Fair Diagnosability in Transition Systems

Marco Bozzano, Alessandro Cimatti, Stefano Tonetta, **Viktória Vozárová**

University of Trento

Fondazione Bruno Kessler

▸ Diagnosability

Real-life systems are not perfect. Even in the case of a fault, they need to detect the fault and respond such that safety is guaranteed. The process of detecting a fault is called the fault diagnosis. Diagnosability is a property of a fault in a system saying that it is possible to detect the fault from the observable part of the system in any scenario [1]. Here, we focus on finite systems with infinite runs modelled as fair transition systems. We extend the work published in [2].

▸ Lightbulb example

Figure 1 shows an example of such system: a lightbulb that is either switched ON or OFF. The fairness condition of the system is $(ON \wedge OK) \vee (OFF \wedge KO)$. This means that if the system is OK, the lightbulb switches ON infinitely many times. However, in the case of a fault KO, it eventually switches OFF and stays there. The diagnosability problem is to decide if on every fair trace we can detect that the lightbulb is KO only from the sequence of ON/OFF.

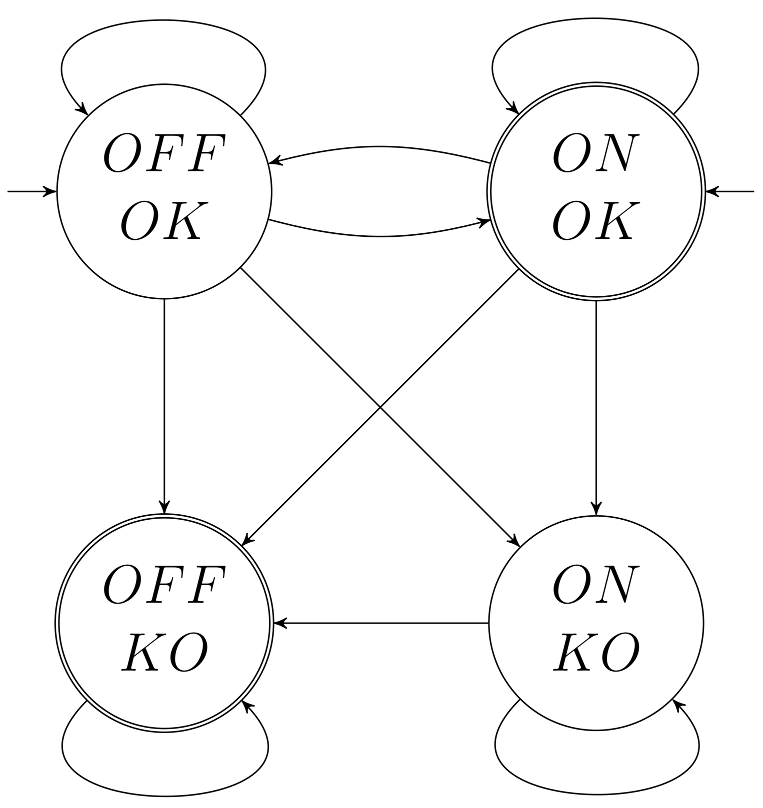

Figure 1: Example of a fair transition system.

▸ Alarm patterns

We consider different diagnosability alarm patterns based on how quickly after the fault should an alarm be raised. If the alarm is raised anytime in the future, the fault is FiniteDel diagnosable. If the alarm is raised exactly in d steps or in at most d steps, the fault is ExactDel(d) or BoundDel(d) diagnosable. Pattern BoundDel$_{O}(d)$ is a weaker version of BoundDel(d). We also introduce existential patterns $\exists$ExactDel$(\cdot)$, $\exists$BoundDel$(\cdot)$ and $\exists$BoundDel$_{O}(\cdot)$ that are diagnosable if there exists d that makes them diagnosable.

▸ Critical pairs

The diagnosability problem can be solved by finding so-called critical pairs. Critical pairs are such pairs of fair traces where only one is faulty and both are observationally equivalent up to some point. The existence of a critical pair is sufficient and necessary for proving the non-diagnosability of patterns ExactDel(d), BoundDel(d) and BoundDel$_{O}(d)$. For FiniteDel, it is only a sufficient condition. To prove the non-diagnosability for existential patterns, we need to find a critical pair for every d.

▸ Ribbon-shaped critical pairs

To decide if there is a critical pair for all d, we designed ribbon-shaped critical pairs. RCPs are critical pairs with a loop after the fault, that can be unrolled arbitrarily many times. With each unrolling of the loop, we create a critical pair for larger and larger ds. We call this loop a ribbon. For the patterns $\exists$ExactDel$(\cdot)$, $\exists$BoundDel$_{O}(\cdot)$ and FiniteDel, one ribbon is sufficient to encode critical pairs for all ds. For $\exists$BoundDel$(\cdot)$, we need an arbitrarily long unrolling both before and after the fault, thus we design double-ribbon-shaped critical pairs. Figure 2 shows an example of RCP for the lightbulb proving non-diagnosability of $\exists$BoundDel$_{O}(\cdot)$.

▸ CTL* algorithm

The existence of RCPs and DRCPs can be encoded in a CTL* formula. As a result, the diagnosability problem is reduced to CTL* model checking problem. One can use a standard CTL* model checking solver or encode the system over BDDs, compute the fair states using Emerson-Lei algorithm [3] and find the states satisfying the CTL* formula using fixpoint operators.

▸ L2S algorithm

To find RCPs and DRCPs in a transition system, we extend the liveness-to-safety reduction [4]. In the original reduction, the system is extended such that a reachability of a loop in the original system is reduced to a reachability of a state in the extended system. Using a similar principle, we reduce the reachability of several consecutive loops to the reachability of a state. We exploit the fact that in finite systems, fairness can be verified by finding a fair loop.

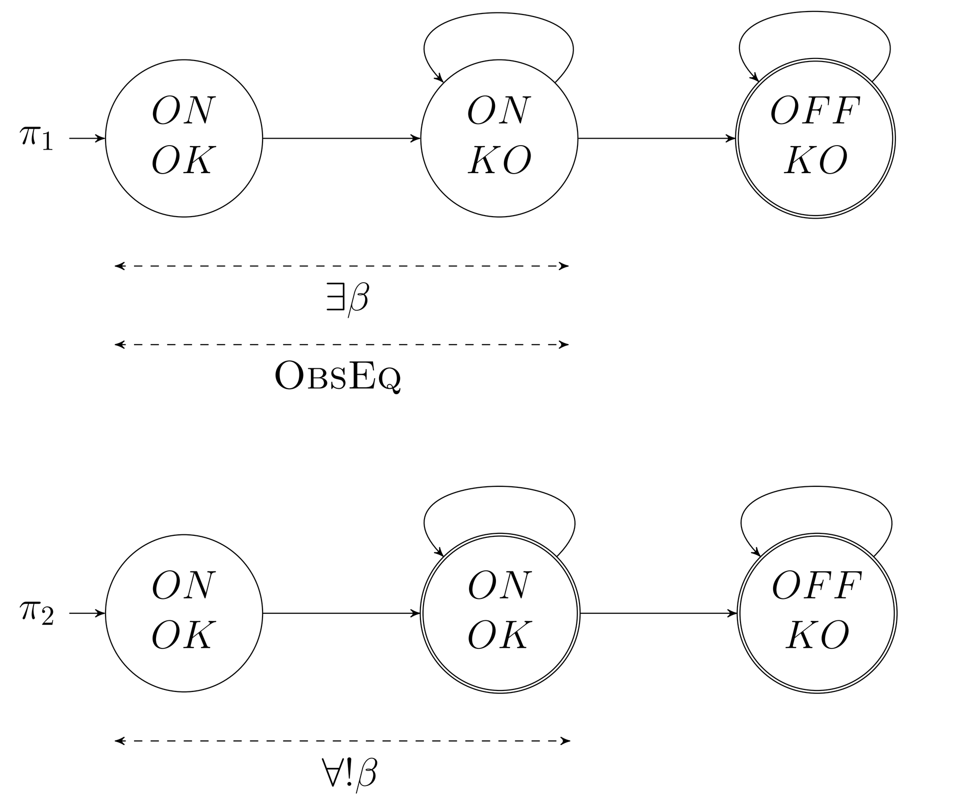

Figure 2: Example of a ribbon-shaped critical pair with one ribbon and one fair loop.

▸ Experiments

We implemented both algorithms on top of the xSAP tool and tested them on several diagnosable benchmarks. We compare CTL* algorithm based on fixpoint computation over BDDs (FP-BDD) and L2S algorithm using IC3 engine to decide reachability (L2S-IC3). We tested RCPs for FiniteDel and $\exists$BoundDel$_{O}(\cdot)$. As shown in Figure 3, L2S-IC3 outperforms FP-BDD.

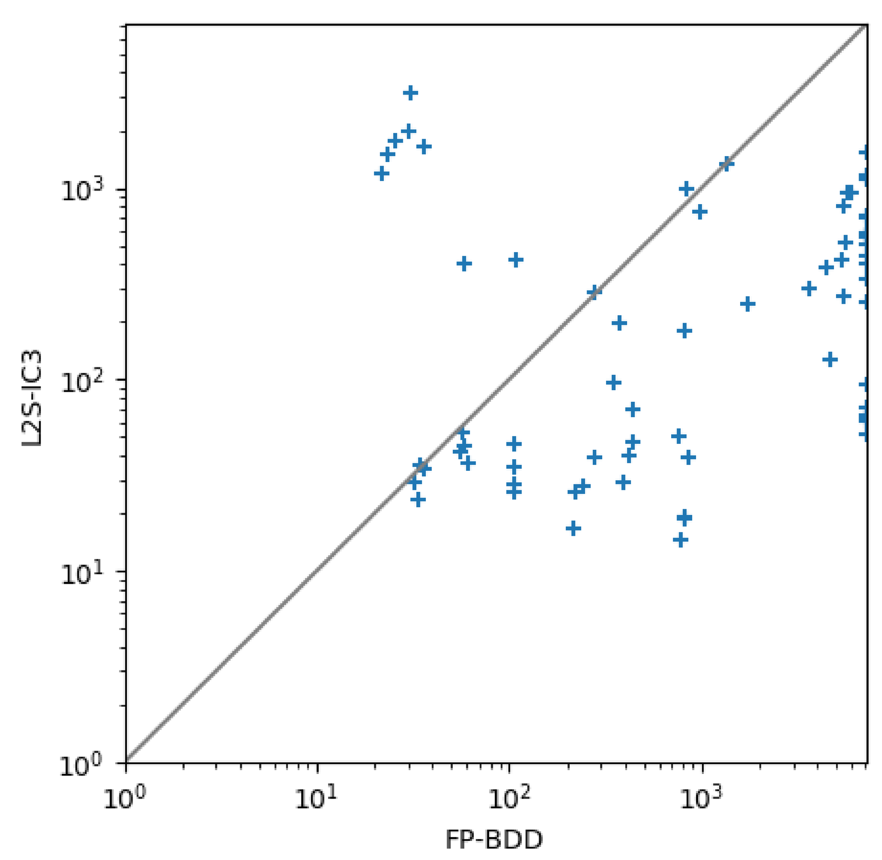

Figure 3: Comparison of L2S-IC3 and FP-BDD runtimes in seconds for FiniteDel pattern.

▸ References

[1] Meera Sampath, Raja Sengupta, Stéphane Lafortune, Kasim Sinnamohideen, and Demosthenis Teneketzis. Diagnosability of Discrete-event Systems. *IEEE Transactions on Automatic Control*, 40(9), 1995.

[2] M. Bozzano and A. Cimatti and S. Tonetta. Testing Diagnosability of Fair Discrete-Event Systems. In *Proc. International Workshop on Principles of Diagnosis (DX-19)*, 2019.

[3] E. Allen Emerson and Chin-Laung Lei. Temporal reasoning under generalized fairness constraints. In *STACS 86*, 1986.

[4] Armin Biere, Cyrille Artho, and Viktor Schuppan. Liveness checking as safety checking. *Electronic Notes in Theoretical Computer Science*, 66(2), 2002.