A certifying extraction with time bounds from Coq to call-by-value λ-calculus

Yannick Forster
Saarland University, Saarland Informatics Campus (SIC), Saarbrücken, Germany
forster@ps.uni-saarland.de

Fabian Kunze
Saarland University, Saarland Informatics Campus (SIC), Saarbrücken, Germany
kunze@ps.uni-saarland.de

Abstract
We provide a plugin extracting Coq functions of simple polymorphic types to the (untyped) call-by-value λ-calculus \( L \). The plugin is implemented in the MetaCoq framework and entirely written in Coq. We provide Ltac tactics to automatically verify the extracted terms w.r.t. a logical relation connecting Coq functions with correct extractions and time bounds, essentially performing a certifying translation and running time validation. We provide three case studies: A universal \( L \)-term obtained as extraction from the Coq definition of a step-indexed self-interpreter for \( L \), a many-reduction from solvability of Diophantine equations to the halting problem of \( L \), and a polynomial-time simulation of Turing machines in \( L \).

2012 ACM Subject Classification  Theory of computation → Type theory; Mathematics of computing → Lambda calculus

Keywords and phrases  cbv λ-calculus, Coq, constructive type theory, extraction, computability

Supplement Material  The Coq development is accessible at https://github.com/uds-psl/certifying-extraction-with-time-bounds

1 Introduction

Every function definable in constructive type theory is computable in a model of computation. This also enables many proof assistants based on constructive type theory to implement extraction into a “real” programming language. On the more foundational side, various realizability models for fragments of constructive type theory increase the trust in this meta-theorem, because realisers for types are the codes of computable functions.

The computability of all definable functions also enables the study of synthetic computability theory in constructive type theory \([7, 4]\). For instance, one can define decidability by \( \text{dec } P := \exists f, \forall x, P x \leftrightarrow f x = \text{true} \) and no reference to a concrete model of computation is needed. The undecidability of a predicate \( p \) can be shown by defining a many-one reduction from the halting problem of Turing machines to \( p \) in Coq, again without referring to a concrete model. The computability of all definable functions can, however, not be proved inside the type theory itself, similar to other true statements like parametricity. At the same time, for every concrete defined function of the type theory, one can always prove computability as theorem in the type theory. Given for instance any concrete function \( f : \mathbb{N} \to \mathbb{N} \) definable in constructive type theory, one can construct a term of the λ-calculus \( t_f \) s.t. for all \( n : \mathbb{N} \), there is a proof in the type theory that \( t_f \, n \) reduces to \( \overline{fn} \) (where \( \overline{\cdot} \) is a suitable encoding of natural numbers). The construction of \( t_f \) from \( f \) is relatively simple, since it is syntax-directed and the terms of type theory are just (possibly type-decorated) terms of an expressive untyped λ-calculus. Another way to see this construction is as extraction from the type theory into the λ-calculus.

We implement one such construction of λ-terms \( t_f \) for a certain subset of type theory:
We use the MetaCoq framework to extend the proof assistant Coq with a command to extract Coq functions of simple polymorphic types into the weak call-by-value $\lambda$-calculus $L$ and provide tactics to automatically prove the correctness of the term. In addition to the correctness, our extraction command can generate recurrence equations that, if instantiated with a function by the user, describe the time complexity as number of $\beta$-steps of the extracted $\lambda$-term on its arguments. Our target calculus $L$ has been used before to formalise computability theory in Coq [12]. Since it is (syntactically) the pure $\lambda$-calculus, recursive functions have to be encoded using a fixed-point combinator and inductive types using Scott’s encoding.

Our extraction has several use cases:

First, while parts of computability theory can be formalised in Coq without referring to a model of computation [7], one needs a deep embedding of computable functions to e.g. construct universal machines. Our framework then allows the user to write all functions in Coq and automatically get $\lambda$-terms computing them, similar to practice on paper where function in the model are never spelled out. For instance, the automated construction of a universal $\lambda$-term takes about 30 lines and no manual proofs, whereas by hand construction and verification take about 500 lines [12].

Second, to the best of our knowledge, there are no formalisations of computational complexity theory in any proof assistant. We hope that our framework can be used to enable formalisations of basic complexity theory. One tedium – even on paper – when doing complexity theory in a way such that all details are spelled out is that constructing and verifying functions in the chosen model of computation is hard. With our framework, this burden is significantly lowered: Implementations can be given in Coq and only a suitable running-time function has to be given by hand. We extract a definition of Turing machines to show that $L$ can simulate $k$ steps of a Turing machine in a number of $\beta$-steps linear in $k$.

Third, synthetic undecidability and the notion of synthetic decidability and enumerability have been analysed in Coq [6, 7, 11, 20]. This resulted in a library of undecidable problems in Coq [10]. All problems of the library are shown undecidable by reduction from the halting problem of Turing machines. To show that all contained problems are actually interreducible with the halting problem, one has to give many-one reductions from the problems to the halting problem. Using extraction, a reduction to the halting problem for $L$ is straightforward: It suffices to prove enumerability in Coq, which follows a clear scheme, and then extract the Coq enumerator automatically to $L$. We demonstrate the power of this method by reducing solvability of Diophantine equations to $L$ halting.

Lastly, it might be beneficial to use classical axioms like choice when verifying reductions. Since the computability of all definable functions does not necessarily hold given classical assumptions, one can extract the used reductions to $L$ to ensure their computability.

**Related Work**

Myreen and Owens [25] implement a proof-producing translation from HOL4 with a state-and-exception monad into CakeML [17]. Hupel and Nipkow [14] give a verified compiler from a deep embedding of Isabelle/HOL to CakeML. Similar to our work, they use a logical relation to connect Isabelle definitions to an intermediate representation.

Mullen et al. [24] provide a verified compiler from a subset of Coq to assembly. Anand et al. [1] report on ongoing work on verifying the full extraction process of Coq, also based on the MetaCoq framework. They extract Coq functions into Clight, an intermediate language of the CompCert compiler, and are thus able to obtain verified assembly code for Coq functions.

Letouzey [21] describes the theoretical foundations of extraction in Coq. Our logical relation can be seen as a light-weight version of his simulation predicate for simple polymorphic types.

Köpp [16] verifies program extraction for functions in the Minlog proof assistant into a
\(\lambda\)-calculus-like system.

Guéneau et al. [13] verify the asymptotic complexity of functional programs in Coq, based on separation logic with time credits.

We have reported on a preliminary version of our extraction plugin in [8].

## 2 The call-by-value \(\lambda\)-calculus \(L\)

We use the weak call-by-value \(\lambda\)-calculus \(L\) defined in [12] and based on [26, 19] as target language. It comes with an inductive type of terms

\[
s, t, u, v : T ::= n \mid st \mid \lambda s \quad (n : \mathbb{N})
\]

and a recursive function \(s^k_u\) providing a simple, capturing substitution operation:

\[
k^k_u := u \quad n^k_u := n \quad (if \ n \neq k)
\]

\[
(st)^k_u := (s^k_u)(t^k_u) \quad (\lambda s^k_u) := \lambda(s^{1+k})
\]

We will freely switch between a named representation for examples and the representation using de Bruijn indices for definitions, i.e. we write \(\lambda x y.x\) for \(\lambda\lambda 1\).

We define an inductive weak call-by-value reduction relation \(s \triangleright t\):

\[
\frac{(\lambda s)(\lambda t) \triangleright s^k_M}{s \triangleright s'} \quad \frac{st \triangleright s't}{t \triangleright t'}
\]

We write \(\triangleright^*\) for the reflexive transitive closure of \(\triangleright\). \(\triangleright^k\) for exactly and \(\triangleright^k\) for at most \(k\) steps.

Note that – contrary to Coq reduction – \(L\)-reduction does not apply below binders. Due to the capturing substitution relation, reduction is only well-behaved on closed terms. We call a term closed if it has no free variables. Closed abstractions are called procedures and are the (only) normal forms of normalising, closed terms.

\(L\) provides for recursion using a fixed-point operator:

\textbf{Lemma 1 (Fact 6 [12]).} There is a function \(\rho : T \to T\) s. t. \((\rho u)v\) reduces to \(u(\rho u)v\) for procedures \(u, v\).

Inductive datatypes can be encoded using Scott encodings [23, 15], which we explain in Section 4.3.

One crucial property of \(L\) reduction is that it is uniformly confluent, making every reduction to a normal form have the same length:

\textbf{Theorem 2 (Corollary 8 [12]).} If \(s \triangleright^k_1 v_1, s \triangleright^k_2 v_2\) for procedures \(v_1, v_2\), then \(v_1 = v_2 \land k_1 = k_2\).

For the remainder of this paper, we will write \(\mathbb{T}\) for the type of types in Coq, \(\mathbb{P}\) for the type of propositions, \(LX\) and \(OX\) for lists and options over \(X\), and \(\mathbb{1}\) (with \(\star : \mathbb{1}\)) for the unit type.

## 3 Correctness and time bounds

We define when a term computes a Coq function using two logical relations, one considering just correctness, and one correctness with time bounds. Crucial for both definitions is the notion of an encoding function:

\textbf{Definition 3.} A function \(\varepsilon_A : A \to T\) is an encoding function for a type \(A\) if \(\varepsilon_A\) is injective and only returns procedures.

Notice that the only types where such a function can be defined are computationally relevant (i.e. non-propositional), countable types like \(\mathbb{B}, \mathbb{N}, \mathbb{O}X\), or \(LX\) over countable \(X\).
We extend the computability predicate to include time bounds. As time measure for a term we define a logical relation $T$ of complexity measures $\tau$ to have a time complexity function $\tau_f : \text{Nat} \to \text{Nat}$ such that $\forall f : \text{Nat} \to \text{Nat}. \tau_f(\varepsilon) \leq \varepsilon \cdot f(L)$. Note that $\sim$ is defined similarly to $\llbracket \cdot \rrbracket$ on inductives and functions in [21].
Given the term $\text{map } X \rightarrow Y$ as above, its complexity measure $\tau_{\text{map } X \rightarrow Y}$ will be $(X \rightarrow Y) \rightarrow (X \rightarrow L \rightarrow N \times 1) \rightarrow L \times (L X \rightarrow L \rightarrow N \times 1)$, which is equivalent to $(X \rightarrow Y) \rightarrow (X \rightarrow N) \rightarrow N \times (L X \rightarrow N)$, i.e. it is a function that, given an argument $f : X \rightarrow Y$ and a complexity measure $\tau_f : C(X \rightarrow Y)$ (being equivalent to $X \rightarrow N$), returns a pair of the number of steps $\text{map } f$ needs to (partially) evaluate, and a function that for $L : L X$ computes the remaining number of steps $\text{map } f L$ needs to evaluate.

We can extend the computability predicate with time bounds into a predicate $t_a \sim^\tau_a a$:

$$\frac{t_f \text{ is a procedure } \land \forall t_a \tau_{t_a}. t_a \sim^\tau_a a \rightarrow \Sigma v : T. t_f t_a \succ^\leq n v \land v \sim^\tau f a \land \tau_f a = (n, \tau)}{}$$ (for $f : A \rightarrow B$)

The first rule is essentially unchanged: Since encoded terms $\varepsilon_{A a}$ are always normal, $\varepsilon_{A a} \sim^\tau a$ holds for every complexity measure $\tau$. For the second rule, we decompose $\tau_{f a} a$ into $n$ and $\tau$. The complexity measure $\tau : C B$ is the complexity measure for $v \sim^\tau f a$ and $n$ is the number of steps $t_f t_a$ needs to reach $v$.

Similar to before, we implement the predicate by recursion on an element of $\mathcal{T}A$:

```coq
Fixpoint computesTime {A} (ty : T A) {struct ty}: A -> T -> C A -> Type := (* ... *).
```

# 4 Extraction

We describe the different tools needed to extract functions, constructors and to generate encoding functions.

## 4.1 Template-Coq

Template-Coq is a quoting library for Coq, now part of the MetaCoq project and originally developed by Malecha [22]. The current state of the project is explained by Anand et al. [2] and Boulier [5].

Template-Coq provides an inductive type $\text{term}$ implementing the abstract syntax of Coq as an inductive type (Figure 1a). It comes with a monad $\text{TemplateMonad : Type \rightarrow Prop}$ (Figure 1b) which allows operations like quoting (i.e. converting Coq terms into their abstract syntax tree), unquoting (i.e. converting abstract syntax trees into Coq terms), evaluating terms, and making definitions. An operation $m : \text{TemplateMonad } A$ can be executed using the Run TemplateProgram $m$ vernacular command.

As an example, the following function obtains the type of its input by unquoting it into a pair of a type and an element, projecting out the type and returning its quotation:

```coq
Definition tmTypeOf (s : term) :=
  u ← tmUnquote s ;;
  u' ← tmEval hnf (my_projT1 u) ;;
  t ← tmQuote u' ;;
  ret t
```

## 4.2 Extracting Terms

We define a monadic function $\text{extract}$ which can extract admissible Coq terms into $L$. In order to extract a Coq term, all the constants appearing in it have to be extracted. To save work, we remember previously generated extracts, similar to Anand et al. [2], who use explicit dictionaries. We employ Coq’s type class mechanism instead:
A certifying extraction with time bounds from Coq to call-by-value λ-calculus

(a) Term representation

\[
\begin{align*}
\text{Inductive} \quad \text{term} : \text{Set} := \\
| \text{tRel} & : \text{nat} \to \text{term} \\
| \text{tLambda} & : \text{name} \to \text{term} \to \text{term} \\
| \text{tLetIn} & : \text{name} \to \text{term} \to \text{term} \to \text{term} \\
| \text{tApp} & : \text{term} \to \text{list term} \to \text{term} \\
| \text{tConst} & : \text{kername} \to \text{universe_instance} \to \text{term} \\
| \text{tConstruct} & : \text{inductive} \to \text{nat} \to \text{universe_instance} \to \text{term} \\
| \text{tCase} & : (\text{inductive} \times \text{nat}) \to \text{term} \to \text{term} \to \text{list (nat \times term)} \to \text{term} \\
| \text{tFix} & : \text{term} \to \text{nat} \to \text{term}
\end{align*}
\]

(b) Monad operations

\[
\begin{align*}
\text{Inductive} \quad \text{TemplateMonad} : \text{Type} \to \text{Prop} := \\
| \text{tmReturn} & : \forall \{A: \text{Type}\}, A \to \text{TemplateMonad} A \\
| \text{tmBind} & : \forall \{A B : \text{Type}\}, \text{TemplateMonad} A \to (A \to \text{TemplateMonad} B) \to \text{TemplateMonad} B \\
| \text{tmPrint} & : \forall \{A: \text{Type}\}, A \to \text{TemplateMonad} \text{unit} \\
| \text{tmFail} & : \forall \{A:\text{Type}\}, \text{string} \to \text{TemplateMonad} A \\
| \text{tmEval} & : \text{reductionStrategy} \to \forall \{A: \text{Type}\}, A \to \text{TemplateMonad} A \\
| \text{tmDefinitionRed} & : \text{ident} \to \text{option reductionStrategy} \to \forall \{A: \text{Type}\}, A \to \text{TemplateMonad} A \\
| \text{tmLemmaRed} & : \text{ident} \to \text{option reductionStrategy} \to \forall A, \text{TemplateMonad} A \\
| \text{tmQuote} & : \forall \{A: \text{Type}\}, A \to \text{TemplateMonad} \text{term} \\
| \text{tmUnquote} & : \text{term} \to \text{TemplateMonad} \{T : \text{Type} & T\} \\
| \text{tmUnquoteTyped} & : \forall A, \text{term} \to \text{TemplateMonad} A
\end{align*}
\]

Figure 1 Template-Coq’s definitions

\[
\text{Class} \quad \text{extracted} \{A : \text{Type}\} \ (a : A) := \text{int_ext} : T.
\]

This also defines a function \text{int_ext} which allows referring to the extracted term corresponding to \(a\) as \text{int_ext} \(a\), if it exists, and otherwise get an error.

We restrict the terms we can extract to admissible terms:

Definition 4. A type \(A\) is admissible if \(A\) is of the form \(\forall X_1 \ldots X_n : T. B_1 \to \cdots \to B_m\) with \(B_m \neq T\). Terms \(a : A\) are admissible if \(A\) is admissible and if all constants \(c : C\) that are proper subterms of \(a\) are either

1. admissible and occur syntactically on the left hand side of an application fully instantiating the type-parameters of \(c\) with constants or
2. of type \(T\) and occur syntactically on the right hand side of an application instantiating type parameters.

This means a type \(A\) is admissible if it has no quantification over terms, quantification over types in \(A\) is in prenex normal form and the return type of \(A\) is not \(T\). The function \text{map} (Figure 2) for instance is admissible. The only constants appearing in its body are \text{nil} and \text{cons}, which are both admissible and occur fully instantiated.
We define an extraction function which correctly extracts admissible terms of a type without type-parameters. If we want to extract polymorphic functions like `map` we use Coq's section mechanism and fix the types `A` and `B` as section variables and extract `map A B`.

The type of the extraction function is

\[
\text{extract} : (\text{nat} \to \text{nat}) \to \text{term} \to \text{nat} \to \text{TemplateMonad} T
\]

The first argument is an environment argument which tracks lifting information for de Bruijn indices for the treatment of fixed points. The last argument is a fuel argument, needed because recursion on the right-hand constituents of an application is not structurally recursive.

Dealing with variables and binders is relatively straightforward, since Template-Coq already uses a de Bruijn representation of terms. Variables translate directly to variables, functions to \(\lambda\) and fixed points can be translated using \(\rho\) from 1. We have to lift variables when entering an abstraction using the standard de Bruijn lifting operation \(\uparrow\):
For all other syntactic constructs we refer to the Coq code.

We wrap the extraction function into an operation which adds definitions:

\[
\begin{align*}
\text{Definition} & \quad \text{tmExtract (nm : option string) (A) (a : A) : TemplateMonad T} \colonequals \\
& \quad \begin{cases} 
q \leftarrow \text{tmUnfoldTerm a} ; ; \\
t \leftarrow \text{extract (fun x \Rightarrow q) FUEL} ; ; \\
\text{match nm with} \\
\quad \text{Some nm} \Rightarrow \begin{cases} 
\text{nm} \leftarrow \text{tmFreshName nm} ; ; \\
\text{tmDefinitionRed nm None (extracted a) t} ; ; \\
\text{tmExistingInstance nm} ; ; \text{ret t} 
\end{cases} \\
\quad \text{| None} \Rightarrow \text{ret t} 
\end{cases} 
\end{align*}
\]

\[\text{end.}\]

\[\text{end.}\]

4.3 Generation of Scott encodings

We use Scott encodings \cite{23, 15} to encode inductive types and its constructors. Scott encodings represent the matches on the inductive type. For instance, the matches on the booleans are \(\varepsilon_B \text{true} = \lambda x y. x\) and \(\varepsilon_B \text{false} = \lambda x y. y\). For natural numbers, the encodings are \(\varepsilon_N 0 = \lambda z s. z\) and \(\varepsilon_N (S n) = \lambda z s. (\varepsilon_N n)\).

As before, we use type classes to remember previously generated encodings:

\[
\begin{align*}
\text{Class} & \quad \text{encodable (A : Type) := enc_f : A} \rightarrow T. \\
\text{Class} & \quad \text{registered (A : Type) := mk_registered} \\
& \quad \begin{cases} 
\text{enc} :> \text{encodable A} ; ; \\
\text{proc_enc : } \forall a, \text{proc (enc a)} ; ; \\
\text{inj_enc : injective enc} 
\end{cases} \\
\quad \text{end.} 
\end{align*}
\]

For an inductive type with \(n\) constructors, the constructor of index \(i\) which takes \(a\) arguments has Scott encoding \(\text{gen_constructor a n i} := \lambda x_1 \ldots x_a. \lambda y_1 \ldots y_n. y_i x_1 \ldots x_a\).

For natural numbers (a type with two constructors, i.e. \(n = 2\)), the constructor \(S\) (which has index \(i = 1\) and takes one argument, i.e. \(a = 1\)) has encoding \(\lambda x. \lambda y_1 y_2. y_2 x\) (or \(\lambda \lambda \lambda (02)\)).

We use \(\text{gen_constructor}\) to define a monadic operation \(\text{tmExtractConstr}\). If we want to extract \(\text{map}\), we first extract the two constants occurring in its definition (i.e. \(\text{nil}\) and \(\text{cons}\)) and then the actual function, always fully applied to their type parameters:

\[\text{Section Fix}_X_Y.\]
\[\text{Context} \{ X Y : \text{Set} \}. \text{Context} \{ \text{encY : encodable Y} \}.\]
\[\text{Run TemplateProgram (tmExtractConstr "nil_term" (\text{nil} X)).}\]
\[\text{Run TemplateProgram (tmExtractConstr "cons_term" (\text{cons} X)).}\]
\[\text{Run TemplateProgram (tmExtract "map_term" (\text{map} X Y)).}\]
\[\text{End Fix}_X_Y.\]

4.4 Generation of Encoding Functions

We restrict our generation of encoding functions to simple inductive types of the form

\[
\text{Inductive} \quad T (X_1 \ldots X_p : \text{Type}) : \text{Type} := \\
\quad (\ast \ldots \ast) | \text{constr}_i : T (A_1 \rightarrow \ldots \rightarrow A_n) \rightarrow X_1 \ldots X_p | (\ast \ldots \ast).
\]

where \(A_j\) for \(1 \leq j \leq n\) is either encodable or exactly \(T X_1 \ldots X_n\).

For a fully instantiated inductive type \(B = T X_1 \ldots X_p\) with \(n\) constructors we define the encoding \(\varepsilon_B\) as follows:

\[
\text{fix} \quad f (b : B) := \text{match} b \text{ with} \\
\quad | \ldots | \text{constr}_i (x_1 : A_1) \ldots (x_n : A_n) \Rightarrow \lambda y_1 \ldots y_p. y_i (f_1 x_1) \ldots (f_n x_n) | \ldots \text{end}
\]
where \( f_j \) for \( 1 \leq j \leq n \) is a recursive call \( f \) if \( A_j = B \), or \( \epsilon A_j \) otherwise.

We implement a monadic function \( \text{tmEncode} \) which can be used like this:

```coq
Section Fix_X.
Variable (X:Type). Context {intX : registered X}.
Run TemplateProgram (tmEncode "list_enc" (list X)).
End Fix_X.
```

Note that in principle, more types are Scott-encodable, but we leave the automatic generation for those types to future work.

### 4.5 Extraction in Coq

To be able to connect extracts \( t_a \) to terms \( a \) using the predicates \( t_a \sim a \) and \( t_a \sim^{\tau_a} a \), we define two type classes: The class `computable` is parameterised over \( a \) and contains an extracted term \( t_a : T \) and a proof of \( t_a \sim a \). The class `computableTime` is in addition parametrised over a time complexity function \( \tau_a \):

```
Class computable {A : Type} {ty : T A} (a : A) : Type :=
  { ext :> extracted a;
    extCorrect : computes ty a ext }.
Class computableTime {A : Type} (ty : T A) (a : A): Type :=
  { extT : extracted a; evalTime : C A ;
    extTCorrect : computesTime ty a extT evalTime }.
```

This way, we can write \( \text{ext} \ a \) or \( \text{extT} \ a \) for previously extracted terms \( t_a \). Note that since all relevant information can be obtained through the parameters and the types of the fields, we can leave all instances of this classes opaque in Coq.

### 5 Automated Verification

We now give an overview over the set of tactics we provide in our framework. All tactics are written in Ltac only, but some of them use the monadic operations explained in the last section. We first explain the tactics to simplify \( \text{L}-\)terms. We then show how to register inductive datatypes to be used with the framework. Lastly, we explain how to prove the computability relation \( t_a \sim a \) and infer recurrence equations for a time bound \( \tau_a \).

#### 5.1 Symbolic Simplification for \( \text{L} \)

All tactics in this section are concerned with proving goals of the form “\( s \) is a procedure” or “\( s \) reduces to \( t \)”, or transforming a goal like “\( s \) reduces to \( t \)” to “\( s' \) reduces to \( t' \)” by simplifying \( s \) to \( s' \). While all terms \( s \) we simplify will be closed, they might not be concrete terms, e.g. contain the encoding of an arbitrary natural number. The tactics will not unfold definitions.

- **Lproc**: The tactic `Lproc` can prove that a term is closed, an abstraction or a procedure. It syntactically decomposes the term and uses a hint database for easier extensibility.
- **Lbeta**: The tactic `Lbeta` simplifies \( \text{L}-\)terms by reducing all \( \beta \)-redices of the form \((\lambda s)t\) which are visible without unfolding definitions. It uses `Lproc` to show that \( t \) is a procedure and that folded definitions used in \( s \) are closed, thus left unchanged by the substitution. `Lbeta` is implemented by reflection, treating names as opaque and using closures to evaluate big terms more efficiently. It can keep track of the number of beta-reductions performed. For example, it simplifies the \( \text{L}-\)term \((\lambda xy. xyy) uv\) in 2 steps to \( uvv \).
- **Lrewrite**: The tactic `Lrewrite` simplifies terms by the use of a hint database with the same name, containing the correctness statements for previously extracted terms, and by the
use of local assumptions, which are important for recursion. For efficiency reasons, it does not use Coq’s built-in rewriting and instead traverses terms to find subterms where a hint from the database is applicable. For example, it simplifies the L-term \( t_1(t_2(\varepsilon_N x)(\varepsilon_N 5))(\varepsilon_N y) \) to \( \varepsilon_N(x + 5 + y) \). While traversing, Lrewrite replaces occurrences of \( t_y \) with \( y : Y \) of the trivial instance with extraction \( \varepsilon_Y y \). This guarantees canonicity of instances of computable for registered types.

Additionally, Lrewrite simplifies \( t_f t_x \) to \( t_f x \) for \( x : X \) and \( f : X \rightarrow Y \). The concrete instance of computable(\( f x \)) is constructed by combining the instances for \( f \) and \( x \).

**Time bounds:** All tactics can be used to analyse time bounds as well: Lbeta, Lrewrite, and Lsimpl transform goals of the form \( s \succ^?) t \) to goals of the form \( s' \succ^?) t \) for an \( s' \) with \( s \succ^k s' \), instantiating the existential variable ?\( k \) with \( k + ?k' \).

### 5.2 Registering Inductive Datatypes

To register an inductive datatype we provide the monadic operation \( \text{tmGenEncode : ident} \rightarrow \text{Type} \rightarrow \text{TemplateMonad unit} \):

```
Run TemplateProgram (tmGenEncode "nat_enc" nat).
```

The operation generates the encoding function and three obligations, which are discharged automatically! The first and second obligation regard procedureness and injectivity of the generated encoding function by tactics register_proc and register_inj.

The third obligation is saved as nat_enc_correct and is generated similarly to the encoding function. It states that the encoding behaves like Scott encoding and is also proven automatically, using the tactic extract match. In the case of natural numbers, it has the following type: \( \text{nat_enc_correct : } \forall (n:nat)(s t:term), \text{proc } s \rightarrow \text{proc } t \rightarrow \text{enc } n \text{ s t } \succ^\leq 2 \text{ match } n \text{ with } 0 \Rightarrow s | S \text{ n' } \Rightarrow t \text{ (enc n') } \text{ end} \). The lemma has to be registered in the hint database Lrewrite manually in order to be used by our tactics.

To work with an inductive type, a user also has to extract its constructors. The constant constructors (e.g. \( 0 \) for natural numbers) are trivially computable by their encoding:

```
Instance reg_is_ext ty (R : registered ty) (x : ty) : computable x.
Proof. \exists (enc x). reflexivity. Defined.
```

A specific instance is only needed for the functional constructors of inductive data types:

```
Instance term_S : computable S. Proof. extract constructor. Qed.
```

The extract constructor tactic extracts constructors as described in Section 4.3 and show their correctness fully-automatically as described in the next section.

### 5.3 Automatically Proving Correctness

As an example, we take the boolean disjunction \( \text{orb x y} := \text{if } x \text{ then true else y} \). For the user, the extraction is fully automatic:

```
```

---

1 Using Global Obligation Tactic of the Program mode shipped with Coq.
The tactic \texttt{extract} first extracts the Coq term as described in Section 4.2. In this case, the result is $\lambda xy. x(\texttt{ext true}) y$. The verification is then performed by iterating the tactic \texttt{cstep}, where in each step a goal is of the form $s \sim f$. The tactic \texttt{cstep} performs simplifications depending on the Coq term $f$.

Here, the initial proof goal reads as follows:

$$(\lambda xy. x(\texttt{ext true}) y) \sim (\texttt{fun} x y \Rightarrow \texttt{if} x \texttt{then} \texttt{true} \texttt{else} y)$$

In case the Coq term is of function type and not syntactically a \texttt{fix}, \texttt{cstep} uses the definition of $\sim$ on function types and assumes a boolean $x$ computed by a term $\texttt{ext} x$. This yields as intermediate goal the existence of a procedure $v$ with

$$(\lambda xy. x(\texttt{ext true}) y)(\texttt{ext} x) \sim^* v \text{ and } v \sim (\texttt{fun} y \Rightarrow \texttt{if} x \texttt{then} \texttt{true} \texttt{else} y)$$

Now \texttt{cstep} uses \texttt{Lsimpl} to derive $v$ by simplifying the term $(\lambda xy. x(\texttt{ext true}) y)(\texttt{ext} x)$ to $\lambda y.(\texttt{ext} x)(\texttt{ext true}) y$, yielding the proof goal

$$\lambda y.(\texttt{ext} x)(\texttt{ext true}) y \sim (\texttt{fun} y \Rightarrow \texttt{if} x \texttt{then} \texttt{true} \texttt{else} y)$$

The next call of \texttt{cstep} assumes a fixed boolean $y$ and simplifies by \texttt{Lrewrite}:

$$\texttt{if} x \texttt{then ext true else ext} y \sim (\texttt{if} x \texttt{then} \texttt{true} \texttt{else} y)$$

In case the Coq term syntactically has a case distinction on top, \texttt{cstep} performs the same case distinction for the proof, here leaving the two goals $\texttt{ext true} \sim \texttt{true}$ and $\texttt{ext} y \sim y$. In both cases the Coq term is of registered type and the next call of \texttt{cstep} proves these goals using the definition of $\sim$.

### 5.3.1 Recursive Functions

Recall that recursive functions in Coq are defined via the \texttt{fix} (or \texttt{Fixpoint}) construct, which allows the application of recursive calls to ‘smaller’ arguments, where the notion ‘smaller’ is due to the guardedness checker of Coq. The tactic \texttt{cstep} proves the correctness using \texttt{fix} as well, with the same recursive calls as the extracted function. Therefore, the guardedness checker will accept the proof for exactly the same reasons it accepted the function definition.

As an example, the extraction of $\texttt{map} A B$ (see Figure 2) for registered types $A$ and $B$ is of shape $\lambda f. \rho v_1$ for a procedure $v_1$, where $\rho$ is the fixed-point combinator from Lemma 1.

To verify this term, the proof goal is

$$\lambda f. \rho v_1 \sim \texttt{fun} f \Rightarrow (\texttt{fix map} l := (...)$$

The first call of \texttt{cstep} is as in Section 5.3 and yields the following goal, where $v_2$ is obtained by replacing the $L$-variable $f$ with $\texttt{ext} f$ for a fixed computable $f : A \rightarrow B$ in $v_1$:

$$(\rho v_2) \sim (\texttt{fix map} l := (...))$$

In case the Coq term is syntactically a \texttt{fix}, \texttt{cstep} uses the definition of $\sim$ on function types, but generalises the goal over all arguments of \texttt{fix} (in this case only 1):

$$\forall \Sigma v : T.(\rho v_2)(\texttt{ext} l) \sim^* v \land v \sim (\texttt{fix map} l := (...))(\texttt{ext} l)$$

\texttt{cstep} now inserts a a $\texttt{fix}$ into the proof term, obtaining an inductive hypothesis $\texttt{IH}$ of the same type as the goal. For the proof term to type-check in the end, $\texttt{IH}$ can only be used on arguments structurally smaller than 1. To guarantee this, \texttt{cstep} always performs a case analysis on the recursive argument first, i.e. in this case on $l$, yielding two goals.

In both resulting cases, \texttt{cstep} calls \texttt{Lrewrite} which uses the inductive hypothesis $\texttt{IH}$ to simplify all occurrences of $(\rho v_2)(\texttt{ext} l')$ to $\texttt{ext} ((\texttt{fix map} l := (...)) l')$. In both goals, \texttt{cstep} needs to obtain a procedure $v$ with $(\rho v_2)(\texttt{ext} l)$, which is done using \texttt{Lsimpl}. For $l = []$, the goal is trivial because $\texttt{ext} [1] \sim [1]$. In the recursive case $l = x :: l'$, \texttt{Lsimpl} yields the trivial goal

$$\texttt{ext} (x :: ((\texttt{fix map} l := (...)) l')) \sim (\texttt{fix map} l := (...)) l'$$
5.3.2 Higher-Order Functions

Terms containing higher-order functions applied to arguments need a syntactic transformation to be supported by our framework. To verify the correctness of e.g. \( \text{map} (\text{fun } x \Rightarrow x + y) l \) as part of a bigger program, we essentially need to show
\[
\text{t}_{\text{map}} (\lambda x.t x y) (\varepsilon l) \sim \text{map} (\text{fun } x \Rightarrow x + y) l
\]

To use the definition of \( \sim \) for \( t_{\text{map}} \), we would have to show
\[
(\lambda x.t x y) \sim (\text{fun } x \Rightarrow x + y).
\]
This introduces several difficulties, one is that the term might contain free variables that need to be beta abstracted, and another one occurs when time bound are of interest: Since our verification of time bounds is only semi-automatic and requires the user to instantiate the recurrences by hand, we would need to interrupt the proof here for a user to fill in the concrete time bounds for \((\lambda x.t x y)\).

We thus restrict the scope of the framework and only cover applications of higher order functions to arguments which syntactically are composed from previously extracted term by application (without the use of abstractions). In this case this would mean that one has to define a Coq term \( f y := \text{fun } x \Rightarrow x + y \), which has to be extracted before \( \text{map} (f y) l \).

5.4 Proving Time Bounds

All simplification tactics also keep track of the number of \( \beta \)-steps in reductions and can thus be used to infer recurrence equations a correct time complexity function has to satisfy. The only obligation left to the user when proving instances of \text{computableTime} is to provide a solution to this recurrence equations. As an example, we consider boolean disjunction again and want to find a time complexity function \( \tau : B \rightarrow 1 \rightarrow N \times (B \rightarrow 1 \rightarrow N \times 1) \):

\[
\text{Instance term_orb : computableTime orb } \tau.
\]

\[
\text{Proof. extract.}
\]

This leaves the user with the recurrence equations \( \pi_1 (\tau x \star) \geq 1 \) and \( \pi_1 (\tau y \star) \geq 3 \), indicating that \( t_{\text{orb}} \) needs one step to reduce to an abstraction if applied to an encoded boolean \( x \) and this abstraction needs 3 further steps to a value if applied to a boolean \( y \). Thus, choosing \( \tau \) as \( \text{fun } _\_ \Rightarrow (1, \text{fun } _\_ \Rightarrow (3, \text{tt}) \) works. We provide the tactic \text{solverec} which simplifies goals containing inequations and tries to show them using the \text{lia} tactic shipped with Coq.

The recurrence equations for the time bound are inferred incrementally by \text{cstep} using an existential variable. To prove \text{computableTime orb } \tau, \text{cstep} first introduces an assumption \( H : ?P \tau \) and opens a new goal \( ?P \tau \). In each step, \text{cstep} performs the transformations described in Section 5.3 while keeping track of the number of steps, asserting that \( \tau \) needs to be larger than the number of \( \beta \)-steps performed by instantiating \( ?P \) further. For non-recursive functions, this will only produce lower bounds for components of \( \tau \), while for recursive correctness proof it produces inequalities that contain \( \tau \) on both sides.

To find time bound functions interactively, we define the opaque polymorphic constant \text{cnst} \{X:Type\} (x:X): nat := 0 which can be used as a place-holder for unknown constants. To find the time complexity for \text{map} one would start with the following:

\[
\text{Lemma termT_map A B (Rx : registered A) (Ry: registered B)}:\n\text{computableTime (map A B) (fun f \tau f \Rightarrow (\text{cnst } "c", \text{fun } l _ \Rightarrow (\text{cnst } ("g", l, \text{tt})))}).
\]

\[
\text{Proof. extract. solverec.}
\]

This yields three conditions: \( 1 \leq \text{cnst } "c", 7 \leq \text{cnst } ("g", \text{ [] }), \) and \( \text{fst } (\tau_f a \text{ tt}) + \text{cnst } ("g", 1) + 11 \leq \text{cnst } ("g", a : : 1) \). Note that \text{cnst} allows os to keep track of the different arguments that the time bound is instantiated with later. As expected, the
time bound of map must also sum up all the time bounds for calling \( f \) on all elements of the list, and indeed, \texttt{solverec} can show the lemma using this time bound:

\[
\text{fun } f \tau_f \Rightarrow (1, \text{fun } l \_ \Rightarrow (\text{fold_right} (\text{fun } x \text{res} \Rightarrow \pi_1 (\tau_f x tt) + \text{res} + 11) 7 l, tt))
\]

### 6 Case studies

We provide three case studies: A universal \( L \)-term obtained as extraction from the Coq definition of a step-indexed self-interpreter for \( L \) (in \texttt{Functions/Universal.v}), a many-one reduction from solvability of Diophantine equations to the halting problem of \( L \) (in \texttt{Reductions/H10.v}), and a linear simulation of Turing machines in \( L \) (in \texttt{TM/TMEncoding.v}).

#### 6.1 Step-indexed \( L \)-interpreter

A step-indexed interpreter for \( L \) is a function \( \text{eva} : \mathbb{N} \to T \to \mathbb{O}_T \) s.t. for closed \( s \) we have \((\exists n. \text{eva} n s \equiv [t]) \leftrightarrow (s \triangleright^* t \land t \text{ is a procedure})\). The function can be defined as follows [12]:

\[
\text{Fixpoint eva (n : nat) (u : term) :=}
\]

\[
\begin{align*}
\text{match u with} \\
\ | \text{var n} & \Rightarrow \text{None} \\
| \text{lam s} & \Rightarrow \text{Some (lam s)} \\
| \text{app s t} & \Rightarrow \begin{cases} \\
& \text{match n with} \\
& | 0 \Rightarrow \text{None} \\
& | S n \Rightarrow \begin{cases} \\
& \begin{cases} \\
& | \text{Some (lam s)}, \text{Some t} \Rightarrow \text{eva n (subst s 0 t)} \\
& | _ , _ \Rightarrow \text{None} \\
\end{cases}
\end{cases}
\end{cases}
\end{align*}
\]

Here \( \text{subst s 0 t} \) denotes substitution, which uses \texttt{Nat.eqb} as boolean equality test on natural numbers. We extract all three functions in reverse order. To do so, we first need encodings for natural numbers and term constructors as shown in Section 5.2 and encodings for terms. We first generate the encoding function and register it:

\[
\text{Run TemplateProgram (tmGenEncode "term_enc" term).}
\]

\[
\text{Hint Resolve term_enc_correct : Lrewrite.}
\]

We then extract all non-constant constructors:

\[
\begin{align*}
\text{Instance term_var : computableTime var (\text{fun n } \_ \Rightarrow (1, tt))).} \\
\text{Proof. extract constructor. solverec. Qed.}
\end{align*}
\]

\[
\begin{align*}
\text{Instance term_app : computableTime app (\text{fun s1 } \_ \Rightarrow (1, (\text{fun s2 } \_ \Rightarrow (1, tt))))).} \\
\text{Proof. extract constructor. solverec. Qed.}
\end{align*}
\]

\[
\begin{align*}
\text{Instance term_lam : computableTime lam (\text{fun s } \_ \Rightarrow (1, tt)).} \\
\text{Proof. extract constructor. solverec. Qed.}
\end{align*}
\]

We can now extract \texttt{Nat.eqb}, \texttt{subst} and \texttt{eva}:

\[
\begin{align*}
\text{Instance termT_nat_eqb :} \\
\text{ computableTime Nat.eqb (fun x \_ \Rightarrow (5, (fun y \_ \Rightarrow ((\min x y) \ast 15 + 8, tt)))}. \\
\text{Proof. extract. solverec. Qed.}
\end{align*}
\]

\[
\begin{align*}
\text{Instance term_substT :} \\
\text{ computableTime subst (fun s \_ \Rightarrow (5, (fun n \_ \Rightarrow (1, (fun t \_ \Rightarrow \\
\text{ \quad (15 + n \ast \text{size s} + 43 \ast \text{size s} - 2 + 13, tt)))))}. \\
\text{Proof. extract. solverec. Qed.}
\end{align*}
\]

\[
\begin{align*}
\text{Instance term_eva : computable eva.} \\
\text{Proof. extract. Qed.}
\end{align*}
\]

Note that the implementation of \texttt{eva} is very naive and needs steps exponential in \( n \), we thus omit its time complexity. A more reasonable implementation could be obtained by extracting the heap-based abstract machine from [18] to \( L \).
6.2 Diophantine equations

The problems contained in the library of undecidable problems in Coq [10] are proven undecidable by a chain of many-one reductions starting at the halting problem for Turing machines. As a matter of fact, all problems contained in the library so far are actually interreducible. The easiest way to prove this is to reduce leafs in the reduction graph to the L-halting problem $E_s := \exists v. (s \approx^* v \land v \text{ is an abstraction})$ and then implement one general reduction from $E$ to the halting problem of Turing machines. As an example how to reduce problems to $E$ we use our framework to reduce solvable Diophantine equations [20], i.e. Hilbert’s tenth problem H10, to $E$.

We first explain the general structure using mathematical notation. In [7], the authors define synthetic notions of decidability and enumerability. If these definitions are enriched with explicit computability assumptions, one obtains:

▶ Definition 5. A predicate $p : X \to \mathbb{P}$ is L-decidable if there exists a computable $f : X \to \mathbb{B}$ s.t. $\forall x. px \leftrightarrow fx = \text{tt}$.

▶ Definition 6. A predicate $p : X \to \mathbb{P}$ is L-enumerable if there exists a computable $f : \mathbb{N} \to \bigotimes X$ s.t. $\forall x. px \leftrightarrow \exists n. fn = \lfloor x \rfloor$.

▶ Theorem 7. If $p : X \to \mathbb{P}$ is L-enumerable and equality on $X$ is L-decidable, then $p \preceq E$.

Proof. Let $f$ be the (computable) enumerator $\mathbb{N} \to \bigotimes X$ and $d : X \times X \to \mathbb{B}$ the (computable) equality decider. We define $s := \lambda x. \mu (\lambda n. t f n (\lambda y. t d xy) t f)$. Here, $\mu$ is an unbounded search operator, i.e. $s$ performs unbounded search for $x$ in the range of $f$. Then $px \leftrightarrow E(s x)$. ◀

Moreover, it is easier to implement concrete enumerators based on lists, i.e. computable enumerators $f : \mathbb{N} \to \mathbb{L} X$ s.t. $px \leftrightarrow \exists n. x \in fn$. The equivalence proof of both notions can be found in [7]. Extending the proof with explicit computability assumptions as needed here is straightforward and we refer to the Coq code.

We now switch to a more technical notation and show how to construct such a list enumerator for H10 in Coq. We first define the type of polynomials, generate its encoding and extract its constructors:

```coq
Inductive poly : Set :=
  poly_cst : nat -> poly | poly_var : nat -> poly

Run TemplateProgram (tmGenEncode "enc_poly" poly).
Hint Resolve enc_poly_correct : Lrewrite.

Instance term_poly_cst : computable poly_cst. extract constructor. Qed.
Instance term_poly_var : computable poly_var. extract constructor. Qed.
Instance term_poly_add : computable poly_add. extract constructor. Qed.
Instance term_poly_mul : computable poly_mul. extract constructor. Qed.

We define evaluation of polynomials under assignments $S : \text{list nat}$ as and the decision problem H10 as follows:

Fixpoint eval (p : poly) (S : list nat) :=
  match p with
  | poly_cst n => n
  | poly_var n => nth n S 0
  | poly_add p1 p2 => eval p1 S + eval p2 S
  | poly_mul p1 p2 => eval p1 S * eval p2 S
  end.

Definition H10 `(p1, p2) := \exists S, eval p1 S = eval p2 S.
Instance term_eval : computable eval. extract. Qed.
```
where \( \text{nth} \) returns the \( n \)-th element in \( S \), or \( d \) if \( S \) is not long enough. We also define a computable function \( \text{poly_eqb} : \text{poly} \to \text{poly} \to \text{bool} \) deciding syntactic equality.

To show that \( H10 \) is \( L \)-enumerable, we enumerate all polynomials using \( \text{L_poly} : \text{nat} \to \text{list poly} \). Due to the restriction that higher-order arguments can not syntactically contain abstractions, we first extract uncurried versions of the constructors:

```coq
Definition poly_add' '(x,y) : poly := poly_add x y.
Instance term_poly_add' : computable poly_add'. extract. Qed.

Definition poly_mul' '(x,y) : poly := poly_mul x y.
Instance term_poly_mul' : computable poly_mul'. extract. Qed.

Fixpoint L_poly n : list (poly) :=
  match n with
  | 0 => []
  | S n => L_poly n ++ map poly_cst (L_nat n) ++ map poly_var (L_nat n)
  ++ map poly_add' (list_prod (L_poly n) (L_poly n))
  ++ map poly_mul' (list_prod (L_poly n) (L_poly n))
  end.

```

The last and crucial lemma is the adaption of Fact 2.9 from [7]:

\[\textbf{Lemma 8.} \text{If } p : X \times Y \to \mathbb{P} \text{ is } L\text{-enumerable, then } \lambda x.\exists y. p(x,y) \text{ is } L\text{-enumerable.}\]

\[\textbf{Theorem 9.} \text{H10 is } L\text{-enumerable.}\]

\[\textbf{Proof.} \text{By Lemma 8 we have to give a list enumerator for two polynomials } p_1 \text{ and } p_2 \text{ together with solutions } S:\]

```coq
fix f n := match n with 0 => []
| S n => f n ++ filter (fun '(p1,p2,S) => Nat.eqb (eval p1 S) (eval p2 S))
  (list_prod (list_prod (L_poly n) (L_list_nat n))) end.
```

where \( \text{list_prod} \) is the cartesian product on lists and \( \text{L_list_nat} \) is a list enumerator for \( \text{list nat} \).

\[\textbf{Corollary 10.} \text{H10 } \trianglelefteq \mathcal{E}\]

\[\textbf{Proof.} \text{By Theorems 9 and 7.}\]

### 6.3 Turing Machines

We show how our framework can be used to reduce the halting problem of multi-tape Turing machines to the halting problem of \( L \). We employ a Coq implementation of the definition of Turing machines by Asperti and Ricciotti [3], who formalise Turing machines in Matita.

```coq
Definition loopM : \forall (sig : finType) (n : nat) (M : mTM sig n),
  mconfig sig (states M) n \to nat \to \text{option} (mconfig sig (states M) n) := (* ... *)

Definition Halt : \{ (Sigma, n) : _ \& mTM Sigma n \& tapes Sigma n \} \to _ :=
  \forall (Sigma, n) \& mTM Sigma n \& tapes Sigma n, \exists (f : mconfig _ (states M)),
  halt (cstate f) = true \wedge \exists k, loopM (mk_mconfig (start M) tp) k = Some f.
```

Their formalisation uses the (dependent) vector type to model multiple tapes and an explicit transition function. Both aspects do not fit in our framework directly. We thus showcase two techniques to extend our framework in certain cases.

First, to encode types not in the scope of the framework, we notice that an encoding for a type \( A \) can be obtained from an encoding function \( \varepsilon_B \) given an injective function \( A \to B \).
We pack this insight in the definition \textbf{registerAs}, which can be used as follows:
Second, we observe that computability is closed under extensional equality:

\[\textbf{Definition 11.}\] We define extensional equality for a type \(A\) with \(ty: \mathbb{T}A\) recursively on \(ty\). Elements \(x, y\) of an encodable type \(A\) are extensionally equal if they are equal. Functions \(f, g: A \rightarrow B\) are extensionally equal if for all \(a : A\), \(fa\) is extensionally equal to \(ga\).

\[\textbf{Lemma 12.}\] If \(f\) and \(g\) are extensionally equal and \(t \sim^\tau f\) then \(t \sim^\tau g\).

Combining those two insights allows us to extract any vector operation by extracting the corresponding list-operation.

Furthermore, we use the fact that functions with finite domain and co-domain can always be translated into a value table containing lists of pairs. We can thus show that every transition function is computable in time independent of the current configuration:

\[\textbf{Instance term_trans : computableTime (trans (m:=M)) (fun _ _ ⇒ (transTime,tt))}.\]

\[\textbf{Proof.} (* ... *) \text{Qed.}\]

\[\textbf{Instance term_loopM :}\]

\[\text{let c1 := (haltTime + n*121 + transTime + 76) in let c2 := 13 + haltTime in}\]

\[\text{computableTime (loopM (M:=M)) (fun _ _ ⇒ (5,fun k _ ⇒ (c1 * k + c2,tt)))}.\]

\[\text{Proof. unfold loopM. extract. solverec. \text{Qed.}}\]

Here \(haltTime\) and \(transTime\) are constants depending on the concrete machine, its number of tapes and its alphabet. By unbounded search over all number of steps \(k\) we obtain:

\[\textbf{Theorem 13.}\] Halt reduces to \(E\).

### 7 Future work

There are several directions in which the framework can be extended. We would like to support more and especially dependent types, possibly containing propositions. In order to do that, the extraction process would have to support proof erasure, which can in principle be implemented using Template-Coq. We also would like to extend the framework to support space bounds in addition to time bounds, based on the space measure defined in [9].

On the more conceptual side, we currently do not separate the notion of correctness from time bounds – we either treat correctness only or correctness plus time bounds. We would like to analyse whether this notions can be treated separately.

Lastly, the extraction basically returns realisers in a realisability model for the treated fragment of Coq’s type theory. We would like to analyse and verify such realisability models using MetaCoq, possibly connecting the (weak call-by-value) evaluation relation defined in MetaCoq with reduction in the realisability model, yielding a proof that for a certain subset of Coq’s type theory, all definable functions are indeed computable.

### References


A certifying extraction with time bounds from Coq to call-by-value $\lambda$-calculus

