UPPSALA UNIVERSITET
Matematiska institutionen
Erik Palmgren

LABORATORY EXERCISE, part 2
Tillämpad logik, ht-08
2008-11-27

Laboratory exercises, part 2

In this part we investigate a formalization in Coq of a theorem in combinatorics.

Definitions. Let U be a given set.

For a function $f : U \to U$ an element $t \in U$ such that $f(t) = t$ is called a *fixed point*.

A function $f : U \to U$ is said to be an *involution* for a subset $S \subseteq U$ if and only if the following two implications hold for any $x \in U$

(1) $x \in S \Longrightarrow f(x) \in S$,

(2) $x \in S \Longrightarrow f(f(x)) = x$.

The following theorem can be used to prove the existence of fixed points:

Theorem A. Let U be a given set and let S be a finite subset of U. Suppose that there exists a function $f : U \to U$ which is an involution on S and has exactly one fixed point in S. Then every involution on S has a fixed point in S.

One application is a proof of the classical number theoretic result that every prime number p of the form $4n + 1$ is the sum of two squares. (E.g. $17 = 4^2 + 1^1$, $29 = 5^2 + 2^2$). A very short proof of this fact was given by D. Zaiger[1] employing Theorem A: Let $U = \mathbb{N}^3$ and $S = \{(x, y, z) \in U : x^2 + 4yz = p\}$. He showed that there is an involution f on S with exactly one fixed point, under the assumption that p is a prime with $p \equiv 1 \pmod 4$ (see cited paper). Now $g(x, y, z) = (x, z, y)$ is easily checked to be an involution on S. By Theorem A there is $(x, y, z) \in S$ with $g(x, y, z) = (x, y, z)$. Thus $y = z$ and

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Thereby p can be written as a sum of squares.

The following lemmas prove Theorem A.

Lemma 1 Let $f : U \to U$ be an involution on $S \subseteq U$. For $s, t \in S$,

$$f(s) = f(t) \Longrightarrow s = t.$$

[1] American Mathematical Monthly 1990

Lemma 2 Let $f : U \to U$ be an involution on $S \subseteq U$. If $t \in S$, then f is an involution on $S \setminus \{t, f(t)\}$.

Lemma 3 For a subset A of U and $x, y \in U$,

$$A \setminus \{x, y\} = (A \setminus \{x\}) \setminus \{y\}.$$

Lemma 4 Let A be a subset of U and suppose $x \in A$. If A has cardinality $n + 1$, then $A \setminus \{x\}$ has cardinality n.

Lemma 5 Let $f : U \to U$ be an involution on finite set $S \subseteq U$. Suppose that S has cardinality n and that set of fixed points

$$F = \{t \in S : f(t) = t\}$$

has cardinality k. Then $n - k$ is an even number.

Corollary 6 Let $f : U \to U$ be an involution on finite set $S \subseteq U$. If the number of elements of S is odd, then f has a least one fixed point in S.

Now Theorem A follows since $f : U \to U$ has exactly one fixed point in S, then by Lemma 3, S must be odd. If now $g : U \to U$ is another involution on S, then g has at least one fixed point in S by Corollary 6.

Problems

The general goal is to formalize and prove as a much as possible of the above results in Coq.

We shall here use one particularly easy approach to the theory of sets in Coq: the theory of ensembles. An *ensemble* on a type U is simply a predicate P on that type. An element a of U is said to be *in* the ensemble P if $P\ a$ holds. The declarations are thus `U:Type` and `P: U -> Prop`. See the standard library of Ciq.

Start Coq and enter the following.

```
Section involution.
Require Import Coq.Sets.Constructive_sets.
Variable U:Set.

Definition Involution (S : Ensemble U)(f : U->U) : Prop :=
  (forall x: U, In U S x -> In U S (f x)) /\
  (forall x: U, In U S x -> (f (f x)) = x).
```

Problem 1. Prove the theorem in Coq:

```
Theorem Lm1: (forall S: Ensemble U,
              forall f: U -> U,
              Involution S f ->
              forall x y:U,
              (In U S x) -> (In U S y) -> (f x) = (f y) -> x = y).
```

Problem 2. Prove in Coq:

```
Theorem Lm2: (forall S: Ensemble U,
              forall f: U -> U,
              forall x:U,
              Involution S f ->
              (In U S x) ->
                    Involution (Setminus U S (Couple U x (f x))) f).
```

Problem 3. Formulate and prove Lemma 3 above in Coq.

Problem 4. Prove Lemmas 4 and 5 and Corollary 6 above by hand using standard set theory.

Problem 5. Try to devise a strategy for formalising your work in Problem 4 in Coq using the below notion of cardinality and cardinality induction. You may use the standard library of Coq and classical reasoning (law of excluded middle). It may be necessary to revise your orginal proof to adapt to facts that are available in the library.

```
 Inductive cardinal : Ensemble U -> nat -> Prop :=
    | card_empty : cardinal (Empty_set U) 0
    | card_add :
      forall (A:Ensemble U) (n:nat),
        cardinal A n -> forall x:U, ~ In U A x -> cardinal (Add U A x) (S n).

Coq < Check cardinal_ind.

cardinal_ind
     : forall (U : Type) (P : Ensemble U -> nat -> Prop),
       P (Empty_set U) 0 ->
       (forall (A : Ensemble U) (n : nat),
        cardinal U A n ->
        P A n -> forall x : U, ~ In U A x -> P (Add U A x) (S n)) ->
       forall (e : Ensemble U) (n : nat), cardinal U e n -> P e n
```

Problem 6*. (Optional) Carry out the above sketch as a Coq proof. Try to avoid classical reasoning, by making extra assumptions in Lemma 5 and Corollary 6 that = on U is decidable and that membership of S is decidable, i.e.

```
(forall x y:U, x = y \/  ~ (x = y))

(forall x:U, (In U S x) \/  ~ (In U S x)).
```

———+———