

Christian-Albrechts-Universität zu Kiel

**Bachelor Thesis**

**TODO:**  
Weitere Formalitäten...

**Title: TBD**

Niels Bunkenburg

SS 2016

# Contents

<b>1</b>	<b>Preliminaries</b>	<b>1</b>
1.1	Coq . . . . .	1
1.1.1	Data types and functions . . . . .	1
1.1.2	Propositions and proofs . . . . .	2
1.1.3	Higher-order constructs . . . . .	5
1.1.4	Inductively defined propositions . . . . .	6
1.2	FlatCurry . . . . .	8
<b>2</b>	<b>Theory</b>	<b>9</b>
<b>3</b>	<b>CuMin</b>	<b>10</b>
<b>4</b>	<b>Curry</b>	<b>12</b>
4.1	FlatCurry . . . . .	12
4.2	Typing . . . . .	12
4.2.1	Differences to CuMin . . . . .	12
4.2.2	Conversion of FlatCurry to Coq . . . . .	12
<b>5</b>	<b>Conclusion</b>	<b>13</b>

# 1 Preliminaries

## 1.1 Coq

The formalization of Curry programs requires a language that allows us to express the code itself and the propositions we intend to prove. Coq<sup>1</sup> is an interactive proof management system that meets these requirements, hence it will be the main tool used in the following chapters.

**TODO:**  
Kommasetzung?

### 1.1.1 Data types and functions

Coq's predefined definitions, contrary to e.g. Haskell's Prelude, are very limited. However, being a functional language, there is a powerful mechanism for defining new data types. A definition of polymorphic lists could look like this:

```
Inductive list (X:Type) : Type :=  
| nil   : list X  
| cons  : X -> list X -> list X.
```

We defined a type named `list` with two constructors: the constant `nil`, which represents an empty list, and a binary constructor `cons` that takes an element and a list of the same type as arguments. In fact, `nil` and `cons` have one additional argument, a type `X`. This is required, because we want polymorphic lists – but we do not want to explicitly state the type. Fortunately, Coq allows us to declare type arguments as implicit by enclosing them in curly brackets:

```
Check (cons nat 8 (nil nat)). (*cons nat 8 (nil nat) : list nat*)  
Arguments nil {X}.  
Arguments cons {X} _ _.
```

Coq's type inference system infers the type of a list automatically now if possible. In some cases this does not work, because there is not enough information about the implicit types present.

```
Fail Definition double_cons x y z := (cons x (cons y z)).  
Definition double_cons {A} x y z := (@cons A x (@cons A y z)).
```

The first definition does not work, as indicated by `Fail`<sup>2</sup>, because Coq cannot infer the implicit type variable of `double_cons`, since `cons` does not have an explicit type either.

---

<sup>1</sup><https://coq.inria.fr/>

<sup>2</sup>`Fail` checks if an expression does indeed cause an error and allows further processing of the file.

By prefixing at least one `cons` with `@`, we can tell Coq to accept explicit expressions for all implicit arguments. This allows us to pass the type of `cons` on to `double_cons`, again as an implicit argument.

```
Check double_cons 2 4 []. (* : list nat *)
Fail Check (cons 2 (cons nil nil)).
(* Error: The term "cons nil nil" has type "list (list ?X0)"
while it is expected to have type "list nat". *)
```

Based on this we can write a function that determines if a list is empty:

```
Definition isEmpty {X : Type} (l : list X) : bool :=
match l with
| nil      => true
| cons _ _ => false
end.
```

Function definitions begin with the keyword `Definition`. `isEmpty` takes an (implicit) type and a list and returns a boolean value. To distinguish empty from non-empty lists, pattern matching can be used on  $n$  arguments by writing `match  $x_0, \dots, x_{n-1}$  with` `|  $p_0 \rightarrow e_0$  | ... |  $p_{m-1} \rightarrow e_{m-1}$`  for  $m$  pattern  $p$ , consisting of a sub-pattern for every  $x_i$  and expressions  $e_i$ .

The definition of recursive functions requires that the function is called with a smaller structure than before in each iteration, which ensures that the function eventually terminates. A recursive function is indicated by using `Fixpoint` instead of `Definition`.

```
Fixpoint app {X : Type} (l1 l2 : list X) : (list X) :=
match l1 with
| nil => l2
| cons h t => cons h (app t l2)
end.
```

In this case  $l_1$  gets shorter with every iteration, thus the function terminates after a finite amount of recursions.

Coq allows us to define notations for functions and constructors by using the keyword `Notation`, followed by the desired syntax and the expression.

```
Notation "x :: y" := (cons x y) (at level 60, right associativity).
Notation "[ ]" := nil.
Notation "[ x ; .. ; y ]" := (cons x .. (cons y []) ..).
Notation "x ++ y" := (app x y) (at level 60, right associativity).
```

### 1.1.2 Propositions and proofs

Every claim that we state or prove has the type `Prop`. Propositions can be any statement, regardless of its truth. A few examples:

## 1 Preliminaries

```
Check 1 + 1 = 2. (* : Prop *)
Check forall (X : Type) (l : list X), l ++ [] = l. (* : Prop *)
Check forall (n : nat), n > 0 -> n * n > 0. (* : Prop *)
Check (fun n => n <> 2). (* : nat -> Prop*)
```

The first proposition is a simple equation, while the second one contains an universal quantifier. This allows us to state propositions about every type of list, or, as shown in the third example, about every natural number greater than zero. Combined with implications we can premise specific properties that limit the set of elements the proposition applies to. The last example contains an anonymous function, which is used by stating the functions' arguments and an expression.

Now how do we prove these propositions? Proving an equation requires to show that both sides are equal, usually by simplifying one side until it looks exactly like the other. Coq allows us to do this by using tactics, which can perform a multitude of different operations.

```
Example e1 : 1+1=2.
Proof. simpl. reflexivity. Qed.
```

After naming the proposition as an example, theorem or lemma it appears in the interactive subgoal list that Coq provides. The `simpl` tactic performs basic simplification like adding two numbers in this case. The updated subgoal is now  $2=2$ , which is obviously true. By using the `reflexivity` tactic we tell Coq to check both sides for equality, which succeeds and clears the subgoal list, followed by `Qed` to complete the proof.

**TODO:**  
Highlighting  
für Proof  
und Qed

```
Example e2 : forall (X : Type) (l : list X), [] ++ l = l.
Proof. intros X l. reflexivity. Qed.
```

Universal quantifiers allow us to introduce variables, the corresponding tactic is called `intros`. The new context contains a type `X` and a list `l`, with the remaining subgoal  $[] ++ l = l$ . Because we defined `app` to return the second argument if the first one is an empty list, `reflexivity` directly proves our goal. `reflexivity` is not useful for obvious equations only, it also simplifies and unfolds definitions until the flat terms match each other if possible.

To prove that the proposition  $l ++ [] = l$  holds, we need more advanced tactics, because we cannot just apply the definition. `app` works by iterating through the first list, but we need to prove the proposition for every list, regardless of its length. One possibility to solve this problem is by using structural induction.

```
Example e3 : forall (X : Type) (l : list X), l ++ [] = l.
Proof. intros X. induction l as [| l' ls IH].
reflexivity.
simpl. rewrite IH. reflexivity.
Qed.
```

The proof begins by introducing type `X`, followed by the `induction` tactic applied to `l`. Coq names newly introduced variables by itself, which can be done manually by adding

`as [c1|...|cn]` to the tactic. Each  $c_i$  represents a sequence of variable names, which will be used when introducing variables in the corresponding case. Cases are ordered as listed in the [Definition](#).

Now we need to prove two cases: the empty list and a cons construct. The first case does not require any new variable names, therefore the first section in the squared brackets is empty. It is easily solved by applying `reflexivity`, because of the definition of `app`. The second case requires variables for the list's head and tail, which we call `l` and `ls` respectively. The variable name `IH` identifies the induction hypothesis `ls ++ [ ] = ls`, which Coq generates automatically. The goal changes as following:

```
(l :: ls) ++ [ ] = l :: ls
l :: ls ++ [ ] = l :: ls (* simpl *)
l :: ls          = l :: ls (* rewrite with IH *)
```

The tactic `rewrite` changes the current goal by replacing every occurrence of the left side of the provided equation with the right side. Both sides are equal now, hence `reflexivity` proves the last case.

Example `e4` is different from the other examples, in the sense that one cannot prove a function by itself and that only supplying an argument returns a verifiable inequality.

**Example e4 :** `(fun n => n <> 2) 1.`

**Proof.**

```
simpl.      (* 1 <> 2 *)
unfold not. (* 1 = 2 -> False *)
intros H.   (* H : 1 = 2, False *)
inversion H. (* No more subgoals. *)
```

**Qed.**

This proof is not as straight forward as the other ones, mainly because of the inequality, which is a notation<sup>3</sup> for `not (x = y)`. Because `not` is the outermost term, we need to eliminate it first by applying `unfold`. This replaces `not` with its definition `fun A : Prop => A -> False`, where `False` is the unprovable proposition. Why does this work? Assuming that a proposition `P` is true, `not P` means that `P` implies `False`, which is false, because something true cannot imply something false. On the other hand, if `P` is false, then `False -> False` is true because anything follows from falsehood, as stated by the principle of explosion.

The current goal `4 = 8 -> False` is further simplified by introducing `4 = 8` as an hypothesis `H`, leaving `False` as the remaining goal. Intuitively we know that `H` is false, but Coq needs a justification for this claim. Conveniently the tactic `inversion` solves this problem easily by applying two core principles of inductively defined data types:

- Injectivity: `C n = C m` implies that `n` and `m` are equal for a constructor `C`.
- Disjoint constructors: Values created by different constructors cannot be equal.

<sup>3</sup>It is often useful to be able to look up notations, `Locate "<>"` returns the term associated with `<>`.

**TODO:**  
verweis?

By applying `inversion` to the hypothesis  $2 = 1$  we tell Coq to add all inferable equations as additional hypotheses. In this case we start with  $2 = 1$  or the Peano number representation  $S(S(0)) = S(0)$ . Injectivity implies that if the previous equation was true,  $S(0) = 0$  must also be true. This is obviously false, since it would allow two different representations of nil. Hence, the application of `inversion` to  $2 = 1$  infers the current goal `False`, which concludes the proof.

Besides directly supplying arguments to functions that return propositions, there are other interesting applications for them, that we will discuss in the next section.

### 1.1.3 Higher-order constructs

Functions can be passed as arguments to other functions or returned as a result, they are first-class citizens in Coq. This allows us create higher-order functions, such as `map` or `fold`.

**TODO:**  
minted bug?

```
Fixpoint map {X Y : Type} (f : X -> Y) (l : list X) : (list Y) :=
  match l with
  | []      => []
  | h :: t => (f h) :: (map f t)
end.
```

Function types are represented by combining two or more type variables with an arrow. Coq does not only allow higher-order functions, but also higher-order propositions. A predefined example is `Forall`, which features a  $A \rightarrow \text{Prop}$  construct from the last section.

```
Forall : forall A : Type, (A -> Prop) -> list A -> Prop
```

`Forall` takes a *property* of  $A$ , which returns a `Prop` for any given  $A$ , plus a list of  $A$  and returns a proposition. It works by applying the property to every element of the given list and can be proven by showing that all elements satisfy the property.

```
Example e5 : Forall (fun n => n <> 8) [2;4].
Proof.
apply Forall_cons. intros H. inversion H.
(* Forall (fun n : nat => n <> 8) [4] *)
apply Forall_cons. intros H. inversion H.
(* Forall (fun n : nat => n <> 8) [ ] *)
apply Forall_nil.
Qed.
```

`Forall` is an inductively defined proposition, which requires rules to be applied in order to prove a certain goal. This will be further explained in the next section, for now it is sufficient to know that `Forall` can be proven by applying the rules `Forall_cons` and `Forall_nil`, depending on the remaining list. Because we begin with a non-empty list, we have to apply `Forall_cons`. The goal changes to  $2 \neq 8$ , the head of the list applied to the property. We have already proven this type of inequality before, `inversion` is

actually able to do most of the work we did manually by itself. Next the same procedure needs to be done for the list's tail [4], which works exactly the same as before. To conclude the proof, we need to show that the property is satisfied by the empty list. `Forall_nil` covers this case, which is trivially fulfilled.

#### 1.1.4 Inductively defined propositions

Properties of a data type can be written in multiple ways, two of which we already discussed: Boolean equations of the form `b x = true` and functions that return propositions. For example the function `InB` returns `true` if a `nat` is contained in a list, the boolean function could look like this:

```
Fixpoint InB (x : nat) (l : list nat) : bool :=
match l with
| [] => false
| x' :: l' => if (beq_nat x x') then true else InB x l'
end.
Example e5 : InB 42 [1;2;42] = true.
Proof. reflexivity. Qed.
```

Because `InB` returns a boolean value, we have to check for equality with `true` in order to get a provable proposition. The proof is fairly simple, `reflexivity` evaluates the expression and checks the equation, nothing more needs to be done.

Properties are another approach that works equally well. This definition connects multiple equations by disjunction, noted as `\|`. The resulting proposition needs to contain a least one true equation to become true itself.

```
Fixpoint In (x : nat) (l : list nat) : Prop :=
match l with
| [] => False
| x' :: l' => x' = x \| In x l'
end.
Example e6 : In 42 [1;2;42].
Proof.
  simpl. (* 1 = 42 \| 2 = 42 \| 42 = 42 \| False *)
  right. (* 2 = 42 \| 42 = 42 \| False *)
  right. (* 42 = 42 \| False *)
  left. (* 42 = 42 *)
  reflexivity.
Qed.
```

Proving the same example as before, we need new tactics to work with logical connectives. By simplifying the original statement we get a disjunction of equations for every element in the list. If we want to show that a disjunction is true, we need to choose a side we believe to be true and prove it. `left` and `right` keep only the respective side as the current goal, discarding the other one. A similar tactic exists for the logical conjunction



$\wedge$ , with the difference that `split` keeps both sides as subgoals, since a conjunction is only true if both sides are true.

The last option to describe this property is by using inductively defined propositions. As already mentioned before, inductively defined propositions consist of rules that describe how an argument can satisfy the proposition. A useful notation for representing these rules are *inference rules*. They consist of an optional list of premises that needs to be fulfilled in order for the conclusion below the line to hold.

We can describe `In` with two rules:

$$\frac{}{\text{In } n \text{ (} n :: l \text{)}} 1 \qquad \frac{\text{In } n \text{ } l}{\text{In } n \text{ (} e :: l \text{)}} 2$$

Rule one states that the list's head is an element of the list. Additionally, if an element is contained in a list, it is also an element of the the same list, prefixed by another element, as described in the second rule. This definition can be transferred to Coq:

```
Inductive InInd : nat -> list nat -> Prop :=
| Head : forall n l, InInd n (n :: l)
| Tail : forall n l, InInd n (tl l) -> InInd n l.
```

Example `e7` : `InInd 42 [2;42]`.

Proof.

```
  apply Tail. (* InInd 42 (tl [2; 42]) *)
  simpl.      (* InInd 42 [42] *)
  apply Head.
```

Qed.

The interesting part about this proof is the deductive approach. Previously we started with a proposition and constructed evidence of its truth. In this case we use `InInd`'s rules "backwards": Because we want to show that 42 is an element of `[2;42]`, we need to argue that it is contained within the list's tail. Since it is the head of `[42]`, we can then apply `Head` and conclude that the previous statement must also be true, because we required 42 to be contained in the list's tail, which is true.

Inductively defined propositions will play an important role in the following chapters, hence some more examples:

```
Inductive Forall (A : Type) (P : A -> Prop) : list A -> Prop :=
| Forall_nil : Forall P []
| Forall_cons : forall (x : A) (l : list A), P x -> Forall P l -> Forall P (x :: l)
```

We already used `Forall` in the previous section without knowing the exact definition, the rules are fairly intuitive. According to `Forall_nil`, a proposition is always true for the empty list. If the list is non-empty, the first element and the list's tail have to satisfy the proposition, as stated in `Forall_cons`, in order for the whole list to satisfy the property. This pattern can be expanded to more complex inductive propositions, `Forall2` takes a binary property plus two lists and checks if  $P a_i b_i$  holds for every  $i < \text{length } l$ .

```
Forall2 : forall A B : Type, (A -> B -> Prop) -> list A -> list B -> Prop
```

## 1.2 FlatCurry

## 2 Theory

In functional languages a data type is a classification of applicable operators and properties of its members. There are primitive data types that store a single date and more complex types that may contain multiple constructors and type variables. Typing describes the process of assigning an expression to a corresponding type in order to avoid programming errors, for example calling an arithmetic function with a character.

Typing an expression requires a context which contains data type definitions, function/constructor/operator declarations and a map that assigns types to variables. Without a context, expressions do not have any useful meaning – 42 could be typed as a number, the character 'B', a string or the answer to everything. The majority of information in a context can be extracted from the source code of a program and is continually updated while typing expressions.

### 3 CuMin

CuMin is a simplified sublanguage of Curry, which restricts the syntax to allow more concrete typing rules and data types. Although it requires some transformations to substitute missing constructs, CuMin can express the majority of Curry programs. Figure 3.1 shows the syntax of CuMin in Backus–Naur Form:

$$\begin{aligned}
 P &::= D; P \mid D \\
 D &::= f :: \kappa \tau; f \overline{x_n} = e \\
 \kappa &::= \forall^\epsilon \alpha. \kappa \mid \forall^* \alpha. \kappa \mid \epsilon \\
 \tau &::= \alpha \mid \text{Bool} \mid \text{Nat} \mid [\tau] \mid (\tau, \tau') \mid \tau \rightarrow \tau' \\
 e &::= x \mid f_{\overline{\tau_m}} \mid e_1 e_2 \mid \text{let } x = e_1 \text{ in } e_2 \mid n \mid e_1 + e_2 \mid e_1 \doteq e_2 \\
 &\quad \mid (e_1, e_2) \mid \text{case } e \text{ of } \langle (x, y) \rightarrow e_1 \rangle \\
 &\quad \mid \text{True} \mid \text{False} \mid \text{case } e \text{ of } \langle \text{True} \rightarrow e_1; \text{False} \rightarrow e_2 \rangle \\
 &\quad \mid \text{Nil}_\tau \mid \text{Cons}(e_1, e_2) \mid \text{case } e \text{ of } \langle \text{Nil} \rightarrow e_1; \text{Cons}(x, y) \rightarrow e_2 \rangle \\
 &\quad \mid \text{failure}_\tau \mid \text{anything}_\tau
 \end{aligned}$$

Figure 3.1: Syntax of CuMin

A program  $P$  is a list of function declarations  $D$ , which contain a function name  $f$ , a list of quantifiers  $\kappa$ , a type  $\tau$  and a function definition. Quantifiers have a tag  $t \in \{\epsilon, *\}$  that determines the valid types of the variable  $\alpha$ . Star-tagged type variables can only be specialized to non-functional types, while  $\epsilon$  allows every specialization. The notation  $\overline{x_n}$  in function definitions represents  $n$  variables  $x_1, \dots, x_n$  that occur after the function name and are followed by an expression  $e$ . A function's type  $\tau$  can consist of type variables, primitive Bool or Nat types, lists, pairs and functions. An example for a CuMin function is **first**, which returns the first element of a pair:

$$\begin{aligned}
 \text{first} &:: \forall^\epsilon \alpha. \forall^\epsilon \beta. (\alpha, \beta) \rightarrow \alpha & \text{one} &:: \epsilon \text{ Nat} \\
 \text{first } p &= \text{case } p \text{ of } \langle (u, v) \rightarrow u \rangle & \text{one} &= \text{first}_{\text{Nat}, \text{Bool}}(1, \text{True})
 \end{aligned}$$

It is important to notice that polymorphic functions need to be explicitly specialized before they are applied to another expression, as shown in **one**, because there is no type inference.

**TODO:**  
Komisches  
4-fach =

Besides function application, there are literal boolean values and natural numbers, variables, arithmetic expressions, let bindings and case constructs and constructors for pairs and lists. The two remaining expressions arise from Curry's logical parts:  $\text{anything}_\tau$  represents every possible value of type  $\tau$ , similar to free variables.  $\text{failure}_\tau$  represents a failed computation, for example  $\text{fail} = \text{anything}_{\text{Nat}} \stackrel{\circ}{=} \text{True}$ . Since  $\text{anything}_{\text{Nat}}$  can be evaluated to natural numbers only, the equation always fails because Nat and Bool are not comparable.

```

Inductive tm : Type :=
| tvar      : id -> tm
| tapp      : tm -> tm -> tm
| tfun      : id -> list ty -> tm
| tlet      : tm -> tm -> tm -> tm
| ttrue     : tm
| tfalse    : tm
| tfail     : ty -> tm
| tany      : ty -> tm
| tzero     : tm
| tsucc     : tm -> tm
| tadd      : tm -> tm -> tm
| teqn      : tm -> tm -> tm
| tpair     : tm -> tm -> tm
| tnil      : tm
| tcons     : tm -> tm -> tm
| tcasep    : tm -> tm -> tm
| tcaseb    : tm -> tm -> tm -> tm
| tcase1    : tm -> tm -> tm -> tm.

Inductive tag : Type :=
| tag_star  : tag
| tag_empty : tag.

Inductive ty : Type :=
| TVar      : id -> ty
| TBool     : ty
| TNat      : ty
| TList     : ty -> ty
| TPair     : ty -> ty -> ty
| TFun      : ty -> ty -> ty.

```

## 4 Curry

### 4.1 FlatCurry

### 4.2 Typing

#### 4.2.1 Differences to CuMin

#### 4.2.2 Conversion of FlatCurry to Coq

## 5 Conclusion