1 Coq

1.1 Introduction

Coq is a proof assistant, built around the Curry-Howard correspondance and the "Calculus of Constructions" (CoC).

CoC can serve as a constructive basis for mathematics—every proof is constructive in nature. Not only do proofs prove that objects exist, or that properties hold, they also gave you examples of the objects for which the property holds, or a counter example if it does not.

The usual formulation leads to the loss of the Law of the Excluded Middle, among other things, though you are free to define addition axioms if you wish. The downside of this is that many proofs will be non-constructive.

One of the major advantages of Coq and constructive proofs, is (in theory), having defined a program and proven it correct in Coq, you can then extract an executable (usually in OCaml or Haskell), which you can be completely assured will run as specified.

Below we give a brief introduction to the calculus of constructions and a simple example of a proof.

1.2 Terms

A term is one of the following:

- `Type`
- `Prop`
- A variable, like x, y, etc.
- If A and B are terms, then so is $A\ B$ (B applied to A).
- If A and B are terms, and x is a variable, then so are $\forall x : A.B$ and $\lambda x : A.B$.

1.3 Judgements

There is one central judgement: the *typing* judgment.

These are of the following form:

$$x_1 : \tau_1, x_2 : \tau_2, \ldots \vdash y : \tau'$$

1.4 Inference Rules

1.4.1 True

$$\frac{}{\Gamma \vdash \texttt{True} : \texttt{True}}$$

1.4.2 Identity

Below, let K be either `Prop` or `Type`.

$$\frac{\Gamma \vdash A : K}{\Gamma, x : A \vdash x : A}$$

1.4.3 Functions

$$\frac{\Gamma, x : A \vdash B : K \quad \Gamma, x : A \vdash N : B}{\Gamma \vdash (\lambda x : A.N) : (\forall (x : A).B) : K}$$

1.4.4 Universal Quantification

$$\frac{\Gamma \vdash M : \forall (x : A).B \quad \Gamma \vdash N : A}{\Gamma \vdash M\ N : B[x := N]}$$

Corresponds to:

$$\frac{A \Rightarrow B, A}{B} \text{ or } A \wedge (A \Rightarrow B) \Rightarrow B$$

1.4.5 Equality

$$\frac{\Gamma \vdash M : A \quad A = B \quad B : K}{\Gamma \vdash M : B}$$

1.5 Definitions

1.5.1 Equality of Values

$$\frac{}{\Gamma \vdash \texttt{eq\_refl} : x = x}$$

Corresponds to:

$$\frac{}{A = A}$$

1.5.2 False

$$\frac{\Gamma \vdash t : \texttt{False}}{\Gamma \vdash x : \tau}$$

This allows us to establish "not" as follows:

$$\frac{\Gamma \vdash p : \tau \to \texttt{False}}{\Gamma \vdash \text{not}(p) : \ \sim \tau}$$

1.5.3 Conjunction

Introduction:

$$\frac{\Gamma \vdash A : K \quad B : K \quad x : A \quad y : B}{\Gamma \vdash \texttt{conj}\ x\ y : A \wedge B}$$

Elimination:

$$\frac{\Gamma \vdash A : K \quad B : K \quad \texttt{conj}\ x\ y : A \wedge B}{\Gamma \vdash x : A} \text{ and } \frac{\Gamma \vdash A : K \quad B : K \quad \texttt{conj}\ x\ y : A \wedge B}{\Gamma \vdash y : B}$$

1.5.4 Existence

$$\frac{\Gamma \vdash \exists x, \varphi(x), \Gamma \vdash \varphi : \tau \to \texttt{Prop}}{\Gamma \vdash x : \tau, \Gamma \vdash \varphi(x) : \texttt{Prop}}$$

1.6 Sample Proof

Consider the following proposition:

$$\frac{A, B, A \wedge B \Rightarrow C}{C}$$

To encode this in Coq we can write:

```
Lemma lemma : forall (A B C : Prop), A -> B -> (A /\ B -> C) -> C.
Proof.
intros A B C.
intros HA HB Prf.
(* HA : A *)
(* HB : B *)
(* conj HA  HB : A /\ B *)
(* Prf : A /\ B -> C *)
exact (Prf (conj HA HB)).
Qed.
```

An alternative using "normal" functions:

```
Definition lemma (A B C : Prop) (HA : A) (HB : B) (Prf : A /\ B -> C) : C :=
    Prf (conj HA HB).
```

In Haskell:

```
lemma :: a -> b -> ((a,b) -> c) -> c
lemma a b prf = prf (a,b)
```

Finally, formalled derived using the inference rules above:

$$\frac{\frac{\Gamma \vdash x:A \quad y:B}{\Gamma \vdash \texttt{conj}\ x\ y:A \wedge B} \quad \Gamma \vdash p : (\forall x : A \wedge B.C)}{\Gamma \vdash p\ (\texttt{conj}\ x\ y) : C}$$

2 Axiomatic Euclidean Geometry

2.1 Notions

- One of the most pervasive concepts in Euclidean geomtry is *length*, though no such thing is formally defined. We define `Length : Type` as a parameter to our Module which is an ordered field.
- The second notion is that of a *point*. Again, this is abstractly defined by a parameter `Point : Type`.
- A *line segment* is defined by two points.
- Critical to our proof are circles, which we define as sets containing `Point`. While they are defined in the list of "Notions", we redefine circles as sets of points because this definition is more convenient. We also define/postulate the following related concepts:
  - Every circle contains at least one point—there is no such thing as an "empty" circle, though circles of a single point are allowed.
  - For every circle, there is some point which we call its *center*.
  - Every circle has an associated length called its *radius*.
  - *A radius* (not to be confused with **the radius** of a circle), is a line segment starting at the center of the circle and ending somewhere on the circle.
  - Every radius has the same length.
  - In particular, a single point defines a radius if and only if it's distance to the center is the same as some other radius.
- An equilateral triangle is a set of triangle (distinct) points such that the distances between any two is the same.
- Two circles centered at different points will *intersect* at either two points, if the sum of their radiuses is less than the length of the line segment connecting their centers; if not, they intersect at zero points. When we say two circles intersect, we are speaking of the sets of points which define them.

2.2 Axioms

Following Euclid, we define the following axioms. Note that several have been left out, as they are not needed by our proof.

- We combine postulate 1 and postulate 2, since we are concerned only with line segments into the following axiom:

  Axiom 1. *For any two points a and b, there is a line segment, (a, b), connecting the two points.*

Note we postulate also that the length of (a, b) is the same as the length of (b, a).

- We replace postulate 3 with the following:

  Axiom 2. *Any two points define a circle, with one of them at the center of the circle and the other on the circle—the line segment defined by these two points is a radius of the circle.*

3 Propositions

3.1 Lemmas

We begin by proving some lemmas establishing basic facts that are necessary to prove anything more complicated.

Lemma 1. *Every circle has a line segment called it's radius.*

Proof. Follows from the postulate that there is no empty circle. □

Lemma 2. *If the length from the center of a circle to some point is the radius of the circle, then that point defines a radius of the circle.*

Proof. Call the point a and the circle c.

We need to show that (center c, a) is a radius of c: that is, it starts at the center of the circle and a is on the circle. The first part is obvious.

The second follows from Lemma 1, the postulate that all radiuses have the same length, and that a line segment is a radius if and only if it's length is the same as that of the circle. □

Lemma 3. *If a point defines a radius of some circle, then the length of the line segment connecting the point and the center of the circle is the radius of the circle.*

Proof. The lemma is the same as the previous, except in the opposite direction. It's proof is therefore quite similar—it follows from the same lemmas and propositions. □

Lemma 4. *Any two distinct points define two circles, which intersect at precisely two points.*

Proof. Let the two points be a and b.

Applying Axiom 2 twice, we obtain the two circles c_1 and c_2, where c_1 is center at a and c_2 is centered at b.

The fact that their centers are not equal follows from the assumption of distinctness of a and b. This allows us to apply the postulate that these two circles either intersect at two points, or no points at all. Recall that two circles intersect at two points when the distance between them is less than the sum of their radiuses.

The distance between the centers of the circles is given by $|(a, b)|$, which is also the radius of the one of the circles (in fact, the radius of both circles, but this fact is unimportant). Because the distance is the same as the radius of one of the circles, plus some additional length, we can conclude that the circles are close enough, and therefore intersect at two points. □

Lemma 5. *The two circles defined by two distinct points have the same radius.*

Proof. This essentially follows from the fact that all radiuses have the same length, and that $|(a, b)| = |(b, a)|$. □

Lemma 6. *If two circles have the same radius, then any two radiuses of the circles have the same length.*

Proof. This also follows from the fact that any radius of a circle has length equal to the radius of the circle. The rest follows from transitivity of equality. □

3.2 Proposition 1

Finally, we may state and prove the first proposition in the book:

Proposition 1. *Any two distinct points defines at least one equilateral triangle: that is, there is some equilateral triangle whose sides have the same length as the length of the line segment connecting the two points.*

Proof. By Lemma 4, any two points define two circles, which intersect at precisely two points. Call these two points a and b. We may arbitrarily pick either point, which will serve as the third point in our equilateral triangle. Call the chosen point x.

This point x is in both circles, so it forms a radius of both circles. Therefore, the distance from a to x is the same as the distance from b to x, by Lemma 6.

Finally, the distance between a and b is the same as the distance from a to x and b to x because they are all radiuses of congruent circle. □