

Diagnosis Properties by Design

Alban Grastien



Australian Government
Department of Communications,
Information Technology and the Arts
Australian Research Council

NICTA Members



Department of State and
Regional Development



NICTA Partners

Diagnosis Properties

DX Focus

- Models
- Algorithms
- System Properties

Example of Properties

- Diagnosability (and variants)
- Cost of computing diagnosis
- Cost of acquiring observations
- Privacy

Issues for Real World Networks

Model

- Is available very late (diagnosis is not a number one priority)
- Changes quickly (network)

Complexity

- Testing diagnosability on the global model is hard
- Testing diagnosability when the network requires reconfiguring is not an option

Idea

Property by Design

Given

- building blocks: component models
- design rules: how the components can be connected

determine if the properties are satisfied

Advantages

- Early computation: the final design is not necessary
- Early feedback: allow to point out design flaws (from a diagnosis perspective) early
- Computed once and for all: as long as the design rules are satisfied, the properties are satisfied

Idea (cont.)

Property by Design

Given

- building blocks: component models
- design rules: how the components can be connected

determine if the properties are satisfied

Drawbacks

- Is undecidable in general
- Puts a strong constraint on the network

Design Rules

How to Make the Rules Applicable

A slightly incorrect design should be easy to correct

- Understandable rules (not a “black box” decision)
- Local rules

How to Test the Property

Because the network is unbounded, the property must be proved locally

- Local rules

Examples

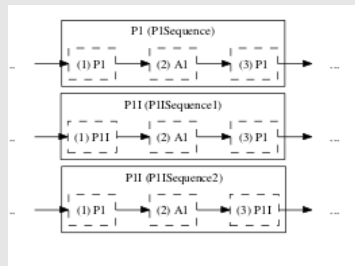
Model-Checking

Browne et al., *Reasoning about networks with many identical finite-state processes*, **Information and Computation**, vol. 81, pp. 13–31, 1989.

Planning

Haslum, *A new approach to tractable planning* **ICAPS-08**, pp. 132–139, 2008.

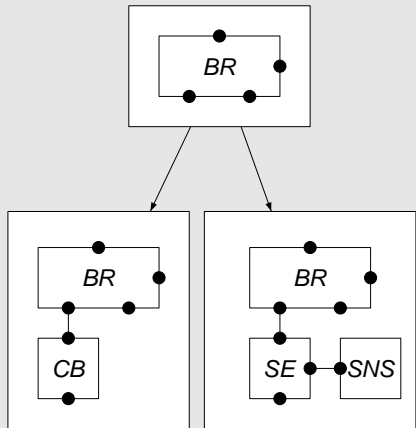
Uses node labeled controlled graph grammars



My View

Design Rules = Patterns

A branching point should be connected to a circuit breaker or to an electrical equipment with a sensor attached to it.



More . . .

Design Rules Synthesis

Given a set of component types, generate the design rules

Contracts

???