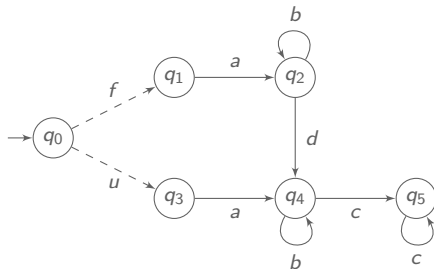


Active diagnosis for probabilistic systems

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

Diagnosis

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

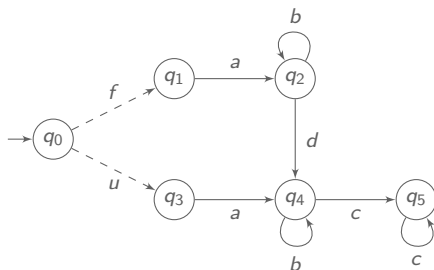


ac^ω	✓	correct
adc^ω	✗	faulty
ab^ω	?	ambiguous

Diagnosability: all observed sequences are unambiguous.

Active diagnosis

Objective: control the system so that it is diagnosable



ab^ω ambiguous

always forbid b
 \implies diagnosable

Controller: based on observation, decides what actions are allowed

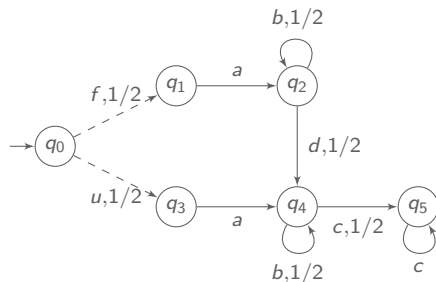
$$\sigma : \Sigma_{\text{obs}}^* \rightarrow \text{Dist}(2^{\Sigma_{\text{cont}}})$$

Active diagnosis problem

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

caution: the system must remain *live*.

Diagnosis of probabilistic systems



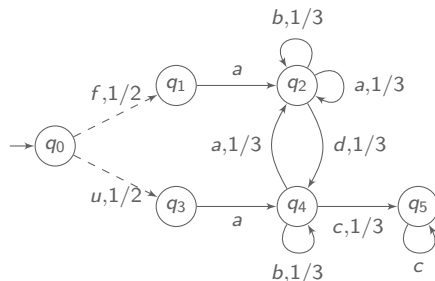
ab^ω ambiguous

$$\mathbb{P}(\pi_{\text{obs}}^{-1}(ab^\omega)) = 0$$

Almost-sure diagnosability: almost all sequences have unambiguous observation

Active probabilistic diagnosis

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



$aadc^\omega$ ambiguous
 $\mathbb{P}(\pi_{\text{obs}}^{-1}(aadc^\omega)) > 0$

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

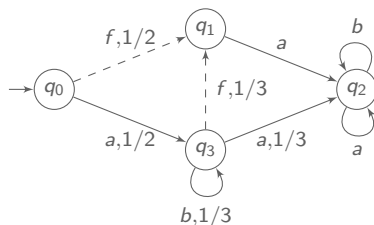
The active probabilistic diagnosis problem is **EXPTIME-complete**.

Proof idea (upper bound)

- ▶ characterize unambiguous sequences by deterministic Büchi automaton \mathcal{B} [HHMS-fttcs13]
- ▶ build the product of probabilistic LTS with \mathcal{B} , and view it as partially observable Markov decision process (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



all observed sequences ambiguous

forbid a after first a
 \implies diagnosable...

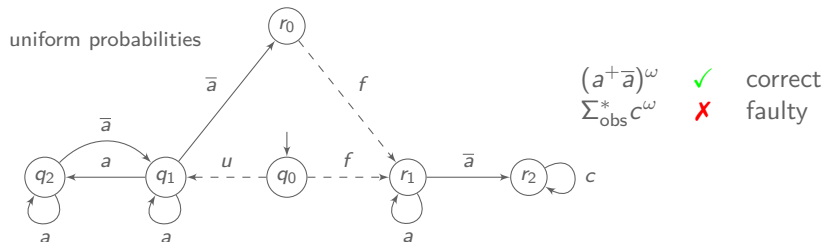
but all sequences faulty!

Safe active probabilistic diagnosis

does there exist a controller such that the system is almost-surely diagnosable **and** correct sequences have positive probability?

Safe active probabilistic diagnosis – beliefs are not enough!

Counting controllers are needed for safe probabilistic diagnosis.



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

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 the previous example where finite-memory strategies are not enough

▶ Details

New result for POMDP

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

nb: 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

Future work

- ▶ combinations of objectives for POMDP
- ▶ visible and non-visible objectives in POMDP
- ▶ predictability for probabilistic systems

Thanks for your attention

Details for the undecidability proof

▶ Back

