Modularity & Overloading
From Mathematical Structures to Monadic Programming
MPRI 2-7-2, lecture 7

Bruno Barras, Matthieu Sozeau

February 7th 2022
Recall from lecture 6

- Dependently-typed programming and extraction
- Working with subset types and inductive families
Today

1. Mathematical Structures
   - Record Types
   - Exercise

2. Elaboration: Coercions, Unification and Implicit Arguments
   - Coercions
   - Exercise

3. Type Classes and Modular Developments
   - Modules vs Type Classes in Coq
   - Type Classes in theory
   - Type Classes in practice
   - Variations on type classes
   - Additional exercises

Goal: familiarize yourself with records and generic formalization techniques along with the elaboration features of Coq.
Record Types

Record \( R \) (\( A : \text{Type} \)) : \( s \) :=
{ \( fl : \text{tau}_1; ..; fn : \text{tau}_n \) }.

Inductive \( R \) (\( A : \text{Type} \)) : \( s \) :=
Build_R (\( fl : \text{tau}_1 \)) .. (\( fn : \text{tau}_n \)) : \( R \ A \).

No indices, no recursion

Projection is pattern-matching

Definition \( fi \) (\( A : \text{Type} \)) (\( r : R \ A \)) : \text{tau}_i[fi \ r/fi] :=
match \( r \) with Build_R \( t1 \) .. \( tn \) => \( ti \) end.
Records II

- **Definitional Equality:**
  \[ f_1 \text{(Build}_\text{rec} \ t_1 \ldots t_n) \rightarrow_{\beta\delta\eta} t_i \]

- **No \( \eta \) law:**
  \[ \text{Build}_R \ (f_1 \ t) \ldots (f_n \ t) \equiv_{\beta\delta\eta} t \] **is not valid** (unless using primitive projections).

- Only derivable for Leibniz equality.

An example declaration:

```coq
Record positive := { pos_nat : nat; pos_proof : 0 < pos_nat }.
```

**Coq defines:**

```coq
pos_nat : positive -> nat
pos_proof : forall (p : positive), 0 < pos_nat p
```
Warm-up demo:

- Define the dependent pair type (aka. sigma types for \( A : \text{Type} \) and \( P : A \to \text{Type} \)) as a record.

- Prove the \( \eta \) rule (surjective pairing) for it.

- Define \( \mathbb{Q} \) as a record of two integers.

- Define the equivalence of two rationals as a proposition.

- Define addition of two rationals and show that it respects the equivalence (on pairwise equivalent arguments, it gives equivalent results).
Mathematical Structures

- **Defining composite structures as first-class objects:***

  ```
  Record monoid := { carrier : Type; unit : carrier;
  op : carrier -> carrier -> carrier;
  left_unit : forall x, op x unit = x; ... }.
  ```

- **Generic programming for any monoid:***

  ```
  Definition monsquare (m : monoid)
  (x : carrier m) : carrier m := op m x x.
  ```

  **Type and value dependency** is essential to make this typecheck.
Mathematical Structures Exercise (20 min)

- Define the full interface of a monoid given partially above.
- Define the \((0, +)\) and \((1, \star)\) monoids on \(\mathbb{N}\). You can use `lia` to solve the goals for laws. \((\text{Require Import Lia first})\)
- Define a generic exponentiation operation \(a^n\) where \(n : \mathbb{N}\) and \(a\) is in a monoid.
- Show that the exponentiation of the unit is always equal to the unit.
Elaboration

Type theory is **verbose**: use an elaboration from source syntax ("expressions") to core terms.

- **User-syntax**: $[3 :: 1]
- **Low-level terms**: \((\texttt{cons}, [\texttt{nat}; (\texttt{S}, [\texttt{S}, [\texttt{S}, \texttt{O}]])])); (\texttt{cons}, [\texttt{nat}; (\texttt{S}, \texttt{O})])\)

To tame this:

- **Notations**: abbreviations of combined terms and a complex **parser**. User-extensible, e.g.:

  Notation ""$\Sigma$’ x .. y , P" := (sigma (fun x ⇒ .. (sigma (fun y ⇒ P)) ..))

- **Coercions**: implicit casting of one type into another
- **Terms with holes** (aka existential variables) and unification
Coercions

Record monoid := { carrier : Type;
    unit : carrier; op : carrier -> carrier -> carrier }.

Generic programming for any monoid:
Coercion carrier : monoid --> Sortclass.

Compare: without the carrier coercion:

Definition monsquare (m : monoid)
    (x : carrier m) : carrier m := op m x x.

With the carrier coercion:

Definition monsquare (m : monoid)
    (x : m) : m := op m x x.

- The term \( m \) is coerced to a sort (its carrier) in the types.
- Closer to informal mathematical notation
Coercions

- Coercions are not displayed (by default, see `Set Printing Coercions`)
- The actual core term is the same as before
- Coherence of coercions (only one path up to conversion between two types) and decidability ensured by a syntactic check.
- Uses: types embedded in records, injections (i.e. from \( N \) to \( Z \)), modeling a subtyping relation...

```
Coercion Z_of_nat : nat --> Z.
```
Define the coercion from \texttt{nat} to \texttt{bool}, sending 0 to \texttt{false} and everything else to the \texttt{true} constructor.

Define the converse coercion from \texttt{bool} to \texttt{nat}, giving value 1 to \texttt{true}.

Show that \texttt{bool} $\rightarrow$ \texttt{nat} $\rightarrow$ \texttt{bool} is the identity (pointwise)

Which one makes more sense as a coercion?
Exercise

Unification

Add a new term former and environment to the calculus: existential variables / metavariables.

\[(X : \Delta \vdash \tau) \in \Sigma\]
\[\Sigma; \Gamma \vdash \sigma : \Delta\]
\[\Sigma; \Gamma \vdash ?X[\sigma] : \tau[\sigma]\]

- Existential variables are shared among a global state $\Sigma$ that declares their types and optionally, their instance.
- $\sigma$ is a substitution for the variables of the existential $(\Delta)$.

Example:

Goal $\forall (x : \text{nat}), \exists y, x < y$.

Proof.

`eexists.`

`(* x : nat` `--------------------------` `x < ?y[x] *)`
Existential variables can be instantiated by well-typed instances:

\[(X : Δ ⊢ τ) ∈ Σ \]
\[Σ; Δ ⊢ t : τ\]
\[Σ[X := t : Δ ⊢ τ]; Γ ⊢\]

Example:

\[\text{Goal } \forall (x : \text{nat}), \exists y, x < y.\]
\[\text{Proof.}\]
\[\text{eexists.}\]
\[\text{instantiate } (1 := S x).\]
\[(x : \text{nat}\]
\[\text{-------------}\]
\[\text{x < S x *})\]

\textbf{BEWARE}: the instance is typed in the context of the existential, NOT the current goal.
Unification

Once we have existential variables we can formalize unification:

\[ \Sigma; \Gamma \vdash t \equiv u \Rightarrow \Sigma' \]

Informally: match-up terms \( t \) and \( u \), assigning holes in one term with the corresponding subterm of the other one, producing an instantiation in \( \Sigma' \).

Using first-order heuristics:

\[ f ?x \equiv f y \Rightarrow ?x := y \]

Up to reduction:

\[ 1 + ?x \equiv 4 \Rightarrow ?x := 3 \]

Not up to equations:

\[ ?P \land Q \land R \equiv R \land Q \land S \not\Rightarrow \]
Unification II

- Is a congruence over all the term/type formers
- Includes $\beta\delta\iota\zeta\mu\nu$-conversion: makes it powerful but also unpredictable sometimes
- Includes instantiation:

$$\Sigma; \Gamma \vdash \exists X[\sigma] \simeq t \iff \Sigma[X := t[\sigma^{-1}]]$$

(under some conditions, notably an occurs-check).

- Is undecidable outside 1st order and pattern fragments ("simple" unification problems). Huet’78: The Undecidability of Unification in Third Order Logic.
Unification for tactics

Unification is at the basis of most tactics. Let’s look at `apply`:

- Assume goal $\Gamma \vdash G$, and lemma $l : \forall x : A, C x \rightarrow B x$.
- `apply l` builds $l (?a[id_\Gamma] : A)(?c : C ?a[id_\Gamma]) : B ?a[id_\Gamma]$
- Tries to unify $B ?a[id_\Gamma]$ with $G$.
- If it succeeds, filling $?a$ with some term $t$, it generates a goal $C ?a[id_\Gamma] \equiv C t[id_\Gamma] \equiv C t$.

Example:

\[ \text{Goal for all (} x : \text{nat), exists } y, \text{ x < y}. \]
\[ \text{Proof.} \]
\[ \text{eexists. (} x : \text{nat } \vdash x < ?y \times) \]
\[ \text{eapply (leS (} \times \text{?z < S ?z \times)).} \]
\[ \text{(* Unifies } ?z \text{ with x and } ?y \text{ with S } ?z = S x \times) \]
\[ \text{Qed.} \]
Implicit arguments:
At each application of a constant, turn the argument into an existential variable to be resolved.

Example:

\[
\text{cons} : \forall \{A\}, A \rightarrow \text{list} \ A \rightarrow \text{list} \ A \\
\text{nil} : \quad \forall \{A\}, \text{list} \ A
\]

Source: \(\text{cons} \ 1 \ \text{nil} : \text{list} \ ?X\)
Unification for implicit arguments

**Implicit arguments:**
At each application of a constant, turn the argument into an existential variable to be resolved.

**Example:**

\[
\text{cons} : \forall\{A\}, A \to \text{list } A \to \text{list } A \\
\text{nil} : \forall\{A\}, \text{list } A
\]

- **Source:** \texttt{cons 1 nil : list ?X}
- **Desugar:** \texttt{cons (S O) nil : list ?X}
Implicit arguments:
At each application of a constant, turn the argument into an existential variable to be resolved.

Example:

\[\text{cons} : \forall\{A\}, A \rightarrow \text{list} \, A \rightarrow \text{list} \, A\]
\[\text{nil} : \forall\{A\}, \text{list} \, A\]

- Source: \texttt{cons} 1 nil : list ?\(X\)
- Desugar: \texttt{cons} (S O) nil : list ?\(X\)
- Implicits: \texttt{@cons} _ (S O) (@nil _) : list ?\(X\)
Unification for implicits

**Implicit arguments:**
At each application of a constant, turn the argument into an existential variable to be resolved.

**Example:**

\[
\text{cons} : \forall\{A\}, A \rightarrow \text{list } A \rightarrow \text{list } A \\
\text{nil} : \forall\{A\}, \text{list } A
\]

- **Source:** `cons 1 nil : list ?X`
- **Desugar:** `cons (S O) nil : list ?X`
- **Implicits:** `@cons _ (S O) (@nil _) : list ?X`
- **Type-checking:**
  \[
  @\text{cons} (?A : \text{Type}) (S O) (@\text{nil} (?B : \text{Type})) : \text{list } ?X
  \]
Unification for implicit arguments

Implicit arguments:
At each application of a constant, turn the argument into an existential variable to be resolved.

Example:

\[
\begin{align*}
\text{cons} & : \forall\{A\}, A \rightarrow \text{list} A \rightarrow \text{list} A \\
\text{nil} & : \forall\{A\}, \text{list} A
\end{align*}
\]

- Source: \texttt{cons 1 nil : list ?X}
- Desugar: \texttt{cons (S O) nil : list ?X}
- Implicits: \texttt{@cons _ (S O) (@nil _) : list ?X}
- Type-checking:
  \texttt{@cons (?A : Type) (S O) (@nil (?B : Type)) : list ?X}
- Type-checking and Unification:
  \texttt{@cons ?A (S O) (@nil ?A) : list ?X \leadsto A := nat; ?X := A}
Implicit arguments:
At each application of a constant, turn the argument into an existent variable to be resolved.

Example:

```
cons : \{A\}, A \rightarrow \text{list } A \rightarrow \text{list } A
nil : \{A\}, \text{list } A
```

- Source: `cons 1 nil : list ?X`
- Desugar: `cons (S O) nil : list ?X`
- Implicits: `@cons _ (S O) (@nil _) : list ?X`
- Type-checking:
  `@cons (?A : Type) (S O) (@nil (?B : Type)) : list ?X`
- Type-checking and Unification:
  `@cons ?A (S O) (@nil ?A) : list ?X \leadsto A := \text{nat}; ?X := A`
- Final term `@cons nat (S O) (@nil nat) : list nat`
1 Mathematical Structures

2 Elaboration: Coercions, Unification and Implicit Arguments

3 Type Classes and Modular Developments
   - Modules vs Type Classes in CoQ
   - Type Classes in theory
   - Type Classes in practice
   - Variations on type classes
   - Additional exercises
**Different concepts**

Modules are:

- **Second-class:**
  
  Module Type Set. Parameter elt : Type. ...

- **ML-style:** functors, signature ascription \( M <: T \), specialization `Set with Definition elt := nat`.

Good for:

- Namespace management
- Implementation hiding (type and value abstraction)
- Seldom used in mathematical developments, more common in computer science developments

Implementation note: a considerable part of the Coq kernel.
Different concepts

Type-classes:

- First-class citizens of the core type theory:
  
  \[
  \text{Class Set (A : Type) := ...} \\
  \text{Record Set (A : Type) := ...}
  \]

- Haskell-style: proof-search for structures, restricted specialization \(\text{Set \ nat}\).

- Overloading (compile-time binding of names).

- Lightweight generic code (no functorization needed).

- Closer to informal math practice.

Records are the standard representation of algebraic structures in type theories.
Enhancing type inference

Overloading:

- **Generic programming** with interfaces instead of implementations.
- **Generic proving**: refer to semantic concepts rather than specific names. E.g. \texttt{reflexivity} \((R := R)\) instead of \texttt{R_refl}.
- We use arbitrary proof search to find instances and resolve overloading, mimicking math practice.

Inference of \textit{arbitrary} additional structure on types or values.
Making *ad-hoc* polymorphism less *ad hoc*

In *HASKELL*, Wadler & Blott, POPL’89.
In *ISABELLE*, Nipkow & Snelting, FPCA’91.

```
class Eq a where
  (==) :: a → a → Bool
```
Making *ad-hoc* polymorphism less *ad hoc*

In **HASKELL**, Wadler & Blott, POPL’89.
In **ISABELLE**, Nipkow & Snelting, FPCA’91.

```haskell
class Eq a where
  (==) :: a \rightarrow a \rightarrow \text{Bool}

instance Eq Bool where
  x == y = if x then y else \text{not} y
```
Making \textit{ad-hoc} polymorphism less \textit{ad hoc}

In \textsc{Haskell}, Wadler & Blott, POPL’89.
In \textsc{Isabelle}, Nipkow & Snelting, FPCA’91.

\begin{verbatim}
class Eq a where
  (==) :: a -> a -> Bool

instance Eq Bool where
  x == y = if x then y else not y

in :: Eq a => a -> [a] -> Bool
in x [] = False
in x (y : ys) = x == y || in x ys
\end{verbatim}
Parameterizing

**Parametrized instances**

```haskell
instance (Eq a) ⇒ Eq [a] where
  [] == [] = True
  (x : xs) == (y : ys) = x == y && xs == ys
  _ == _ = False
```
Parameterizing

Parametrized instances

\[
\text{instance } (\text{Eq } a) \Rightarrow \text{Eq } [a] \text{ where }
\]
\[
[ ] == [ ] = \text{True}
\]
\[
(x : xs) == (y : ys) = x == y \&\& xs == ys
\]
\[
_ == _ = \text{False}
\]

Super-classes

\[
\text{class Num } a \text{ where }
\]
\[
(+) :: a \rightarrow a \rightarrow a \ldots
\]

\[
\text{class } (\text{Num } a) \Rightarrow \text{Fractional } a \text{ where }
\]
\[
(\div) :: a \rightarrow a \rightarrow a \ldots
\]
3 Type Classes and Modular Developments

- Modules vs Type Classes in CoQ
- Type Classes in theory
  - Motivation and setup
  - Type Classes from Haskell
  - Type Classes in CoQ
- Type Classes in practice
- Variations on type classes
- Additional exercises
Mathematical Structures, Overloading and Monadic Programming

Type Classes and Modular Developments

Type Classes in theory

A cheap implementation

- Parametrized dependent records

\[
\text{Class \textbf{Id} } (\alpha_1 : \tau_1) \cdots (\alpha_n : \tau_n) := \\
\{ f_1 : \phi_1 ; \cdots ; f_m : \phi_m \}.
\]
A cheap implementation

- Parametrized dependent records
  
  \[
  \text{Record } \text{Id} \ (\alpha_1 : \tau_1) \cdots (\alpha_n : \tau_n) := \\
  \{ f_1 : \phi_1 ; \cdots ; f_m : \phi_m \}.
  \]
A cheap implementation

- Parametrized dependent records

\[
\text{Record } \text{ld} \ (\alpha_1 : \tau_1) \cdots (\alpha_n : \tau_n) := \\
\{ f_1 : \phi_1 ; \cdots ; f_m : \phi_m \}.
\]

Instances are just definitions of conclusion \( \text{ld} \rightarrow t_n \).
A cheap implementation

- Parametrized dependent records
  \[
  \text{Record } \text{Id} \ (\alpha_1 : \tau_1) \cdot \cdots (\alpha_n : \tau_n) := \\
  \{ f_1 : \phi_1 ; \cdots ; f_m : \phi_m \}.
  \]
  Instances are just definitions of conclusion \( \text{Id} \rightarrow t_n \).

- Custom implicit arguments of projections
  \[
  f_1 : \forall \ \alpha_n : \tau_n \ , \ \text{Id} \ \alpha_n \rightarrow \phi_1
  \]
A cheap implementation

- Parametrized dependent records
  
  \textbf{Record} \text{Id} (\alpha_1 : \tau_1) \cdots (\alpha_n : \tau_n) := 
  \{f_1 : \phi_1 ; \cdots ; f_m : \phi_m\}. 

  Instances are just definitions of conclusion \text{Id} \rightarrow t_n.

- Custom implicit arguments of projections
  
  \( f_1 : \forall \{\alpha_n : \tau_n\}, \{\text{Id} \alpha_n\} \rightarrow \phi_1 \)
Elaboration with classes, an example

\[
\lambda x \ y : \text{bool. } \text{eqb} \ x \ y
\]
Elaboration with classes, an example

\[ \lambda x \ y : \text{bool}. \ \text{eqb} \ x \ y \]
\[ \rightsquigarrow \{ \text{Implicit arguments}\} \]
\[ \lambda x \ y : \text{bool}. \ \text{@eqb} \_ \_ \ x \ y \]
Elaboration with classes, an example

\[ \lambda x \ y : \text{bool}. \ e q b \ x \ y \]
\[ \leadsto \{ \text{Implicit arguments} \} \]
\[ \lambda x \ y : \text{bool}. \ @e q b \_\_ \ x \ y \]
\[ \leadsto \{ \text{Typing} \} \]
\[ \lambda x \ y : \text{bool}. \ @e q b \ (\_A : \text{Type}) \ (\_eq : \text{Eq} \ ?A) \ x \ y \]
Elaboration with classes, an example

\[ \lambda x \ y : \text{bool}. \ \text{eqb} \ x \ y \]
\[ \leadsto \{ \text{Implicit arguments} \} \]

\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \_ \_ \ x \ y \]
\[ \leadsto \{ \text{Typing} \} \]

\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \ (?A : \text{Type}) \ (?eq : \text{Eq} \ ?A) \ x \ y \]
\[ \leadsto \{ \text{Unification} \} \]

\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \ \text{bool} \ (?eq : \text{Eq} \ \text{bool}) \ x \ y \]
Elaboration with classes, an example

\[ \lambda x \ y : \text{bool}. \ \text{eqb} \ x \ y \]
\[ \rightsquigarrow \{ \text{Implicit arguments} \} \]
\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \ \_ \ \_ \ x \ y \]
\[ \rightsquigarrow \{ \text{Typing} \} \]
\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \ (?A : \text{Type}) \ (\_eq : \text{Eq A}) \ x \ y \]
\[ \rightsquigarrow \{ \text{Unification} \} \]
\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \ \text{bool} \ (\_eq : \text{Eq bool}) \ x \ y \]
\[ \rightsquigarrow \{ \text{Proof search for Eq bool returns Eq\_bool} \} \]
\[ \lambda x \ y : \text{bool}. \ @\text{eqb} \ \text{bool} \ \text{Eq\_bool} \ x \ y \]
Proof-search tactic with instances as lemmas:

\[ A : \text{Type}, \quad eqa : \text{Eq } A \vdash \ ? : \text{Eq } (\text{list } A) \]

- Simple depth-first search with higher-order unification
- Returns the first solution only
+ Extensible through LTAC
1 Mathematical Structures

2 Elaboration: Coercions, Unification and Implicit Arguments

3 Type Classes and Modular Developments
   - Modules vs Type Classes in Coq
   - Type Classes in theory
   - Type Classes in practice
     - Playing with numbers
     - Instance Inference
     - Dependent Classes
     - A programming example: Generic exponentiation
     - Monadic Programming with Type Classes
     - Exercise
     - Logic programming: Reification
   - Variations on type classes
   - Additional exercises
Numeric overloading

Class \textbf{Num} \( \alpha \) := \{ \text{zero} : \alpha ; \text{one} : \alpha ; \text{plus} : \alpha \rightarrow \alpha \rightarrow \alpha \}.  

\[ \text{Instance} \ \text{nat} \text{num} := \{ \text{zero} := 0\% \text{nat} ; \text{one} := 1\% \text{nat} ; \text{plus} := \text{Peano.plus} \}. \]

\[ \text{Instance} \ \text{Z} \text{num} := \{ \text{zero} := 0\% \text{Z} ; \text{one} := 1\% \text{Z} ; \text{plus} := \text{Zplus} \}. \]

\[ \text{Notation} \ "0" := \text{zero}. \]

\[ \text{Notation} \ "1" := \text{one}. \]

\[ \text{Infix} \ "+" := \text{plus}. \]

\[ \text{Check} (\lambda x : \text{nat}, x + (1 + 0 + x)). \]

\[ \text{Check} (\lambda x : \text{Z}, x + (1 + 0 + x)). \]

\[ \text{(* Defaulting *)} \]

\[ \text{Check} (\lambda x, x + 1). \]
Numeric overloading

Class **Num** $\alpha$ := \{ zero : $\alpha$ ; one : $\alpha$ ; plus : $\alpha \to \alpha \to \alpha$ \}.

Instance **nat_num** : Num nat :=
\{ zero := 0%nat ; one := 1%nat ; plus := Peano.plus \}.

Instance **Z_num** : Num Z :=
\{ zero := 0%Z ; one := 1%Z ; plus := Zplus \}.
### Numeric overloading

Class **Num** \(\alpha\) := \{ zero : \alpha ; one : \alpha ; plus : \alpha \rightarrow \alpha \rightarrow \alpha \}.

Instance nat_num : Num nat :=
\{ zero := 0\%nat ; one := 1\%nat ; plus := Peano.plus \}.

Instance Z_num : Num Z :=
\{ zero := 0\%Z ; one := 1\%Z ; plus := Zplus \}.

Notation "0" := zero.
Notation "1" := one.
Infix "+" := plus.
### Numeric overloading

**Class** `Num α := \{ zero : α ; one : α ; plus : α → α → α \}.`  

**Instance** `nat_num : Num nat :=`  
`\{ zero := 0%nat ; one := 1%nat ; plus := Peano.plus \}.`  

**Instance** `Z_num : Num Z :=`  
`\{ zero := 0%Z ; one := 1%Z ; plus := Zplus \}.`  

**Notation** "0" := zero.  
**Notation** "1" := one.  
**Infix** "+" := plus.  

**Check** $(\lambda x : nat, x + (1 + 0 + x))$.  
**Check** $(\lambda x : Z, x + (1 + 0 + x))$. 
Numeric overloading

Class **Num** \(\alpha := \{ \text{zero} : \alpha ; \text{one} : \alpha ; \text{plus} : \alpha \to \alpha \to \alpha \} \).

Instance **nat_num** : **Num** nat :=

\[ \{ \text{zero} := 0\%\text{nat} ; \text{one} := 1\%\text{nat} ; \text{plus} := \text{Peano.plus} \} \].

Instance **Z_num** : **Num** Z :=

\[ \{ \text{zero} := 0\%\text{Z} ; \text{one} := 1\%\text{Z} ; \text{plus} := \text{Zplus} \} \].

Notation "0" := zero.
Notation "1" := one.
Infix "+" := plus.

Check \((\lambda x : \text{nat}, x + (1 + 0 + x))\).
Check \((\lambda x : \text{Z}, x + (1 + 0 + x))\).

(* Defaulting *)
Check \((\lambda x, x + 1)\).
Instance inference

Class \textbf{EqDec} \ A := \text{eq\_dec} : \forall \ x \ y : \ A, \{ x = y \} + \{ x \neq y \}.

Instance: \textbf{EqDec nat} := \{ \text{eq\_dec} := \text{eq\_nat\_dec} \}.

Instance: \textbf{EqDec bool} := \{ \text{eq\_dec} := \text{bool\_dec} \}.
### Instance inference

**Class** $\text{EqDec } A := \text{eq\_dec} : \forall x \ y : A, \{x = y\} + \{x \neq y\}$.

**Instance**: $\text{EqDec } \text{nat} := \{ \text{eq\_dec} := \text{eq\_nat\_dec} \}$.

**Instance**: $\text{EqDec } \text{bool} := \{ \text{eq\_dec} := \text{bool\_dec} \}$.

**Program Instance**: $\forall A, \text{EqDec } A \rightarrow \text{EqDec } (\text{option } A) := \{ \\
\text{eq\_dec } x \ y := \text{match } x, y \text{ with } \\
| \text{None, None } \Rightarrow \text{in\_left} \\
| \text{Some } x, \text{Some } y \Rightarrow \text{if } \text{eq\_dec } x \ y \text{ then in\_left else in\_right} \\
| _, _ \Rightarrow \text{in\_right} \\
\text{end} \}$. 
Instance inference

Class:  \textbf{EqDec} \ A := eq\_dec : \forall \ x \ y : A, \{ x = y \} + \{ x \neq y \}.

Instance:  \textbf{EqDec} \ \textbf{nat} := \{ \ \text{eq\_dec} := \text{eq\_nat\_dec} \}.
Instance:  \textbf{EqDec} \ \textbf{bool} := \{ \ \text{eq\_dec} := \text{bool\_dec} \}.

Program Instance:  \forall \ A, \ \textbf{EqDec} \ A \rightarrow \ \textbf{EqDec} \ (\text{option} \ A) := \{
\text{eq\_dec} \ x \ y := \text{match} \ x, \ y \ \text{with} \\
\ | \ \text{None}, \ \text{None} \Rightarrow \text{in\_left} \\
\ | \ \text{Some} \ x, \ \text{Some} \ y \Rightarrow \text{if} \ \text{eq\_dec} \ x \ y \ \text{then} \ \text{in\_left} \ \text{else} \ \text{in\_right} \\
\ | \ _, \ _ \Rightarrow \text{in\_right} \\
\end{\text{match}}
\}

Check \ (\lambda \ x : \ \text{option} \ (\text{option} \ \text{nat}), \ \text{eq\_dec} \ x \ \text{None}) .
: \forall \ x : \ \text{option} \ (\text{option} \ \text{nat}), \ \{ x = \text{None} \} + \{ x \neq \text{None} \}

Eval \ \text{compute in} \ (\text{eq\_dec} \ (\text{Some} \ (\text{Some} \ 0)) \ (\text{Some} \ \text{None})) .
= \text{in\_right} : \{ \text{Some} \ (\text{Some} \ 0) = \text{Some} \ \text{None} \} + \{ \text{Some} \ (\text{Some} \ 0) \neq \text{Some} \ \text{None} \}
Dependent classes

\[
\text{Class Reflexive } \{ A \} \ (R : \text{relation } A) := \\
\text{refl} : \forall x, R x x.
\]
Dependent classes

Class Reflexive \{A\} (R : relation A) :=
  refl : \forall x, R x x.

Instance eq_refl A : Reflexive (@eq A) := @refl_equal A.
Instance iff_refl : Reflexive iff.
Proof. red. tauto. Qed.
Dependent classes

Class \textbf{Reflexive} \{A\} (R : relation A) :=
  refl : \forall x, R x x.

Instance \textbf{eq_refl A} : Reflexive (@eq A) := @refl_equal A.

Instance \textbf{iff_refl} : Reflexive iff.
Proof. red. tauto. Qed.

Goal \forall P, P \leftrightarrow P.
Proof. apply refl. Qed.

Goal \forall A (x : A), x = x.
Proof. intros A ; apply refl. Qed.
Dependent classes

Class Reflexive \{A\} (R : relation A) := 
    refl : \forall x, R x x.

Instance eq_refl A : Reflexive (@eq A) := @refl_equal A.

Instance iff_refl : Reflexive iff.
Proof. red. tauto. Qed.

Goal \forall P, P \leftrightarrow P.
Proof. apply refl. Qed.

Goal \forall A (x : A), x = x.
Proof. intros A ; apply refl. Qed.

Lemma foo '{Reflexive nat R} : R 0 0.
Proof. intros. apply refl. Qed.
Implicit Generalization

An old convention: the free variables of a statement are implicitly universally quantified. E.g., when defining a set of equations:

\[
\begin{align*}
  x + y &= y + x \quad (\forall x, y \in \mathbb{N}) \\
  x + 0 &= 0 \quad (\forall x \in \mathbb{N}) \\
  x + S\, y &= S\,(x + y) \quad (\forall x, y \in \mathbb{N})
\end{align*}
\]
Implicit Generalization

An old convention: the free variables of a statement are implicitly universally quantified. E.g., when defining a set of equations:

\[
\begin{align*}
  x + y &= y + x & (\forall x, y \in \mathbb{N}) \\
  x + 0 &= 0 & (\forall x \in \mathbb{N}) \\
  x + S\, y &= S\, (x + y) & (\forall x, y \in \mathbb{N})
\end{align*}
\]

We introduce new syntax to automatically generalize the free variables of a given term or binder, as implicit arguments:

\[
\begin{align*}
\Gamma \vdash \texttt{'}(t) : \textbf{Type} & \triangleq \Gamma \vdash \Pi_{\mathcal{FV}(t) \setminus \Gamma}, t \\
\Gamma \vdash \texttt{'}(t) : T : \textbf{Type} & \triangleq \Gamma \vdash \lambda_{\mathcal{FV}(t) \setminus \Gamma}, t \\
(x_i : \tau_i) \texttt{'}\{y : T\} & \triangleq (x_i : \tau_i) \{\mathcal{FV}(T) \setminus \overrightarrow{x_i}\} \{y : T\} \\
(x_i : \tau_i) \texttt{'}(y : T) & \triangleq (x_i : \tau_i) \{\mathcal{FV}(T) \setminus \overrightarrow{x_i}\} (y : T)
\end{align*}
\]
Implicit Generalization example

When writing:

```
Lemma foo `{Reflexive nat R} : R 0 0.
```

Elaboration introduces a new quantifier for \( R \):

```
Lemma foo \{R : relation nat\} \{Reflexive nat R\} : R 0 0.
```
Outline

1. Mathematical Structures

2. Elaboration: Coercions, Unification and Implicit Arguments

3. Type Classes and Modular Developments
   - Type Classes in practice
     - A programming example: Generic exponentiation
The following definition is very naïve, but obviously correct:

Fixpoint power (a : Z) (n : nat) :=
  match n with
  | 0%nat ⇒ 1
  | S p ⇒ a × power a p
  end.

Eval vm_compute in power 2 40.
= 1099511627776 : Z
An efficient tail-recursive version

This is more efficient but relies on a more elaborate property:

Function \texttt{binary\_power\_mult} (\texttt{acc} \: x : \mathbb{Z}) (\texttt{n} : \texttt{nat})
{measure (\texttt{fun} \: i \Rightarrow i) \: \texttt{n}} : \mathbb{Z} :=
\texttt{match} \: \texttt{n} \: \texttt{with}
\ | \: 0\%\texttt{nat} \Rightarrow \texttt{acc}
\ | \_ \Rightarrow \texttt{if} \:\:\texttt{Even.even\_odd\_dec} \: \texttt{n}
\quad \texttt{then} \: \texttt{binary\_power\_mult} \: \texttt{acc} \: (x \times x) \: (\texttt{div2} \: \texttt{n})
\quad \texttt{else} \: \texttt{binary\_power\_mult} \: (\texttt{acc} \times x) \: (x \times x) \: (\texttt{div2} \: \texttt{n})
\texttt{end}.

Definition \texttt{binary\_power} (\texttt{x:Z}) (\texttt{n:nat}) :=
\texttt{binary\_power\_mult} 1 \: x \: \texttt{n}.

\texttt{Eval vm\_compute in} \: \texttt{binary\_power} 2 40.
= 1099511627776 : \mathbb{Z}

\texttt{Check} \: \texttt{eq\_refl} : (\texttt{binary\_power} 2 234 = \texttt{power} 2 234).
Questions

- Is `binary_power` correct (w.r.t. `power`)?
Questions

- Is `binary_power` correct (w.r.t. `power`)?
- Is it worth proving this correctness only for powers of integers?
Questions

- Is `binary_power` correct (w.r.t. `power`)?
- Is it worth proving this correctness only for powers of integers?
- And prove it again for powers of rational numbers, matrices?
Questions

- Is `binary_power` correct (w.r.t. `power`)?
- Is it worth proving this correctness only for powers of integers?
- And prove it again for powers of rational numbers, matrices?

**NO!**

Program with interfaces, here a monoid.
Class Monoid \( \{ A : \text{Type} \} (\text{dot} : A \rightarrow A \rightarrow A) (\text{one} : A) : \text{Type} := \)

\[
\begin{align*}
\text{dot_assoc} : & \forall x y z : A, \text{dot} x (\text{dot} y z) = \text{dot} (\text{dot} x y) z; \\
\text{one_left} : & \forall x, \text{dot} \text{one} x = x; \\
\text{one_right} : & \forall x, \text{dot} x \text{one} = x .
\end{align*}
\]

Operations as parameters, distinguishing Monoid \textit{plus} 0 and Monoid \textit{mult} 1.
Implicit Generalization

Quantification on parameters:

Definition two \( \{A \text{ dot one}\} \{M : @\text{Monoid } A \text{ dot one}\} := \text{dot one one} \).

Using implicit generalization:

Generalizable Variables \( A \text{ dot one} \).

Definition three \( \{\text{Monoid } A \text{ dot one}\} := \text{dot two one} \).
Global names for parameters:

Definition monop ‘\{Monoid A dot one\} := dot.
Definition monunit ‘\{Monoid A dot one\} := one.

Generic notations:

Infix "×" := monop.
Notation "1" := monunit.
Generic power

Generic **power** and **binary_power**.

**Section** Power.

**Context** `{Monoid A dot one}`.

**Fixpoint** `power (a : A) (n : nat) : A :=
  match n with
  | 0%nat ⇒ 1 ← lookup for a Monoid A ?dot ?one
  | S p ⇒ a × (power a p)
  end.`

**Lemma** `power_of_unit : ∀ n : nat, power 1 n = 1.`

**Proof.** ... Qed.
Generic binary exponentiation

Function \texttt{binary\_power\_mult} \((\texttt{acc} \ x : A) \ (n : \texttt{nat})\)
{measure (fun \(i\mapsto i\) \(n\}) : A :=
match \(n\) with
| \(0\%\texttt{nat} \Rightarrow \texttt{acc}\)
| _  \Rightarrow \texttt{if Even.even\_odd\_dec \(n\)
then \texttt{binary\_power\_mult} \texttt{acc} (x \times x) (\texttt{div2} \(n\)
else \texttt{binary\_power\_mult} (\texttt{acc} \times x) (x \times x) (\texttt{div2} \(n\)
end.

Definition \texttt{binary\_power} \((x : A) \ (n : \texttt{nat}) \) := \texttt{binary\_power\_mult} 1 x n.

Lemma \texttt{binary\_spec} \(x \ n : \texttt{power} x n = \texttt{binary\_power} x n\).
Proof. ... Qed.

End Power.
A **Monoid** instance is just a value of the record type:

```latex
Instance \texttt{ZMult} : \texttt{Monoid} \texttt{Zmult} 1\%\texttt{Z}.
```

Proof.

```
\texttt{split}.

\texttt{subgoal 1 is:} \\
\forall \ x \ y \ z : \texttt{Z}, \ x \times (y \times z) = x \times y \times z

\texttt{subgoal 2 is:} \\
\forall \ x : \texttt{Z}, 1 \times x = x

\texttt{subgoal 3 is:} \\
\forall \ x : \texttt{Z}, x \times 1 = x

\ldots \ \texttt{Qed.}
```
Instantiation

power is parameterized by a Monoid implementation.

About power.

\[ \forall (A : \text{Type}) \ (dot : A \rightarrow A \rightarrow A) \ (one : A), \ \text{Monoid} \ dot \ one \rightarrow A \rightarrow \text{nat} \rightarrow A \]

Arguments A, dot, one, H are implicit and maximally inserted
power is parameterized by a Monoid implementation.

About power.
\[ \forall (A : \text{Type}) \ (dot : A \to A \to A) \ (one : A), \ \text{Monoid} \ \text{dot} \ \text{one} \to A \to \text{nat} \to A \]

Arguments \(A\), \(dot\), \(one\), \(H\) are implicit and maximally inserted

Set Printing Implicit.
Check power 2 100.
@power \(\mathbb{Z}\) \(\mathbb{Z}.\text{mul}\) 1 \(\mathbb{Z}\text{Mult}\) 2 100 : \(\mathbb{Z}\)
power is parameterized by a Monoid implementation.

About power.

\[ \forall (A : \text{Type}) \ (dot : A \to A \to A) \ (one : A), \ Monoid \ dot \ one \to A \to \text{nat} \to A \]

Arguments \( A, \ dot, \ one, \ H \) are implicit and maximally inserted

Set Printing Implicit.

Check power 2 100.

@power Z Z.mul 1 ZMult 2 100 : Z

Compute power 2 100.

= 1267650600228229401496703205376 : Z
1. Mathematical Structures

2. Elaboration: Coercions, Unification and Implicit Arguments

3. Type Classes and Modular Developments
   - Type Classes in practice
     - Monadic Programming with Type Classes
Monadic programming: ML vs HASKELL

- Direct effects in ML:
  ```ml
  val counter : unit → nat
  let counter =
    let x = ref 0 in
    fun () => let x' = !x in x := x' + 1; x'
  ```

- Monadic effects in HASKELL:
  ```haskell
  type State α = nat → α × nat

  return :: α → State α
  return x = \s -> (x, s)

  bind :: State α → (α → State β) → State β
  bind m f = \s -> let (a, s') = m s in f a s'

  get :: State nat
  put :: nat → State ()

  counter :: State nat
  counter = do x' <- get; put (x' + 1); return x'
  ```
In our setting, a monad will be defined as:

```
Class Monad (M : Type -> Type) := {

  return: forall {A}, A -> M A;

  bind : forall {A B}, M A -> (A -> M B) -> M B;

  bind_assoc {A B f g} (m : M A) :
    bind (bind m f) g = bind m (fun x : A => bind (f x) g);

  bind_return_left : ...; bind_return_right : ... }
```
Monad Instances

Instances of the monad interface:

- **Identity monad**: `id`
- **Error / partiality monad**: `option`, with `error` action
- **“nondeterminism” monad**: `list` (unit `x = [x]`, bind `m f = concat (map f m)`)
- **Continuations** (with `callcc`), “computation” ...

Exercise

1. Define `Monad` as a type class with overloaded bind and return/unit operations.

2. Define monadic multiplication “mult” of type
   \( \forall A, M (M A) \rightarrow M A \) for any monad \( M \).

3. State and prove what is its relation to the return/unit operation.

4. Define the identity monad instance.

5. Define the `option` instance (return is injection, bind propagates “errors” represented as `None`), with its "error" action of type `option A`. You will need the functional extensionality axiom

6. Define the generic `mapM` operator for any monad (it processes the effects from left to right):
   `mapM : forall A, list (m A) -> m A`. 
1. Mathematical Structures

2. Elaboration: Coercions, Unification and Implicit Arguments

3. Type Classes and Modular Developments
   - Type Classes in practice
     - Logic programming: Reification
Boolean formulas

\[
\text{Inductive \ formula} := \\
\mid \text{cst} : \text{bool} \rightarrow \text{formula} \\
\mid \text{not} : \text{formula} \rightarrow \text{formula} \\
\mid \text{and} : \text{formula} \rightarrow \text{formula} \rightarrow \text{formula} \\
\mid \text{or} : \text{formula} \rightarrow \text{formula} \rightarrow \text{formula} \\
\mid \text{impl} : \text{formula} \rightarrow \text{formula} \rightarrow \text{formula}.
\]
Boolean formulas

**Inductive** formula :=
| cst : bool → formula
| not : formula → formula
| and : formula → formula → formula
| or : formula → formula → formula
| impl : formula → formula → formula.

**Fixpoint** interp f :=
match f with
  | cst b ⇒ if b then True else False
  | not b ⇒ ¬ interp b
  | and a b ⇒ interp a ∧ interp b
  | or a b ⇒ interp a ∨ interp b
  | impl a b ⇒ interp a → interp b
end.
Class **Reify** \((prop : Prop) :=\)

\[
\{ \text{reification} : \text{formula} ; \\
\text{reify\_correct} : \text{interp reification} \leftrightarrow prop \}. 
\]
Reification

Class **Reify** \((\text{prop} : \text{Prop}) :=\)

\[
\{ \text{reification} : \text{formula} ;
\text{reify\_correct} : \text{interp} \ \text{reification} \leftrightarrow \text{prop} \}.
\]

Check \((\text{@reification} : \forall \ \text{prop} : \text{Prop}, \ \text{Reify} \ \text{prop} \rightarrow \text{formula}).\)

Arguments **reification** \(\text{prop} \ \{\text{Reify}\}.$
Reification

Class **Reify** (*prop : Prop*) :=

\{ reification : formula ;
    reify_correct : interp reification \(\leftrightarrow\) *prop* \}.  

Check (@reification : \(\forall\) *prop : Prop*, **Reify** *prop* \(\rightarrow\) formula).  

Arguments reification *prop* \{Reify\}.  

Program Instance **true_reif** : **Reify** True :=

\{ reification := cst true \}.  

Program Instance **not_reif** \((Rb : \text{Reify} \ b) : \text{Reify} \ (\lnot \ b) :=

\{ reification := not (reification \ b) \}.  

Example

\text{example} *prop* :=

reification ((True \(\land\) \(\lnot\) False) \(\rightarrow\) \(\lnot\) \(\lnot\) False).  

Check (**refl_equal** : example *prop* = impl (and (cst true) (not (cst false))) (not (not (cst false)))).
Reification

Class **Reify** \((prop : Prop) :=\)
\[
\{ \text{reification : formula ;}
\text{reify\_correct : interp reification } \leftrightarrow prop \}.\]

Check (@reification : \(\forall \ prop : Prop, \text{Reify } prop \rightarrow formula\)).

Arguments reification prop \{Reify\}.

Program Instance **true\_reif** : Reify True :=
\[
\{ \text{reification := cst true } \}.
\]

Program Instance **not\_reif** \((Rb : \text{Reify } b) : \text{Reify } (\neg b) :=\)
\[
\{ \text{reification := not (reification } b \} \}.
\]

Example example\_prop :=
\[
\text{reification } ((\text{True } \land \neg \text{False}) \rightarrow \neg \neg \text{False}).
\]

Check (refl\_equal _ : example\_prop =
\[
\text{impl } (\text{and } (\text{cst true}) (\text{not } (\text{cst false}))) (\text{not } (\text{not } (\text{cst false}))).\]
Implement domain-specific proof-automation:

- Discharge separation logic disjointness side-conditions (Nanevsky et al, ICFP’11)
- Generalized rewriting tactic using proof-search for morphisms (Sozeau, JFR’09)
- Derive continuity, monotonicity conditions...
1. Mathematical Structures

2. Elaboration: Coercions, Unification and Implicit Arguments

3. Type Classes and Modular Developments
   - Modules vs Type Classes in CoQ
   - Type Classes in theory
   - Type Classes in practice
   - Variations on type classes
   - Additional exercises
Variations on type classes

Type Classes implementations:
- In HASKELL by WADLER et al. (POPL’89, second class)
- In ISABELLE by NIPKOW et al. (POPL’93, same)
- In AGDA by DEVRIESE AND PIÉSSENS (ICFP’11, non-recursive proof search)
- In LEAN and IDRIS as well

In COQ and MATITA:
- Coercive Subtyping and Canonical Structures (SAÏBI, POPL’97). Used by GONTHIER et al. (TPHOLs’09), NANEVSKI et al. (ICFP’11).
- Unification hints, a more general framework studied by ASPERTI et al. (TPHOLs’09).
Another way to use records to represent structures, capable of doing much the same as type classes.

Based on unification instead of general proof search.

Scales better than type-classes but requires more knowledge of unification and type-checking.

At the basis of the Ssreflect methodology and the Mathematical Components library (largest and broadest development of mathematics in Coq and probably any proof assistant to date).

See Mahboubi and Tassi [ITP’13] for a gentle introduction and comparison, and Ziliani et al [ICFP’11] for examples using both representations.
Libraries using typeclasses in Coq

- `stdpp, extlib...` Standard library extensions: sets and maps, monadic programming
- Generalized rewriting (`SOZEAU`, JFR’09), ACI rewriting (`BRAIBANT & POUS`, ITP’11, `aac-tactics`)
- Universal algebra, category theory and computable reals (`math-classes, hott`) (`SPITTERS et al., ITP’10`)
- ...

See DeepSpec Summer School 2017 lecture on Type Classes by B. C. Pierce for tips and tricks.

https://youtu.be/lj0Hy7nJoQc
Exercise: reification of monoids

We want to write a reflexive tactic for simplifying monoidal expressions in any monoid, inspired by the simplification of boolean expressions we just saw. Complete the partial script in `monoid_reification.v`.
Optional Exercises

1. Complete the proof of correctness of `fibonacci` and give an efficient implementation based on matrix computations, following the generic exponentiation development from 2: `matrices.v`

2. Define the state monad and prove a tree labeling algorithm with it: `Monad.v`