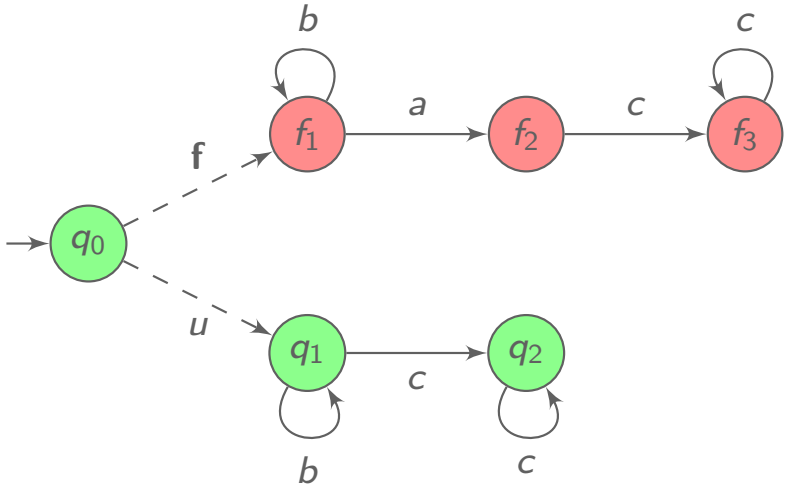
Foundation of Diagnosis and Predictability in Probabilistic Systems

Nathalie Bertrand[1], Serge Haddad[2], Engel Lefaucheux[1,2]

1 Inria Rennes, France
2 LSV, ENS Cachan & CNRS & Inria Saclay, France

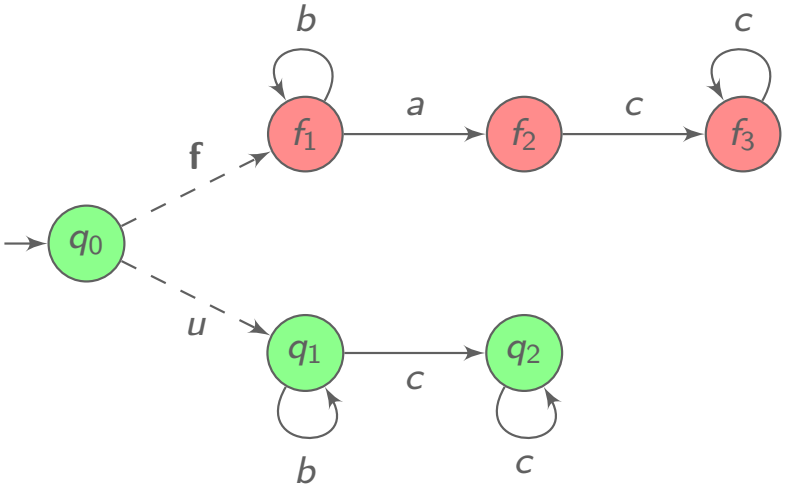
Diagnosis of discrete event systems

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



Diagnosis of discrete event systems

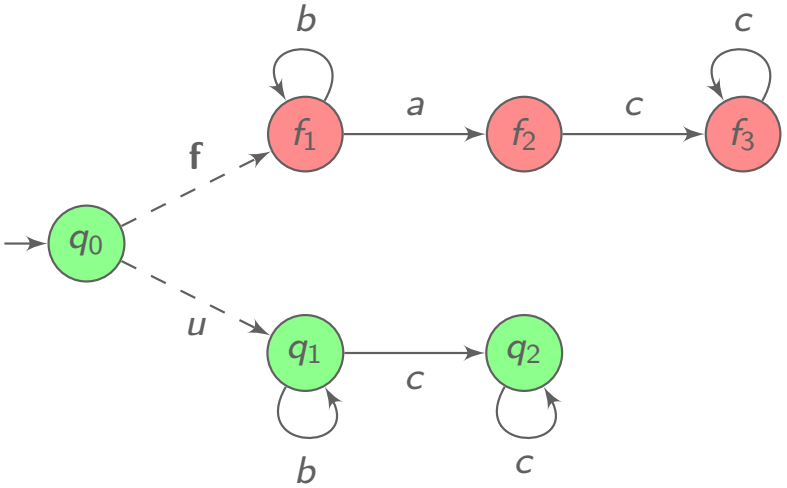
Objective: tell whether a fault **f** occurred, based on observations.



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

Diagnosis of discrete event systems

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

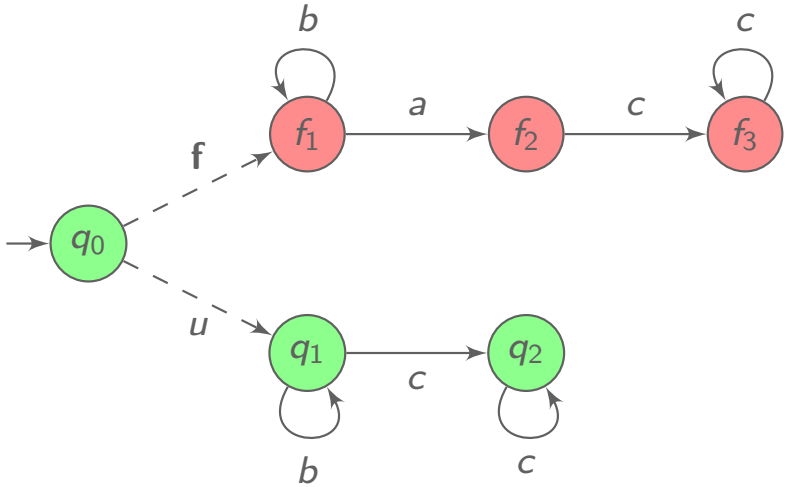


c^+	✓	correct
ac^+	✗	faulty
b^+	?	ambiguous

Diagnosability: all observed sequences are unambiguous.

Diagnosis of discrete event systems

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



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

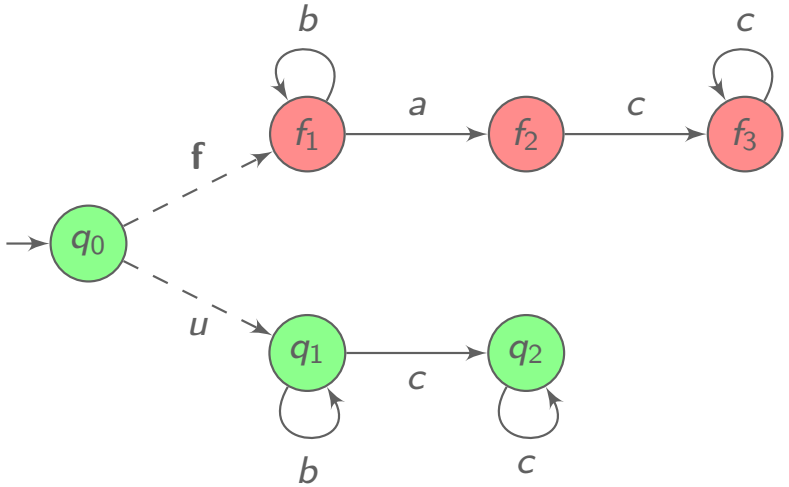
Diagnosability: all observed sequences are unambiguous.

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

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

Diagnosis of discrete event systems

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



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

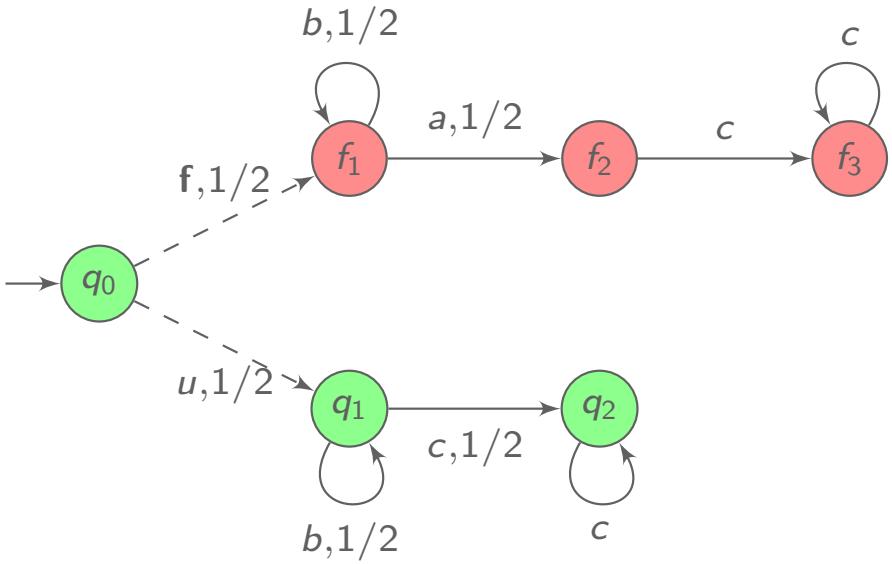
Diagnosability: all observed sequences are unambiguous.

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

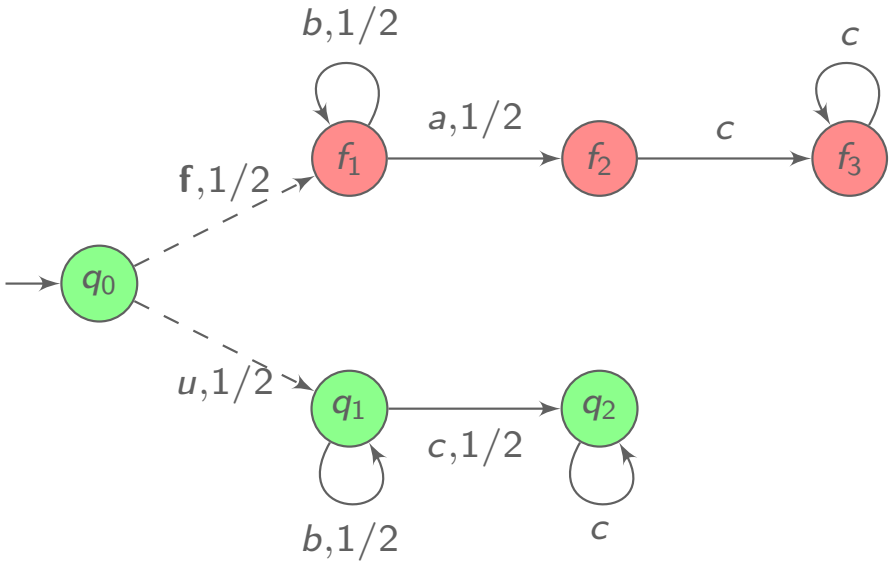
- **Soundness**: if a fault is claimed, a fault occurred.
- **Reactivity**: every fault will be detected.

Diagnosability and diagnoser synthesis in PTIME [Jiang et al. TAC 2001]

Diagnosis of probabilistic systems

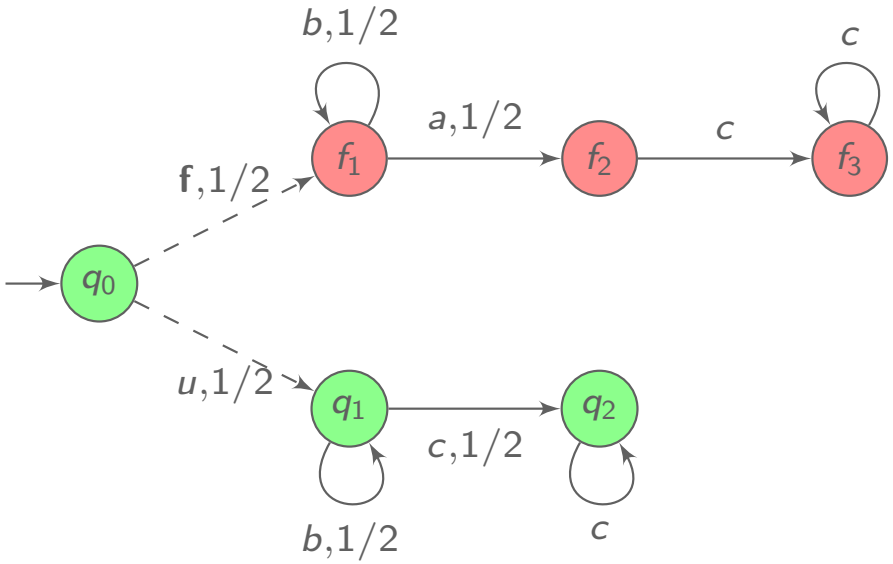


Diagnosis of probabilistic systems



b^+ ambiguous but...

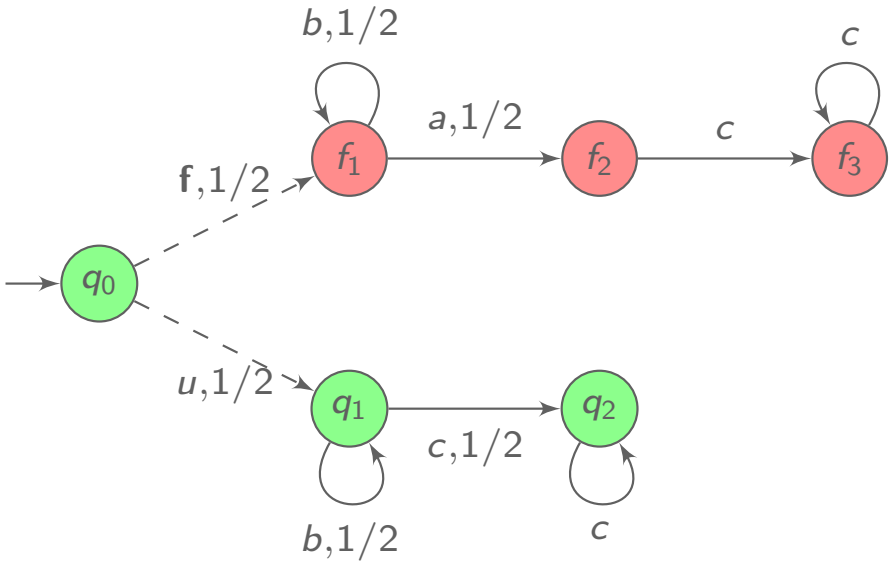
Diagnosis of probabilistic systems



b^+ ambiguous but...

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

Diagnosis of probabilistic systems



b^+ ambiguous but...

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

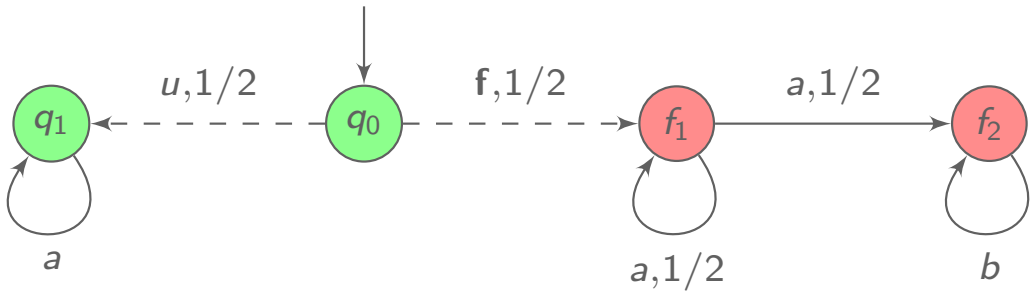
Our contribution

- Relevant soundness and reactivity criteria in probabilistic setting
- Decidability and complexity of diagnosability
- Optimal diagnoser construction
- Beyond diagnosis: predictability and prediagnosis

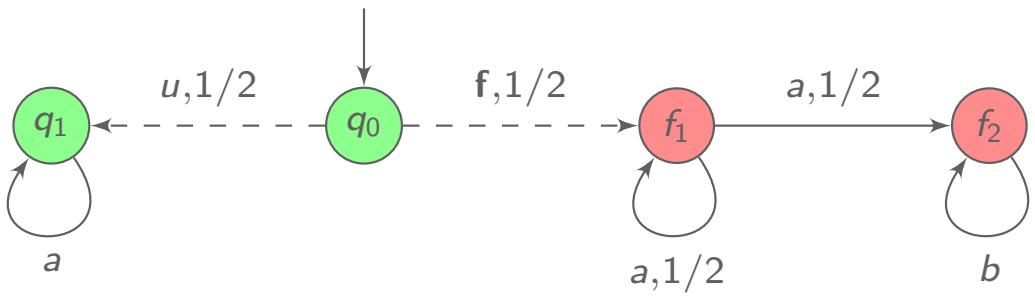
Outline

Outline

All runs or faulty runs?

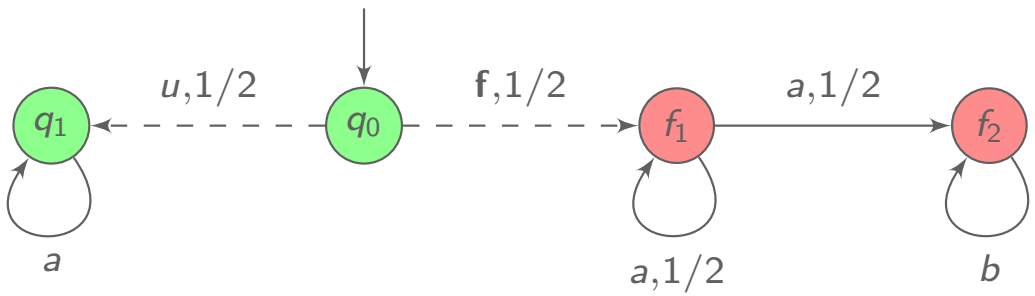


All runs or faulty runs?



a^+ is ambiguous

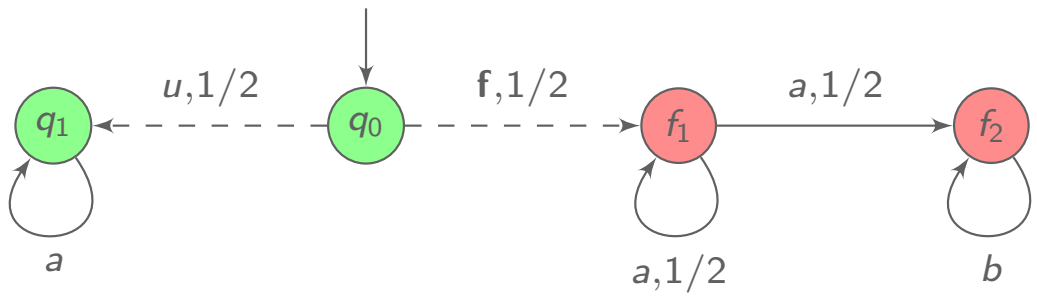
All runs or faulty runs?



a^+ is ambiguous

$$\lim_{n\to\infty} \mathbb{P}(\mathbf{f}a^n) = 0$$

All runs or faulty runs?

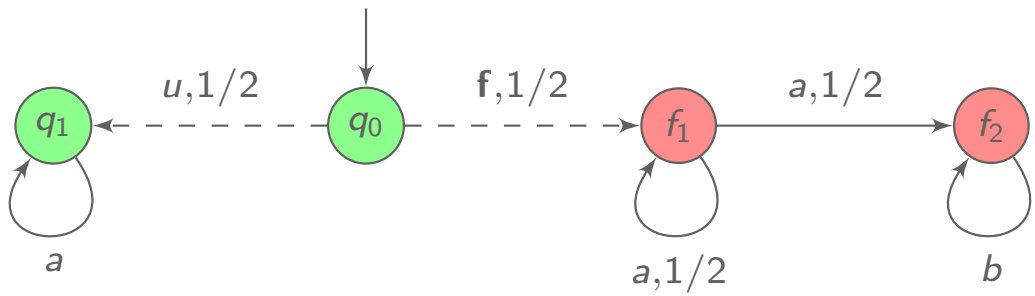


a^+ is ambiguous

$$\lim_{n\to\infty} \mathbb{P}(\mathbf{f}a^n) = 0$$

$$\lim_{n\to\infty} \mathbb{P}(ua^n) = \frac{1}{2}$$

All runs or faulty runs?



a^+ is ambiguous

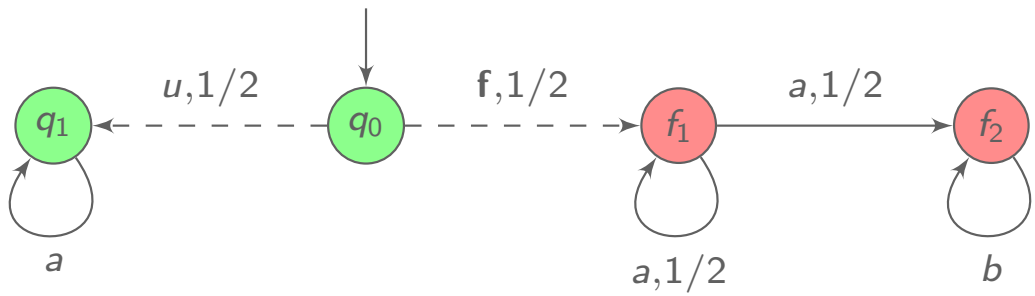
$$\lim_{n\to\infty} \mathbb{P}(\mathbf{f}a^n) = 0$$

$$\lim_{n\to\infty} \mathbb{P}(ua^n) = \frac{1}{2}$$

Reactivity specifications:

- Detect a fault, almost surely.

All runs or faulty runs?



a^+ is ambiguous

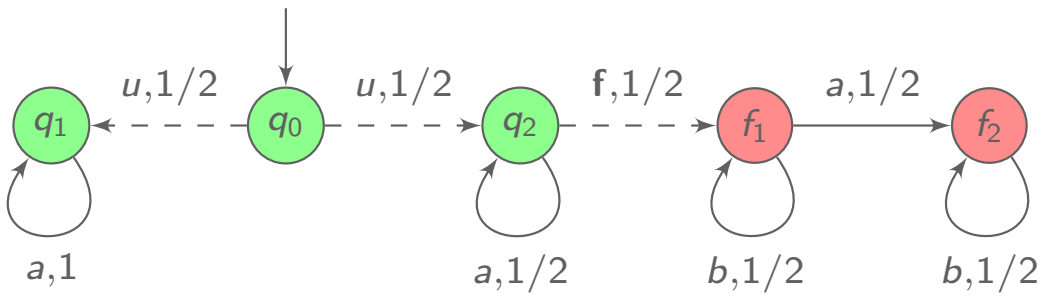
$$\lim_{n\to\infty} \mathbb{P}(\mathbf{f}a^n) = 0$$

$$\lim_{n\to\infty} \mathbb{P}(ua^n) = \frac{1}{2}$$

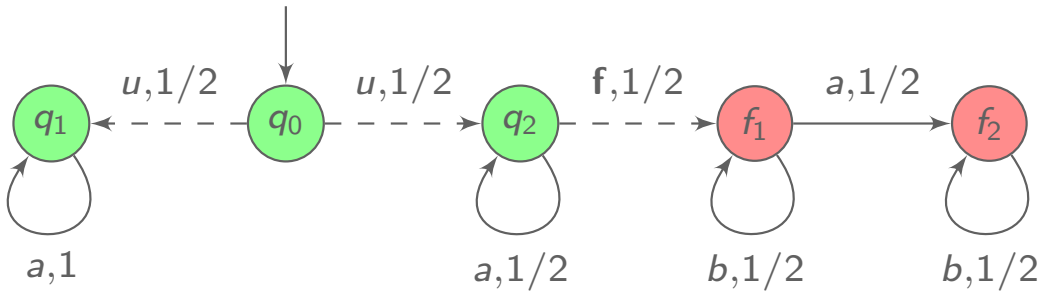
Reactivity specifications:

- Detect a fault, almost surely.
- Detect if a run is faulty or correct, almost surely.

Infinite sequences or their finite prefixes?

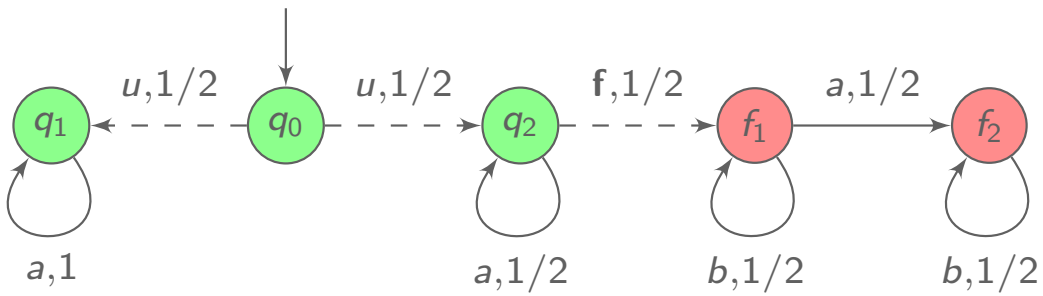


Infinite sequences or their finite prefixes?



a^ω is correct.

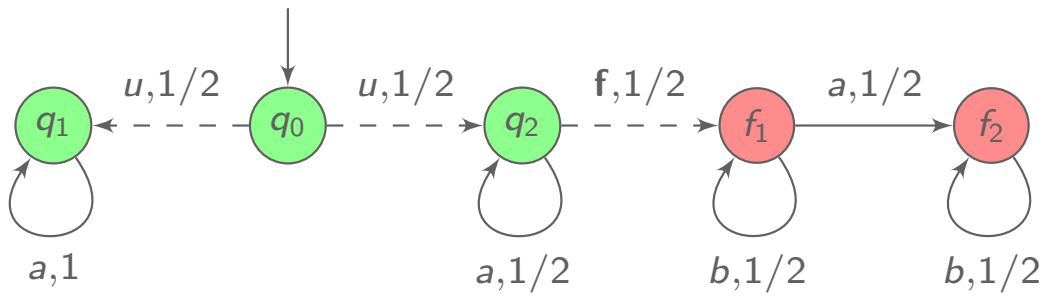
Infinite sequences or their finite prefixes?



a^ω is correct.

a^n is ambiguous and $\mathbb{P}(q_0 u (q_1 a)^n) = \frac{1}{2}$.

Infinite sequences or their finite prefixes?

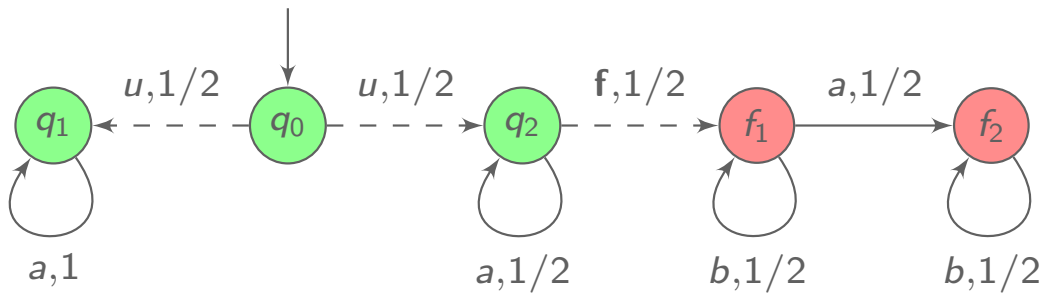


a^ω is correct.

a^n is ambiguous and $\mathbb{P}(q_0 u (q_1 a)^n) = \frac{1}{2}$.

- Infinite sequences are almost surely non ambiguous.

Infinite sequences or their finite prefixes?



a^ω is correct.

a^n is ambiguous and $\mathbb{P}(q_0 u (q_1 a)^n) = \frac{1}{2}$.

- Infinite sequences are almost surely non ambiguous.
- The probability of ambiguous prefixes tends to 0.

Four diagnosability notions

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

Four diagnosability notions

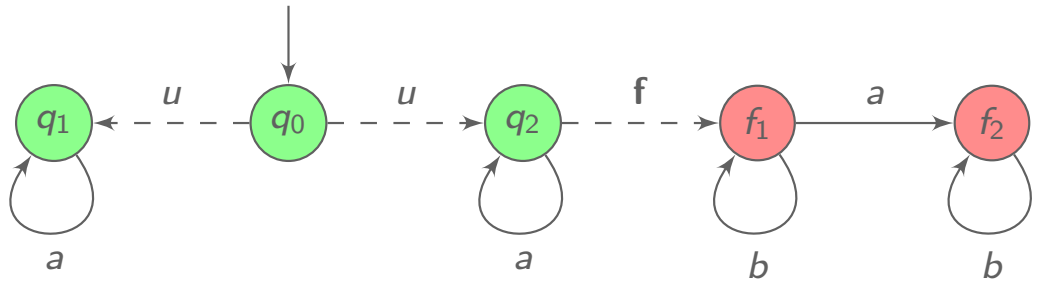
Diagnosability	All runs		Faulty runs
Finite prefixes	FA	$\Rightarrow$ $\not\Leftarrow$	FF
	$\Downarrow\not\Uparrow$		$\Downarrow\Uparrow$
Infinite sequences	IA	$\Rightarrow$ $\not\Leftarrow$	IF

Focus on IF in this talk.

Characterisation of diagnosability

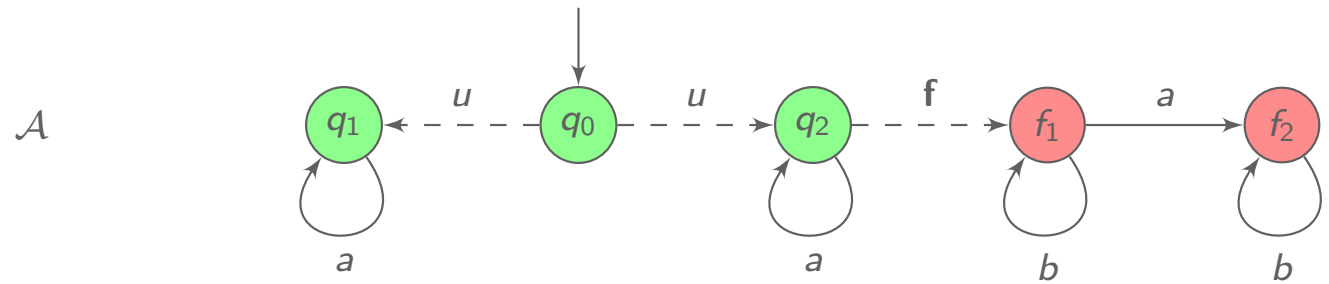
Specification of IF-diagnosability: Infinite sequences, Fault diagnosis

$\mathcal{A}$

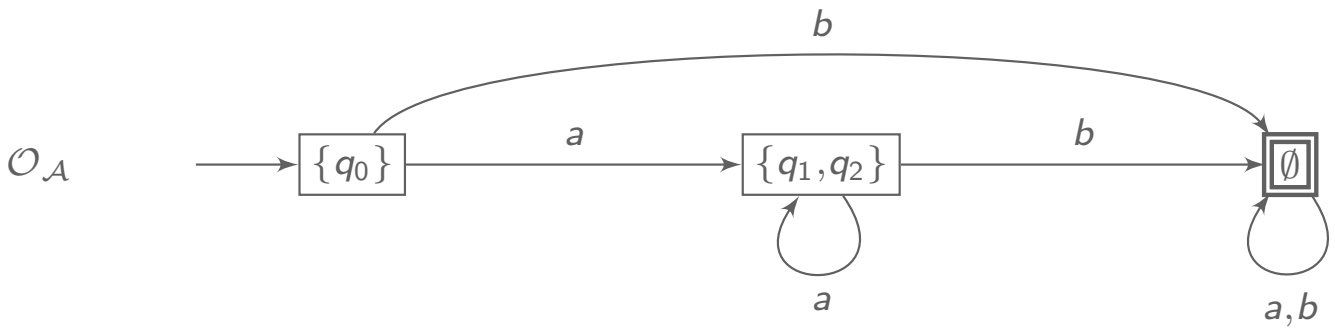


Characterisation of diagnosability

Specification of IF-diagnosability: Infinite sequences, Fault diagnosis

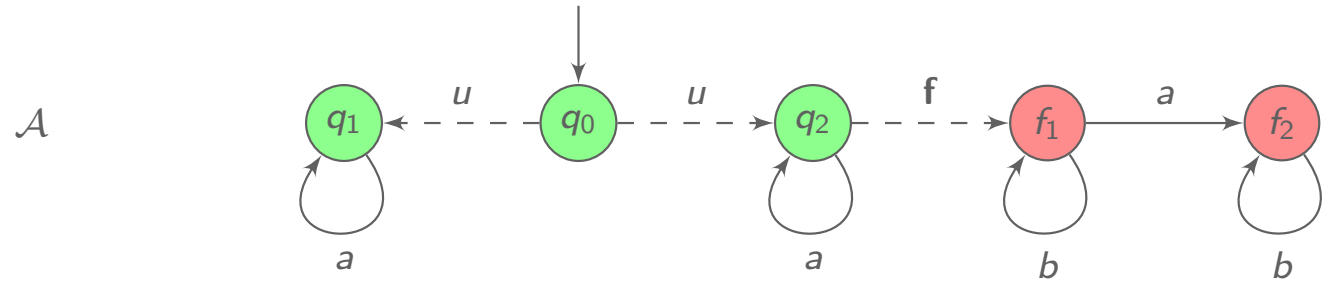


Observer: tracks possible correct states after given observed sequence.

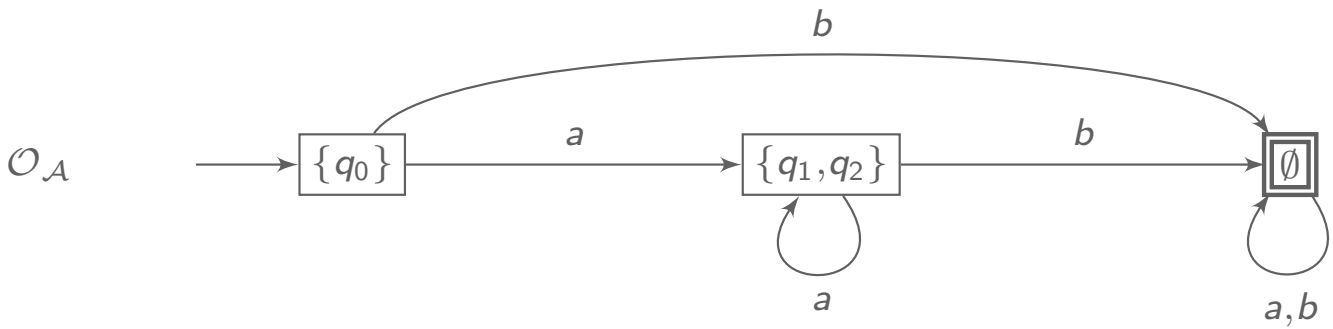


Characterisation of diagnosability

Specification of IF-diagnosability: Infinite sequences, Fault diagnosis



Observer: tracks possible correct states after given observed sequence.



$\mathcal{A}$ is not IF-diagnosable
iff
there exists a state (q, U) in a BSCC of $\mathcal{A} \times \mathcal{O}_{\mathcal{A}}$ with q faulty and $U \neq \emptyset$.

Diagnoser synthesis

For every IF-diagnosable system with n correct states
one can build an IF-diagnoser with at most 2^n states.

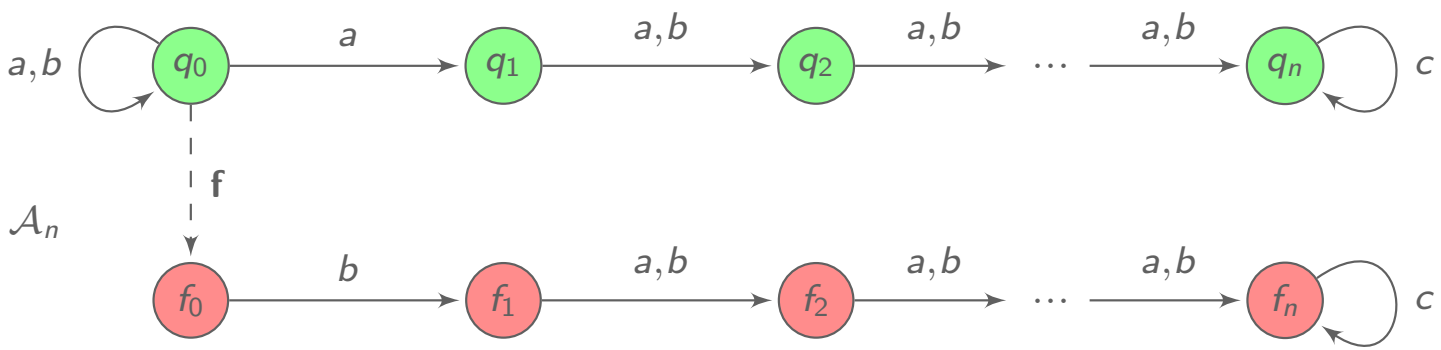
Diagnoser derived from observer $\mathcal{O}_{\mathcal{A}}$: emits ✗ in state $\emptyset$.

Diagnoser synthesis

For every IF-diagnosable system with n correct states
one can build an IF-diagnoser with at most 2^n states.

Diagnoser derived from observer $\mathcal{O}_{\mathcal{A}}$: emits ✗ in state $\emptyset$.

There is a family $(\mathcal{A}_n)$ of IF-diagnosable systems such that
$\mathcal{A}_n$ has $n+1$ correct states and any IF-diagnoser needs 2^n states.



Diagnosability is in PSPACE

Diagnosability is decidable in PSPACE for probabilistic systems.

Diagnosability is in PSPACE

Diagnosability is decidable in PSPACE for probabilistic systems.

Sketch of proof

- relies on the characterisation on $\mathcal{A} \times \mathcal{O}_{\mathcal{A}}$
- avoids building the product
- uses Savitch's theorem for appropriate guesses

Diagnosability is PSPACE-hard

$\mathcal{L} \subseteq \Sigma^*$ is *eventually universal* if $\exists v \in \Sigma^*, v^{-1}\mathcal{L} = \Sigma^*$.

The eventual universality problem for NFA is PSPACE-hard.

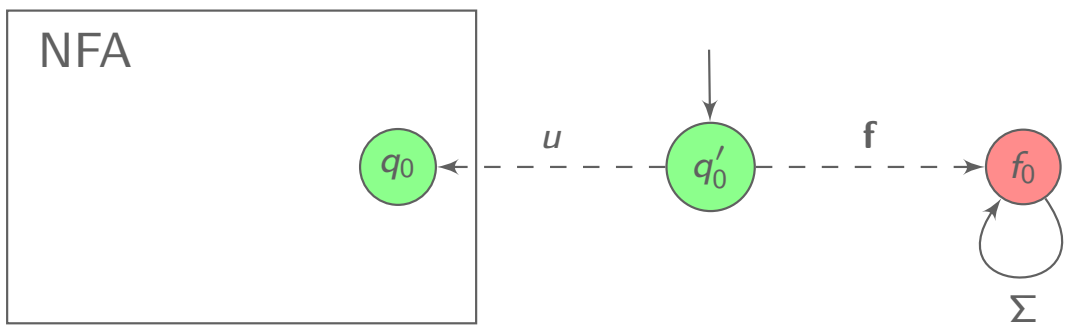
Diagnosability is PSPACE-hard

$\mathcal{L} \subseteq \Sigma^*$ is *eventually universal* if $\exists v \in \Sigma^*, v^{-1}\mathcal{L} = \Sigma^*$.

The eventual universality problem for NFA is PSPACE-hard.

Diagnosability is PSPACE-hard.

Reduction from eventual universality to diagnosability.



$\mathcal{A}$ not diagnosable iff
$\mathcal{A} \times \mathcal{O}_{\mathcal{A}}$ contains a BSCC where each state has the form (f_0, U) with $U \neq \emptyset$

Comparison with non-probabilistic discrete event systems

Diagnosability is PSPACE-complete for probabilistic systems.

Comparison with non-probabilistic discrete event systems

Diagnosability is PSPACE-complete for probabilistic systems.

Diagnosability is decidable in PTIME for non-probabilistic systems.
[Jiang, Huang, Chandra, Kumar TAC 2001]

Sketch of proof

- build the twin-product with a copy restricted to correct states
- check for SCC with faulty states in the first component

Comparison with non-probabilistic discrete event systems

Diagnosability is PSPACE-complete for probabilistic systems.

Diagnosability is decidable in PTIME for non-probabilistic systems.
[Jiang, Huang, Chandra, Kumar TAC 2001]

Sketch of proof

- build the twin-product with a copy restricted to correct states
- check for SCC with faulty states in the first component

Erroneous adaptation to probabilistic case in [Chen, Kumar TASE 2013].

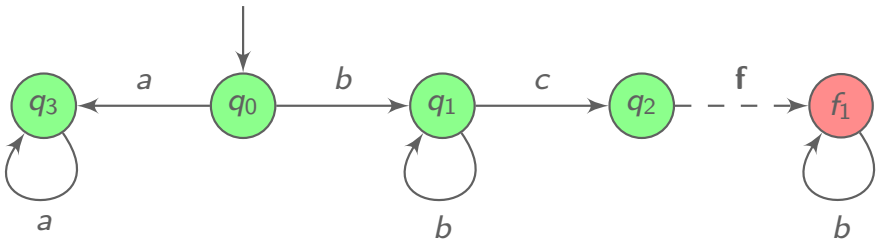
Outline

Predictability

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

Predictability

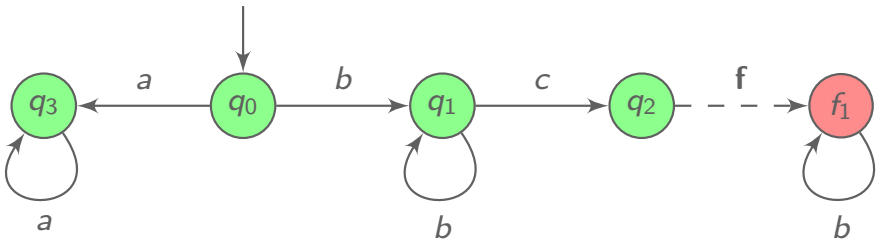
Objective: tell whether a fault *will* occur, based on observations.



a^+	✓	correct
b^+c	✗	surely eventually faulty
b^+	✗	a.s. eventually faulty

Predictability

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



a^+	✓	correct
b^+c	✗	surely eventually faulty
b^+	✗	a.s. eventually faulty

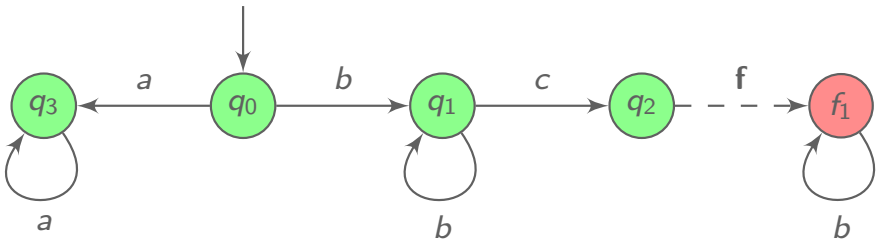
Two notions of **soundness**:

- sure: if a fault is claimed, a fault will occur
- almost-sure: if a fault is claimed, a fault will almost-surely occur

Reactivity: a fault is detected at least k steps before occurrence.

Predictability

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



a^+	✓	correct
b^+c	✗	surely eventually faulty
b^+	✗	a.s. eventually faulty

surely 0-predictable almost surely 1-predictable not 2-predictable

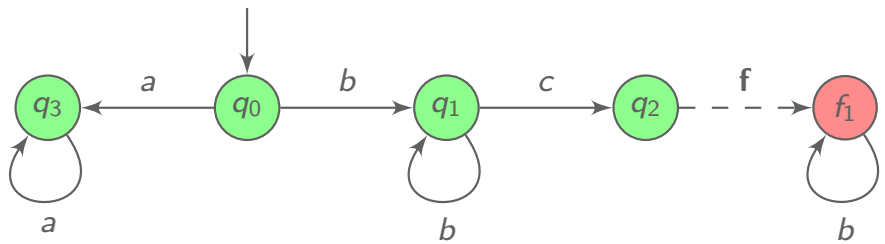
Two notions of **soundness**:

- sure: if a fault is claimed, a fault will occur
- almost-sure: if a fault is claimed, a fault will almost-surely occur

Reactivity: a fault is detected at least k steps before occurrence.

Predictability

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



a^+	✓	correct
b^+c	✗	surely eventually faulty
b^+	✗	a.s. eventually faulty

surely 0-predictable almost surely 1-predictable not 2-predictable

Two notions of **soundness**:

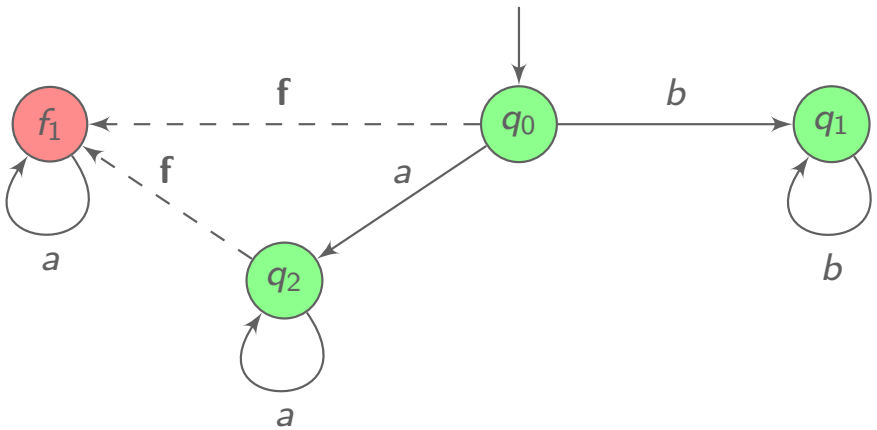
- sure: if a fault is claimed, a fault will occur
- almost-sure: if a fault is claimed, a fault will almost-surely occur

Reactivity: a fault is detected at least k steps before occurrence.

Predictability is NLOGSPACE-complete for probabilistic systems.

Prediagnosability

Objective: detect and foresee faults analysing past and future

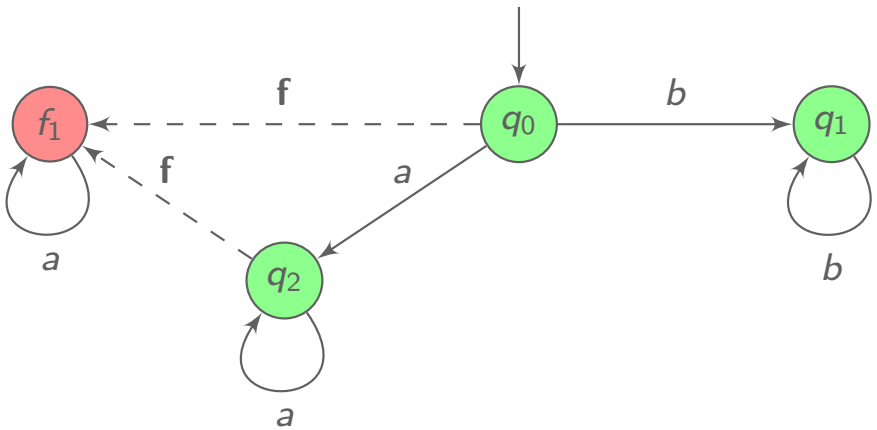


b^+ ✓ correct

a^+ ✗ a.s. eventually faulty

Prediagnosability

Objective: detect and foresee faults analysing past and future



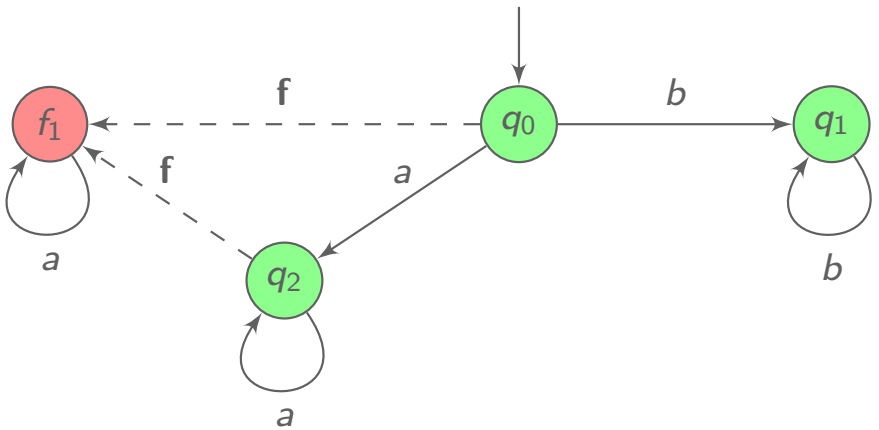
b^+ ✓ correct

a^+ ✗ a.s. eventually faulty

Soundness: If a fault is claimed, a fault happened or (almost) surely will.
Reactivity: Faults are almost surely claimed.

Prediagnosability

Objective: detect and foresee faults analysing past and future



b^+ ✓ correct

a^+ ✗ a.s. eventually faulty

Soundness: If a fault is claimed, a fault happened or (almost) surely will.
Reactivity: Faults are almost surely claimed.

Prediagnosability is PSPACE-complete.

Conclusion: Foundation of probabilistic diagnosis

Summary of contributions

- Investigation of semantical issues
- Tight complexity bounds for diagnosability and diagnoser synthesis problems
- Introduction of prediagnosability

Conclusion: Foundation of probabilistic diagnosis

Summary of contributions

- Investigation of semantical issues
- Tight complexity bounds for diagnosability and diagnoser synthesis problems
- Introduction of prediagnosability

Future work

- Approximate diagnosis (relaxing soundness)
- Other paradigms related to partial observation (detectability, opacity, etc.)
- Space and time optimisation of observations