ITI8531 - Software Synthesis and Verification

LTL Assignment

A railroad wants to make a new controller for single-track railroad crossings. Naturally, they don't want any accidents with cars at the crossing, so they want to verify their controller. Their propositions include train_is_approaching, train_is_crossing, light_is_flashing, and gate_is_down.

Using natural English, these are some properties we'd like to have true:

1. Whenever a train passing, the gate is down.
2. If a train is approaching or passing, then the light is flashing.
3. If the gate is up and the light is not flashing, then no train is passing or approaching.
4. If a train is approaching, the gate will be down before the next train passes.
5. If a train has finished passing, then later the gate will be up.
6. The gate will be up infinitely many times.
7. If a train is approaching, then it will be passing, and later it will be done passing with no train approaching.

To formalize such statements, we would start with the primitive propositions involved. These could be:

1. **a** (a train is approaching the crossing)
2. **p** (a train is passing the crossing)
3. **l** (the light is flashing)
4. **g** (the gate is down)

Assignment:

1) Encode properties 1-7 in LTL, define inputs and outputs.
2) Solve it using Acacia+ tool.
3) Write a report and explain in natural language: a) properties 1-7 b) the result of Acacia+ tool.

Traffic Light Example (from Lily tool - https://www.iaik.tugraz.at/content/research/opensource/lily/)

We specify a small traffic light system for a crossing of a highway and a farm road. The systems has only two lights, which are either green or red. Signals hl and fl, which are output signals, encode these two lights. The highway light is green iff hl = 1, and similarly for the crossing farm road and fl. The input signal car indicates that a car is waiting at the farm road and timer represents the expiration of a timer. The specification assumes that the timer expires regularly. It requires that a green lamp stays green until the timer expires. Furthermore, one of the lamps must always be red, every car at the farm road is eventually allowed to drive on, and the highway lamp is regularly set to green.

Specification in LTL

```
G(F(timer=1)) -> (G(fl=1 -> (fl=1 U timer=1)) *
                   G(hl=1 -> (hl=1 U timer=1)) *
                   G(car=1 -> F(fl=1)) *
                   G(F(hl=1)) *
                   G(!(hl=1 * fl=1)));
```

Partition file

```
.inputs timer car
.outputs hl fl
```