Proofs are Programs

Tactics

Organisational

- The exercise group on Monday will become "on-demand"

  - If you would like to make use of it please write a direct message on Moodle (to Sebastian & Maxi)

- Midterm on May 23rd, 12:45 -13:45 (room to be announced)

  - Registration on Moodle

Short Recap

Polymorphism

```
Inductive list (X:Type) : Type :=
  | nil
  | cons (x : X) (l : list X).
```

Higher-order functions

```
Fixpoint filter {X:Type}
    (test: X->bool)
    (l:list X) : list X :=
…
```

Anonymous Functions

```
fun n => n * n
```

Functions that construct functions

```
Definition constfun {X: Type} (x: X)
    : nat -> X :=
  fun (k:nat) => x.
```

Applying Hypotheses

- General logical principle: if P and $P \to Q$ hold then also Q holds

- In other words: for showing Q if $P \to Q$ is known then it is sufficient to show P

- In particular: for showing P if P is known then there is nothing left to show (because P is equivalent to True $\to P$)

- Also: for showing $Q(c)$ if $\forall x \,.\, P(x) \to Q(x)$ is known then it is sufficient to show $P(c)$

Properties of Constructors

- Constructors need to be **injective**

  - A function f is injective if $\forall xy \, . \, f(x) = f(y) \rightarrow x = y$

- Constructors need to be **disjoint**

  - Functions f and g are disjoint if $\forall xy \, . \, f(x) \neq g(y)$

- Constructors are functions (and, hence **functional**)
  $\forall xy \, . \, x = y \rightarrow f(x) = f(y)$

Quiz 1

Suppose Coq's proof state looks like

```
x : bool
y : bool
H : negb x = negb y
==============================
 y = x
```

and we apply the tactic `injection H as Hxy`. What will happen?

1) "No more subgoals."

2) The tactic fails.

3) Hypothesis `H` becomes `Hxy : x = y`.

4) None of the above.

Quiz 2

Now suppose Coq's proof state looks like

```
x : nat
y : nat
H : x + 1 = y + 1
==============================
  y = x
```

and we apply the tactic `injection H as Hxy`. What will happen?

1) "No more subgoals."

2) The tactic fails.

3) Hypothesis `H` becomes `Hxy : x = y`.

4) None of the above.

Quiz 3

Finally, suppose Coq's proof state looks like

```
x : nat
y : nat
H : 1 + x = 1 + y
==============================
  y = x
```

and we apply the tactic `injection H as Hxy`. What will happen?

1) "No more subgoals."

2) The tactic fails.

3) Hypothesis `H` becomes `Hxy : x = y`.

4) None of the above.

Modifying Hypotheses

Strengthening the Induction Hypothesis

$$\forall nm . \text{ double } n = \text{double } m \rightarrow n = m$$

```
Fixpoint double (n:nat) :=
  match n with
  | O => O
  | S n' => S (S (double n'))
  end.
```

Unfolding Definitions

Case Analysis on Compound Expressions

Summary

Applying lemmas and hypotheses

```
apply

apply … with (x:= …)
```

Exploiting properties of constructors

```
injection … as …

discriminate
```

Generalising inductive hypotheses

```
generalize dependent
```

Other tactics

```
symmetry

transitivity

unfold
```