Formal Methods in Software Development
Exercise 1 (November 7)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

October 11, 2011

The result is to be submitted by the deadline stated above *via the Moodle interface* of the course as a *.zip or .tgz* file which contains

1. a PDF file with
   - a cover page with the course title, your name, Matrikelnummer, and email address,
   - a section for each part of the exercise with the requested deliverables and
   - a (nicely formatted) copy of the ProofNavigator file,
   - for each proof of a formula F, a readable screenshot of the RISC ProofNavigator after executing the command `proof` F,
   - an explicit statement whether the proof succeeded,
   - optionally any explanations or comments you would like to make;
2. the RISC ProofNavigator (.pn) file(s) used in the exercise;
3. the proof directories generated by the RISC ProofNavigator.

Email submissions are *not* accepted.

Exercise 1a: RISC ProofNavigator

Take the file "exercise1a.pn" and use the RISC ProofNavigator to prove the formulas A, B, and C in this file. The proofs only require the commands `scatter`, `split`, and `instantiate`.

For developing the proofs, you may also try `auto`; the submitted proofs, however, must *not* make use of the `auto` command. Please also try the repeated application of the command `flatten` (rather than `scatter`) to see the gradual decomposition of the proof.

Exercise 1b: Formalization

Develop in the RISC ProofNavigator a theory that formalizes each of the following statements as formulas $F_1, \ldots, F_6$.

1. If Superman were able and willing to prevent evil, he would do so.
2. If Superman were unable to to prevent evil, he would be impotent.
3. If Superman were unwilling to prevent evil, he would be malevolent.
4. Superman does not prevent evil.
5. If Superman exists, then he is neither impotent or malevolent.
6. Superman does not exist.

Use an atomic predicate like *superman*(x) to denote a statement like "x is superman" (you will need multiple such predicates). Statement 6 can be then formalized as $\neg\exists x : superman(x)$.

Prove in the RISC ProofNavigator the argument $F_1 \wedge F_2 \wedge F_3 \wedge F_4 \wedge F_5 \Rightarrow F_6$.

Exercise 1c: Verification Conditions

Derive the verification condition(s) for the Hoare triple

$\{n = oldn \wedge n \geq 0\}$

```
s = 0; i= 1;
if (i <= n) { s = s+i; i = i+1; }
if (i <= n) { s = s+i; i = i+1; }
```

$\{i \leq n + 1 \wedge (n < 1 \Rightarrow s = 0) \wedge (n = 1 \Rightarrow s = 1) \wedge (n > 1 \Rightarrow s = 3)\}$

i.e. the set of plain logic formulas whose validity implies the correctness of the Hoare triple.

Show each step of the derivation (not only the derived conditions).

Formalize the conditions in the RISC ProofNavigator (declaring integer constants `n:INT`, `oldn:INT`, etc) and prove them.