Fault diagnosis for Probabilistic Systems

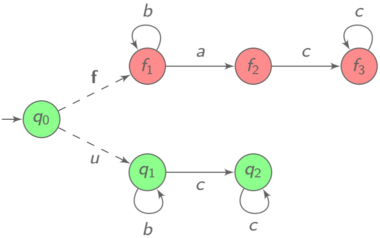
Nathalie Bertrand

Inria Rennes, France

based on joint work with Éric Fabre, Stefan Haar, Serge Haddad, Loïc Hélouët and Engel Lefaucheux

Fault diagnosis in discrete event systems [SSLST95]

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

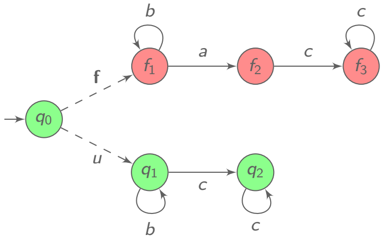


f fault
$\Sigma_o = \{a, b, c\}$ observables

[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

Fault diagnosis in discrete event systems [SSLST95]

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



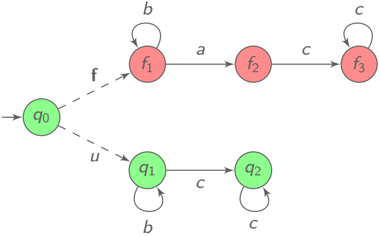
f fault
$\Sigma_o = \{a, b, c\}$ observables

c^+	✓	correct
ac^+	✗	faulty
b^+	?	ambiguous

[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

Fault diagnosis in discrete event systems [SSLST95]

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



f fault
$\Sigma_o = \{a, b, c\}$ observables

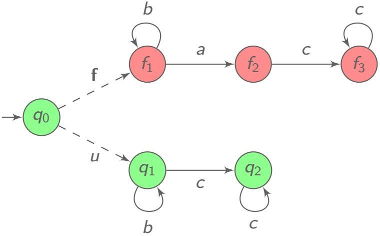
c^+	✓	correct
ac^+	✗	faulty
b^+	?	ambiguous

convergence assumption: no infinite sequence of unobservable events

[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

Fault diagnosis in discrete event systems [SSLST95]

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



f fault
$\Sigma_o = \{a, b, c\}$ observables

c^+	✓	correct
ac^+	✗	faulty
b^+	?	ambiguous

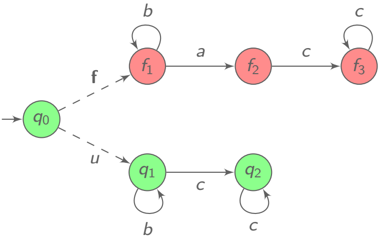
convergence assumption: no infinite sequence of unobservable events

Diagnosability: all observed sequences are unambiguous.

[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

Fault diagnosis in discrete event systems [SSLST95]

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



f fault
$\Sigma_o = \{a, b, c\}$ observables

c^+	✓	correct
ac^+	✗	faulty
b^+	?	ambiguous

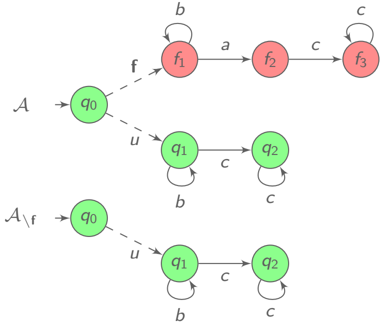
convergence assumption: no infinite sequence of unobservable events

Diagnosability: all observed sequences are unambiguous.

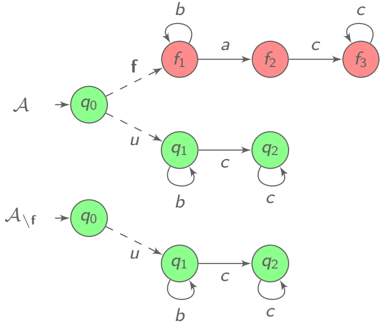
Remark: w.l.o.g. state space partitionned into correct and faulty states

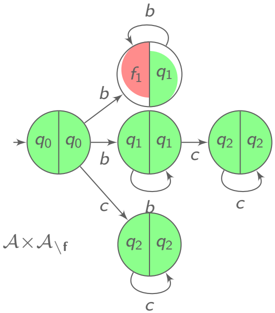
[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

Deciding diagnosability in discrete event systems

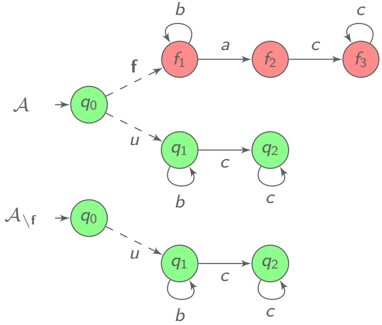


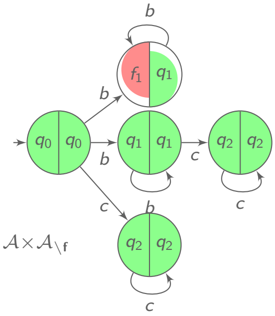
Deciding diagnosability in discrete event systems





Deciding diagnosability in discrete event systems

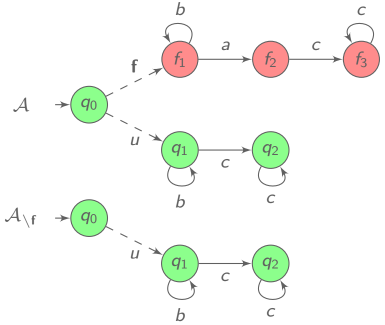


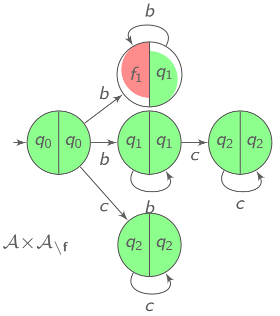


indeterminate cycle: $(f_0, q_0) \cdots \to (f_n, q_n) \to (f_0, q_0)$ s.t. f_i faulty and q_i correct

$\mathcal{A}$ is not diagnosable iff
there exists a reachable indeterminate cycle in $\mathcal{A} \times \mathcal{A}_{\setminus \mathbf{f}}$.

Deciding diagnosability in discrete event systems





indeterminate cycle: $(f_0, q_0) \cdots \rightarrow (f_n, q_n) \rightarrow (f_0, q_0)$ s.t. f_i faulty and q_i correct

$\mathcal{A}$ is not diagnosable iff
there exists a reachable indeterminate cycle in $\mathcal{A} \times \mathcal{A}_{\setminus \mathbf{f}}$.

Decidability and complexity of diagnosability [JHCK01]
Diagnosability is decidable in PTIME.

[JHCK01] Jiang, Huang, Chandra and Kumar, *A polynomial algorithm for testing diagnosability of discrete-event systems*, TAC, 2001.

Diagnosers

Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, \text{✗}, ?\}$

Diagnoser requirements

- **Soundness**: if a fault is claimed, a fault occurred.
- **Reactivity**: every fault is eventually detected.

Diagnosers

Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, \text{✗}, ?\}$

Diagnoser requirements

- **Soundness**: if a fault is claimed, a fault occurred.
- **Reactivity**: every fault is eventually detected.

Diagnosability and diagnosers

$\mathcal{A}$ is diagnosable iff there exists a sound and reactive diagnoser.

Diagnosers

Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, \text{✗}, ?\}$

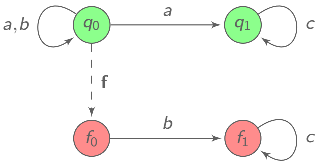
Diagnoser requirements

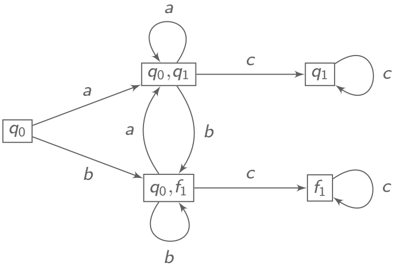
- **Soundness**: if a fault is claimed, a fault occurred.
- **Reactivity**: every fault is eventually detected.

Diagnosability and diagnosers

$\mathcal{A}$ is diagnosable iff there exists a sound and reactive diagnoser.

Diagnosers can be represented by deterministic finite state automata.





Diagnosers

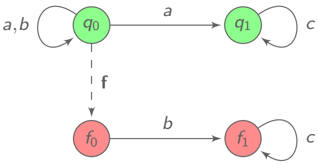
Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, ✗, ?\}$

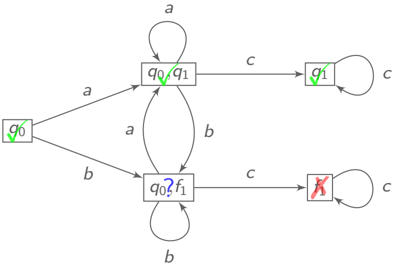
Diagnoser requirements

- **Soundness**: if a fault is claimed, a fault occurred.
- **Reactivity**: every fault is eventually detected.

Diagnosability and diagnosers
$\mathcal{A}$ is diagnosable iff there exists a sound and reactive diagnoser.

Diagnosers can be represented by deterministic finite state automata.





Diagnoser synthesis

Complexity of diagnoser synthesis [JHCK01]
Diagnoser synthesis is in EXPTIME.

intuition: subset construction to track possible correct and faulty states

[JHCK01] Jiang, Huang, Chandra and Kumar, *A polynomial algorithm for testing diagnosability of discrete-event systems*, TAC, 2001.

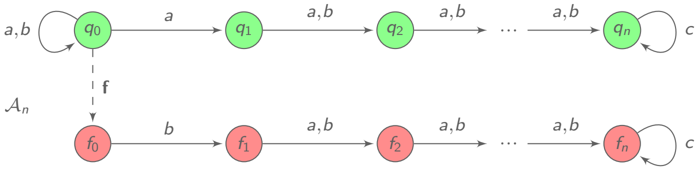
Diagnoser synthesis

Complexity of diagnoser synthesis [JHCK01]

Diagnoser synthesis is in EXPTIME.

intuition: subset construction to track possible correct and faulty states

There is a family $(\mathcal{A}_n)$ of diagnosable systems such that $\mathcal{A}_n$ has $2n+2$ states and any diagnoser needs 2^n states.

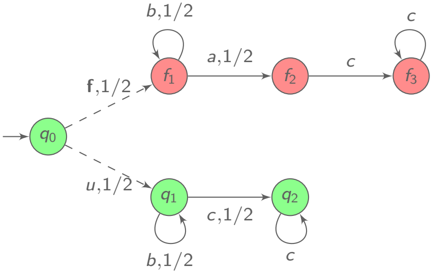


diagnoser must remember the last n events: 2^n possibilities

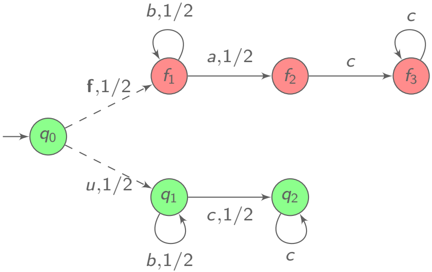
[JHCK01] Jiang, Huang, Chandra and Kumar, *A polynomial algorithm for testing diagnosability of discrete-event systems*, TAC, 2001.

Outline

Diagnosis of probabilistic systems

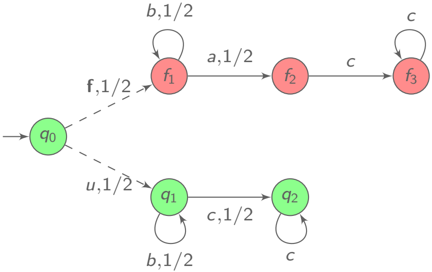


Diagnosis of probabilistic systems



b^ω is ambiguous . . .

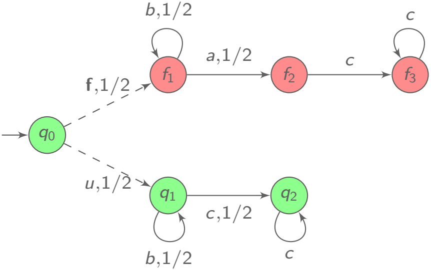
Diagnosis of probabilistic systems



b^ω is ambiguous ...

... yet $\mathbb{P}(\mathbf{f}b^\omega + ub^\omega) = 0$

Diagnosis of probabilistic systems



b^ω is ambiguous ...

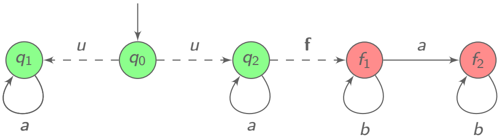
... yet $\mathbb{P}(\mathbf{f}b^\omega + ub^\omega) = 0$

Diagnosability: Probability of infinite ambiguous sequences is zero.

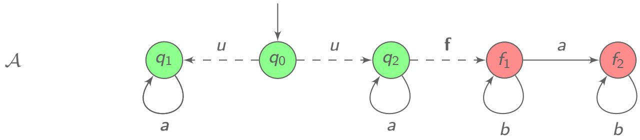
[TT05] Thorsley and Teneketzis, *Diagnosability of stochastic discrete-event systems*, TAC, 2005.
[CK13] Chen and Kumar, *Polynomial test for stochastic diagnosability of dicrete-event systems*, TASE, 2013.
[BHL14] **B.**, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS'14.

Characterisation of diagnosability

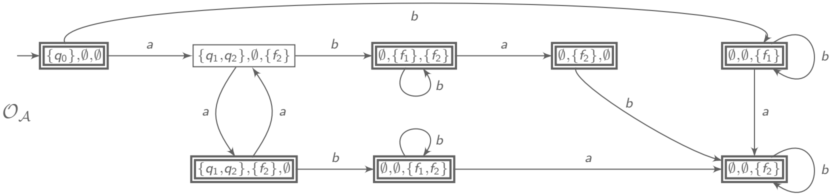
$\mathcal{A}$



Characterisation of diagnosability

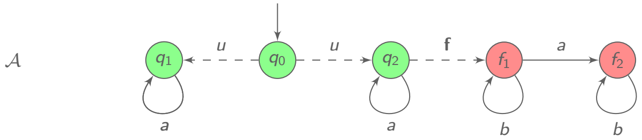


deterministic Büchi automaton $\mathcal{O}_\mathcal{A}$ characterizes non-ambiguous sequences

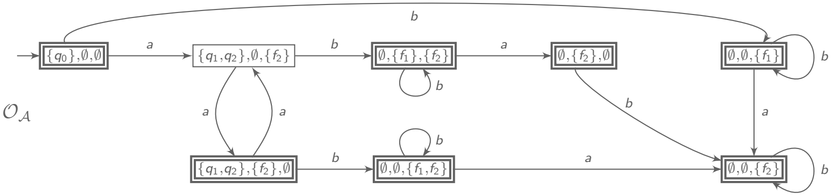


states (U, V, W) with U possible correct states; V waiting room for possible faulty states; W possible faulty states for latest faults [HHMS13]

Characterisation of diagnosability



deterministic Büchi automaton $\mathcal{O}_\mathcal{A}$ characterizes non-ambiguous sequences



states (U, V, W) with U possible correct states; V waiting room for possible faulty states; W possible faulty states for latest faults [HHMS13]

$\mathcal{A}$ is not diagnosable iff
there exists a BSCC of $\mathcal{A} \times \mathcal{O}_\mathcal{A}$ where every state (q, U, V, W) satisfies
q faulty and $U \neq \emptyset$ or q correct and $W \neq \emptyset$.

[HHMS13] Haar, Haddad, Melliti and Schwoon, *Optimal constructions for active diagnosis*, FSTTCS'13.

Complexity of diagnosability

Diagnosability is in PSPACE for probabilistic systems.

Complexity of diagnosability

Diagnosability is in PSPACE for probabilistic systems.

NFA $\mathcal{A}$ is eventually universal if there exists w such that $w\Sigma^* \subseteq \mathcal{L}(\mathcal{A})$.

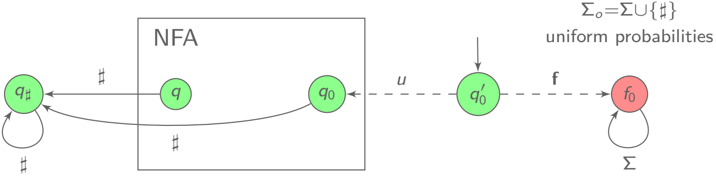
The eventual universality problem for live NFA
in which all states are accepting is PSPACE-hard.

Complexity of diagnosability

Diagnosability is in PSPACE for probabilistic systems.

NFA $\mathcal{A}$ is eventually universal if there exists w such that $w\Sigma^* \subseteq \mathcal{L}(\mathcal{A})$.

The eventual universality problem for live NFA
in which all states are accepting is PSPACE-hard.

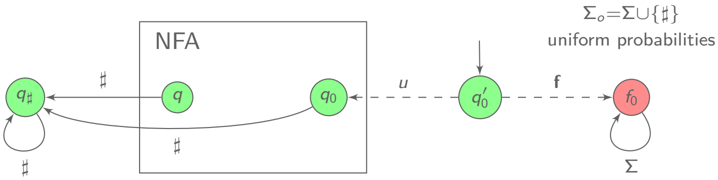


Complexity of diagnosability

Diagnosability is in PSPACE for probabilistic systems.

NFA $\mathcal{A}$ is eventually universal if there exists w such that $w\Sigma^* \subseteq \mathcal{L}(\mathcal{A})$.

The eventual universality problem for live NFA
in which all states are accepting is PSPACE-hard.



Diagnosability is PSPACE-complete for probabilistic systems. [BHL14]

[BHL14] **B.**, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS'14.

Diagnosers

Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, ✗, ?\}$

Diagnoser requirements

- **Soundness**: 1) If a fault is claimed, a fault occurred
  2) If ✓ is emitted, then the length of a surely correct prefix increases.
- **Reactivity**: almost surely infinitely often ✓ or eventually always ✗.

Diagnosers

Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, \text{✗}, ?\}$

Diagnoser requirements

- **Soundness**: 1) If a fault is claimed, a fault occurred
  2) If ✓ is emitted, then the length of a surely correct prefix increases.
- **Reactivity**: almost surely infinitely often ✓ or eventually always ✗.

Diagnosability and diagnosers [BHL14]
$\mathcal{A}$ is diagnosable iff there exists a sound and reactive diagnoser.

For every diagnosable system with n correct states
one can build a diagnoser with at most 3^n states.

[BHL14] **B.**, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS'14.

Diagnosers

Diagnoser: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, ✗, ?\}$

Diagnoser requirements

- **Soundness**: 1) If a fault is claimed, a fault occurred
  2) If ✓ is emitted, then the length of a surely correct prefix increases.
- **Reactivity**: almost surely infinitely often ✓ or eventually always ✗.

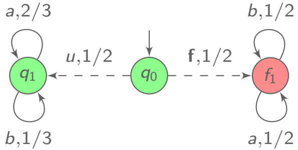
Diagnosability and diagnosers [BHL14]
$\mathcal{A}$ is diagnosable iff there exists a sound and reactive diagnoser.

For every diagnosable system with n correct states
one can build a diagnoser with at most 3^n states.

Diagnoser derived from observer $\mathcal{O}_{\mathcal{A}}$: ✗ in states $(\emptyset, V, W)$
✓ in states $(U, V, \emptyset)$ with $U \neq \emptyset$
? otherwise.

[BHL14] **B.**, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS'14.

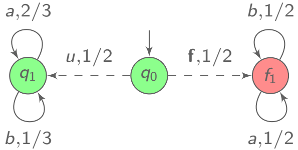
Accurate approximate diagnosis



Not diagnosable: All observed sequences are ambiguous!

[TT05] Thorsley and Teneketzis, *Diagnosability of stochastic discrete-event systems*, TAC, 2005.

Accurate approximate diagnosis

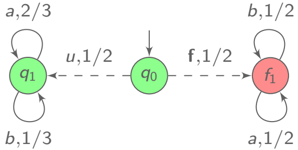


Not diagnosable: All observed sequences are ambiguous!

Approximate diagnosis: [TT05]
claim a fault when proportions of a's and b's are sensibly equal.

[TT05] Thorsley and Teneketzis, *Diagnosability of stochastic discrete-event systems*, TAC, 2005.

Accurate approximate diagnosis



Not diagnosable: All observed sequences are ambiguous!

Approximate diagnosis: [TT05]
claim a fault when proportions of a's and b's are sensibly equal.

Decidability of approximate diagnosability [BHL16?]
Approximate diagnosability is decidable in PTIME.

[TT05] Thorsley and Teneketzis, *Diagnosability of stochastic discrete-event systems*, TAC, 2005.
[BHL16?] **B.**, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems* , submitted.

Outline

Introduction to fault diagnosis

Diagnosability in probabilistic systems

Control for probabilistic diagnosability

Conclusion

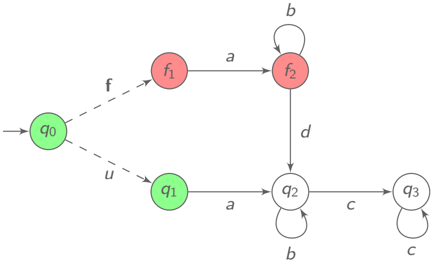
Active diagnosis

Objective: control the system so that it is diagnosable

[SLT98] Sampath, Lafortune and Teneketzis, *Active diagnosis of discrete-event systems*, TAC, 1998.
[CP09] Chanthery and Pencole, *Monitoring and active diagnosis for discrete-event systems*, SafeProcess'09.
[HHMS13] Haar, Haddad, Melliti and Schwoon,*Optimal constructions for active diagnosis*, FSTTCS'13.

Active diagnosis

Objective: control the system so that it is diagnosable

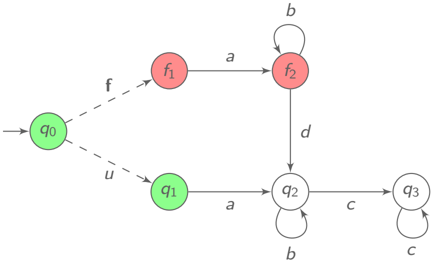


$\Sigma_c = \{a, b, c, d\}$ controllables

[SLT98] Sampath, Lafortune and Teneketzis, *Active diagnosis of discrete-event systems*, TAC, 1998.
[CP09] Chanthery and Pencole, *Monitoring and active diagnosis for discrete-event systems*, SafeProcess'09.
[HHMS13] Haar, Haddad, Melliti and Schwoon,*Optimal constructions for active diagnosis*, FSTTCS'13.

Active diagnosis

Objective: control the system so that it is diagnosable



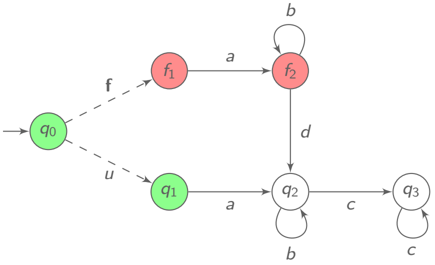
$\Sigma_c = \{a, b, c, d\}$ controllables

ab^ω ambiguous

[SLT98] Sampath, Lafortune and Teneketzis, *Active diagnosis of discrete-event systems*, TAC, 1998.
[CP09] Chanthery and Pencole, *Monitoring and active diagnosis for discrete-event systems*, SafeProcess'09.
[HHMS13] Haar, Haddad, Melliti and Schwoon,*Optimal constructions for active diagnosis*, FSTTCS'13.

Active diagnosis

Objective: control the system so that it is diagnosable



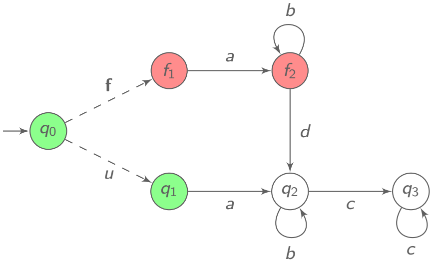
$\Sigma_c = \{a, b, c, d\}$ controllables

ab^ω ambiguous
disable $b \implies$ diagnosable

[SLT98] Sampath, Lafortune and Teneketzis, *Active diagnosis of discrete-event systems*, TAC, 1998.
[CP09] Chanthery and Pencole, *Monitoring and active diagnosis for discrete-event systems*, SafeProcess'09.
[HHMS13] Haar, Haddad, Melliti and Schwoon,*Optimal constructions for active diagnosis*, FSTTCS'13.

Active diagnosis

Objective: control the system so that it is diagnosable



$\Sigma_c = \{a, b, c, d\}$ controllables

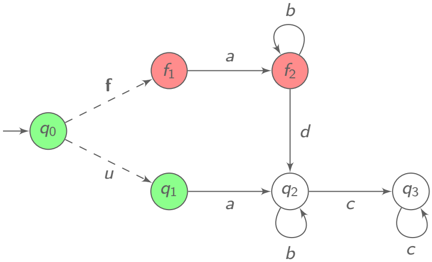
ab^ω ambiguous
disable $b \implies$ diagnosable

Controller: based on observation, decides which actions are allowed
$\sigma : \Sigma_o^* \to 2^{\Sigma_c}$

[SLT98] Sampath, Lafortune and Teneketzis, *Active diagnosis of discrete-event systems*, TAC, 1998.
[CP09] Chanthery and Pencole, *Monitoring and active diagnosis for discrete-event systems*, SafeProcess'09.
[HHMS13] Haar, Haddad, Melliti and Schwoon, *Optimal constructions for active diagnosis*, FSTTCS'13.

Active diagnosis

Objective: control the system so that it is diagnosable



$\Sigma_c = \{a, b, c, d\}$ controllables

ab^ω ambiguous
disable $b \implies$ diagnosable

Controller: based on observation, decides which actions are allowed
$\sigma : \Sigma_o^* \to 2^{\Sigma_c}$

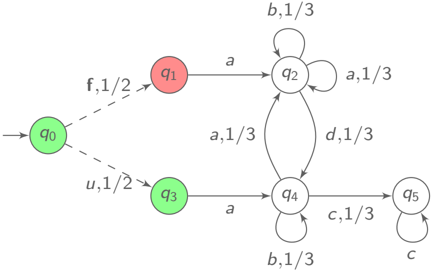
Active diagnosis problem
does there exist a controller such that the system is diagnosable?

caution: the system must remain *live*.

[SLT98] Sampath, Lafortune and Teneketzis, *Active diagnosis of discrete-event systems*, TAC, 1998.
[CP09] Chanthery and Pencole, *Monitoring and active diagnosis for discrete-event systems*, SafeProcess'09.
[HHMS13] Haar, Haddad, Melliti and Schwoon,*Optimal constructions for active diagnosis*, FSTTCS'13.

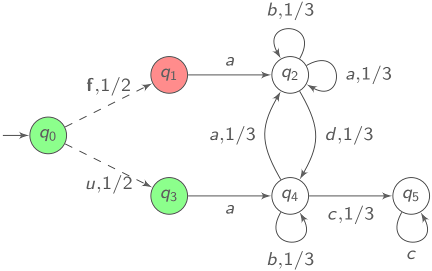
Active probabilistic diagnosis

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



Active probabilistic diagnosis

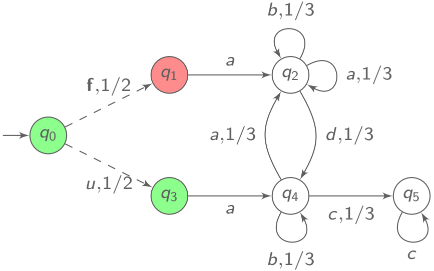
Objective: control the system so that it is almost-surely diagnosable



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

Active probabilistic diagnosis

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

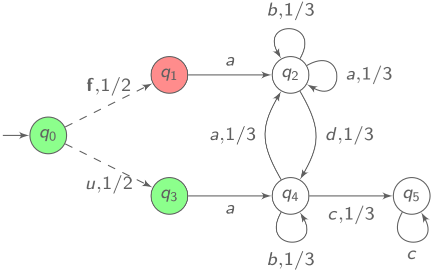


$aadc^\omega$ ambiguous
$\mathbb{P}(\mathbf{f}aadc^\omega + uaadc^\omega) > 0$

disable a after first a

Active probabilistic diagnosis

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



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

disable a after first a

Controller $\sigma : \Sigma_o^* \to \mathsf{Dist}(2^{\Sigma_c})$

Active probabilistic diagnosis problem [BFHHH14]
does there exist a controller such that the system is almost-surely diagnosable?

[BFHHH14] **B.**, Fabre, Haar, Haddad and Hélouët, *Active diagnosis for probabilistic systems*, FoSSaCS'14.

Solving active probabilistic diagnosis

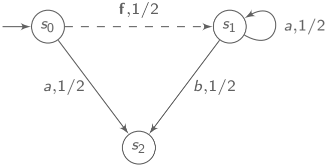
The active probabilistic diagnosis problem is EXPTIME-complete.

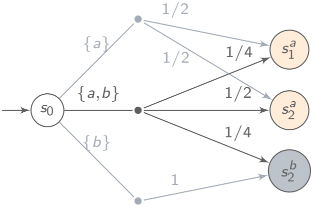
Solving active probabilistic diagnosis

The active probabilistic diagnosis problem is EXPTIME-complete.

Proof idea (upper bound)

- characterize unambiguous sequences by deterministic Büchi automaton $\mathcal{B}$ [HHMS13]
- 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 $\mathcal{P}$ [BBG08,CDGH10]

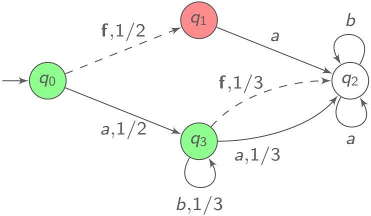
[HHMS13] Haar, Haddad, Melliti and Schwoon, *Optimal constructions for active diagnosis*, FSTTCS'13.
[BBG08] Baier, **B.** and Größer, *On decision problems for probabilistic Büchi automata*, FoSSaCS'08.
[CDGH10] Chatterjee, Doyen, Gimbert and Henzinger, *Randomness for free*, MFCS'10.

Safe active probabilistic diagnosis

Objective: avoid fault-provocative controllers

Safe active probabilistic diagnosis

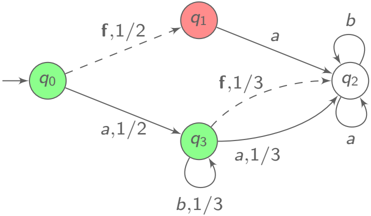
Objective: avoid fault-provocative controllers



all observed sequences ambiguous

Safe active probabilistic diagnosis

Objective: avoid fault-provocative controllers

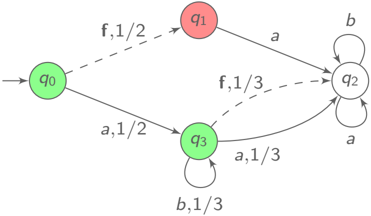


all observed sequences ambiguous

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 [BFHHH14]
does there exist a controller such that the system is almost-surely diagnosable **and** correct runs have positive probability?

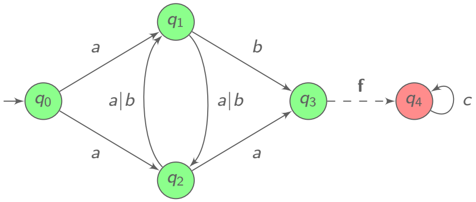
[BFHHH14] **B.**, Fabre, Haar, Haddad and Hélouët, *Active diagnosis for probabilistic systems*, FoSSaCS'14.

Beliefs are not enough!

Positional belief-based controllers do not suffice
for safe probabilistic diagnosis.

Beliefs are not enough!

Positional belief-based controllers do not suffice
for safe probabilistic diagnosis.

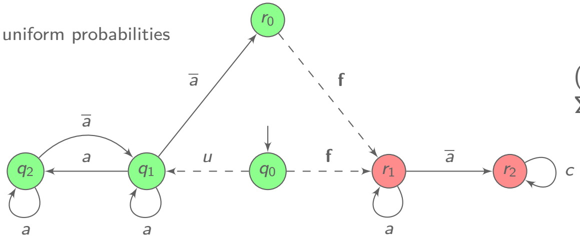


Finite-memory is not enough!

Infinite memory is needed for safe probabilistic diagnosis.

Finite-memory is not enough!

Infinite memory is needed for safe probabilistic diagnosis.



$(a^+\overline{a})^\omega$	✓	correct
$\Sigma_{\mathrm{obs}}^* c^\omega$	✗	faulty

- 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.

Solving safe active probabilistic diagnosis?

The safe active probabilistic diagnosis problem is undecidable.

Solving 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

Solving 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

The existence of a strategy ensuring a Büchi objective almost-surely and a safety objective positively is undecidable for POMDP.

Solving 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

The existence of a strategy ensuring a Büchi objective almost-surely and a safety objective positively is undecidable for POMDP.

The safe active probabilistic diagnosis problem restricted to **finite memory strategies** is EXPTIME-complete.

Outline

Introduction to fault diagnosis

Diagnosability in probabilistic systems

Control for probabilistic diagnosability

Conclusion

Concluding remarks

Contributions: Foundations of stochastic diagnosis

- Investigation of semantical issues
- Tight complexity bounds for diagnosability
  and diagnoser synthesis problems
- Active diagnosability: controller synthesis to ensure diagnosability

Concluding remarks

Contributions: Foundations of stochastic diagnosis

- Investigation of semantical issues
- Tight complexity bounds for diagnosability
  and diagnoser synthesis problems
- Active diagnosability: controller synthesis to ensure diagnosability

Perspectives: Towards more quantitative questions

- Bounded-delay diagnosis
  tradeoff: delay *vs* diagnosability probability
- Space and time optimisation of observations
  tradeoff: observation cost *vs* diagnosability probability
- Active approximate diagnosis