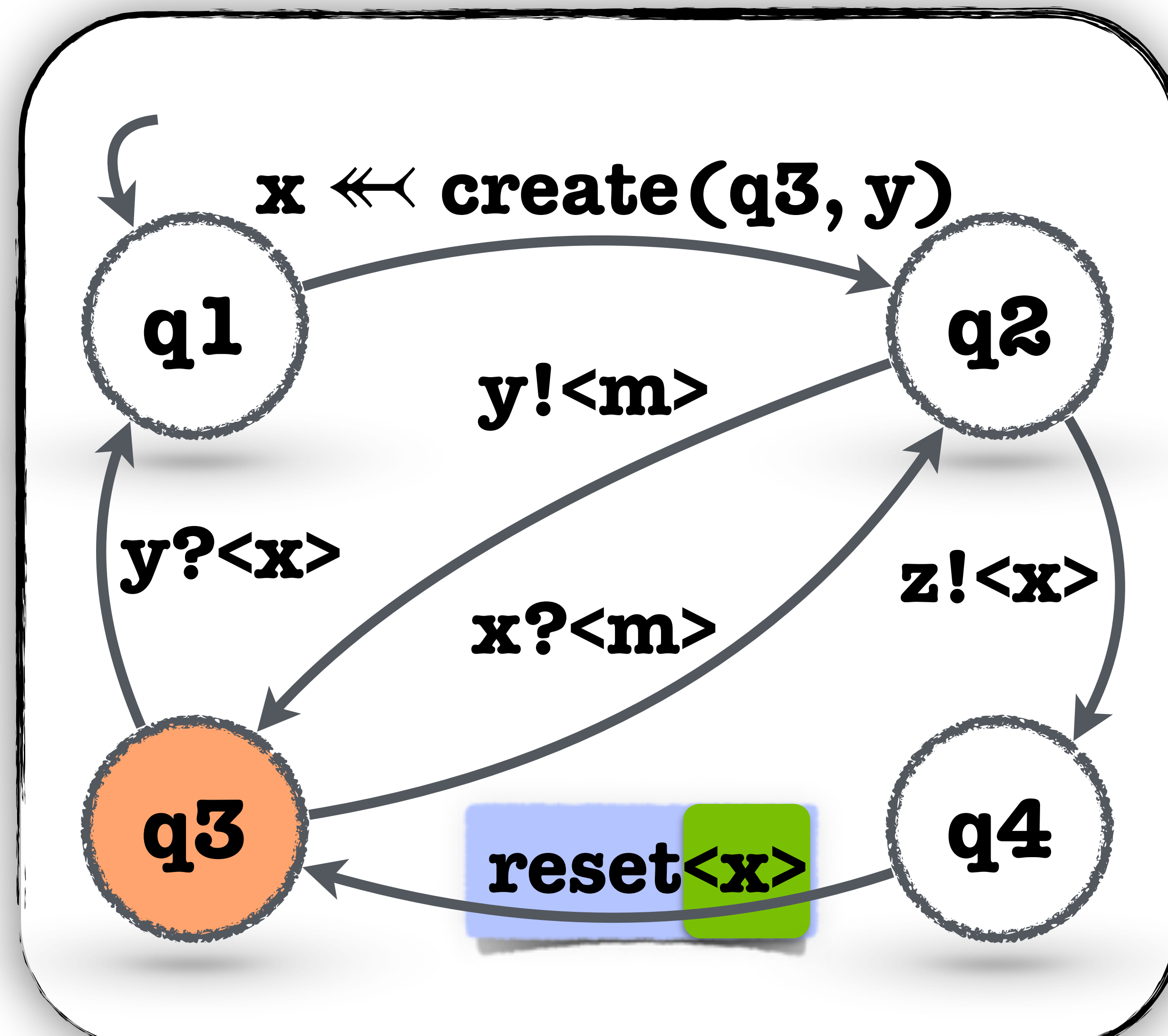
Configuration

Transition Relation

Register Reset

Process Model



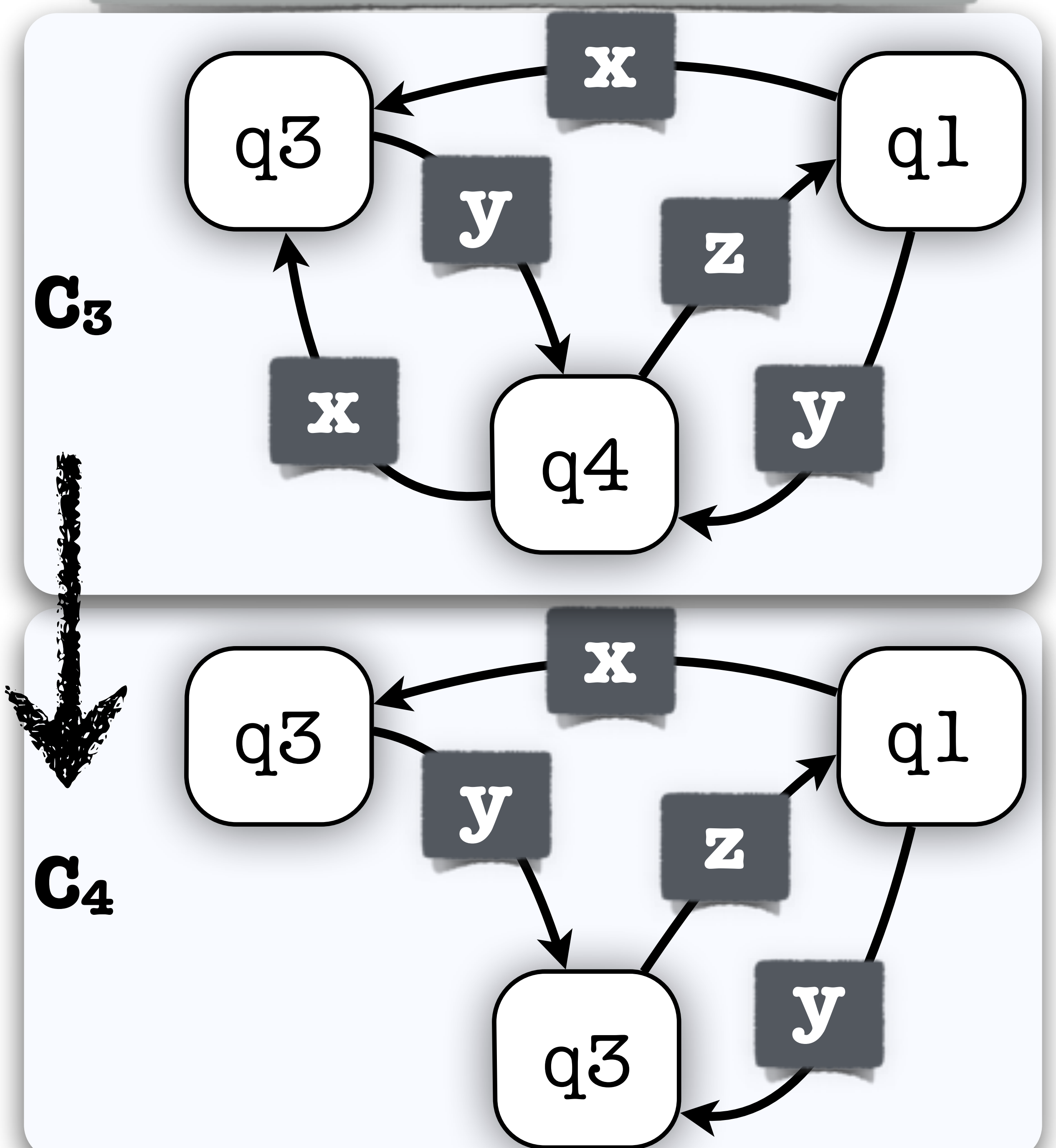


Dynamic Register Automata

Formal Model

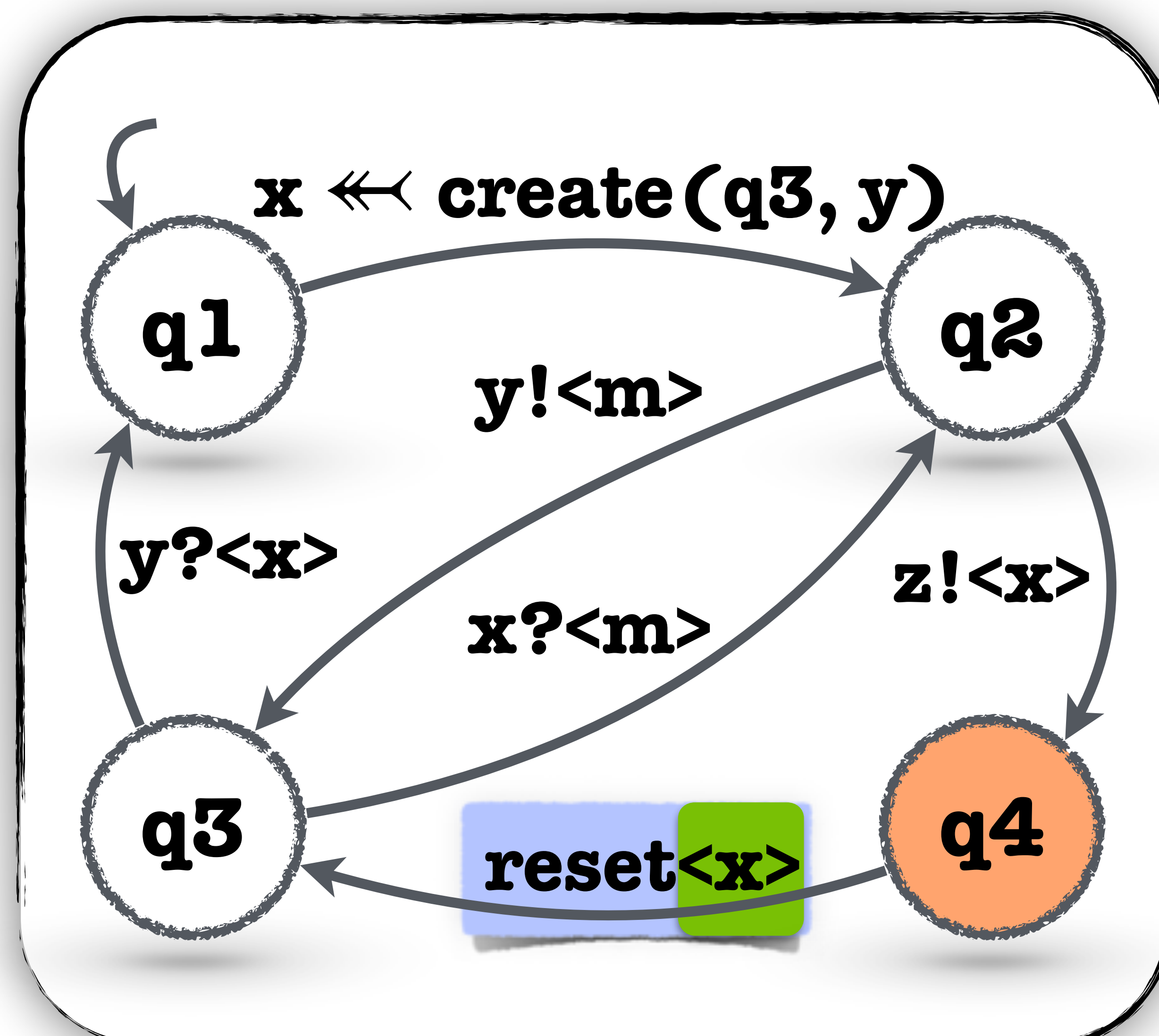
Configuration

Transition Relation



Process Model

Register Reset



Dynamic Register Automata

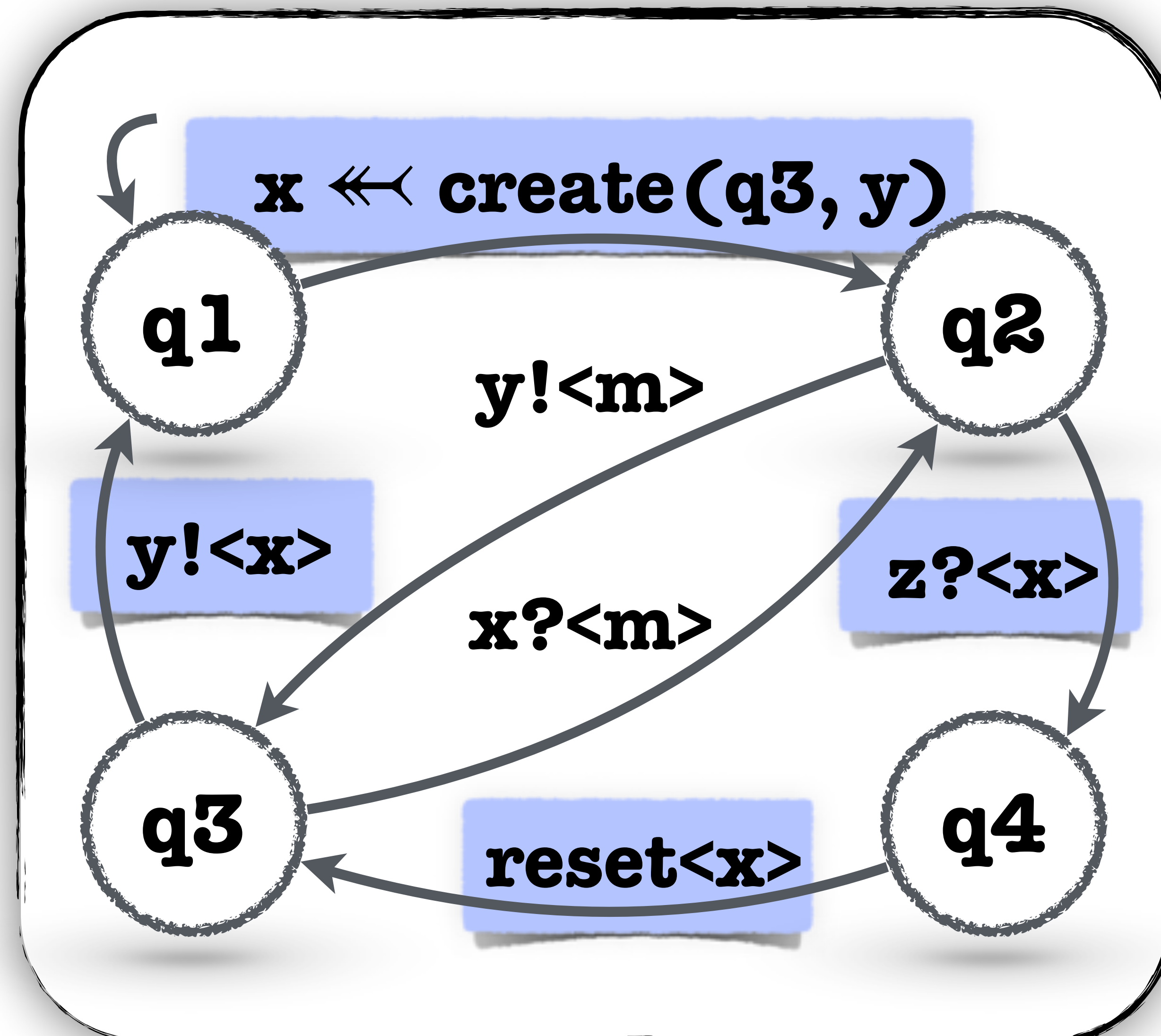
Formal Model

Configuration

Process Model

Transition Relation

- Process Creation
- Send & Receive ID
- Register Reset



Dynamic Register Automata

Applications

Formal Model

- **Process Model**
- **Configuration**
- **Transition Relation**

Dynamic Register Automata

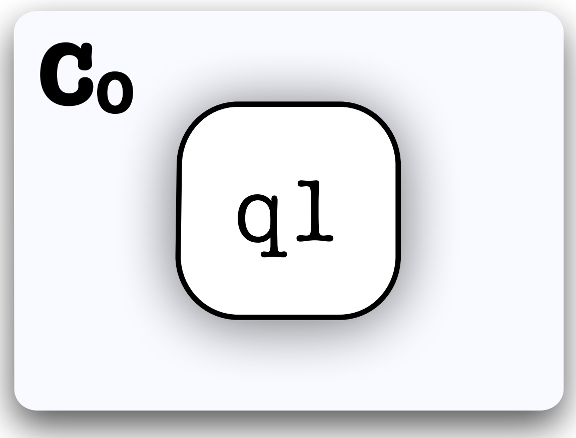
Applications

Formal Model

State Reachability

Dynamic Register Automata

State Reachability

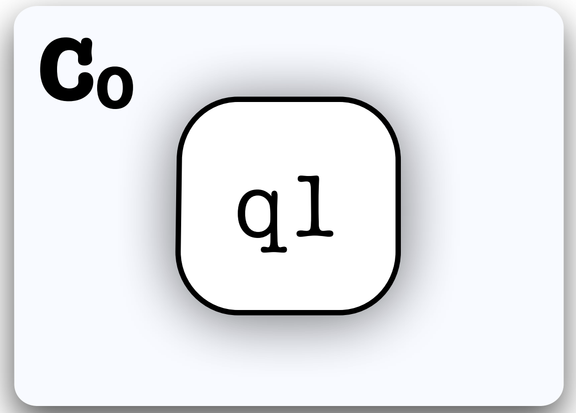


Initial Configuration

Dynamic Register Automata

State Reachability

Initial Configuration

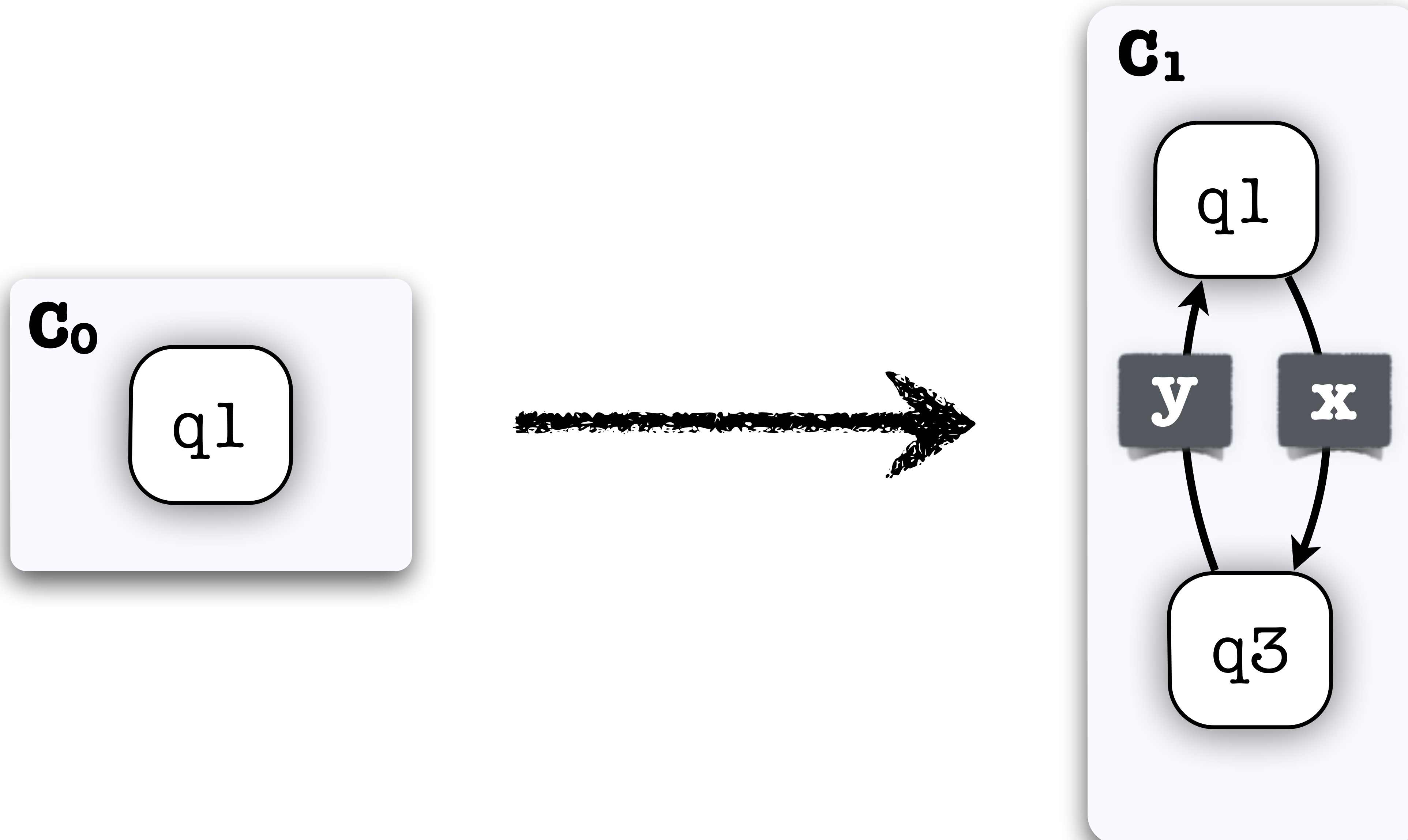


Run: C_0

Dynamic Register Automata

State Reachability

Initial Configuration

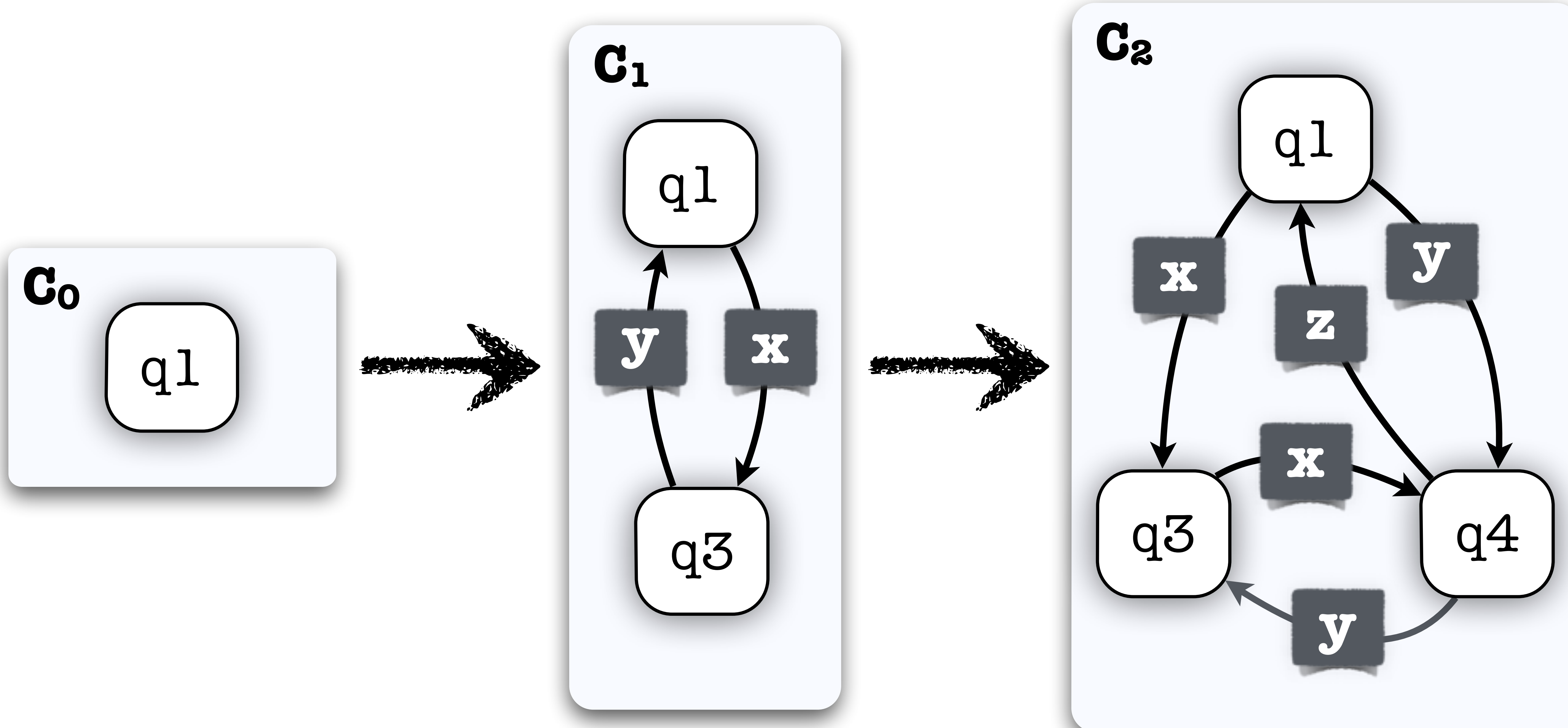


Run: C_0, C_1

Dynamic Register Automata

State Reachability

Initial Configuration

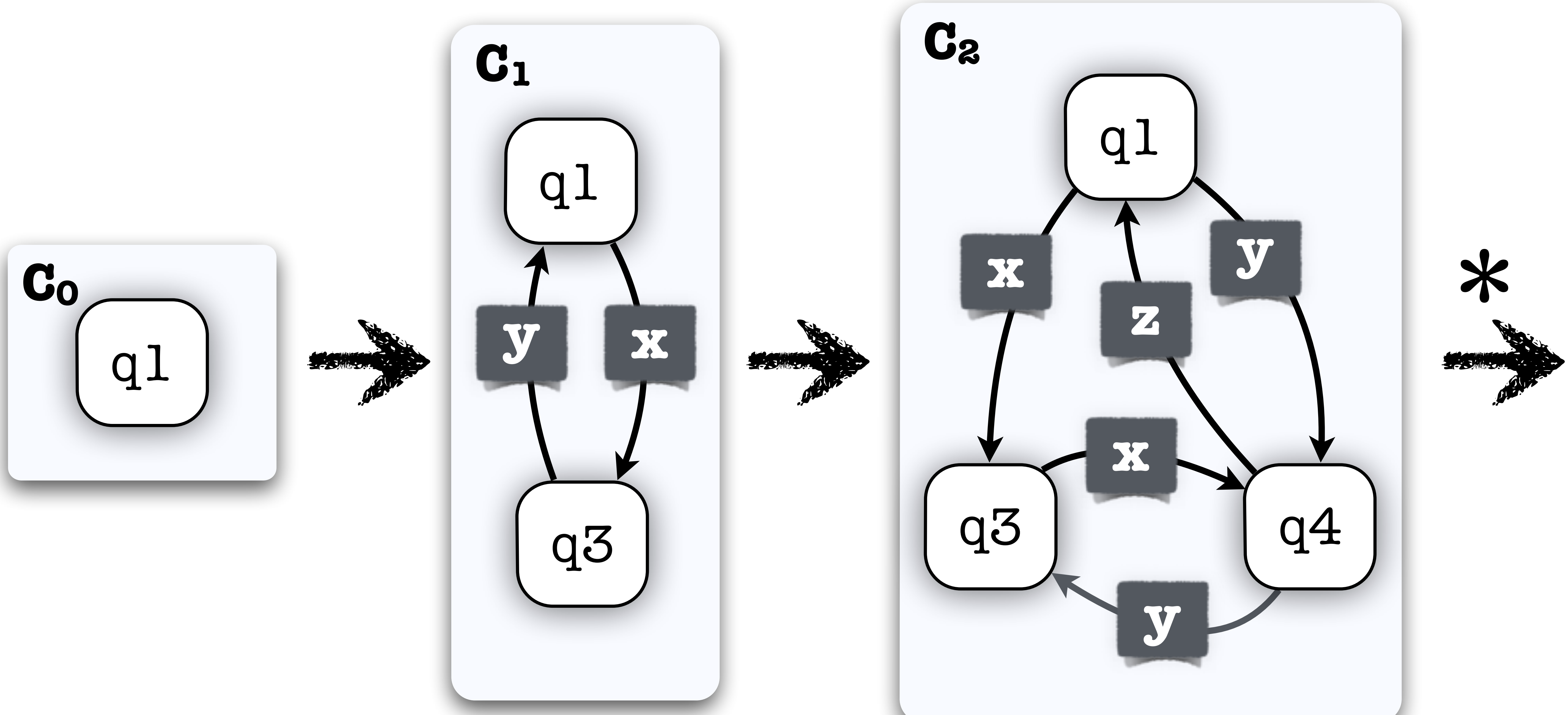


Run: C_0, C_1, C_2

Dynamic Register Automata

State Reachability

Initial Configuration

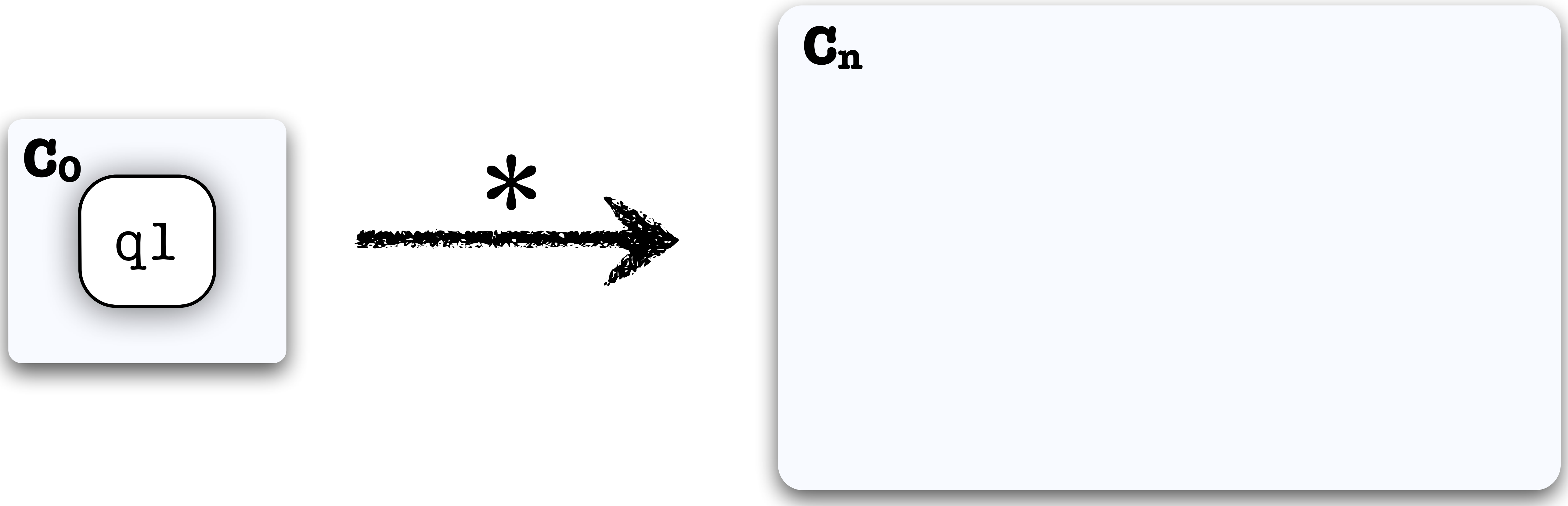


Run: $C_0, C_1, C_2, \ldots$

Dynamic Register Automata

State Reachability

Initial Configuration



Run: C_0, C_1, C_2, … , C_n

Dynamic Register Automata

State Reachability

Initial Configuration

Run: C_0, C_1, C_2, ... , C_n

State Reachability Problem:

Dynamic Register Automata

State Reachability

Initial Configuration

Run: $C_0, C_1, C_2, \ldots, C_n$

State Reachability Problem:

Given a control state q_{BAD}, is there a run starting from the initial configuration that reaches a configuration where q_{BAD} occurs.

Dynamic Register Automata

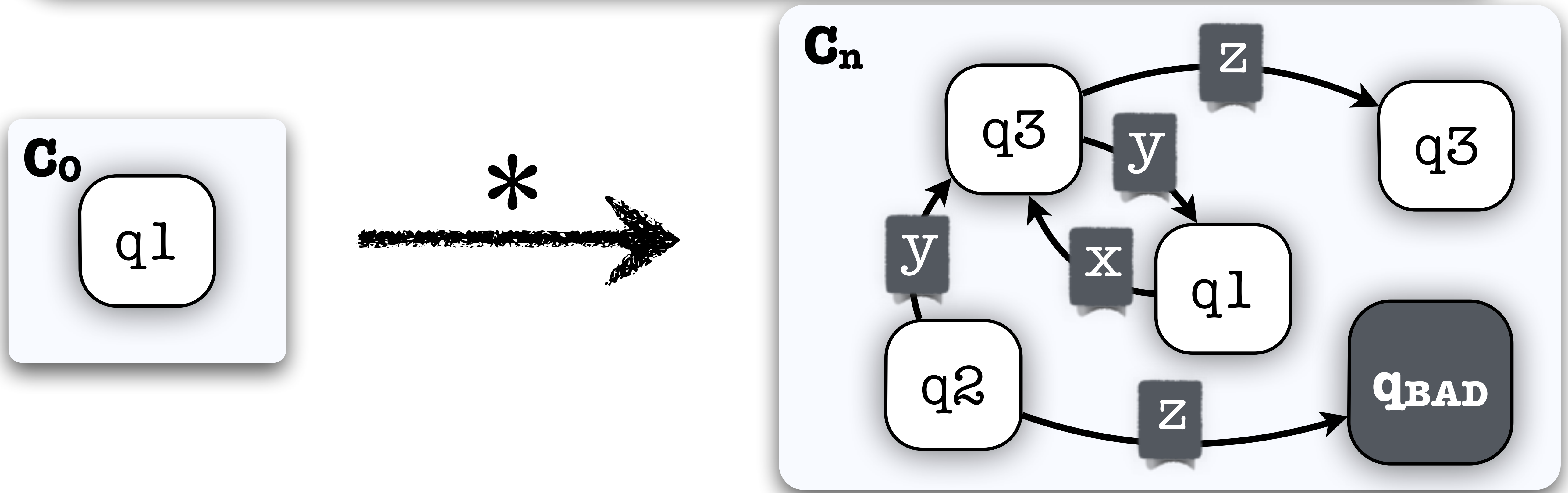
State Reachability

Initial Configuration

Run: $C_0, C_1, C_2, \ldots, C_n$

State Reachability Problem:

Given a control state q_{BAD}, is there a run starting from the initial configuration that reaches a configuration where q_{BAD} occurs.



Dynamic Register Automata

State Reachability

Initial Configuration

Run: $C_0, C_1, C_2, \ldots, C_n$

State Reachability Problem:

Given a control state $\mathbf{q_{BAD}}$, is there a run starting from the initial configuration that reaches a configuration where $\mathbf{q_{BAD}}$ occurs.

Undecidable

Dynamic Register Automata

Applications

Formal Model

State Reachability

Undecidable

Contribution

State Reachability

Study of the decidability and complexity for different sub-classes of the problem

Contribution

State Reachability

Study of the decidability and complexity for different sub-classes of the problem

Bounded DRA **Undecidable**

Contribution

State Reachability

Study of the decidability and complexity for different sub-classes of the problem

Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**

Contribution

State Reachability

Study of the decidability and complexity for different sub-classes of the problem

Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable**
	Non-Primitive Recursive

Contribution

State Reachability

Study of the decidability and complexity for different sub-classes of the problem

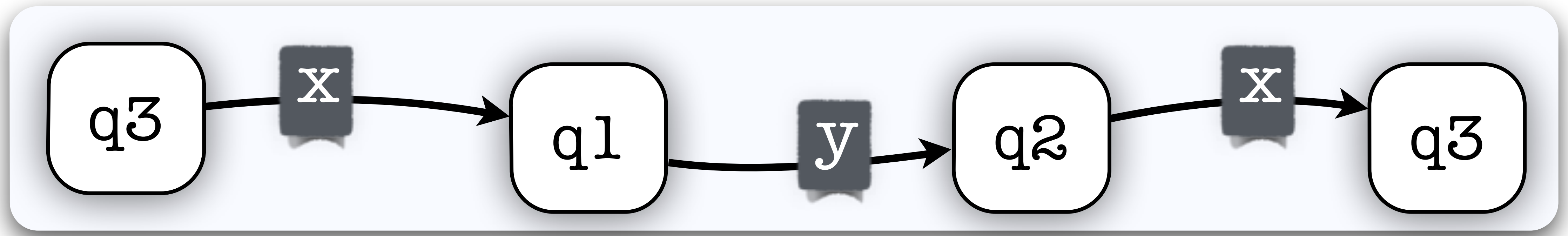
Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable**
	Non-Primitive Recursive

Bounded DRA

Bound the Simple Path Length of the configuration graph

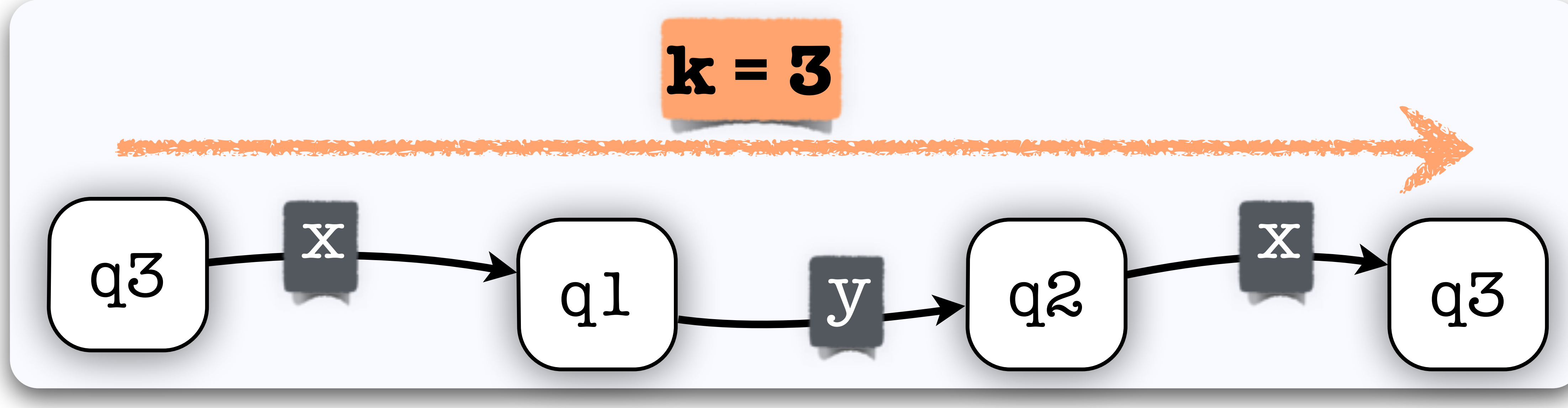
Bounded DRA

Bound the Simple Path Length of the configuration graph



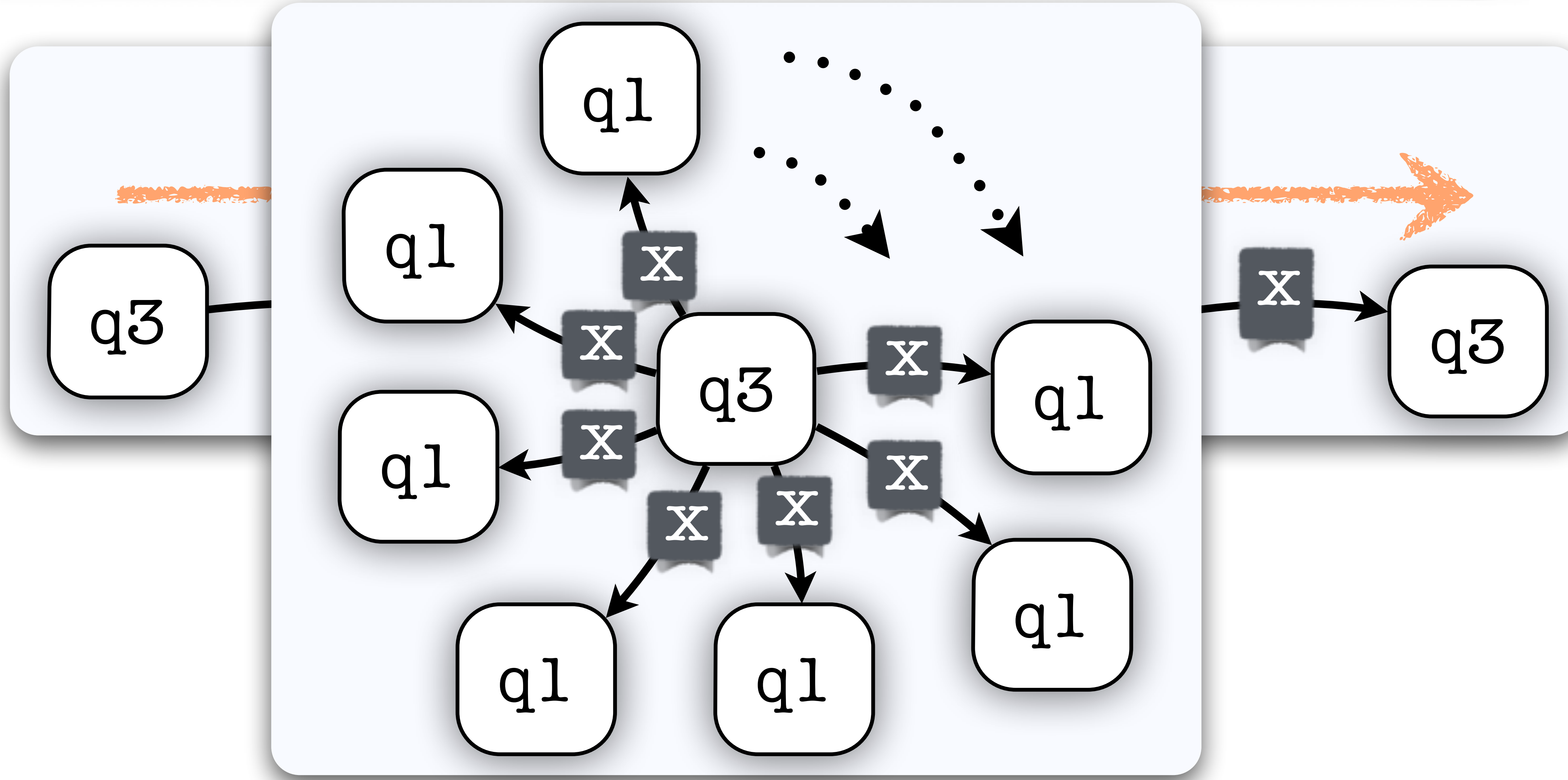
Bounded DRA

Bound the Simple Path Length of the configuration graph



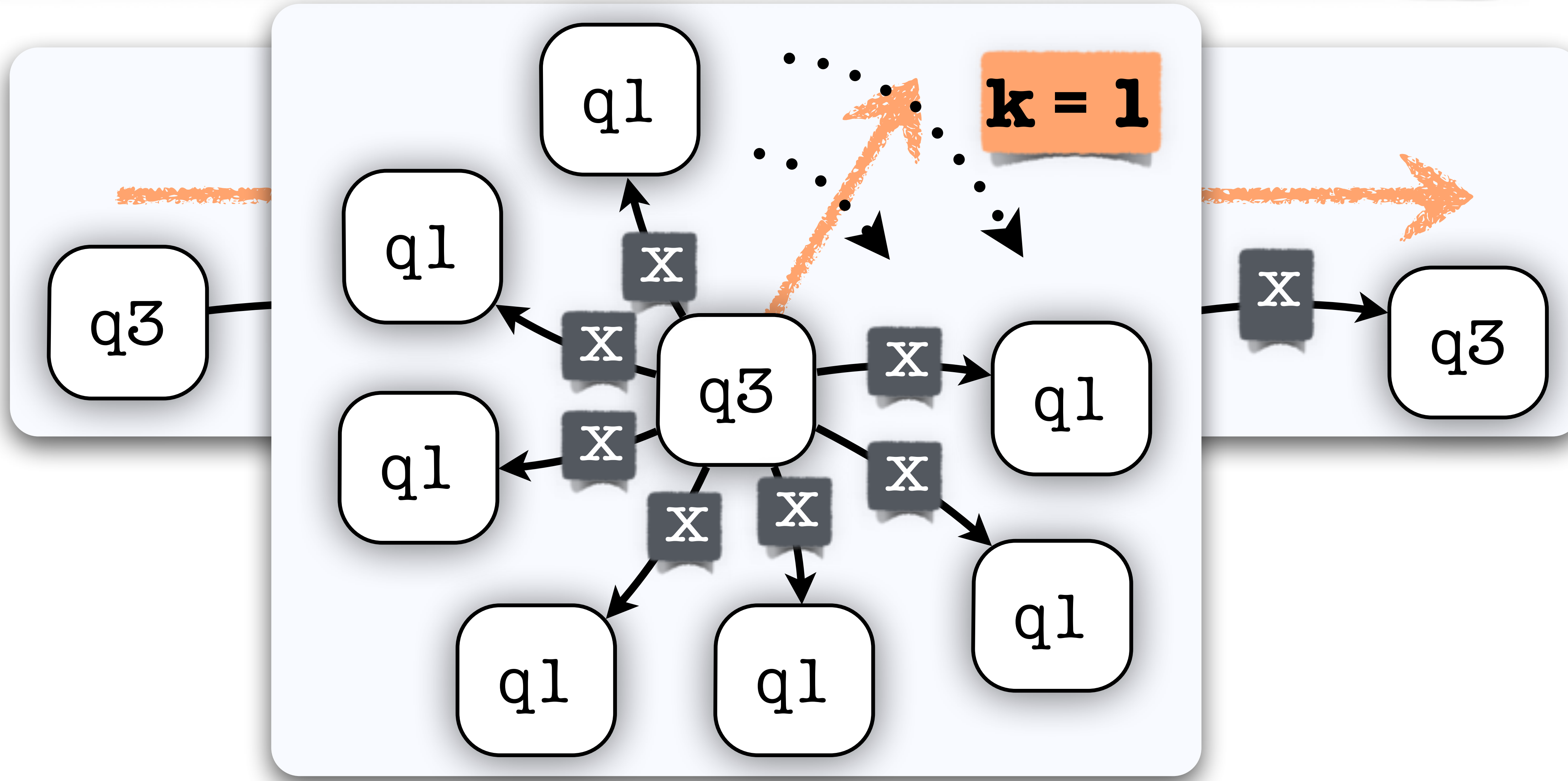
Bounded DRA

Bound the Simple Path Length of the configuration graph



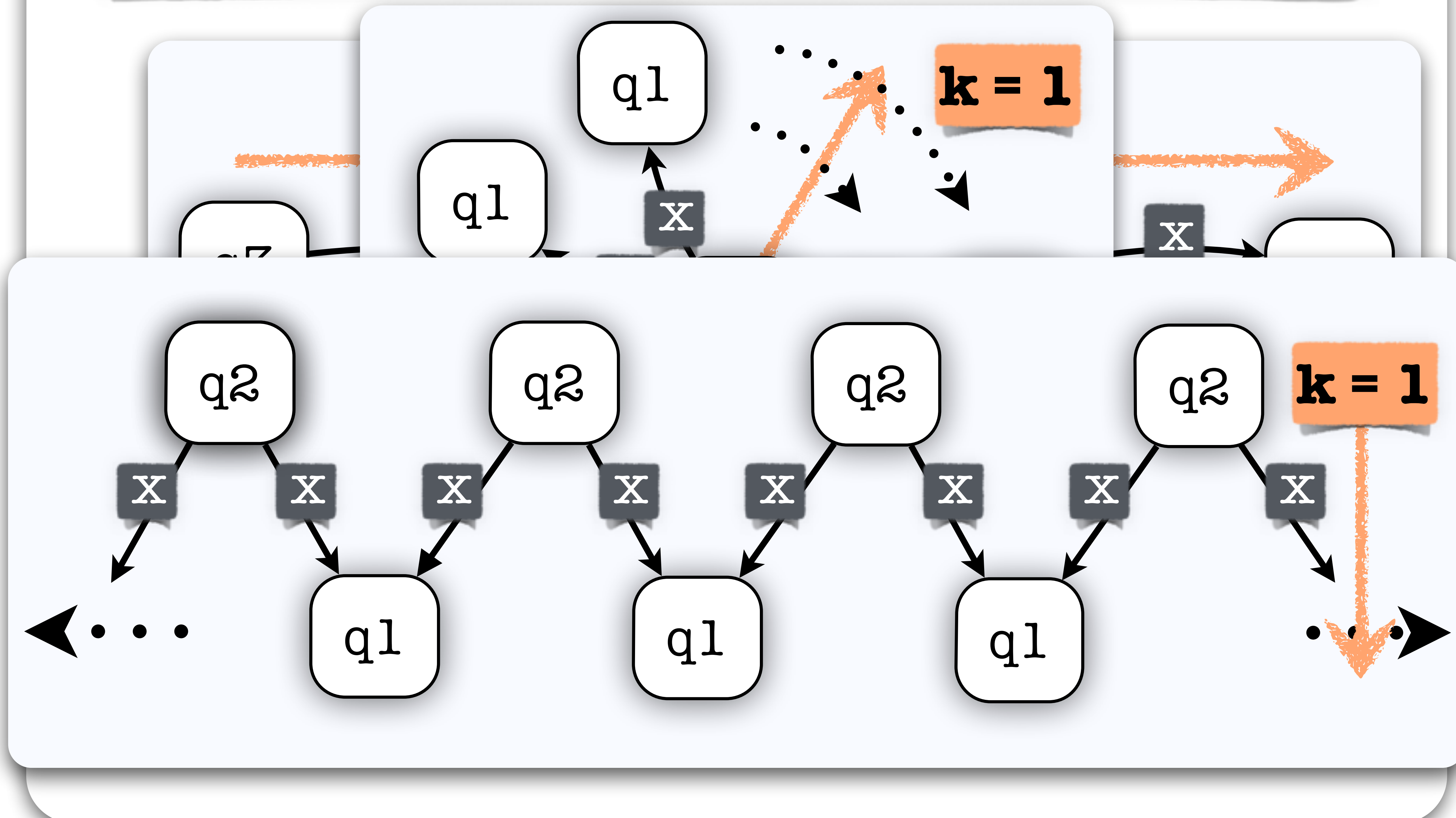
Bounded DRA

Bound the Simple Path Length of the configuration graph



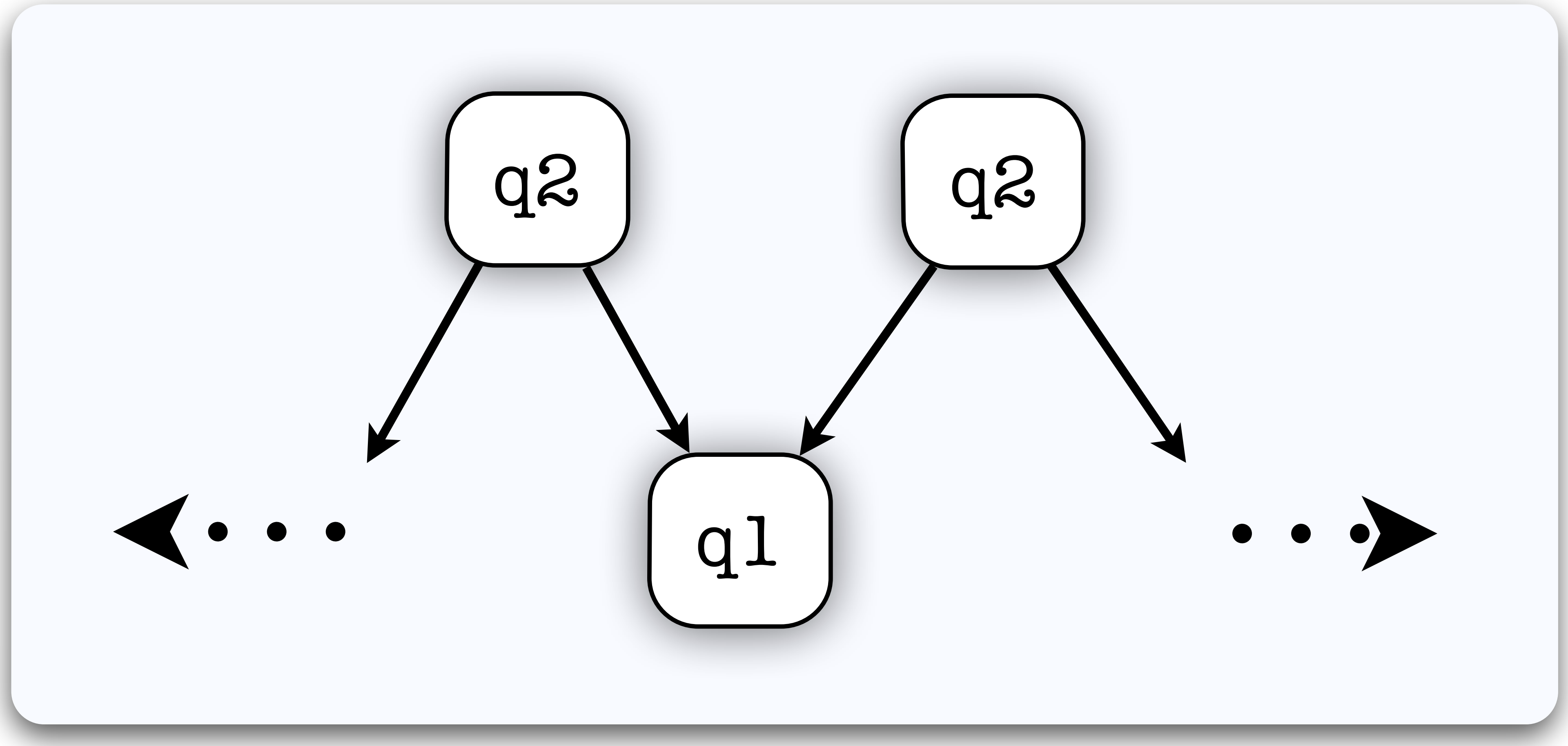
Bounded DRA

Bound the Simple Path Length of the configuration graph



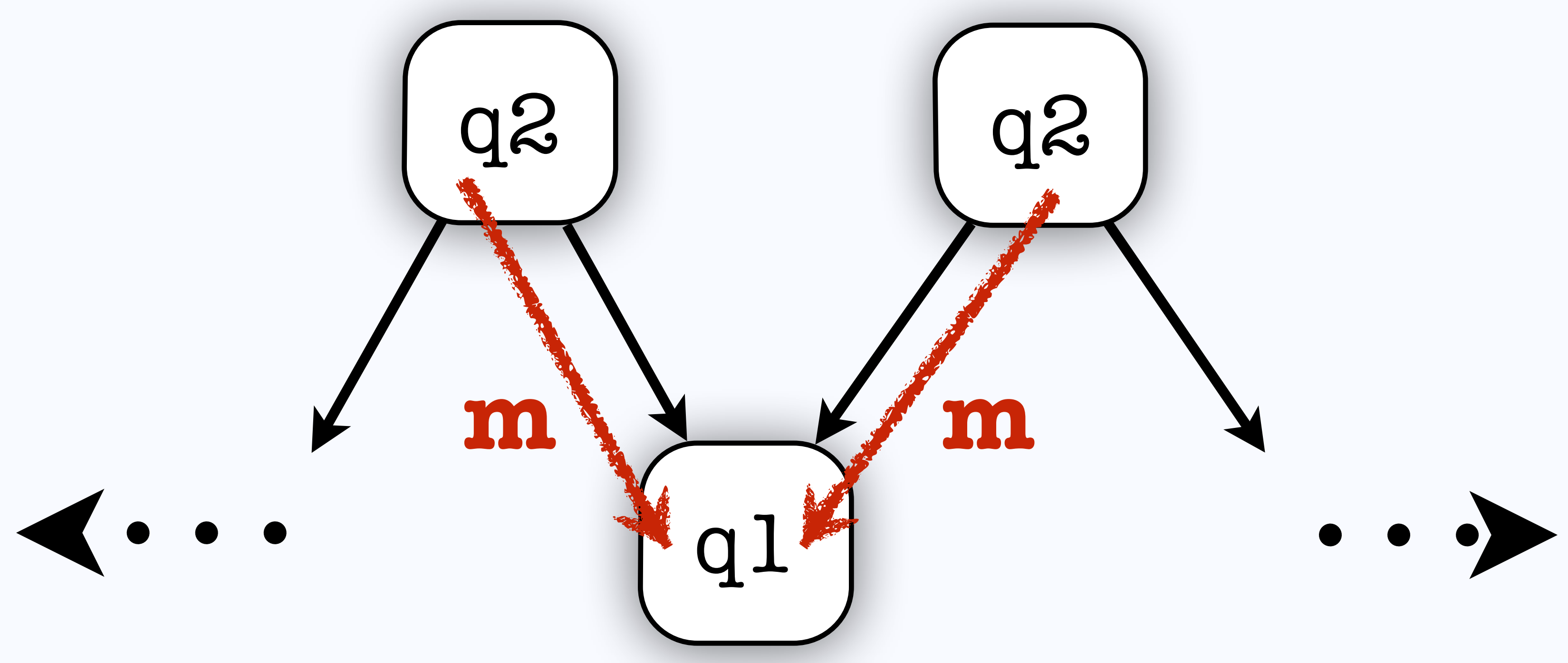
Bounded DRA

Bound the Simple Path Length of the configuration graph



Bounded DRA

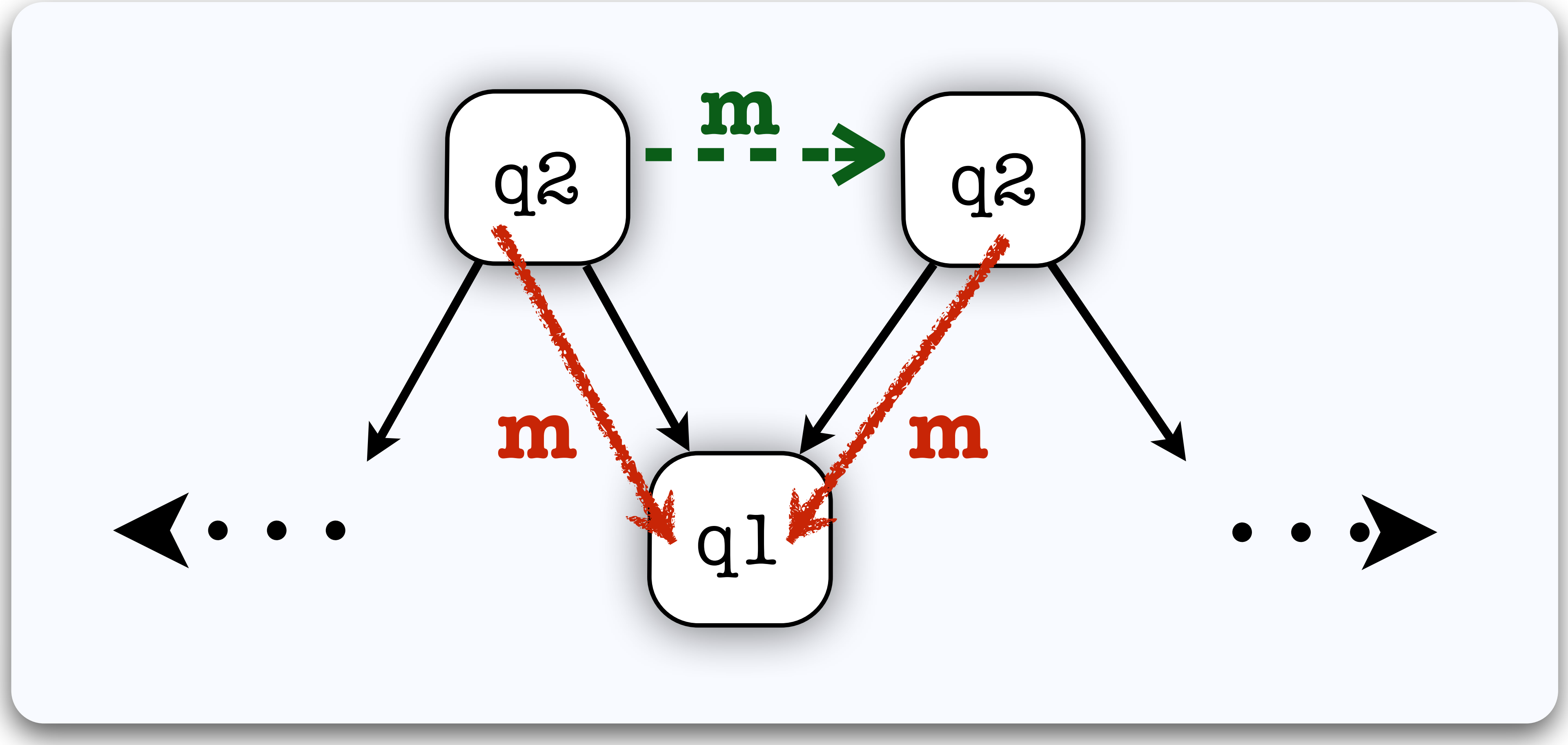
Bound the Simple Path Length of the configuration graph



Using Rendez-Vous Communication

Bounded DRA

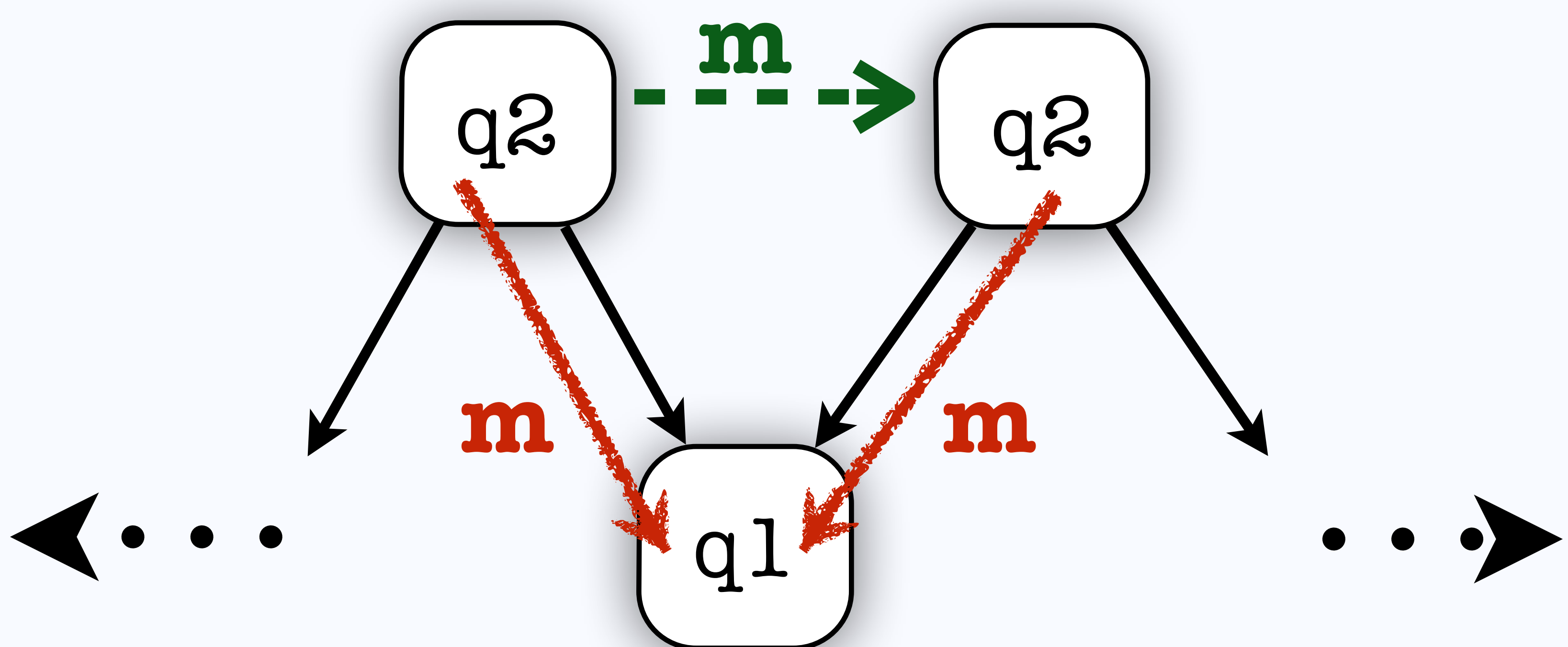
Bound the Simple Path Length of the configuration graph



Using Rendez-Vous Communication

Bounded DRA

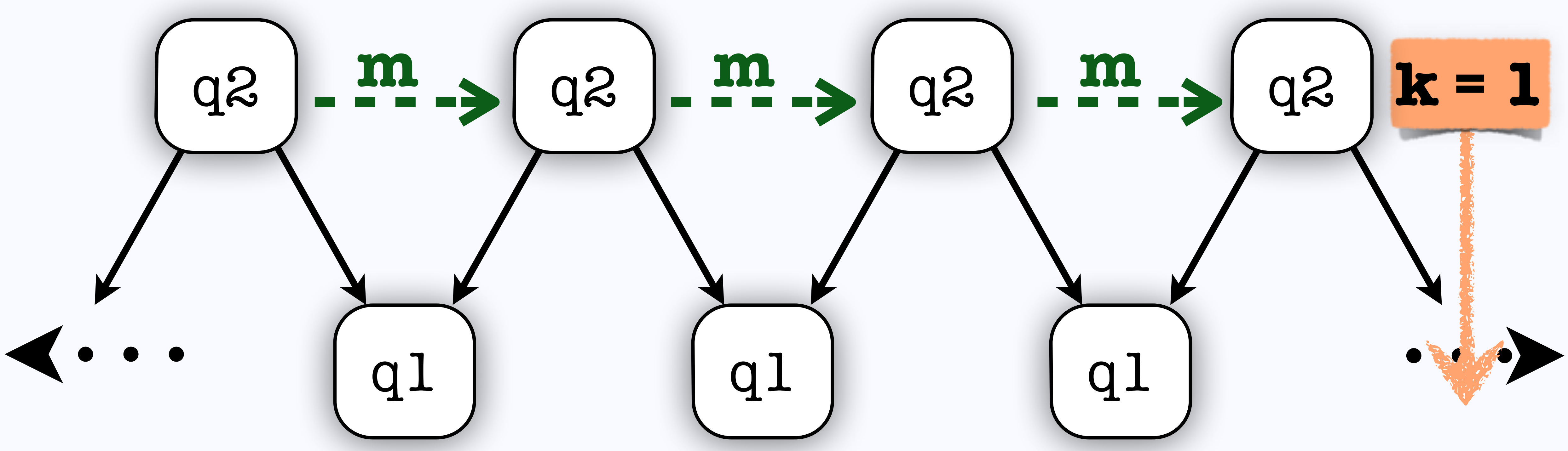
Bound the Simple Path Length of the configuration graph



Using Rendez-Vous Communication

Bounded DRA

Bound the Simple Path Length of the configuration graph



Undecidable

Contribution

State Reachability

Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable**
	Non-Primitive Recursive

Contribution

State Reachability

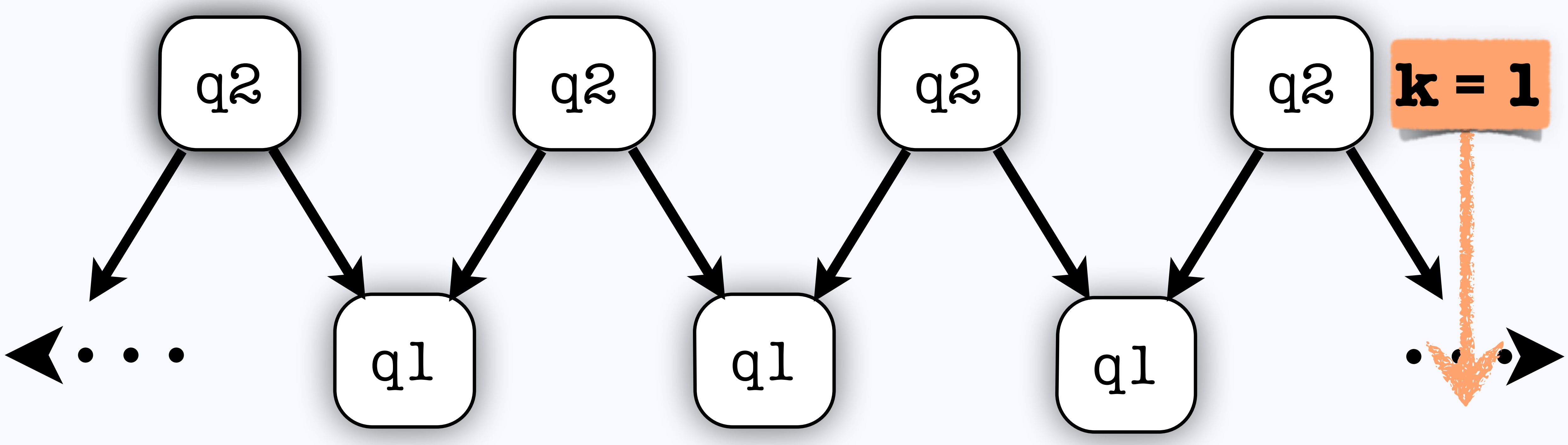
Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable**
	Non-Primitive Recursive

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph

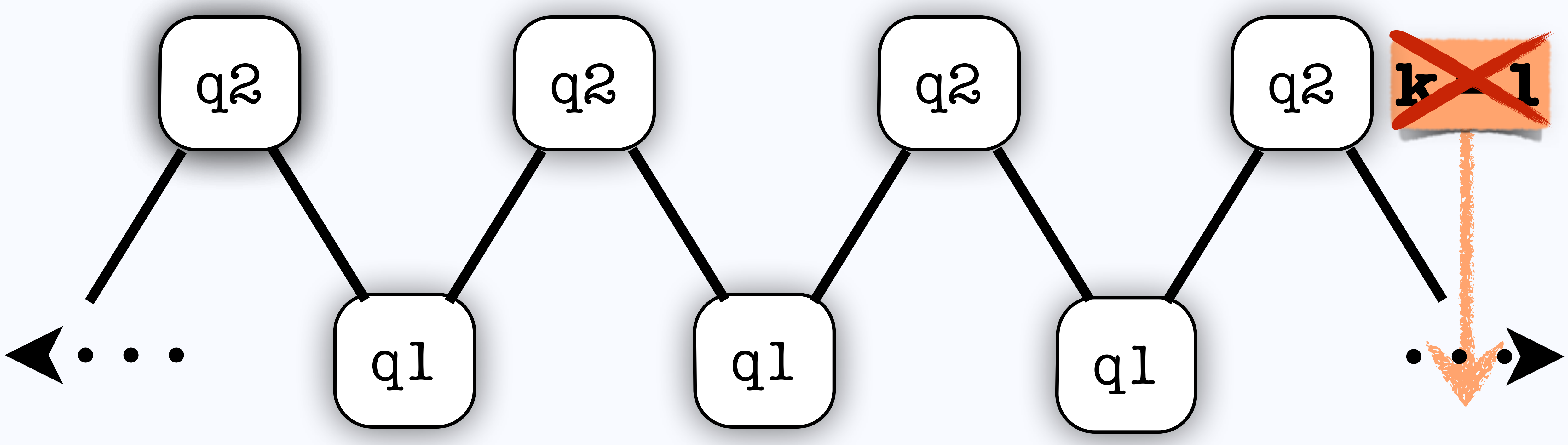
Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph



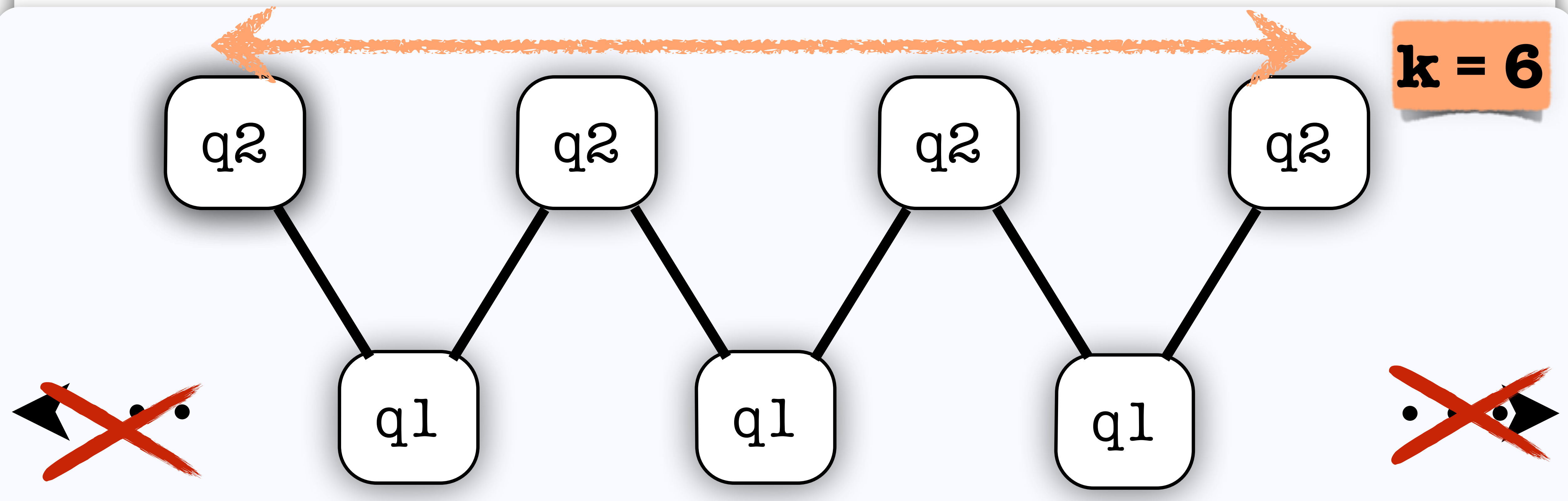
Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph



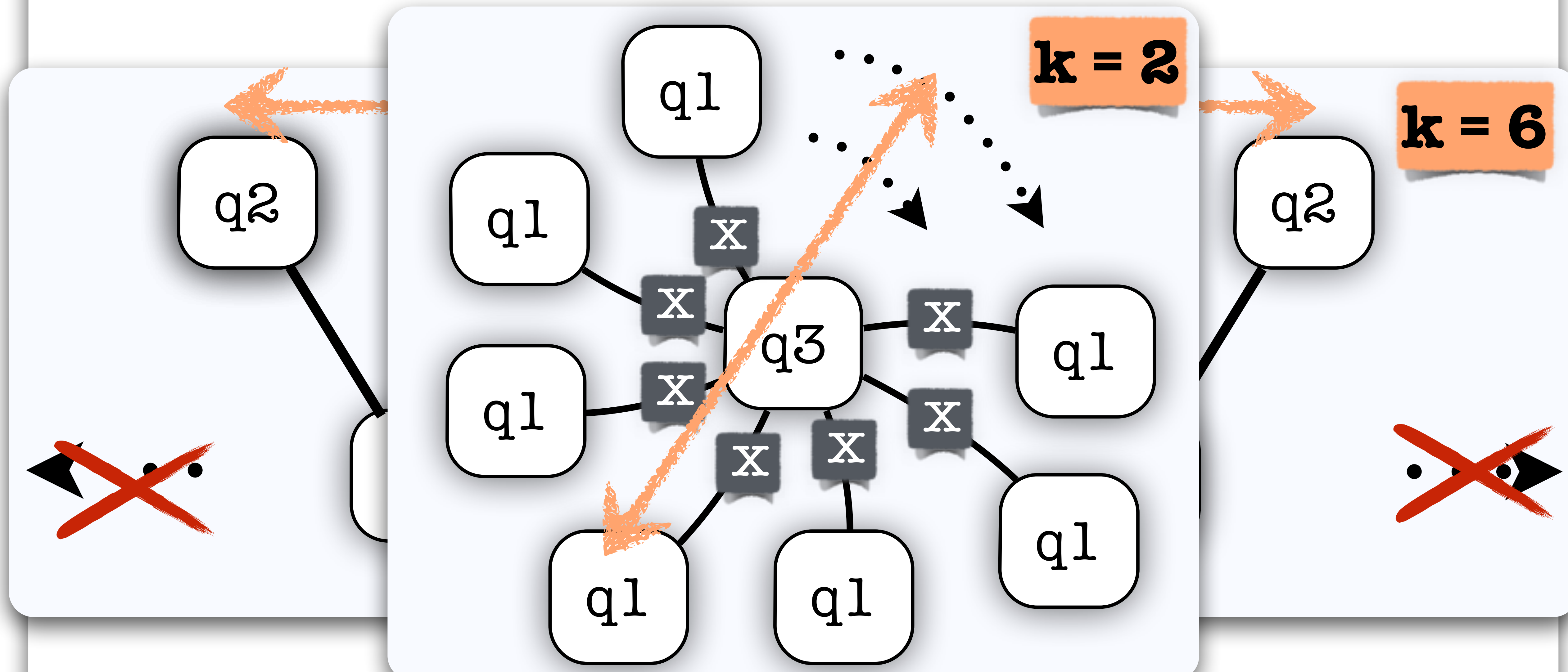
Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph



Strongly Bounded DRA

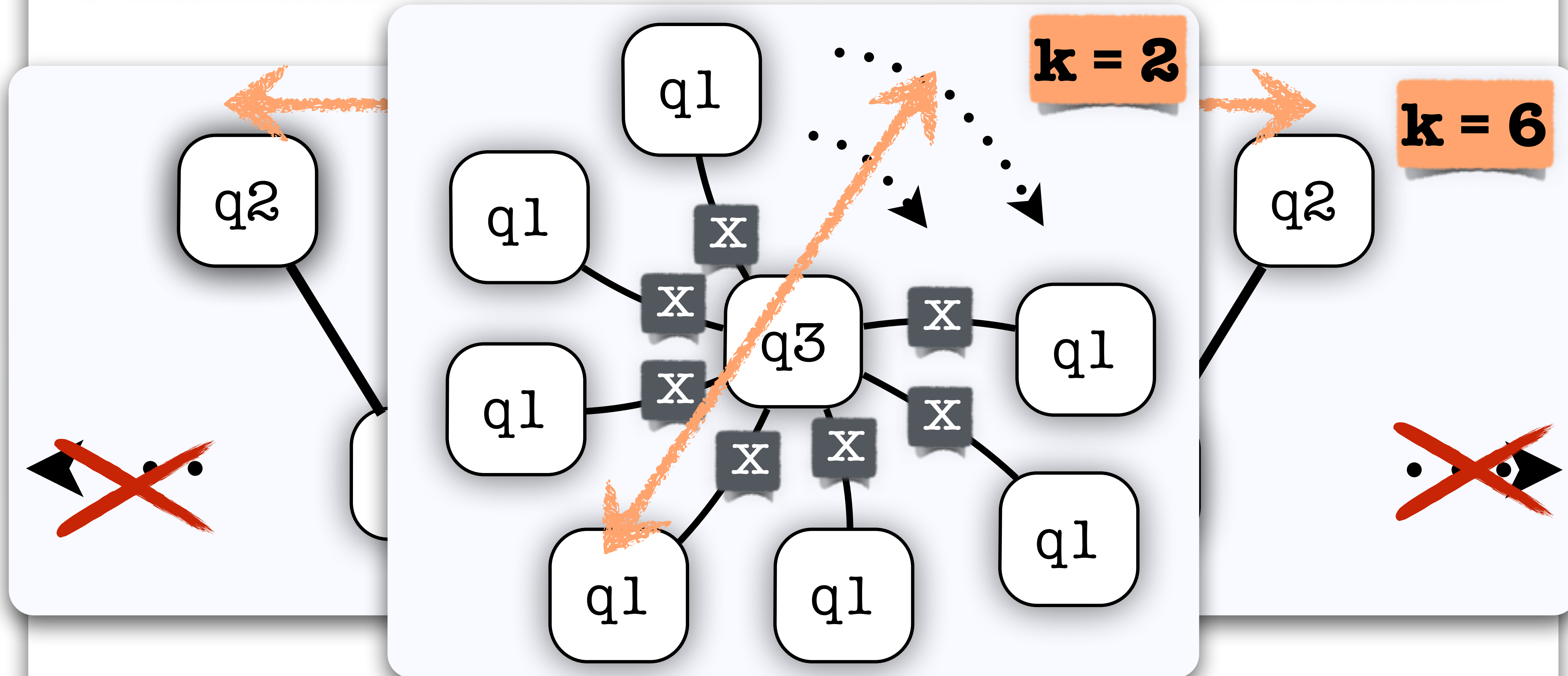
Bound the Simple Path Length of the underlying undirected configuration graph



Still: Unbounded Number of Processes

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph



Undecidable

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**

Two counters Minsky Machine

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph

Undecidable

Two counters Minsky Machine

↓

Strongly-Bounded Reachability

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**

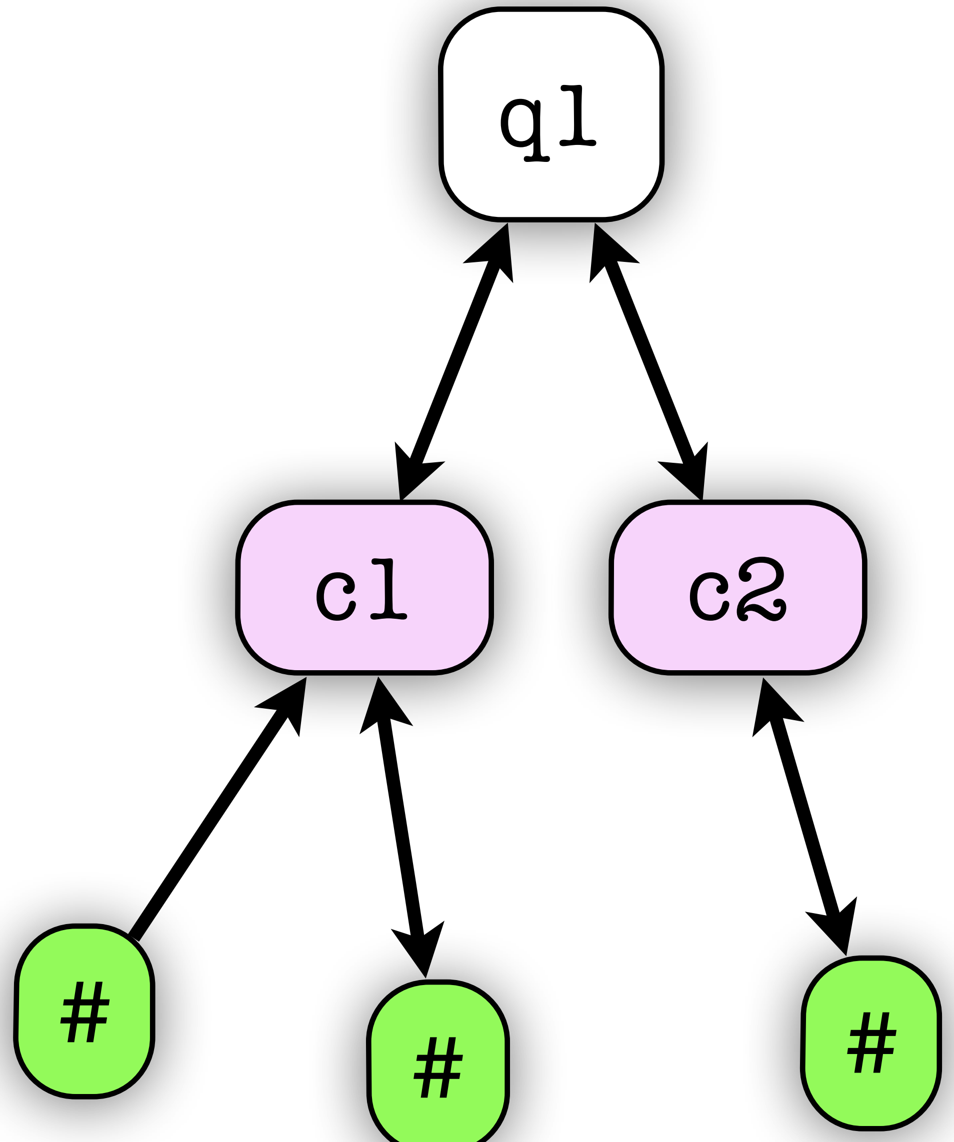
Two counters Minsky Machine

↓

k = 4 Strongly-Bounded Reachability

Strongly Bounded DRA

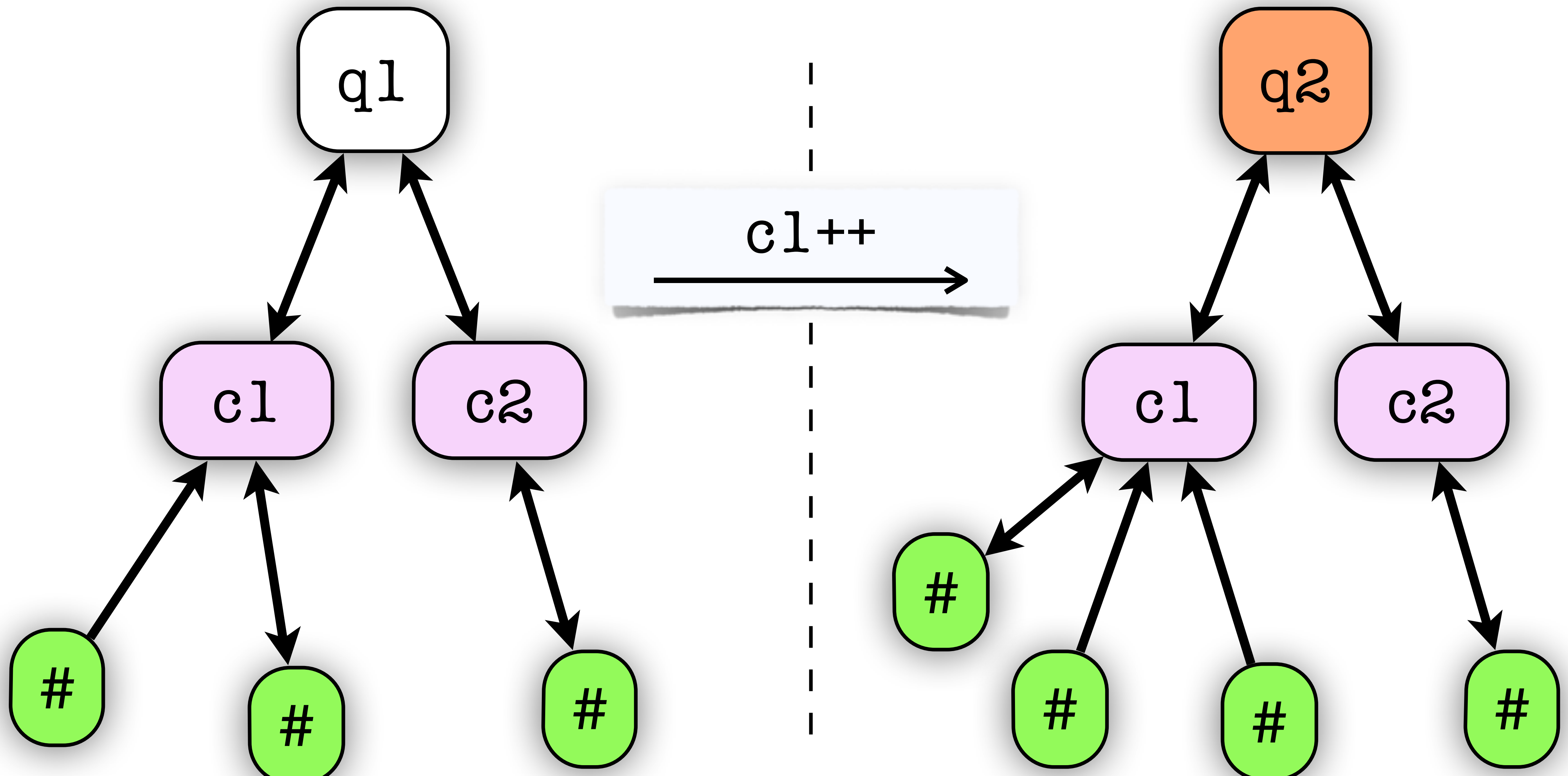
Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**



Two counters Minsky Machine

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**

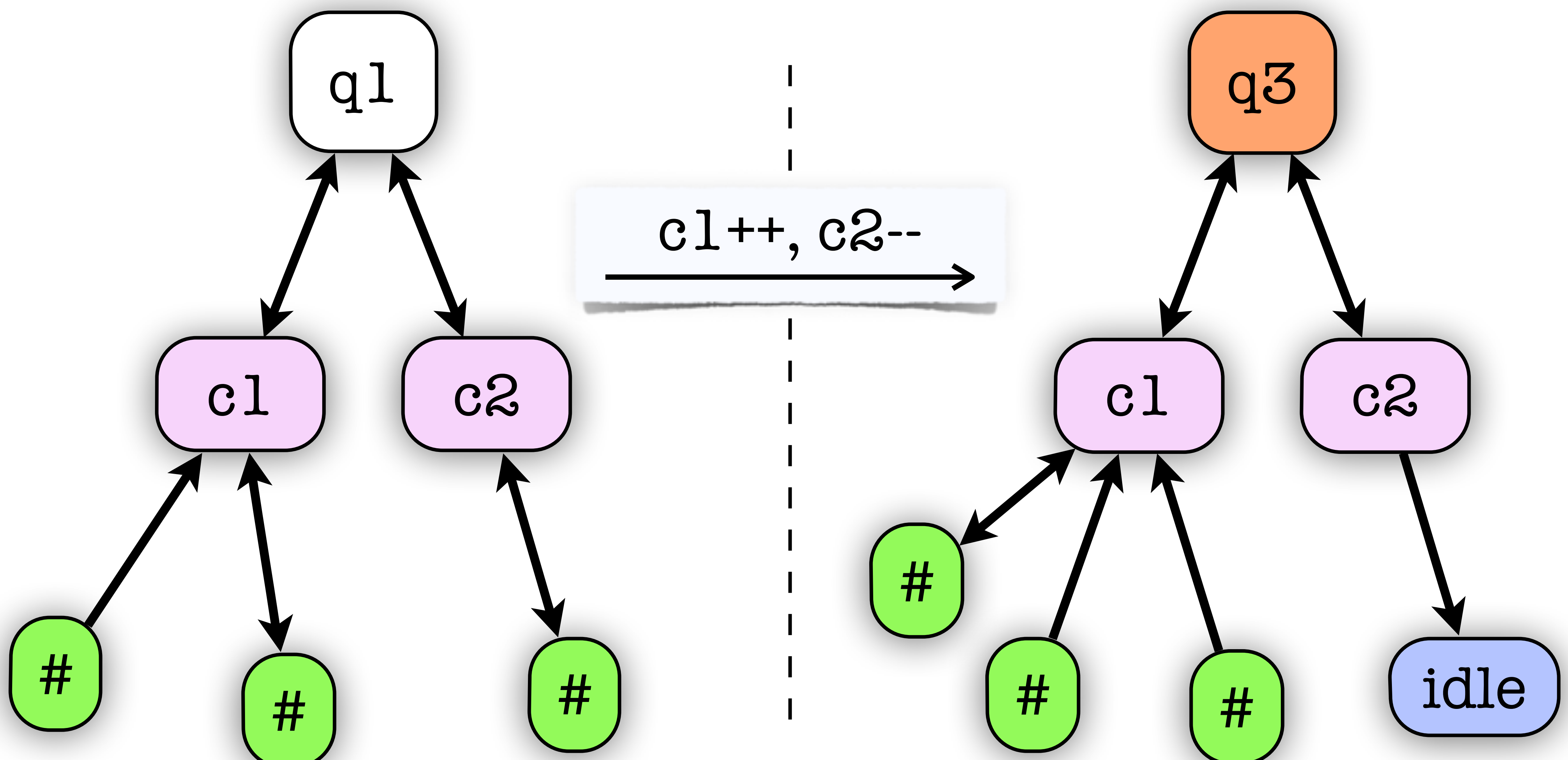


Two counters Minsky Machine

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph

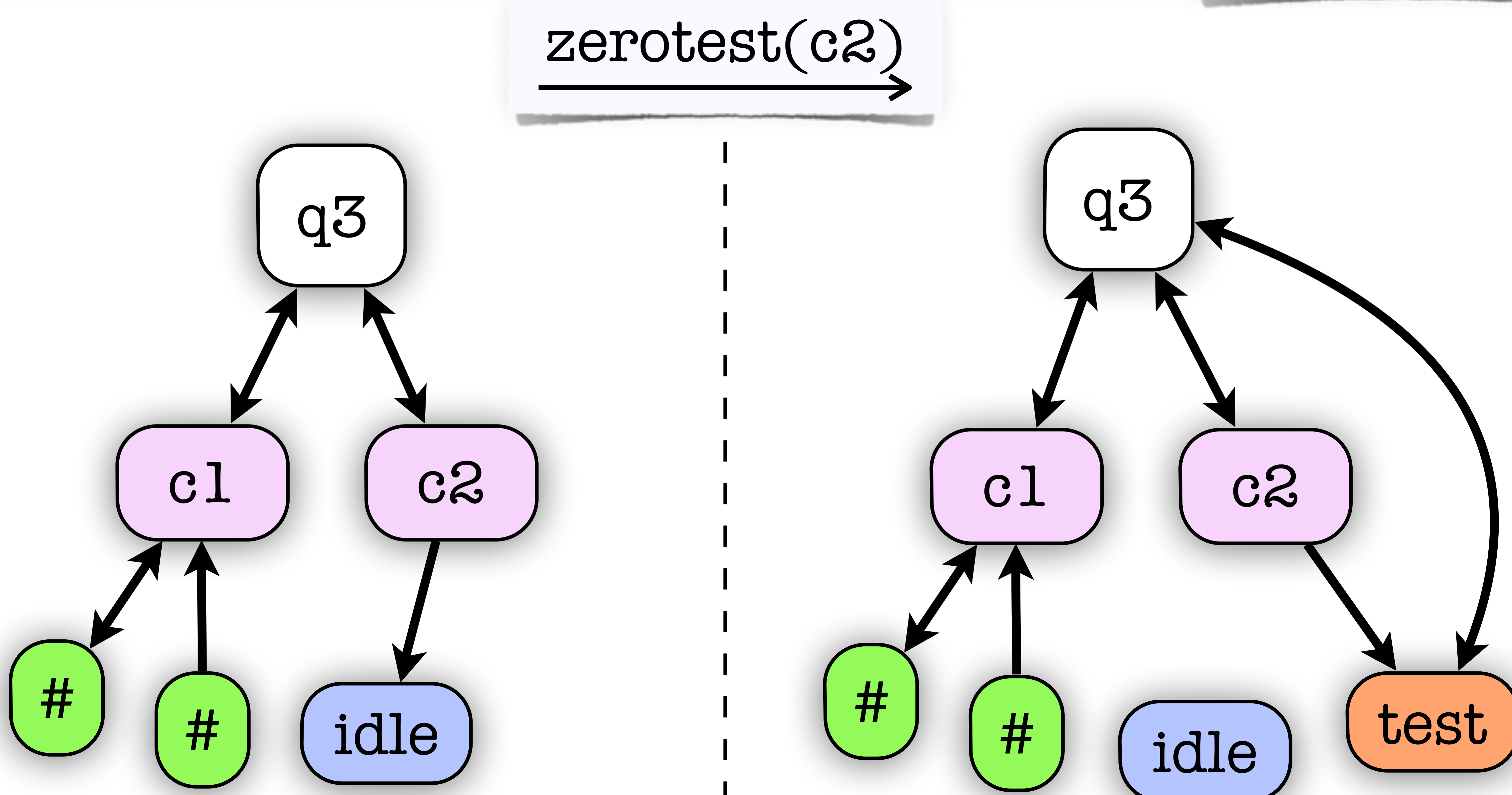
Undecidable



Two counters Minsky Machine

Strongly Bounded DRA

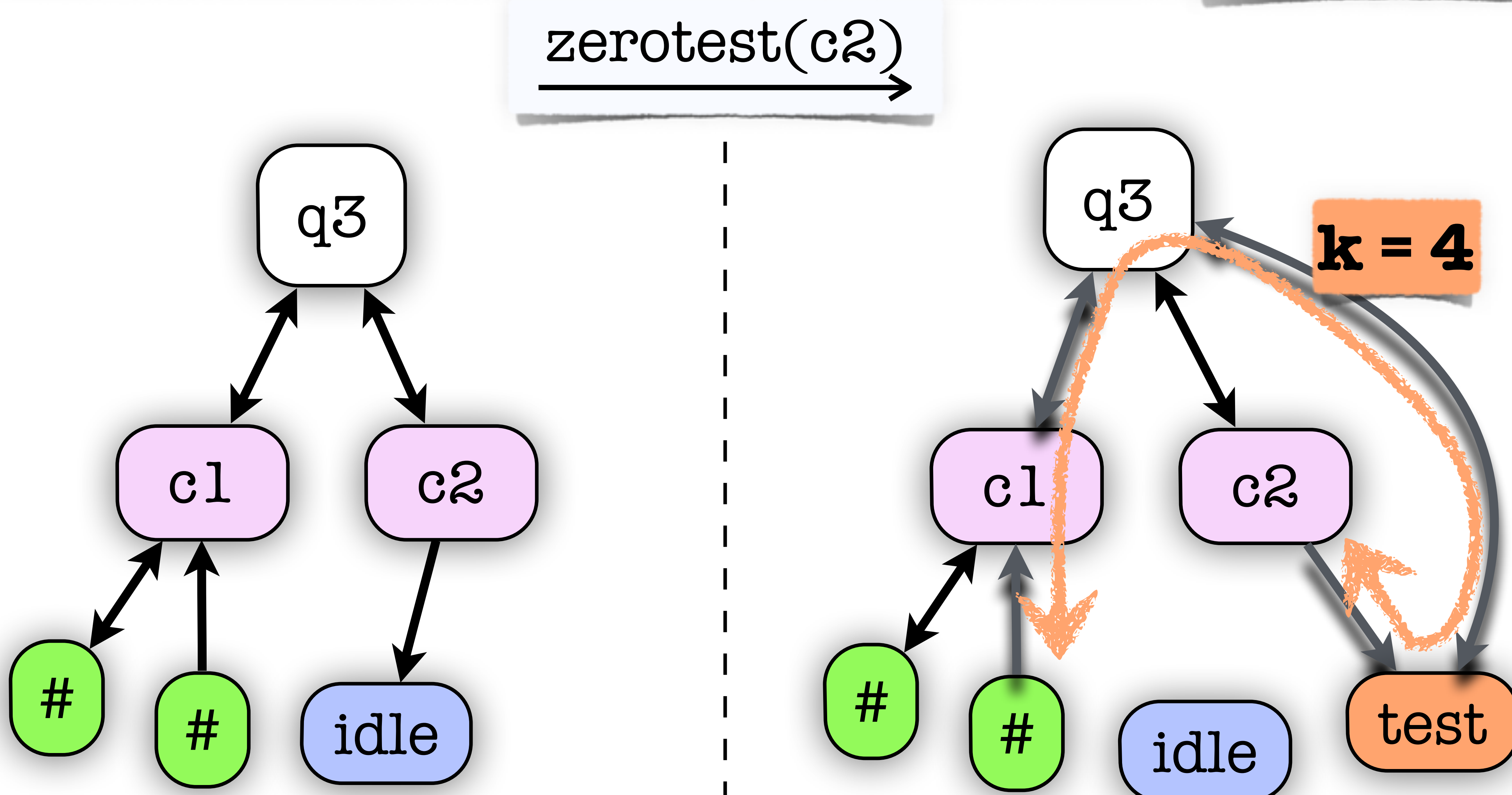
Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**



Two counters Minsky Machine

Strongly Bounded DRA

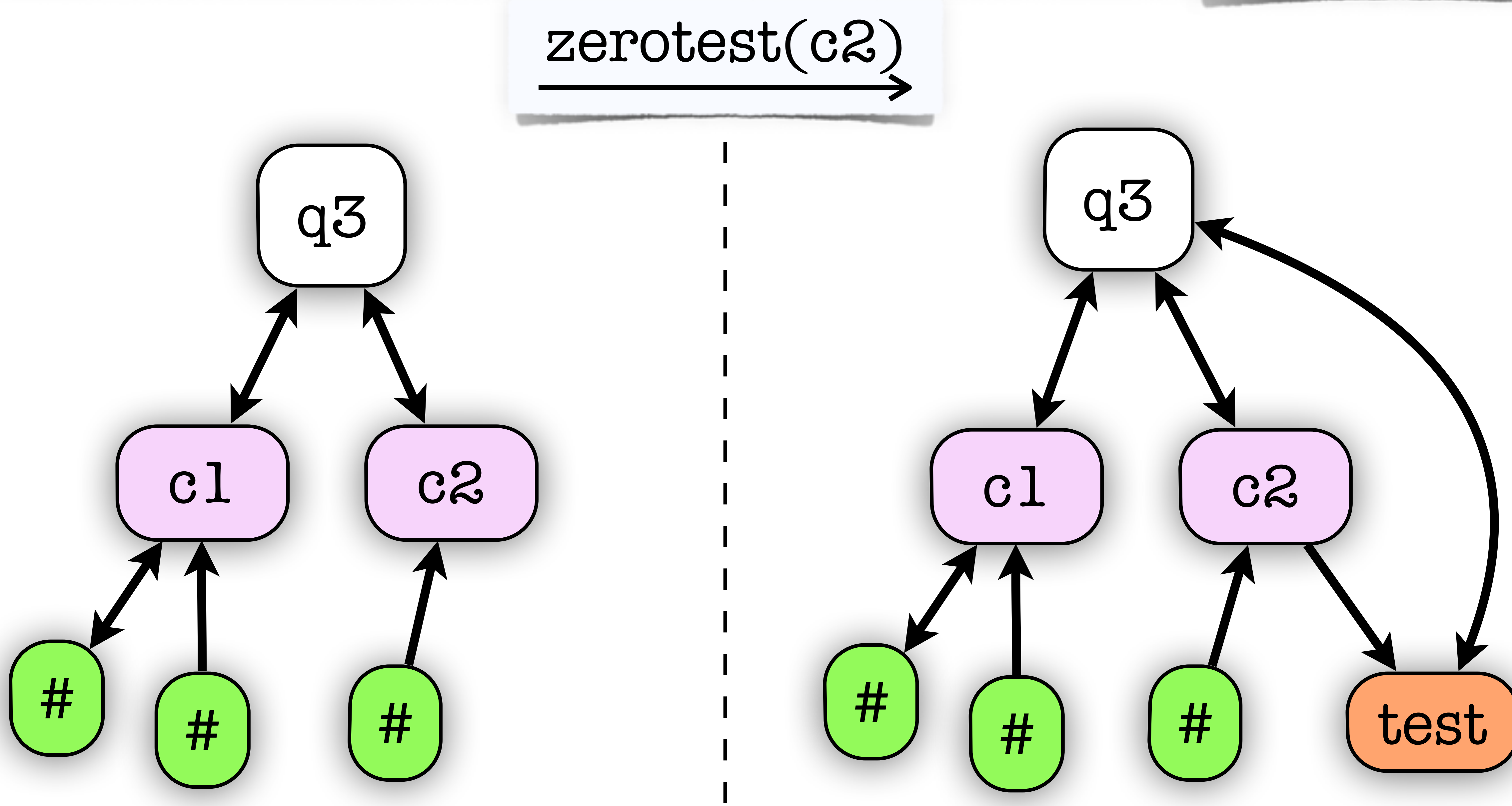
Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**



Two counters Minsky Machine

Strongly Bounded DRA

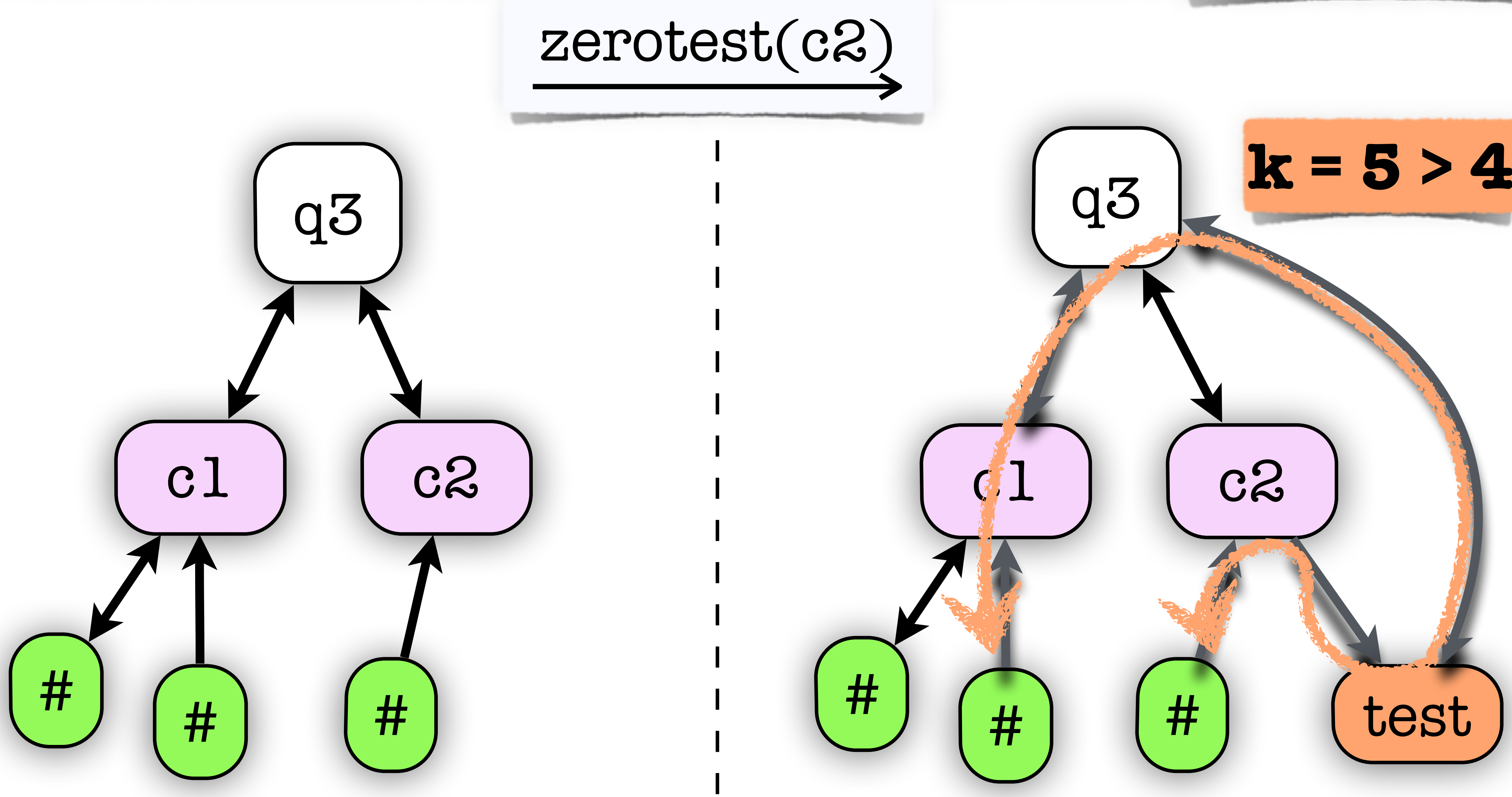
Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**



Two counters Minsky Machine

Strongly Bounded DRA

Bound the Simple Path Length of the underlying undirected configuration graph **Undecidable**



Two counters Minsky Machine

Contribution

State Reachability

Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable**
	Non-Primitive Recursive

Contribution

State Reachability

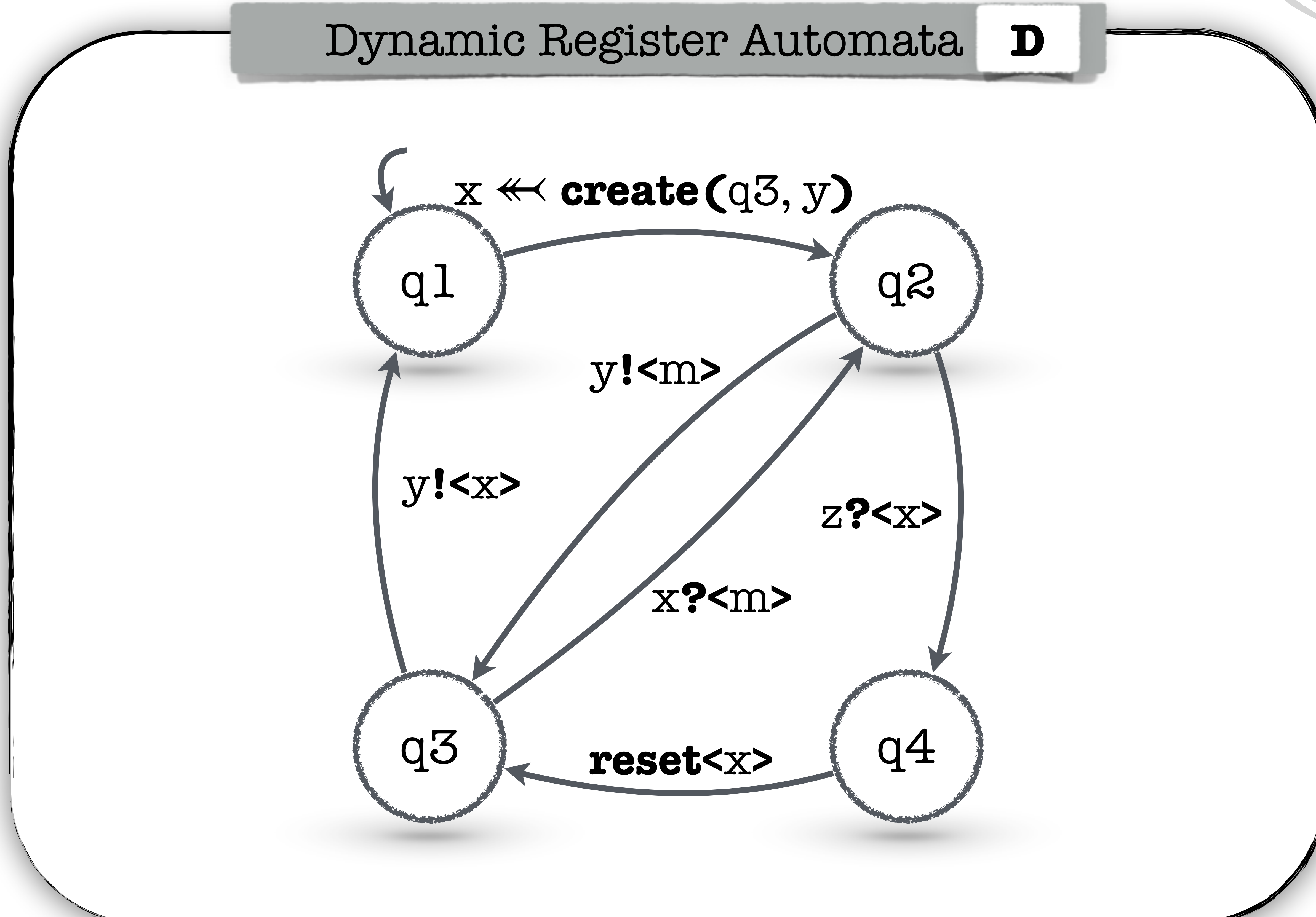
Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable** — **Non-Primitive Recursive**

Contribution

State Reachability

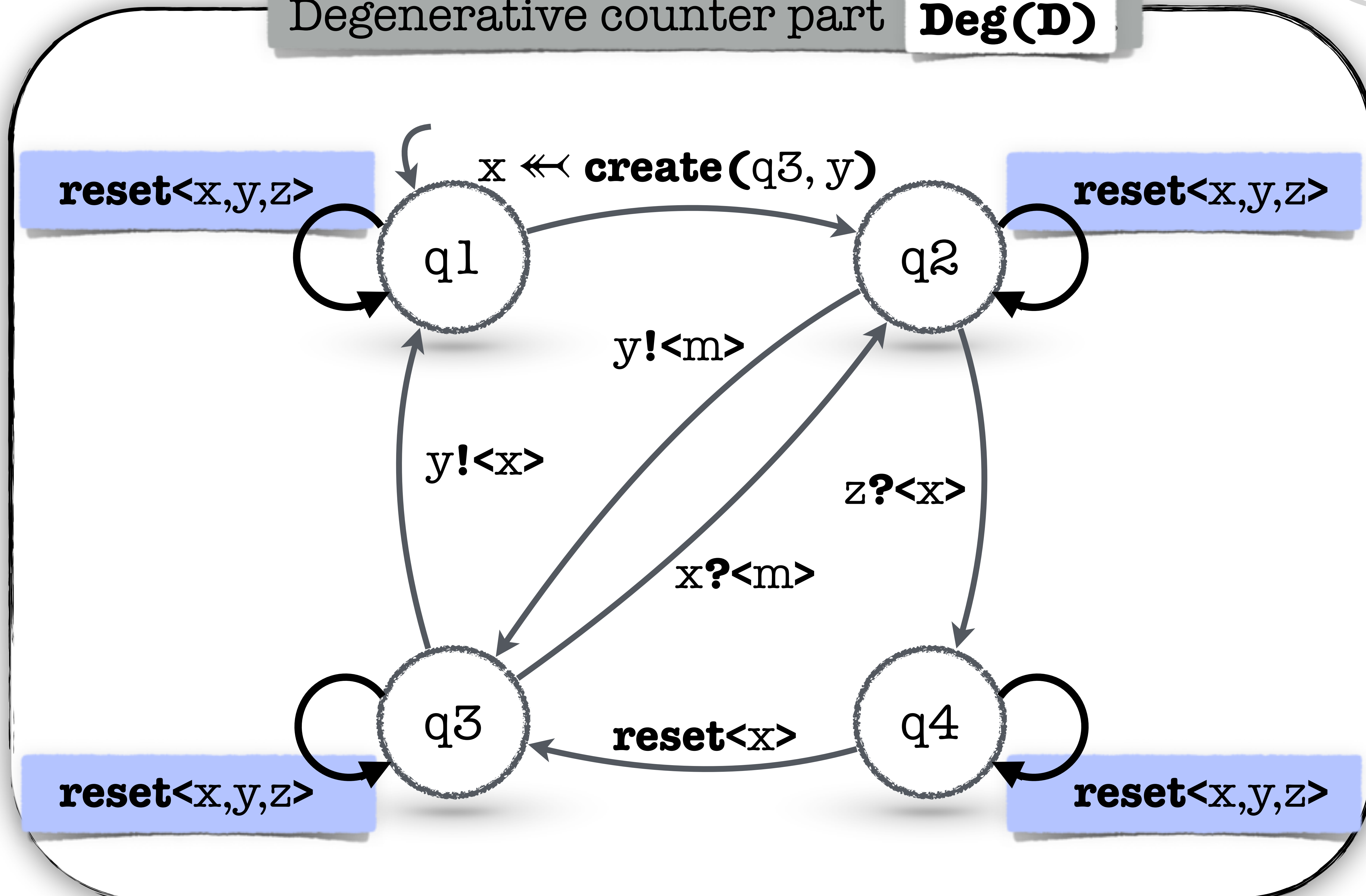
Bounded DRA	Undecidable
Strongly Bounded DRA	Undecidable
Strongly Safe DRA	Decidable
Degenerative DRA	Non-Primitive Recursive

Degenerative DRA



Degenerative DRA

Degenerative counter part **Deg(D)**



Contribution

State Reachability

Bounded DRA — Undecidable

Strongly Bounded DRA — Undecidable

Strongly Safe DRA — Decidable

Degenerative DRA — Non-Primitive Recursive

Strongly Safe DRA

DRA is degenerative

+

Bound the Simple Path Length of the underlying undirected configuration graph

Strongly Safe DRA

DRA is degenerative +

Bound the Simple Path Length of the underlying undirected configuration graph

Well-Structured Transition Systems

[Abdulla et al. 1996], [Finkel et al. 2001]

Symbolic representation of infinite set of configurations

Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations
- Prove **Monotonicity** of Transition Relation
- Provide an algorithm to compute the **Pre** of an upward closed set

Strongly Safe DRA

Well-Structured Transition Systems

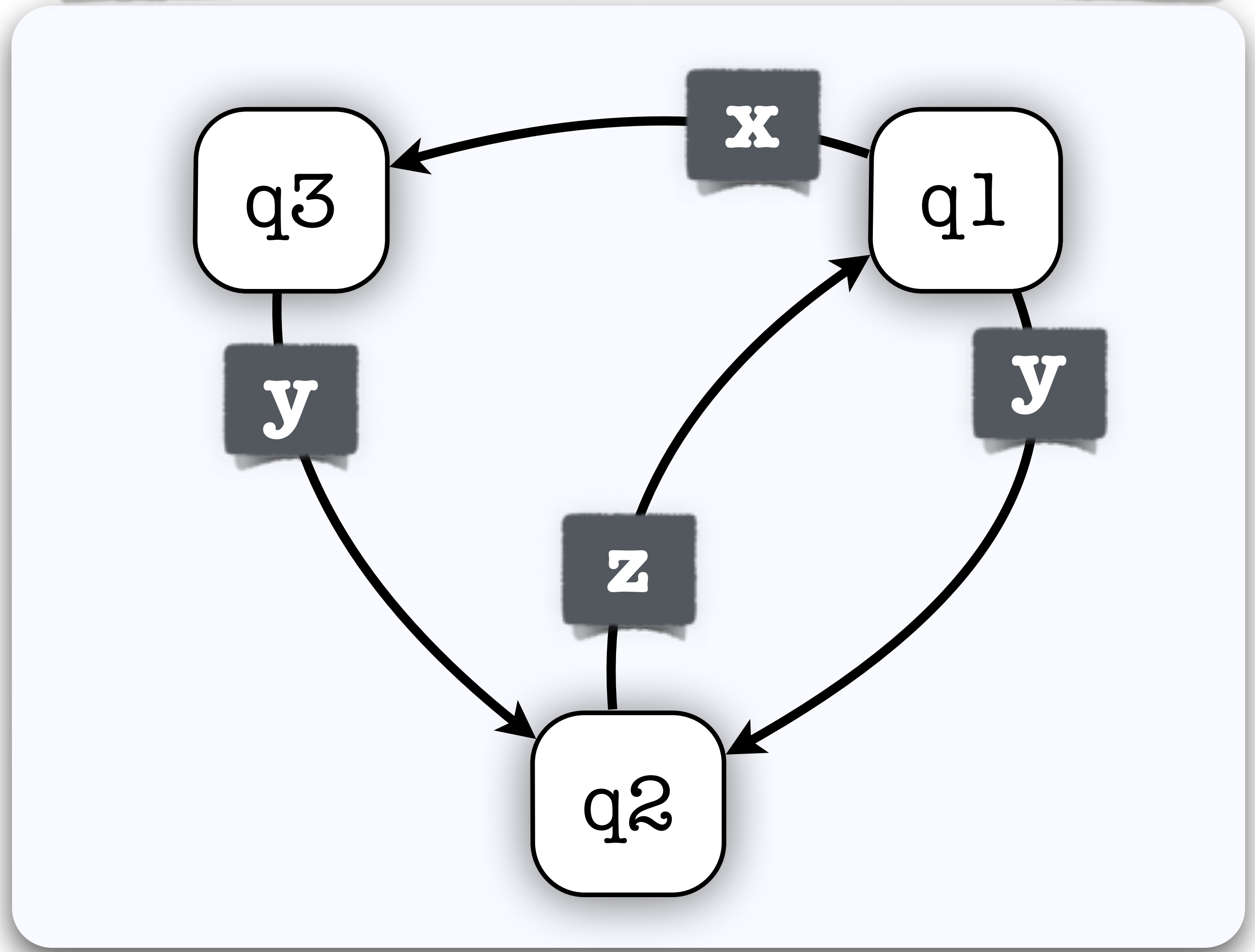
- Define a **Well-Quasi Order** on configurations
- Prove **Monotonicity** of Transition Relation
- Provide an algorithm to compute the **Pre** of an upward closed set

Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations

Ordering: subgraph relation

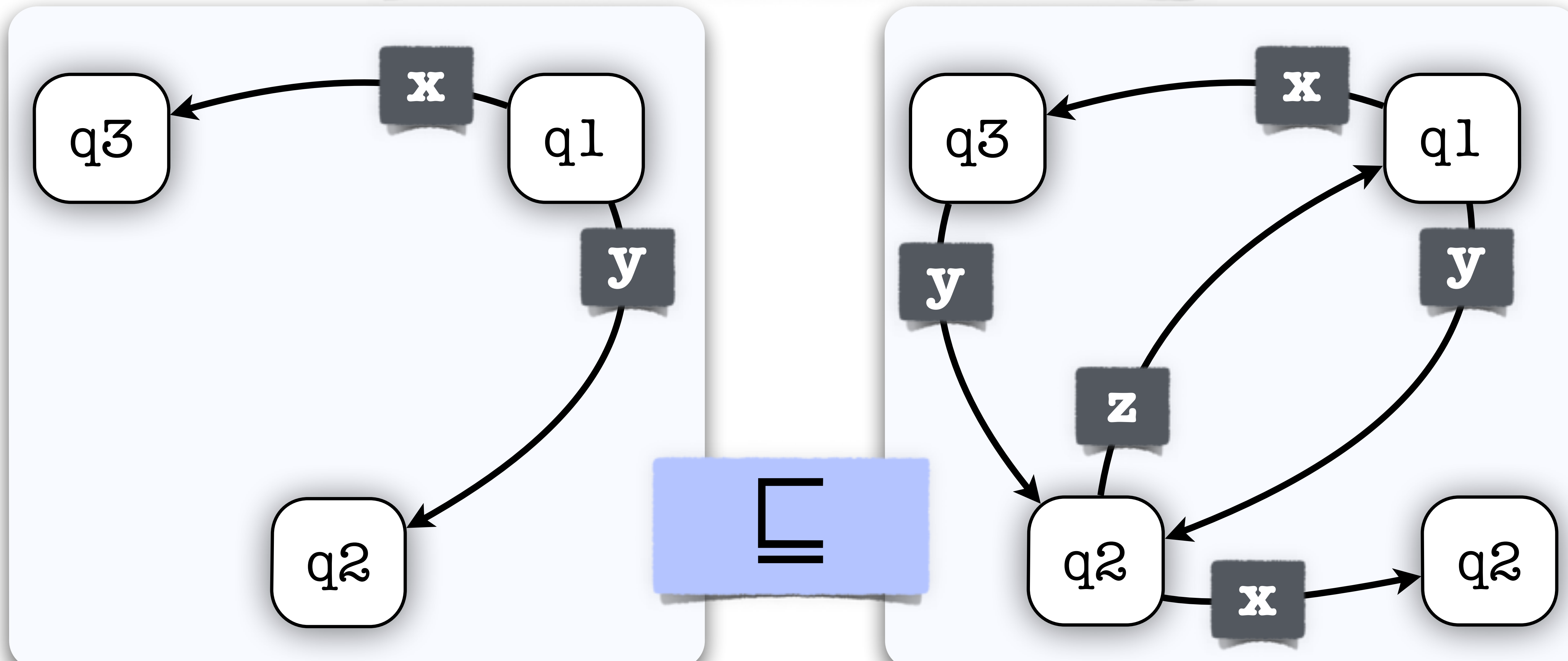


Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations

Ordering: subgraph relation



Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations

Ordering: subgraph relation

[Ding, 1992] Subgraphs and Well-Quasi Ordering

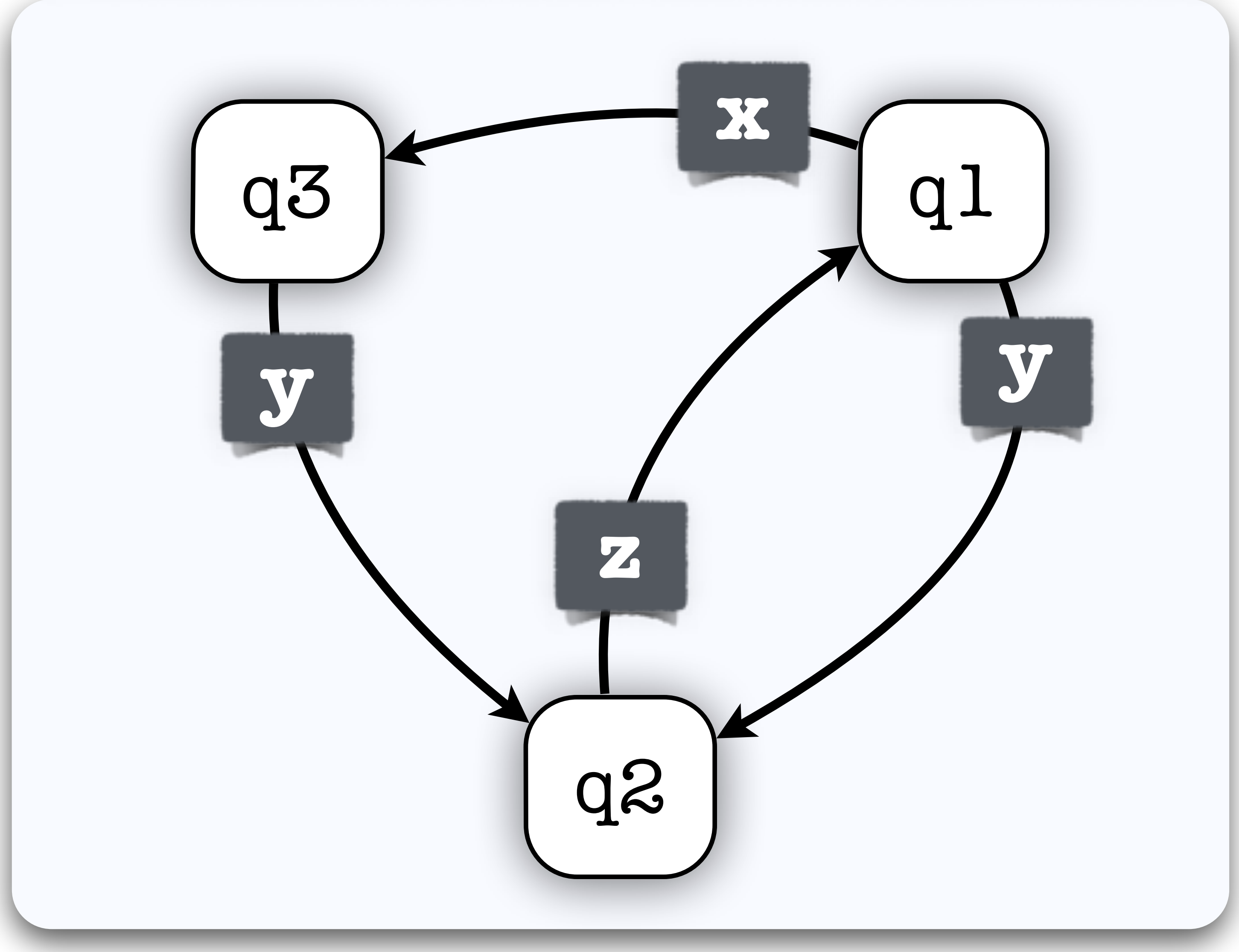
(Induced) subgraph relation is a WQO on Strongly-Bounded graphs

Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations

Ordering: subgraph relation

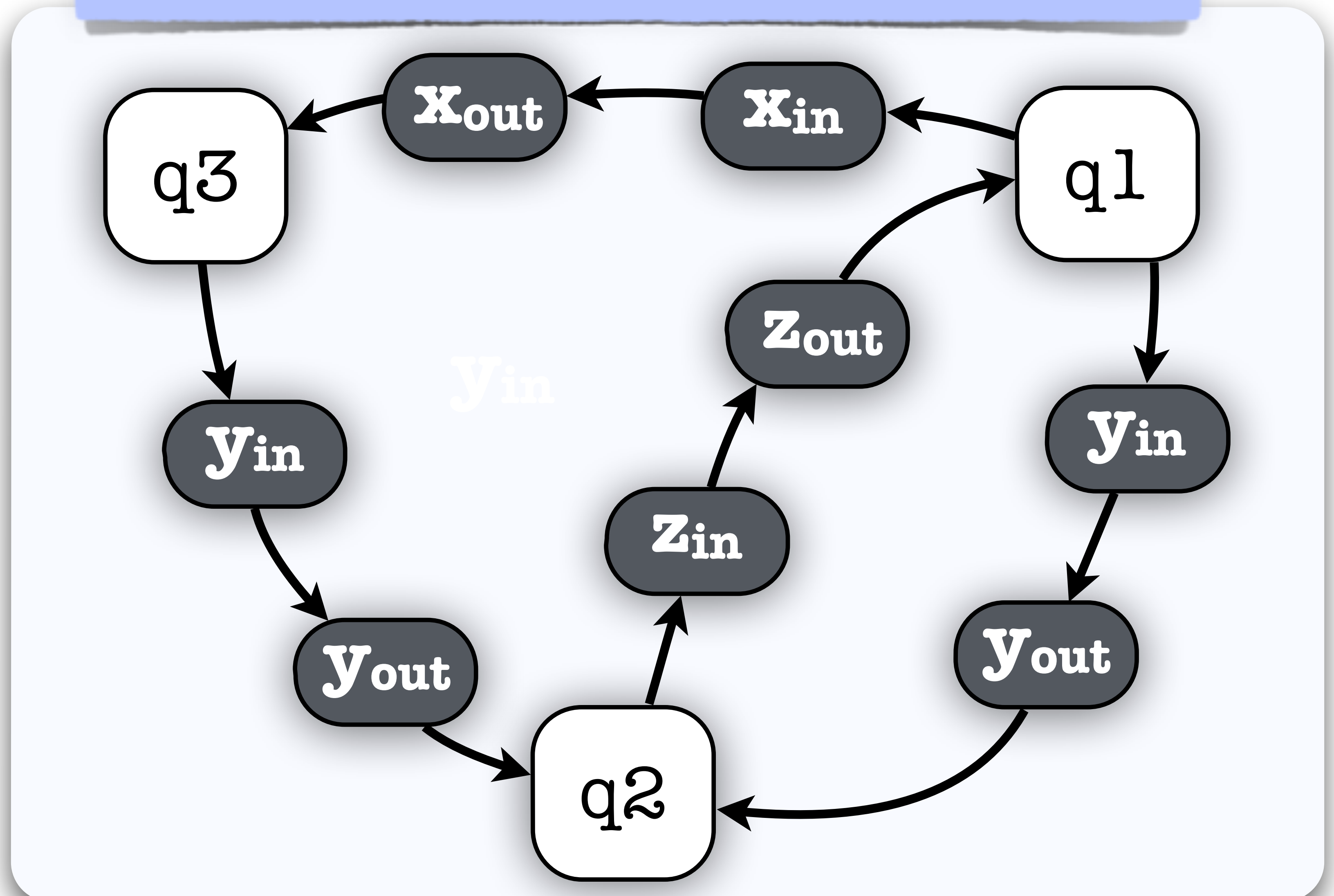


Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations

Ordering: subgraph relation



Strongly **Safe** DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations
- Prove **Monotonicity** of Transition Relation
- Provide an algorithm to compute the **Pre** of an upward closed set

Strongly Safe DRA

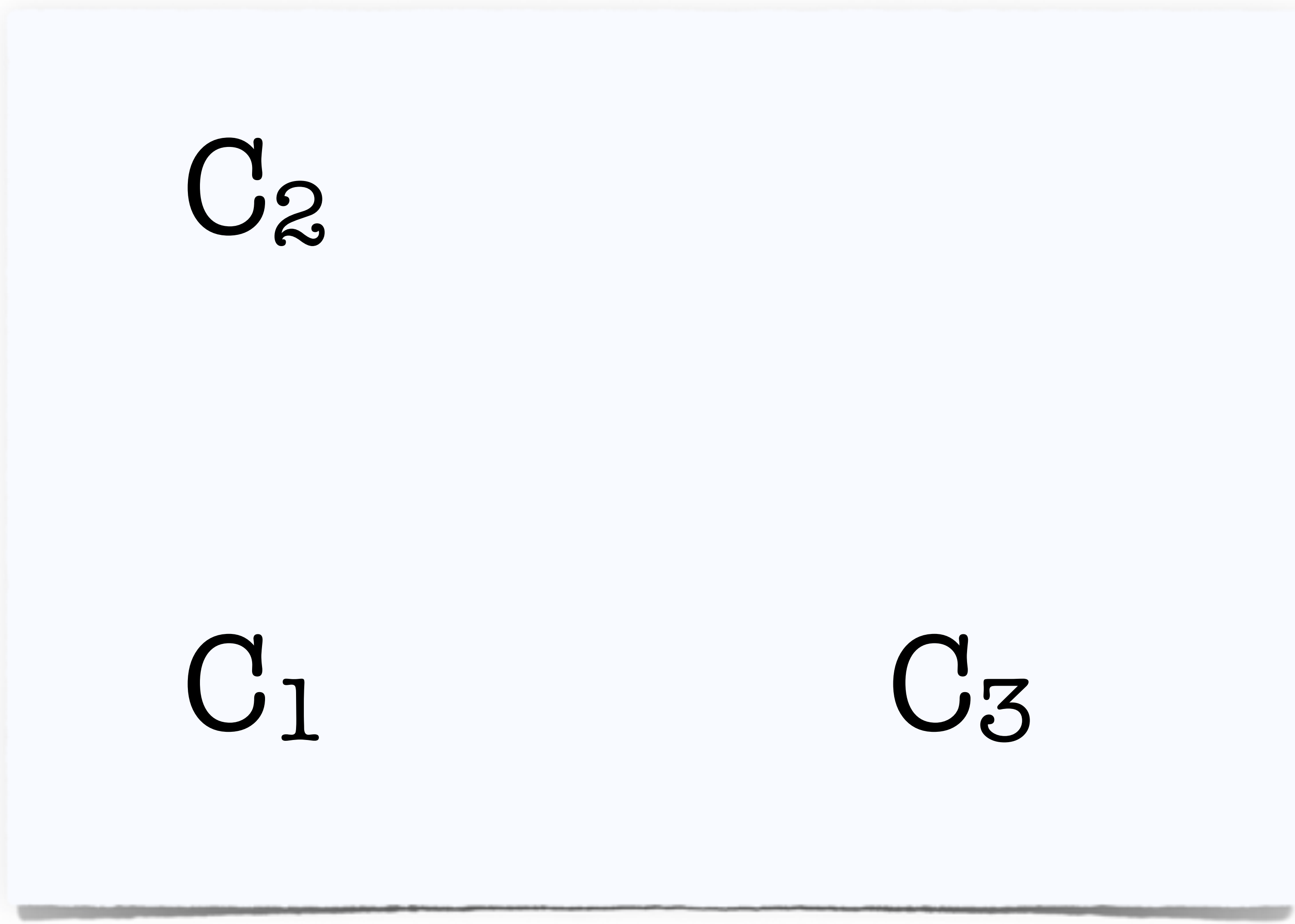
Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations
- Prove **Monotonicity** of Transition Relation
- Provide an algorithm to compute the **Pre** of an upward closed set

Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation



Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

$$c_2$$

$$\sqsubseteq$$

$$c_1 \qquad\qquad c_3$$

Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

$$\begin{array}{ccc} c_2 & & \\ \rotatebox{90}{$\sqsupseteq$} & & \\ c_1 & \longrightarrow & c_3 \end{array}$$

Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

$$\begin{array}{ccc} c_2 & & c_4 \\ \sqsupseteq & & \\ c_1 & \longrightarrow & c_3 \end{array}$$

Strongly **Safe** DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

$$
\begin{array}{ccc}
c_2 & \longrightarrow & c_4 \\
\sqsubseteq & & \\
c_1 & \longrightarrow & c_3
\end{array}
$$

Strongly Safe DRA

Well-Structured Transition Systems

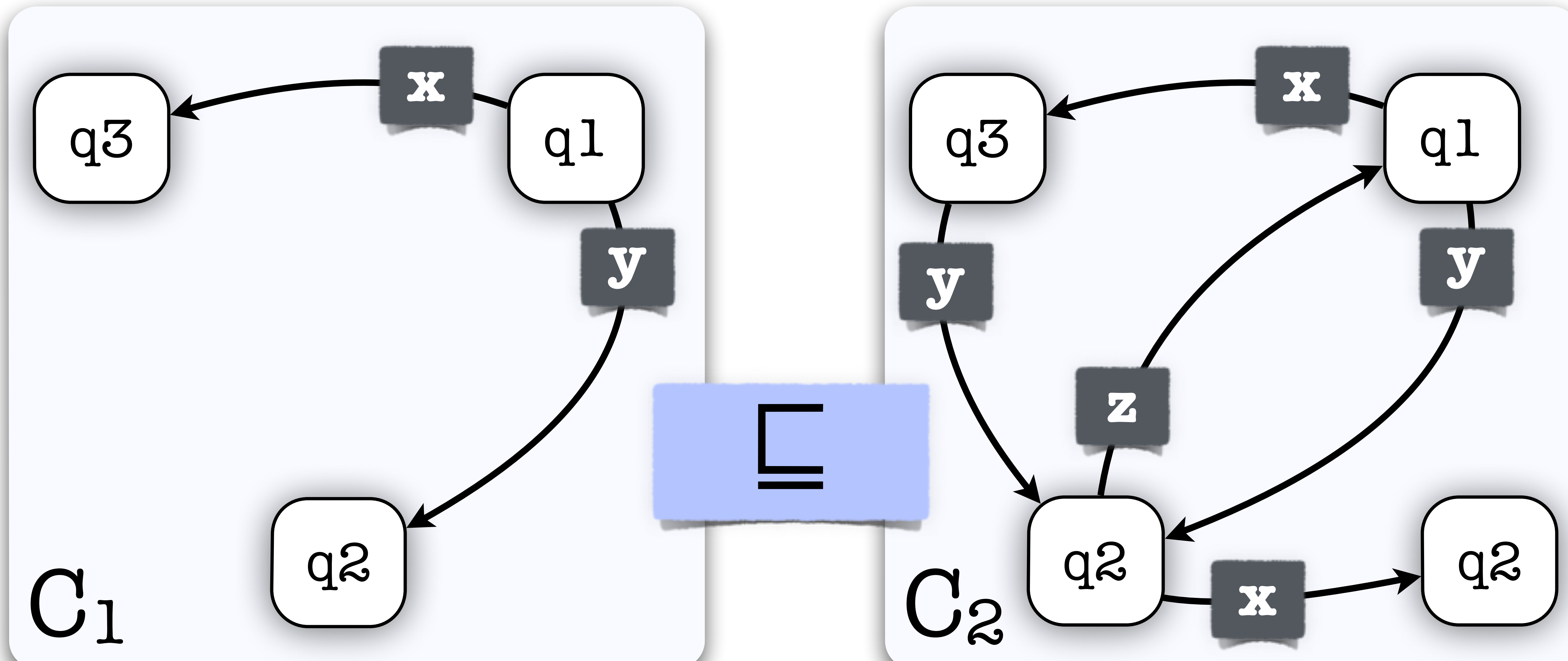
- Prove **Monotonicity** of Transition Relation

$$\begin{array}{ccc} c_2 & \longrightarrow & c_4 \\ \rotatebox{90}{$\sqsubseteq$} & & \rotatebox{90}{$\sqsubseteq$} \\ c_1 & \longrightarrow & c_3 \end{array}$$

Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

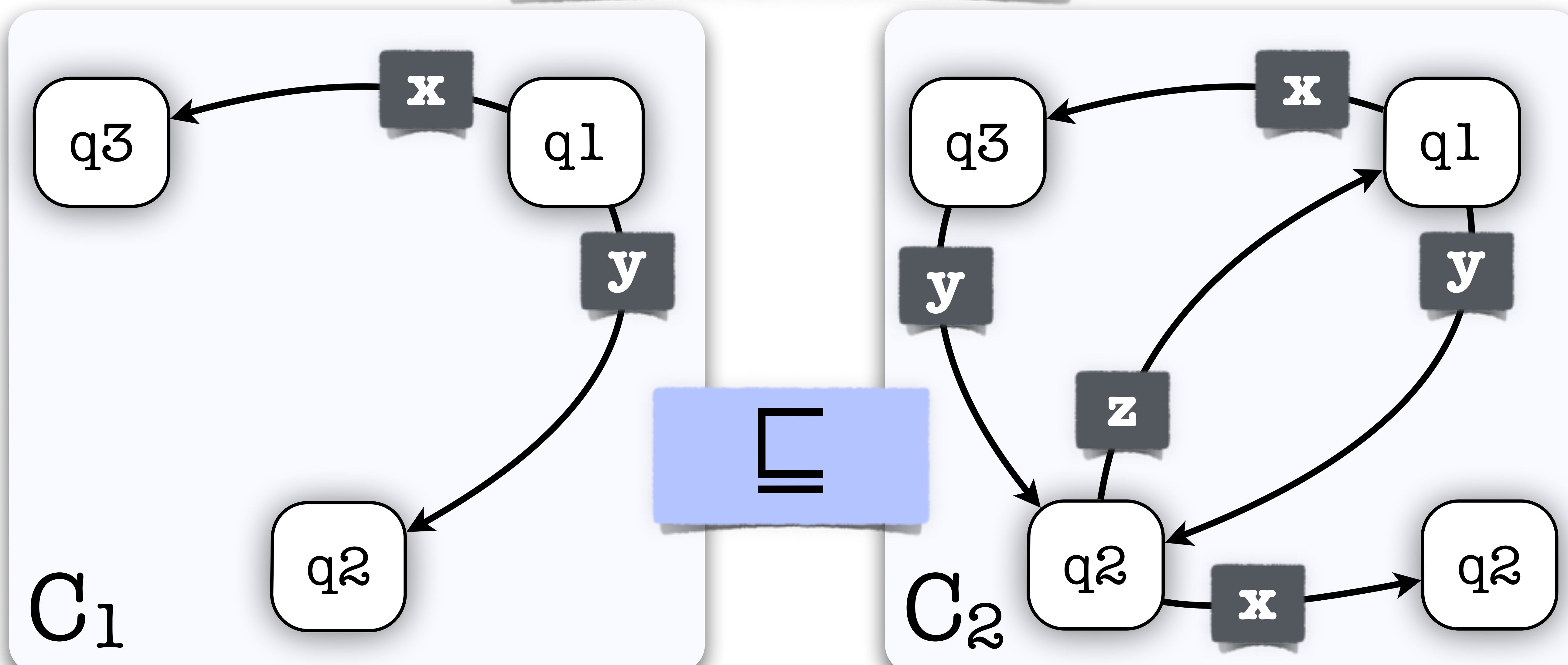


Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

Degenerative

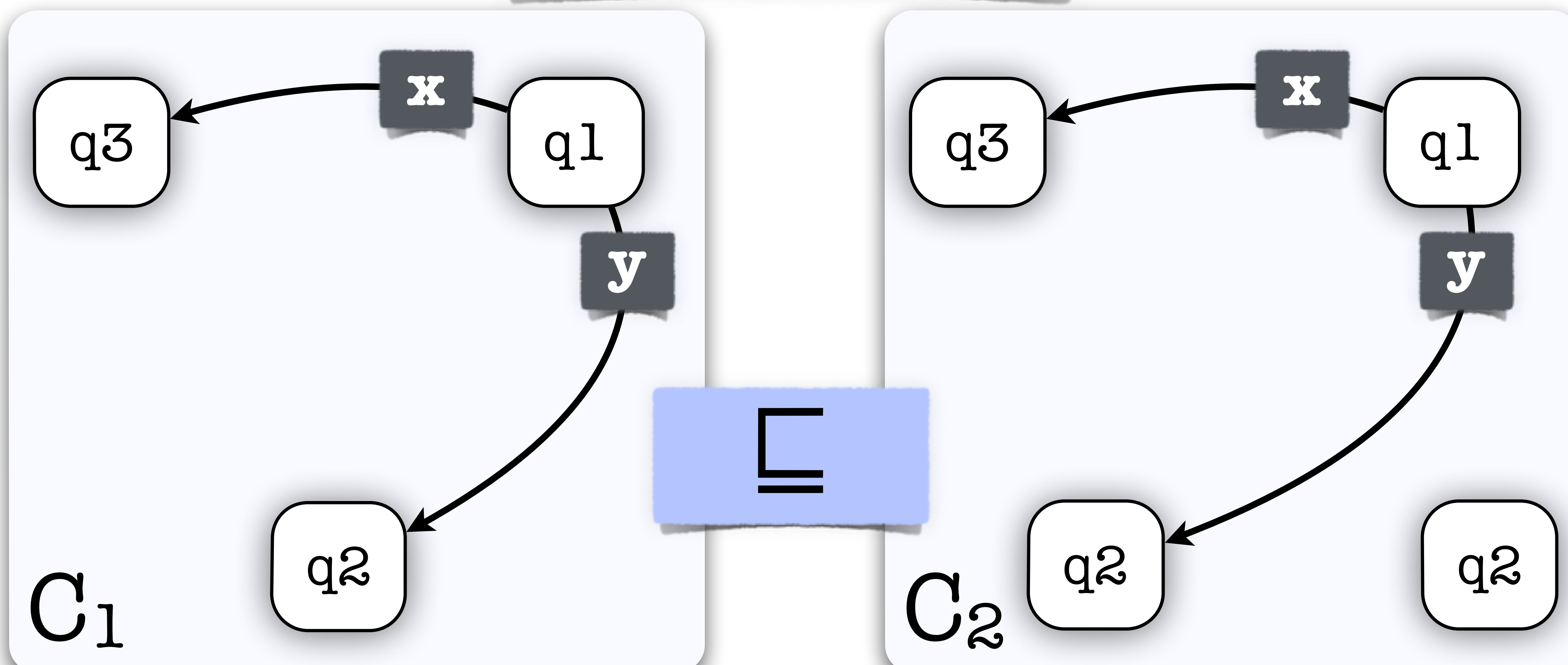


Strongly **Safe** DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

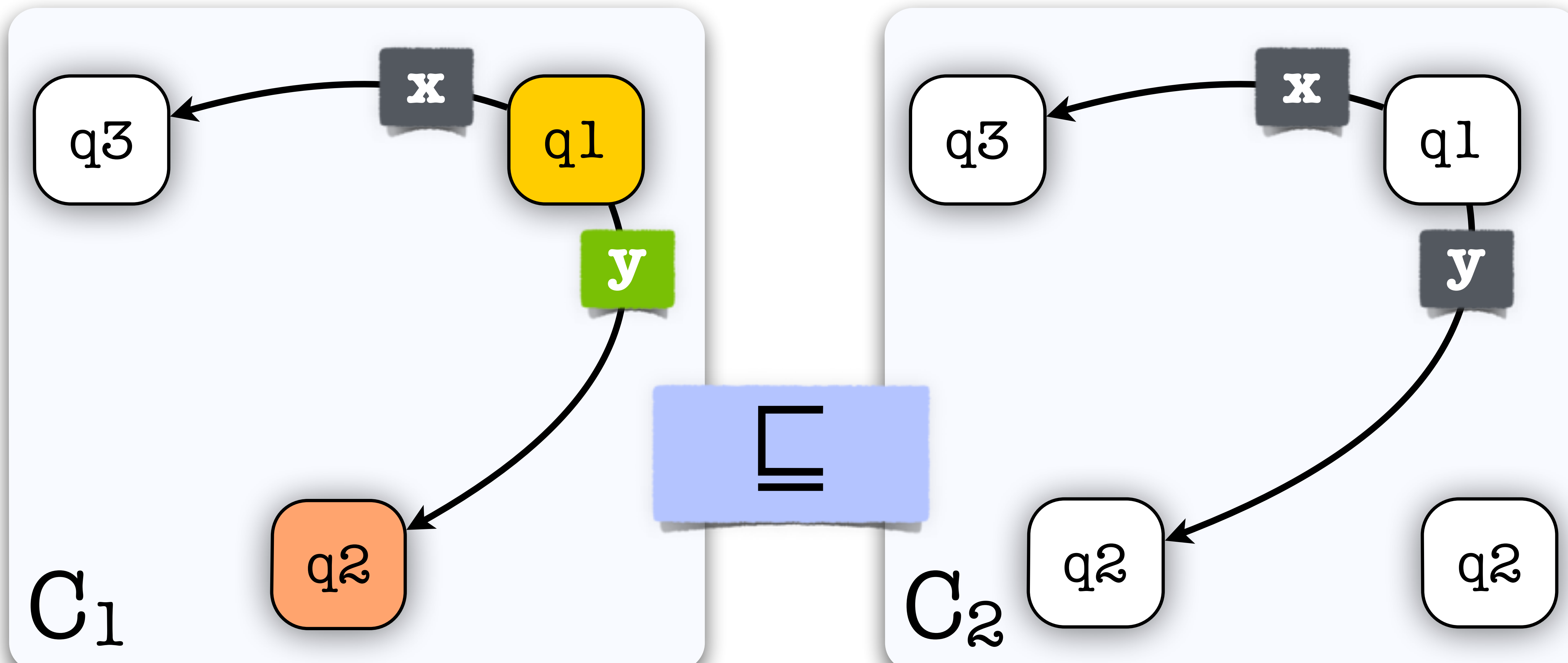
Degenerative



Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

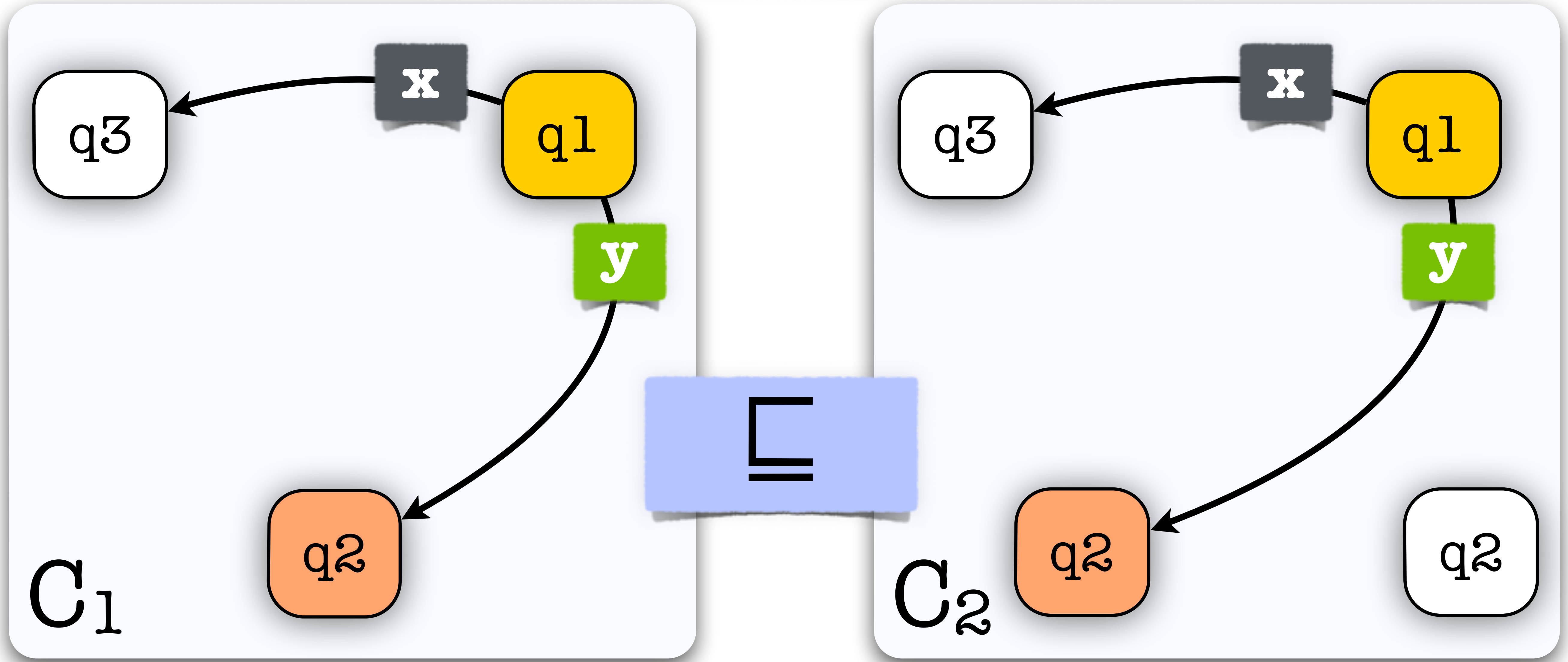


Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

Subgraph relation: Register Mapping & States preserved

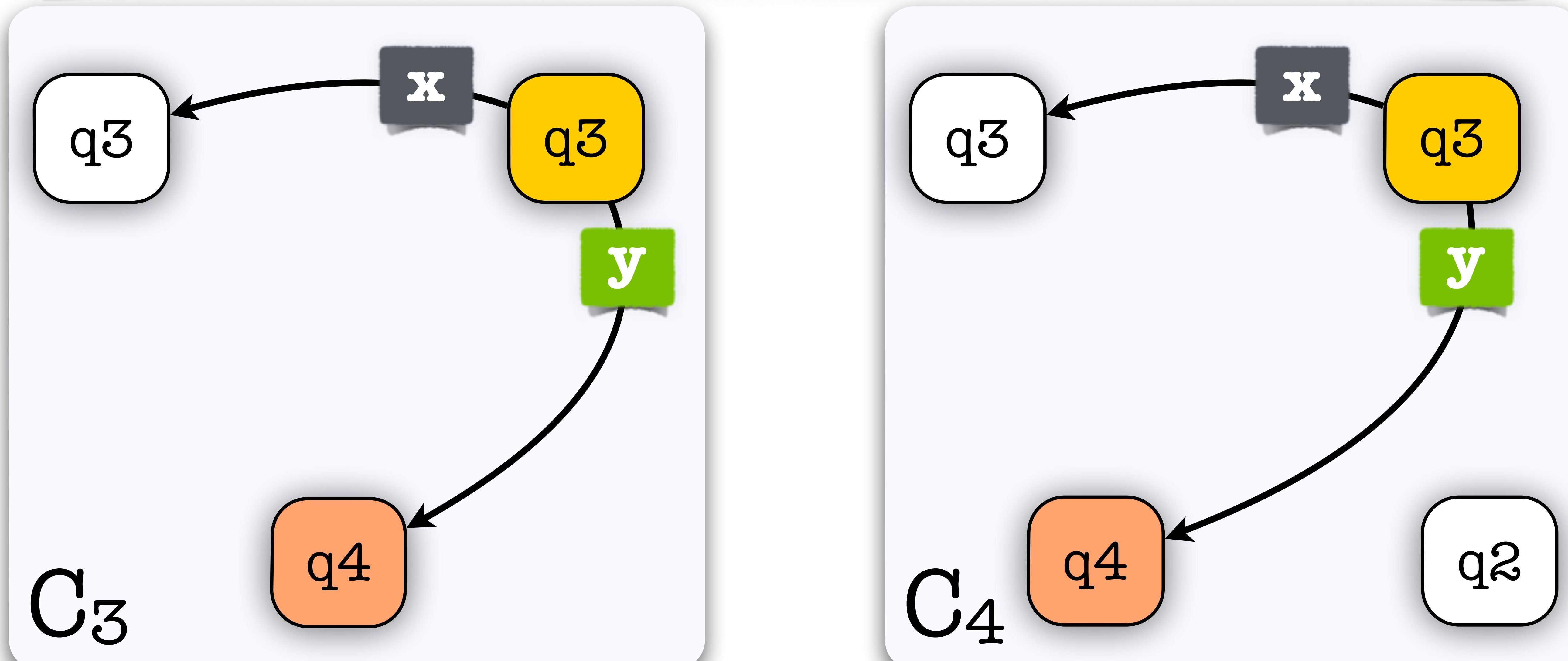


Strongly Safe DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

Subgraph relation: Register Mapping & States preserved

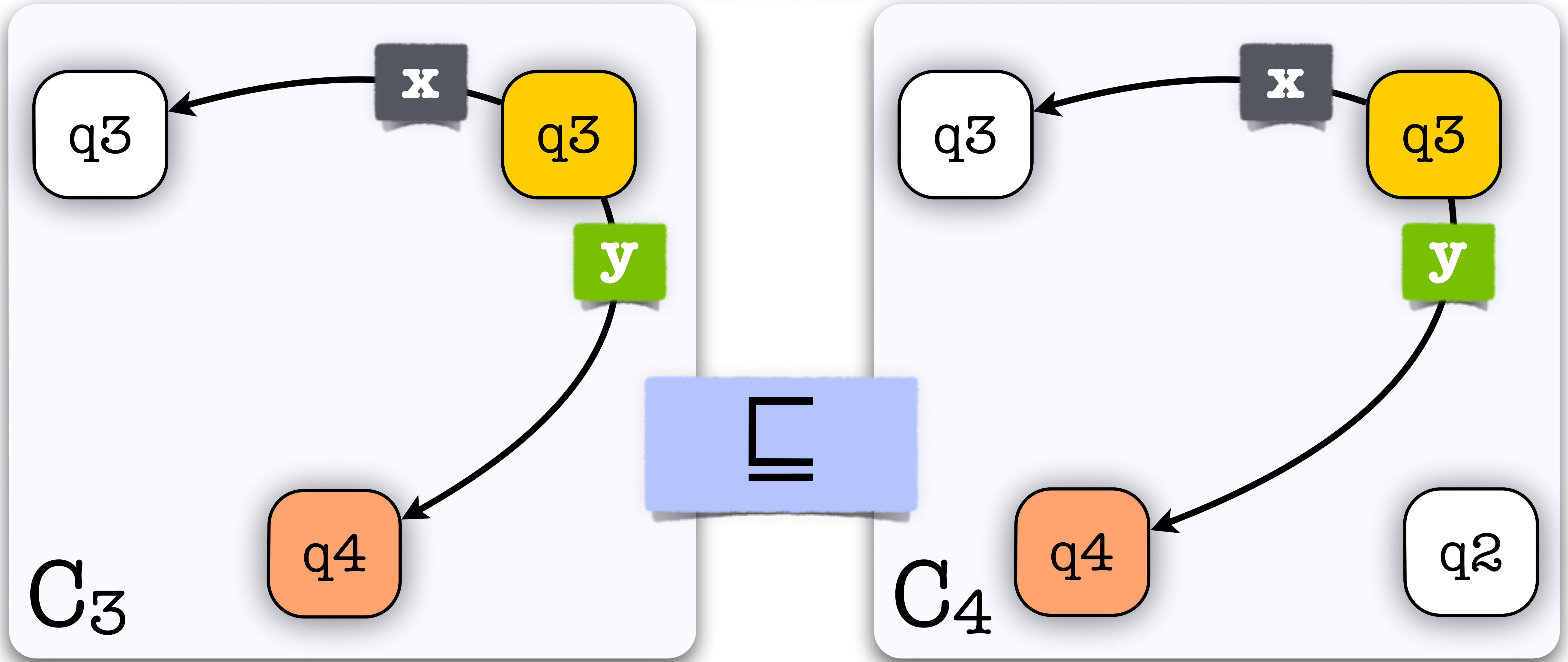


Strongly **Safe** DRA

Well-Structured Transition Systems

- Prove **Monotonicity** of Transition Relation

Subgraph relation: Register Mapping & States preserved



Strongly **Safe** DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations
- Prove **Monotonicity** of Transition Relation
- Provide an algorithm to compute the **Pre** of an upward closed set

Strongly Safe DRA

Well-Structured Transition Systems

- Define a **Well-Quasi Order** on configurations
- Prove **Monotonicity** of Transition Relation
- Provide an algorithm to compute the **Pre** of an upward closed set

Contribution

State Reachability

Bounded DRA	**Undecidable**
Strongly Bounded DRA	**Undecidable**
Strongly Safe DRA	**Decidable**
Degenerative DRA	**Non-Primitive Recursive**

Conclusion

Dynamic Register Automata

- Dynamic Creation of Processes
- Point-to-Point Comm.
- Register Mapping
- Rendez-Vous Comm.

State Reachability

Bounded DRA	Undecidable
Strongly Bounded DRA	Undecidable
Strongly Safe DRA	Decidable
	Non-Primitive Recursive

S·ACADEMIAE UBSALIENSIS

GRATIAE

VERITAS

NATURAE