Lab Session 1
The Coq Proof Assistant

Construction and Verification of Software

Nova School of Science and Technology
Mário Pereira `mjp.pereira@fct.unl.pt`

Version of September 15, 2024

The main purpose of this lab session is for you to get the first feeling of the Coq proof assistant. The exercises from this lab session are inspired by the first chapter of *Software Foundations, Volume 1*: `https://softwarefoundations.cis.upenn.edu/lf-current/Basics.html`. I strongly recommend you to read this chapter and go trough the remaining exercises.

1 Proof by Simplification

1.1 Boolean Values

Consider the following definition of Boolean values in Coq:

```
Inductive bool : Type :=
  | true
  | false.
```
Coq

Exercise 1. Give definitions for the following functions:

- `negb`, Boolean negation
- `andb`, Boolean conjunction
- `orb`, Boolean disjunction

□

Exercise 2. Prove the following lemma:

```
Lemma unfold_andb: ∀ b1 b2: bool,
  andb b1 b2 = if b1 then b2 else false.
```
Coq

□

Exercise 3. Prove the following lemma:

```
Lemma andb_true_b: ∀ b: bool,
  andb true b = b.
```
Coq

□

Exercise 4. Prove the following lemma:

```
Lemma andb_false_b: ∀ b: bool,
  andb false b = false.
```
Coq

□

1.2 Natural Numbers

Consider the following definition of natural numbers in Coq:

```
Module NatPlayground.
  Inductive nat : Type :=
    | O
    | S (n: nat)
```
Coq

Exercise 5. Give definitions for the following functions:

- `plus`, addition of two natural numbers
- `mult`, multiplication of two natural numbers

□

Exercise 6. Prove the following lemma:

```
Lemma plus_O_n: ∀ n: nat,
  plus O n = n.
```
Coq

□

Exercise 7. Prove the following lemma:

```
Lemma mult_O_l: ∀ n: nat,
  mult O n = O.
```
Coq

□

2 Proof by Rewriting

Exercise 8. Prove the following lemma:

```
Lemma plus_id: ∀ n m: nat,
  n = m →
  plus n n = plus m m.
End NatPlayground.
```
Coq

□

Exercise 9. Prove the following lemma:

```
Lemma mult_n_O_m_O: ∀ p q: nat,
  plus (mult p O) (mult q O) = O.
```
Coq

□

Exercise 10. Prove the following lemma:

```
Lemma mult_n_1: ∀ n: nat,
  mult n (S O) = n.
```
Coq

□

3 Proof by Case Analysis

3.1 Boolean Values

Exercise 11. Prove the following lemma:

```
Lemma andb_b_false: ∀ b: bool,
  andb b false = false.
```
Coq

□

Exercise 12. Prove the following lemma:

```
Lemma negb_involutive: ∀ b: bool,
  negb (negb b) = b.
```
Coq

□

Exercise 13. Prove the following lemma:

```
Lemma andb_commutative: ∀ b c: bool,
  andb b c = andb c b.
```
Coq

□

Exercise 14. Prove the following lemma:

```
Lemma andb_true_elim: ∀ b c : bool,
  andb b c = true →c = true.
```
Coq

□

Exercise 15. Prove the following lemma:

```
Lemma students_favorite: ∀ b : bool,
  b = if b then true else false.
```
Coq

□

3.2 Natural Numbers

Exercise 16. Give definitions for the following function:

- `eqb`, equality between two natural numbers

□

Exercise 17. Prove the following lemma:

```
Lemma plus_1_neq_0: ∀ n: nat,
  eqb (plus n (S 0)) 0 = false.
```
Coq

□