Active diagnosis for probabilistic systems

Nathalie Bertrand, Éric Fabre, Stefan Haar,
Serge Haddad, Loïc Hélouët

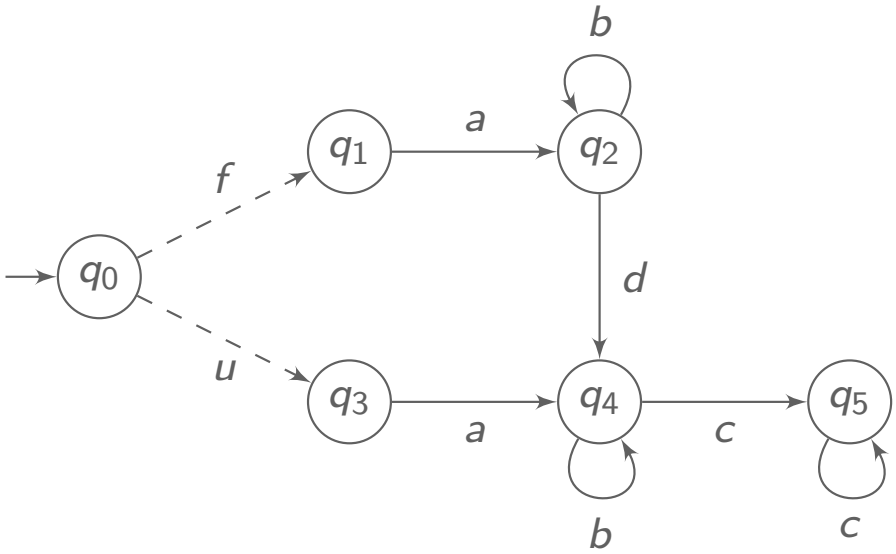
Inria

Diagnosis

Objective: tell whether a fault occurred, based on observations.

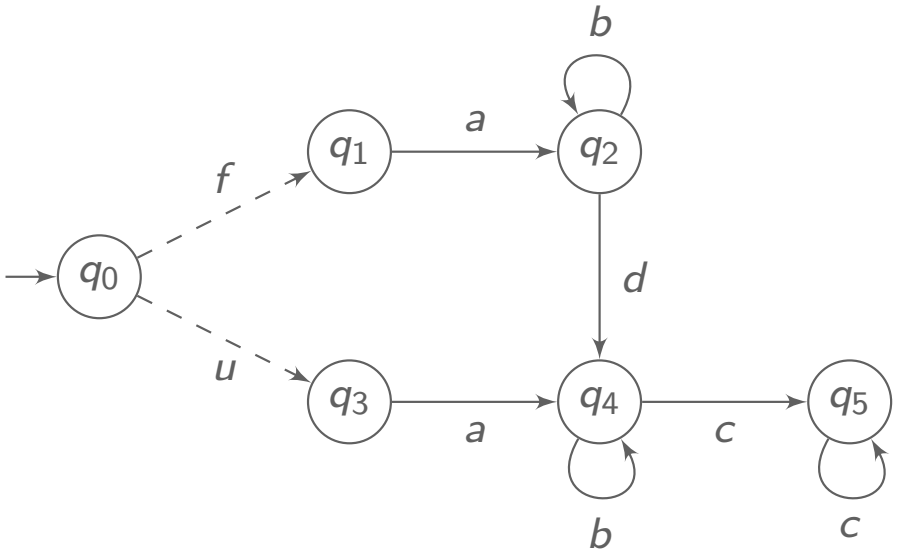
Diagnosis

Objective: tell whether a fault occurred, based on observations.



Diagnosis

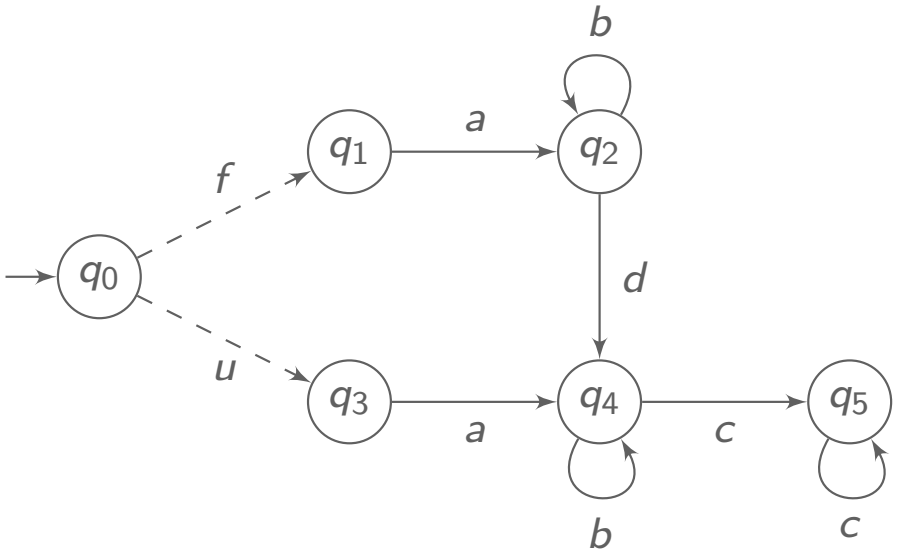
Objective: tell whether a fault occurred, based on observations.



ac^ω	✓	correct
adc^ω	✗	faulty
ab^ω	?	ambiguous

Diagnosis

Objective: tell whether a fault occurred, based on observations.

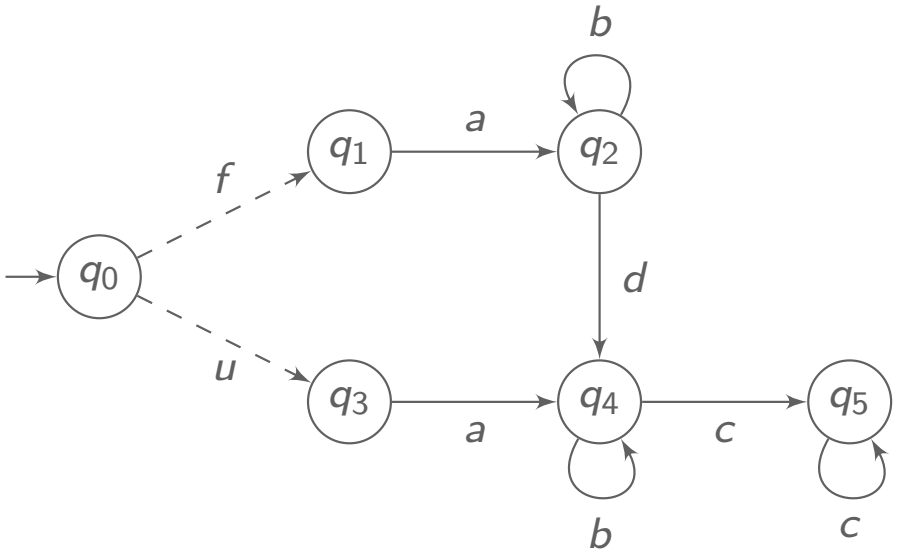


ac^ω	✓	correct
adc^ω	✗	faulty
ab^ω	?	ambiguous

convergence hyp.: no infinite sequence of unobservable events

Diagnosis

Objective: tell whether a fault occurred, based on observations.



ac^ω	✓	correct
adc^ω	✗	faulty
ab^ω	?	ambiguous

convergence hyp.: no infinite sequence of unobservable events

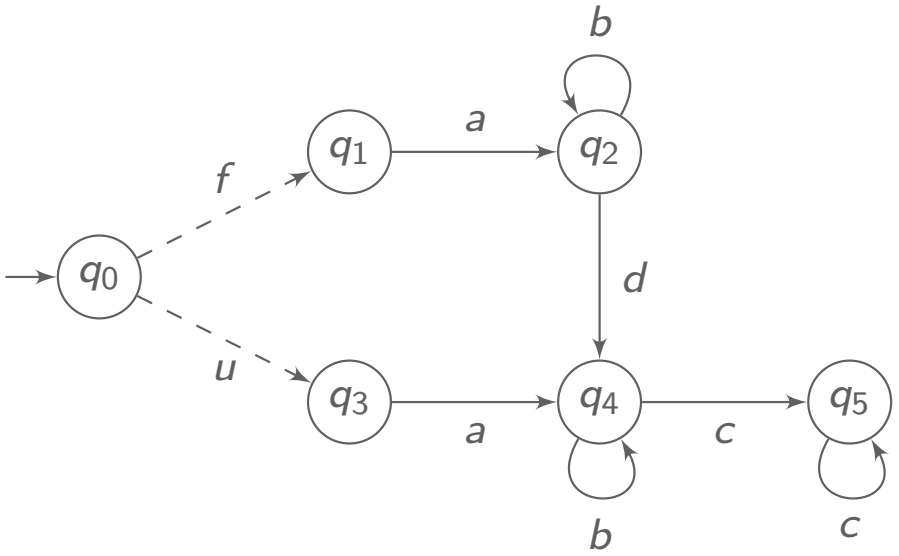
Diagnosability: all infinite observed sequences are unambiguous.

Active diagnosis [HHMS-fsttcs13]

Objective: control the system so that it is diagnosable

Active diagnosis [HHMS-fsttcs13]

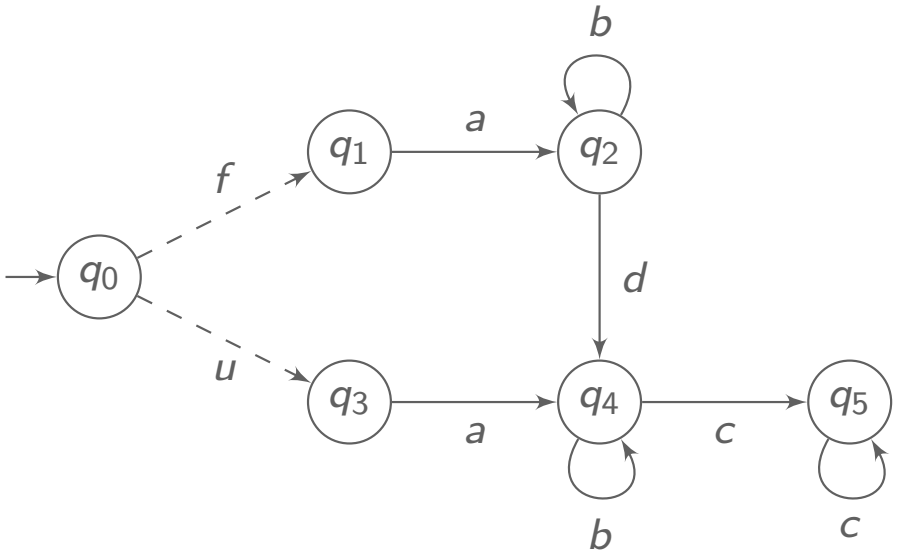
Objective: control the system so that it is diagnosable



ab^ω ambiguous

Active diagnosis [HHMS-fsttcs13]

Objective: control the system so that it is diagnosable

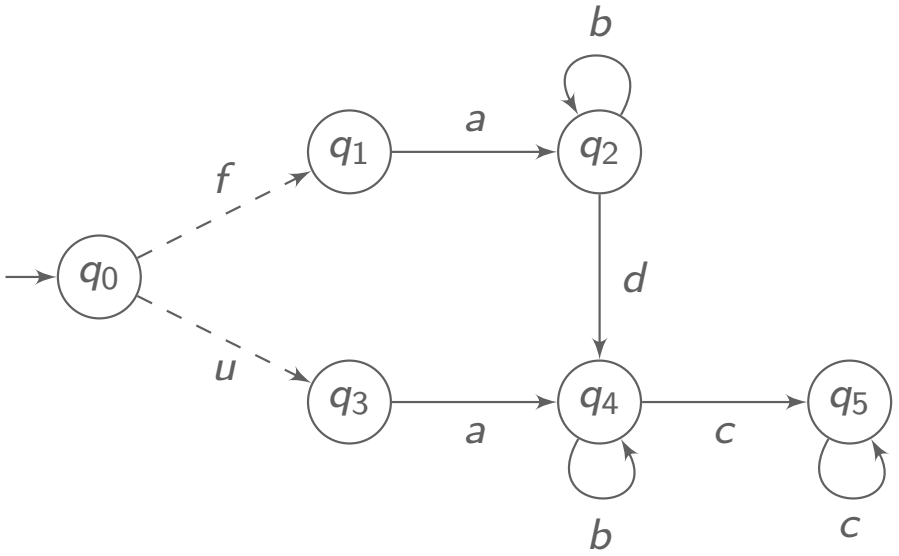


ab^ω ambiguous

always forbid b
$\Longrightarrow$ diagnosable

Active diagnosis [HHMS-fsttcs13]

Objective: control the system so that it is diagnosable



ab^ω ambiguous

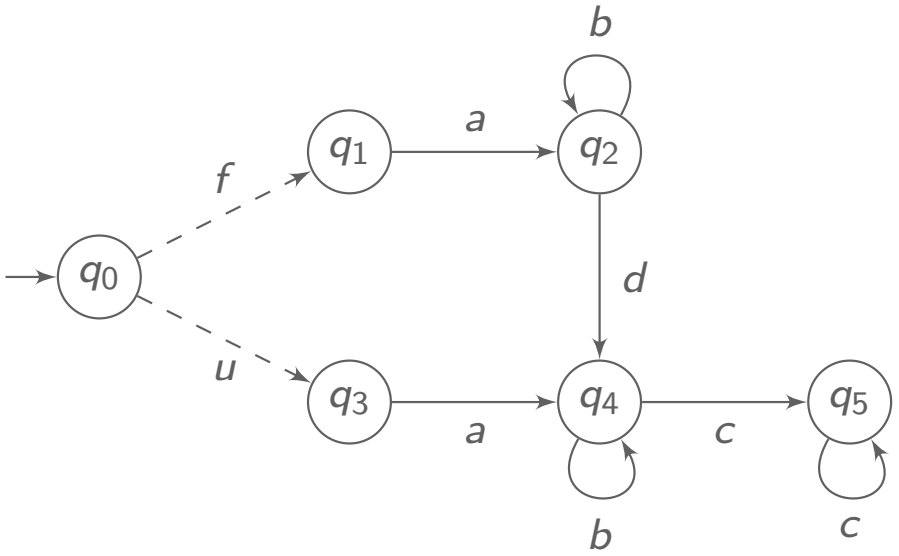
always forbid b
$\Longrightarrow$ diagnosable

Controller: based on observation, decides which actions are allowed

$\sigma : \Sigma_{\text{obs}}^* \to 2^{\Sigma_{\text{cont}}}$ (Σ_{cont} controllable actions)

Active diagnosis [HHMS-fsttcs13]

Objective: control the system so that it is diagnosable



ab^ω ambiguous

always forbid b
$\Longrightarrow$ diagnosable

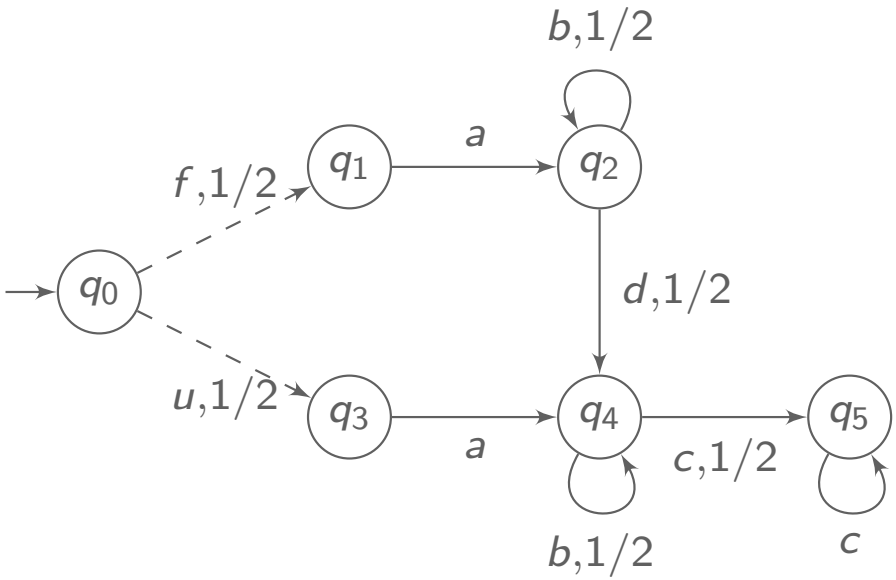
Controller: based on observation, decides which actions are allowed

$\sigma : \Sigma_{\text{obs}}^* \to 2^{\Sigma_{\text{cont}}}$ (Σ_{cont} controllable actions)

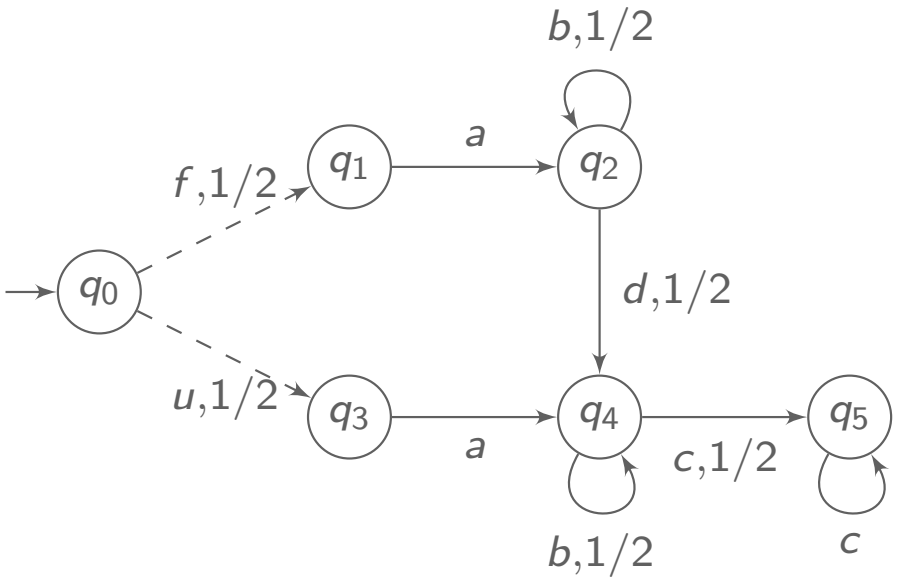
Active diagnosis problem
does there exist a controller such that the system is diagnosable?

caution: the system must remain *live*.

Diagnosis of probabilistic systems

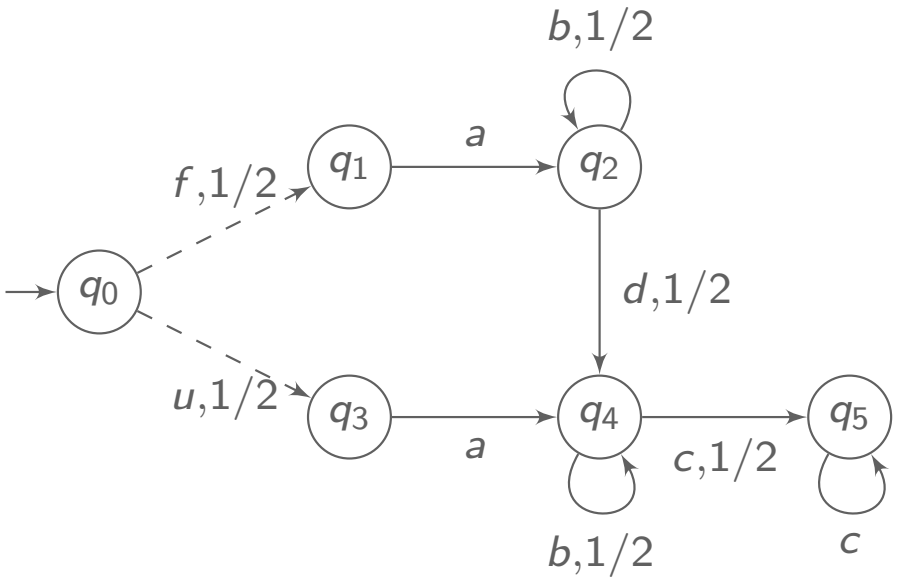


Diagnosis of probabilistic systems



ab^ω ambiguous

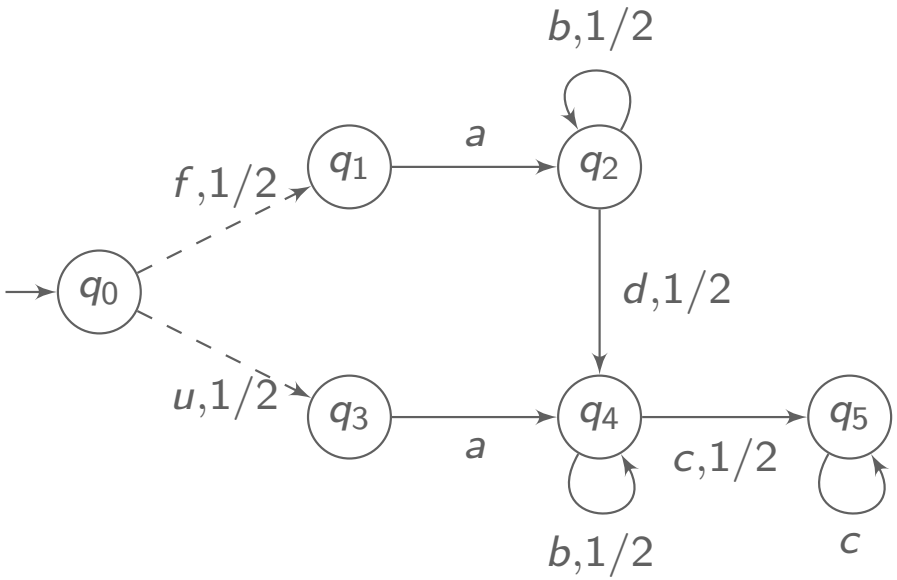
Diagnosis of probabilistic systems



ab^ω ambiguous

$\mathbb{P}(fab^\omega + uab^\omega) = 0$

Diagnosis of probabilistic systems



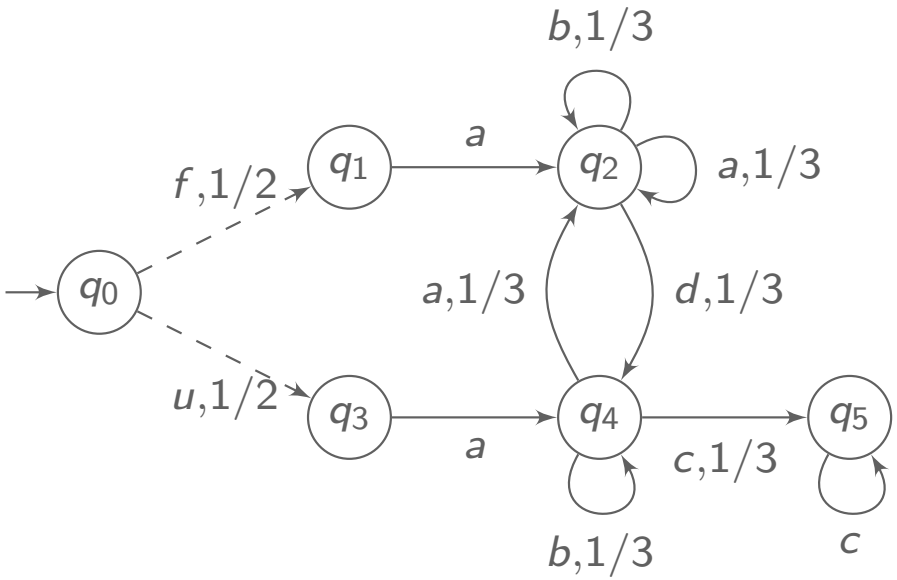
ab^ω ambiguous

$\mathbb{P}(fab^\omega + uab^\omega) = 0$

Almost-sure diagnosability: **almost all** runs have unambiguous observation

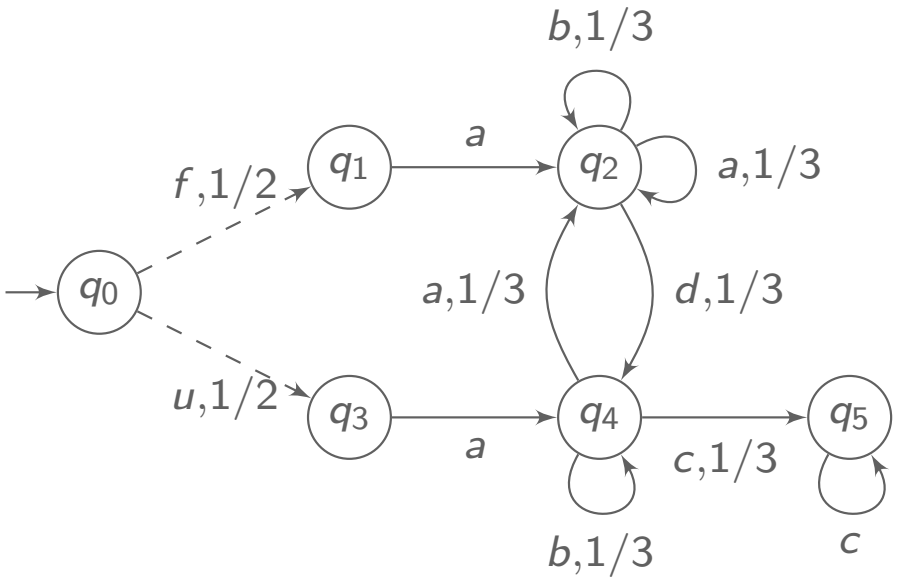
Active probabilistic diagnosis

Objective: control the system so that it is almost-surely diagnosable



Active probabilistic diagnosis

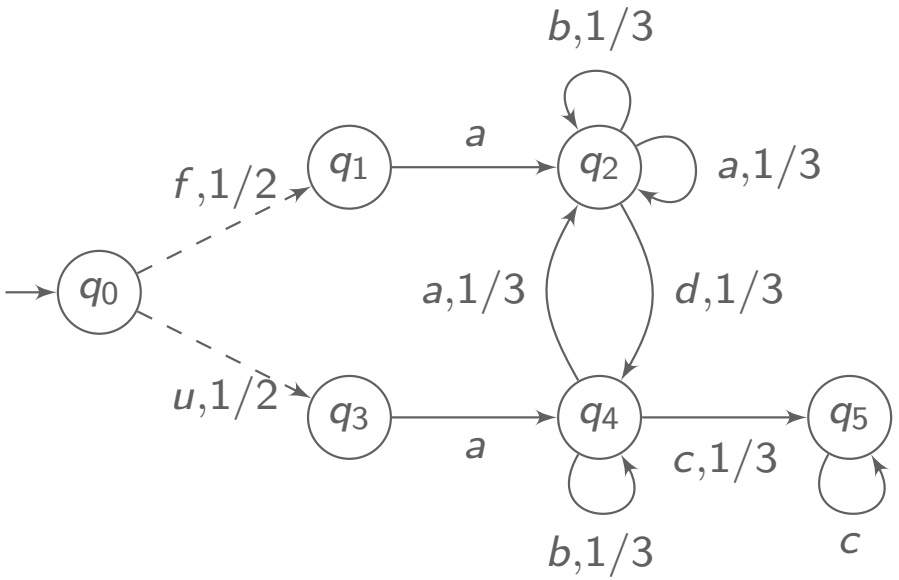
Objective: control the system so that it is almost-surely diagnosable



$aadc^\omega$ ambiguous
$\mathbb{P}(faadc^\omega + uaadc^\omega) > 0$

Active probabilistic diagnosis

Objective: control the system so that it is almost-surely diagnosable

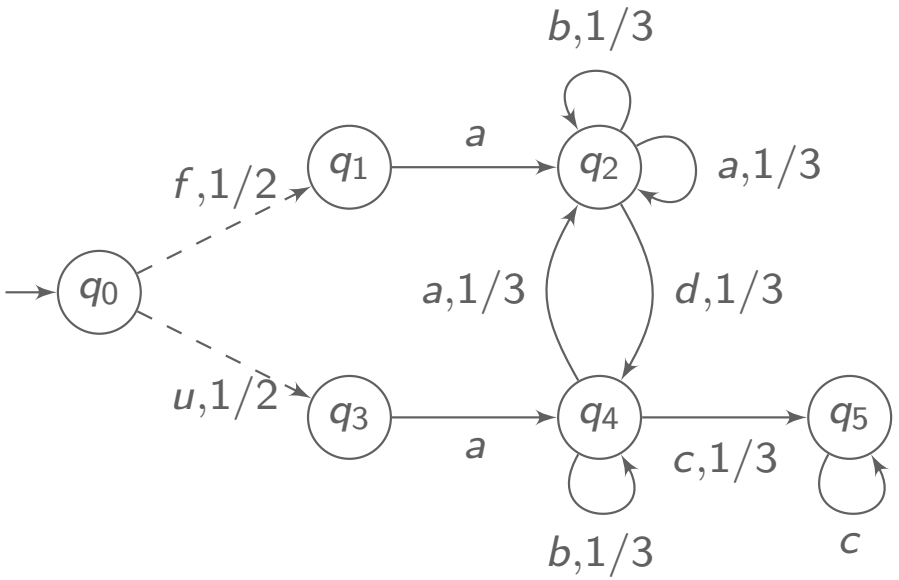


$aadc^\omega$ ambiguous
$\mathbb{P}(faadc^\omega + uaadc^\omega) > 0$

forbid a after first a

Active probabilistic diagnosis

Objective: control the system so that it is almost-surely diagnosable



$aadc^\omega$ ambiguous
$\mathbb{P}(faadc^\omega + uaadc^\omega) > 0$

forbid a after first a

Active probabilistic diagnosis problem
does there exist a controller such that the system is almost-surely diagnosable?

Active probabilistic diagnosis

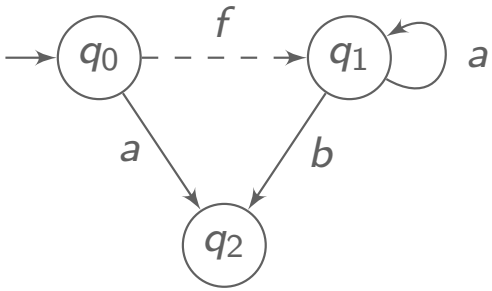
The active probabilistic diagnosis problem is EXPTIME-complete.

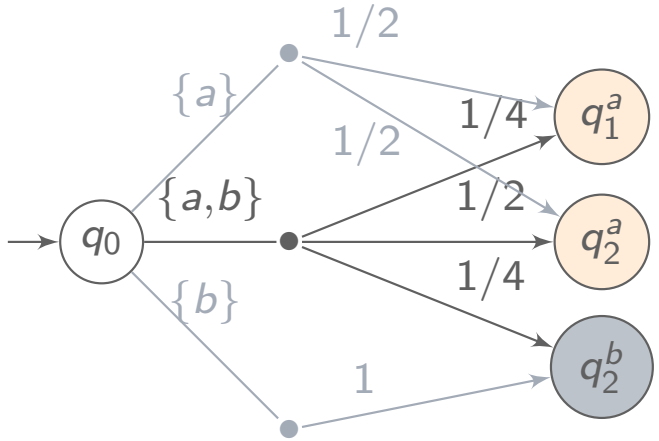
Active probabilistic diagnosis

The active probabilistic diagnosis problem is EXPTIME-complete.

Proof idea (upper bound)

- characterize unambiguous sequences by deterministic Büchi automaton $\mathcal{B}$ [HHMS-fsttcs13]
- build the product of probabilistic LTS with $\mathcal{B}$
- view it as POMDP $\mathcal{P}$





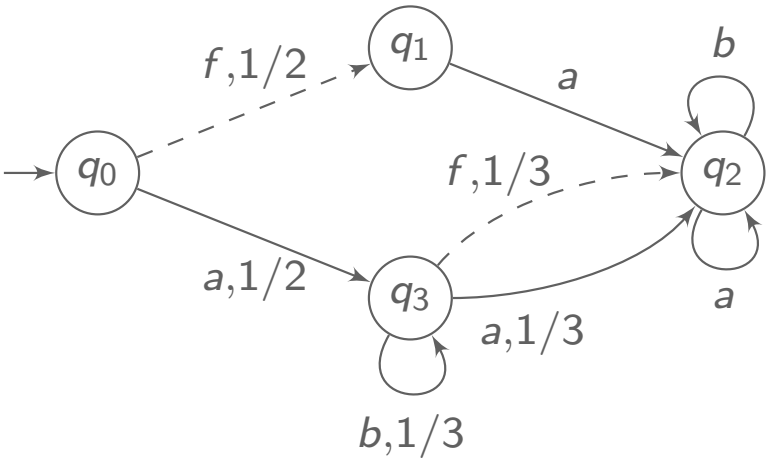
- decide whether there is an almost-surely winning strategy for the Büchi condition on $\mathcal{P}$ [BBG-fossacs08,CDGH-mfcs10]

Safe active probabilistic diagnosis

Objective: avoid fault-provocative controllers

Safe active probabilistic diagnosis

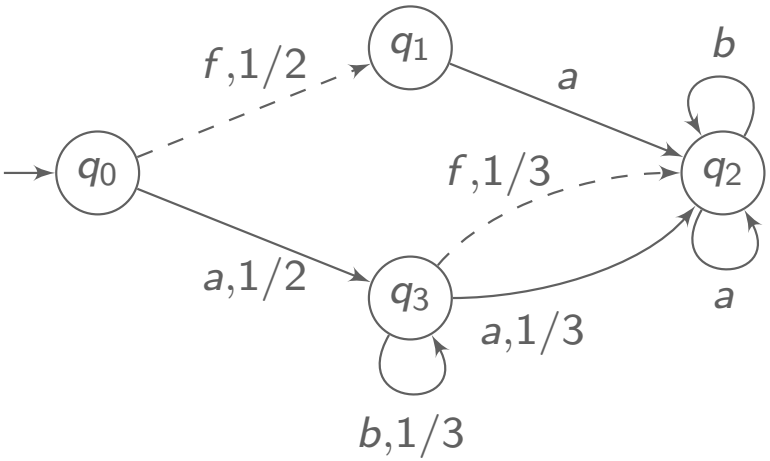
Objective: avoid fault-provocative controllers



all observed sequences ambiguous

Safe active probabilistic diagnosis

Objective: avoid fault-provocative controllers

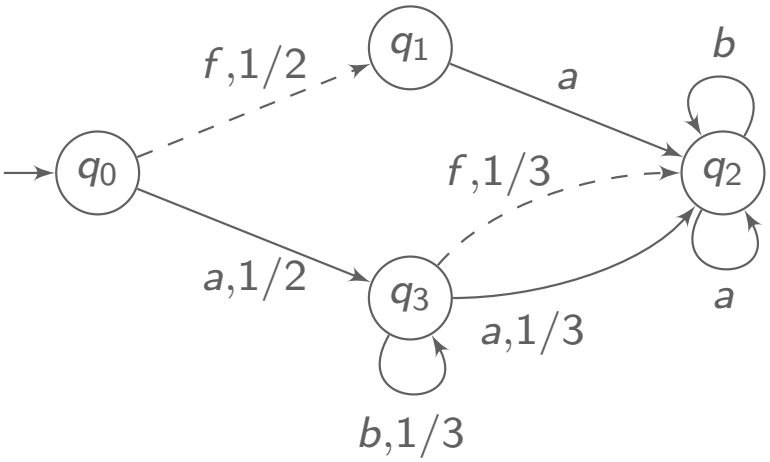


all observed sequences ambiguous

forbid a after first a
$\Longrightarrow$ diagnosable...
but almost all sequences faulty!

Safe active probabilistic diagnosis

Objective: avoid fault-provocative controllers



all observed sequences ambiguous

forbid a after first a
$\Longrightarrow$ diagnosable...
but almost all sequences faulty!

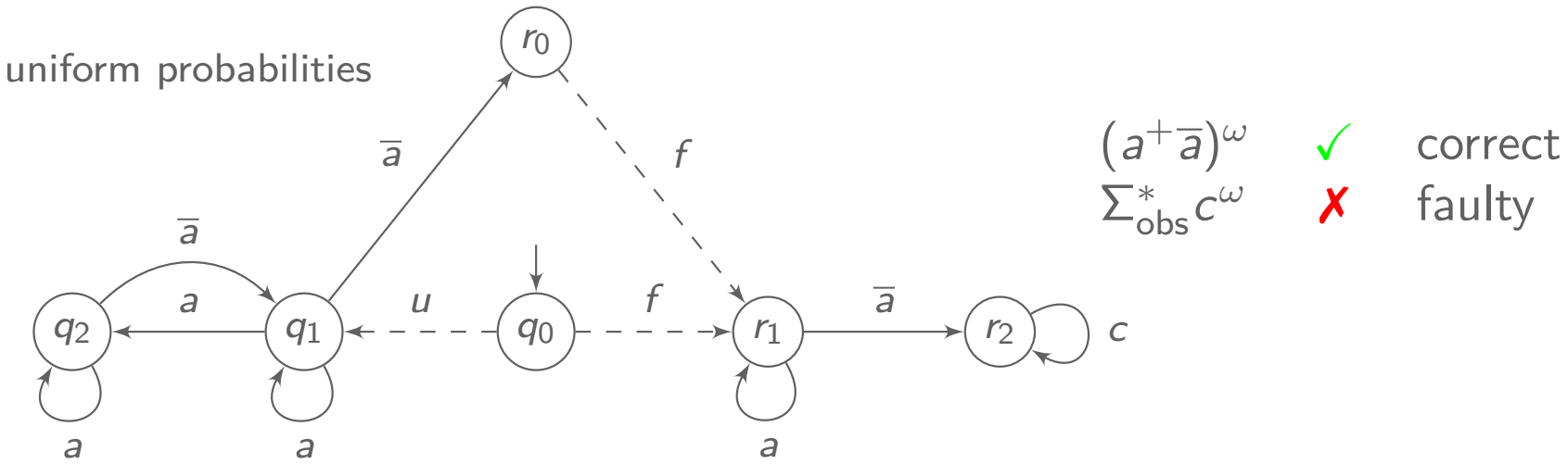
Safe active probabilistic diagnosis
does there exist a controller such that the system is almost-surely diagnosable **and** correct runs have positive probability?

Safe active probabilistic diagnosis – beliefs are not enough!

Infinite memory is needed for safe probabilistic diagnosis.

Safe active probabilistic diagnosis – beliefs are not enough!

Infinite memory is needed for safe probabilistic diagnosis.



- Safe controller: infinitely many $\overline{a}$'s to diagnose all faults...
  but not too often, to have non-negligible correct runs
- Finite-memory controllers almost-surely force a fault.

Safe active probabilistic diagnosis

The safe active probabilistic diagnosis problem is undecidable.

Safe active probabilistic diagnosis

The safe active probabilistic diagnosis problem is undecidable.

Proof idea

- reduction from the existence, in a blind POMDP, of a strategy ensuring a Büchi objective with positive probability
- mimicking example where infinite-memory is needed

Safe active probabilistic diagnosis

The safe active probabilistic diagnosis problem is undecidable.

Proof idea

- reduction from the existence, in a blind POMDP, of a strategy ensuring a Büchi objective with positive probability
- mimicking example where infinite-memory is needed

New result for POMDP

The existence of a strategy ensuring a Büchi objective almost-surely and a safety objective with positive probability is undecidable.

while independently, both problems are decidable

Conclusion

Summary

- (safe) active diagnosis problem for probabilistic systems
- partially observable Markov decision process framework
- active probabilistic diagnosis EXPTIME-complete
- safe active probabilistic diagnosis
  - undecidable in general
  - EXPTIME-complete for **finite memory** controllers (new result)

Conclusion

Summary

- (safe) active diagnosis problem for probabilistic systems
- partially observable Markov decision process framework
- active probabilistic diagnosis EXPTIME-complete
- safe active probabilistic diagnosis
  - undecidable in general
  - EXPTIME-complete for **finite memory** controllers (new result)

Future work

- combinations of objectives for POMDP
- towards quantitative questions
- predictability for probabilistic systems

Thanks for your attention

Details for the undecidability proof