ECE 413: Senior Project Development II **Spring 2019**

S-TaLiRo Investigation

Student Name: Justin Patterson *Industry Sponsor: Galois Inc*

May 10, 2019

S-TaLiRo is a Matlab toolbox used for verification of a Cyber-Physical System Model. Unlike Kind2, where properties of a system are verified, S-TaLiRo performs a stochastic search of system trajectories that falsify a temporal logic specification [1]. The toolbox searches for paths with minimal robustness by using global optimization techniques which include the simulated annealing method, cross-entropy method, uniform sampling, and the genetic algorithm. The notion of a robustness metric is a measure of how satisfiable a trajectory is from the temporal specification. A positive robustness corresponds to a trajectory, along with a neighborhood of trajectories, that satisfies the specification, where as a negative robustness implies that the trajectory does not meet the specification [1].

Logical operators are *conjunction* ($\wedge$), *disjunction* ($\vee$), *negation* ($\neg$), *implication* ($\rightarrow$), and *equivalence* ($\leftrightarrow$). Common temporal operators are *eventually* ($\Diamond_{\mathcal{I}}$), *always* ($\Box_{\mathcal{I}}$), and *until* ($\mathcal{U}_{\mathcal{I}}$), where $\mathcal{I}$ is a timing constraint. If there is no timing constraint then the specification is a Linear Temporal Logic (LTL) formula; otherwise, it is a Metric Temporal Logic (MTL) formula.

In the latter, we present the verification of a discrete PID controller using S-TaLiRo. First, let us consider the system in Fig. 1.

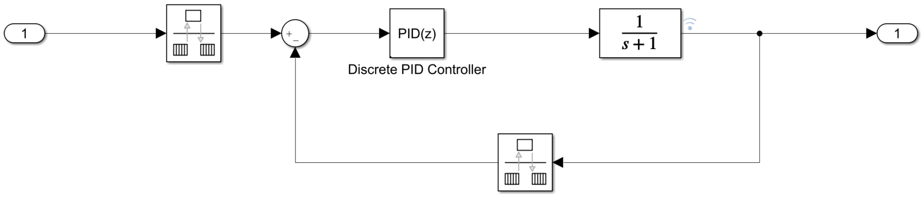
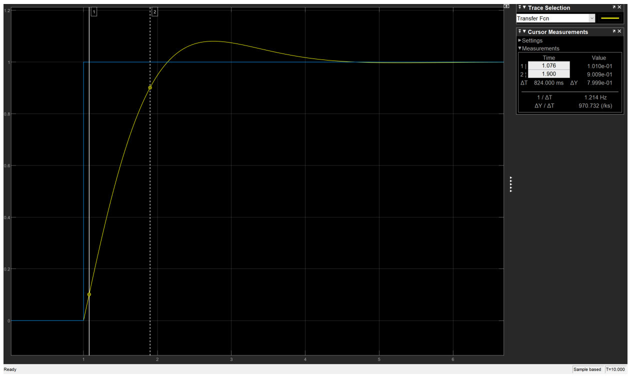


Figure 1: Simulink model of discrete PID controller cascaded with the plant. The plant has the transfer function $\frac{1}{s+1}$.



```
        Time        Value
1 |     1.076       1.010e-01
2 ¦     1.900       9.009e-01
ΔT  824.000 ms  ΔY  7.999e-01

    1 / ΔT          1.214 Hz
    ΔY / ΔT         970.732 (/ks)
```

Figure 2: Step of response of system. Note that the rise time of the output is approximately 0.8 sec.

Noting the rise time in Fig. 2, the MTL formula we want to falsify is

$$r_{10} \rightarrow \Diamond_{[0,0.1]} r_{90} \tag{1}$$

which reads as ”when the output is greater than 10% of the input, the output will be greater than 90% of the input some time between 0 and 0.1 seconds.”

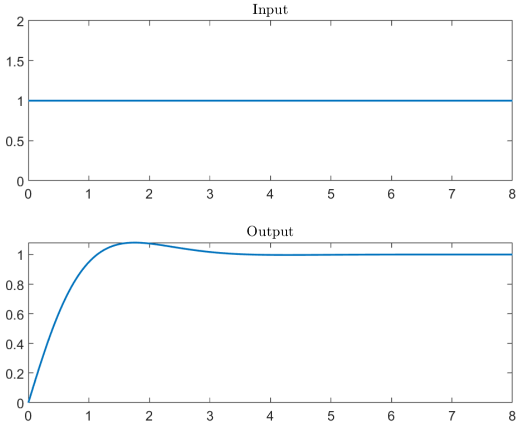


Figure 3: S-TaLiRo output

Although the S-TaLiRo output is similar to that in Fig. 2, the MTL formula was not falsified. We expect the formula to be falsified because the simulated rise time was found to be 0.82 seconds. The optimization method used was uniform random sampling for a total 100 tests. The best (minimum) robustness value was found to be 0.0029261 at a program run time of 203 seconds.

May 13, 2019

Using the *always* operator, the MTL formula was then changed to

$$\Box(r_{10} \rightarrow \Diamond_{[0.8,0.85]} r_{90}) \tag{2}$$

which reads ”it will always be true that when the output is greater than 10% of the input, the output will be greater than 90% of the input some time between 0.8 and 0.85 seconds.”

At a run time of 12.8655 sec, the best robustness was found to be -0.1659. Hence, the MTL formula was falsified. We expect the formula to be satisfied because the simulated rise time was found to be 0.82 seconds.

Experimenting with and without the *always* operator, the S-TaLiRo output contradicted the simulation for both cases.

References

[1] G. E. Fainekos, S. Sankaranarayanan, K. Ueda, and H. Yazarel, "Verification of automotive control applications using s-taliro," *American Control Conference*, 2012.