Formal Methods in Software Development
Exercise 1 (October 29)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

October 12, 2012

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: Predicate Logic Proofs

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 $F_1, \ldots, F_6$ as a boolean constant

1. All magors like sports and videogames.
2. Every womba likes dancing, unless (s)he likes singing.
3. Those who like sports don't like dancing.
4. Those who like singing don't like television.
5. Those who don't like television don't like videogames.
6. No magor is also a womba.

For instance, F_1 requires a definition

```
F1: BOOLEAN = ...;
```

To write the corresponding definitions, first introduce an undefined type T of objects

```
T: TYPE;
```

and, for each required property, an atomic predicate on T, e.g.,

```
magor: T->BOOLEAN;
```

You can then denote by the atomic formula `magor(x)` the statement "x is a magor".

Finally, define a formula

```
F: FORMULA F1 AND ... AND F5 => F6;
```

and prove it.

Exercise 1c: Verification Conditions

Derive verification condition(s) for the Hoare triple

$\{a = olda \wedge b = oldb \wedge x = oldx\}$

```
s = 0; i = 1;
if (a == x) { s = s+i; } i = i+1;
if (b == x) { s = s+i; } i = i+1;
```

$$\left\{\begin{array}{l} a = olda \wedge b = oldb \wedge x = oldx \wedge \\ (a \neq x \wedge b \neq x \Rightarrow s = 0) \wedge (a = x \wedge b \neq x \Rightarrow s = 1) \wedge \\ (a \neq x \wedge b = x \Rightarrow s = 2) \wedge (a = x \wedge b = x \Rightarrow s = 3) \end{array}\right\}$$

i.e. a 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). *Don't try to "guess" the condition(s) but derive them by application of the Hoare axioms respectively of the predicate transformer calculus!*

Formalize the conditions in the RISC ProofNavigator (declaring constants `a:INT`, `olda:INT`, etc) and prove them.