1 Quantifiers

\[
\begin{array}{c}
\frac{\Gamma, A \rightarrow B}{\Gamma \rightarrow A \supset B} \quad \triangleright R \\
\frac{\Gamma, A \supset B \rightarrow A}{\Gamma, A \supset B \rightarrow C} \quad \triangleright L \\
\frac{\Gamma \rightarrow A}{\Gamma \rightarrow A \wedge B} \quad \triangleright R \\
\frac{\Gamma, A \rightarrow C}{\Gamma, A \wedge B \rightarrow C} \quad \triangleright L \\
\frac{\Gamma \rightarrow A \lor B}{\triangleright R_1} \\
\frac{\Gamma \rightarrow B}{\triangleright R_2} \\
\frac{\Gamma, A \rightarrow C}{\Gamma, A \lor B \rightarrow C} \quad \triangleright L \\
\end{array}
\]

\[
\begin{array}{c}
\frac{\Gamma \rightarrow A(c)}{\Gamma \rightarrow \forall x.A(x)} \quad \forall R \\
\frac{\Gamma, \forall x.A(x), A(t) \rightarrow C}{\Gamma \rightarrow \forall x.A(x) \rightarrow C} \quad \forall L \\
\frac{\Gamma \rightarrow A(t)}{\Gamma \rightarrow \exists x.A(x) \rightarrow C} \quad \exists R \\
\frac{\Gamma, \exists x.A(x) \rightarrow C}{\Gamma, A(c) \rightarrow C} \quad \exists L
\end{array}
\]

**Task 1.** Prove the following formula in KeYmaera I (try to prove it by hand first to see the pattern).

\[p(z) \land (\forall x.p(x) \supset p(s(x))) \supset p(s^9(z))\]

**Solution 1:**

\[
\begin{array}{c}
\frac{p(z), \forall x.p(x) \supset p(s(x)), p(z) \supset p(s(z)) \rightarrow p(z)}{p(z), \forall x.p(x) \supset p(s(x)), p(z) \supset p(s(z)) \rightarrow p(s^9(z))} \quad \forall L \\
\frac{\Gamma, A(c) \rightarrow C}{p(z), \forall x.p(x) \supset p(s(x)), \forall x.p(x) \supset p(s(x)), p(s(z)) \rightarrow p(s^9(z))} \quad \forall L
\end{array}
\]

Where \(\varphi\) is:

\[
\begin{array}{c}
\frac{p(z), \forall x.p(x) \supset p(s(x)), p(s(z)) \supset p(s^2(z)) \rightarrow p(s(z))}{p(z), \forall x.p(x) \supset p(s(x)), p(s(z)) \supset p(s^2(z)) \rightarrow p(s^9(z))} \quad \forall L \\
\frac{\Gamma, A(c) \rightarrow C}{p(z), \forall x.p(x) \supset p(s(x)), p(s(z)) \supset p(s^2(z)) \rightarrow p(s^9(z))} \quad \forall L
\end{array}
\]

Observe how the sequent would not be provable if we erase the \(\forall\) formula on the left after instantiating it the first time.

**Task 2.** Can you think of a cut-formula that can make this proof shorter?
Solution 2: Cut-formula: \( \forall x.p(x) \supset p(s^3(x)). \)

\[
\frac{\varphi_l}{p(z), \forall x.p(x) \supset p(s(x)) \to \forall x.p(x) \supset p(s^3(x))}{\varphi_l}
\]

\[
\frac{\varphi_r}{\Gamma, p(z), \forall x.p(x) \supset p(s(x)) \to p(s^3(z))}{\text{cut}}
\]

Where \( \varphi_l \) is \( \{p(z), \forall x.p(x) \supset p(s(x))\} \):

\[
\frac{\Gamma, p(s^2(a)), \ldots \to p(s^2(a))}{\Gamma, p(s^2(a)), \ldots \to p(s^3(a))} \quad \frac{\Gamma, p(s^3(a)), \ldots \to p(s^3(a))}{\text{init}}
\]

\[
\frac{\Gamma, p(s^3(a)), \ldots \to p(s^3(a))}{\text{init}}
\]

And \( \varphi_r \) is \( \{p(z), \forall x.p(x) \supset p(s(x)), \forall x.p(x) \supset p(s^3(z))\} \):

\[
\frac{\Gamma, p(s^3(z)), p(s^3(z)) \supset p(s^3(z)) \to p(s^3(z))}{\text{init}}
\]

\[
\frac{\Gamma, p(s^3(z)), p(s^3(z)) \supset p(s^3(z)) \to p(s^3(z))}{\text{init}}
\]

Note that, using cuts, we only need to instantiate quantifiers 6 times, as opposed to 9 times in a cut-free proof.
2 Logic programming

You might be familiar with functional and imperative programming. Today we will see yet another programming paradigm: logic programming. Logic programming can be seen as a fragment of intuitionistic logic called Horn clauses (remember last homework?). A Horn clause is either an atom or a formula of the shape $A_1 \land \ldots \land A_n \supset H$, where $H$ is called the head and $A_1 \land \ldots \land A_n$ is the body. In prolog syntax, this is written as:

\[ h :- a_1, a_2, \ldots, a_n. \]

Let’s step through a simple prolog program to understand how computation (or proof search) works. Consider the following simple code:

\begin{align*}
\text{ocean\_level}(\text{rising}). \\
\text{temperature}(\text{extreme}). \\
\text{global\_warming}(\text{conspiracy}) & :- \text{ocean\_level}(\text{stable}), \text{temperature}(\text{normal}). \\
\text{global\_warming}(\text{real}) & :- \text{ocean\_level}(\text{rising}), \text{temperature}(\text{extreme}).
\end{align*}

If we query prolog for $\text{global\_warming}(X)$, it will look at the head of all (four) clauses trying to find one that “matches” (unifies) with the goal. In this case, it finds the clauses in lines 3 and 4. Prolog will process the options in order, so it will first go to clause in line 3 and unify $X$ with conspiracy, generating the new goals $\text{ocean\_level}(\text{stable})$ and $\text{temperature}(\text{normal})$. A proof-theoretic interpretation of this step is the following (predicate names are abbreviated for the sake of space):

\[
\frac{\text{ol(ris), temp(xtr), \ldots \rightarrow ol(sta) \quad ol(ris), temp(xtr), \ldots \rightarrow temp(nml)}}{\frac{\text{ol(ris), temp(xtr), \ldots \rightarrow ol(sta) \land temp(nml)}}{\frac{\text{ol(ris), temp(xtr), ol(sta) \land temp(nml) \supset gw(csp), ol(ris) \land temp(xtr) \supset gw(real) \rightarrow gw(X)}}{\frac{X \text{ is csp\quad gw(csp), \ldots \rightarrow gw(X)}}{\frac{\text{init\quad \supset L}}{\text{\rightarrow L}}}\frac{\text{\rightarrow L}}{\text{\rightarrow L}}}}
\]

In this derivation, $X$ is a special variable that is unified on initial rules, and this unification propagates to the next branch if there were occurrences of $X$ there as well. When trying to prove the two open sequents, or the new goals, prolog will realize that $\text{ocean\_level}(\text{stable})$ or $\text{temperature}(\text{normal})$ are not true... oops, are not in the context nor they are unifiable with any clause head. Time to backtrack. We know that $\land R$ is an invertible rule, so no use in backtracking there. We go back to the choice of clauses (i.e., $\supset L$) and try to use the one on line 4. This time the unification will be $X \text{ is real}$ and the new goals $\text{ocean\_level}(\text{rising})$ and $\text{temperature}(\text{extreme})$, which can be proved.

As a final note, logic programs hold some resemblance to functional programs in the way programs are written. You will find that sometimes the clauses used look a lot like the cases you would need in, say, SML. This kind of programming style is referred to as declarative programming (you write what your program does as opposed to how it does it).

**Task 3.** Implement a prolog program that computes the truncated subtraction between natural number along the same lines as the plus and times implementations given in the lecture notes.

**Solution 3:**
\[
\text{pred}(z, z). \\
\text{pred}(s(M), M). \\
\text{minus}(N, z, N). \\
\text{minus}(N, s(M), Q) :- \text{minus}(N, M, P), \text{pred}(P, Q).
\]

---

\[\text{It is also a fragment of classical logic. Since it is such a simple fragment, intuitionistic and classical logic coincide.}\]