Asymmetric Diagnosability Analysis of Discrete-Event Systems

Marina Zanella
University of Brescia (Italy)

DX 2017
Brescia, September 27
DES model

- Observable events in yellow
- Unobservable events in blue (f is a fault)
- Assumption:
  - Prefix-closed and live language, both for all events and for observable events
Diagnosability

- Defined in [Sampath et al. 1995]
- This DES is not diagnosable
  - If \((a \mid b)^* a c^+\) is observed, we cannot single out the occurred fault (\(f\) or no fault?)
Twin plant method
[Jiang et al. 2001]
Twin plant: synchronization of two identical verifiers

Verifier

Twin plant

(F,N) (F,F) (F,N) (F,F) (F,F) (F,N) (C,N) (C,N) (A,N) (A,N) (B,N) (B,N) (D,N) (D,N)
Twin plant: check

- Diagnosability (necessary and sufficient) condition: no *ambiguous cycle*
- Here this condition is not met
Ambiguous cycles

Symmetry = redundancy
Idea: asymmetry for redundancy reduction

Bad twin (B) = verifier

Good twin (G) = B without any faulty state
Asymmetric twin plant: synchronization of B and G

The diagnosability condition is the same as for the symmetric twin plant.
Idea for further reduction:
transition-based representation
TB asymmetric twin plant

TB bad twin
B = TB verifier

TB good twin
G = B without any faulty transition

Ambiguous transition
TB twin plant

- Diagnosability (necessary and sufficient) condition: no *ambiguous transition* that either precedes a cycle or belongs to a cycle
- Here this condition is not met
Previous work

- The traditional notion of diagnosability relies on a totally temporally ordered observation.

- The observation may be temporally uncertain (level of temporal uncertainty = maximum number of observable events received in a row whose relative emission order may be unknown).

- New diagnosability analysis: is a DES diagnosable for a given level of temporal uncertainty?
Previous work

- Diagnosability with temporal uncertainty of level 1 is indeed the old diagnosability.
- How can we check diagnosability with level > 1? The method is still based on the twin plant, where the size of the plant increases with the level of uncertainty.
Diagnosable DES model

... a d c⁺ : f

Equivalent DES model of level 2
Incremental construction of the bad twin

TB bad twin of level 1

TB bad twin of level 2
Sufficient conditions for TB diagnosability with level $\ell$

- The TB bad twin of level $\ell$ is deterministic
- Non-faulty and faulty transitions of the TB bad twin of level $\ell$ do not share any (compound) observable event
- As far as a sufficient condition holds, we do not need the twin plant (this is valid also for diagnosability with no uncertainty in the observation)
Incremental construction of
the twin plant

- The TB asymmetric twin plant of level \( \ell \)
can be obtained by adding to that of level \( \ell - 1 \) the transitions relevant to compound events of level \( \ell \).

- Such transitions can be built by exploiting the information included in the TB asymmetric twin plant of level \( \ell - 1 \).
Conclusions

- Asymmetry reduces redundancy in the twin plant.
- A transition-based representation reduces the size of the twin plant (very important for uncertain observations).
- Defined the necessary and sufficient diagnosability condition for the transition-based twin plant and some sufficient conditions.
Conclusions and future work

- The twin(s) of level \( \ell > 1 \) can be obtained by incrementing those of level \( \ell - 1 \)
- The same applies to the twin plant
- Experiments needed