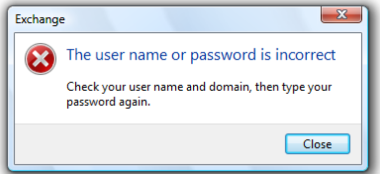
Controlling information in probabilistic systems
The case of fault diagnosis

PhD defence of Engel Lefaucheux

Supervisors: Nathalie Bertrand and Serge Haddad

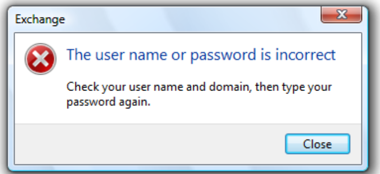
Septembre 24th 2018 – IRISA/LSV/Inria Rennes

Systems give information



Information disclosure

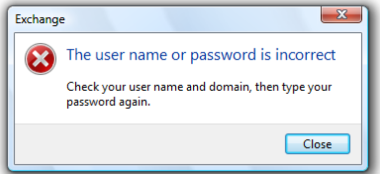
Systems give information



- Disclose useful information to the user

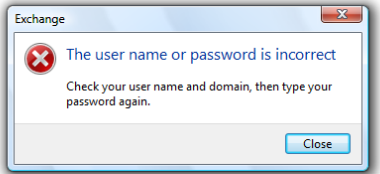
Information disclosure

Systems give information



- Disclose useful information to the user
- Disclose secret information to an attacker

Systems give information



- Disclose useful information to the user
- Disclose secret information to an attacker

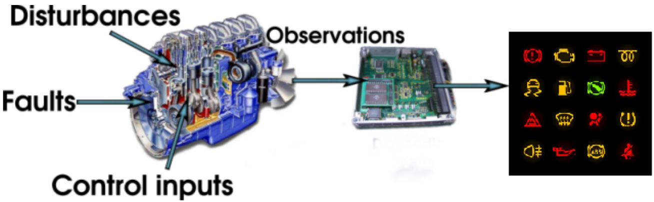
Analysing and controlling the revealed information is crucial

Fault diagnosis

Detecting faulty behaviours

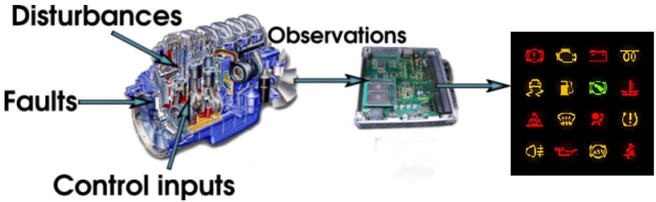
Fault diagnosis

Detecting faulty behaviours



Fault diagnosis

Detecting faulty behaviours



Diagnoser: must emit a verdict when faults occur, based on observations

Features of a diagnoser

Verdict: information provided

Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Features of a diagnoser

Verdict: information provided

Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Diagnosability: does there exist a diagnoser?

Features of a diagnoser

Verdict: information provided

Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Diagnosability: does there exist a diagnoser?
Synthesis: how to build a diagnoser?

Why diagnosis?

Faults and/or failures are unavoidable for some systems

- Components have a finite lifetime
- Reactive systems suffer from unpredictable behaviours of the environment

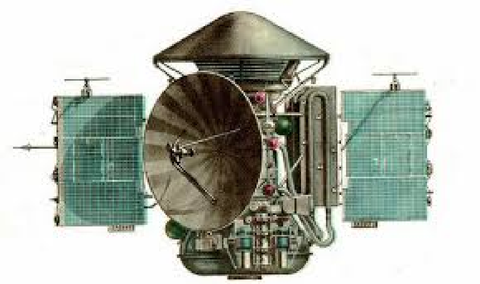
Why diagnosis?

Faults and/or failures are unavoidable for some systems

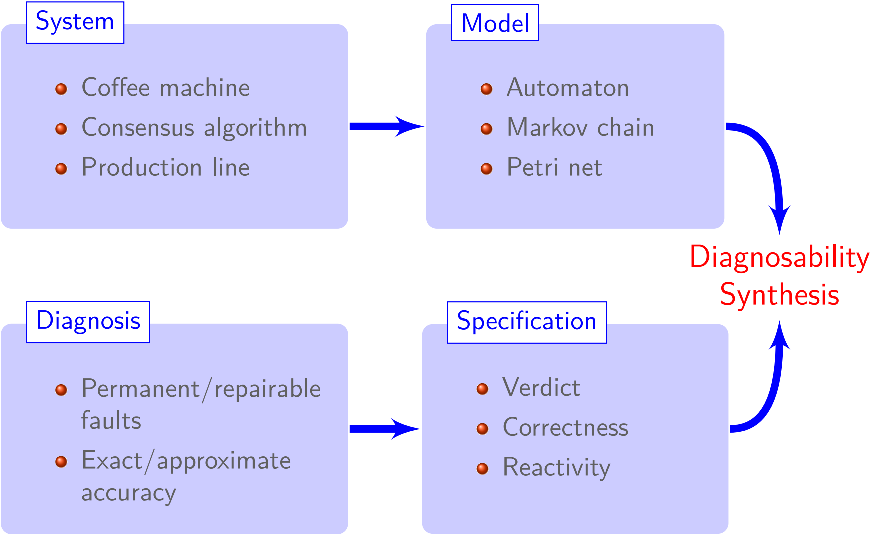
- Components have a finite lifetime
- Reactive systems suffer from unpredictable behaviours of the environment

Consequences of unhandled faults may be critical

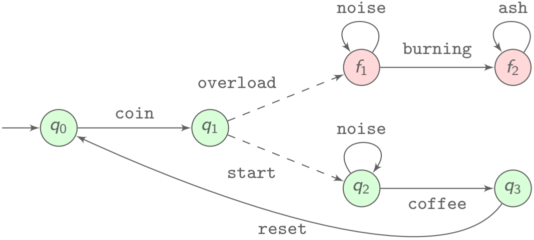
- Financial losses
- Human casualties



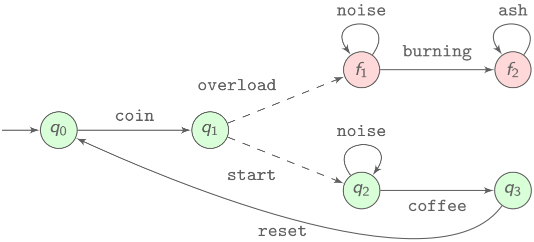
The model-based approach



A model for the coffee machine

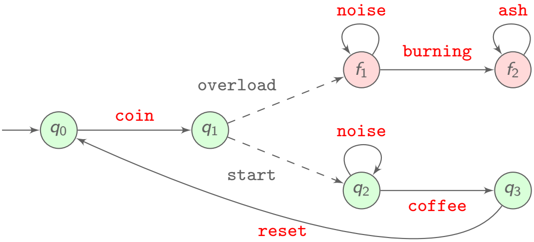


A model for the coffee machine



Partial observation

A model for the coffee machine

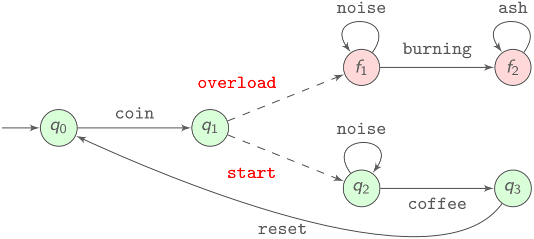


Partial observation

Observable events

$\rightarrow$

A model for the coffee machine

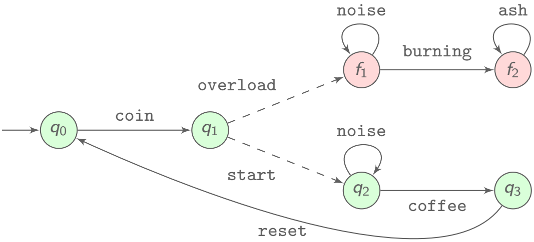


Partial observation

Observable events/unobservable events

$\longrightarrow$ / $\dashrightarrow$

A model for the coffee machine



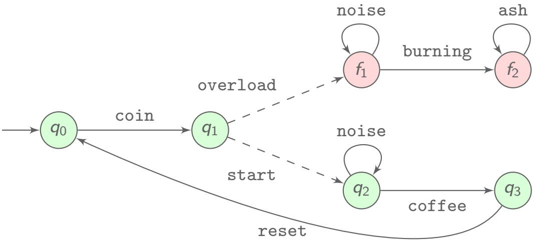
Partial observation

Observable events/unobservable events

$\rightarrow$ / $\dashrightarrow$

Run: $q_0 \xrightarrow{\texttt{coin}} q_1 \overset{\texttt{start}}{\dashrightarrow} q_2 \xrightarrow{\texttt{noise}} q_2$ | *Observation:* `coin noise`

A model for the coffee machine



Partial observation

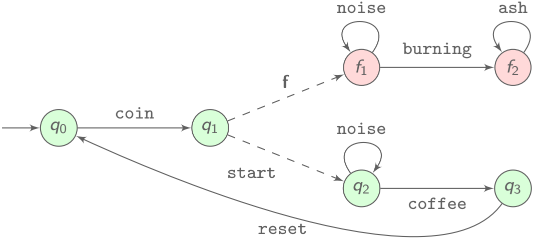
Observable events/unobservable events

$\rightarrow$ / $\dashrightarrow$

Run: $q_0 \xrightarrow{\texttt{coin}} q_1 \overset{\texttt{start}}{\dashrightarrow} q_2 \xrightarrow{\texttt{noise}} q_2$ | *Observation:* coin noise

One special event: A run is faulty iff the fault **f** occurs

A model for the coffee machine



Partial observation

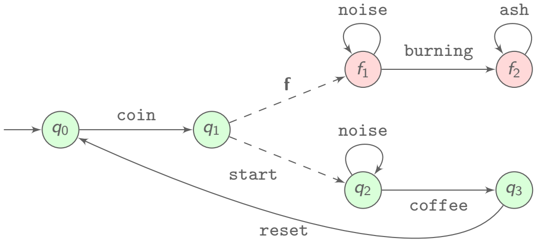
Observable events/unobservable events

$\rightarrow$ / $\dashrightarrow$

Run: $q_0 \xrightarrow{\texttt{coin}} q_1 \overset{\texttt{start}}{\dashrightarrow} q_2 \xrightarrow{\texttt{noise}} q_2$ | *Observation:* `coin noise`

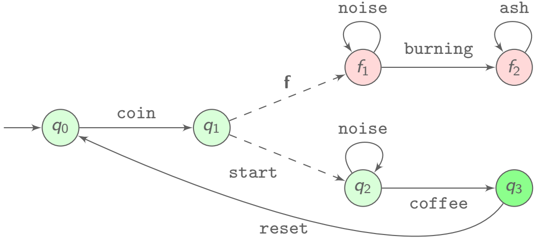
One special event: A run is faulty iff the fault **f** occurs

Classifying observations



Observation $\longrightarrow$ Set of potential states of the system

Classifying observations

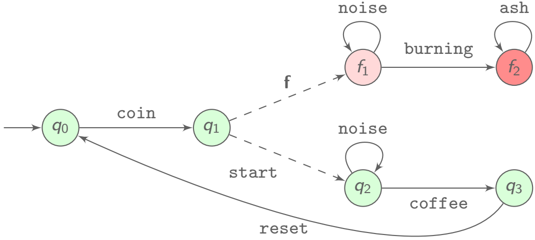


Observation $\longrightarrow$ Set of potential states of the system

✓ `coin coffee` *surely correct*

$$\mathtt{Obs}^{-1}(\mathtt{coin\ coffee}) = \{q_0 \xrightarrow{\mathtt{coin}} q_1 \xrightarrow{\mathtt{start}} q_2 \xrightarrow{\mathtt{coffee}} q_3\}$$

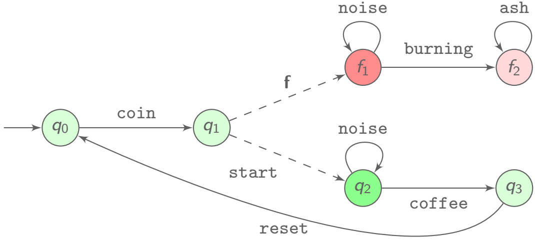
Classifying observations



Observation $\longrightarrow$ Set of potential states of the system

✓	`coin coffee`	*surely correct*
✗	`coin burning`	*surely faulty*

$$\mathtt{Obs}^{-1}(\mathtt{coin\ burning}) = \{q_0 \xrightarrow{\mathtt{coin}} q_1 \xrightarrow{\mathbf{f}} f_1 \xrightarrow{\mathtt{burning}} f_2\}$$

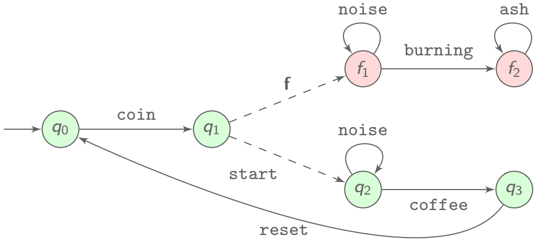


Observation $\longrightarrow$ Set of potential states of the system

✓	`coin coffee`	*surely correct*
✗	`coin burning`	*surely faulty*
?	`coin noise`	*ambiguous*

$$\mathtt{Obs}^{-1}(\mathtt{coin\ noise}) = \{q_0 \xrightarrow{\mathtt{coin}} q_1 \xrightarrow{\mathtt{start}} q_2 \xrightarrow{\mathtt{noise}} q_2, q_0 \xrightarrow{\mathtt{coin}} q_1 \xrightarrow{\mathbf{f}} f_1 \xrightarrow{\mathtt{noise}} f_1\}$$

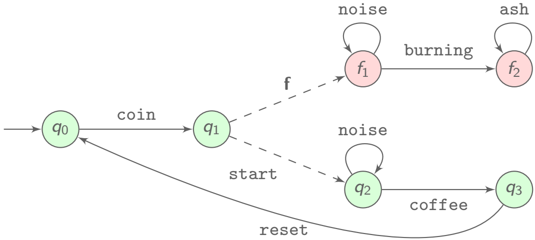
Diagnosers for logical systems [SSLST95]



- Verdict: detection of faults
- Correctness: if a fault is claimed, a fault occurred
- Reactivity: every fault will be detected after a bounded delay

[SSLST96] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis, *Failure diagnosis using discrete-event models*, IEEE TCST, 1996.

Diagnosers for logical systems [SSLST95]

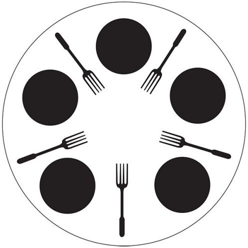


- Verdict: detection of faults
- Correctness: if a fault is claimed, a fault occurred
- Reactivity: every fault will be detected after a bounded delay

Correct but not reactive diagnoser: claiming a fault when `burning` occurs

[SSLST96] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis, *Failure diagnosis using discrete-event models*, IEEE TCST, 1996.

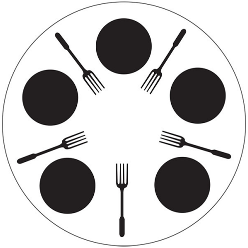
Useful to model some systems



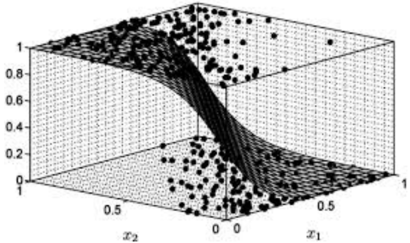
Internal random behaviour

The call for probabilistic models

Useful to model some systems



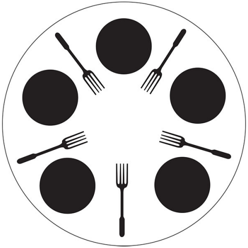
Internal random behaviour



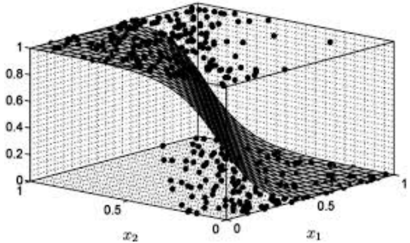
Models through statistical analysis

The call for probabilistic models

Useful to model some systems



Internal random behaviour

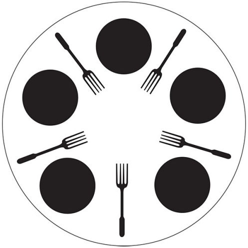


Models through statistical analysis

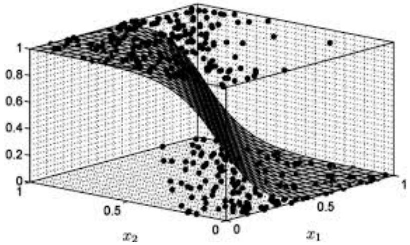
Enable quantitative requirements

The call for probabilistic models

Useful to model some systems



Internal random behaviour

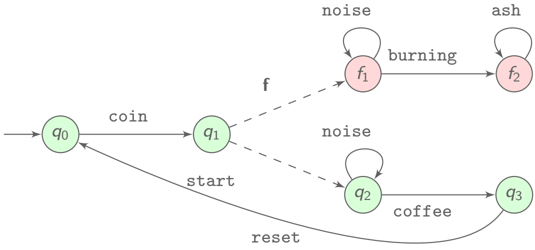


Models through statistical analysis

Enable quantitative requirements

- Is the system diagnosable, ignoring negligible behaviours?
- What is the measure of undetected faults?
- What is the average delay of fault detection?

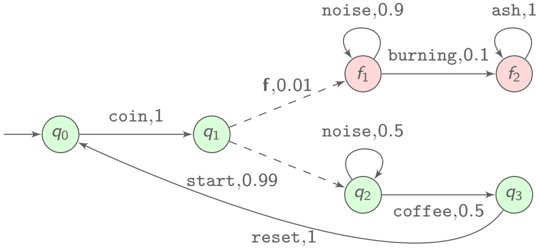
A probabilistic model for the coffee machine



Probability of a run

Run $\rho = q_0 \xrightarrow{\texttt{coin}} q_1 \overset{\texttt{start}}{\dashrightarrow} q_2 \xrightarrow{\texttt{noise}} q_2$

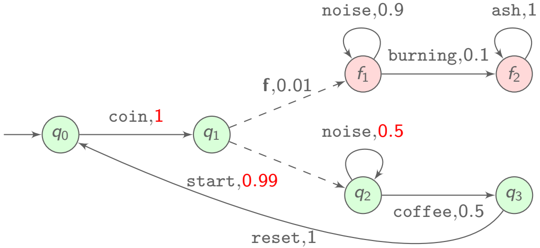
A probabilistic model for the coffee machine



Probability of a run

Run $\rho = q_0 \xrightarrow{\texttt{coin}} q_1 \overset{\texttt{start}}{\dashrightarrow} q_2 \xrightarrow{\texttt{noise}} q_2$

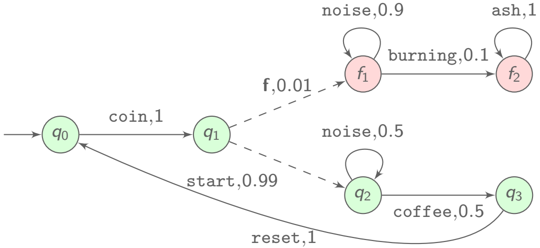
A probabilistic model for the coffee machine



Probability of a run

Run $\rho = q_0 \xrightarrow{\texttt{coin}} q_1 \xrightarrow{\texttt{start}} q_2 \xrightarrow{\texttt{noise}} q_2$ | *Probability* $\mathbb{P}(\rho) = 1 \times 0.99 \times 0.5$

A probabilistic model for the coffee machine

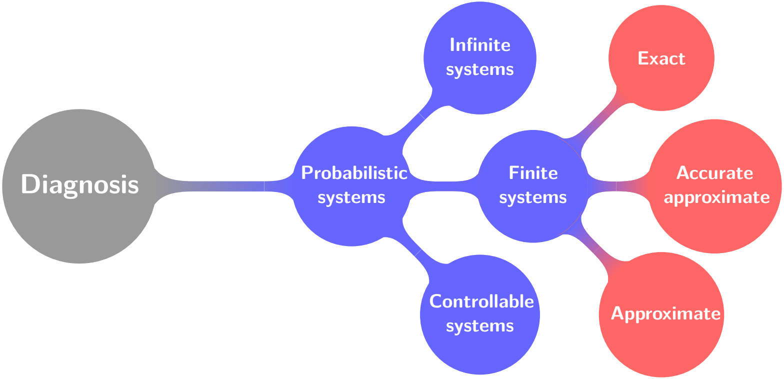


Probability of a run

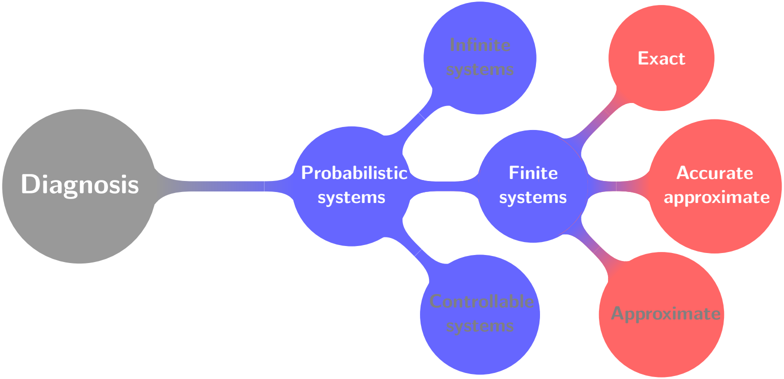
Run $\rho = q_0 \xrightarrow{\texttt{coin}} q_1 \xrightarrow{\texttt{start}} q_2 \xrightarrow{\texttt{noise}} q_2$ | *Probability* $\mathbb{P}(\rho) = 1 \times 0.99 \times 0.5$

$\rightarrow$ Defines a probability measure on the set of infinite runs

Contributions on the diagnosis of probabilistic systems



Contributions on the diagnosis of probabilistic systems



Challenges

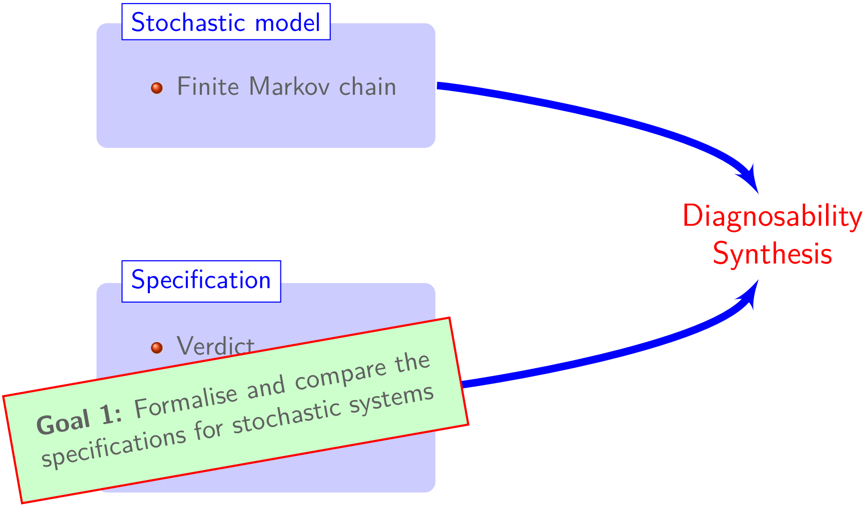
Stochastic model

- Finite Markov chain

Specification

- Verdict
- Correctness
- Reactivity

Diagnosability
Synthesis


Stochastic model
Finite Markov chain
Specification
Verdict
Diagnosability
Synthesis
Goal 1: Formalise and compare the specifications for stochastic systems

Challenges

Stochastic model

- Finite Markov chain

Specification

- Verdict

Diagnosability
Synthesis

Goal 2: Decidability and complexity of diagnosability and synthesis

Goal 1: Formalise and compare the specifications for stochastic systems

Challenges

Stochastic model

- Finite Markov chain

Specification

- Verdict

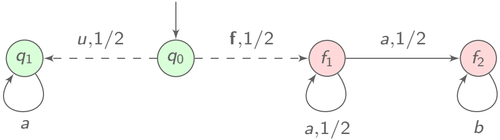
Diagnosability
Synthesis

Goal 1: Formalise and compare the specifications for stochastic systems

Goal 2: Decidability and complexity of diagnosability and synthesis

Many possible specifications

Verdict: information provided

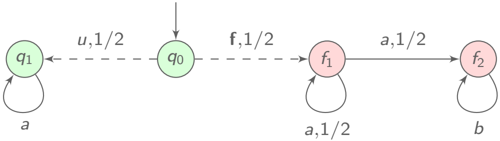


Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided

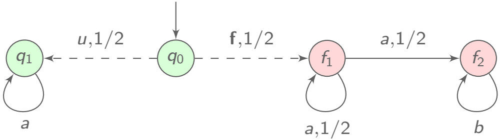


a^n is ambiguous

Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Verdict: information provided



a^n is ambiguous

Faults are detected almost surely:

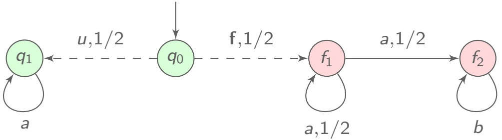
$$\lim_{n\to\infty} \mathbb{P}(\{q_0 \xrightarrow{\mathbf{f}} f_1(\xrightarrow{a} f_1)^n, q_0 \xrightarrow{\mathbf{f}} (f_1 \xrightarrow{a})^n f_2\}) = 0$$

Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided



a^n is ambiguous

Faults are detected almost surely:

$$\lim_{n\to\infty} \mathbb{P}(\{q_0 \xrightarrow{\mathbf{f}} f_1(\xrightarrow{a} f_1)^n, q_0 \xrightarrow{\mathbf{f}} (f_1 \xrightarrow{a})^n f_2\}) = 0$$

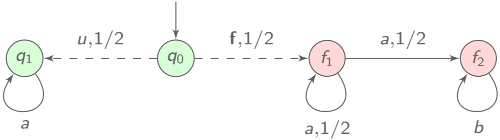
Correct runs stay ambiguous: $\lim_{n\to\infty} \mathbb{P}(\{q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^n\}) = \frac{1}{2}$

Correctness: accuracy of the verdict

Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided



a^n is ambiguous

Faults are detected almost surely:

$$\lim_{n\to\infty} \mathbb{P}(\{q_0 \xrightarrow{\mathbf{f}} f_1(\xrightarrow{a} f_1)^n, q_0 \xrightarrow{\mathbf{f}} (f_1 \xrightarrow{a})^n f_2\}) = 0$$

Correct runs stay ambiguous: $\lim_{n\to\infty} \mathbb{P}(\{q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^n\}) = \frac{1}{2}$

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

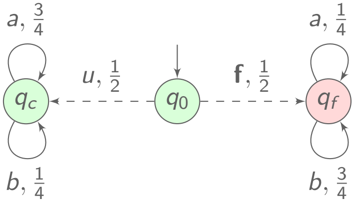
Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict



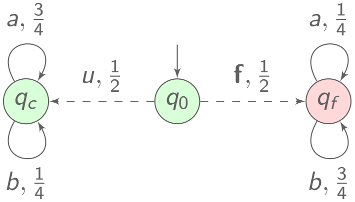
Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict



Not exactly diagnosable

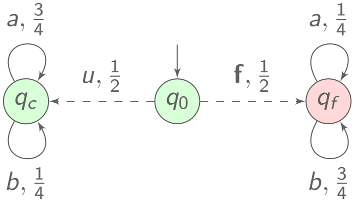
Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict



Not exactly diagnosable

However a high proportion of b implies a highly probable faulty run

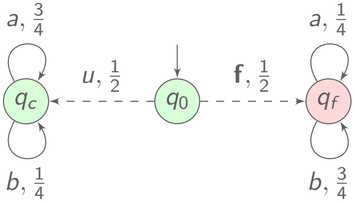
Reactivity: delay before a verdict is given

Many possible specifications

Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict



Not exactly diagnosable

However a high proportion of b implies a highly probable faulty run

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given

Many possible specifications

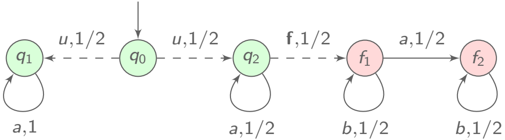
Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given



a^n is ambiguous: $q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^n, q_0 \xrightarrow{u} q_2(\xrightarrow{a} q_2)^{n-1} \xrightarrow{\mathbf{f}} f_1 \xrightarrow{a} f_2$

Many possible specifications

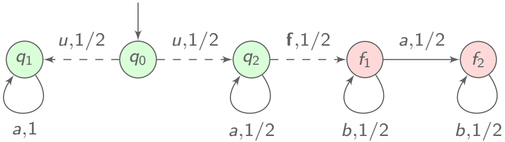
Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given



a^n is ambiguous: $q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^n, q_0 \xrightarrow{u} q_2(\xrightarrow{a} q_2)^{n-1} \xrightarrow{\mathbf{f}} f_1 \xrightarrow{a} f_2$

a^n is likely to be observed $\mathbb{P}(a^n) = \frac{1}{2} + \frac{1}{2^n} + \frac{1}{2^{n-1}}$

Many possible specifications

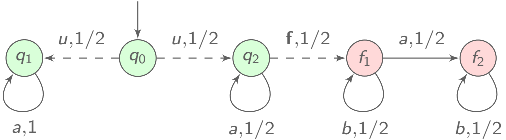
Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given



a^n is ambiguous: $q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^n, q_0 \xrightarrow{u} q_2(\xrightarrow{a} q_2)^{n-1} \xrightarrow{\mathbf{f}} f_1 \xrightarrow{a} f_2$

a^n is likely to be observed $\mathbb{P}(a^n) = \frac{1}{2} + \frac{1}{2^n} + \frac{1}{2^{n-1}}$

However, a^ω is surely correct: $q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^\omega, q_0 \xrightarrow{u} q_2(\xrightarrow{a} q_2)^\omega$

Many possible specifications

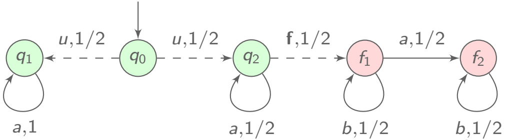
Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given



a^n is ambiguous: $q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^n, q_0 \xrightarrow{u} q_2(\xrightarrow{a} q_2)^{n-1} \xrightarrow{\mathbf{f}} f_1 \xrightarrow{a} f_2$

a^n is likely to be observed $\mathbb{P}(a^n) = \frac{1}{2} + \frac{1}{2^n} + \frac{1}{2^{n-1}}$

However, a^ω is surely correct: $q_0 \xrightarrow{u} q_1(\xrightarrow{a} q_1)^\omega, q_0 \xrightarrow{u} q_2(\xrightarrow{a} q_2)^\omega$

Almost sure, uniform almost sure or infinite?

Many possible specifications

Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given

Almost sure, uniform almost sure or infinite?

Each combination of features defines a diagnoser notion

Many possible specifications

Verdict: information provided

Faulty runs or all ambiguous runs?

Correctness: accuracy of the verdict

Exact, approximate or accurate approximate?

Reactivity: delay before a verdict is given

Almost sure, uniform almost sure or infinite?

Each combination of features defines a diagnoser notion

$\rightarrow$ Semantical analysis of the relations

Formalising diagnosability notions

Verdict: Detection of faulty runs

Reactivity: Finite delay

Formalising diagnosability notions

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability	FF-diagnosability $\lim_{n\to\infty} \mathbb{P}(FAmb_n) = 0$
Accurate approximate	Uniform AFF-diagnosability	AFF-diagnosability $\forall \varepsilon > 0, \lim_{n\to\infty} \mathbb{P}(FAmb_n^{\varepsilon}) = 0$
Approximate	Uniform εFF-diagnosability	εFF-diagnosability

Formalising diagnosability notions

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability [TT05][BHL18]	FF-diagnosability [BHL14][BHL18] $\lim_{n\to\infty} \mathbb{P}(FAmb_n) = 0$
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	AFF-diagnosability [BHL16][BHL18] $\forall \varepsilon > 0, \lim_{n\to\infty} \mathbb{P}(FAmb_n^{\varepsilon}) = 0$
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Formalising diagnosability notions

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure		Almost sure
Exact	Uniform FF-diagnosability [TT05][BHL18]	$\Longleftrightarrow$	FF-diagnosability [BHL14][BHL18] $\lim_{n\to\infty} \mathbb{P}(FAmb_n) = 0$
	$\Downarrow$		$\Downarrow$
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	$\Longrightarrow$	AFF-diagnosability [BHL16][BHL18] $\forall \varepsilon > 0, \lim_{n\to\infty} \mathbb{P}(FAmb_n^{\varepsilon}) = 0$
	$\Downarrow$		$\Downarrow$
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	$\Longrightarrow$	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Formalising diagnosability notions

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure		Almost sure
Exact	Uniform FF-diagnosability [TT05][BHL18]	$\Longleftrightarrow$	FF-diagnosability [BHL14][BHL18] $\lim_{n \to \infty} \mathbb{P}(FAmb_n) = 0$
	$\Downarrow$		$\Downarrow$
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	$\Longrightarrow$	AFF-diagnosability [BHL16][BHL18] $\forall \varepsilon > 0, \lim_{n \to \infty} \mathbb{P}(FAmb_n^{\varepsilon}) = 0$
	$\Downarrow$		$\Downarrow$
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	$\Longrightarrow$	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Stochastic model

- Finite Markov chain

Specification

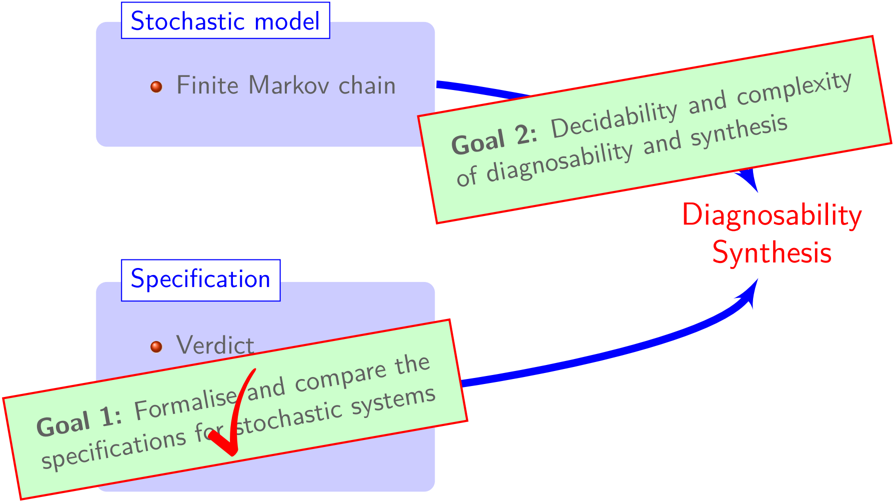
- Verdict

Goal 2: Decidability and complexity of diagnosability and synthesis

Goal 1: Formalise and compare the specifications for stochastic systems

Diagnosability
Synthesis

Challenges

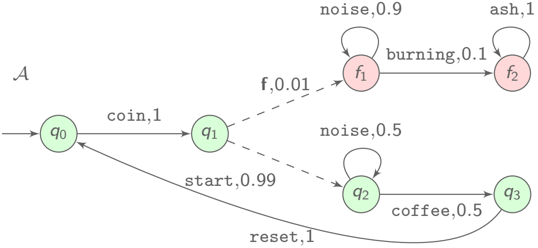


Stochastic model
Finite Markov chain
Specification
Verdict
Goal 2: Decidability and complexity of diagnosability and synthesis
Diagnosability
Synthesis
Goal 1: Formalise and compare the specifications for stochastic systems

FF-diagnosability

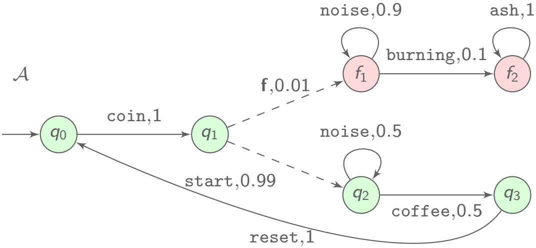
Definition

The probability of faulty ambiguous runs converges to 0



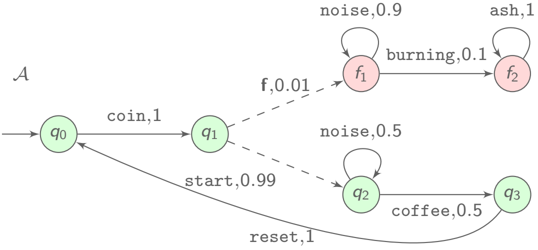
Faulty ambiguous runs: ending with $(f_1 \xrightarrow{noise} f_1)^*$

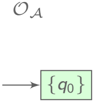
The belief construction



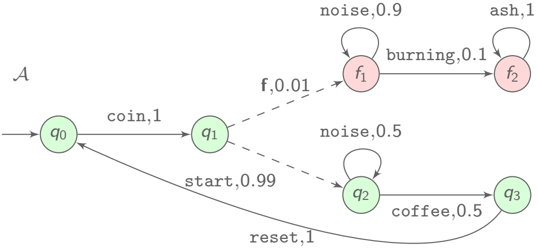
$\mathcal{O}_\mathcal{A}$: sequence of observations $\mapsto$ set of possible current states

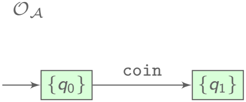
The belief construction



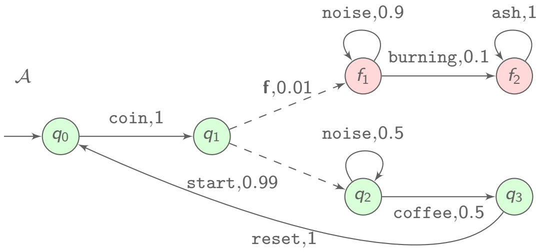


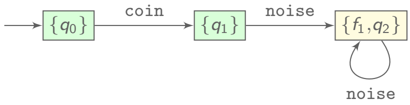
The belief construction



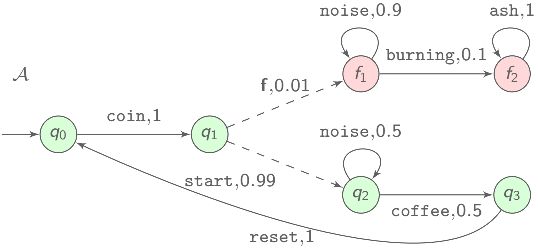


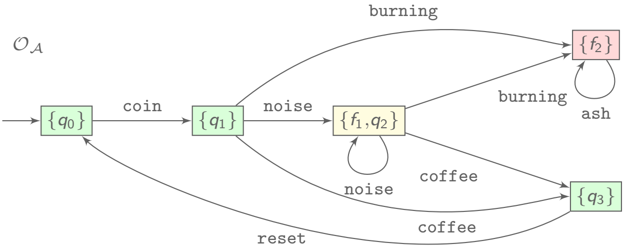
The belief construction



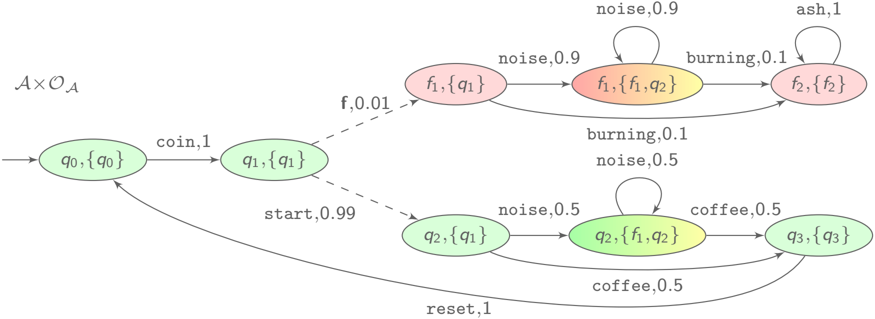


The belief construction

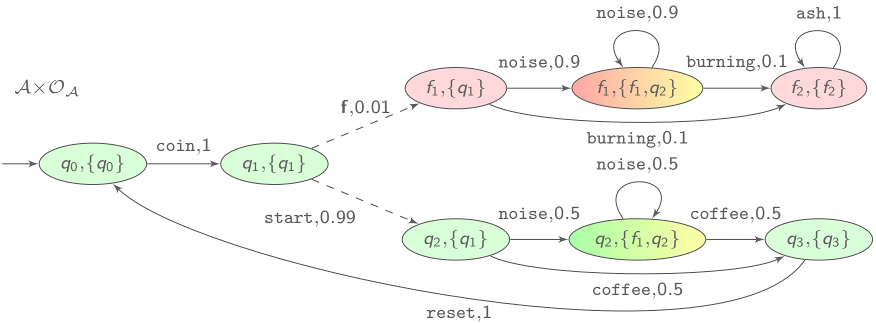




Synchronised product

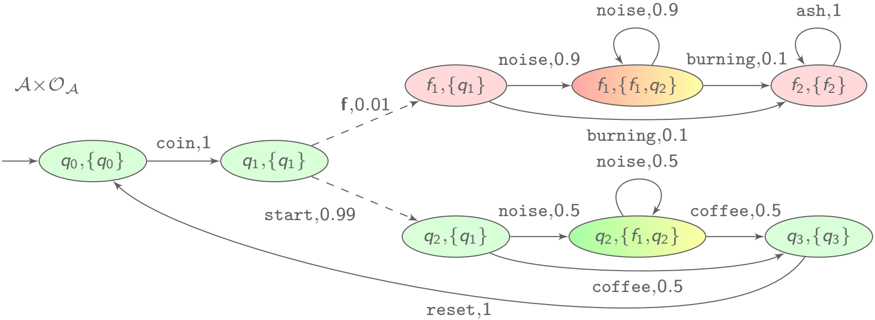


Synchronised product



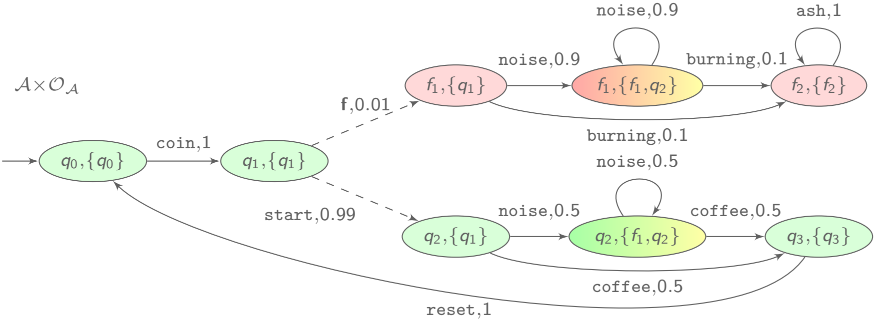
- Same stochastic behaviour as $\mathcal{A}$

Synchronised product



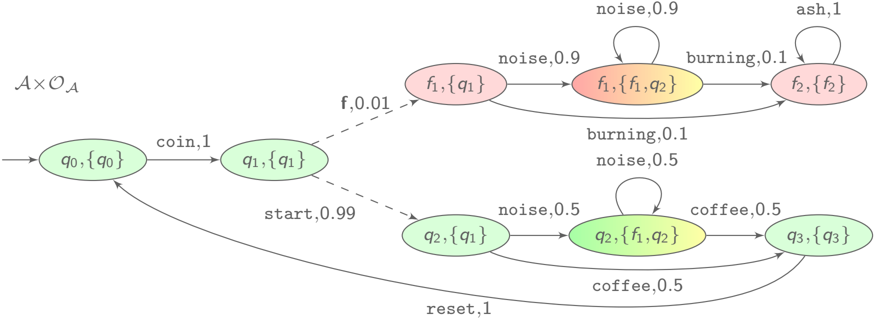
- Same stochastic behaviour as $\mathcal{A}$
- Ambiguity of a run deduced from its last state

Synchronised product



- Same stochastic behaviour as $\mathcal{A}$
- Ambiguity of a run deduced from its last state
- Possibly exponential in the size of $\mathcal{A}$

Synchronised product



- Same stochastic behaviour as $\mathcal{A}$
- Ambiguity of a run deduced from its last state
- Possibly exponential in the size of $\mathcal{A}$

FF-diagnosable iff
no BSCC contains a faulty ambiguous state

Complexity of FF-diagnosability

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability [TT05] [BHL18]	FF-diagnosability PSPACE-complete [BHL14][BHL18]
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	AFF-diagnosability [BHL16][BHL18]
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Complexity of FF-diagnosability

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability [TT05] PSPACE-complete [BHL18]	FF-diagnosability PSPACE-complete [BHL14][BHL18]
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	AFF-diagnosability [BHL16][BHL18]
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Complexity of FF-diagnosability

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability EXPTIME [TT05] PSPACE-complete [BHL18]	FF-diagnosability PSPACE-complete [BHL14][BHL18]
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	AFF-diagnosability [BHL16][BHL18]
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

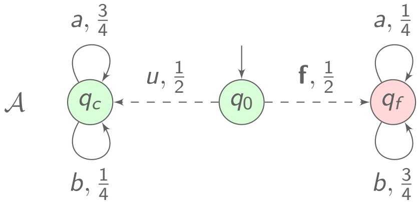
[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

AFF-diagnosability

Definition

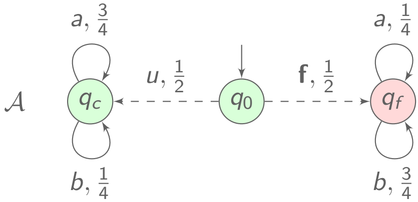
Faults are almost surely detected with arbitrarily small probability of false positive



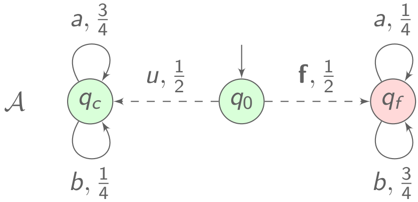
$\mathbb{P}(\text{correct} \mid bba) = \frac{1}{4}$

$\mathbb{P}(\text{correct} \mid bbab) = \frac{1}{10}$

High proportion of $b \Rightarrow$ small probability of being correct



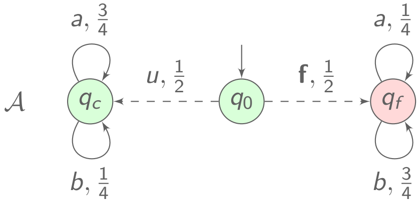
Distance between q_c and q_f: $\sup\limits_{E \subseteq \{a,b\}^\omega} \mathbb{P}_{q_f}(E) - \mathbb{P}_{q_c}(E)$.



Distance between q_c and q_f: $\sup\limits_{E \subseteq \{a,b\}^\omega} \mathbb{P}_{q_f}(E) - \mathbb{P}_{q_c}(E)$.

$E = \{$infinite words with proportion of b greater than half$\}$

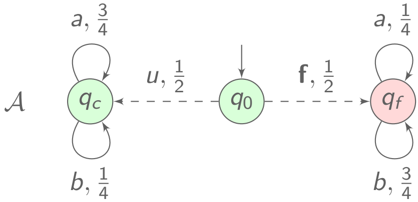
Distance between states



Distance between q_c and q_f: $\sup_{E \subseteq \{a,b\}^\omega} \mathbb{P}_{q_f}(E) - \mathbb{P}_{q_c}(E)$.

$E = \{$infinite words with proportion of b greater than half$\}$

E separates q_c and q_f: $\mathbb{P}_{q_c}(E) = 0$ and $\mathbb{P}_{q_f}(E) = 1$

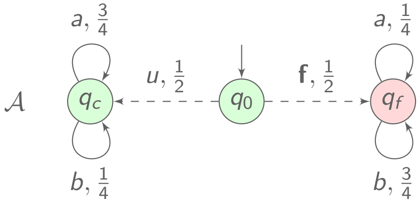


Distance between q_c and q_f: $\sup_{E \subseteq \{a,b\}^\omega} \mathbb{P}_{q_f}(E) - \mathbb{P}_{q_c}(E)$.

$E = \{$infinite words with proportion of b greater than half$\}$

E separates q_c and q_f: $\mathbb{P}_{q_c}(E) = 0$ and $\mathbb{P}_{q_f}(E) = 1$

$\longrightarrow$ The distance between q_c and q_f is 1



Distance between q_c and q_f: $\sup_{E \subseteq \{a,b\}^\omega} \mathbb{P}_{q_f}(E) - \mathbb{P}_{q_c}(E)$.

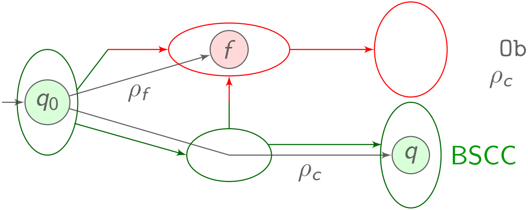
$E = \{$infinite words with proportion of b greater than half$\}$

E separates q_c and q_f: $\mathbb{P}_{q_c}(E) = 0$ and $\mathbb{P}_{q_f}(E) = 1$

$\longrightarrow$ The distance between q_c and q_f is 1

$\longrightarrow$ $\mathcal{A}$ is AFF-diagnosable

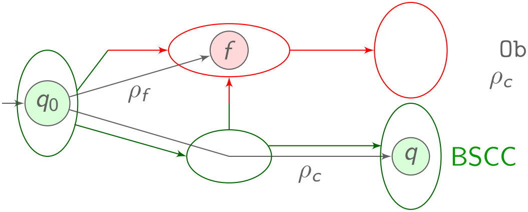
- Identifying **relevant pairs** of states



$\mathtt{Obs}(\rho_c) = \mathtt{Obs}(\rho_f)$
ρ_c correct, ρ_f faulty

Solving AFF-diagnosability

- Identifying **relevant pairs** of states

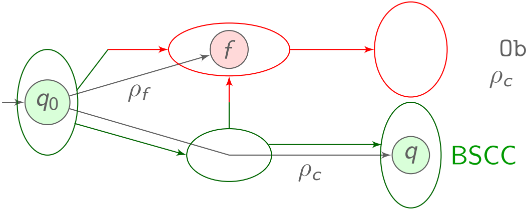


$\mathtt{Obs}(\rho_c) = \mathtt{Obs}(\rho_f)$
ρ_c correct, ρ_f faulty

- Checking distance 1 for all relevant pairs

Solving AFF-diagnosability

- Identifying **relevant pairs** of states



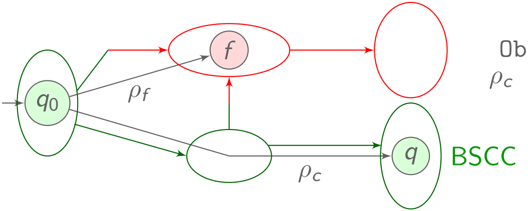
$\mathtt{Obs}(\rho_c) = \mathtt{Obs}(\rho_f)$
ρ_c correct, ρ_f faulty

- Checking distance 1 for all relevant pairs

AFF-diagnosable iff distance 1 for all relevant pairs

Solving AFF-diagnosability

- Identifying **relevant pairs** of states



$\mathtt{Obs}(\rho_c) = \mathtt{Obs}(\rho_f)$
ρ_c correct, ρ_f faulty

- Checking distance 1 for all relevant pairs

AFF-diagnosable iff distance 1 for all relevant pairs

- The distance 1 problem is in PTIME [CK14]

[CK14] Chen and Kiefer, *On the Total Variation Distance of Labelled Markov Chains*, CSL-LICS, 2014.

Complexity of AFF-diagnosability

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability EXPTIME [TT05] PSPACE-complete [BHL14][BHL18]	FF-diagnosability PSPACE-complete [BHL18]
Accurate approximate	Uniform AFF-diagnosability [TT05][BHL16][BHL18]	AFF-diagnosability PTIME [BHL16][BHL18]
Approximate	Uniform εFF-diagnosability [BHL16][BHL18]	εFF-diagnosability [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Complexity of AFF-diagnosability

Verdict: Detection of faulty runs

Reactivity: Finite delay

Reactivity / Correctness	Uniform almost sure	Almost sure
Exact	Uniform FF-diagnosability EXPTIME [TT05] PSPACE-complete [BHL14][BHL18]	FF-diagnosability PSPACE-complete [BHL18]
Accurate approximate	Uniform AFF-diagnosability [TT05] undecidable [BHL16][BHL18]	AFF-diagnosability PTIME [BHL16][BHL18]
Approximate	Uniform εFF-diagnosability undecidable [BHL16][BHL18]	εFF-diagnosability undecidable [BHL16][BHL18]

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

[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS, 2014.

[BHL16] Bertrand, Haddad and Lefaucheux, *Accurate approximate diagnosability of stochastic systems*, LATA, 2016.

[BHL18] Bertrand, Haddad and Lefaucheux, *A Tale of Two Diagnoses in Probabilistic Systems*, I&C, 2018.

Challenges

Stochastic model

- Finite Markov chain

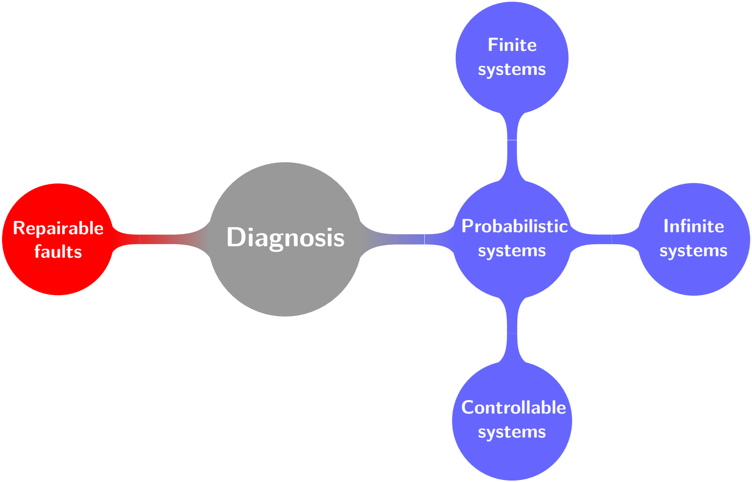
Specification

- Verdict

Diagnosability
Synthesis

Goal 2: Decidability and complexity of diagnosability and synthesis ✓

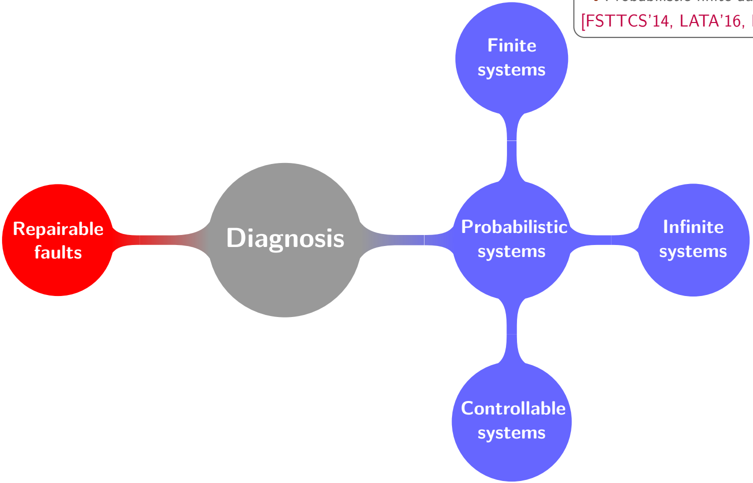
Goal 1: Formalise and compare the specifications for stochastic systems ✓


Repairable faults
Diagnosis
Probabilistic systems
Finite systems
Infinite systems
Controllable systems

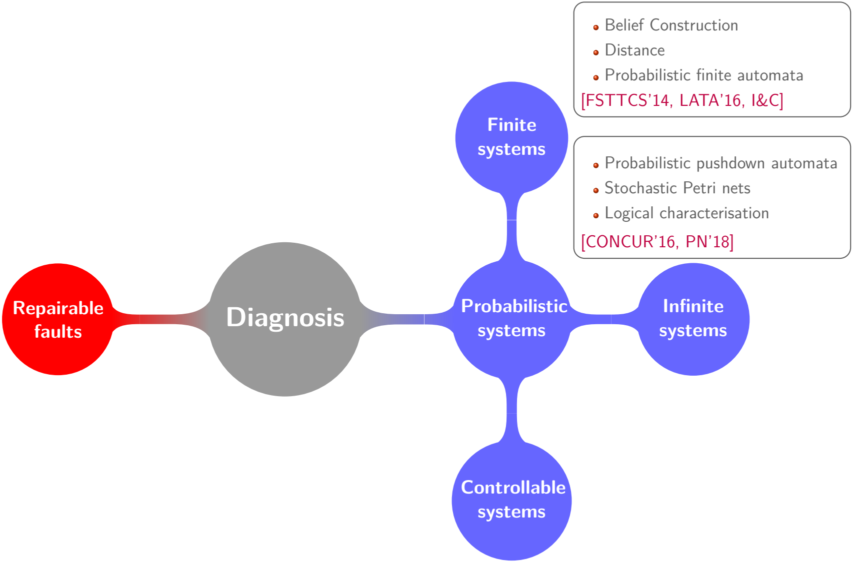
Contributions

- Belief Construction
- Distance
- Probabilistic finite automata

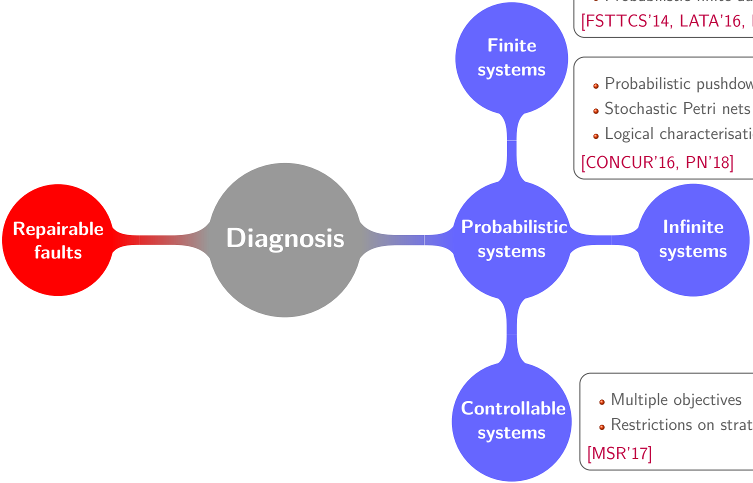
[FSTTCS'14, LATA'16, I&C]



Contributions



Contributions



- Belief Construction
- Distance
- Probabilistic finite automata

[FSTTCS'14, LATA'16, I&C]

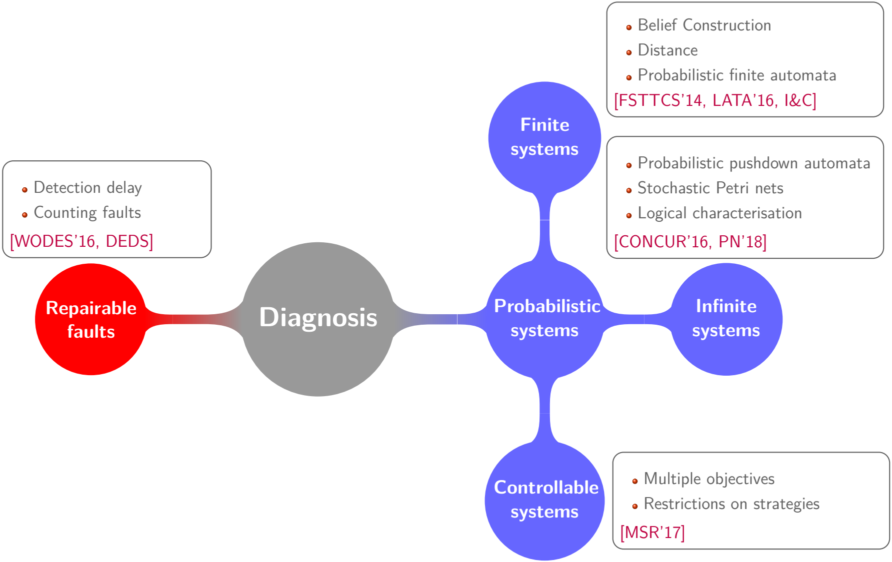
- Probabilistic pushdown automata
- Stochastic Petri nets
- Logical characterisation

[CONCUR'16, PN'18]

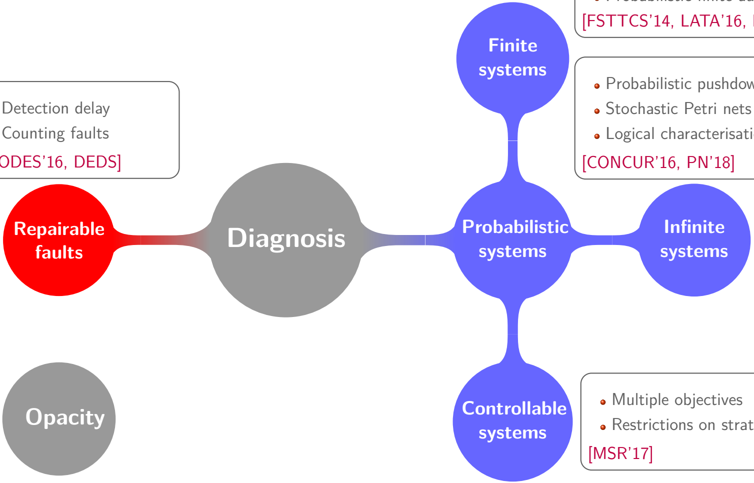
- Multiple objectives
- Restrictions on strategies

[MSR'17]

Contributions



Contributions



- Belief Construction
- Distance
- Probabilistic finite automata

[FSTTCS'14, LATA'16, I&C]

- Probabilistic pushdown automata
- Stochastic Petri nets
- Logical characterisation

[CONCUR'16, PN'18]

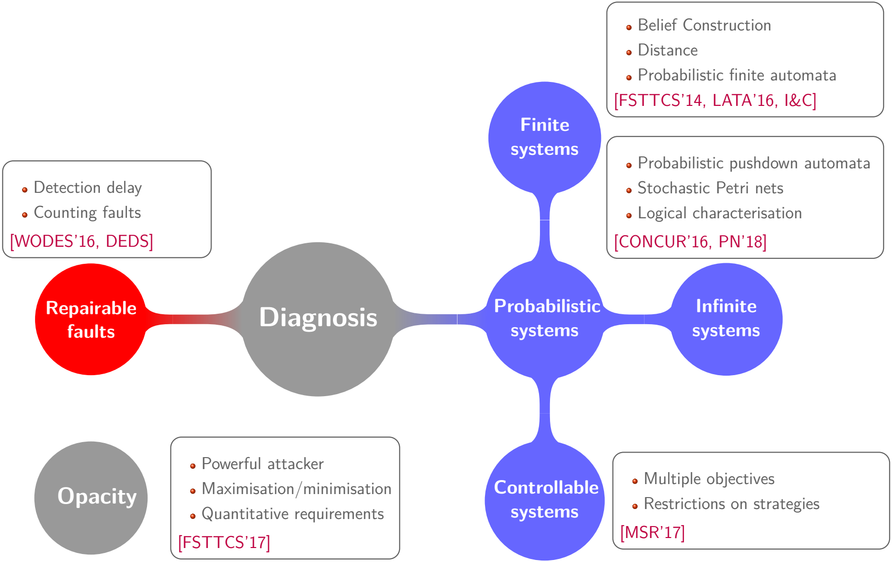
- Detection delay
- Counting faults

[WODES'16, DEDS]

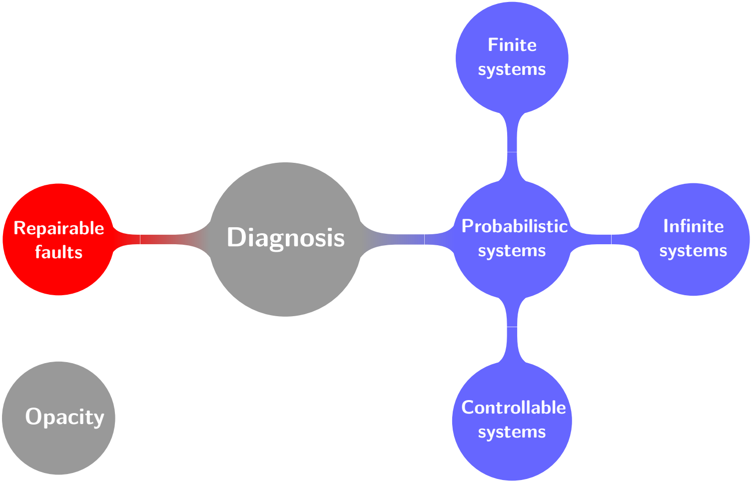
- Multiple objectives
- Restrictions on strategies

[MSR'17]

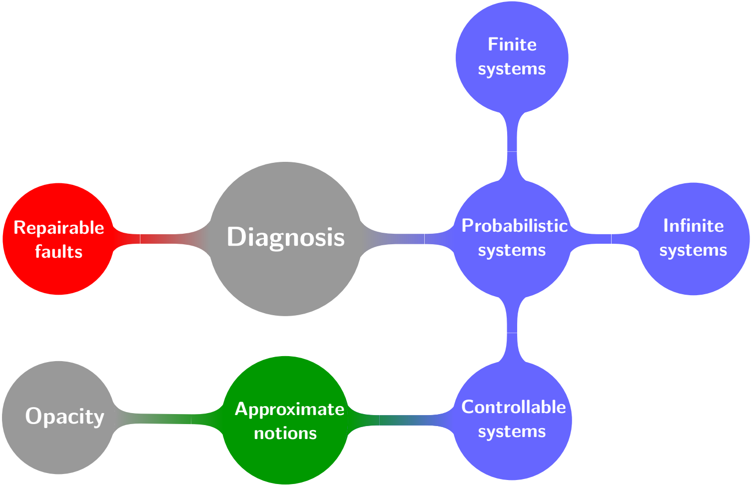
Contributions



Perspectives



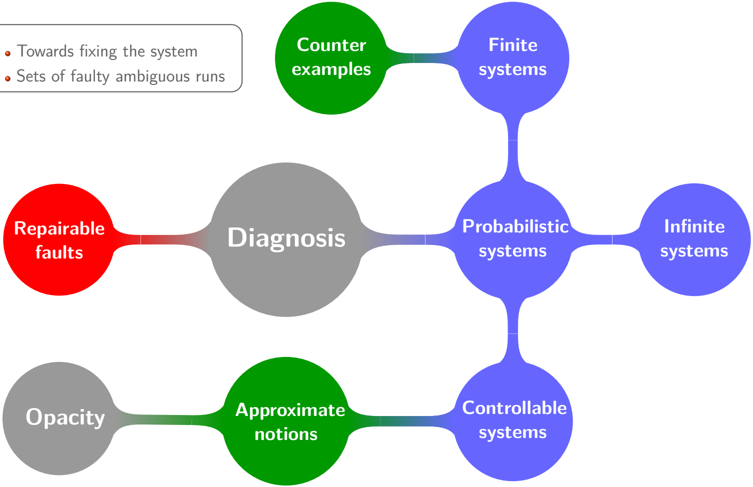
Perspectives



- Realistic
- Risk of undecidability

Perspectives

- Towards fixing the system
- Sets of faulty ambiguous runs



- Realistic
- Risk of undecidability

Perspectives