Case studies evaluated for manifestability checking

We provide here a set of case studies that are used to evaluate our algorithm to verify manifestability in our paper titled *How to be sure a faulty system does not always appear healthy? – Fault manifestability analysis for discrete event and timed systems*. We will show especially the original systems (modified literature systems) and then explain how we extend them by constructing subsystems in an arbitrary way while keeping the same verdict. For each example shown in the document, we only consider one type of fault, noted by F. An observable (resp. unobservable) event is represented by oi (resp. ui). For some distributed original literature systems (some with multiple types of faults), its corresponding modified one chooses a subpart of its synchronized product that is interesting for our algorithm with only one type of fault.

1 Table 1

In this section, we show some of the original systems modified from literature examples used for the evaluation presented in Table 1. As for those hand-crafted ones, we have explained in the end of the document how to generate them based on these original ones in semi-arbitrary ways.

1.1 Ex.2

In the system shown in Figure 1, as explained in the paper, the fault is (strongly) manifestable and not diagnosable. The reason is that there is a critical pair for the faulty trajectory containing $u1$. But the occurrence of the faulty also has a future that can be distinguished from the correct one by observing $o3$ before $o1$. Since there is only one occurrence of the fault, then it is manifestable as well as strongly manifestable.

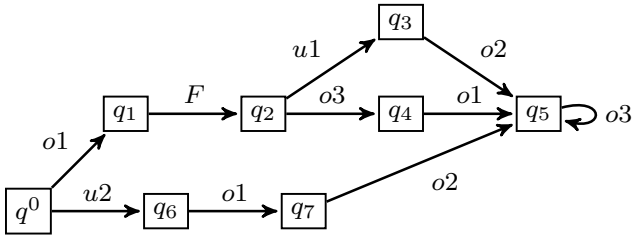

Fig. 1: System $Ex.2$ in Table 1..

1.2 ls_1 (similar ls_2)

The system ls_1 shown in Figure 2 is manifestable but not strongly manifestable neither diagnosable. The reason is that the fault from the initial state to q_1 has

one future (F u2 o1 o2 o1*) that can manifest itself from all correct trajectories. While the fault from the initial state to q_7 cannot manifest itself for each of its future trajectories. The system ls_2 in Table 1 has similar character as this one.

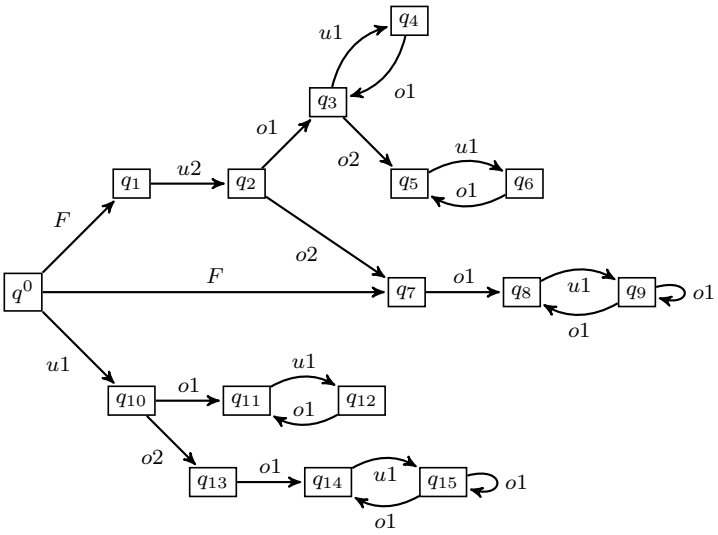

Fig. 2: System ls_1 in Table 1.

1.3 ls_3

The system ls_3 shown in Figure 3 is strongly manifestable but not diagnosable. Any faulty trajectory containing $o3$ manifests itself, i.e., is distinguishable from all correct trajectories, where there is no $o3$. However, the infinite faulty trajectory containing infinitely $o2$ has a corresponding correct trajectory with the same observations, thus non-diagnosable. Since there is only one occurrence of the fault event, thus it is manifestable as well as strongly manifestable.

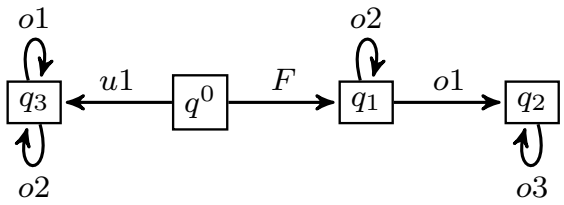

Fig. 3: System ls_3 in Table 1.

1.4 ls_4

In the system ls_4, depicted in Figure 4, the fault is strongly manifestable and non-diagnosable. For each occurrence of the fault, if the system executes the transition from q_4 to q_6 with $o6$, then it can always be distinguished from all correct trajectories, for which $o2$ must occur after $o3$ instead of $o6$. Thus, it is strongly manifestable. However, the faulty trajectory (u1 o1 o3 F o2 u1 (o4 o6 u2 u1 o2)*) has a corresponding correct one (u1 o1 o3 (u1 o2 o4 o6 u2 u1)*) with the same observation and thus the fault is not diagnosable.

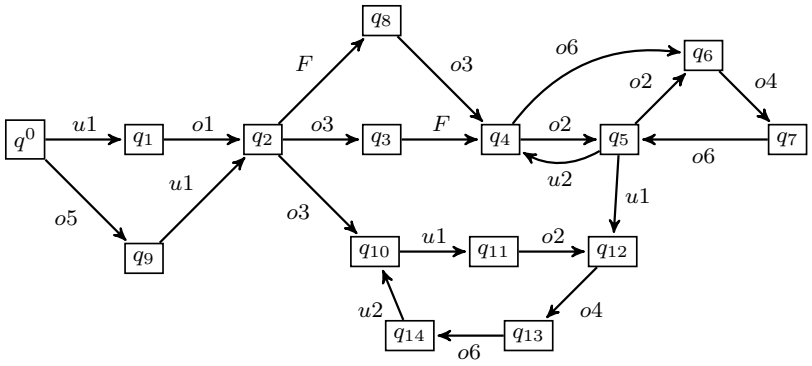

Fig. 4: System ls_4 in Table 1.

1.5 ls_5

The system ls_5, depicted in Figure 5, is diagnosable and thus (strongly) mani-

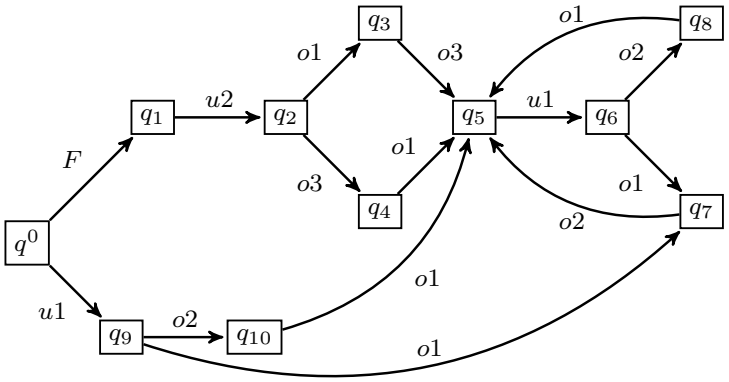

Fig. 5: System ls_5 in Table 1.

festable. After the fault occurrence, any infinite future must contain $o3$. However, for any infinite normal trajectory, there is no $o3$. Thus there is no critical pair in this system, which is thus diagnosable.

1.6 ls_6

The system ls_6, depicted in Figure 6, is not manifestable, thus non-diagnosable neither strongly manifestable. One can see that after any occurrence of fault, each future trajectory has always its corresponding correct one with the same observations. There is no chance at all to detect the fault occurrence whatever trajectory the system executes.

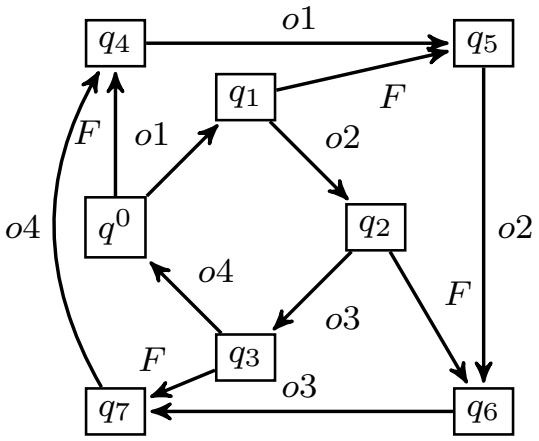

Fig. 6: System ls_6 in Table 1.

2 Table 2

Now we give the original systems in Table 2.

2.1 ex_{00} and ex_{01}

As described in the paper, the system ex_{00} (see Figure 7) is manifestable because the faulty trajectory that contains $o2$ can be distinguished from the normal trajectory by observing the event $o2$ within 3 time units after the occurrence of the observable event $o1$. Now, for the system ex_{01} (see Figure 8), we modify the guard on the transition from q_3 to q_5, such that the system becomes non-manifestable since each faulty trajectory has a corresponding correct one with the same observations.

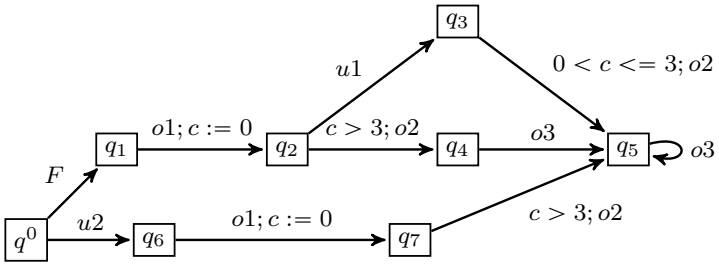

Fig. 7: System ex_{00} in Table 2.

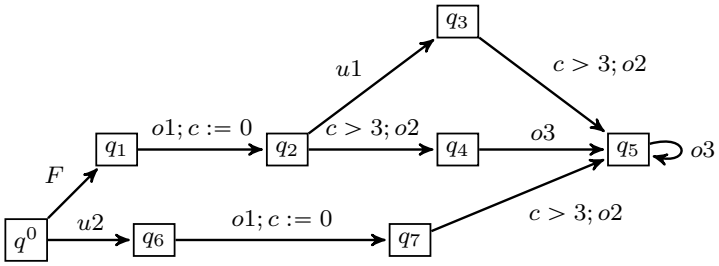

Fig. 8: System ex_{01} in Table 2.

2.2 ex_{10} and ex_{11}

The fault is manifestable in the system ex_{10} depicted in Figure 9 because the fault trajectory with at least two successive $o2$ without observing $o1$ can be distinguished from any correct one since, for the latter, the time between any two successive $o2$ must be smaller than 2 time units, different from the faulty one, where this time should be not smaller than 2 time units. To make this system non-manifestable, it suffices to modify the guard on the self transition of the state q_1, as shown in Figure 10 for the system ex_{11}.

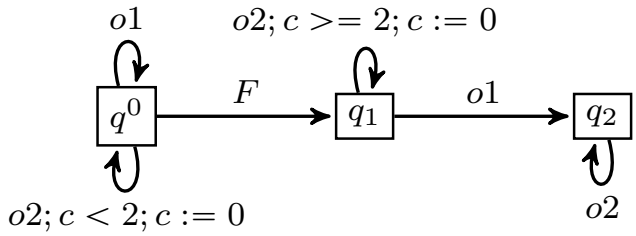

Fig. 9: System ex_{10} in Table 2.

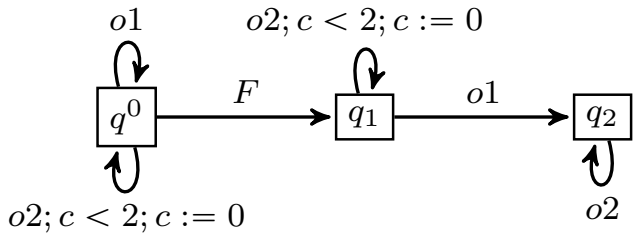

Fig. 10: System ex_{11} in Table 2.

2.3 ex_{20} and ex_{21}

In the system ex_{20}, depicted in Figure 11, the fault is manifestable because the faulty trajectory where the occurrence of $o3$ is before that of $o2$ is distinguishable from all correct ones, either by the order of $o2$ and $o3$ or by the different time between the occurrence of $o1$ and that of $o3$. Thus, to make it non-manifestable, one can modify the guard on the transition from q_3 to q_4, as depicted in Figure 12 for the system ex_{21}, such that all faulty trajectories have their corresponding correct ones with the same observations.

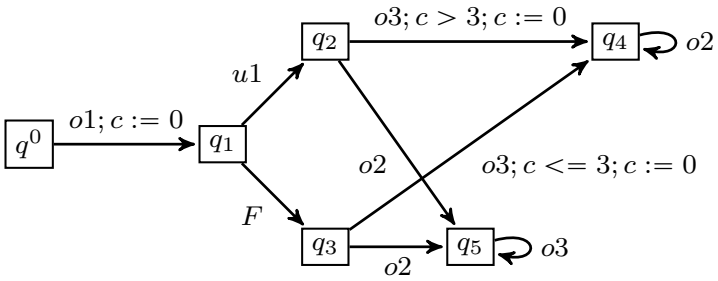

Fig. 11: System ex_{20} in Table 2.

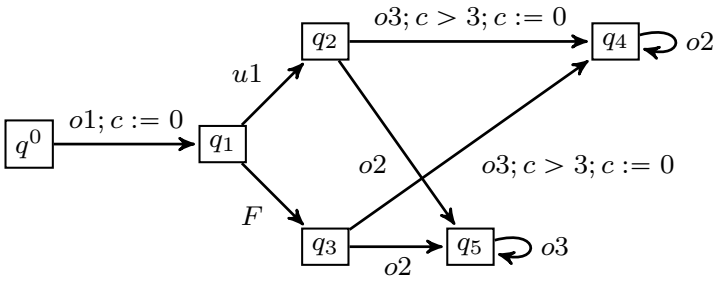

Fig. 12: System ex_{21} in Table 2.

2.4 Hand-crafted systems

The above original systems are quite small, which is often the case for literature examples. Thus to show the scalability of our algorithm, we now explain how we construct hand-crafted system shown in Table 2.

For those manifestable systems, we have written a script to generate subsystems without fault in an arbitrary way, which are then added to the original system in the following way:

- a subsystem can be added to a state reachable by a correct trajectory by adding a transition whose event is a new observable event.
- a subsystem can be added to a state up to which the fault must occur by adding a transition with any event.

In this way, one can easily prove that such a system remains manifestable because the distinguishable faulty trajectory in the original system keeps distinguishable.

As for the non-manifestable systems, one can add a subsystem generated in the same way as above to the original system in the following way: a subsystem can be added to any state up to which the fault has necessarily not occurred by adding a transition with any event. In this way, any faulty trajectory always has its corresponding correct one with the same observations. Hence, the system remains non-manifestable.