15-424/15-624 Recitation 4: Invariants and Proofs
15-424/15-624 Foundations of Cyber-Physical Systems
Notes: Jan-David Quesel (jquesel+fcps@cs)

1. **Questions**

   (a) "What do open goals in KeYmaera mean?"

   Suppose you want to prove a property ϕ and using KeYmaera you get into a state where there are open goals labeled by ψ_1,...,ψ_n then you have proven that $\psi_1, \ldots, \psi_n \models \phi$. However, in order to prove that ϕ is valid you will have to eliminate the assumptions $\psi_1, \ldots, \psi_n$ by closing these goals.

   (b) "How to prove $\models x \leq y \vee x > y$?"

   Our base logic, first-order logic over the reals, is deciable. Thus, this question can be decided by quantifier elimination.

   (c) "KeYmaera hangs with MathKernel at 100% CPU"

   With the default settings KeYmaera uses Mathematica for quantifier elimination. This procedure is doubly exponential in the number of variables (in its current implementation) and at least doubly exponential in the number of quantifier alternations in theory. Thus, it might not finish within given time or memory bounds. In addition, for loops KeYmaera needs to find loop invariants which it will try to deduce automatically. However, as the problem of finding a loop invariant is undecidable it will not be able to find one in the general case. Thus, it might be stuck trying a hierarchy of "wrong" loop invariants.

2. **Sequent Calculus and Propositional Logic**

   We discussed two proofs for the theorem $A \to B \models [?A]B$. The first one uses a search heuristics that expands formulas on the right side of the sequent first. The second one applied rules to the formulas on the left first.

3. **Moving Point** Consider the following $\mathsf{d}\mathcal{L}$ formula:

$$
\begin{aligned}
(p = -4 \wedge x^2 < (4 * c)^2) \to [\ & (\text{if } \ (x > 0) \text{ then } a := p \\
& \qquad\qquad\qquad\quad \text{else } a := 4 \\
& \text{fi}; \\
& t := 0; \\
& \{x' = a, t' = 1, t \leq c\})^*](p = -4 \wedge x^2 < (4 * c)^2)
\end{aligned}
$$

   During the recitation we discussed a proof for this by hand and considered how to do this proof in KeYmaera. You can find the KeYmaera input files on the webpage.

4. **Quiz**

   Suppose you have a proof for the following $\mathsf{d}\mathcal{L}$ formula:

$$x = 5 \to [((x := 5; x := x + 1) \cup (x := x + 1; x := 5))^*](x = 5 \vee x = 6)$$

   Prove by hand using the calculus rules from the lectures that this formula is valid.