Reveal Your Faults: It's Only Fair!

Stefan Haar   César Rodríguez   Stefan Schwoon

LSV, ENS Cachan & CNRS, INRIA Saclay, France

DATE Workshop Cordoba, Nov 1st, 2013

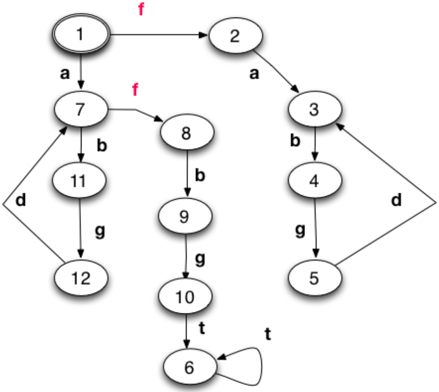
Fault Diagnosis

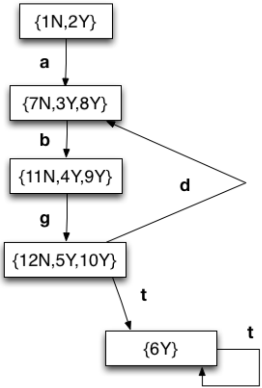
- Partially observable system: observable + unobservable actions
- Some unobservable actions are faults
- Given observation, all executions consistent with it contain a fault?

Fault Diagnosis

- Partially observable system: observable + unobservable actions
- Some unobservable actions are faults
- Given observation, all executions consistent with it contain a fault?
- This talk:
  - Fault diagnosis in concurrent systems
  - Using weak fairness assumptions

Classical Approach [SSL+95]





Diagnosis Problem

Do all runs that explain a given observation $s \in \Sigma^*$ contain a fault?

Diagnosis for Concurrent Systems

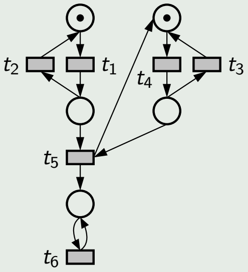
1. Concurrent systems have huge number of states!
2. Global time can be a hard assumption
   - Partially-ordered observations [BFHJ03]
3. System has no unobservable cycle
   - Solved only for sequential observations [EK12]
4. Assuming progress, or weak-fairness, is reasonable

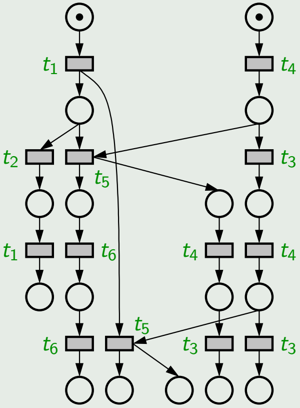
Contribution

We build on [BFHJ03, EK12] to:

- Allow for unobservable cycles and partially-ordered observations
- weak diagnosis: diagnosis + weak fairness
- Characterize weak diagnosis with reveals relation
- SAT-based algorithms for deciding weak diagnosis

Petri Net Unfoldings



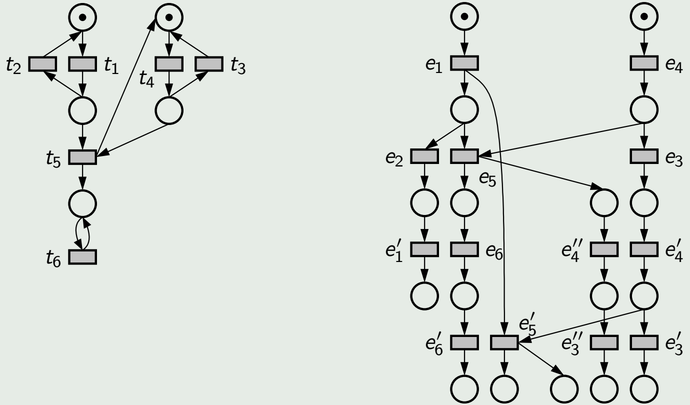


Remarks

- $\mathcal{U}_N$ is acyclic, 1-safe
- Events and conditions
- Labelling is a homomorphism
- Infinite in general

Structural Relations

The structure of an unfolding induces three relations over its events:



Causality:	$e < e'$	iff	e' occurs $\Rightarrow$ e occurs before
Conflict:	$e \# e'$	iff	e and e' never occur in the same run
Concurrency:	$e \parallel e'$	iff	not $e < e'$ and not $e' < e$ and not $e \# e'$

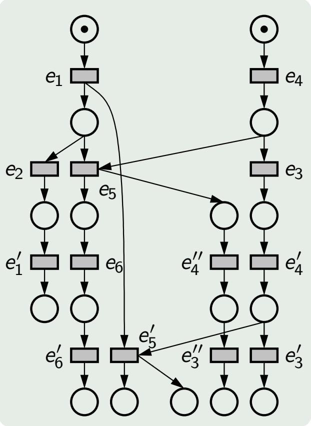
Configurations and Weak Fairness

Configuration

A set of events $\mathcal{C}$ is a configuration iff:

1. $e \in \mathcal{C} \wedge e' < e \Rightarrow e' \in \mathcal{C}$ (causally closed)
2. $\neg e \# e'$ for all $e, e' \in \mathcal{C}$ (conflict free)

Intuition: $\mathcal{C}$ configuration iff all its events can be arranged to form a run.



Configurations and Weak Fairness

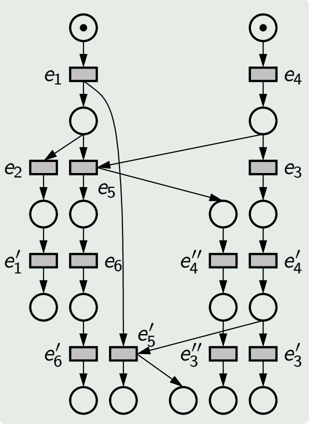
Configuration

A set of events $\mathcal{C}$ is a configuration iff:
[...]

Weakly Fair Firing Sequence

$e_1, e_2, \ldots \in E^\omega$ is weakly fair iff it eventually fires one spoiler of each e enabled, where

$$spoilers(e) := \{e' : {}^\bullet e \cap {}^\bullet e' \neq \emptyset\}$$



Configurations and Weak Fairness

Configuration

A set of events $\mathcal{C}$ is a configuration iff:
[...]

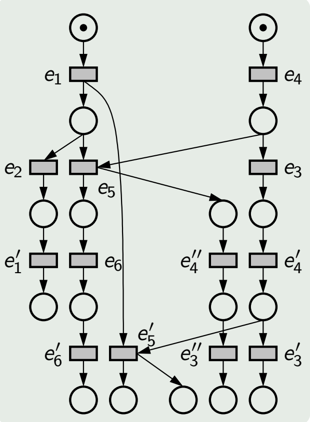
Weakly Fair Firing Sequence

$e_1, e_2, \ldots \in E^\omega$ is weakly fair iff it eventually fires one spoiler of each e enabled, where

$$spoilers(e) := \{e' : {}^\bullet e \cap {}^\bullet e' \neq \emptyset\}$$

Maximal Configuration

Run $e_1, e_2, \ldots$ weakly fair
iff
$\{e_1, e_2, \ldots\}$ maximal configuration w.r.t. $\subseteq$
iff
$\{e_1, e_2, \ldots\}$ does not enable any event



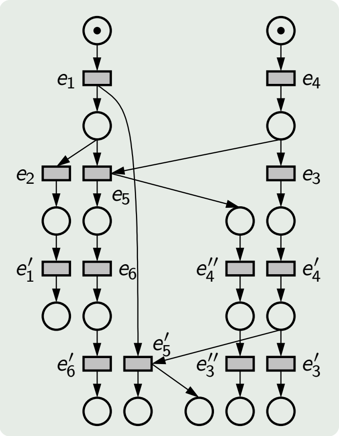
- Ω: set of maximal configurations

Reveals Relation

Definition [Haa10]

Event e reveals event e', written $e \triangleright e'$, iff for all $\omega \in \Omega$,

$$\text{if } e \in \omega, \text{ then } e' \in \omega.$$



Reveals Relation

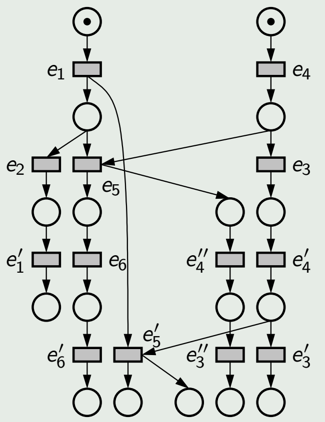
Definition [Haa10]

Event e **reveals** event e', written $e \triangleright e'$, iff for all $\omega \in \Omega$,

$$\text{if } e \in \omega, \text{ then } e' \in \omega.$$

Example

- if $e < e'$, then $e' \triangleright e$
- $e_1 \triangleright e_4$ (all ω contain e_4)
- $e_3 \triangleright e'_4$ (by progress assumption)
- $e_2 \triangleright e_3$ (e_2 disables e_5 + progress)

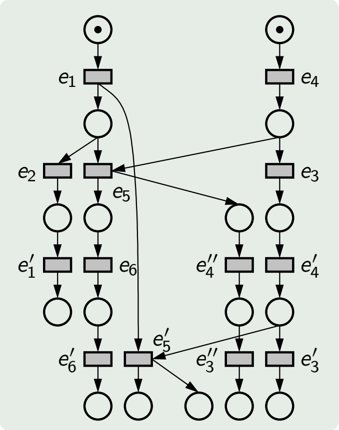


Extended Reveals Relation

Definition [BCH11]

Let A, B be sets of events. A extended-reveals B, written $A \twoheadrightarrow B$, iff for all $\omega \in \Omega$,

$$\text{if } A \subseteq \omega, \text{ then } B \cap \omega \neq \emptyset.$$



Extended Reveals Relation

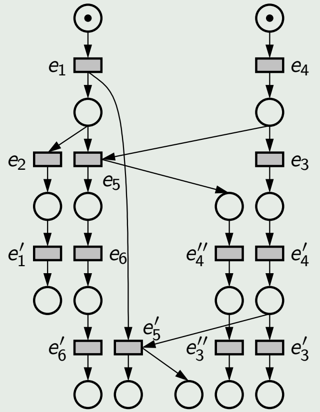
Definition [BCH11]

Let A, B be sets of events. A extended-reveals B, written $A \twoheadrightarrow B$, iff for all $\omega \in \Omega$,

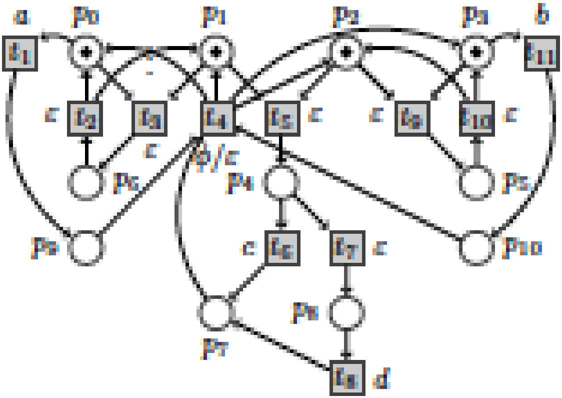
$$\text{if } A \subseteq \omega, \text{ then } B \cap \omega \neq \emptyset.$$

Example

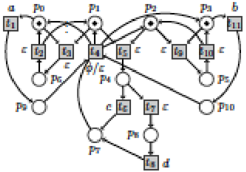
- if $e \triangleright e'$, then $\{e\} \twoheadrightarrow \{e'\}$
- $\{e_1\} \twoheadrightarrow \{e_2, e_5\}$ (due to progress)

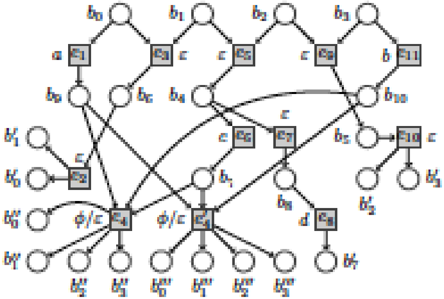


Example

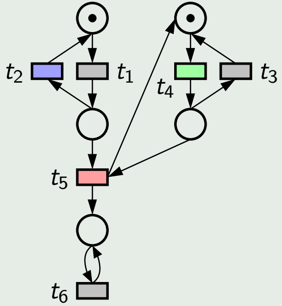

a
p0
p1
p2
p3
b
t1
t11
c
t2
t3
t4
t5
t9
t10
ϕ/c
p4
p5
p6
p9
p10
t6
t7
d
p7
p8
t8

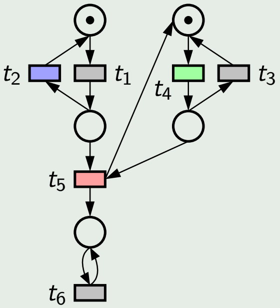
Example



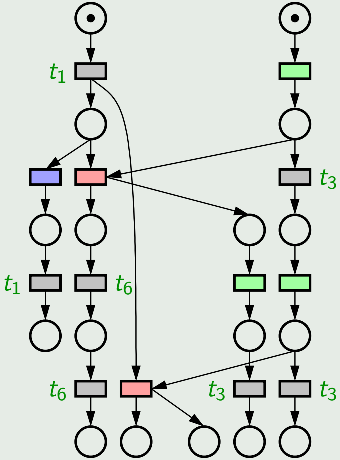


Observation Setup



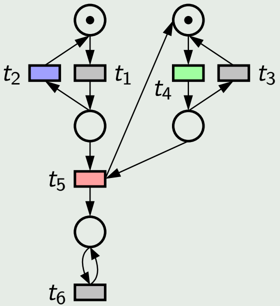


t_2
t_1
t_4
t_3
t_5
t_6

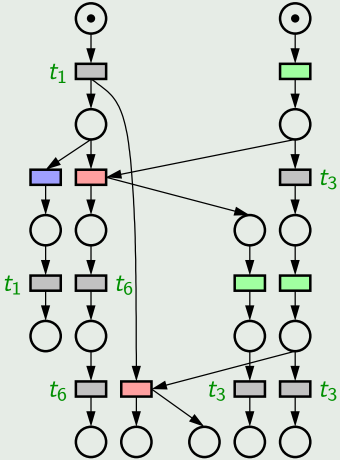


t_1
t_3
t_1
t_6
t_6
t_3
t_3

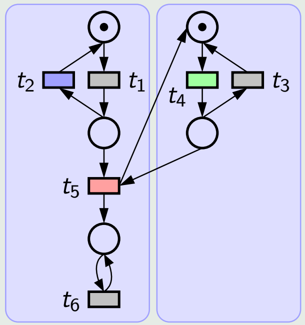
Observation Setup

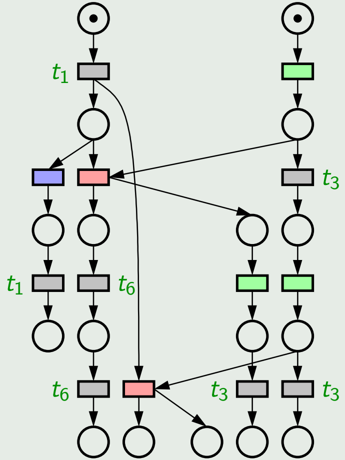


1. Sequential Observations



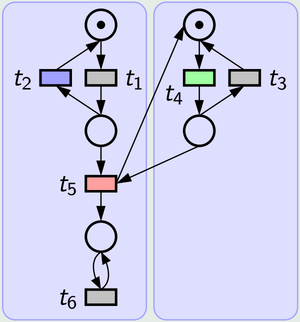
Observation Setup



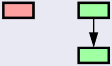


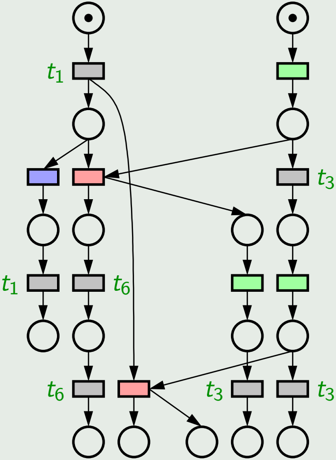
1. Sequential Observations

Observation Setup

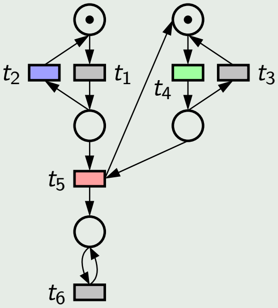


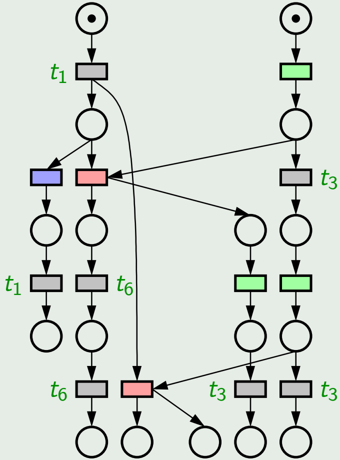
2. Ordered Observations





Explaining Observations



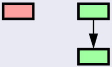


Given observation α,

$$\mathit{expl}(\alpha)$$

are the configurations that explain α:

- Same visible projection
- No order contradiction



Weak Diagnosis

Definition

Observation α weakly diagnoses a fault ϕ iff

for all $\mathcal{C} \in expl(\alpha)$, $\mathcal{C} \twoheadrightarrow E_\phi$,

i.e., any maximal configuration that contains an explanation $\mathcal{C} \in expl(\alpha)$, also contains a fault.

Violating Execution

Given α, find $\mathcal{C} \in expl(\alpha)$ and $\omega \in \Omega$ such that:

1. $\mathcal{C} \subseteq \omega$
2. ω is fault-free

Two Problems

- $expl(\alpha)$ may be infinite due to unobservable loops
- Need finite representation of Ω that allows for checking set inclusion

Verbose Configurations

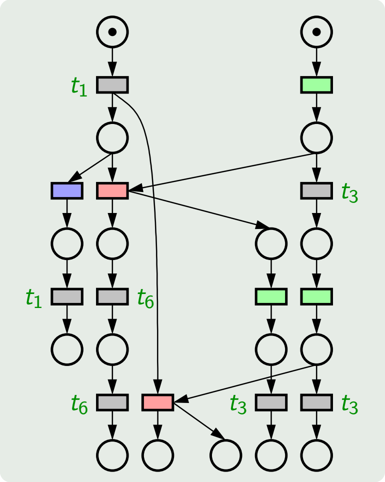
Definition

Configuration $\mathcal{C}$ is verbose if it contains events e, e' such that:

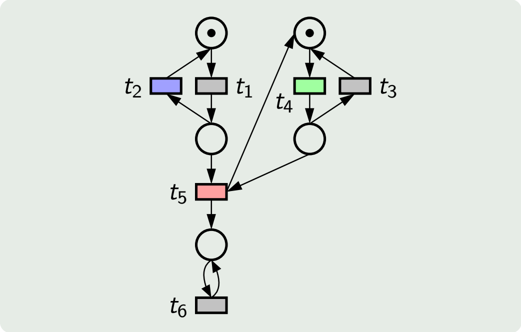
1. $e < e'$
2. $mark([e]) = mark([e'])$
3. $obs([e]) = obs([e'])$

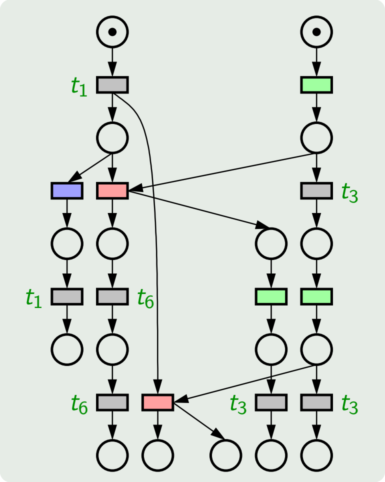
i.e., it contains an unobservable loop

- If $\mathcal{C}$ not verbose, it is succinct



Verbose Configurations





Finitely Many Succinct Explanations

Proposition

Any observation has finitely many succinct explanations

So they fit in a finite unfolding prefix!

1. Synchronize observation and net: $\alpha \times N$
2. Construct unfolding prefix $\mathcal{P}_{\alpha \times N}$ prunning with:

Definition

Event e cutoff iff there is e' such that

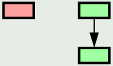
- $e' < e$
- $mark([e']) = mark([e])$

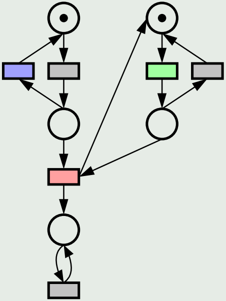
3. $\mathcal{C}$ explanation iff $mark(\mathcal{C})$ covers maximal places of α

Synchronization Example

Example

α $\times$ N

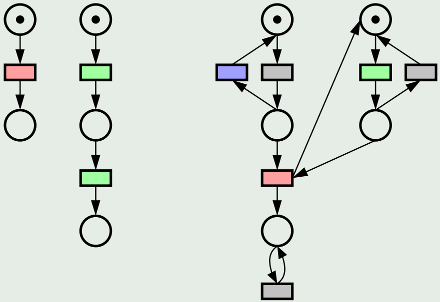




Synchronization Example

Example

$\alpha \quad \times \quad N$



Characterizing Maximal Configurations

Violating Execution

Given α, find $\mathcal{C} \in \mathit{expl}(\alpha)$ and $\omega \in \Omega$ such that:

1. $\mathcal{C} \subseteq \omega$
2. ω is fault-free

Characterizing Maximal Configurations

Violating Execution

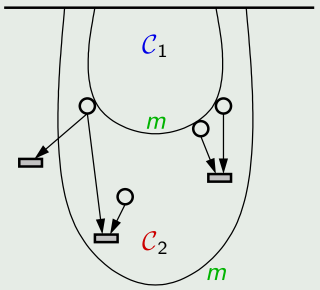
Given α, find $\mathcal{C} \in \mathit{expl}(\alpha)$ and $\omega \in \Omega$ such that:

1. $\mathcal{C} \subseteq \omega$
2. ω is fault-free

Lemma

There is ω weakly-fair and fault-free iff there are configurations $\mathcal{C}_1, \mathcal{C}_2$ such that:

1. $\mathcal{C}_1 \subseteq \mathcal{C}_2$
2. $\mathit{mark}(\mathcal{C}_1) = \mathit{mark}(\mathcal{C}_2)$
3. $\mathcal{C}_1$ enables $e \Rightarrow \mathit{spoilers}(e) \cap \mathcal{C}_2 \neq \emptyset$
4. $\mathcal{C}_2$ is fault-free



Problem: not quite yet a solution: $\mathcal{C}_2$ can be unboundedly large!

Finite Characterization of Maximal Configurations

Solution: define unfolding prefixes $\mathcal{P}^1, \mathcal{P}^2$ such that

1. $\mathcal{P}^1 \subseteq \mathcal{P}^2$
2. $\mathcal{C}_1, \mathcal{C}_2$ exist iff $\mathcal{P}^1, \mathcal{P}^2$ contain *small copies* $\widehat{\mathcal{C}}_1, \widehat{\mathcal{C}}_2$

Finite Characterization of Maximal Configurations

Solution: define unfolding prefixes $\mathcal{P}^1, \mathcal{P}^2$ such that

1. $\mathcal{P}^1 \subseteq \mathcal{P}^2$
2. $\mathcal{C}_1, \mathcal{C}_2$ exist iff $\mathcal{P}^1, \mathcal{P}^2$ contain *small copies* $\widehat{\mathcal{C}}_1, \widehat{\mathcal{C}}_2$

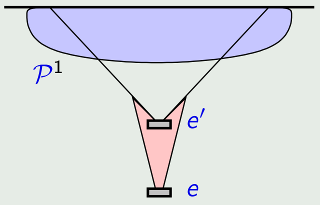
Definition

- $\mathcal{P}^1$: any marking-complete unfolding prefix (McMillan's algorithm)
- $\mathcal{P}^2$: largest unfolding prefix free of sp-cutoffs:

Definition

Event e sp-cutoff iff there is e' such that:

1. $e' < e$
2. $mark([e']) = mark([e])$
3. $\mathcal{P}^1 \cap {}^{\bullet}D = \emptyset$, where $D := [e] \setminus [e']$



Putting All Together

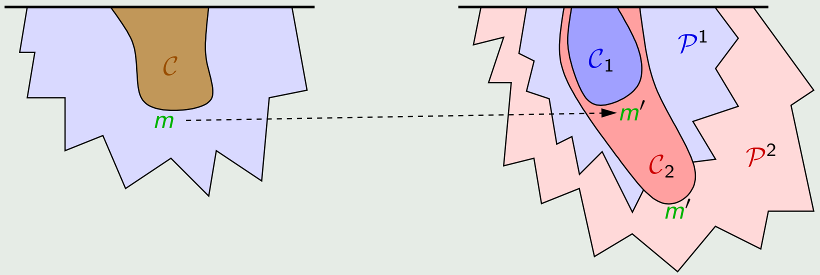
Theorem

α does not diagnose ϕ iff there is configurations

$$\mathcal{C} \in \mathcal{P}_{\alpha \times N}, \qquad \mathcal{C}_1 \in \mathcal{P}^1, \qquad \mathcal{C}_2 \in \mathcal{P}^2$$

such that

1. $\mathcal{C}$ marks maximal places
2. $mark(\mathcal{C}) \rightsquigarrow mark(\mathcal{C}_1)$
3. $\mathcal{C}_1 \subseteq \mathcal{C}_2$
4. $\mathcal{C}_2$ is fault-free
5. $mark(\mathcal{C}_1) = mark(\mathcal{C}_2)$
6. $\mathcal{C}_1$ enables $e \Rightarrow spoilers(e) \cap \mathcal{C}_2 \neq \emptyset$



Summary

- Weak diagnosis: diagnosis + weak fairness
- Unfolding-based method for solving weak diagnosis
- SAT-based algorithms (in the paper)

Future work

- Bounds on necessary unfolding prefixes
- Review decision procedures for weak diagnosability
- Implementation

Summary

- Weak diagnosis: diagnosis + weak fairness
- Unfolding-based method for solving weak diagnosis
- SAT-based algorithms (in the paper)

Future work

- Bounds on necessary unfolding prefixes
- Review decision procedures for weak diagnosability
- Implementation

Thank you for your attention

References I

Sandie Balaguer, Thomas Chatain, and Stefan Haar.
Building tight occurrence nets from reveals relations.
In *Proc. ACSD*, pages 44–53. IEEE, 2011.

Albert Benveniste, Éric Fabre, Stefan Haar, and Claude Jard.
Diagnosis of asynchronous discrete event systems: A net unfolding approach.
IEEE Transactions on Automatic Control, 48(5):714–727, May 2003.

Javier Esparza and Christian Kern.
Reactive and proactive diagnosis of distributed systems using net unfoldings.
In *Proc. ACSD*, pages 154–163, 2012.

Stefan Haar.
Types of asynchronous diagnosability and the Reveals-relation in occurrence nets.
IEEE Transactions on Automatic Control, 55(10):2310–2320, October 2010.

References II

Meera Sampath, Raja Sengupata, Stéphane Lafortune, Kasim Sinnamohideen, and Demosthenis Teneketzis.

Diagnosability of discrete-event systems.

IEEE Transactions on Automatic Control, 40(9):1555–1575, 1995.