Software Verification
Exercise: Separation Logic

In the lecture you have seen how separation logic can be used to prove

\{\text{tree } p\} \text{disptree}(p) \{\text{empty}\}

Now prove

\{\text{tree } \tau \ i\} \text{copytree}(i; j) \{\text{tree } \tau \ i \ast \text{tree } \tau \ j\}

where

\text{copytree}(i; j) =
\text{if } i = \text{nil} \text{ then }
\quad j := i
\text{else }
\quad \text{newvar } i_1, i_2, v, j_1, j_2 \text{ in }
\quad i_1 := [i];
\quad v := [i + 1];
\quad i_2 := [i + 2];
\quad \text{copytree}(i_1, j_1);
\quad \text{copytree}(i_2, j_2);
\quad j := \text{cons}(j_1, v, j_2);
\quad \text{end }
\quad \text{end }

Only a proof outline similar to the one in the lecture (i.e. assertion-annotated code) is required, since a detailed proof would be very large.