Reconfigurable Heterogeneous Quorum Systems

Xiao Li, Mohsen Lesani
University of California, Santa Cruz

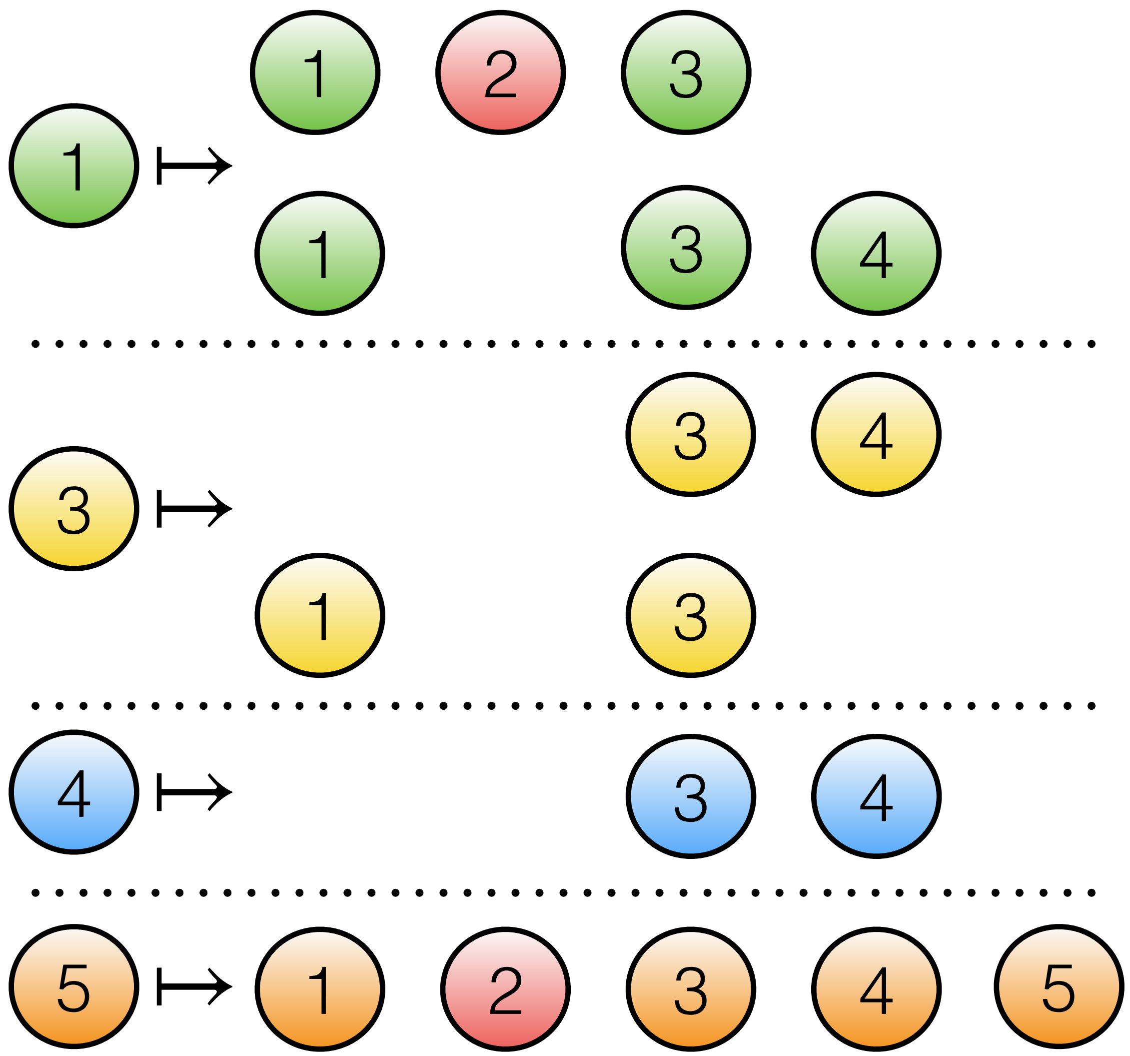
Contributions

- A graph characterization of heterogeneous quorum systems, and its application to optimize reconfiguration and a sink discovery protocol
- Trade-offs between reconfiguration guarantees
- Reconfiguration protocols for joining and **leaving of a process**, and adding and removing of a quorum, and their proofs of correctness

Heterogeneous Quorum Systems (HQS)

$$\mathcal{P} = \mathcal{W} \cup \mathcal{B}, \quad \mathcal{W} = \{1,3,4,5\}, \quad \mathcal{B} = \{2\}$$

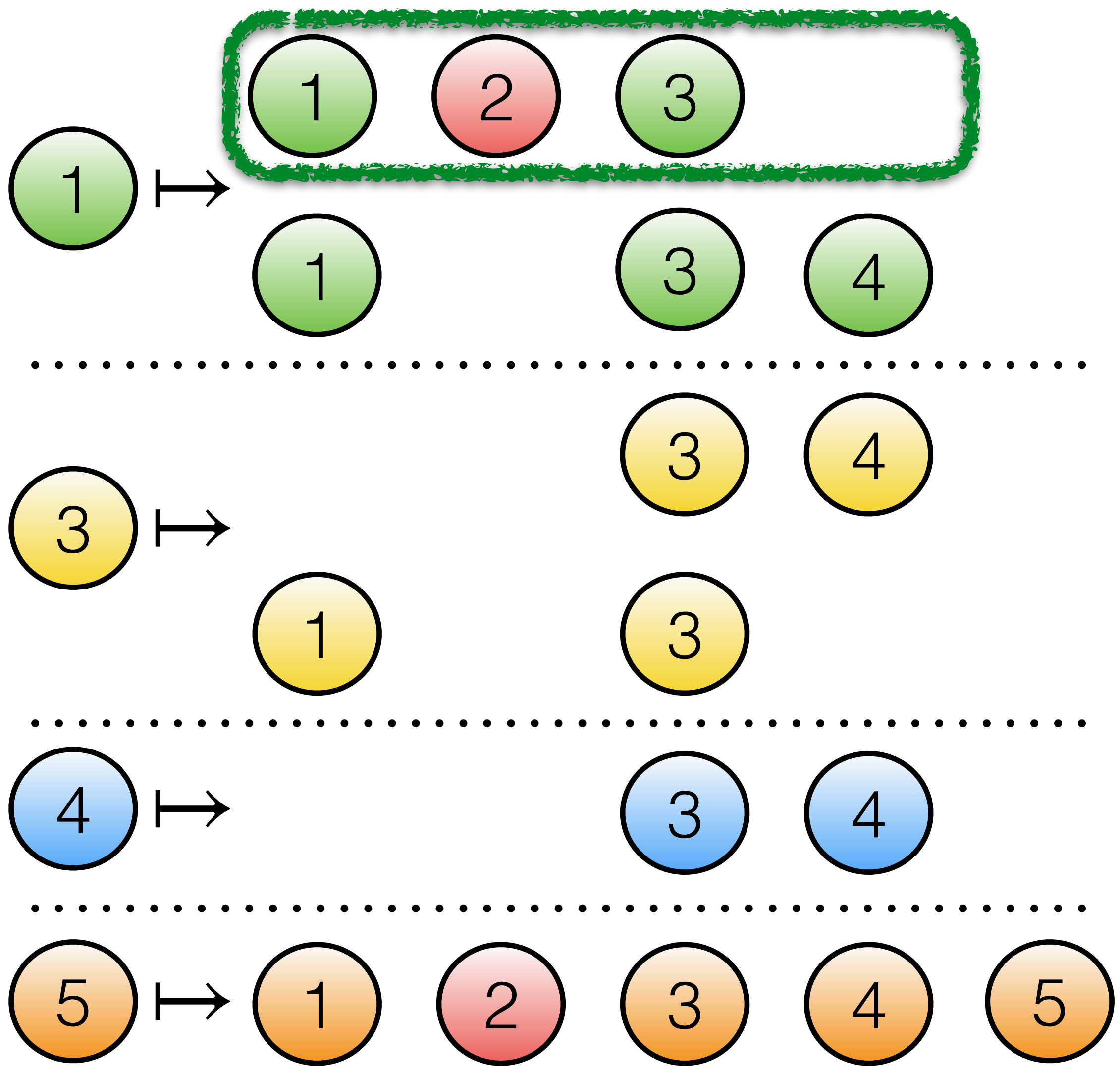
$$\begin{aligned}\mathcal{Q} = \{1 &\mapsto \{\{1,2,3\},\{1,4\}\},\\ 3 &\mapsto \{\{3,4\},\{1,3\}\}\\ 4 &\mapsto \{\{3,4\}\}\\ 5 &\mapsto \{\{1,2,3,5\}\}\}\end{aligned}$$



Heterogeneous Quorum Systems (HQS)

$$\mathcal{P} = \mathcal{W} \cup \mathcal{B}, \quad \mathcal{W} = \{1,3,4,5\}, \quad \mathcal{B} = \{2\}$$

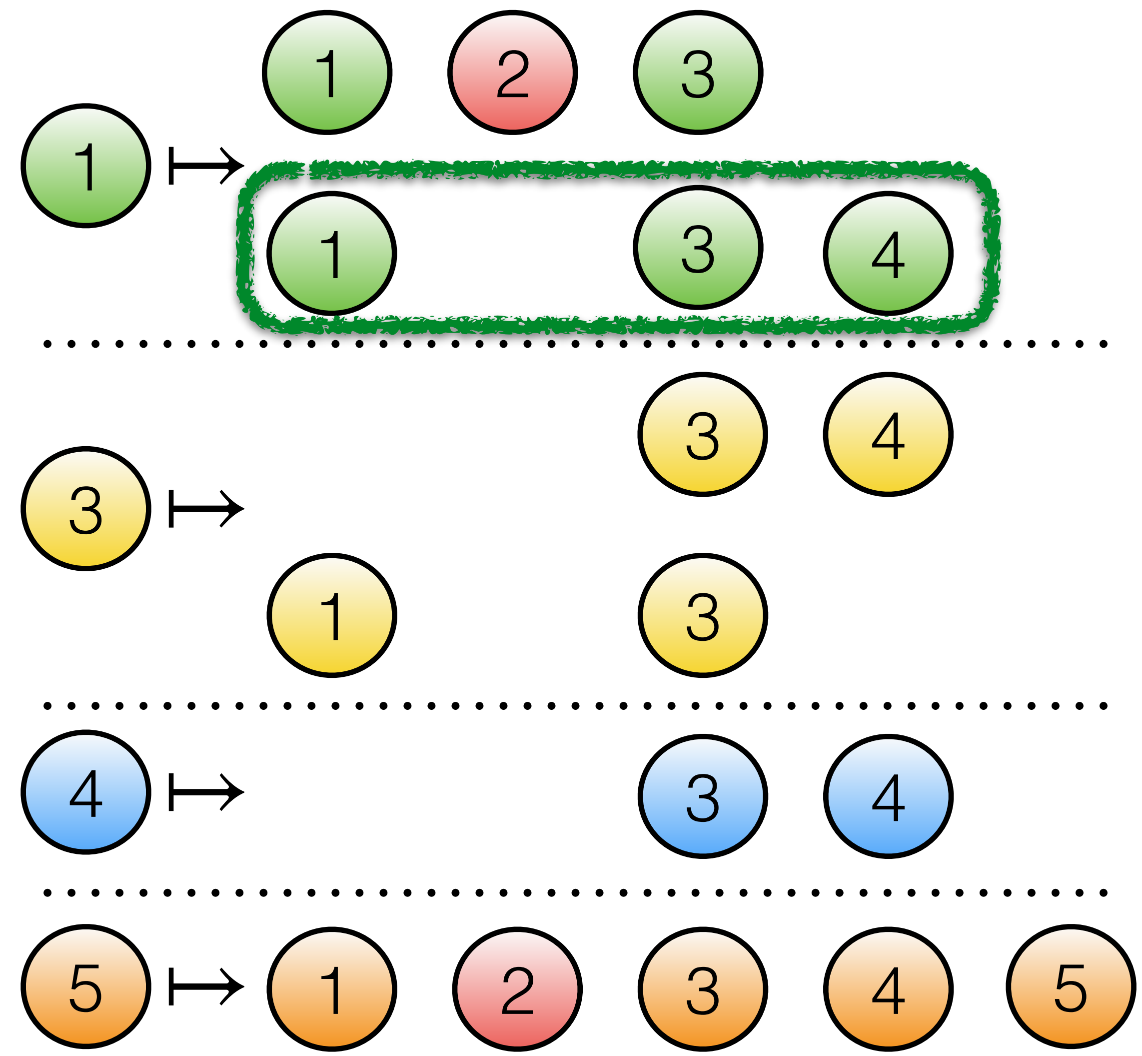
$$\begin{aligned}\mathcal{Q} = \{1 &\mapsto \{\{1,2,3\},\{1,4\}\},\\ 3 &\mapsto \{\{3,4\},\{1,3\}\}\\ 4 &\mapsto \{\{3,4\}\}\\ 5 &\mapsto \{\{1,2,3,5\}\}\}\end{aligned}$$



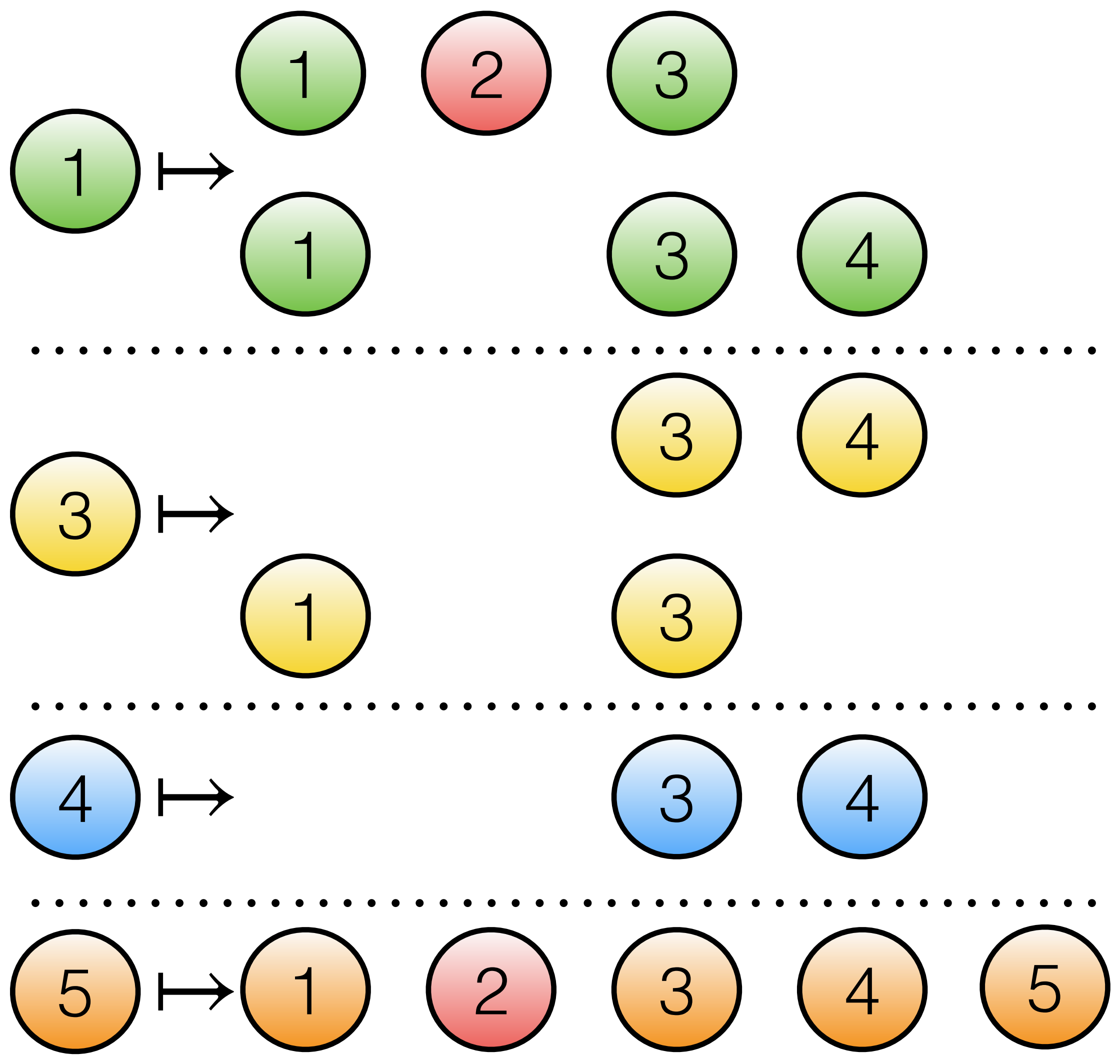
Heterogeneous Quorum Systems (HQS)

$$\mathcal{P} = \mathcal{W} \cup \mathcal{B}, \quad \mathcal{W} = \{1, 3, 4, 5\}, \quad \mathcal{B} = \{2\}$$

$$\begin{aligned} \mathcal{Q} = \{1 &\mapsto \{\{1, 2, 3\}, \{1, 4\}\}, \\ 3 &\mapsto \{\{3, 4\}, \{1, 3\}\} \\ 4 &\mapsto \{\{3, 4\}\} \\ 5 &\mapsto \{\{1, 2, 3, 5\}\}\} \end{aligned}$$

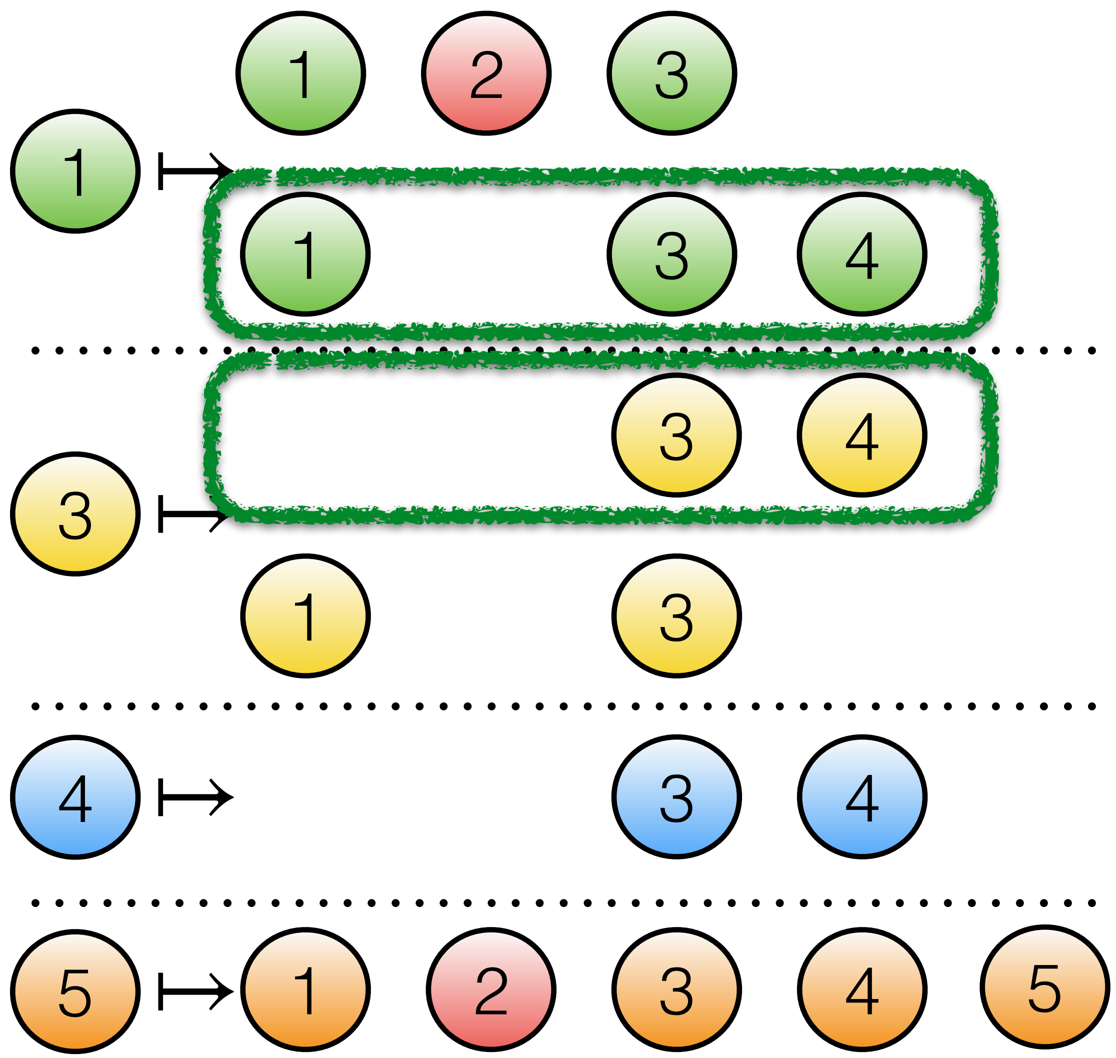


Quorum Intersection at $\mathcal{O}$

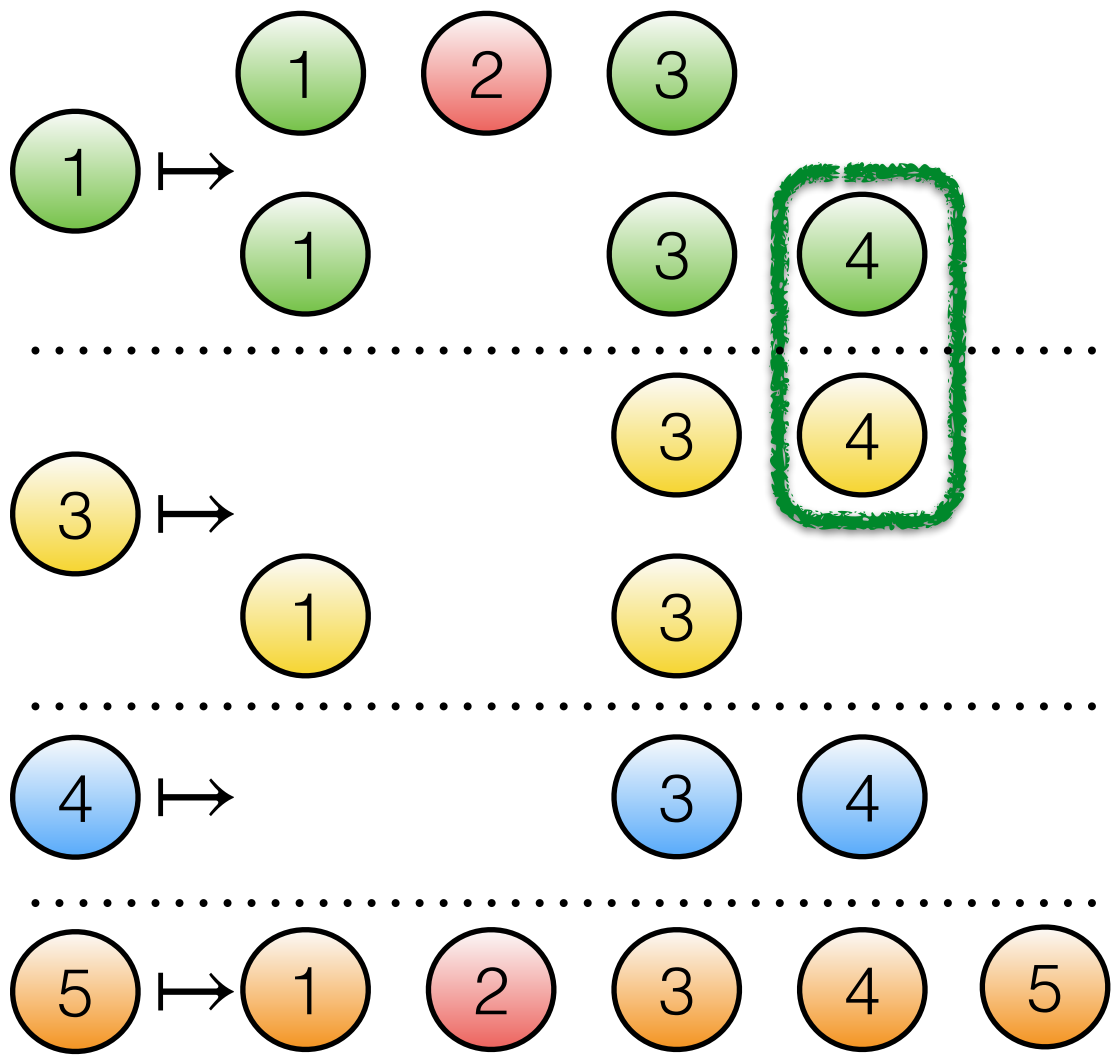


$$\mathcal{O} = \{1, 3, 4\}$$

Quorum Intersection at $\mathcal{O}$

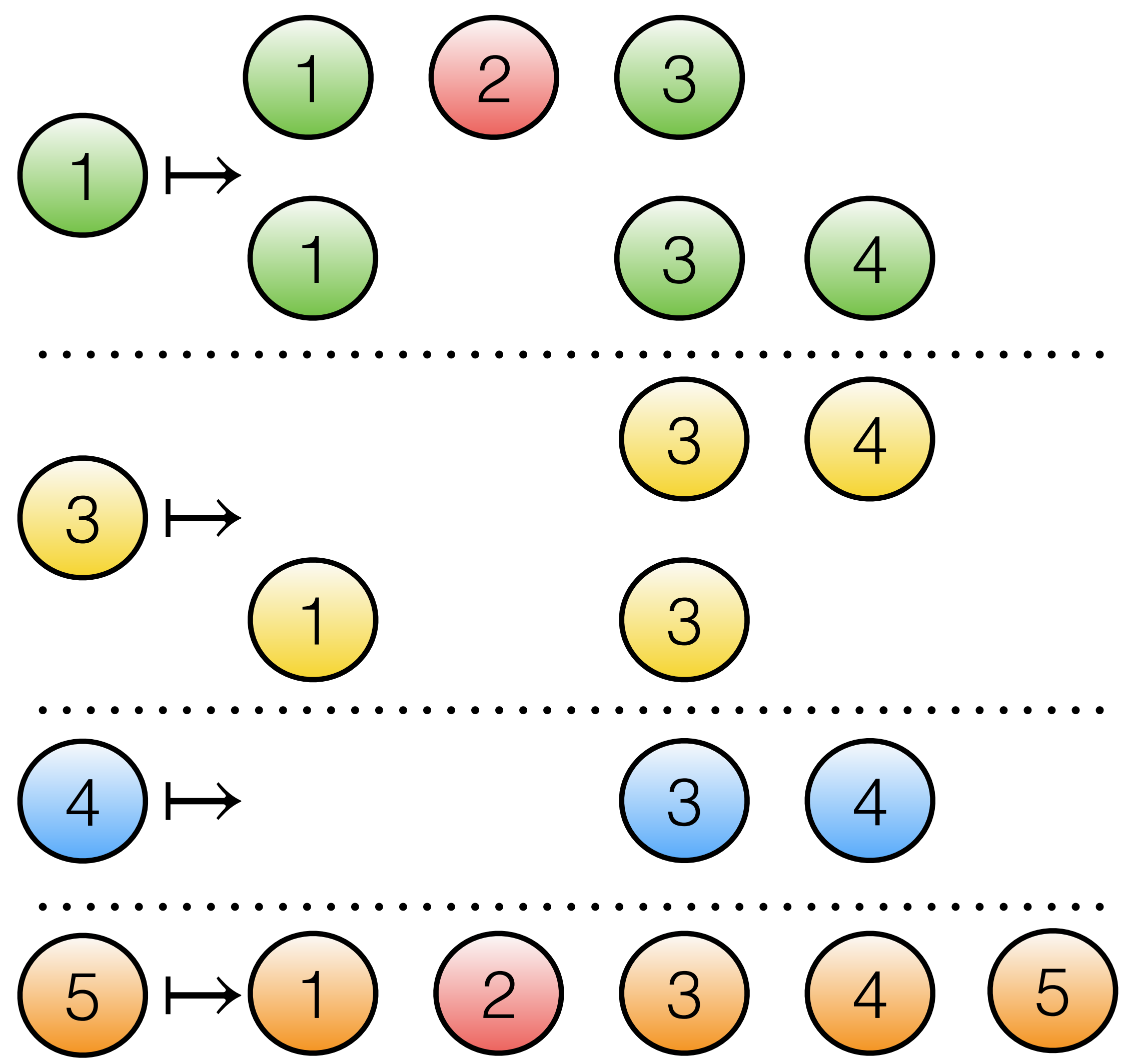


$$\mathcal{O} = \{1, 3, 4\}$$

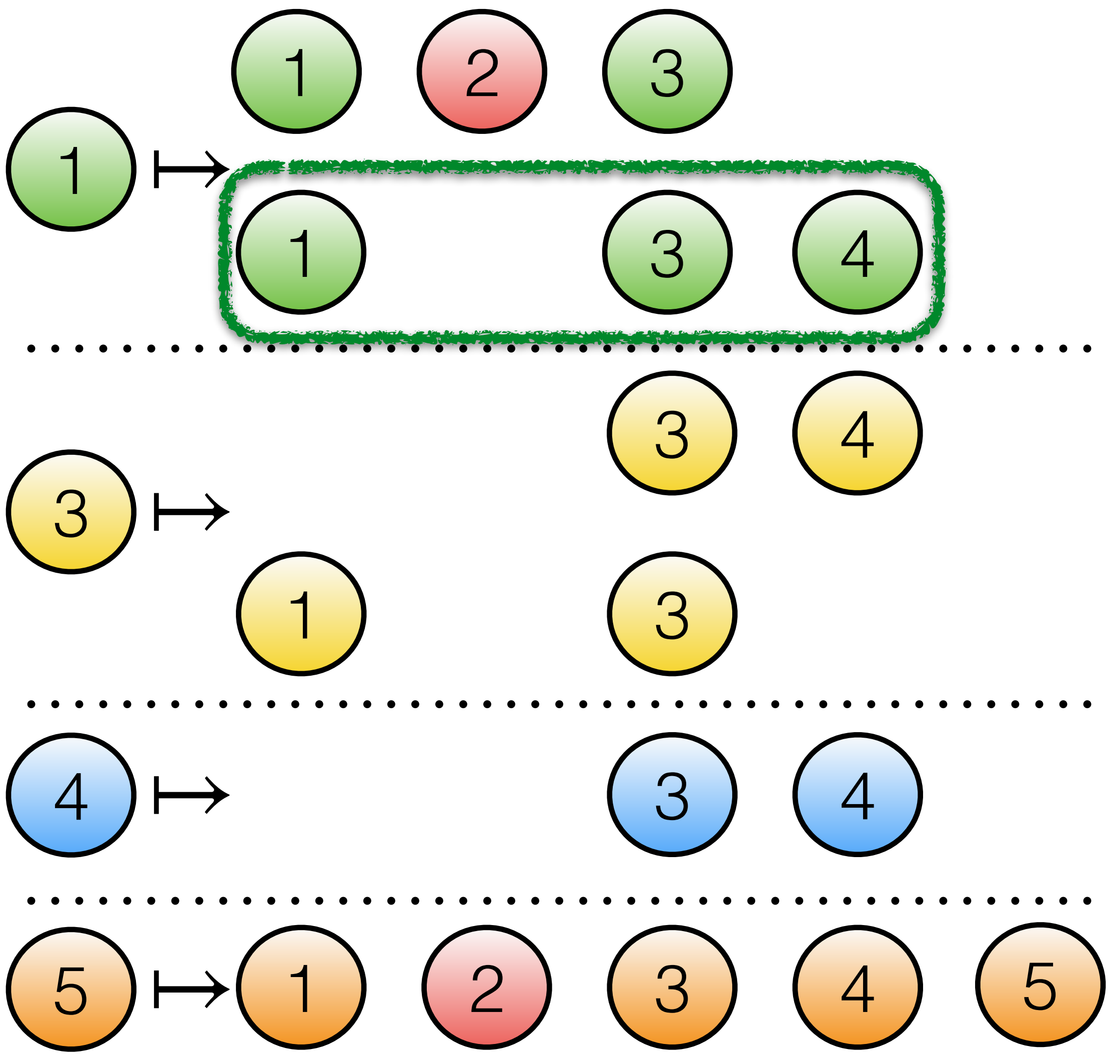


$$\mathscr{O} = \{1, 3, 4\}$$

Availability inside $\mathcal{O}$

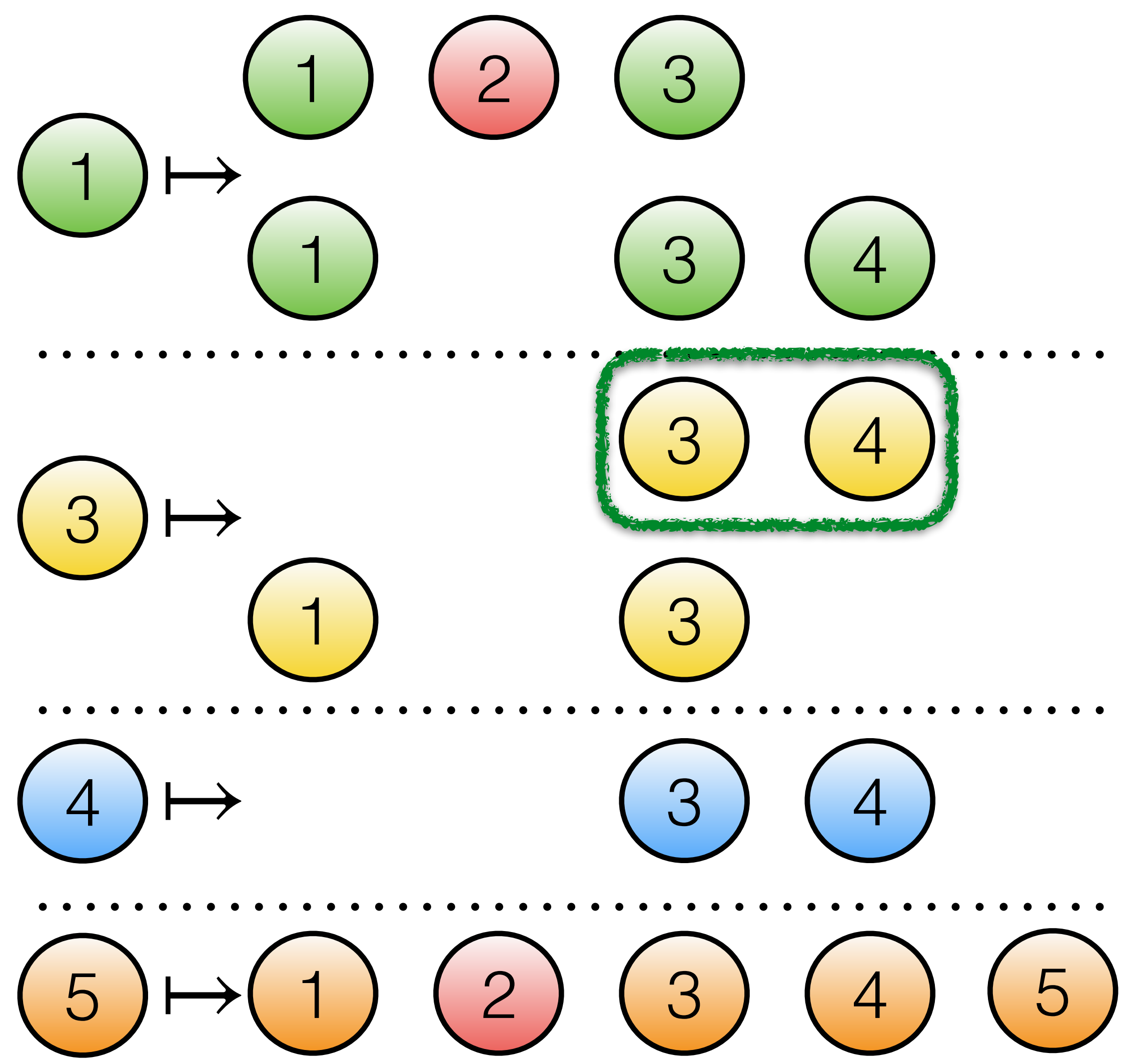


$$\mathcal{O} = \{1, 3, 4\}$$



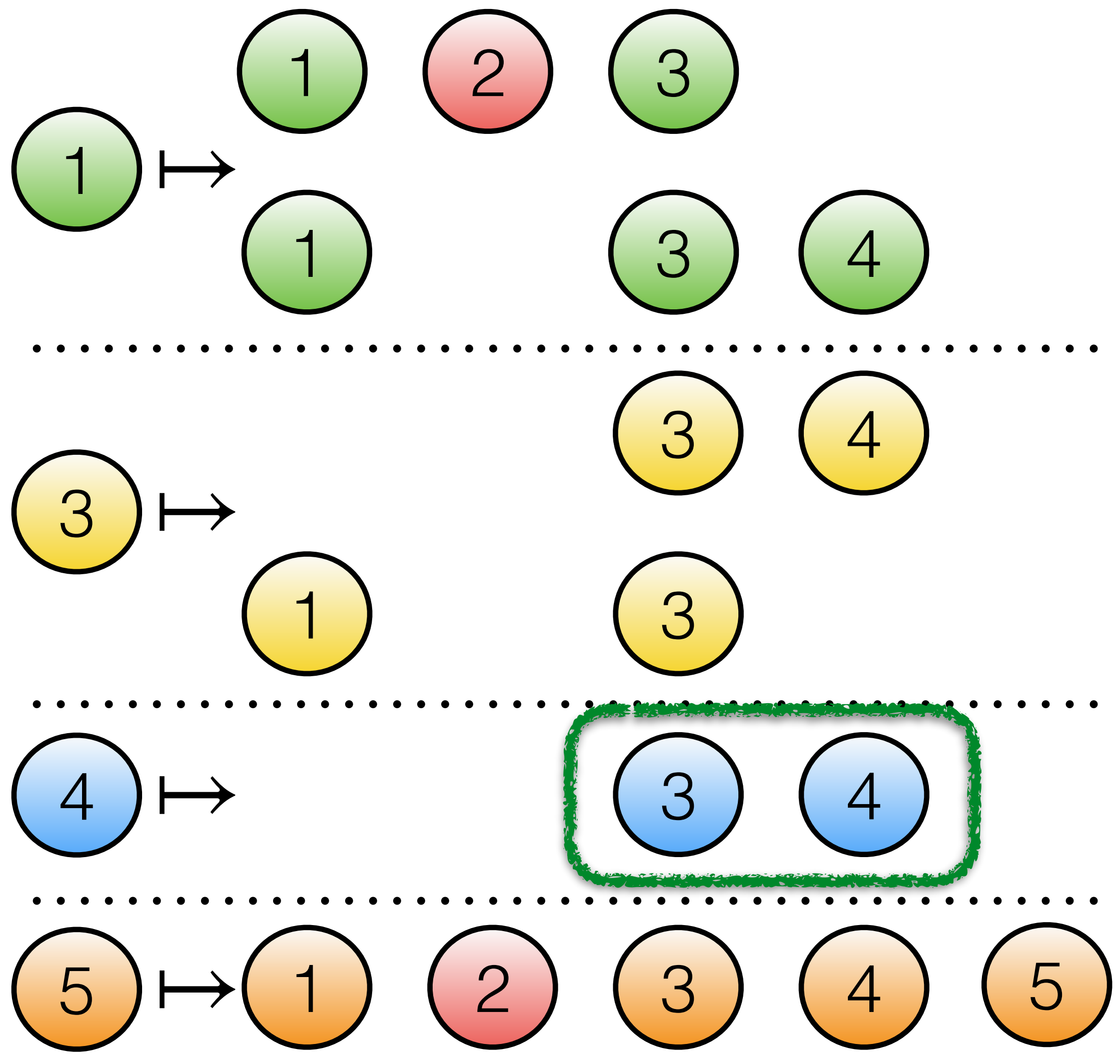
$$\mathcal{O} = \{1, 3, 4\}$$

Availability inside $\mathcal{O}$



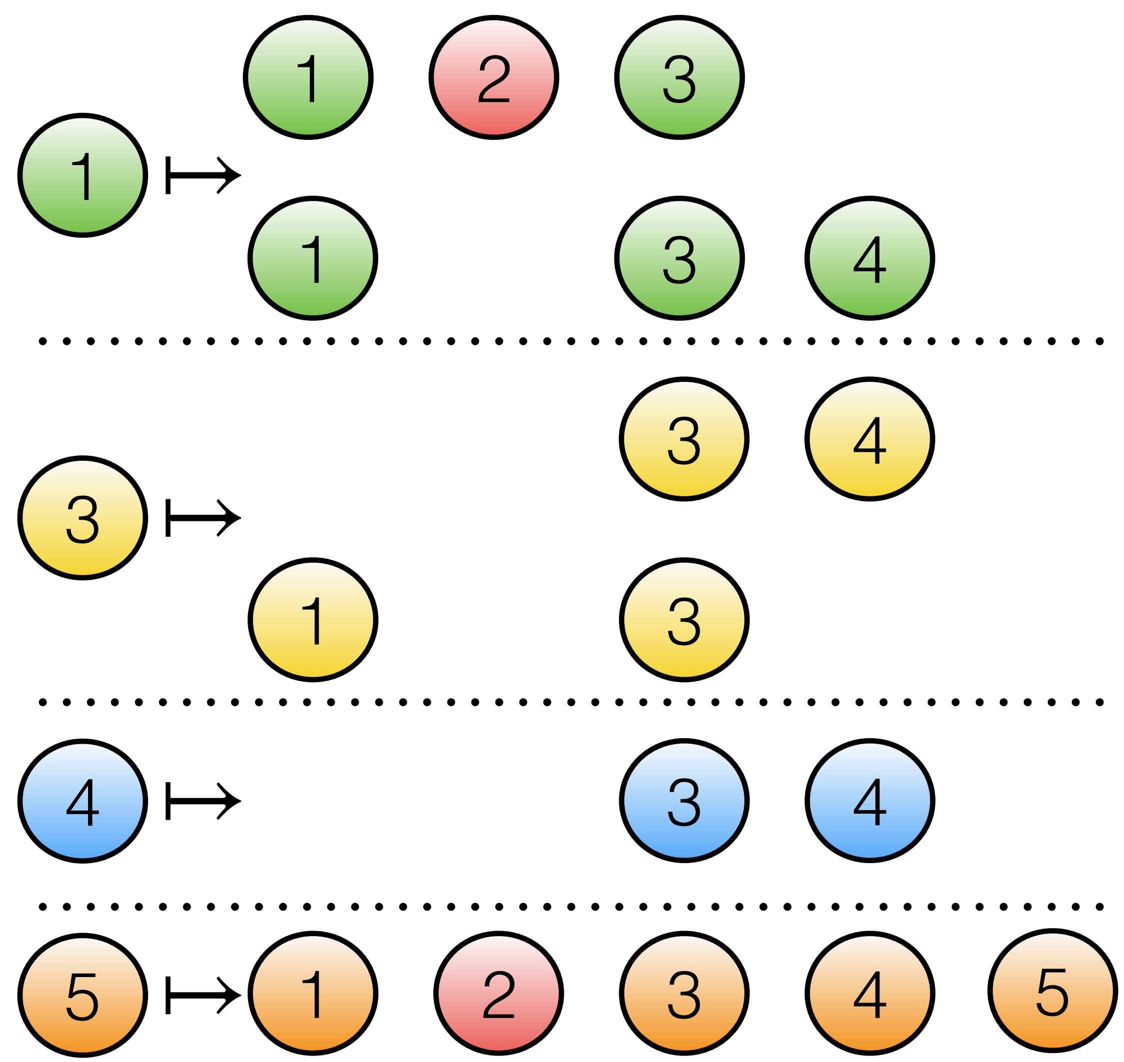
$$\mathcal{O} = \{1, 3, 4\}$$

Availability inside $\mathcal{O}$



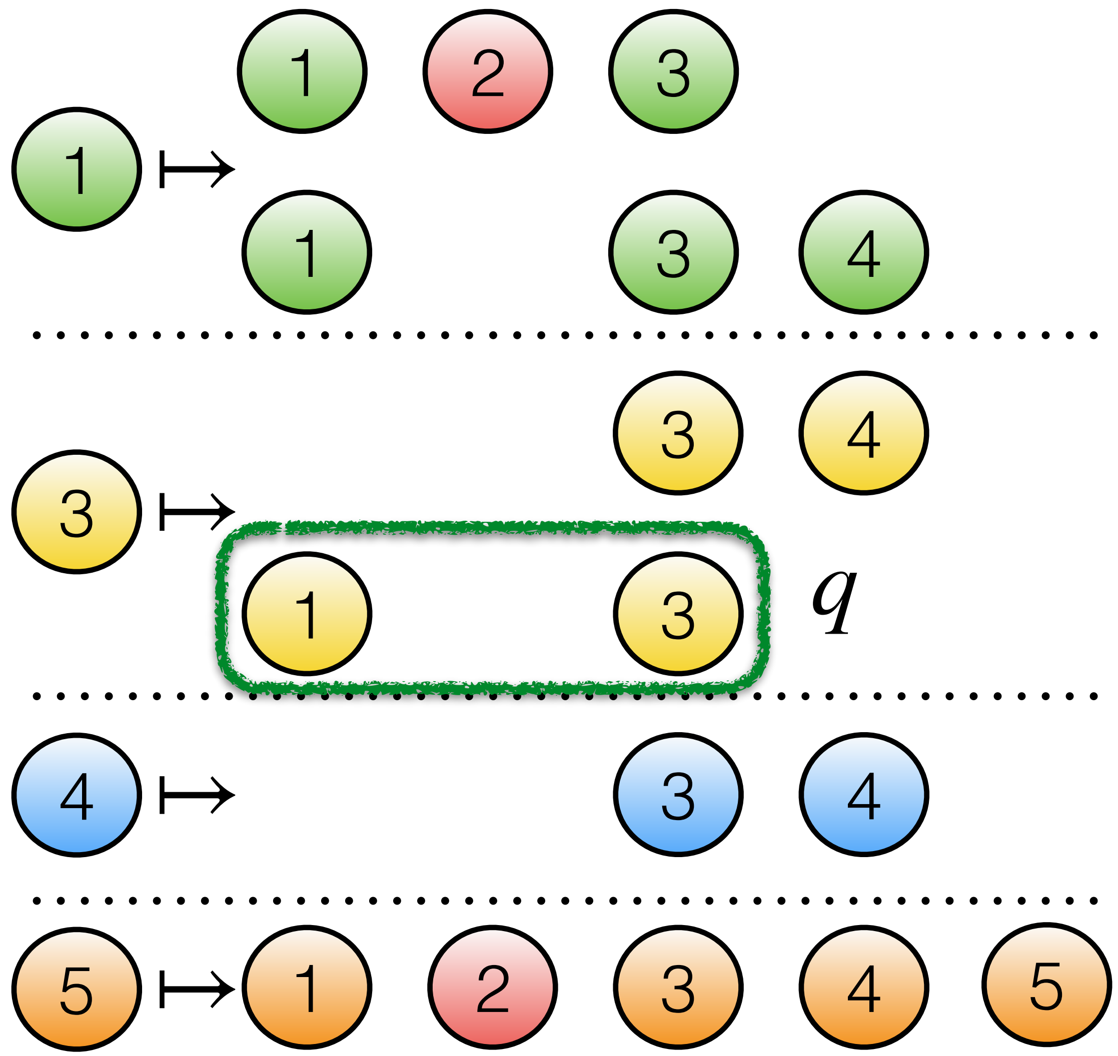
$$\mathcal{O} = \{1, 3, 4\}$$

Quorum Inclusion for $\mathcal{O}$



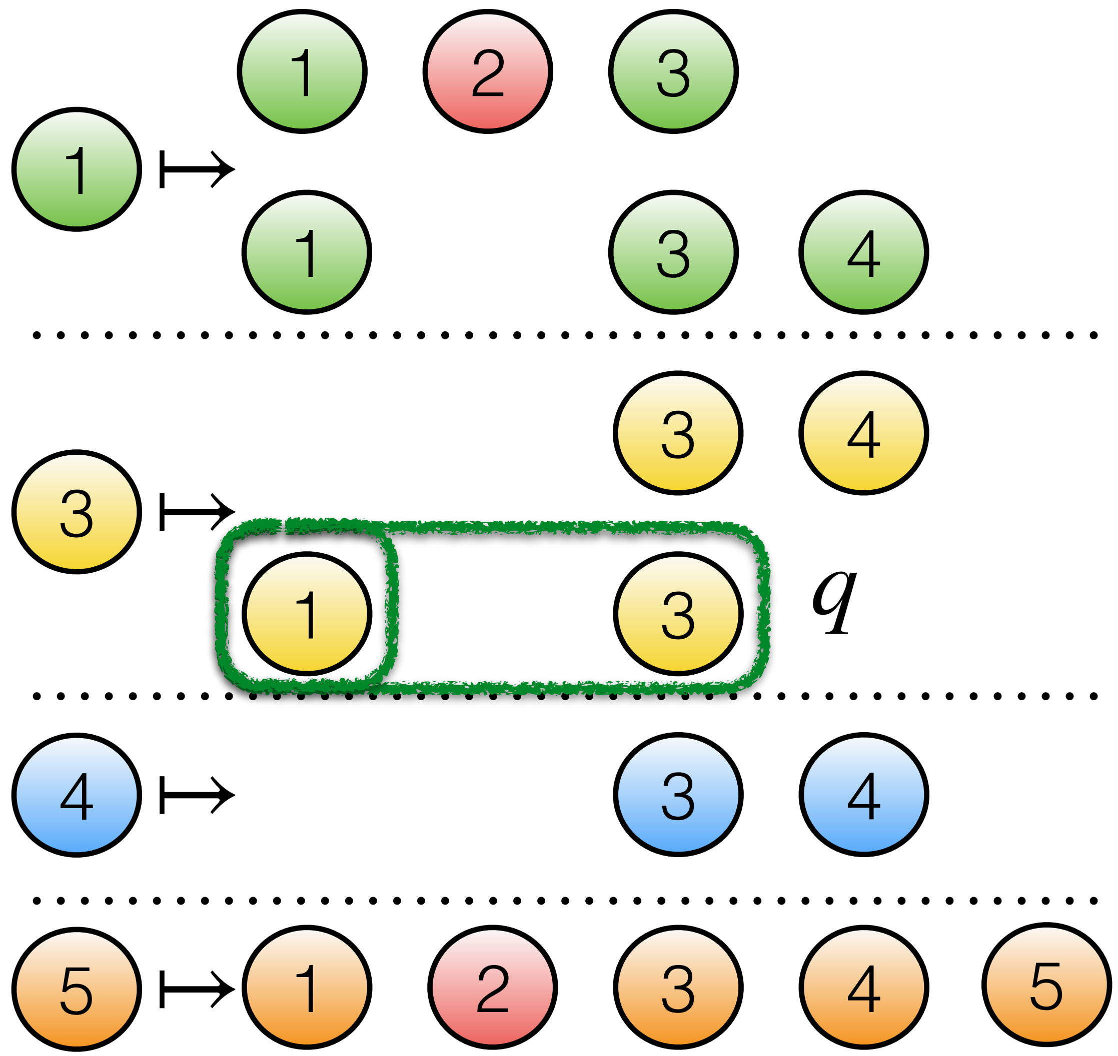
$$\mathcal{O} = \{1, 3, 4\}$$

Quorum Inclusion for $\mathcal{O}$



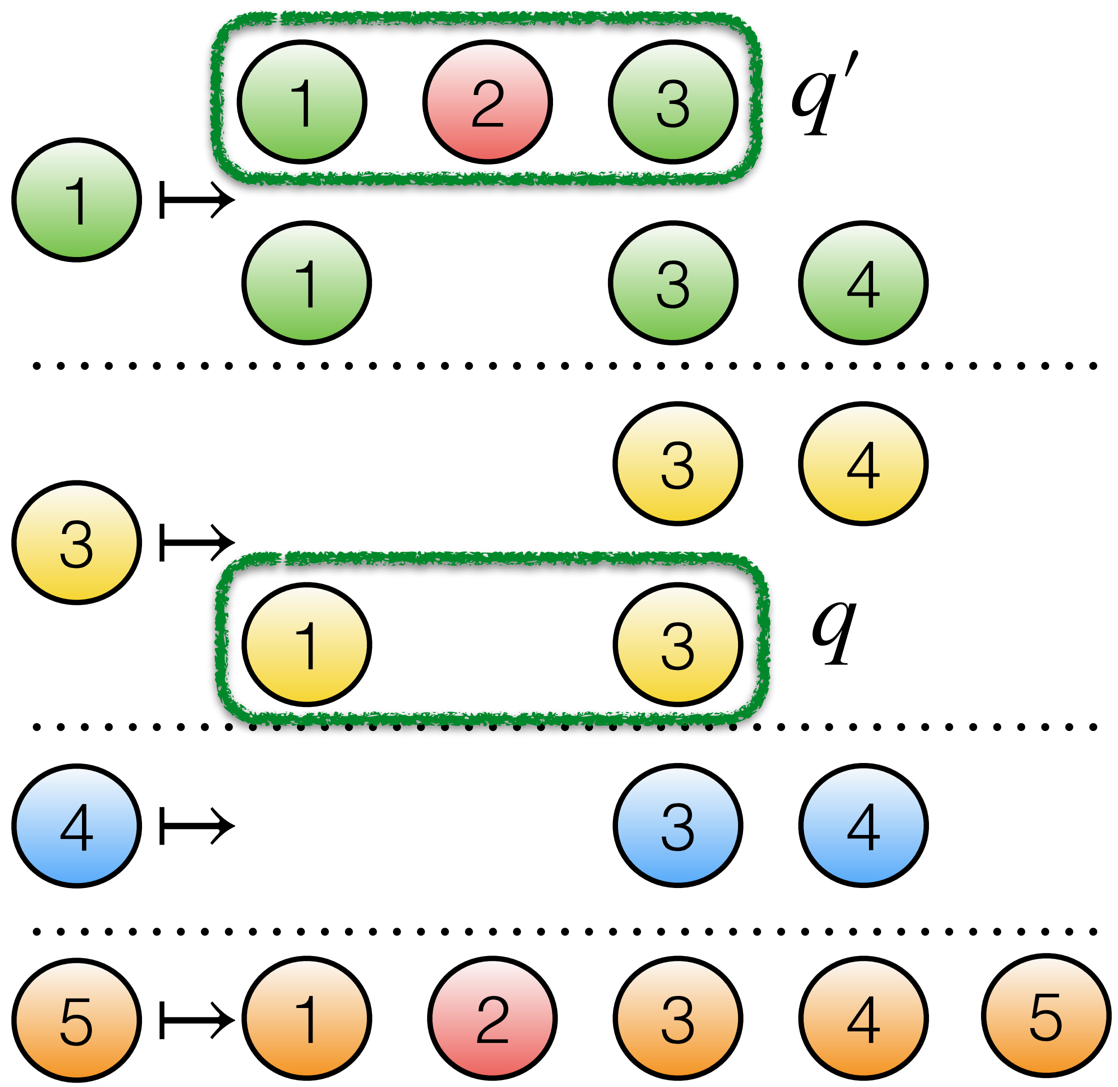
$$\mathcal{O} = \{1, 3, 4\}$$

Quorum Inclusion for $\mathcal{O}$



$$\mathcal{O} = \{1, 3, 4\}$$

Quorum Inclusion for $\mathcal{O}$



$$\mathcal{O} = \{1, 3, 4\}$$

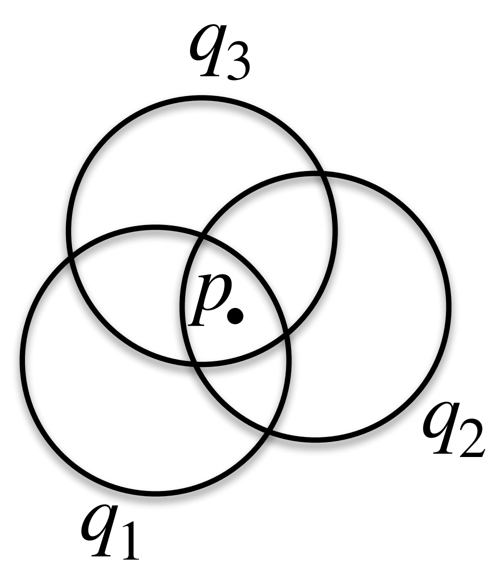
There is a set of well-behaved processes $\mathcal{O}$ such that the quorum system has

- quorum intersection at $\mathcal{O}$,
- quorum availability inside $\mathcal{O}$, and
- quorum inclusion for $\mathcal{O}$.

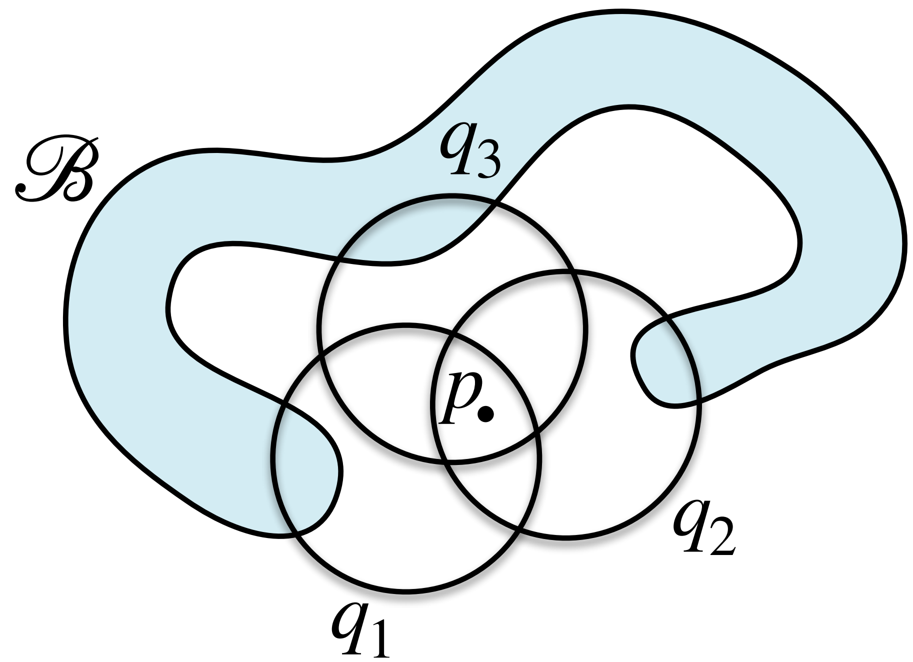
Blocking Set

p

Blocking Set



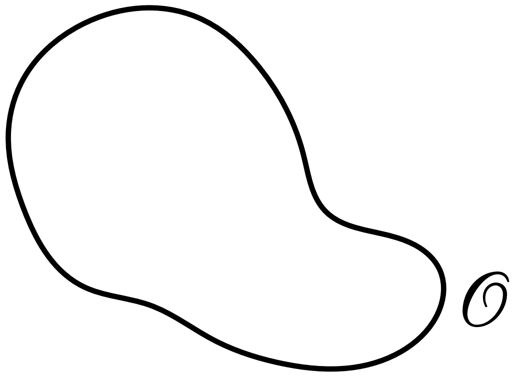
Blocking Set



Lemma for blocking set

If

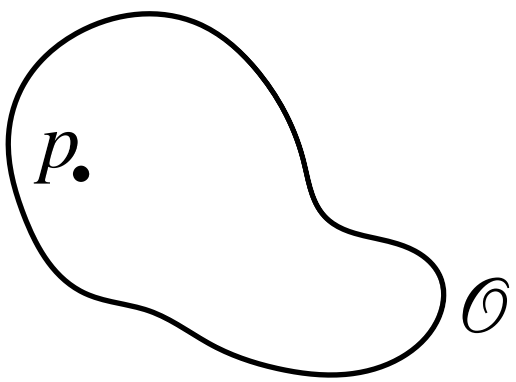
- Quorum system $\mathscr{Q}$ is available inside $\mathscr{O}$



Lemma for blocking set

If

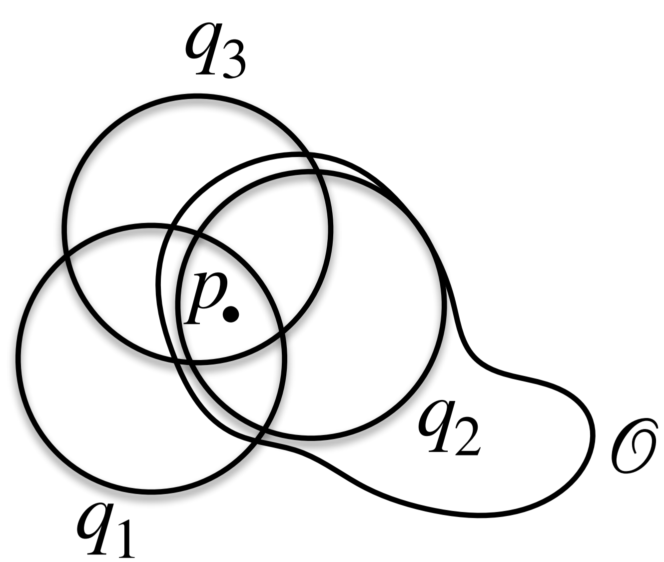
- Quorum system $\mathcal{Q}$ is available inside $\mathcal{O}$
- Process p is in $\mathcal{O}$



Lemma for blocking set

If

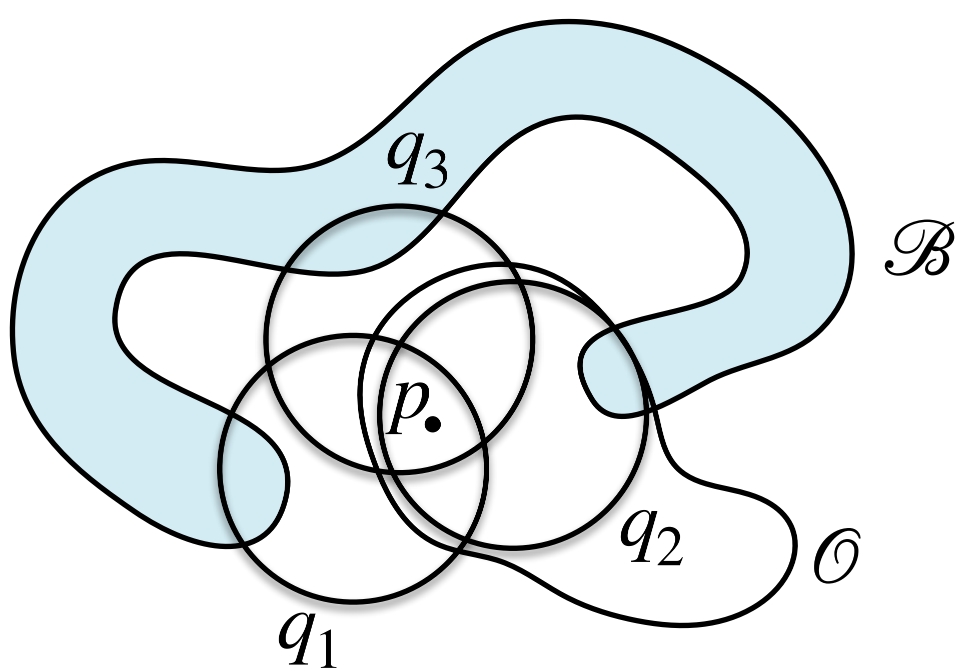
- Quorum system $\mathcal{Q}$ is available inside $\mathcal{O}$
- Process p is in $\mathcal{O}$



Lemma for blocking set

If

- Quorum system $\mathscr{Q}$ is available inside $\mathscr{O}$
- Process p is in $\mathscr{O}$
- $\mathscr{B}$ is a blocking set for p



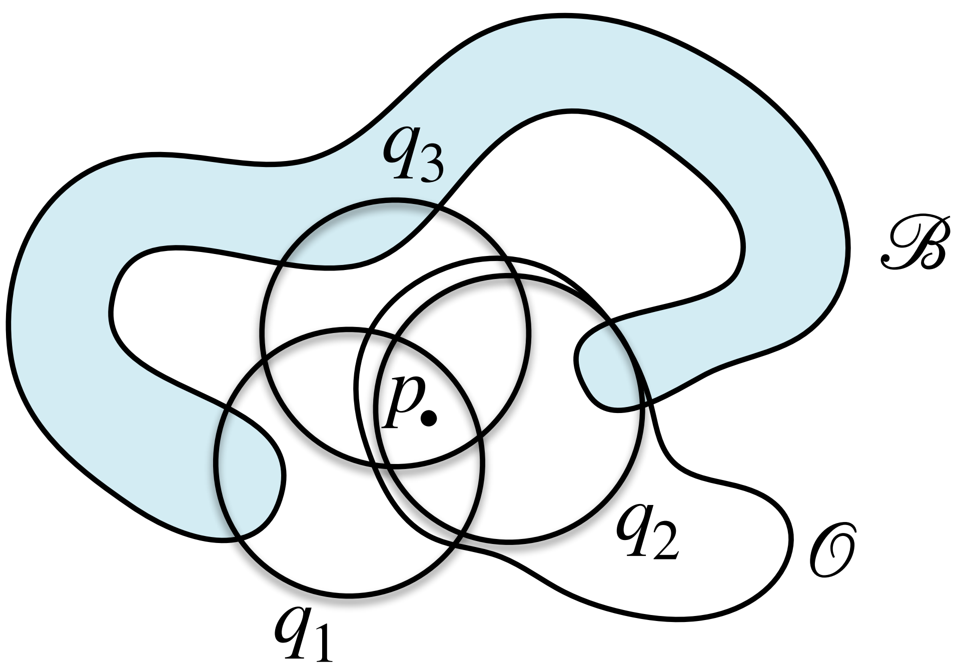
Lemma for blocking set

If

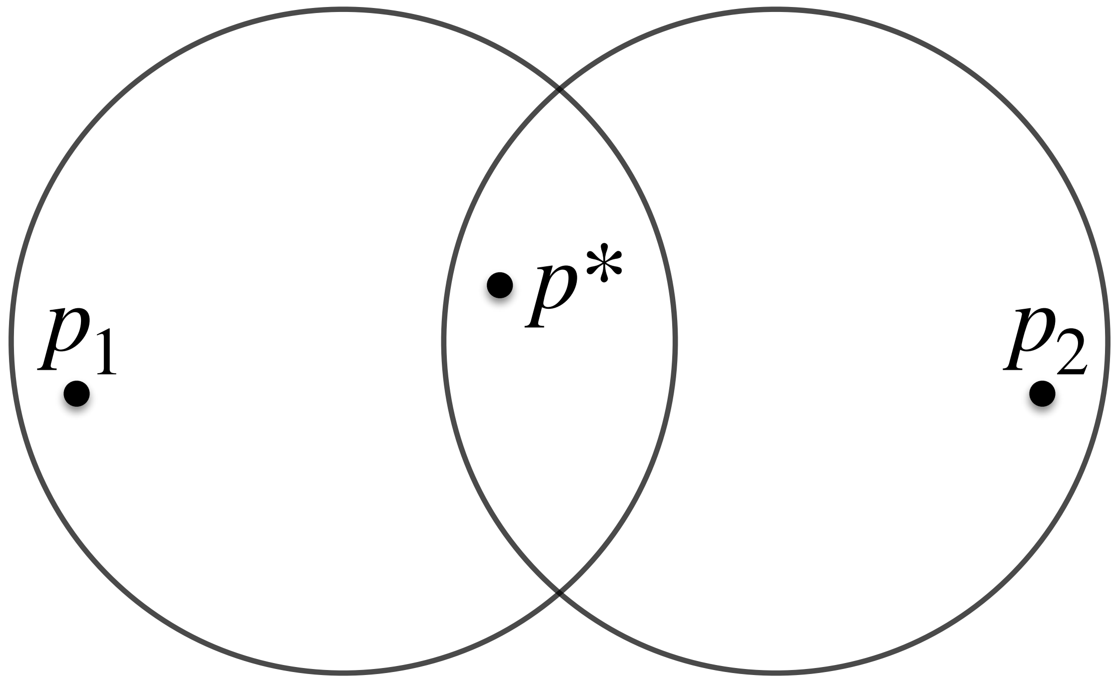
- Quorum system $\mathscr{Q}$ is available inside $\mathscr{O}$
- Process p is in $\mathscr{O}$
- $\mathscr{B}$ is a blocking set for p

Then

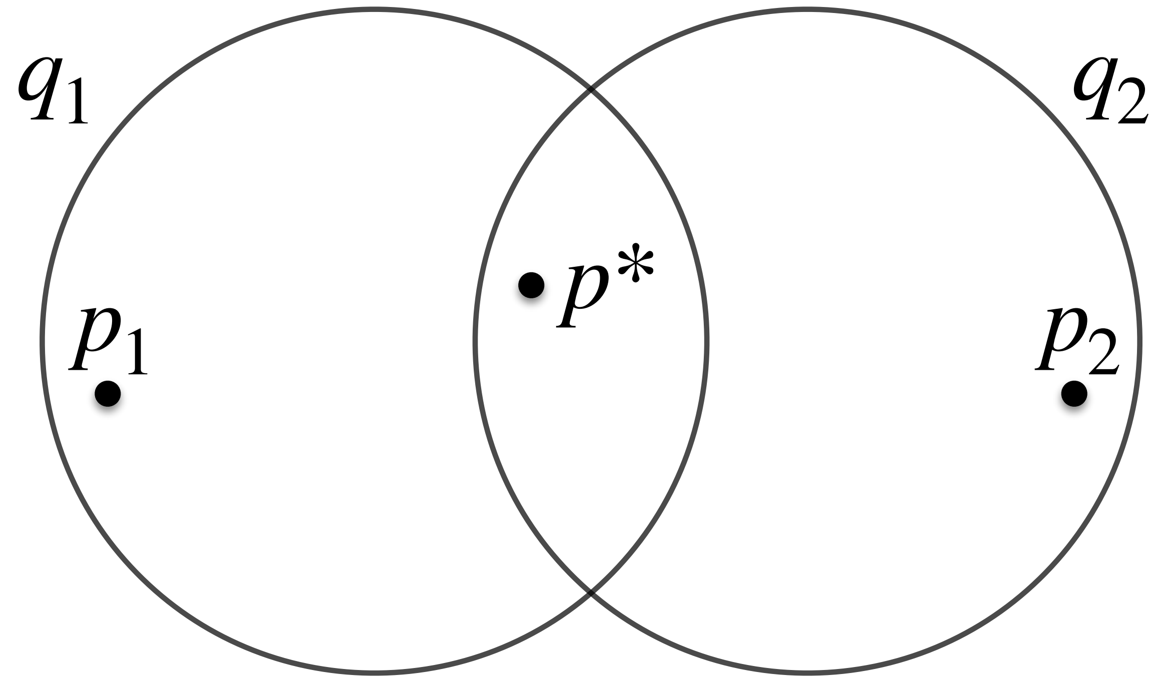
- $\mathscr{B}$ intersects with $\mathscr{O}$



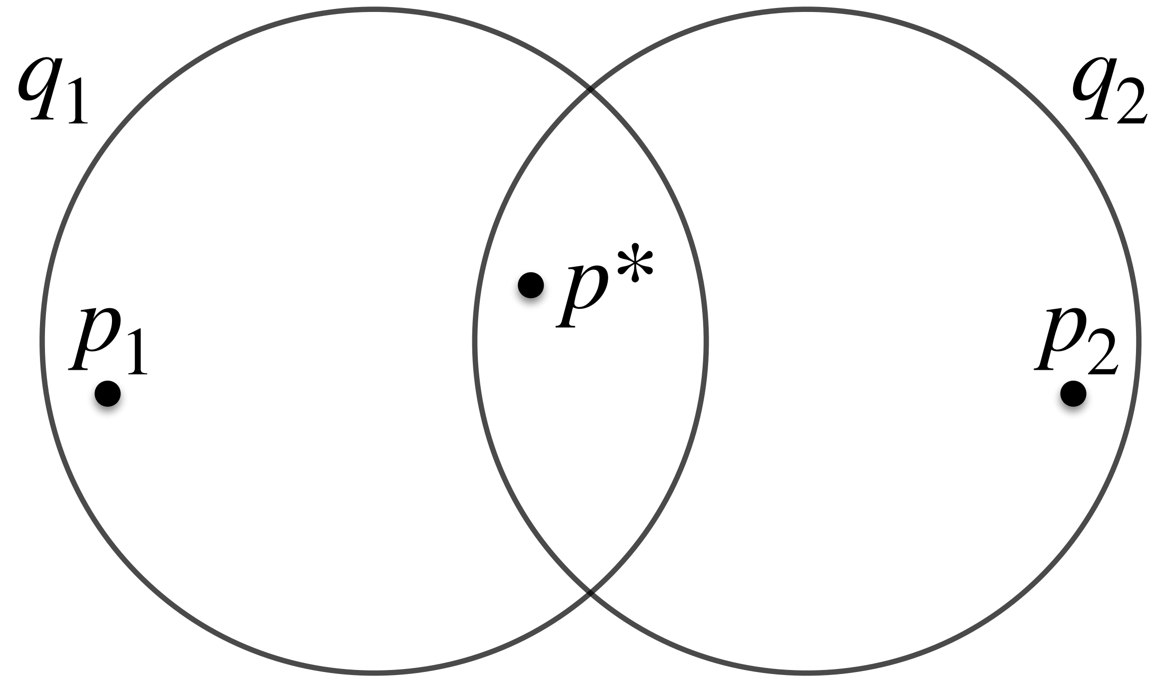
Leave Protocol



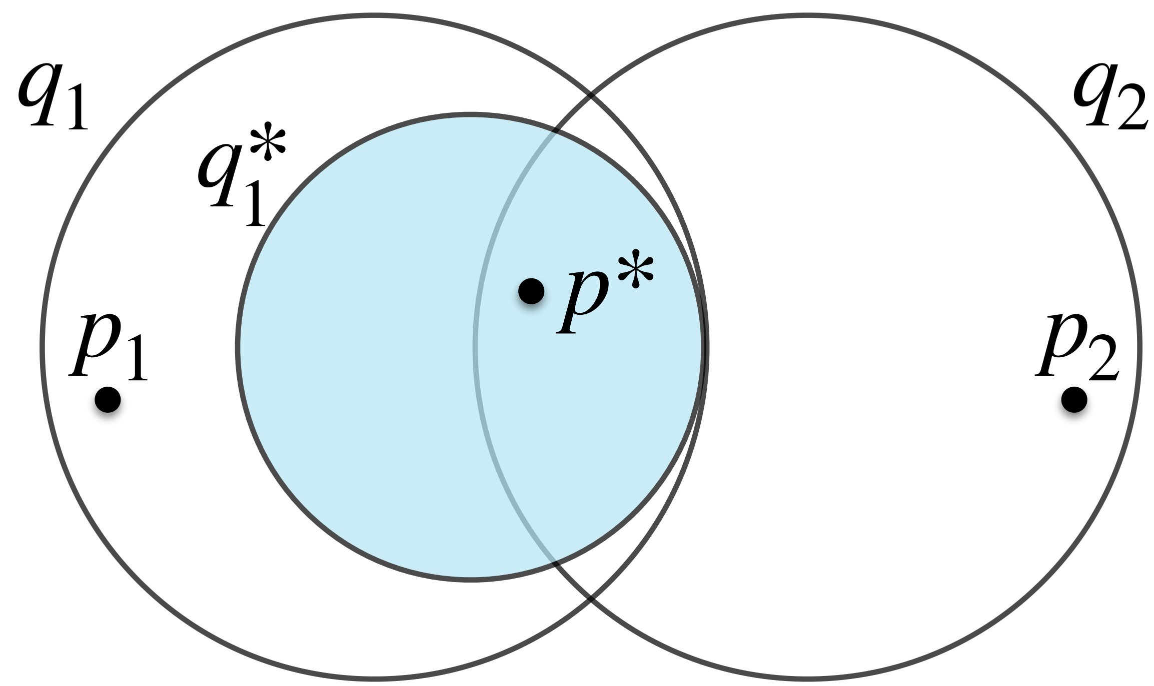
Leave Protocol



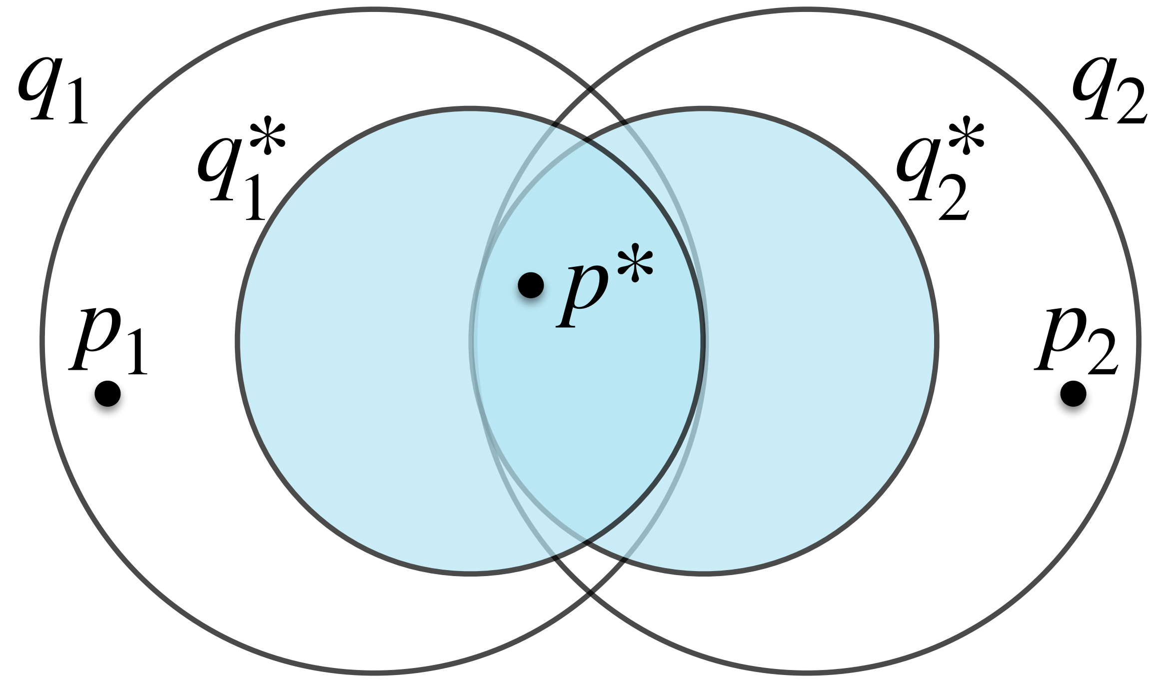
Leave Protocol



$\mathcal{Q}$ has quorum inclusion for $\mathcal{O}$

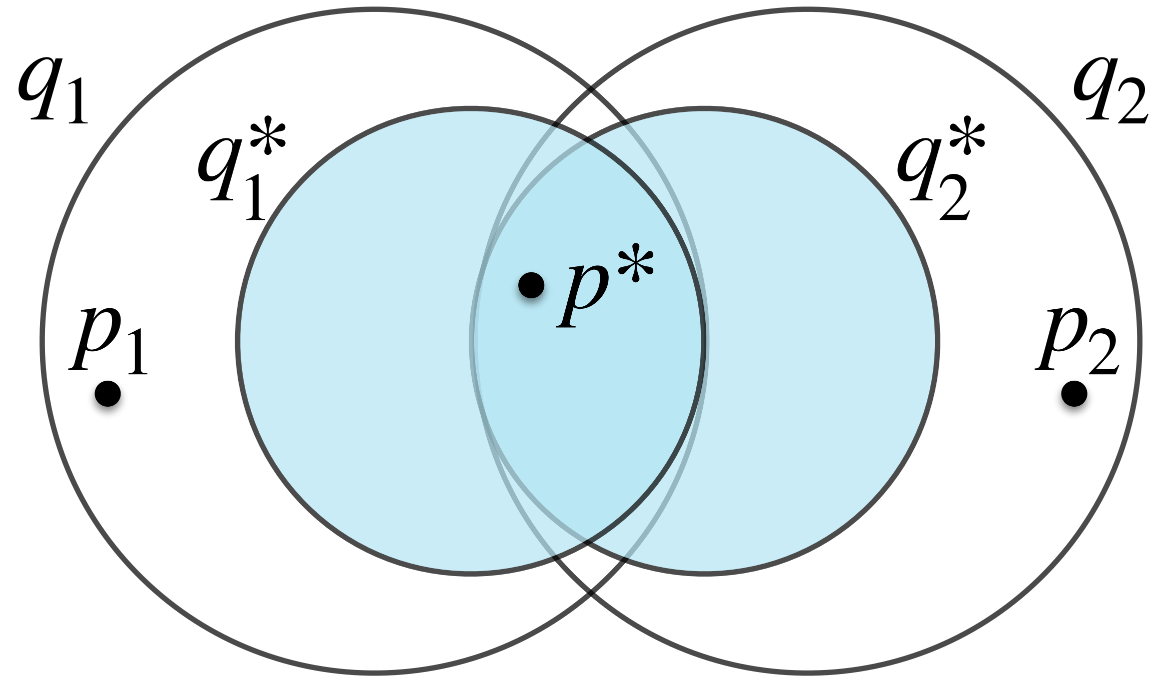


$\mathcal{Q}$ has quorum inclusion for $\mathcal{O}$

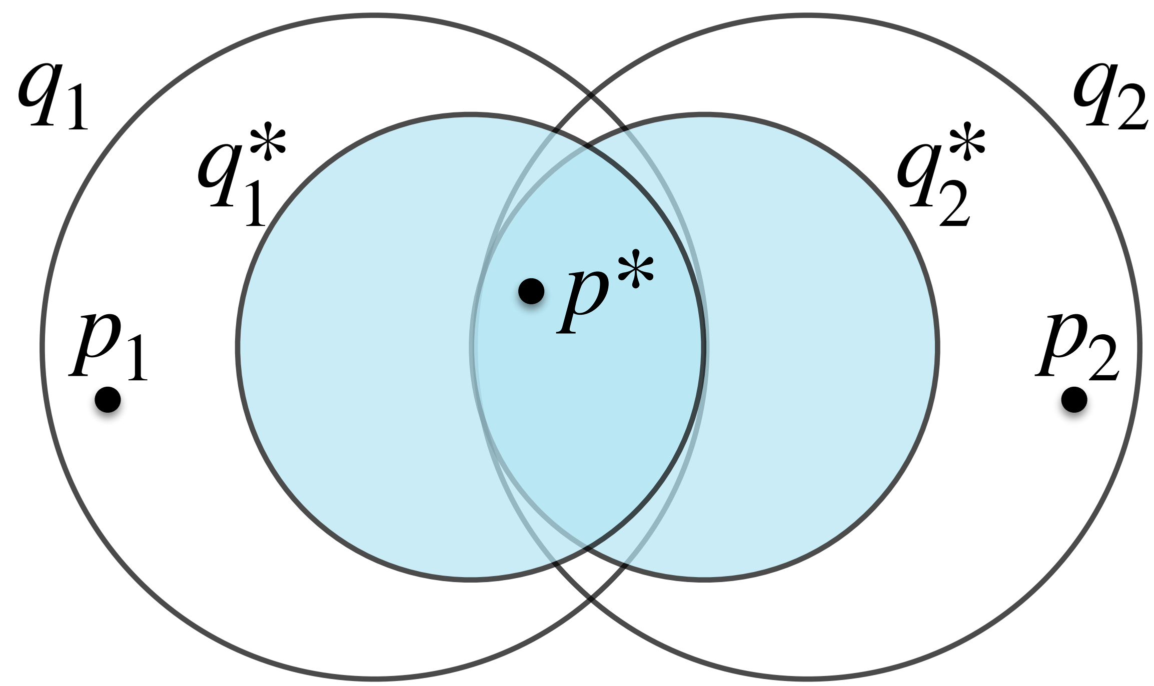


$\mathcal{Q}$ has quorum inclusion for $\mathcal{O}$

Leave Protocol

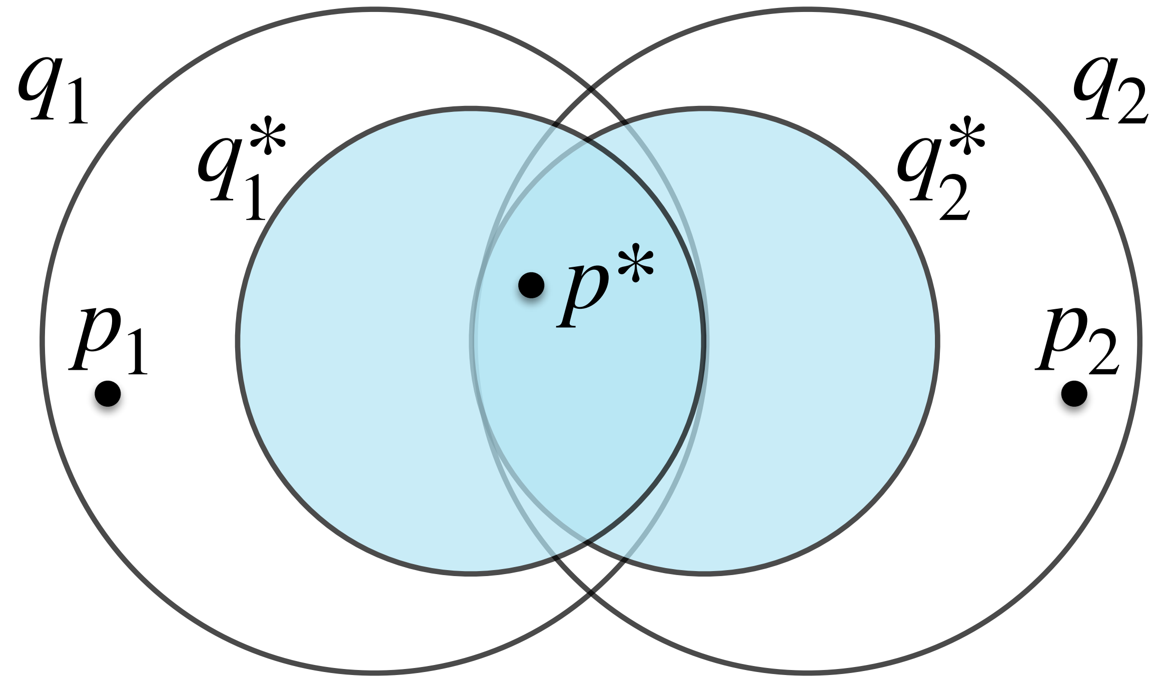


Leave Protocol



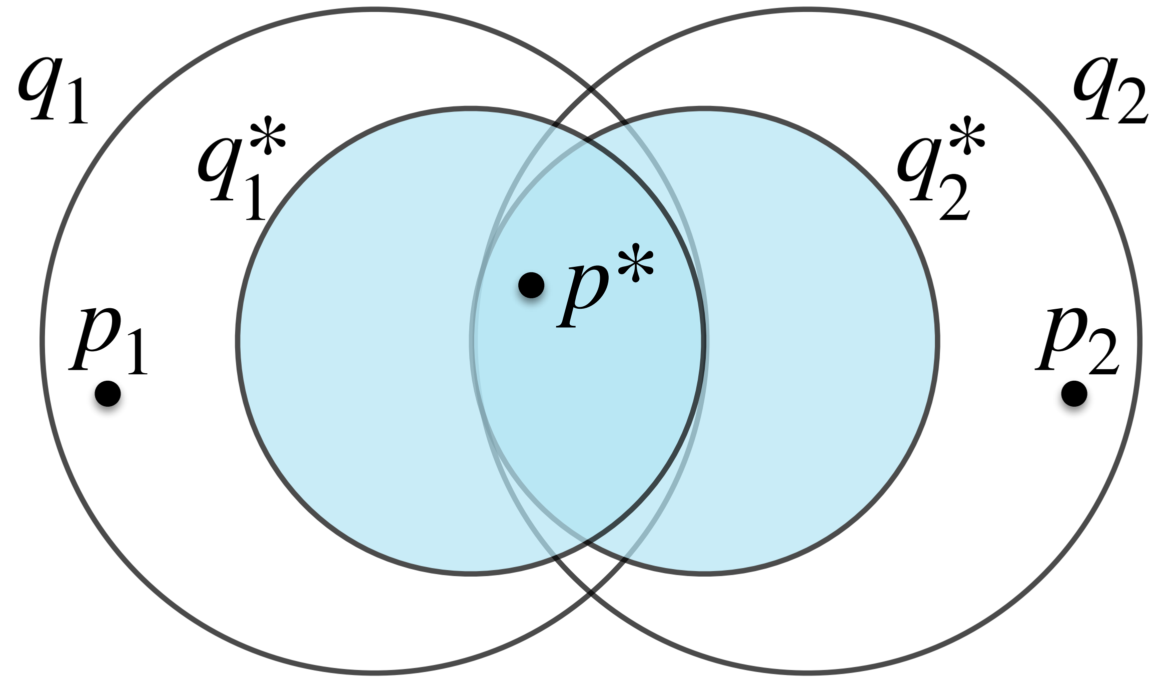
$(q_1^* \cap q_2^*) \setminus \{p^*\}$ is p^*-blocking

Leave Protocol



$(q_1^* \cap q_2^*) \setminus \{p^*\}$ is p^*-blocking

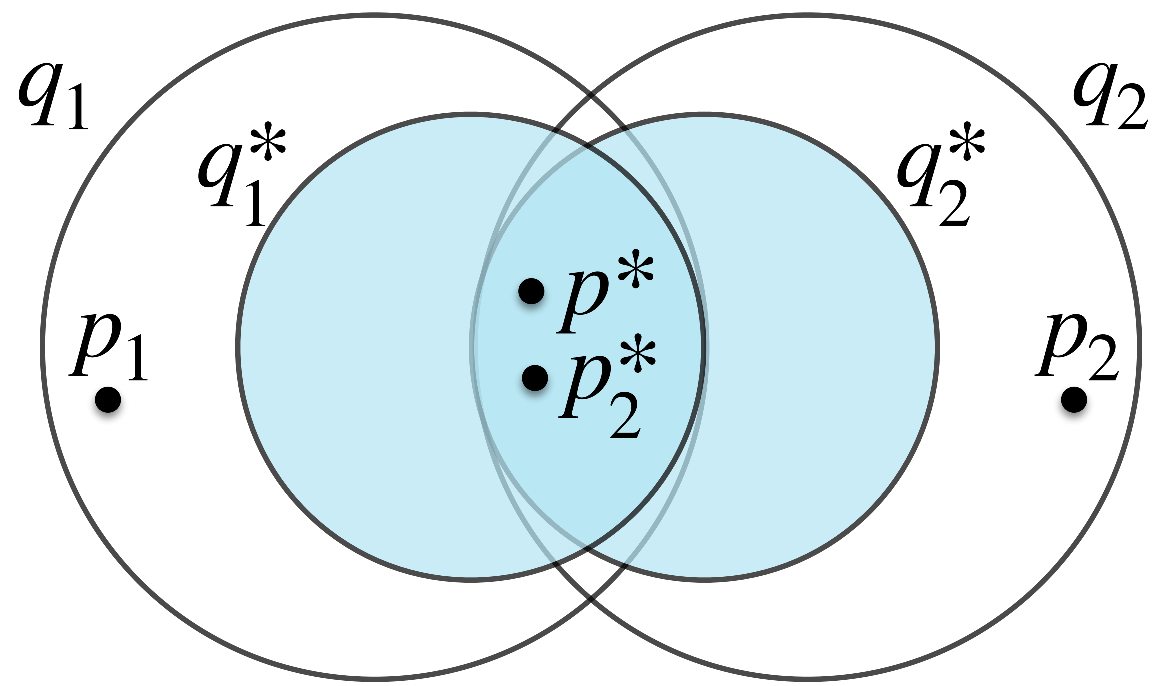
$\mathcal{Q}$ is available inside $\mathcal{O}$



$(q_1^* \cap q_2^*) \setminus \{p^*\}$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p^*\}$ intersects $\mathcal{O}$

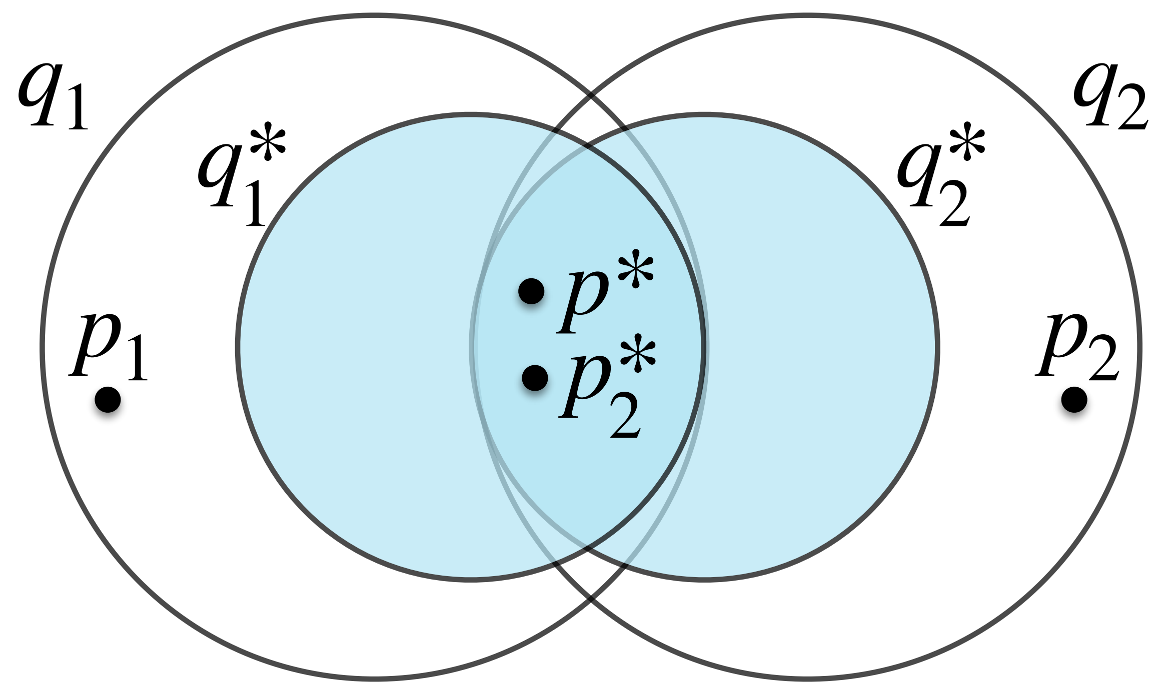
$\mathcal{Q}$ is available inside $\mathcal{O}$



$(q_1^* \cap q_2^*) \setminus \{p^*\}$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p^*\}$ intersects $\mathcal{O}$

$\mathcal{Q}$ is available inside $\mathcal{O}$



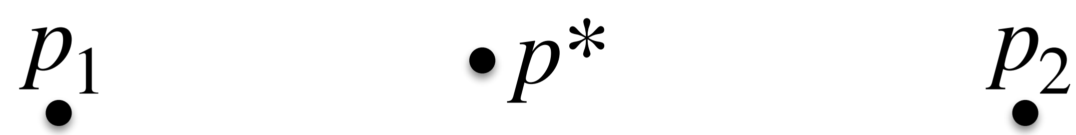
$(q_1^* \cap q_2^*) \setminus \{p^*\}$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p^*\}$ intersects $\mathcal{O}$

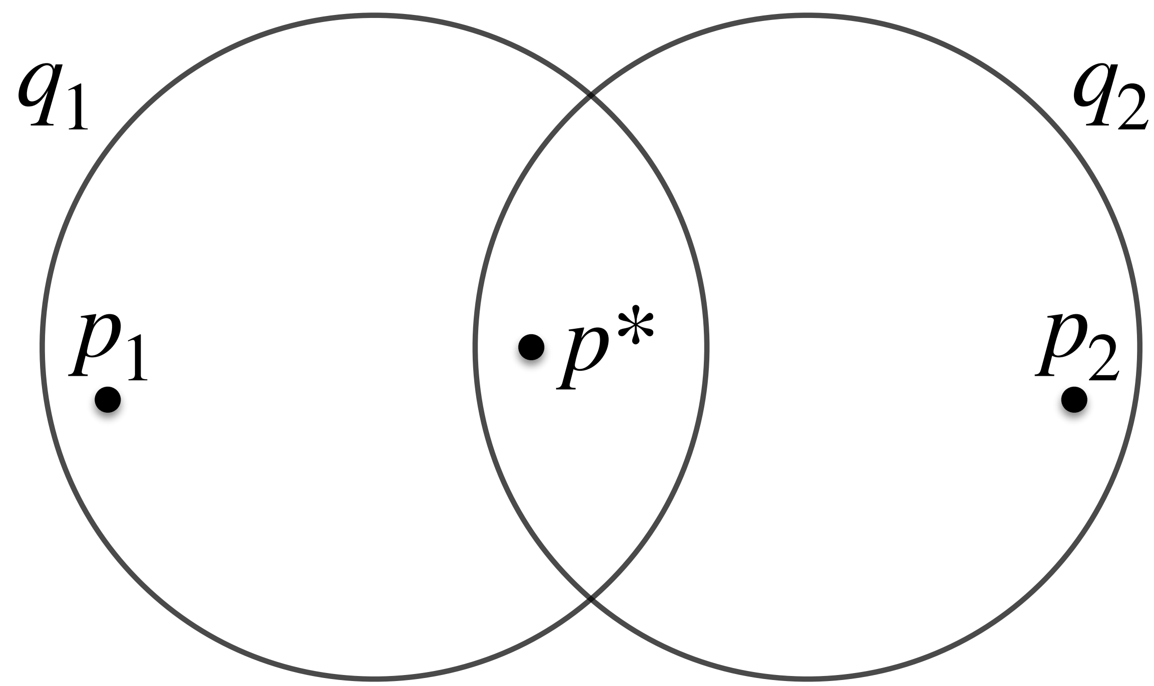
$(q_1 \cap q_2) \setminus \{p^*\}$ intersects $\mathcal{O}$

$\mathcal{Q}$ is available inside $\mathcal{O}$

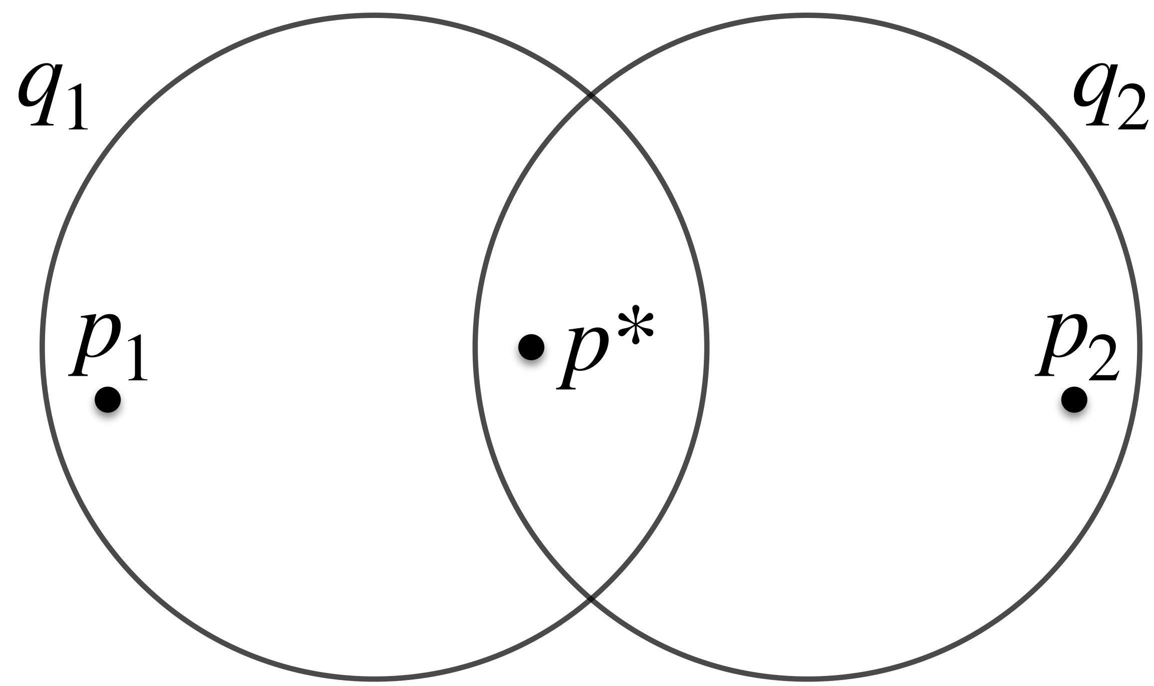
Leave Protocol



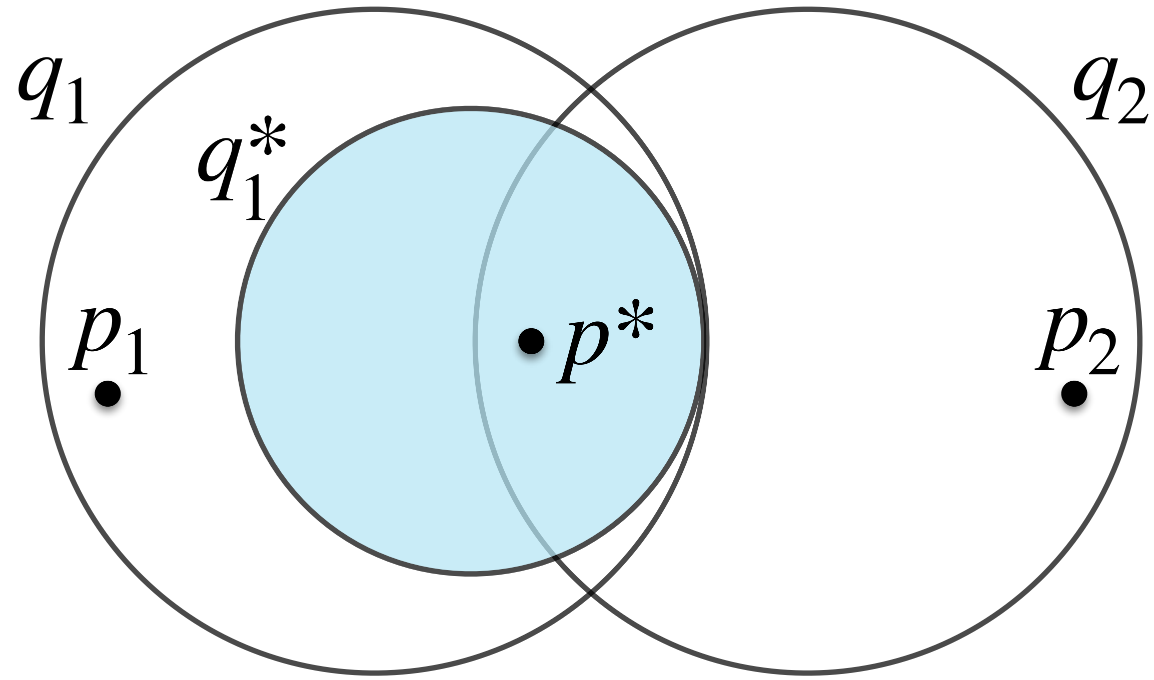
Leave Protocol



Leave Protocol

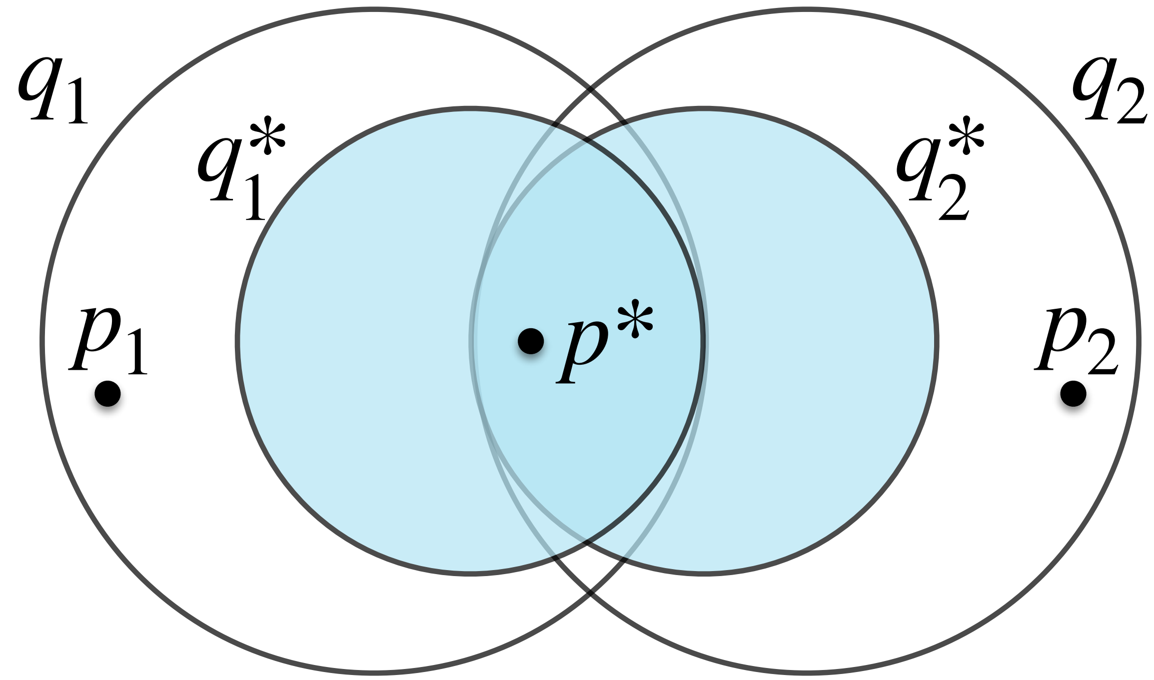


$\mathcal{Q}$ has quorum inclusion for $\mathcal{O}$



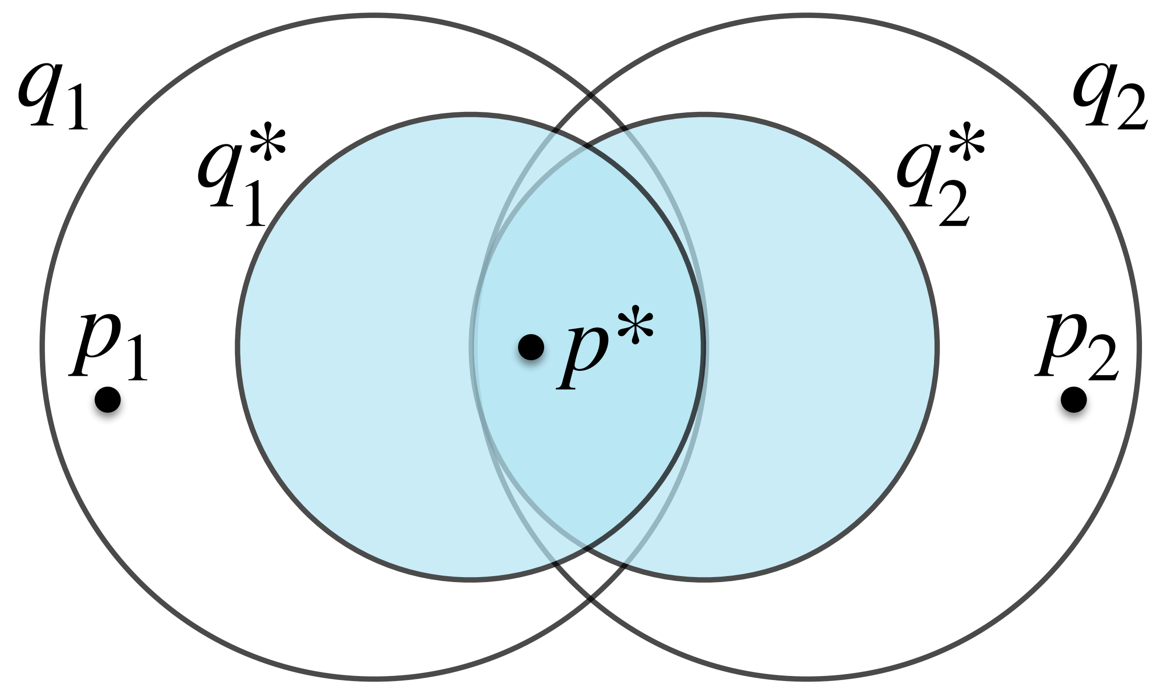
$\mathcal{Q}$ has quorum inclusion for $\mathcal{O}$

Leave Protocol

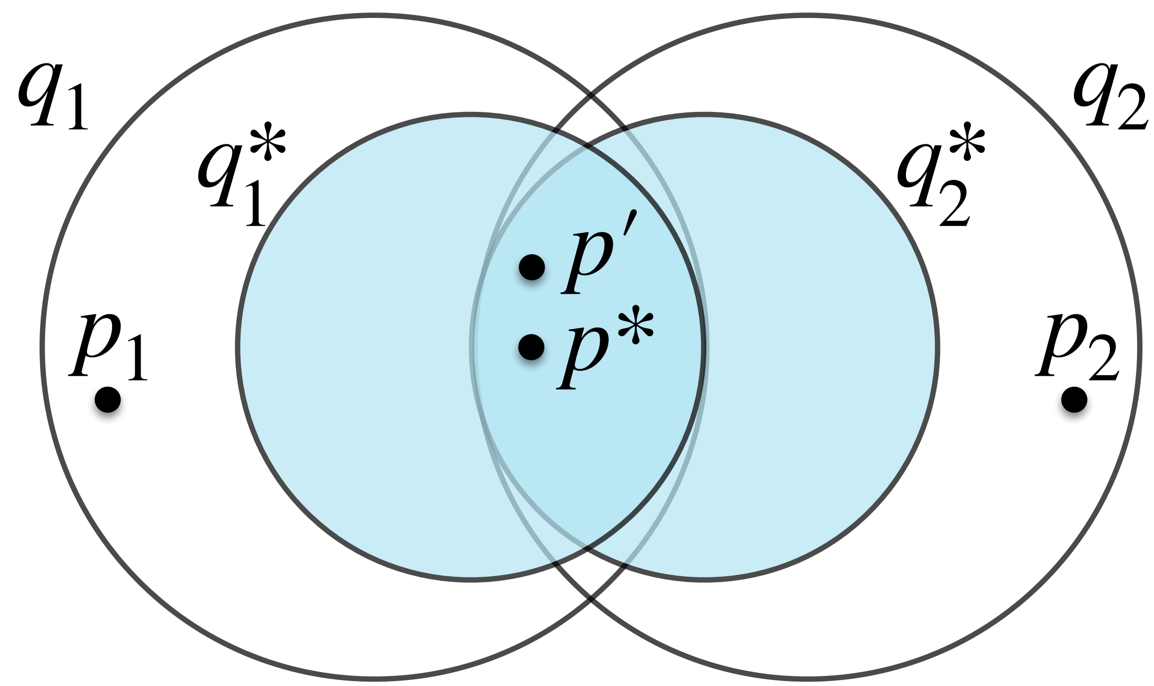


$\mathscr{Q}$ has quorum inclusion for $\mathscr{O}$

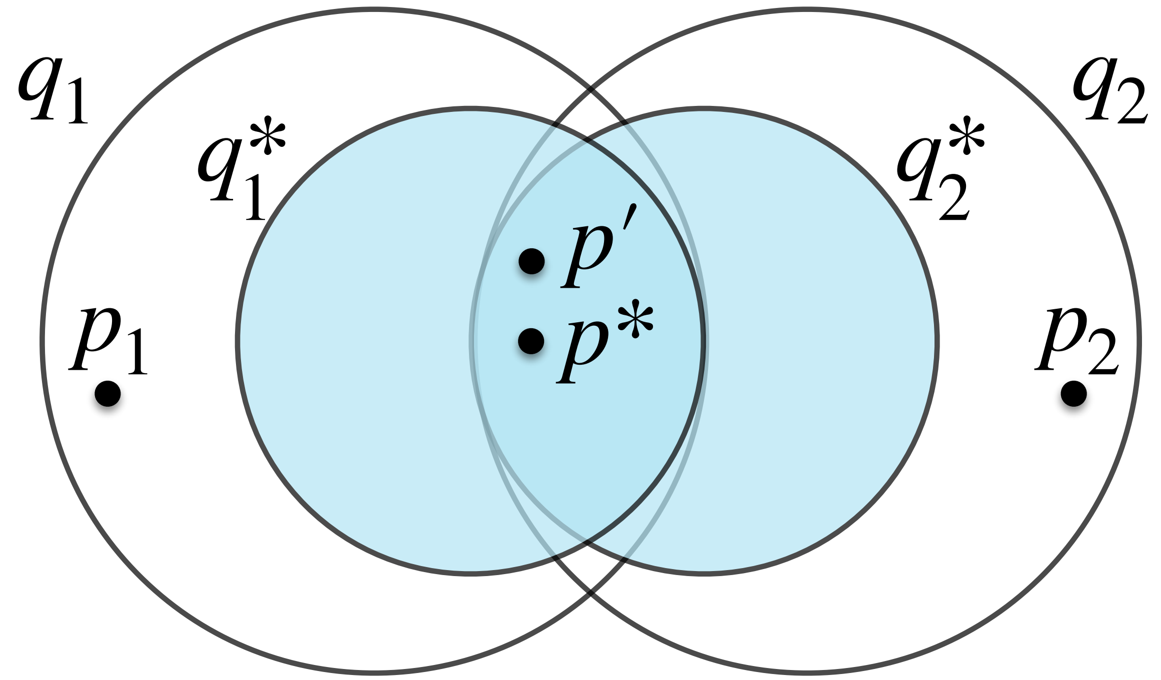
Leave Protocol



Leave Protocol

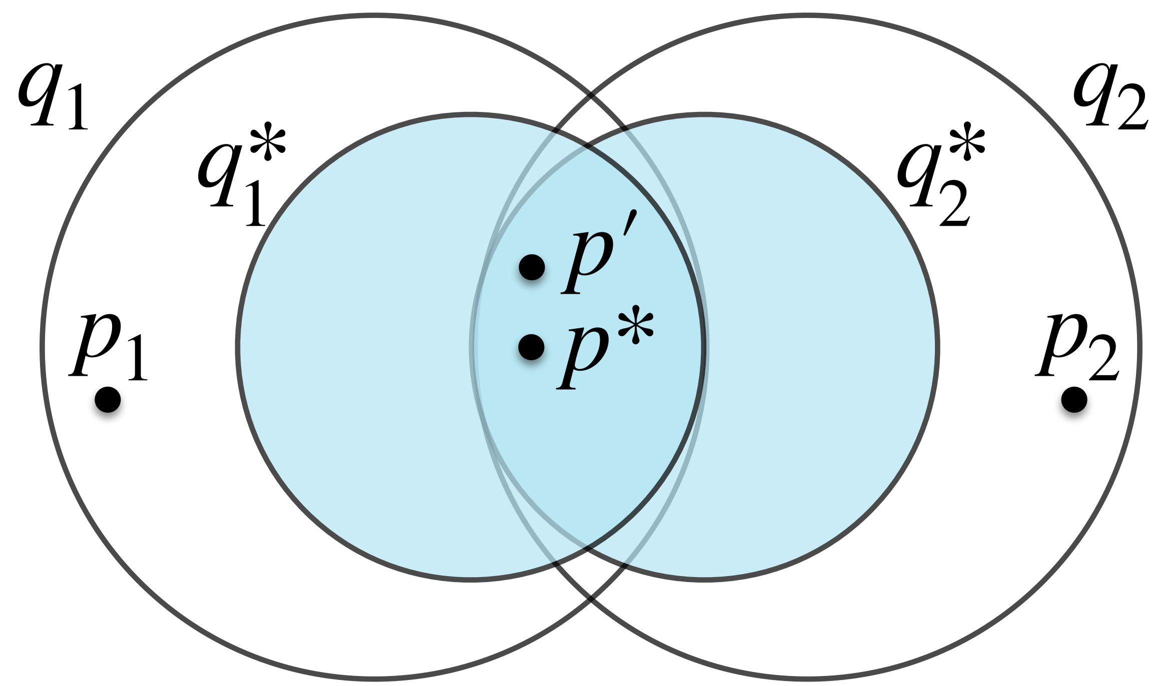


Leave Protocol



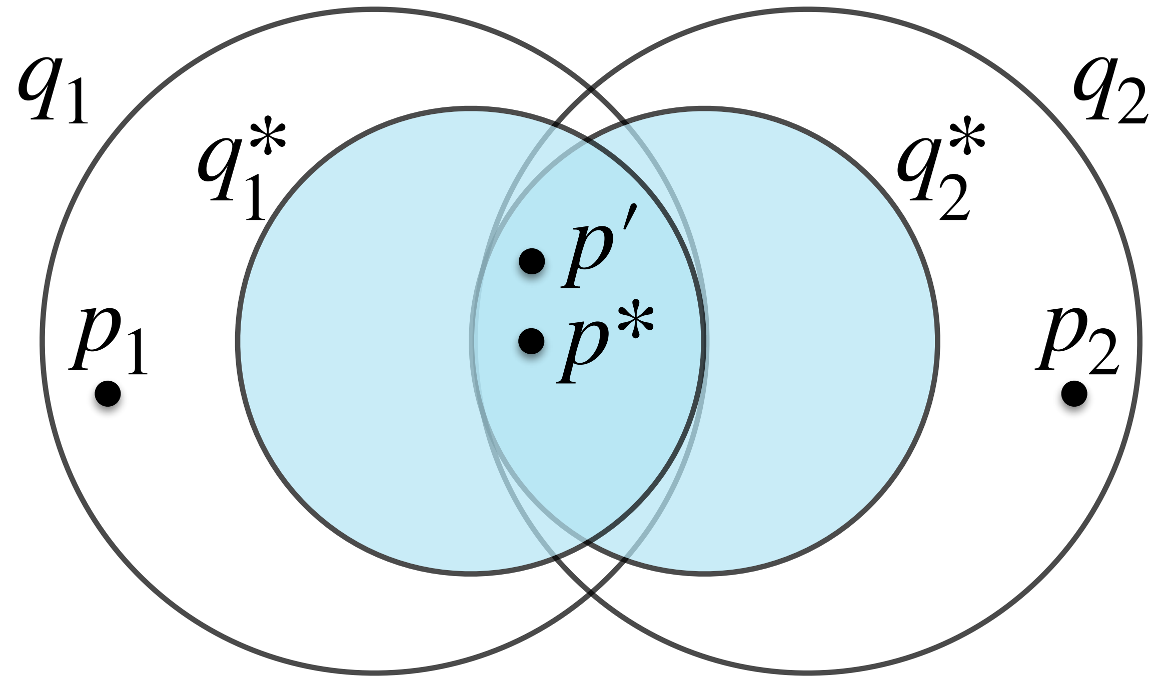
$p' \in tomb$

Leave Protocol



$p' \in tomb$

$\forall q_1, q_2 \in Q \,.\, (q_1 \cap q_2) \setminus (tomb \cup \{p^*\})$ is p^*-blocking

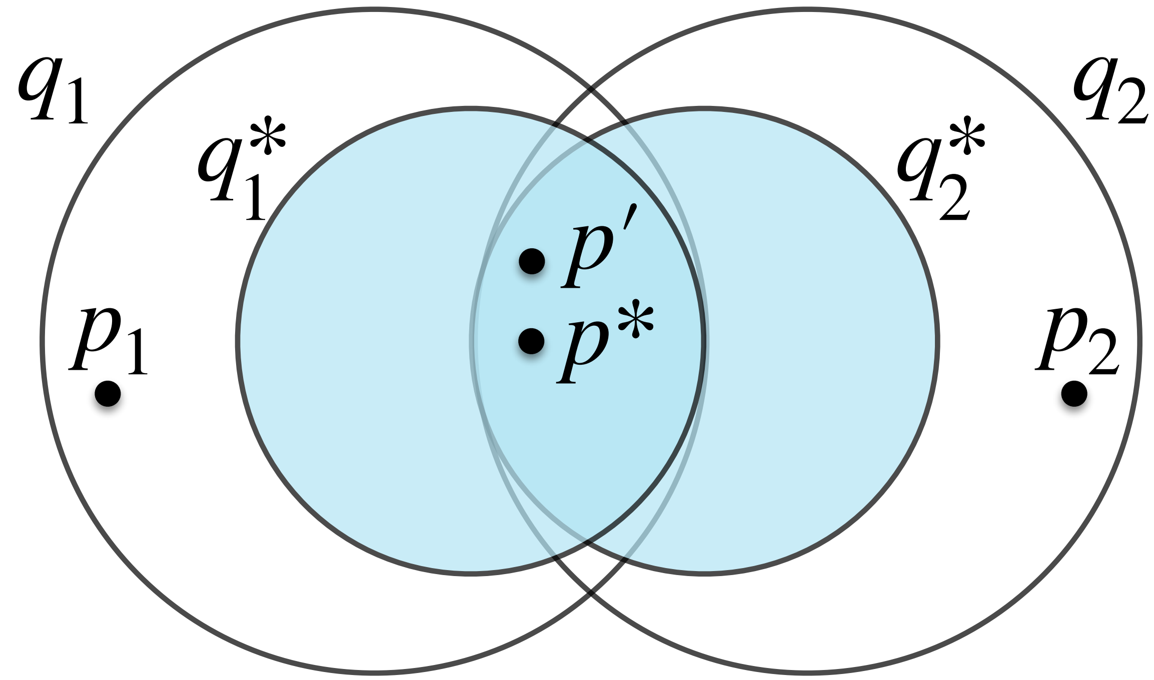


$p' \in \mathit{tomb}$

$\forall q_1, q_2 \in Q \,.\, (q_1 \cap q_2) \setminus (\mathit{tomb} \cup \{p^*\})$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p', p^*\}$ is p^*-blocking

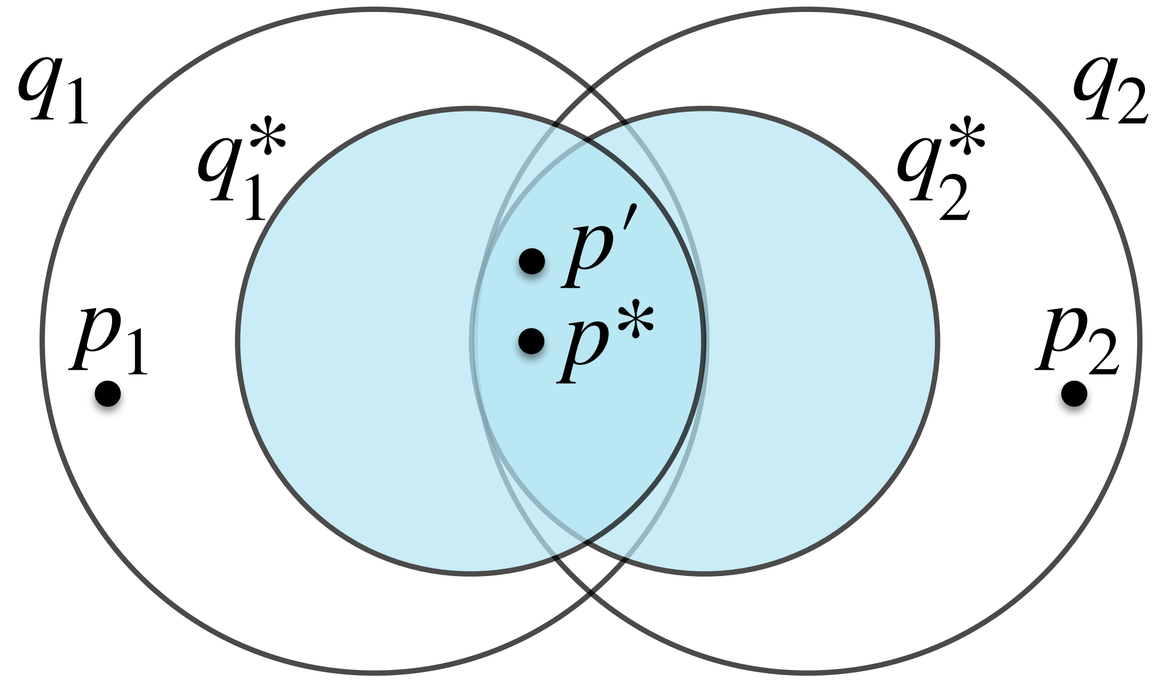
Leave Protocol



$p' \in tomb$

$\forall q_1, q_2 \in Q \,.\, (q_1 \cap q_2) \setminus (tomb \cup \{p^*\})$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p', p^*\}$ is p^*-blocking $\qquad$ $\mathcal{Q}$ is available inside $\mathcal{O}$



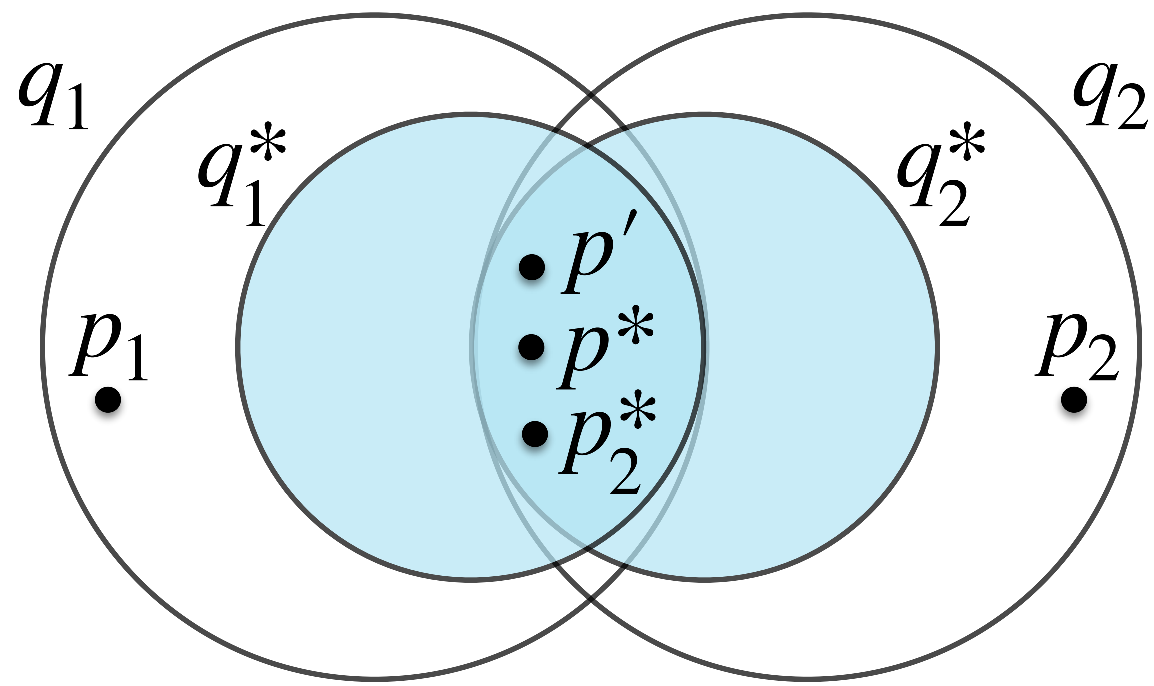
$p' \in tomb$

$\forall q_1, q_2 \in Q \,.\, (q_1 \cap q_2) \setminus (tomb \cup \{p^*\})$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p', p^*\}$ is p^*-blocking $\qquad \mathcal{Q}$ is available inside $\mathcal{O}$

$(q_1^* \cap q_2^*) \setminus \{p', p^*\}$ intersects $\mathcal{O}$

Leave Protocol

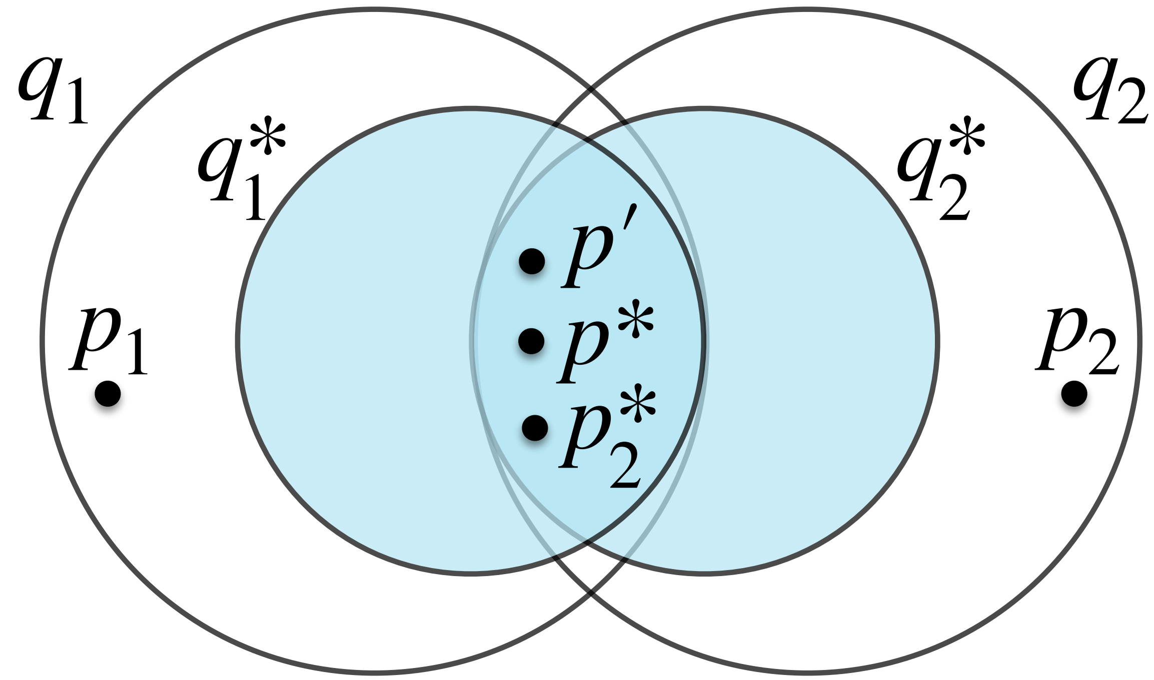


$p' \in tomb$

$\forall q_1, q_2 \in Q \,.\, (q_1 \cap q_2) \setminus (tomb \cup \{p*\})$ is $p*$-blocking

$(q_1^* \cap q_2^*) \setminus \{p', p*\}$ is $p*$-blocking $\qquad$ $\mathscr{Q}$ is available inside $\mathscr{O}$

$(q_1^* \cap q_2^*) \setminus \{p', p*\}$ intersects $\mathscr{O}$



$p' \in tomb$

$\forall q_1, q_2 \in Q\,.\,(q_1 \cap q_2) \setminus (tomb \cup \{p^*\})$ is p^*-blocking

$(q_1^* \cap q_2^*) \setminus \{p', p^*\}$ is p^*-blocking $\qquad \mathcal{Q}$ is available inside $\mathcal{O}$

$(q_1^* \cap q_2^*) \setminus \{p', p^*\}$ intersects $\mathcal{O}$

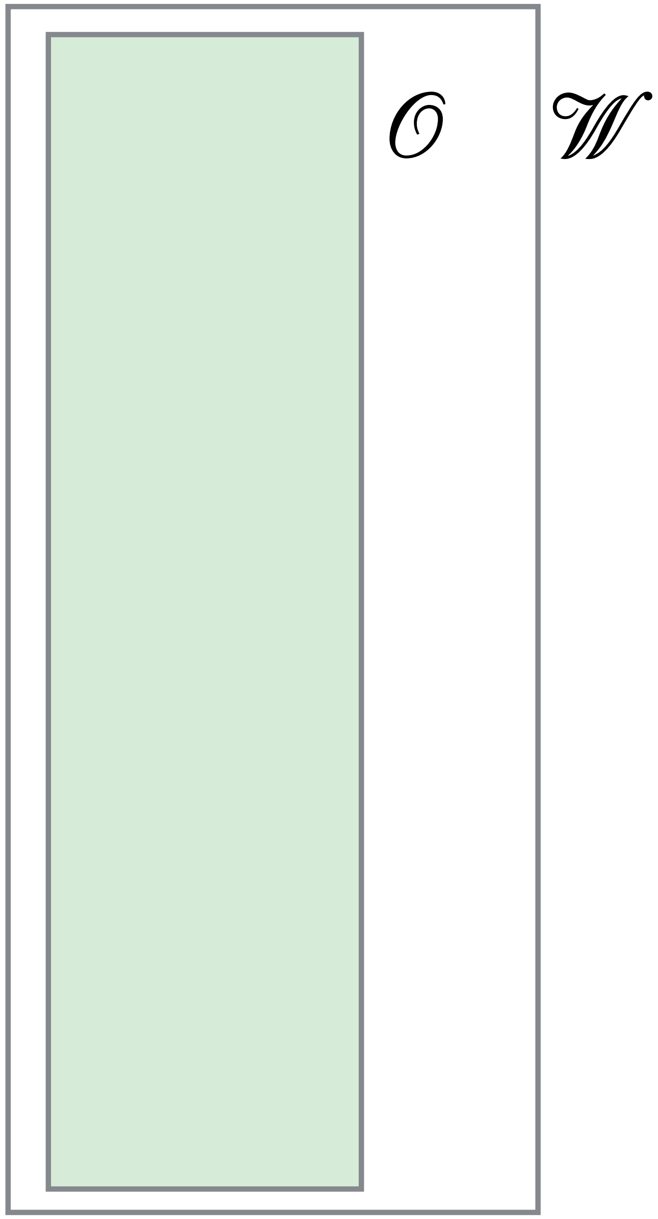
$(q_1 \cap q_2) \setminus \{p', p^*\}$ intersects $\mathcal{O}$

Reconfigurable Heterogeneous Quorum Systems

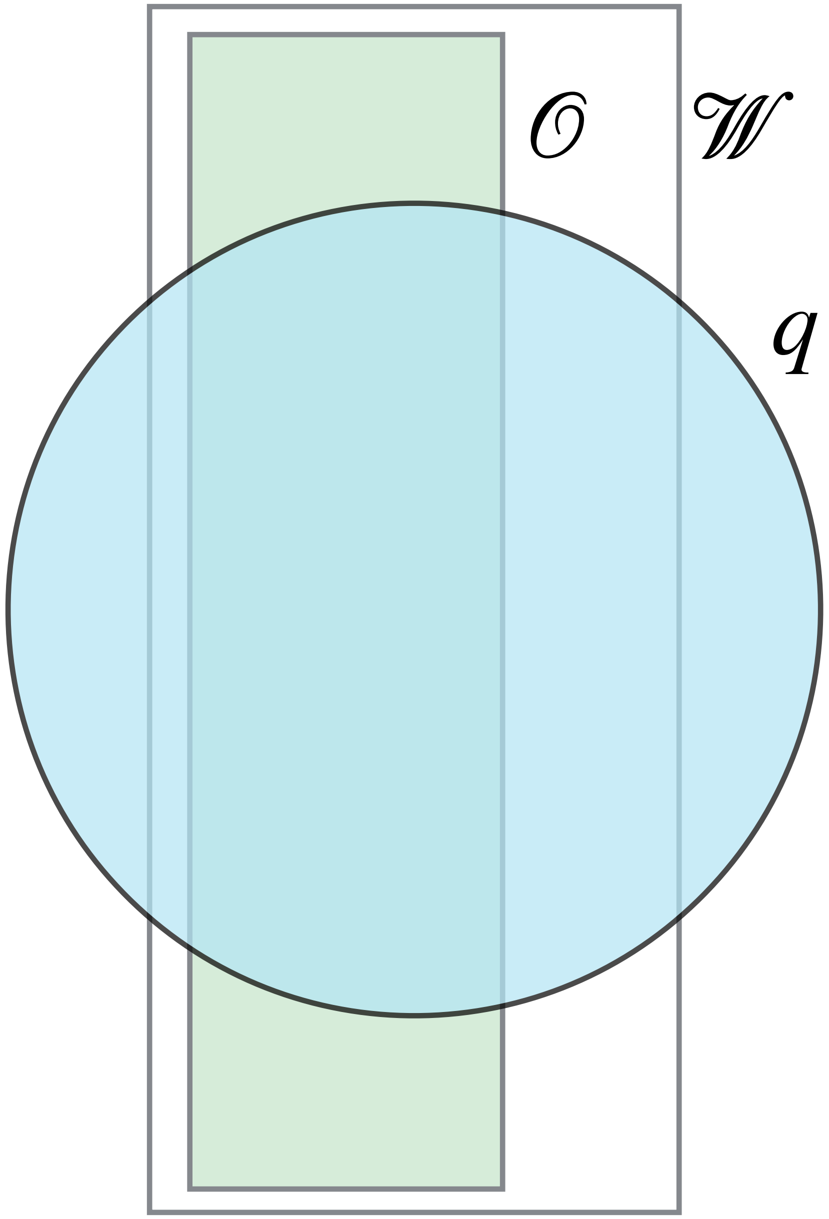
Xiao Li, Mohsen Lesani
University of California, Santa Cruz

Reconfigurability, the last missing property

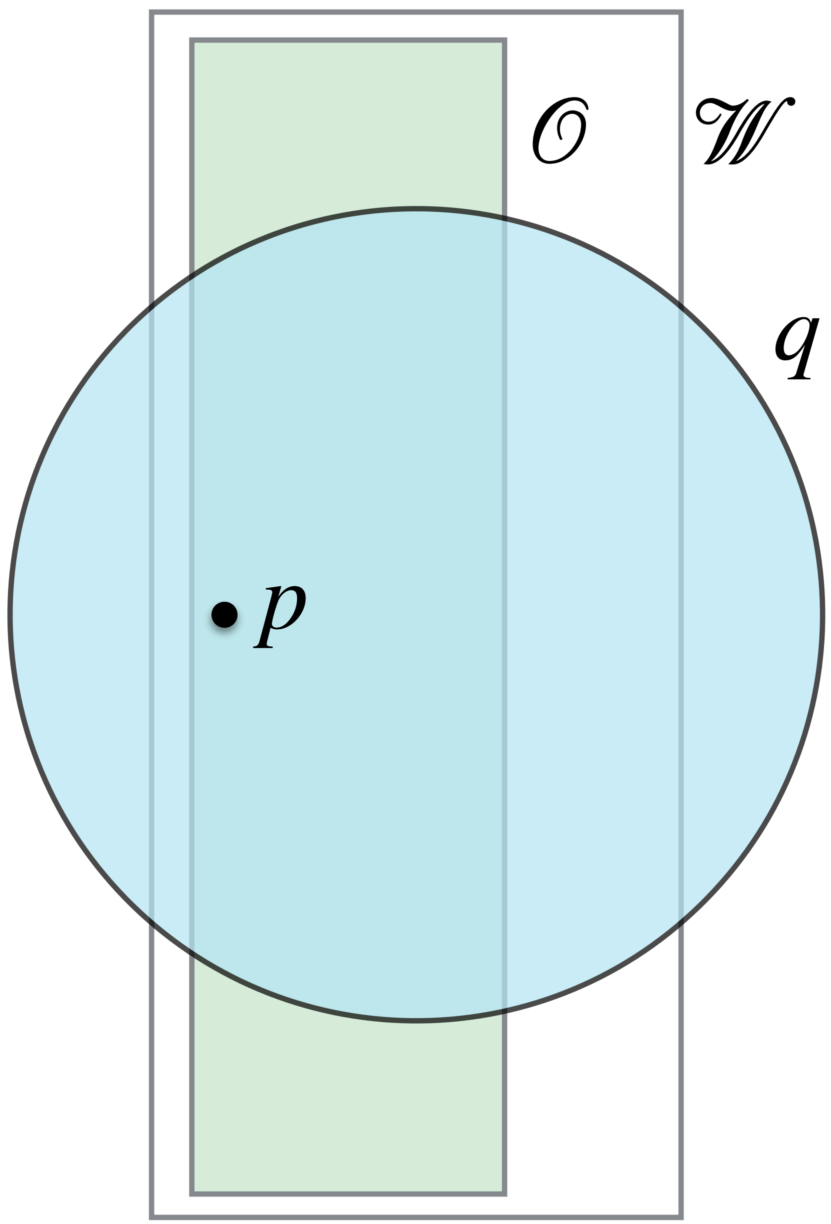
	Proof-of-work	Proof-of-stake	Byzantine Replication	HQS	Reconfigurable HQS
Heterogenous trust	✓	✓	✗	✓	✓
Reconfigurability (Openness)	✓	✓	✗	✗	✓
Energy efficiency	✗	✓	✓	✓	✓
Consistency	✓	✓	✓	✓	✓
Finality	✗	✗	✓	✓	✓
Equity	✓	✗	✓	✓	✓


$\mathscr{O}$
$\mathscr{W}$

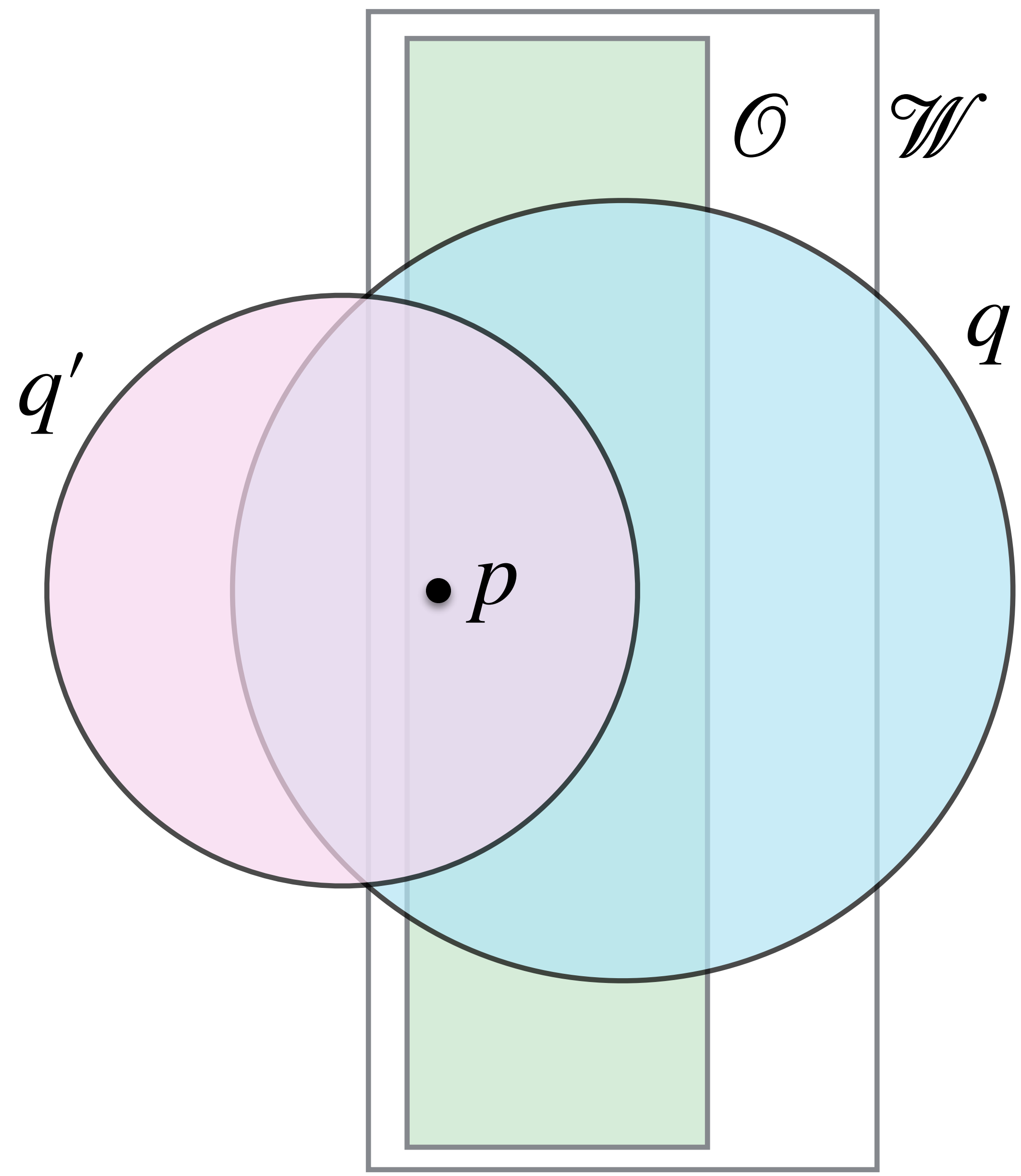
Quorum Inclusion for $\mathscr{O}$



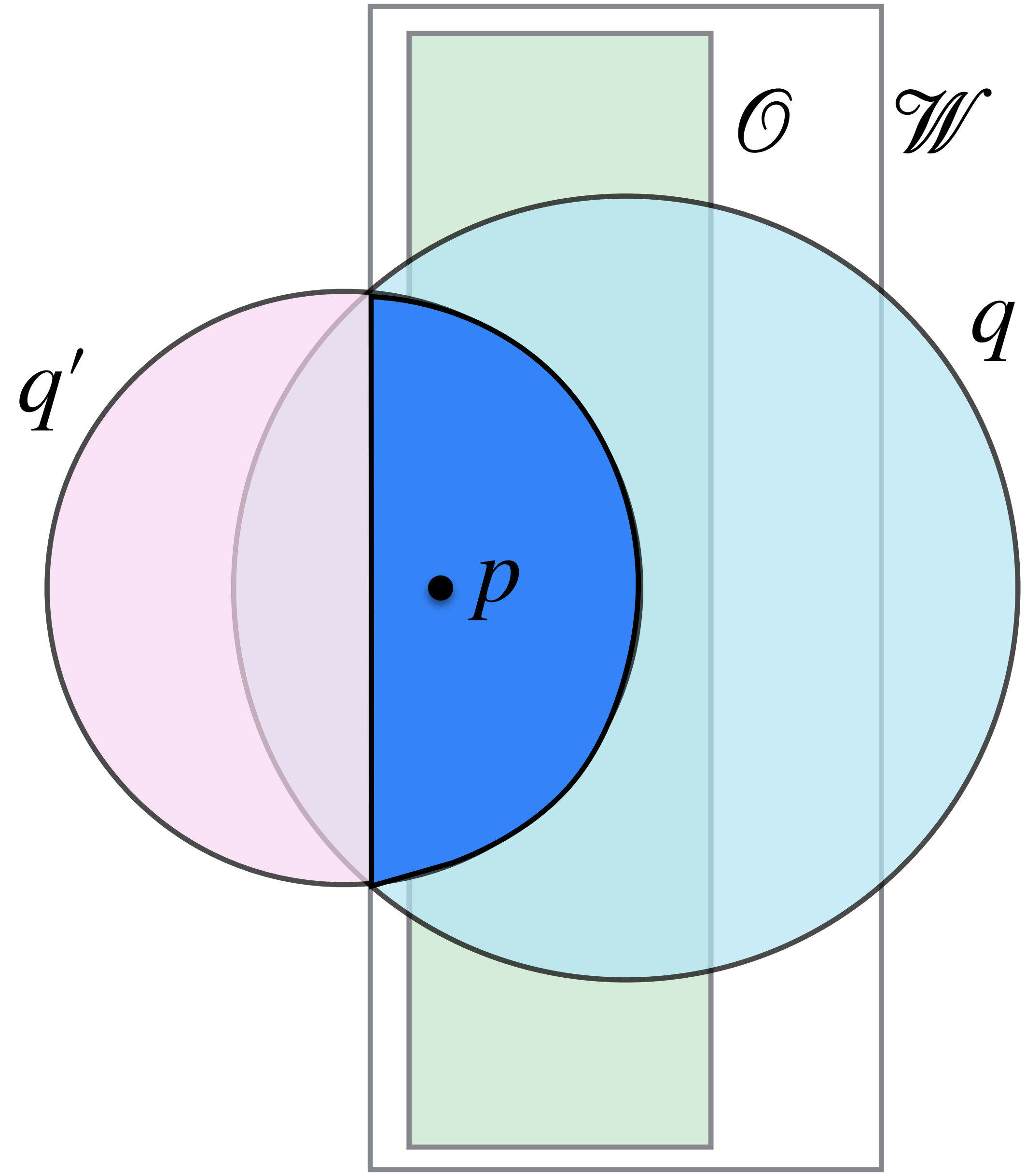
Quorum Inclusion for $\mathscr{O}$



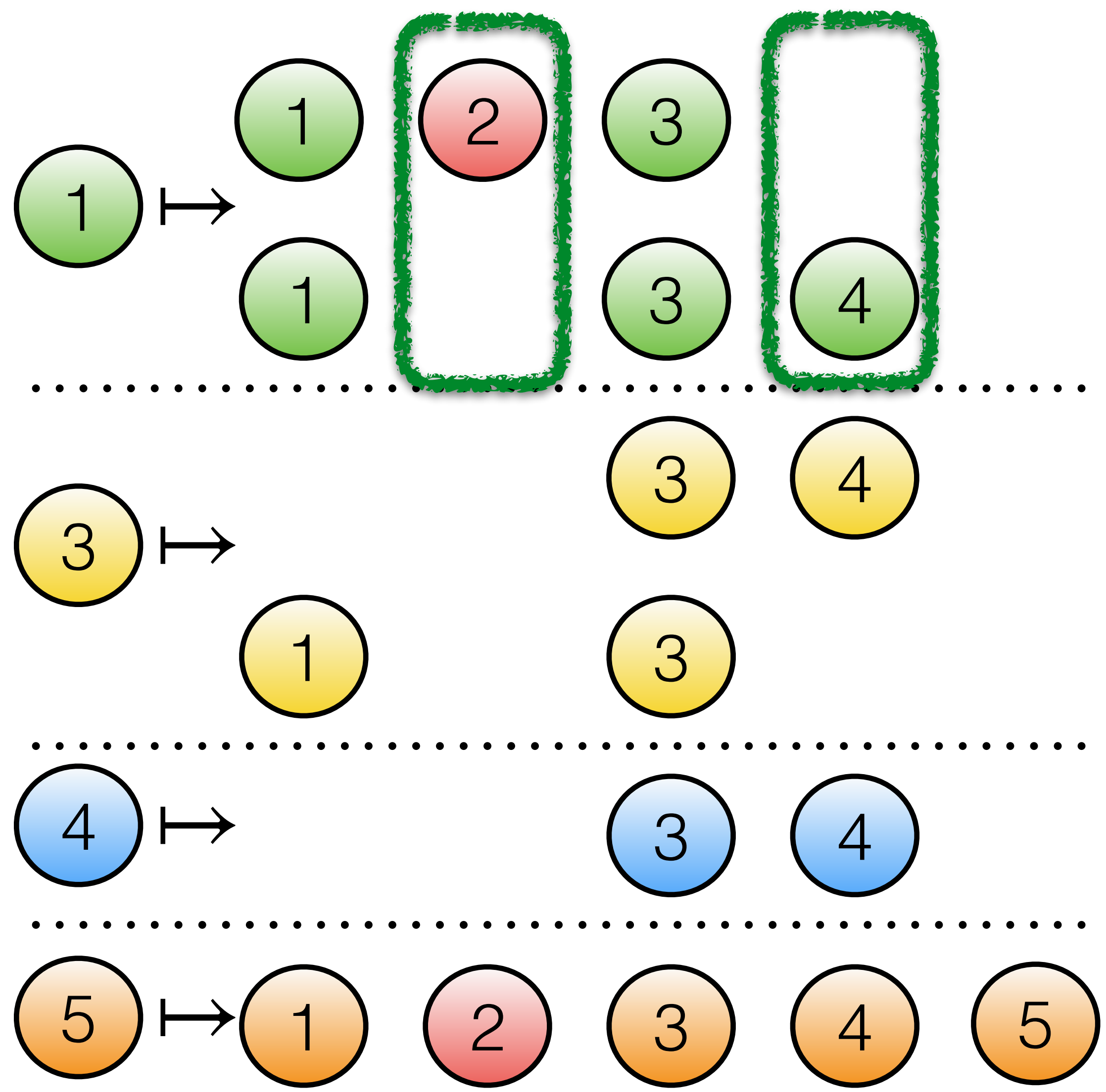
Quorum Inclusion for $\mathscr{O}$



Quorum Inclusion for $\mathscr{O}$



Blocking set

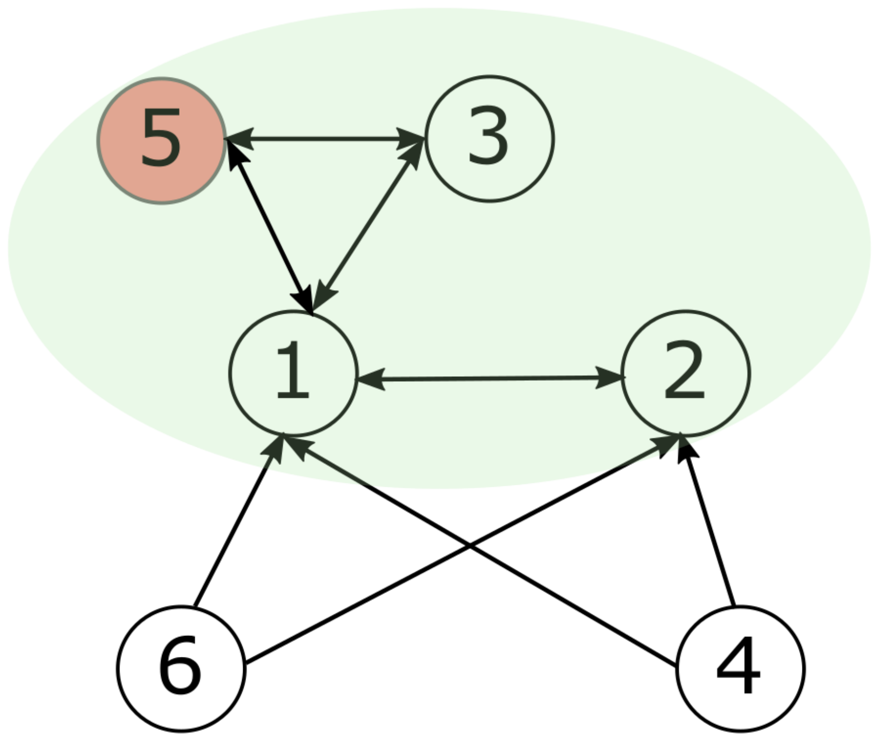


$$\mathscr{B} = \{2, 4\}$$

Quorum Graphs and the Sink Component

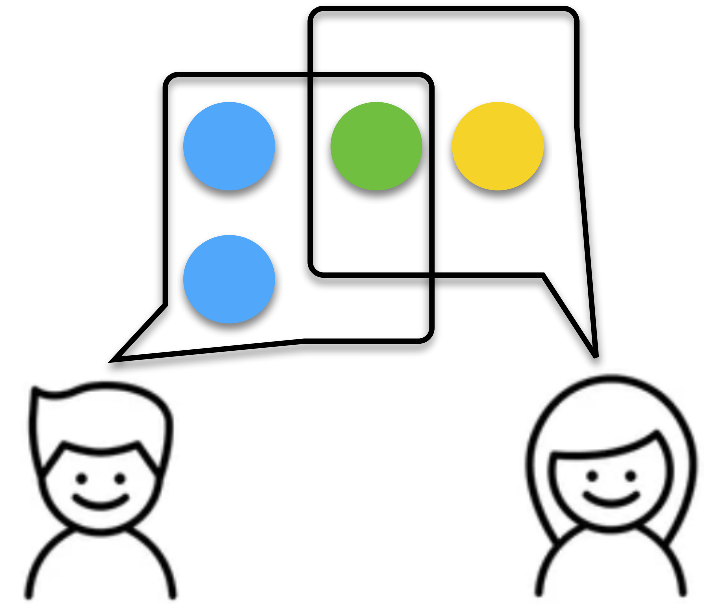
Theorem: In any quorum system with consistency and quorum sharing,
there is one sink component.
all well-behaved processes of the minimal quorums are in the sink component.

$$\mathcal{P} = \{1, 2, 3, 4, 5, 6\}, \mathcal{B} = \{5\},$$
$$\mathcal{Q}(1) = \{\{1, 2\}, \{1, 3, 5\}\},$$
$$\mathcal{Q}(2) = \{\{1, 2\}\},$$
$$\mathcal{Q}(3) = \{\{1, 3, 5\}\},$$
$$\mathcal{Q}(4) = \{\{1, 2, 4\}\},$$
$$\mathcal{Q}(5) = \{\{1, 3, 5\}\},$$
$$\mathcal{Q}(6) = \{\{1, 2, 6\}\}$$
$$MQ(\mathcal{Q}) = \{\{1, 2\}, \{1, 3, 5\}\}$$

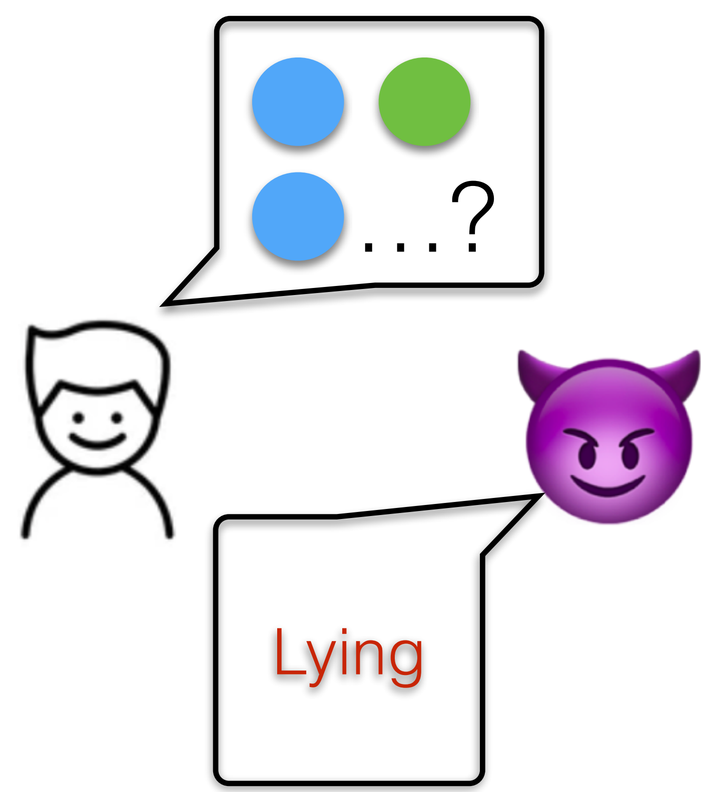


Motivation for Heterogeneous Quorum Systems

- **Uniform Trust**:
  All processes trust the same sets of quorums.
  No personal preference.



- **Public Trust**:
  All processes know the quorums that others trust.
  Not feasible in an open network.
  Byzantine nodes can lie about quorums.



Reconfiguration Trade-offs

Theorem: There is no Leave or Remove reconfiguration protocol that is policy-preserving, availability-preserving and terminating.

Reconfiguration Trade-offs

Theorem: There is no Leave or Remove reconfiguration protocol that is policy-preserving, availability-preserving and terminating.

The Leave protocol that we saw availability-preserving and terminating.

Reconfiguration Trade-offs

Theorem: There is no Leave or Remove reconfiguration protocol that is policy-preserving, availability-preserving and terminating.

The Leave protocol that we saw availability-preserving and terminating.

Theorem: There is no Add reconfiguration protocol that is consistency-preserving, policy-preserving, and terminating.