MANCHESTER 1824

The University of Manchester

Formal Methods Group

# Subset-Simulation as Model Minimality Criterion

Fabio Papacchini  Renate A. Schmidt

The University of Manchester

August 22, 2012

# (Minimal) Model Generation

(Minimal) Model generation is used in Computer Science for

- hardware verification
- software verification
- fault analysis
- ...

# (Minimal) Model Generation

(Minimal) Model generation is used in Computer Science for

- hardware verification
- software verification
- fault analysis
- ...

In [PapSch11] we presented a tableau calculus for the generation of minimal modal Herbrand models for multi-modal logic $\mathbf{K}$ and extensions with reflexivity and symmetry.

[PapSch11] F. Papacchini and R. A. Schmidt, A tableau calculus for minimal modal model generation, *ENTCS*, 278(3):159–172, 2011.

# Minimal Modal Herbrand Models

Semantics is defined as usual except for diamond formulae.

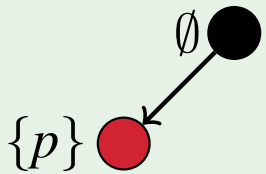
$\mathfrak{M}, u \models \Diamond\phi$ iff $(u, f_{\Diamond\phi}(u)) \in R$ and $\mathfrak{M}, f_{\Diamond\phi}(u) \models \phi$

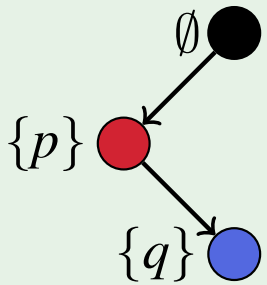
A modal Herbrand model can be represented as a set of true atoms and relations.

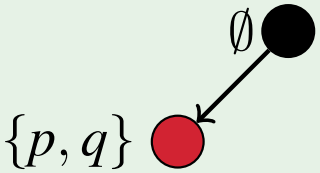
Minimality is defined by means of the subset relationship.

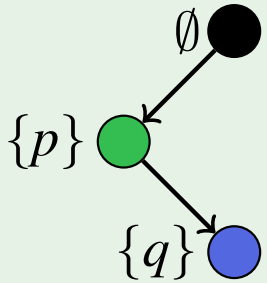
$H$ is minimal iff for any other $H'$ s.t. $H' \subseteq H$, then $H = H'$.

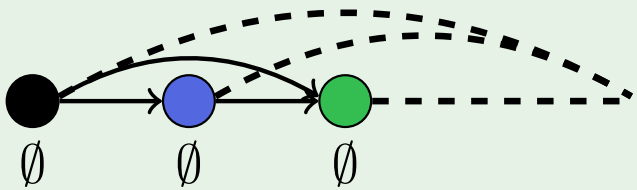
# Minimal Modal Herbrand Models Example



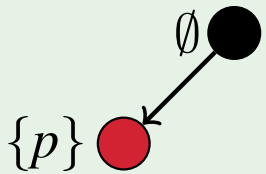



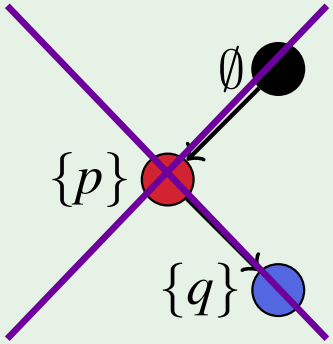



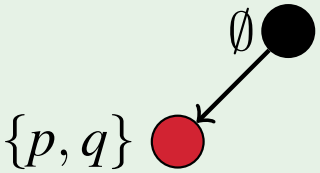



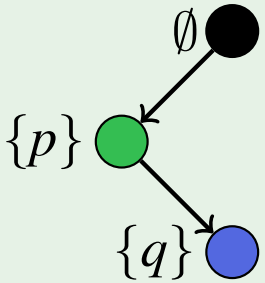



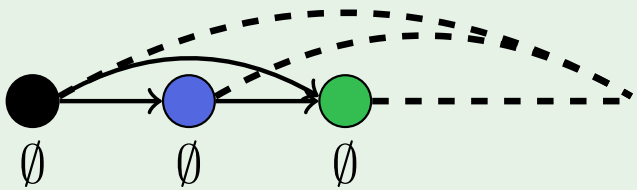
# Minimal Modal Herbrand Models Example



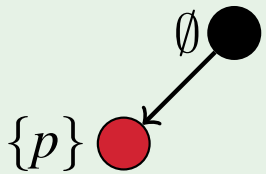



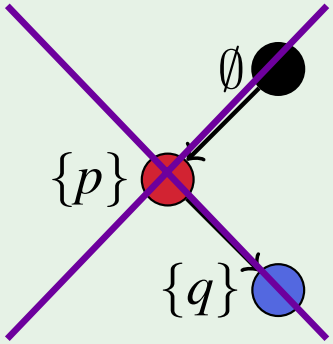



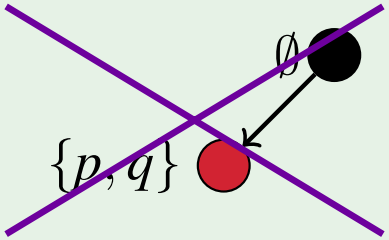



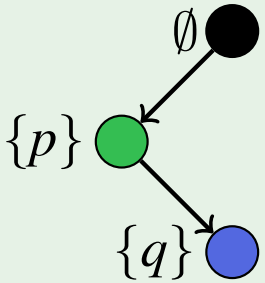



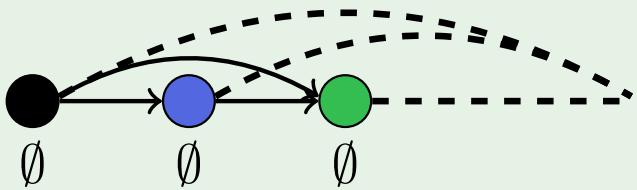
# Minimal Modal Herbrand Models Example



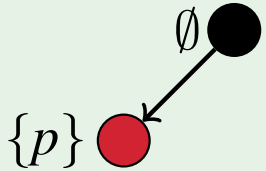



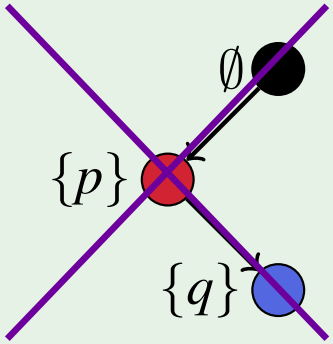



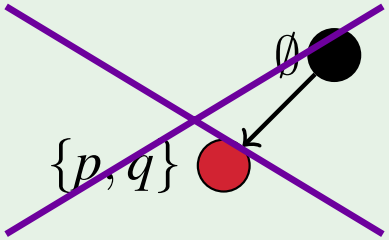



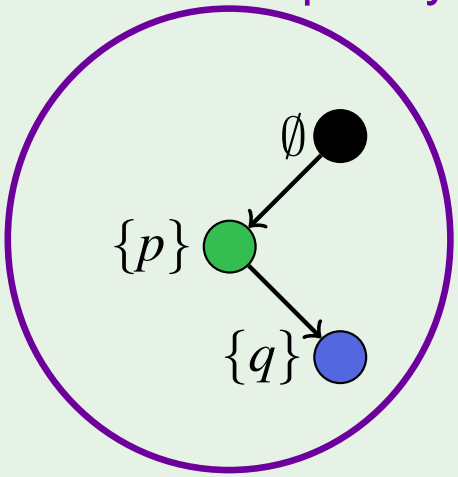
# Minimal Modal Herbrand Models Example

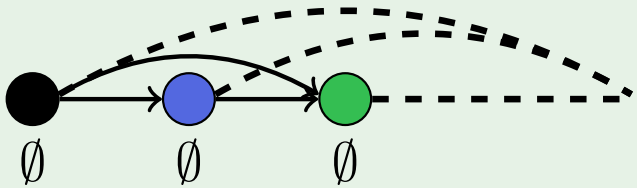


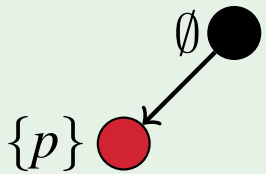

Minimal because the criterion is purely syntactic!

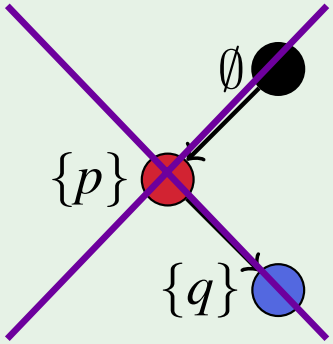


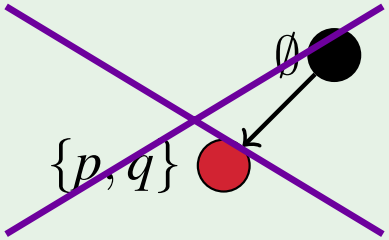



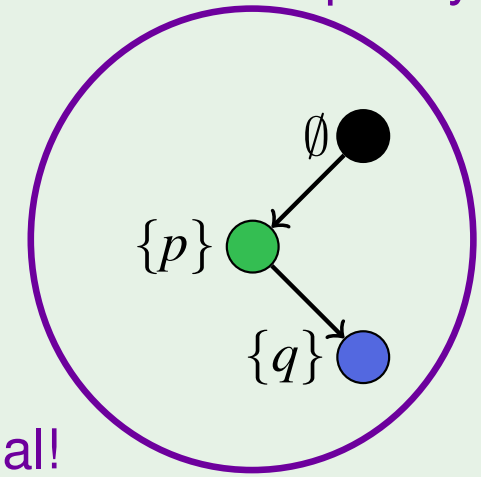
# Minimal Modal Herbrand Models Example



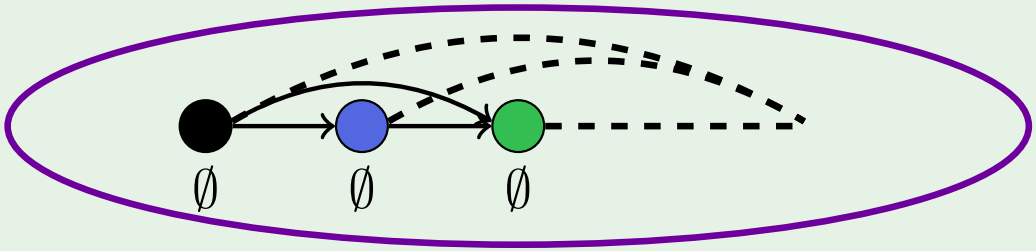




Minimal because the criterion is purely syntactic!




Infinite and minimal!



# Minimal Modal Herbrand Models Limitations

Two main limitations:

- it is a syntactic criterion
  - some minimal model might be semantically redundant
  - some minimal model might be semantically non-minimal
- minimal modal Herbrand models might be infinite, even for logics with the finite model property

# Minimal Modal Herbrand Models Limitations

Two main limitations:

- it is a syntactic criterion
  - some minimal model might be semantically redundant
  - some minimal model might be semantically non-minimal
- minimal modal Herbrand models might be infinite, even for logics with the finite model property

## Our Solution

Use a different method for model generation and a new minimality criterion based on semantics: *Minimality Modulo Subset-Simulation*

# Subset-Simulation

Let $\mathfrak{M} = (W, R, V)$ and $\mathfrak{M}' = (W', R', V')$ be two models of a modal formula $\phi$. A *subset-simulation* is a total binary relation $S_{\subseteq} \subseteq W \times W'$ such that for any two worlds $u \in W$ and $u' \in W'$, $uS_{\subseteq}u'$ if the following hold.

- $V(u) \subseteq V'(u')$ $[V(u) = \{p \in \Sigma \mid \mathfrak{M}, u \models p\}]$ and
- if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$.

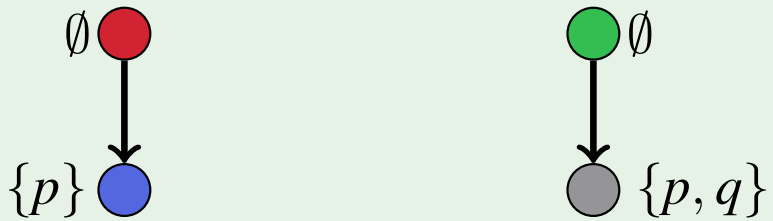
If such a subset-simulation exists we say that $\mathfrak{M}$ *subset-simulates* $\mathfrak{M}'$.

The idea of subset-simulation is to establish if a model is completely embedded in another.

# Subset-Simulation: First Property

$$V(u) \subseteq V'(u')$$

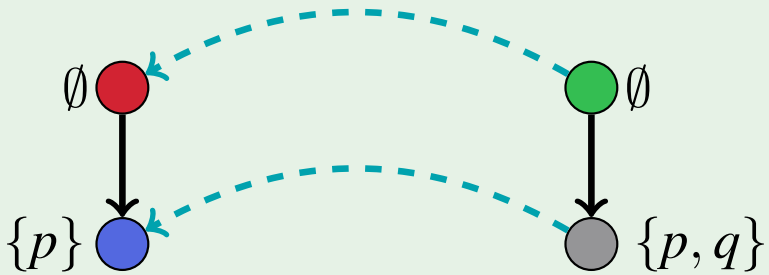
- unlike minimal modal Herbrand models, $u$ can be different from $u'$
- like minimal modal Herbrand models, the contents are compared by means of a subset relationship



# Subset-Simulation: First Property

$$V(u) \subseteq V'(u')$$

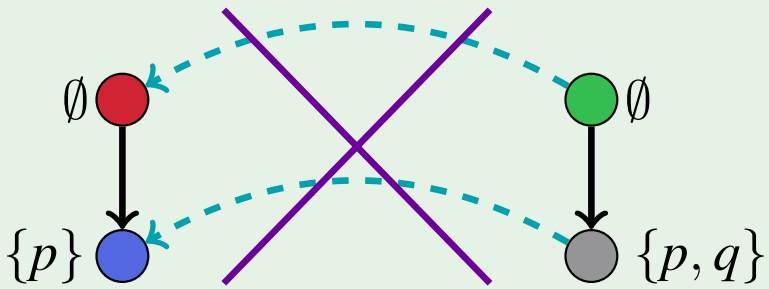
- unlike minimal modal Herbrand models, $u$ can be different from $u'$
- like minimal modal Herbrand models, the contents are compared by means of a subset relationship



# Subset-Simulation: First Property

$$V(u) \subseteq V'(u')$$

- unlike minimal modal Herbrand models, $u$ can be different from $u'$
- like minimal modal Herbrand models, the contents are compared by means of a subset relationship

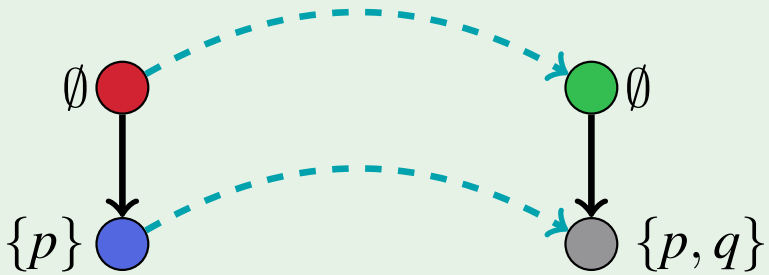



$$\{p, q\} \not\subseteq \{p\}$$

# Subset-Simulation: First Property

$$V(u) \subseteq V'(u')$$

- unlike minimal modal Herbrand models, $u$ can be different from $u'$
- like minimal modal Herbrand models, the contents are compared by means of a subset relationship



# Subset-Simulation: First Property

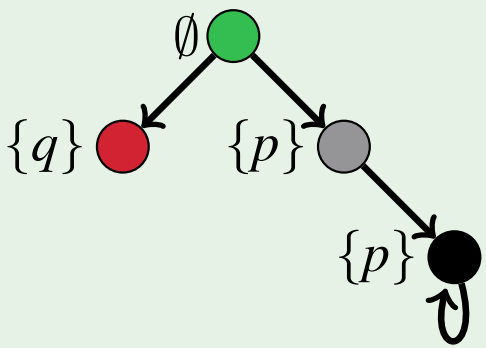
$$V(u) \subseteq V'(u')$$

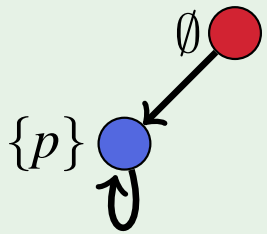
- unlike minimal modal Herbrand models, $u$ can be different from $u'$
- like minimal modal Herbrand models, the contents are compared by means of a subset relationship

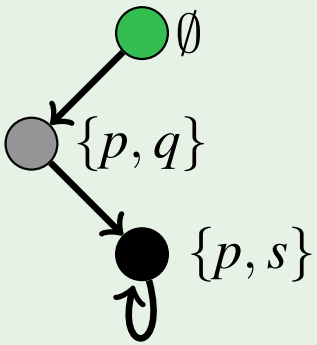
# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models



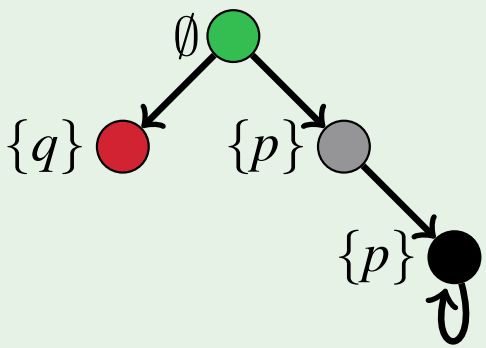



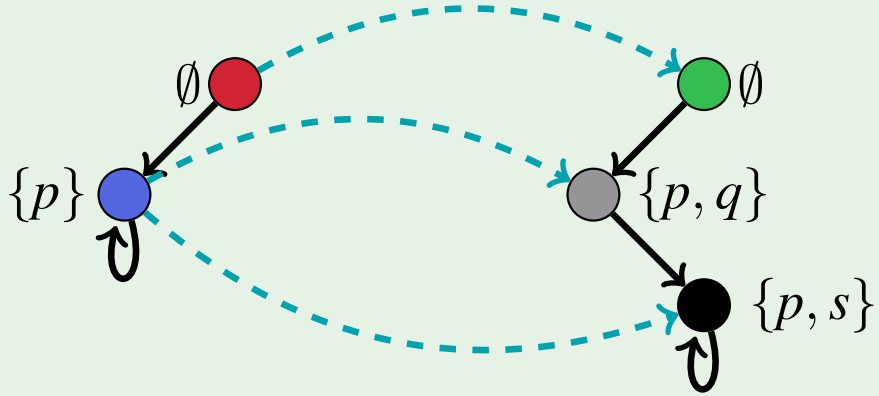



# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models

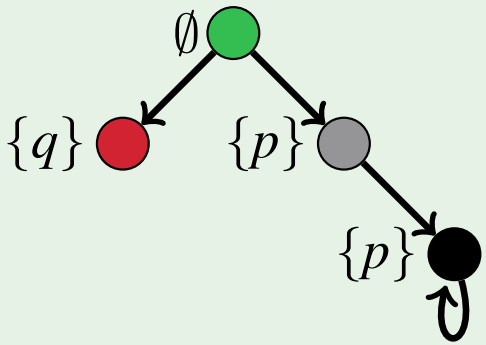


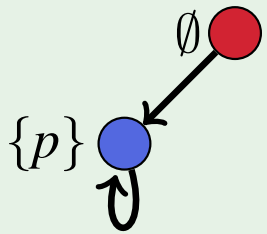



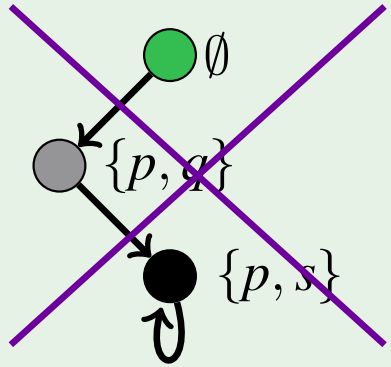
# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models



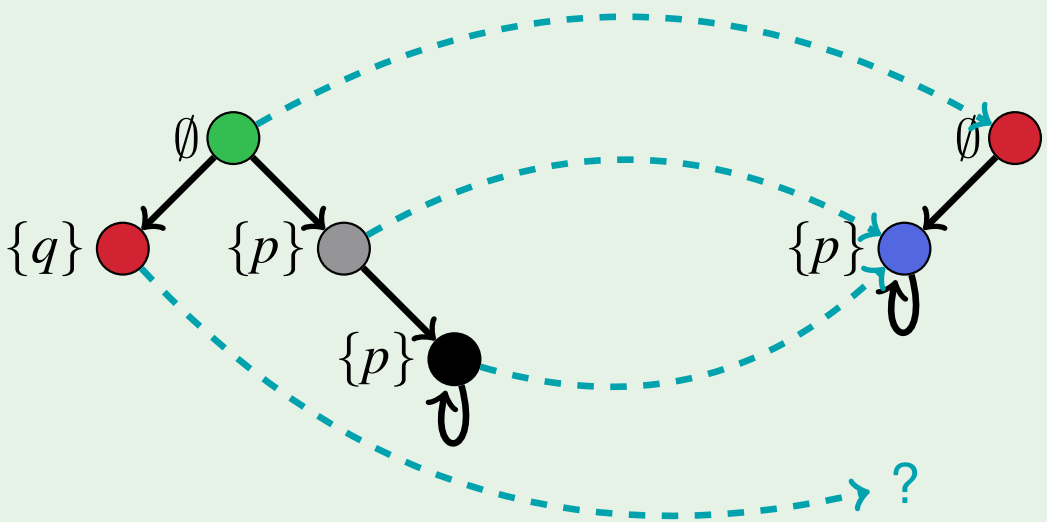



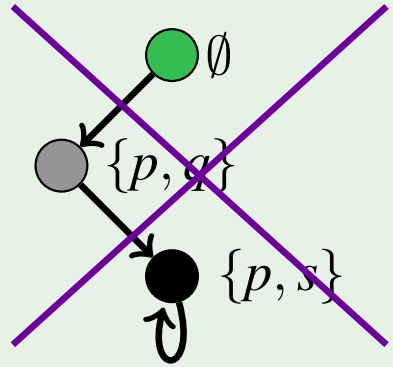



# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models

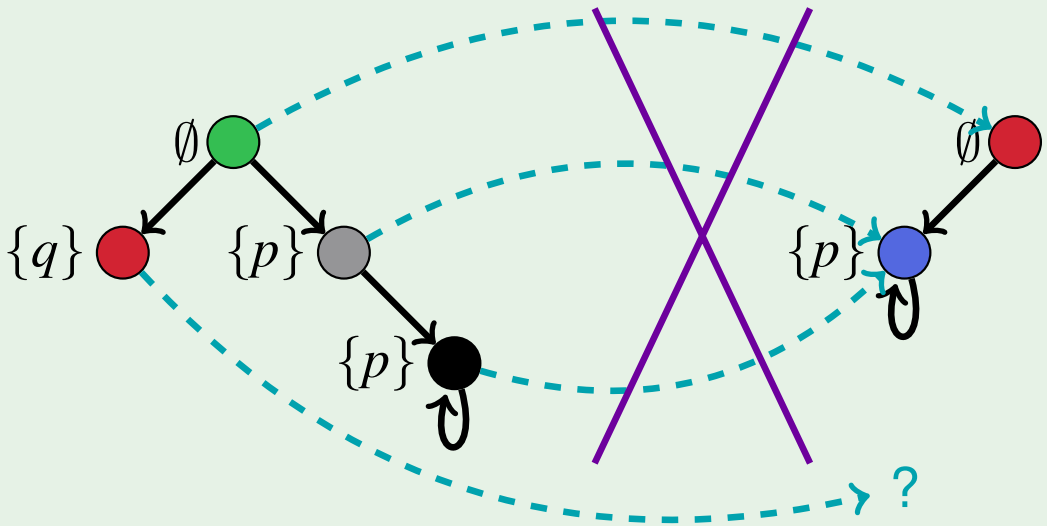


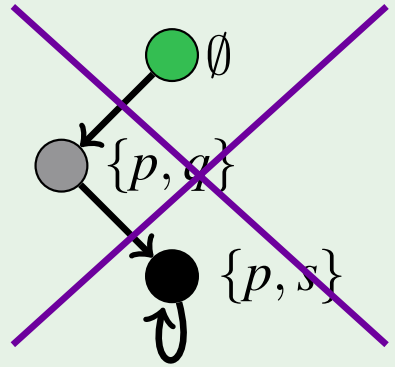



# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models

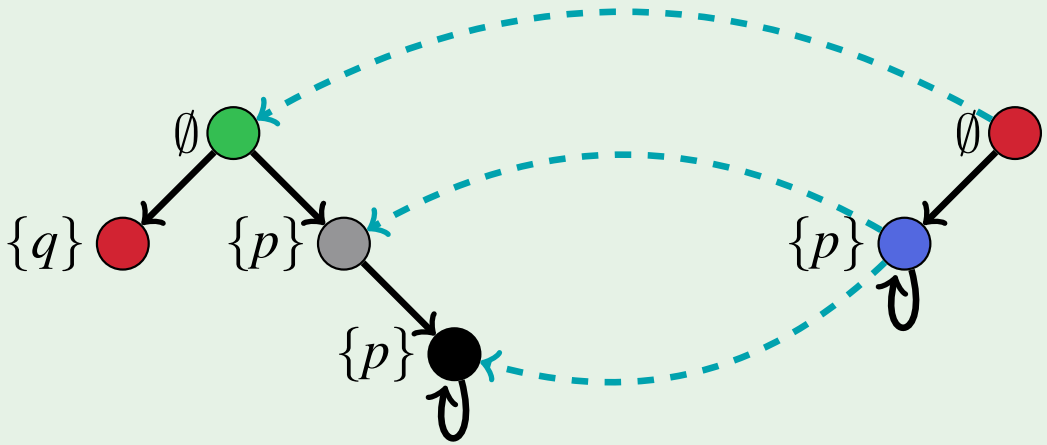


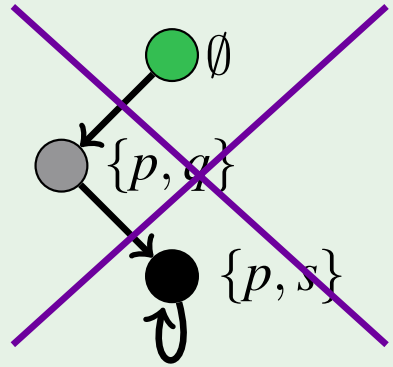



# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models

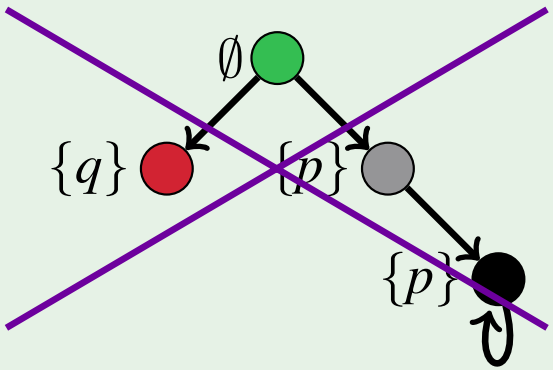


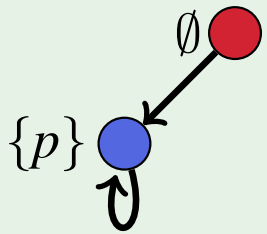



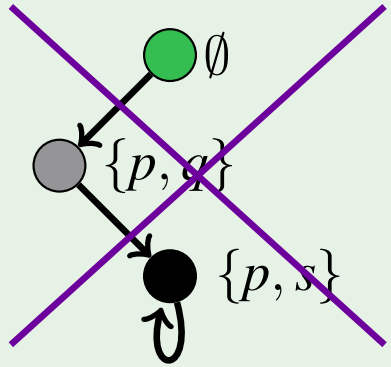
# Subset-Simulation: Second Property

if $uRv$ then there exists a $v' \in W'$ such that $vS_{\subseteq}v'$ and $u'R'v'$

- same as the bisimulation “zig” condition
- does not give us the possibility to minimise relations
- gives us the necessary flexibility to check complex submodel relations
- logics with the finite model property have finite minimal models



# Subset-Simulation as Model Minimality Criterion

Subset-simulation is a preorder relation over models

- Reflexivity: when $S_{\subseteq} \subseteq W \times W$ and $S_{\subseteq} = \{(u,u) \mid \text{for all } u \in W\}$
- Transitivity:
  - if a model subset-simulates another, then the first model is embedded in the second
  - if the second model is embedded in a third model, so is the first

# Subset-Simulation as Model Minimality Criterion

Subset-simulation is a preorder relation over models

- Reflexivity: when $S_{\subseteq} \subseteq W \times W$ and $S_{\subseteq} = \{(u, u) \mid \text{for all } u \in W\}$
- Transitivity:
  - if a model subset-simulates another, then the first model is embedded in the second
  - if the second model is embedded in a third model, so is the first

## Minimality Modulo Subset-Simulation

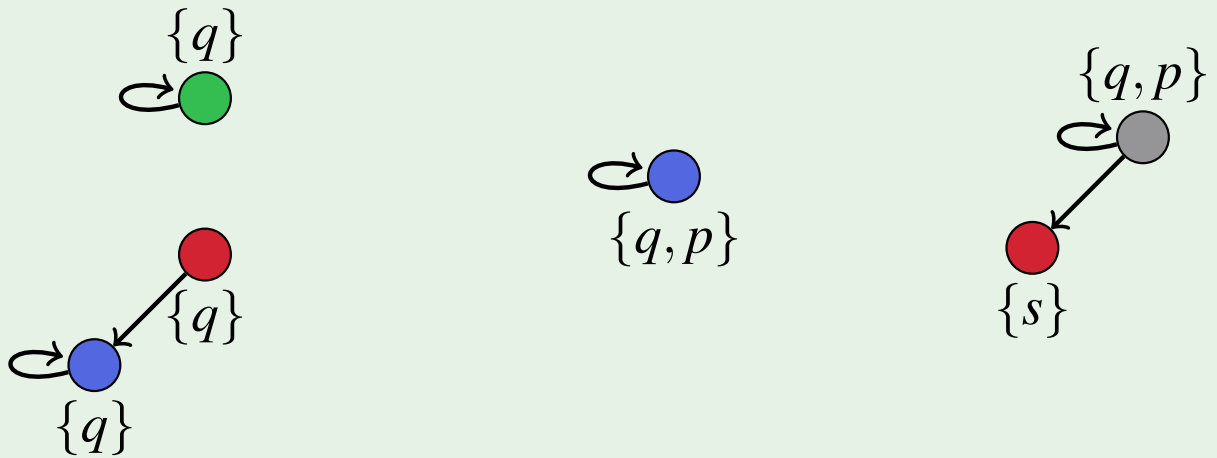
Given a modal formula $\phi$ and a model $\mathfrak{M}$, $\mathfrak{M}$ is a *minimal model modulo subset-simulation* of $\phi$ iff for any other model $\mathfrak{M}'$ of $\phi$, if $\mathfrak{M}'$ subset-simulates $\mathfrak{M}$, then $\mathfrak{M}$ subset-simulates $\mathfrak{M}'$.

# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

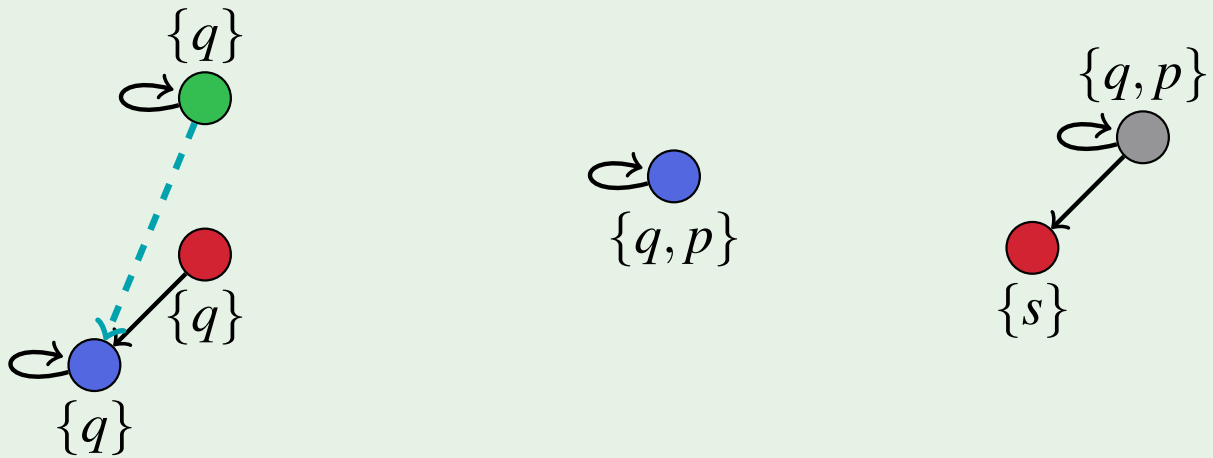


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

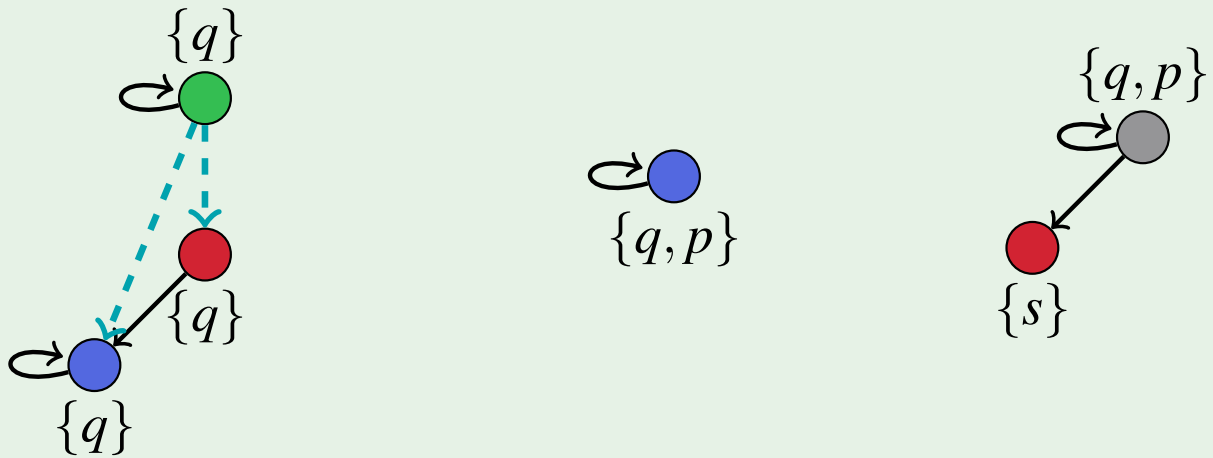


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

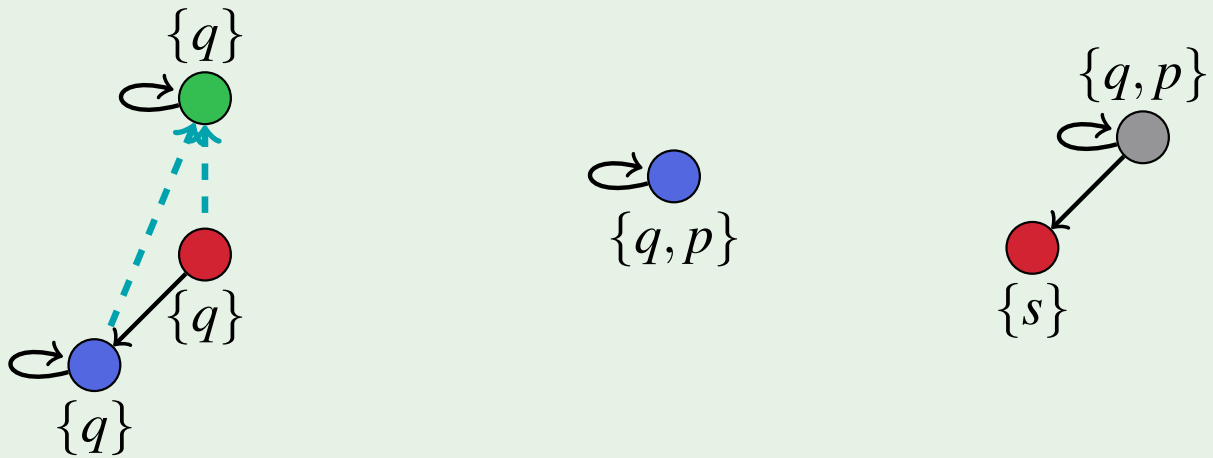


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

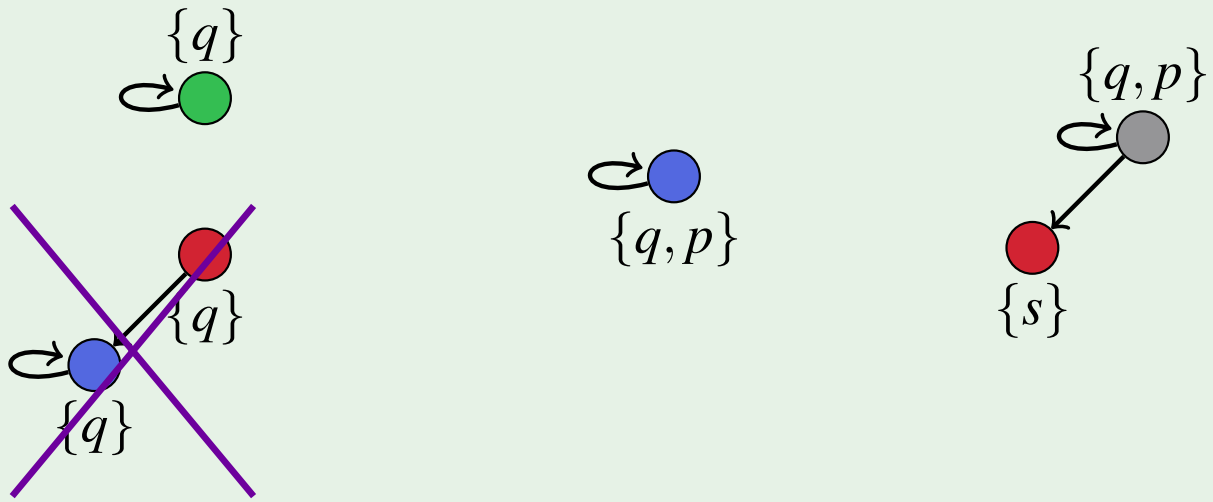


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

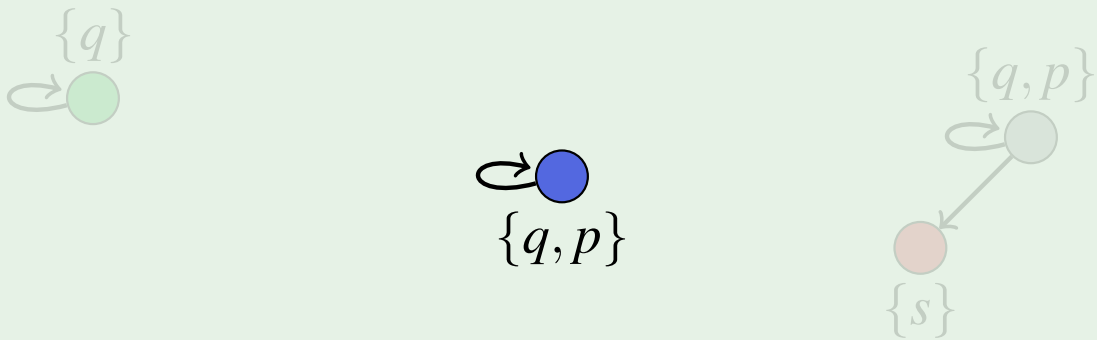


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

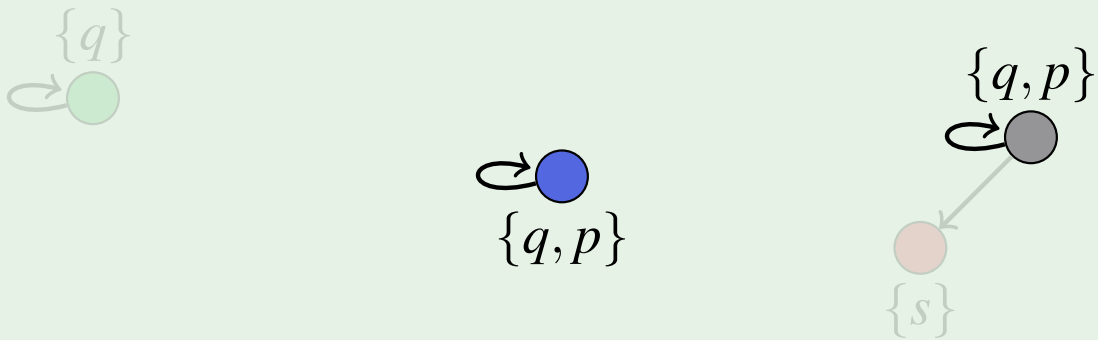


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

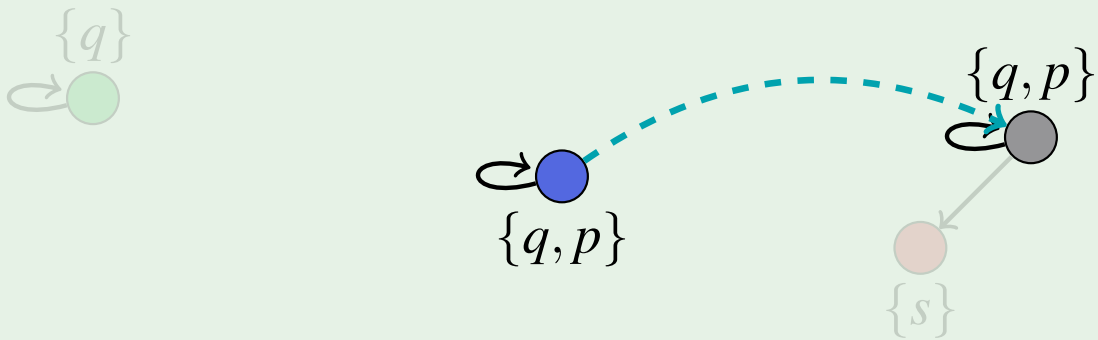


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

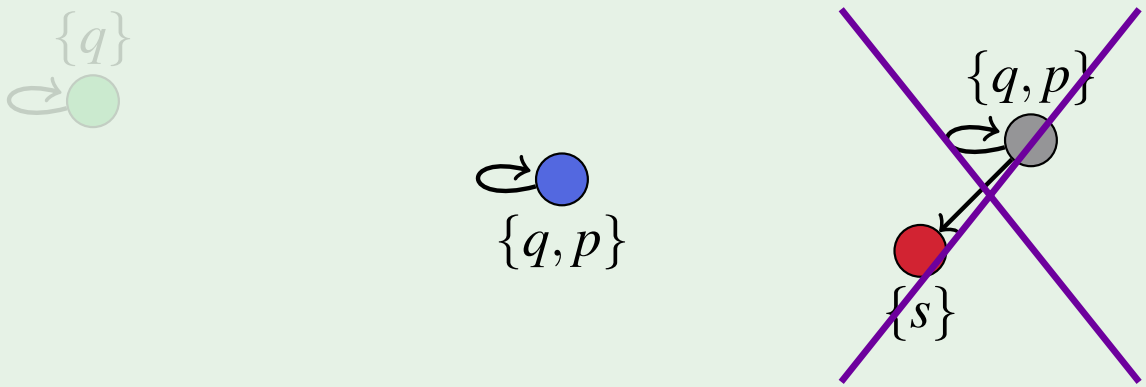


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

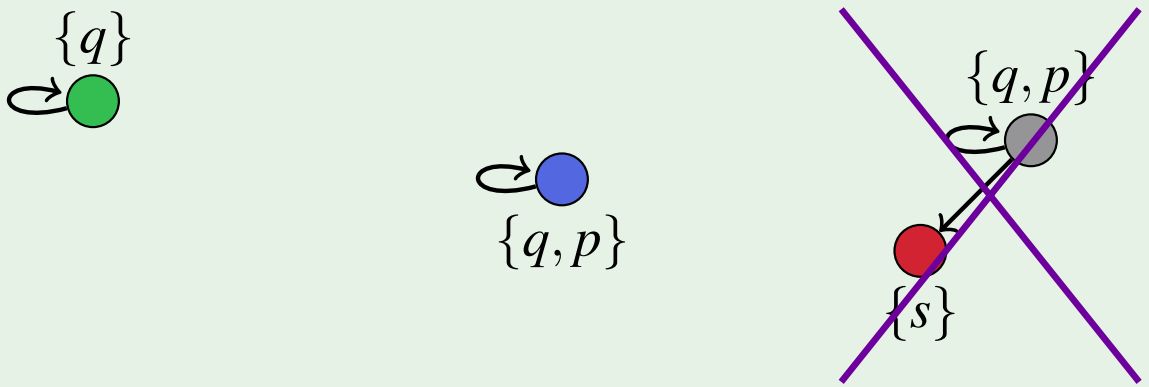


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

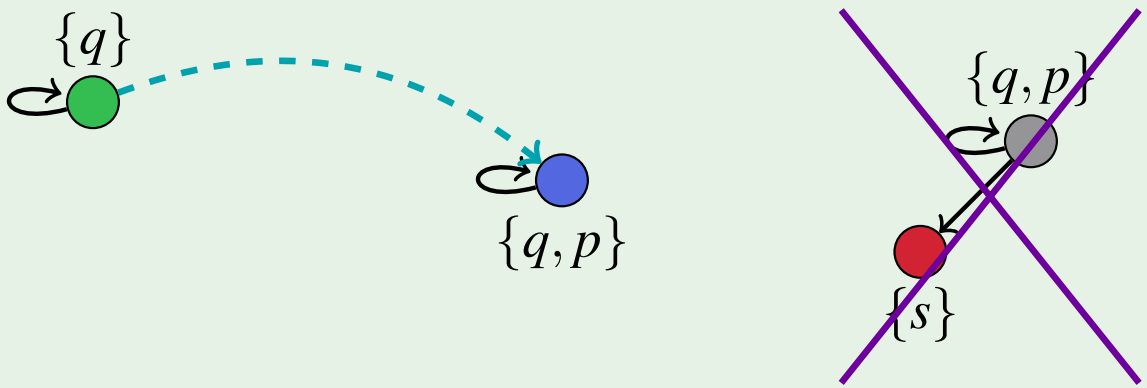


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.

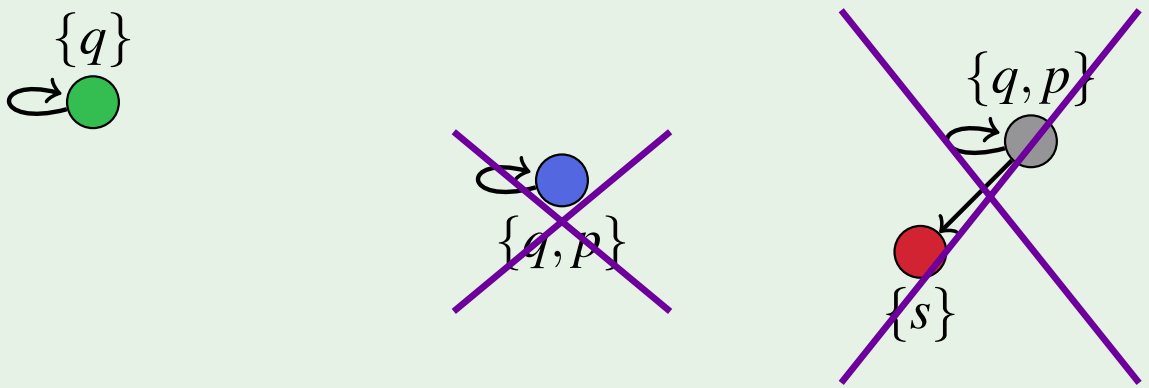


# Practical Remarks

While computing minimal models it is enough to keep only one element of the equivalence class obtained by bisimulation.

This induces a kind of semantic partial order among models.

Minimal models can be computed in an iterative manner.



# Conclusion

We have presented a new minimality criterion that

- is based on semantics
- is able to compare, through a subset relation, the true atoms of distinct worlds in distinct models
- results in finite minimal models for logics with the finite model property

The main draw back w.r.t. to minimal modal Herbrand models is that the minimisation is only on propositional variables and not on relations.

# Conclusion

We have presented a new minimality criterion that

- is based on semantics
- is able to compare, through a subset relation, the true atoms of distinct worlds in distinct models
- results in finite minimal models for logics with the finite model property

The main draw back w.r.t. to minimal modal Herbrand models is that the minimisation is only on propositional variables and not on relations.

There are still few open questions.

- How to efficiently do subset-simulation tests?
- Minimal model completeness is not to aim for. What are reasonable properties that a calculus should have?

*Thank You!*