

Technical report

Lasse Letager Hansen
Kira Kutscher

May 22, 2019

Contents

1	Introduction (Finished 12.06.)	2
2	Theory and existing frameworks (Finished: 27.05.)	2
2.1	Complete partial orders	3
2.1.1	Recursive definitions as fixed point iterations	3
2.2	Interpreting probabilistic definitions	4
2.2.1	The concept of measures	5
2.2.2	A monadic interpretation	6
2.3	The functional approach: $\mathcal{R}ml$	6
2.4	EASYCRYPT and pwhile (or 'The imperative approach')	8
3	Our approach (Ready draft: 03.06.)	9
3.1	Translating while to a functional language	9
3.2	Translation from Rml to typed λ -calculus	11
3.2.1	Example: Fib	11
3.3	Interpreting λ -calculus in the space of ω -cpos	12
3.4	Interpreting while directly	12
3.5	All translations (forward)	13
4	Our contribution (Draft: 03.06; Finished 10.06.)	13
5	Comparisons and future work (Finished 12.06.)	13
6	Conclusion (Finished 12.06.)	13
7	Appendix	14

1 Introduction (Finished 12.06.)

Probabilistic algorithms are widely used, but far less widely proved correct. We explore some probabilistic languages and how to embed them in the widely known and trusted proof assistant Coq. Having an interpretation of such a language in Coq makes it possible to prove facts about the algorithms in Coq's proof logic.

We explore both a functional design, as presented in [...], and an imperative one, as in [...].

2 Theory and existing frameworks (Finished: 27.05.)

As mentioned before we focused our work on developing a framework for proofs of randomised algorithms in the proof assistant Coq. Coq is known to be a reliable tool and proofs formalised with it are widely trusted. Coq is, however, also known to be notoriously difficult to code things in due to a strict type system that requires determinism and certain termination of all programs written in it. Obviously these two are not the optimal conditions for the encoding of randomised algorithms that may not terminate.

This means that we need a way to encode an interpretation general recursion (or iteration) as well as randomness in such a way that we can still reason about our programs in the proof system of Coq without having to run them.

We will in this section present a monadic interpretation into probability distribution over the outcome of a randomised program as well as a way of interpreting general recursion.

In this section we will have a look at how to use complete partial orders to interpret general recursion (Section 2.1), and how we can represent the result of a probabilistic computation using a monadic interpretation of probability measures (Section 2.2). Afterwards we will move on to presenting two different developments that have worked with probabilistic languages in Coq: the functional `Rml` (Section 2.3) and the imperative `pwhile` (Section 2.4).

2.1 Complete partial orders

A partially ordered set (poset) is a set with an associated binary ordering relation \leq which is both reflexive and transitive. The order is partial when the ordering relation is not defined on every pair of elements in the set.

There exist a number of different completeness properties that a poset can have. We will here have a look at ω -complete partial orders, which we will use in order to interpret general recursion and probabilistic programs.

Definition 1. *ω -complete partial order (ω -cpo)*

An ω -cpo is a partially ordered set that, additionally, has a distinct least element and where there exist least upper bounds on all monotonic sequences.

2.1.1 Recursive definitions as fixed point iterations

Before using ω -cpo to interpret recursion, let us first have a look at some interesting things that our definition entails.

A monotonic sequence on an ω -cpo X can be viewed as a monotonic function $f : \mathbb{N} \xrightarrow{m} X$ where $f(n)$ is the n th element of the sequence (or the least upper bound of the sequence, if n is larger than the length of the sequence).

There is a standard way of defining fixed point iterations on an ω -cpo:

Consider an operator $F : X \xrightarrow{m} X$ on some ω -cpo X ; with this we define the monotonic sequence $F_i \mapsto \underbrace{F(F(\dots F(0_X) \dots))}_{i \text{ times}}$ of repeated application

of F to the least element of X . By our choice of F and the definition of ω -cpo, it is clear that there has to exist a least upper bound on F_i . This least upper bound is the fixed point of F and it will hold that $\text{fix } F = F(\text{fix } F)$ if F is continuous.

For an ω -cpo with underlying set B we can also define an ω -cpo on functions from any set A whose co-domain is B .

To reiterate the definition, let us think of what we need for an ω -cpo. We need an ordering relation, a least element, and a least upper bound operation. Those can be defined as follows:

$$f \leq_{A \rightarrow B} g \Leftrightarrow \forall x : f(x) \leq_B g(x) \quad (\text{pointwise order})$$

$$0_{A \rightarrow B} := f(x) = 0_B \quad (\text{least element})$$

$$\text{lub}_{A \rightarrow B} f_n := g(x) = \text{lub}_B(f_n(x)) \quad (\text{least upper bound operation})$$

The result of an interpretation of programs in the language of discourse will be in an ω -cpo, so according to the above discussion functions will have

an ω -cpo structure as well. Together with the above definition of fixed points we can use this structure to interpret general recursive definitions.

We define a functional, F , taking as input a function and “adding a step to it”. Let us look at the example of the factorial function $f(n) = n!$. The recursive definition is well known:

$$fac(n) := \text{if } n = 0 \text{ then } 1 \text{ else } n \cdot fac(n - 1)$$

For the interpretation of this definition, we want to define $F : (\mathbb{N} \rightarrow \mathbb{N}) \rightarrow (\mathbb{N} \rightarrow \mathbb{N})$ in such a way that its fixed point is the same as the above recursive definition. We choose

$$F(F_i(n)) := \text{if } n = 0 \text{ then } 1 \text{ else } n \cdot F_i(n - 1)$$

Where $F_0(n)$ is $0_{\mathbb{N} \rightarrow \mathbb{N}}$ (the function that takes a natural number and returns 0), by the above definition of the least element in the ω -cpo defined on a function space. By repeated application of F the function will slowly approach the real factorial function, which is the fixed point of F . The beginning of the iteration will be

$$\begin{aligned} F_1(n) = F(F_0(n)) &= \begin{cases} 1 & \text{if } n \text{ is } 0 \\ 0 & \text{otherwise} \end{cases} \\ F_2(n) = F(F(F_0(n))) &= \begin{cases} 1 & \text{if } n \text{ is } 0 \\ 1 & \text{if } n \text{ is } 1 \\ 0 & \text{otherwise} \end{cases} \\ F_3(n) = F(F(F(F_0(n)))) &= \begin{cases} 1 & \text{if } n \text{ is } 0 \\ 1 & \text{if } n \text{ is } 1 \\ 2 & \text{if } n \text{ is } 2 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

In this case it is easy to see that $F_0 \leq F_1 \leq F_2 \leq F_3 \leq \dots$. In the general case this follows from the fact that F has to be monotone and F_0 is always the least element of the function space F operates on.

2.2 Interpreting probabilistic definitions

In order to interpret probabilistic definitions, we need a way of expressing the distribution of possible results. For this we will use probability measures as described in [...].

2.2.1 The concept of measures

In layman's terms, we can describe a measure on a set A as exactly that: a way of measuring subsets of A . More precisely, a measure on A assigns a non-negative real number to every "suitable" subset of A , where "suitable" means fulfilling certain arbitrary conditions. We will henceforth write $\mu(X)$ to signify the value of $X \subseteq A$ under the measure μ .

In order for a function to be a measure, there are three properties it has to have: It must take only non-negative values, $\mu(\emptyset) = 0$, and it has to be countably additive. Being countably additive means that for every set of pairwise disjoint objects, the value of this set is equal to the sum of the values of each object:

$$\mu(X) = \mu\left(\bigcup_{x \in X} x\right) = \sum_{x \in X} \mu(x)$$

An example might be to choose A to be a set of 3-dimensional objects and a possible measure would be the total volume of objects in a subset.

We can understand a measure on A as integral over functions from A to \mathbb{R}^+ . From this perspective, the above example would consist of the function that given an object in A returns its volume. The integral over this function would be the volume of all objects in A . Now the challenge is to measure only a subset of A . We can do this by introducing the characteristic function of a subset X :

Is this understood correctly?

$$\mathbb{I}_X(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{otherwise} \end{cases}$$

By multiplying the characteristic function for X with the volume function on objects in A , we get a new function, f , such that $\int f \, d\mu = \mu(X)$. With this in place, we will allow ourselves to be sloppy in our notation and write $\mu(f)$ instead of $\int f \, d\mu$.

It is easy to see that the integral perspective still satisfies all the requirements that a function has to fulfil in order to be a measure, and the reader is invited to check this for herself.

Now why all this talk about measures? Wasn't it probabilistic programs we were talking about?

Well, yes. The cool thing is, that being able to measure function whose co-domain is the real numbers in the unit interval, $\tau \rightarrow [0, 1]$, gives us a way of representing probability distributions. A measure on type τ can

be expressed with the type $(\tau \rightarrow [0, 1]) \rightarrow [0, 1]$. An interpretation of a probabilistic term whose type is τ can now be understood as a measure on type τ , or equivalently as a transformation of a probability distribution.

Something of type $\tau \rightarrow [0, 1]$ can be understood as the function that returns the probability of its input happening, or in other words, we can understand it as a probability density function. We can view our programs as a transformation of a distribution: If we input an initial distribution (this might also just be the characteristic function of a single value), we will as output receive the integral over the transformed distribution; with other words, we will receive the probability of the result of an actual pseudorandomised run of our program producing a result within the input distribution.

Or something like that... I am very unsure about what exactly we get when we input an initial distribution... help?

2.2.2 A monadic interpretation

Monadic transformation. Should we add a subsection on monads or should we just mention them?

We should mention them and refer to our FP project. This is to make sure that our censor knows that we know stuff about monads.

2.3 The functional approach: $\mathcal{R}ml$

The first approach to proving something about randomised algorithms in Coq that we will examine here is due to Philippe Audebaud and Christine Paulin-Mohring and features the functional language $\mathcal{R}ml$.

We have two representations of $\mathcal{R}ml$, continuations and distributions. Both build on a monad, for ease of use.

The data structure used to represent $\mathcal{R}ml$ terms is as follows:

```

Inductive Rml :=
| Var : (N * Type) → Rml
| Const : ∀ (A : Type), A → Rml
| Let_stm : (N * Type) → Rml → Rml → Rml
| Fun_stm : Type → (N * Type) → Rml → Rml
| If_stm : Rml → Rml → Rml → Rml
| App_stm : Type → Rml → Rml → Rml
| Let_rec : Type → Type → N → N → Rml → Rml → Rml.

```

We use all cog types, as possible types of Rml expressions, since there are no real restrictions on the types. We encode variables, as a type and a natural number, so two variables are the same only if they have the same number and refer to the same type.

We have defined a relation `well_formed`, that checks that no variables are escaping the scope of an Rml program, that is there is always a binding for an expression of type `Var p`. We furthermore define a relation `rml_valid_type`, which checks that a given Rml expression can be typed under a given type. We have shown that if a Rml program is valid then it is well formed. We have then constructed a simplified form of Rml called sRml (for simple Rml), to make it easier to reason about and evaluate expressions, with the following data structure:

```

Inductive sRml {A : Type} :=
| sVar : N → sRml
| sConst : A → sRml
| sFun : ∀ C (p : N * Type), A = (p.2 → C) →
  ·sRml C → sRml
| sIf : ·sRml bool → sRml → sRml → sRml
| sApp : ∀ T, ·sRml (T → A) → ·sRml T → sRml
| sFix : ∀ B (nf nx : N), ·sRml (B → A) → ·sRml B →
  sRml.

```

That is Rml where we remove expressions with variables, from `let_stm` statements (not `let_rec` statements). We then show that given a valid typing of an Rml expression, we can simplify that expression, and maintain the valid typing (under the same type). With this we can make an interpreter from an interpreter of sRml, which can be constructed as (for continuations). We have a similar function for Rml, using the possibility distributions as interpretations. We see similar patterns arising, since both interpretations are monadic.

2.4 EasyCrypt and `pwhile` (or ‘The imperative approach’)

EASYCRYPT is a framework that has been developed in order to help in the construction of machine-checkable proofs about cryptographic constructions and protocols. A standard approach to this kind of proofs is based on so-called games; in EASYCRYPT cryptographic algorithms as well as games are modelled as *modules* consisting of procedures written in a simple imperative language called `pwhile`. The `p` in `pwhile` stands for “probabilistic”, so in total the name refers to a probabilistic extension of the well-known minimalistic `while` language.

We will in this section give an overview of the language as well as its interpretation in Coq, which is due to a development by Pierre-Yves Strub¹. We will not concern ourselves with the module system of EASYCRYPT since the focus of the present development is on probabilistic languages and their interpretation rather than their use.

`pwhile` consists of the following expressions and commands:

$$\begin{aligned} \text{exp} &::= x \mid \text{const} \mid \text{prp } (p : \text{pred mem}) \mid e_1 \ e_2 \\ \text{cmd} &::= \text{abort} \mid \text{skip} \mid x := e \mid x \$ = e \\ &\mid \text{if } b \text{ then } c_1 \text{ else } c_2 \mid \text{while } b \text{ do } c \mid c_1; c_2 \end{aligned}$$

The embedding of `pwhile` in Coq is a so-called shallow embedding, which means that we use Coq terms and types as part of programs in `pwhile`. This is used in order to form expressions: Constants in `pwhile` are Coq constants, hence an expression in `pwhile` can have any Coq type. In the implementation, expressions are parameterised by their type.

Most of the above constructs are fairly standard and should be known to most readers. We give a full formal semantics in Figure .

In addition to the standard expressions and commands, `pwhile` has the expression `prp p`, which we will have a look at here. `prp` takes a single argument of type `pred mem`. This is a Coq type specified with the type constructor `pred = $\forall \tau : \tau \rightarrow \mathbb{B}$` applied to the type of memories defined in the `xhl` development. The predicate over memories that is `prps` argument is mapped over the working memory at the time of evaluation.

For more clarity, we will look at an example. Let us take the situation where we only want to proceed with a computation, if a certain variable, x is defined in the memory; we want to access x , but want to avoid our program crashing if x has not been defined. We now write the function `x_defined`

¹<https://github.com/strub/xhl>

Insert reference to semantics-figure

that, given a memory, returns true if x is defined in said memory and false otherwise. By branching on `prp x_defined`, we can now make sure that we only take the branch accessing x if it is present in the memory and do not end up with a program that may crash.

At this point a comment about “crashing” programs is in order. There are multiple ways in which a program can lead to an undefined result: encountering undefined behaviour, non-termination, and the `abort` command. The interpretation of all of these is the same: We recall that the result of interpreting a `pwhile` program in Coq is a probability distribution over memories; now the result of interpreting a “crash” is by simply returning the null-distribution over memories.

is this the right word choice? It doesn't seem that that's what a null distribution is. But the keyword use is `dnull`.

3 Our approach (Ready draft: 03.06.)

3.1 Translating while to a functional language

In order to do the translations properly, let us first have a look at a translation from the simple, widely known `while` language to a simple functional language resembling `Rml`. The thought behind this is that once this translation is in place, all we have to do to translate `pwhile` to `Rml` is to add probability.

- (1) $exp ::= x | n | \text{true} | \text{false} | f \ x$
- (2) $stm ::= \text{skip} | x := e | \text{if } e \text{ then } s_1 \text{ else } s_2 | \text{while } e \text{ do } s | s_1 ; s_2$

The syntax of our functional language is the same as `Rml` modulo the pre-defined probabilistic functions.

The translation of expressions is completely straightforward: variables are mapped to variables, constants to constants, and function applications to function applications.

In order to translate statements we choose a set of SML-style matching rules; this choice is due to the translation of sequences being dependent on what the first statement is. We will in the following write the translation of a `while` statement s to an expression in our functional language as $\llbracket s \rrbracket$.

The result of a computation in `while` is the state of a memory, while the result of a functional computation is a value. A simple way to make

up for this difference is by choosing a variable name that is designated the return variable and encapsulates the information we are interested in after the computation. This is the result of a program translated from **while** to our functional language; in the following we choose x_r as the symbol for the chosen return variable.

$$(3) \quad \text{skip} ; s \mapsto \llbracket s \rrbracket$$

$$(4) \quad \text{skip} \mapsto x_r$$

$$(5) \quad x := e ; s \mapsto \text{let } x := e \text{ in } \llbracket s \rrbracket$$

$$(6) \quad x_r := e \mapsto e$$

$$(7) \quad x := e \mapsto x_r$$

$$(8) \quad (\text{if } e \text{ then } s_1 \text{ else } s_2) ; s_3 \mapsto \begin{array}{l} \text{if } e \\ \text{then } \llbracket s_1 ; s_3 \rrbracket \\ \text{else } \llbracket s_2 ; s_3 \rrbracket \end{array}$$

$$(9) \quad \text{if } e \text{ then } s_1 \text{ else } s_2 \mapsto \text{if } e \text{ then } \llbracket s_1 \rrbracket \text{ else } \llbracket s_2 \rrbracket$$

$$(10) \quad (\text{while } e \text{ do } s_1) ; s_2 \mapsto \begin{array}{l} \text{let rec } f \text{ } x := \text{if } e \\ \quad \text{then } \llbracket s_1 ; f \text{ } x \rrbracket \\ \quad \text{else } \llbracket s_2 \rrbracket \\ \text{in } f \text{ } 0 \end{array}$$

$$(11) \quad \text{while } e \text{ do } s_1 \mapsto \begin{array}{l} \text{let rec } f \text{ } x := \text{if } e \\ \quad \text{then } \llbracket s_1 ; f \text{ } x \rrbracket \\ \quad \text{else } x_r \\ \text{in } f \text{ } 0 \end{array}$$

Note that in 10 and 11 we create recursive functions with a name and an argument, both of which are not present in the while construct we translate

from. This means that we have to be careful about the translation: Both f and x have to be chosen fresh; and even fresher than that, they can not occur in the body of the while loop we are translating either, because that would break the recursive call.

Further notice that the recursive functions are always called with a dummy argument. This is because they act as procedures, but since our syntax requires an argument for recursive definitions, we give a dummy argument.

3.2 Translation from Rml to typed λ -calculus

This section is preliminary and needs either huge changes or deletion before the report is finalised.

Rml	typed λ -calculus
Var (x, A)	$x : A$
Const $A \ c$	$c : A$
Let $(x, A) \ e_1 \ e_2$	$(\lambda x : A. e_2) \ e_1$
Fun $(x, A) \ e$	$\lambda x : A. e$
App $e_1 \ e_2$	$e_1 \ e_2$
Let_rec $(f, A \rightarrow B) (x, A) \ e_1 \ e_2$	$(\lambda f : A \rightarrow B. e_2) (Y (\lambda f : A \rightarrow B. \lambda x : A. e_1))$

The problem here is that we need to translate e_1 and e_2 to their simple forms, so we do an intermediate translation:

Let

3.2.1 Example: Fib

Expression:

```

Let_rec (f,  $\mathbb{N} \rightarrow \mathbb{N}$ ) (x,  $\mathbb{N}$ )
  (if  $x \leq 0$ 
   then 0
   else  $f \ (x - 1) + f \ (x - 2)$ )
(f 3)

```

Typing:

```
Let_rec (f,  $\mathbb{N} \rightarrow \mathbb{N}$ ) (x,  $\mathbb{N}$ )  
  ((if (x  $\leq$  0 :  $\mathbb{B}$ )  
    then (0 :  $\mathbb{N}$ )  
    else (f :  $\mathbb{N} \rightarrow \mathbb{N}$ ) (x - 1 :  $\mathbb{N}$ ) + (f :  $\mathbb{N} \rightarrow \mathbb{N}$ ) (x - 2 :  $\mathbb{N}$ ) :  $\mathbb{N}$ )  
  ((f :  $\mathbb{N} \rightarrow \mathbb{N}$ ) (3 :  $\mathbb{N}$ ) :  $\mathbb{N}$ )
```

Semi-simple

```
Let_stm f  
  sFix  
    sFun (f,  $\mathbb{N} \rightarrow \mathbb{N}$ )  
      sFun (x,  $\mathbb{N}$ )  
        ((if (x  $\leq$  0)  
          then 0  
          else f (x - 1) + f (x - 2)))  
  (f 3)
```

Simple form:

```
sApp sFix  
  sFun (f,  $\mathbb{N} \rightarrow \mathbb{N}$ )  
    sFun (x,  $\mathbb{N}$ )  
      ((if (x  $\leq$  0)  
        then 0  
        else f (x - 1) + f (x - 2)))  
  3
```

3.3 Interpreting λ -calculus in the space of ω -cpos

What do ω -cpos have to do with this?

3.4 Interpreting while directly

This should probably mainly refer back to the interpretation of `pwhile`.

3.5 All translations (forward)

What is the point of this section?

Rml	@sRml A	typed λ -calculus
Var (x, A)	sVar x	$x : A$
Const $A\ c$	sConst c	$c : A$
Let $(x, T)\ e_1\ e_2$	e'_2	$(\lambda x : T, e_2 : A)\ (e_1 : T) : A$
Fun $(x, T)\ e$	sFun $S\ (x, T)\ e'$	$(\lambda x : T, e : S) : T \rightarrow S$
App $T\ e_1\ e_2$	sApp $T\ e'_1\ e'_2$	$(e_1 : T \rightarrow A)\ (e_2 : T) : A$
Let rec $T\ S\ f\ x\ e_1\ e_2$	sApp $(T \rightarrow S)$ (sFun $A\ (f, T \rightarrow S)\ e'_2$) (sFun $S\ (x, T)$ (sFix $T\ f\ x\ e'_1\ (sVar\ x)))$	$(\lambda f : T \rightarrow S, e_2 : A)$ $(Y\ (\lambda f : T \rightarrow S, \lambda x : T, e_1 : S) : T \rightarrow S) : A$

4 Our contribution (Draft: 03.06; Finished 10.06.)

5 Comparisons and future work (Finished 12.06.)

6 Conclusion (Finished 12.06.)

7 Appendix

Example - Error: Stack Overflow.

```

Fixpoint replace_all_variables_aux_type
  A (x : Rml) (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A (map fst env) fl x} : sRml A

with replace_all_variables_aux_type_const
  A0 A a (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A0 (map fst env) fl (Const A a)} : sRml A0
with replace_all_variables_aux_type_let
  A p x1 x2 (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A (map fst env) fl (Let_stm p x1 x2)} : sRml A
with replace_all_variables_aux_type_fun
  A T p x (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A (map fst env) fl (Fun_stm T p x)} : sRml A
with replace_all_variables_aux_type_if
  A x1 x2 x3 (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A (map fst env) fl (If_stm x1 x2 x3)} : sRml A
with replace_all_variables_aux_type_app
  A T x1 x2 (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A (map fst env) fl (App_stm T x1 x2)} : sRml A
with replace_all_variables_aux_type_let_rec A T T0 n n0 x1 x2 (env : seq (N * Type * Rml))
  (fl : seq (N * Type)) '{env_valid : valid_env env fl}
  '{x_valid : rml_valid_type A (map fst env) fl (Let_rec T T0 n n0 x1 x2)} : sRml A.

Proof.
  (** Structure **)
  {
    induction x ; intros ; refine (sVar (0,A)).
  }

  all: refine (sVar (0,A)).
Defined.

```