Computing and Software 734

Formalized Mathematics

Winter 2005

Exercises

Revised: February 8, 2005

For each of the IMPS exercises below, send the instructor an IMPS file (i.e., a file with a `.t` extension) that includes:

1. All the def-forms that you used.
2. Proofs for all the def-theorems in the file.
3. Comments of the form

   `;;;[`*comment*`]`

   expressing your experiences in doing the exercise. Most of your mark will be given on the basis of what your comments are.

For each of the PVS exercises below, send the instructor a PVS dump file (i.e., a file with a `.dmp` extension) that includes:

1. All the specification text that you used.
2. Proofs for all the theorems in the file.
3. Comments of the form

   `%%%[`*comment*`]`

   expressing your experiences in doing the exercise. Most of your mark will be given on the basis of what your comments are.

Exercise 1

Due: February 8, 2005.

1. With your fellow students choose one of the leading ITPSs (Coq, HOL, Isabelle/HOL, Isabelle/ZF, Mizar, Nuprl, or PVS) and then install it in the `group` directory of the account `cas734`.

2. Write individually a one-page paper that explains the reasons for your choice and lists, in your opinion, the major strengths and weaknesses of your choice.

Exercise 2

Due: March 1, 2005.

Do the IMPS indicators-exercise.

Exercise 3

Due: March 1, 2005.

Do the IMPS calculus-exercise.

Exercise 4

Due: March 1, 2005.

Formalize in PVS the following definitions, lemmas, and proofs (written by Henk Barendregt):

Let $\mathbf{N}$ be the set of natural numbers and P be the predicate on $\mathbf{N}$ defined by

$$\forall\, m : \mathbf{N}\,.\; P(m) \equiv \exists\, n : \mathbf{N}\,.\; 0 < m \wedge m^2 = 2n^2.$$

Lemma 1 $\forall\, m : \boldsymbol{N}\,.\; P(m) \supset \exists\, m' : \boldsymbol{N}\,.\; (m' < m \wedge P(m'))$.

Proof Indeed suppose $0 < m$ and $m^2 = 2n^2$. It follows that m^2 is even, but then m must be even, as odds square to odds. So $m = 2k$ and we have $2n^2 = m^2 = 4k^2$ which implies $n^2 = 2k^2$. Since $0 < m$, if follows that $0 < m^2$, $0 < n^2$, and $0 < n$. Therefore $P(n)$ holds. Moreover, $n^2 < n^2 + n^2 = m^2$, so $n^2 < m^2$ and hence $n < m$. So we can take $m' = n$. $\square$

Lemma 2 $\forall\, m, n : \boldsymbol{N}\,.\; m^2 = 2n^2 \supset m = n = 0$.

Proof By Lemma 1, $\forall m : \mathbf{N} \;.\; \neg P(m)$, since there are no infinite descending sequences of natural numbers. Now suppose $m^2 = 2n^2$ with $m \neq 0$. Then $0 < m$ and hence $P(m)$, which is a contradiction. Therefore, $m = 0$. But then also $n = 0$. □

Exercise 5

Due: March 1, 2005.

Do Exercise 4 in IMPS.

Exercise 6

Due: March 8, 2005.

Do the IMPS groups-exercise in PVS.

Exercise 7

Due: March 15, 2005.

Using Lemma 2 of Exercises 4, prove in PVS that the square root of 2 is irrational.

Exercise 8

Due: March 15, 2005.

Using Lemma 2 of Exercises 5, prove in IMPS that the square root of 2 is irrational.

Exercise 9

Due: March 22, 2005.

Starting from scratch, create an IMPS theory of Peano arithmetic called `peano1` with the constants 0, S, $+$, and $*$ and the following axioms:

1. 0 is not a successor.
2. S is injective.
3. Induction.

4. The two axioms that specify + recursively.

5. The two axioms that specify $*$ recursively.

Prove the following theorems in `peano1`:

1. 0 is the additive identity.

2. $S(0)$ is the multiplicative identity.

3. + is associative.

4. $*$ is associative.

5. + is commutative.

6. $*$ is commutative.

Create a compound macete that reduces any ground expression of `peano1` (i.e., any expression containing no variables and no constants other than 0, S, +, and $*$) to an expression of the form $S^m(0)$ (i.e., S applied to 0 m times). Give several examples expressed as theorems to show that it works.

Exercise 10

Due: March 29, 2005.

Create the following three interpretations:

1. An interpretation of `peano1` in `h-o-real-arithmetic`.

2. An interpretation of `commutative-monoid-theory` in the additive part of `peano1`.

3. An interpretation of `commutative-monoid-theory` in the multiplicative part of `peano1`.

Exercise 11

Due: April 5, 2005.

Do Exercise 9 in PVS.

Exercise 12

Due: April 5, 2005.

Do Exercise 10 in PVS.

Exercise 13

Due: April 12, 2005.

Starting from scratch, create an IMPS theory of Peano arithmetic called `peano2` with the constants 0 and S and the following axioms:

1. 0 is not a successor.
2. S is injective.
3. Induction.

Define $+$ and $*$ recursively in `peano2` using `def-recursive-constant`. Do Exercises 9 and 10 using `peano2` in place of `peano1`.