CS 773 Winter 2002

Exercise Set 2

Instructor: William M. Farmer

Revised: 4 March 2002

With the approval of the instructor, choose one of the following interactive theorem proving systems. (Each student will be required to choose a different system.)

(1) ACL2 (A Computational Logic for Applicative Common Lisp)

(2) Coq proof assistant

(3) Ergo interactive proof tool

(4) EVES tool

(5) HOL (Higher Order Logic) theorem prover

(6) Isabelle generic theorem prover

(7) LP (Larch Prover)

(8) Metamath Proof Explorer

(9) Mizar tool

(10) Nqthm (Boyer-Moore prover)

(11) Nuprl tool

(12) PhoX proof assistant

(13) PVS specification and verification system

(14) Theorema theorem prover

See

`http://www.cas.mcmaster.ca/~wmfarmer/CS-773-02/references.html`

for references. Install the system in your home directory on the department file system. Make the system accessible to the instructor and the students of the course.

Presentation 1

Due no later than 22-MAR-2002, required

After learning how to use the system, give a 10–15 minute presentation of the system to the class.

Exercise 2

60 pts., due no later than 22-MAR-2002, required

Formalize in your chosen system 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 $m' = n$. □

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 $n = 0$. □

Send the instructor the set of files that you produce. The files should be commented and should load in the system you chose to use. If it is not possible to formalize something in your chosen system, explain why. A partially completed exercise will be given an appropriate partial mark.

Exercise 3

50 pts., due no later than 5-APR-2002, optional

Starting from scratch, use your chosen system to formulate a theory M of monoids. Define an interval product operator in M that multiplies an interval of monoid elements. Prove the analogs in M of the following theorems in the IMPS theory of monoids:

(1) monoid-prod-out

(2) monoid-triv-prod

(3) monoid-null-prod

(4) locality-for-monoid-prod

(5) interval-multiplicativity

(6) translation-invariance

Extend M to a theory M' of commutative monoids. In M' prove that the interval product of a product is the product of two interval products (i.e, the analog of the IMPS theorem `monoid%prod-distributes-over-**`).

Send the instructor the set of files that you produce. The files should be commented and should load in your chosen system.

Presentation 2

Due no later than 5-APR-2002, required.

In a 10–15 minute presentation describe your experiences doing Exercises 2 and 3. Explain how your chosen system differs from IMPS.