COM 6854: Verification and Testing

Exercise Sheet 8

Exercise 1: Give examples for

(a) a safety property,

(b) a liveness property,

(c) a strong fairness property.

Formalise these properties in LTL.

Exercise 2: Give the LTL-semantics of the following operators.

(a) F^∞,

(b) G^∞,

(c) the *weak until* (or *unless*) operator U_w, such that $\phi U_w \psi$ holds iff ϕ holds as long as ψ does not (even if ψ never holds),

(d) the *before* operator B, such that $\phi B \psi$ holds iff whenever ψ holds in the future it must be strictly preceeded by an occurrence of ϕ.

Exercise 3: As mentioned in the lecture, LTL and CTL are incomparable with respet to expressivity. This exercise further analyses this fact.

(a) Consider a transition systems with states s_0, s_1 and s_2 and transition relation given by $s_0 \to s_0$, $s_0 \to s_1$, $s_1 \to s_2$ and $s_2 \to s_2$. Let proposition p hold in s_0 and s_2, but not in s_1. Argue that the LTL-formula FGp is satisfied by every path in the transition system starting with s_0. What about satisfiability of $AFAGp$ in CTL?

(b) Consider the following two LTS:

- $\mathcal{A}_1$ has states s_0^1, s_1^1, s_2^1, s_3^1 and transitions $s_0^1 \to s_1^1$, $s_1^1 \to s_2^1$, $s_1^1 \to s_3^1$. Propositions p and q hold in s_0^1, p holds in s_1^1, $\neg p$ holds in s_2^1 and q holds in s_3^1.
- $\mathcal{A}_2$ has states s_0^2, s_1^2, s_2^2, s_3^2, s_4^2 and transitions $s_0^2 \to s_1^2$, $s_0^2 \to s_1^2$, $s_1^2 \to s_3^2$, $s_2^2 \to s_4^2$. Propositions p and q hold in s_0^2, p holds in s_1^2 and s_2^2, $\neg p$ holds in s_3^2 and q holds in s_4^2.

Can LTL distinguish between $\mathcal{A}_1$ and $\mathcal{A}_2$? Which CTL-formula can distinguish between the two systems? In order to answer this question, find a formula that holds in one transition system, but not in the other.