# Fault diagnosis for Probabilistic Systems a semantical and algorithmic journey

Nathalie Bertrand

Inria Rennes, France

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

# Two tales of smoke and observation

Original idea by Stefan Schwoon

# Two tales of smoke and observation

Original idea by Stefan Schwoon

Assuming the behaviour of a system is known, an observer may deduce the occurrence of internal events from the outputs.

# Two tales of smoke and observation

Original idea by Stefan Schwoon

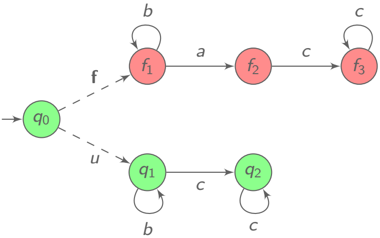
Assuming the behaviour of a system is known, an observer may deduce the occurrence of internal events from the outputs.

Diagnosis, non-interference, information flow, opacity, etc.

# Outline

# Fault diagnosis in discrete event systems [SSLST95]

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

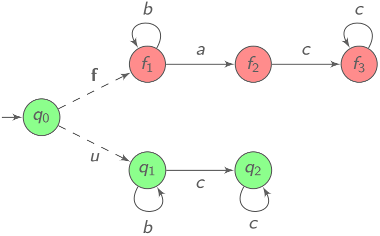



**f** fault
$\Sigma_o = \{a, b, c\}$ observables

[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.



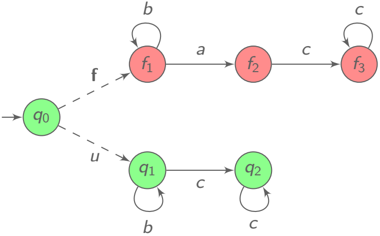

**f** fault
$\Sigma_o = \{a, b, c\}$ observables

| | | |
|---|---|---|
| $c^+$ | ✓ | 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

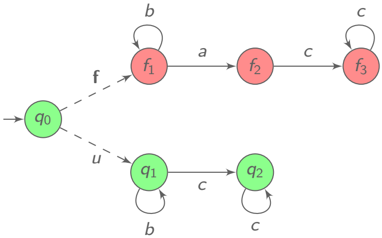
| | | |
|---|---|---|
| $c^+$ | ✓ | correct |
| $ac^+$ | ✗ | faulty |
| $b^+$ | ? | ambiguous |

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 |

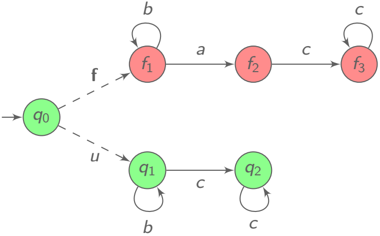
convergence assumption: no infinite sequence of unobservable events

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 |

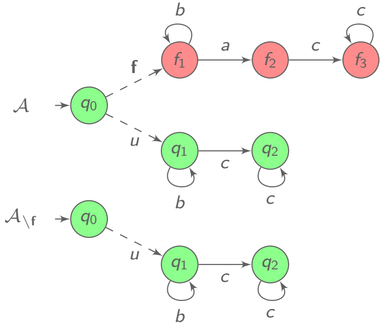
convergence assumption: no infinite sequence of unobservable events

Diagnosability: all observed sequences are unambiguous.

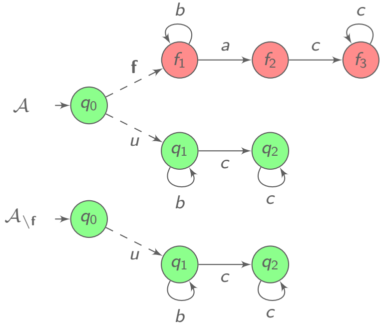
Remark: w.l.o.g. state space partitionned into correct and faulty states

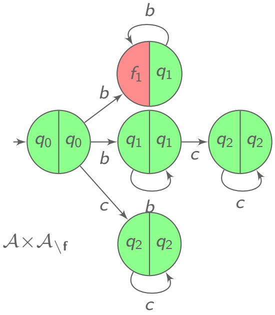
[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

# Deciding diagnosability in discrete event systems

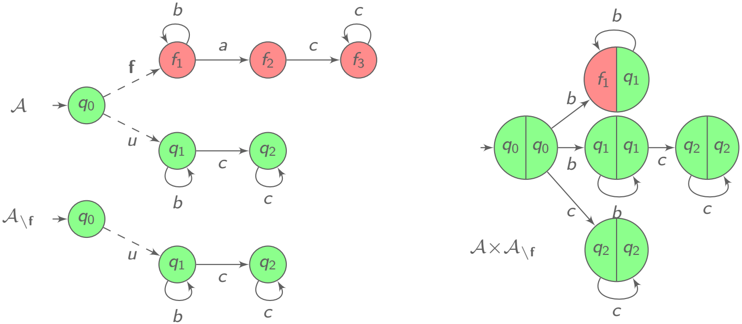


# Deciding diagnosability in discrete event systems



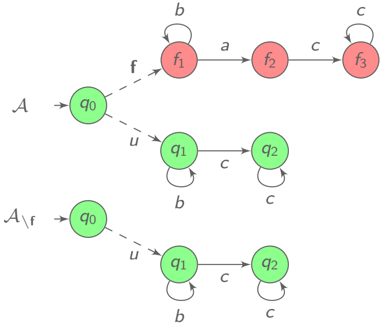
# Deciding diagnosability in discrete event systems

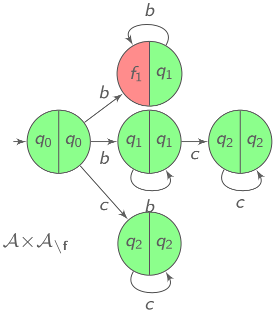



*indeterminate cycle*: $(f_0, q_0) \cdots \to (f_n, q_n) \to (f_0, q_0)$ s.t. $f_i$ faulty and $q_i$ correct

$\mathcal{A}$ 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*: $(f_0, q_0) \cdots \to (f_n, q_n) \to (f_0, q_0)$ s.t. $f_i$ faulty and $q_i$ correct

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

**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 $D : \Sigma_o^* \rightarrow \{✓, ✗, ?\}$

Diagnoser requirements

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

# 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 claimed.

**Diagnosability and diagnosers**

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

# Diagnosers

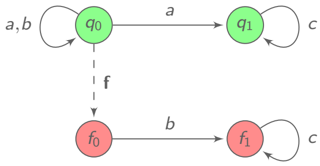
**Diagnoser**: assigns verdicts to observed sequences $D : \Sigma_o^* \to \{\checkmark, ✗, ?\}$

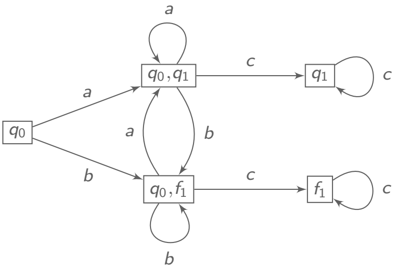
Diagnoser requirements

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

**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 $D : \Sigma_o^* \to \{✓, ✗, ?\}$

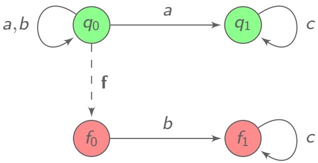
Diagnoser requirements

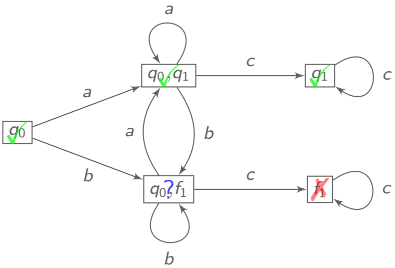
- **Soundness**: if a fault is claimed ✗, a fault occurred.
- **Reactivity**: every fault is eventually claimed.

**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**
Diagnoser synthesis is in EXPTIME.

**intuition**: subset construction to track possible correct and faulty states

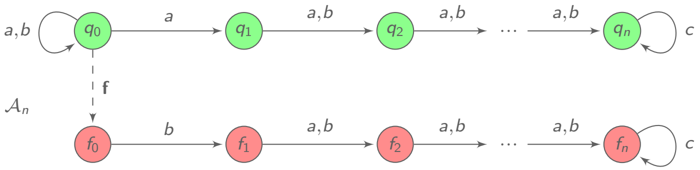
[JHCK01] Jiang, Huang, Chandra and Kumar, *A polynomial algorithm for testing diagnosability of discrete-event systems*, TAC, 2001.
[HHMS13] Haar, Haddad, Melliti and Schwoon, *Optimal constructions for active diagnosis*, FSTTCS'13.

# Diagnoser synthesis

**Complexity of diagnoser synthesis**
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.

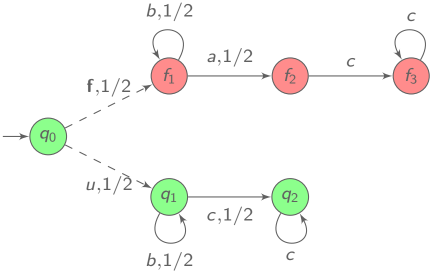



diagnoser must remember the last $n$ events: $2^n$ possibilities

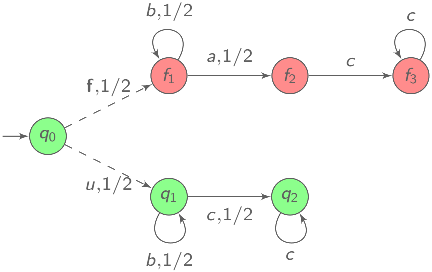

[JHCK01] Jiang, Huang, Chandra and Kumar, *A polynomial algorithm for testing diagnosability of discrete-event systems*, TAC, 2001.
[HHMS13] Haar, Haddad, Melliti and Schwoon, *Optimal constructions for active diagnosis*, FSTTCS'13.

# Outline

# Diagnosis of probabilistic systems

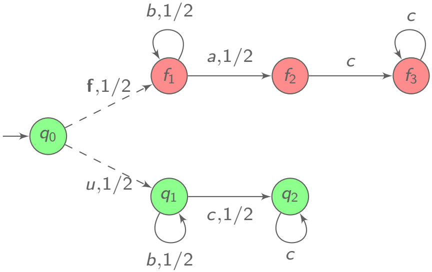


# Diagnosis of probabilistic systems




$b^N$ is ambiguous . . .

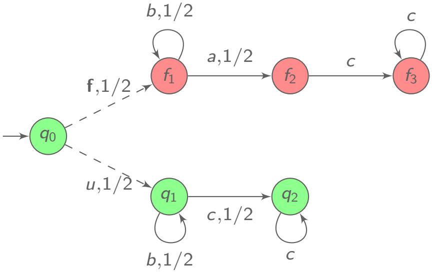
# Diagnosis of probabilistic systems




$b^N$ is ambiguous ...

yet $\lim_{N\to\infty} \mathbb{P}(\mathbf{f}b^N + ub^N) = 0$

# Diagnosis of probabilistic systems




$b^N$ is ambiguous ...

yet $\lim_{N\to\infty} \mathbb{P}(\mathbf{f}b^N + ub^N) = 0$

How to adapt the framework to probabilistic systems?

- diagnosability notion(s)
- soundness and correctness for diagnosers
- algorithms for diagnosability checking and diagnoser synthesis


[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.

# Outline

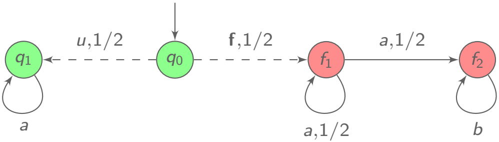
# Specifying diagnosability for probabilistic systems

Two discriminating criteria:

# Specifying diagnosability for probabilistic systems

Two discriminating criteria:

1. Detect faults, or tell whether a run is faulty or correct?



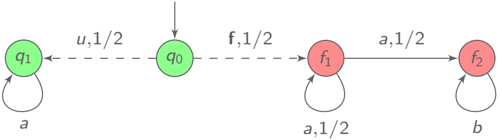

Fault is almost surely followed by occurrence of $b$.

Ambiguous sequences have probability $\frac{1}{2}$.

# Specifying diagnosability for probabilistic systems

Two discriminating criteria:

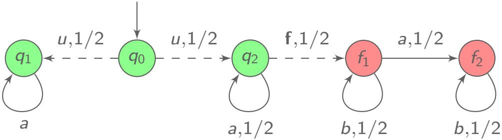
1. Detect faults, or tell whether a run is faulty or correct?




Fault is almost surely followed by occurrence of $b$.

Ambiguous sequences have probability $\frac{1}{2}$.

2. Consider infinite observed sequences or their finite prefixes?




Infinite sequence $a^\omega$ is surely correct.

For every $N$, $a^N$ is ambiguous, and has probability greater than $\frac{1}{2}$.

# Four diagnosability specifications

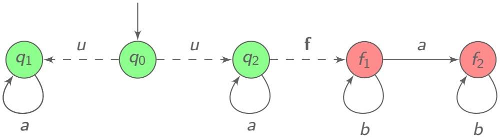
| Diagnosability | All runs | | Faulty runs |
|---|---|---|---|
| Finite prefixes | FA | $\Rightarrow$ $\not\Leftarrow$ | FF |
| | $\Downarrow$ $\not\Uparrow$ | | $\Downarrow\Uparrow^*$ |
| Infinite sequences | IA | $\Rightarrow$ $\not\Leftarrow$ | IF |

* assuming finitely-branching models

# Characterizing diagnosability

*e.g.* FA-diagnosability
disambiguation of All runs, relying on Finite observation sequences.

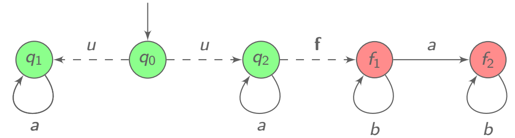
$\mathcal{A}$



# Characterizing diagnosability

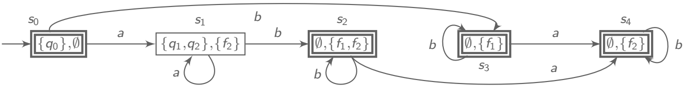
*e.g.* FA-diagnosability
disambiguation of All runs, relying on Finite observation sequences.

$\mathcal{A}$




Observer $\mathcal{O}_\mathcal{A}$: tracks possible correct and faulty states in two subsets

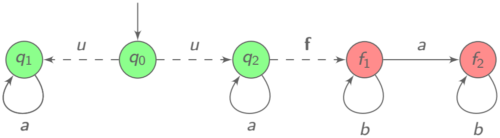
$\mathcal{O}_\mathcal{A}$



# Characterizing diagnosability

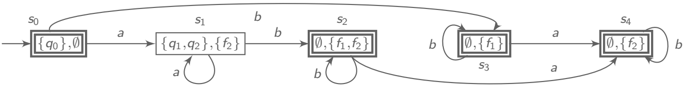
*e.g.* FA-diagnosability
disambiguation of All runs, relying on Finite observation sequences.

$\mathcal{A}$




Observer $\mathcal{O}_{\mathcal{A}}$: tracks possible correct and faulty states in two subsets

$\mathcal{O}_{\mathcal{A}}$




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

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

# Solving diagnosability

Methodology to decide all diagnosability notions for probabilistic systems:

- build a deterministic observer $\mathcal{O}_\mathcal{A}$ by an *ad hoc* subset construction
- form the product $\mathcal{A} \times \mathcal{O}_\mathcal{A}$ to recover probabilistic behaviour
- check graph-based characterization on $\mathcal{A} \times \mathcal{O}_\mathcal{A}$

# Solving diagnosability

Methodology to decide all diagnosability notions for probabilistic systems:

- build a deterministic observer $\mathcal{O}_{\mathcal{A}}$ by an *ad hoc* subset construction
- form the product $\mathcal{A} \times \mathcal{O}_{\mathcal{A}}$ to recover probabilistic behaviour
- check graph-based characterization on $\mathcal{A} \times \mathcal{O}_{\mathcal{A}}$

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) Upon verdict ✗, the observation sequence is surely faulty, 2) Upon verdict ✓, the observation sequence is surely correct.
- **Reactivity**: almost surely, the sequence of verdicts stabilizes to ✗ or ✓

# Diagnosers

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

Diagnoser requirements

- **Soundness**: 1) Upon verdict ✗, the observation sequence is surely faulty, 2) Upon verdict ✓, the observation sequence is surely correct.
- **Reactivity**: almost surely, the sequence of verdicts stabilizes to ✗ or ✓

**Diagnosability and diagnosers** [BHL14]

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

For every diagnosable system with $n$ 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 $D : \Sigma_o^* \to \{\checkmark, ✗, ?\}$

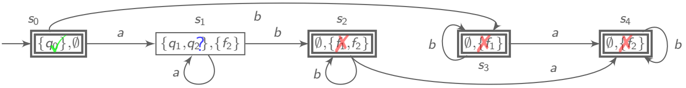
Diagnoser requirements

- **Soundness**: 1) Upon verdict ✗, the observation sequence is surely faulty, 2) Upon verdict ✓, the observation sequence is surely correct.
- **Reactivity**: almost surely, the sequence of verdicts stabilizes to ✗ or ✓

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

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

Diagnoser derived from observer $\mathcal{O}_\mathcal{A}$:




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

# Outline

Introduction to fault diagnosis

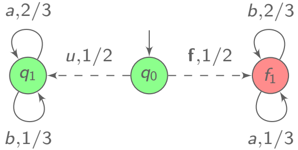
Diagnosability in probabilistic systems

- Exact Diagnosis
- Approximate diagnosis

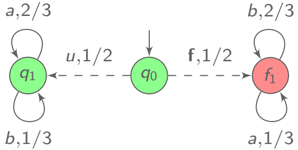
Control for probabilistic diagnosability

Conclusion

# Motivation for approximate diagnosis

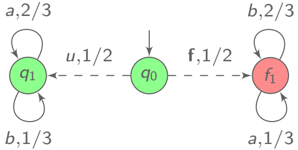


# Motivation for approximate diagnosis



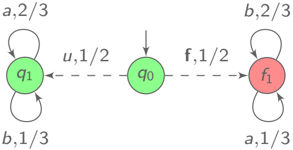

Not diagnosable: All observed sequences are ambiguous!

# Motivation for approximate diagnosis




Not diagnosable: All observed sequences are ambiguous!
Yet a high proportion of $b$'s indicates a faulty run with high confidence.

# Motivation for approximate diagnosis




Not diagnosable: All observed sequences are ambiguous!
Yet a high proportion of $b$'s indicates a faulty run with high confidence.

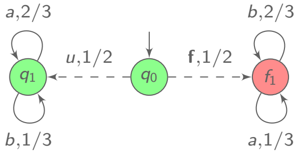
Relaxed soundness: if a fault is claimed, the probability of error is small.

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

# Formalisation of accurate approximate diagnosability

**Correcness proportion** of an observation sequence $\sigma$

$$\mathrm{CorP}(\sigma) = \frac{\mathbb{P}(\{\pi^{-1}(\sigma) \cap \mathsf{correct}\})}{\mathbb{P}(\{\pi^{-1}(\sigma)\})}$$

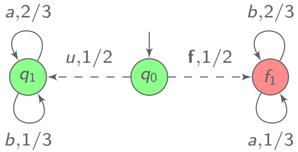



$\mathrm{CorP}(a) = 2/3$,

# Formalisation of accurate approximate diagnosability

**Correcness proportion** of an observation sequence $\sigma$

$$\mathrm{CorP}(\sigma) = \frac{\mathbb{P}(\{\pi^{-1}(\sigma) \cap \mathsf{correct}\})}{\mathbb{P}(\{\pi^{-1}(\sigma)\})}$$

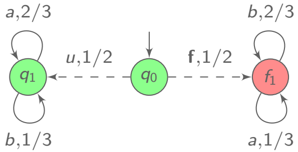



$\mathrm{CorP}(a) = 2/3$, $\mathrm{CorP}(ab) = 1/2$,

# Formalisation of accurate approximate diagnosability

**Correcness proportion** of an observation sequence $\sigma$

$$\mathrm{CorP}(\sigma) = \frac{\mathbb{P}(\{\pi^{-1}(\sigma) \cap \mathrm{correct}\})}{\mathbb{P}(\{\pi^{-1}(\sigma)\})}$$




$\mathrm{CorP}(a) = 2/3$, $\mathrm{CorP}(ab) = 1/2$, $\mathrm{CorP}(abb) = 1/3$, $\mathrm{CorP}(abbb) = 1/5$, ...

# Accurate approximate diagnosers

$\varepsilon$-Diagnoser requirements

- **Soundness**: if a fault is claimed after $\sigma$, then $\mathrm{CorP}(\sigma) \leq \varepsilon$.
- **Reactivity**: almost surely verdict ✗ is emitted after a fault.

# Accurate approximate diagnosers

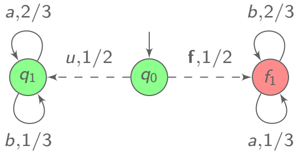
$\varepsilon$-Diagnoser requirements

- **Soundness**: if a fault is claimed after $\sigma$, then $\mathsf{CorP}(\sigma) \leq \varepsilon$.
- **Reactivity**: almost surely verdict ✗ is emitted after a fault.
- **Uniformity** (optional): the convergence rate for reactivity is independent of the sample faulty run.

# Accurate approximate diagnosers

$\varepsilon$-Diagnoser requirements

- **Soundness**: if a fault is claimed after $\sigma$, then $\text{CorP}(\sigma) \leq \varepsilon$.
- **Reactivity**: almost surely verdict ✗ is emitted after a fault.
- **Uniformity** (optional): the convergence rate for reactivity is independent of the sample faulty run.




admits $\varepsilon$-diagnoser, for every $\varepsilon > 0$
has no uniform $\varepsilon$-diagnoser, for any $\varepsilon > 0$

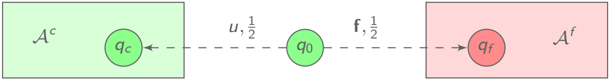
# Solving (uniform) accurate approximate diagnosability

Accurate approximate diagnosability is decidable in PTIME. [BHL16]

# Solving (uniform) accurate approximate diagnosability

Accurate approximate diagnosability is decidable in PTIME. [BHL16]

- Simple case: initial-fault models

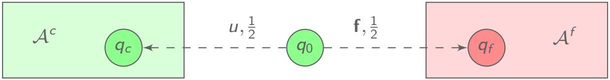



$\mathcal{A}$ is accurate approximate diagnosable iff $\text{dist}(\mathcal{A}^c, \mathcal{A}^f) = 1$
*i.e.* there exists an event $E \subseteq \Sigma_o^\omega$ s.t. $|\mathbb{P}_{\mathcal{A}^c}(E) - \mathbb{P}_{\mathcal{A}^c}(E)| = 1$

# Solving (uniform) accurate approximate diagnosability

Accurate approximate diagnosability is decidable in PTIME. [BHL16]

- Simple case: initial-fault models



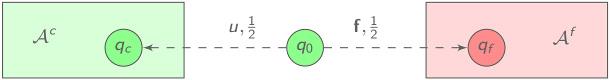

  $\mathcal{A}$ is accurate approximate diagnosable iff $\text{dist}(\mathcal{A}^c, \mathcal{A}^f) = 1$
  *i.e.* there exists an event $E \subseteq \Sigma_o^\omega$ s.t. $|\mathbb{P}_{\mathcal{A}^c}(E) - \mathbb{P}_{\mathcal{A}^c}(E)| = 1$

- General case: polynomially many distance 1 tests.

# Solving (uniform) accurate approximate diagnosability

Accurate approximate diagnosability is decidable in PTIME. [BHL16]

- Simple case: initial-fault models



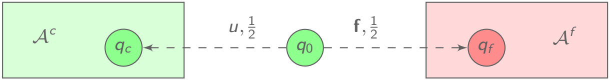

$\mathcal{A}$ is accurate approximate diagnosable iff $\text{dist}(\mathcal{A}^c, \mathcal{A}^f) = 1$
*i.e.* there exists an event $E \subseteq \Sigma_o^\omega$ s.t. $|\mathbb{P}_{\mathcal{A}^c}(E) - \mathbb{P}_{\mathcal{A}^c}(E)| = 1$

- General case: polynomially many distance 1 tests.
- Distance 1 is decidable in PTIME. [CK14]

# Solving (uniform) accurate approximate diagnosability

Accurate approximate diagnosability is decidable in PTIME. [BHL16]

- Simple case: initial-fault models




$\mathcal{A}$ is accurate approximate diagnosable iff $\text{dist}(\mathcal{A}^c, \mathcal{A}^f) = 1$
*i.e.* there exists an event $E \subseteq \Sigma_o^\omega$ s.t. $|\mathbb{P}_{\mathcal{A}^c}(E) - \mathbb{P}_{\mathcal{A}^c}(E)| = 1$

- General case: polynomially many distance 1 tests.
- Distance 1 is decidable in PTIME. [CK14]

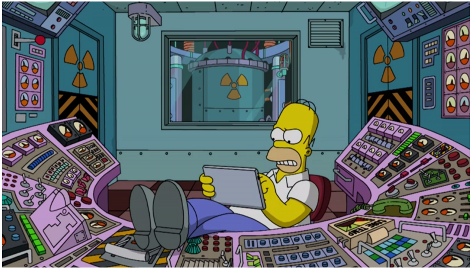
Uniform accurate approximate diagnosability is undecidable. [BHL16]

[CK14] Chen and Kiefer, *On the Total Variation Distance of Labelled Markov Chains*, CSL-LICS'14.
[BHL16] **B.**, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA'16.

# Outline

# From passive to active diagnosis

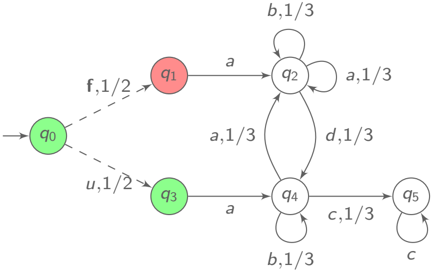
# From passive to active diagnosis



Original idea by Stefan Schwoon

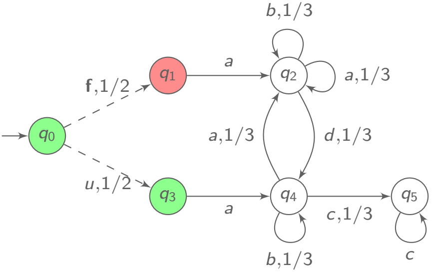
# Active probabilistic diagnosis

**Objective**: control the probabilistic system so that it is diagnosable



# Active probabilistic diagnosis

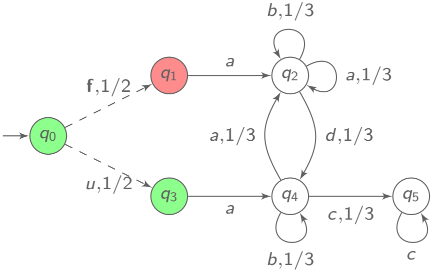
**Objective**: control the probabilistic system so that it is diagnosable




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

# Active probabilistic diagnosis

**Objective**: control the probabilistic system so that it is diagnosable

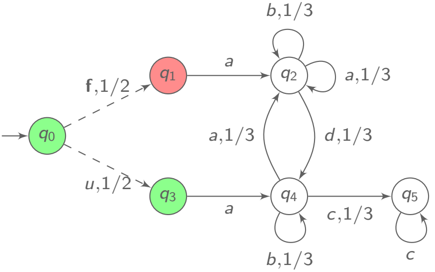



$aadc^\omega$ ambiguous
$\mathbb{P}(\mathbf{f}aadc^\omega + uaadc^\omega) > 0$

$\{a, b, c, d\}$ controllable

# Active probabilistic diagnosis

**Objective**: control the probabilistic system so that it is diagnosable

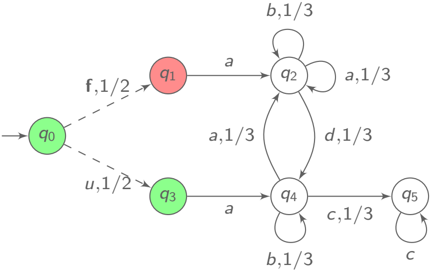



$aadc^\omega$ ambiguous
$\mathbb{P}(\mathbf{f}aadc^\omega + uaadc^\omega) > 0$

$\{a, b, c, d\}$ controllable
disable $a$ after first $a$

# Active probabilistic diagnosis

**Objective**: control the probabilistic system so that it is diagnosable




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

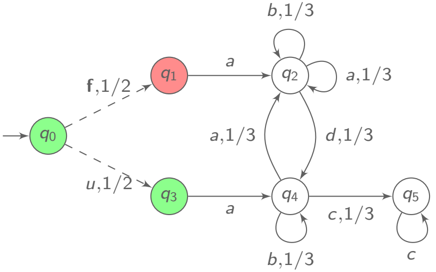
$\{a, b, c, d\}$ controllable
disable $a$ after first $a$

**Controller**: based on observation, decides which actions are allowed

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

# Active probabilistic diagnosis

**Objective**: control the probabilistic system so that it is diagnosable




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

$\{a, b, c, d\}$ controllable
disable $a$ after first $a$

**Controller**: based on observation, decides which actions are allowed

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

The active probabilistic diagnosis problem is EXPTIME-complete.

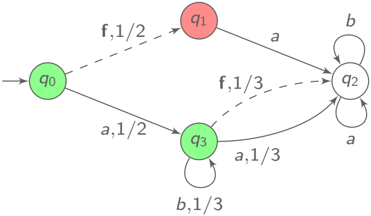
[BFHHH14] **B.**, Fabre, Haar, Haddad and Hélouët, *Active diagnosis for probabilistic systems*, FoSSaCS'14.

# Safe active probabilistic diagnosis

**Objective**: avoid fault-provocative controllers

# Safe active probabilistic diagnosis

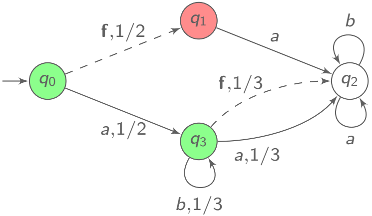
**Objective**: avoid fault-provocative controllers




all observed sequences ambiguous

# Safe active probabilistic diagnosis

**Objective**: avoid fault-provocative controllers

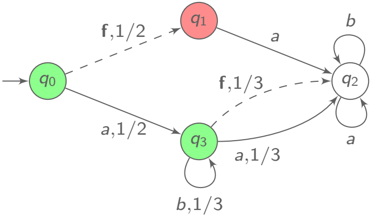



all observed sequences ambiguous

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

# Safe active probabilistic diagnosis

**Objective**: avoid fault-provocative controllers



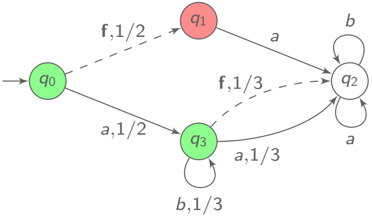

all observed sequences ambiguous

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?

# Safe active probabilistic diagnosis

**Objective**: avoid fault-provocative controllers




all observed sequences ambiguous

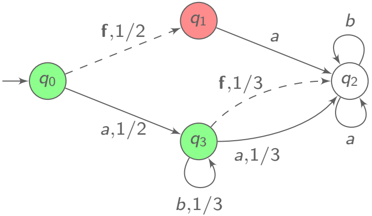
forbid *a* after first *a*
$\Longrightarrow$ diagnosable...
but almost all sequences faulty!

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

The safe active probabilistic diagnosis problem is undecidable.

# 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?

The safe active probabilistic diagnosis problem is undecidable.

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

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

# Outline

Introduction to fault diagnosis

Diagnosability in probabilistic systems
- Exact Diagnosis
- Approximate diagnosis

Control for probabilistic diagnosability

Conclusion

# Concluding remarks

Contributions: Foundations of stochastic diagnosis

- Investigation of semantical issues
- Exact diagnosis: tight complexity bounds for diagnosability and diagnoser synthesis problems
- Accurate approximate diagnosis: PTIME algorithm
- Active diagnosability

# Concluding remarks

Contributions: Foundations of stochastic diagnosis

- Investigation of semantical issues
- Exact diagnosis: tight complexity bounds for diagnosability and diagnoser synthesis problems
- Accurate approximate diagnosis: PTIME algorithm
- Active diagnosability

Perspectives: Towards more quantitative questions

- Bounded-delay diagnosis
  tradeoff: delay *vs* diagnosability precision
- Space and time optimisation of observations
  tradeoff: observation cost *vs* diagnosability probability
- Challenge: control, partial observation, quantitative properties