Towards Palatable Programming with Dependent Type Theories

Donovan Crichton

May 2023

Preliminaries

- Slides and Examples available at:
  https://github.com/donovancrichton/Talks
- This talk: BFPG/PalatableProgrammingWithDTT

Who am I?

- PhD Candidate,
  Research School of Computing,
  The Australian National University.
  Supervisors: Dr Dirk Pattinson, Dr Ranald Clouston, Dr Michael Norrish
- Visiting Scholar,
  Trusted Systems Laboratory,
  Institute for Integrated and Intelligent Systems,
  Griffith University.
- ANU-ASD Co-Lab Scholar,
  The Australian Signals Directorate.

Syntax

What do GADTs actually look like?

```haskell
{-# LANGUAGE GADTs #-}
-- this is the data constructor
data Expr :: * -> * where
-- these are the type constructors:
  EInt :: Int -> Expr Int
  EBool :: Bool -> Expr Bool
  EAdd :: Expr Int -> Expr Int -> Expr Int
  EAnd :: Expr Bool -> Expr Bool -> Expr Bool
  EIsZero :: Expr Int -> Expr Bool
```

Limitations of Algebraic Data Types

Imagine a list with a concrete constructor and a polymorphic one.

```haskell
-- this is just fine.
data List a =
  Nil
  | Cons a (List a)
  | CInt Int (List Int)

-- this is not!
tl :: List a -> List a
tl Nil = Nil
tl (Cons x xs) = xs
tl (CInt k ks) = ks
```

Limitations of Algebraic Data Types 2

- If we *parameterise* our data types we can't fix that parameter later.
- In PLT, TT and Logic we have object and meta languages.
- We would like to use the binding in our meta language for our object language.

Polymorphic Evaluation

```haskell
{-# Langauge GADTs #-}
data Expr a where
  EInt :: Int -> Expr Int
  EBool :: Bool -> Expr Bool
  EAdd :: Expr Int -> Expr Int -> Expr Int
  EAnd :: Expr Bool -> Expr Bool -> Expr Bool
  EIsZero :: Expr Bool -> Expr Int

eval :: Expr a -> a
eval (EInt x) = x
eval (EBool b) = b
eval (EAdd x y) = eval x + eval y
eval (EAnd p q) = eval p && eval q
eval (EIsZero k) = (eval k) == 0
```

GADT Demo

- let's see the demo.

Correctness by Construction

- GADTs now type-check our object language expressions in our meta language.
- It is *not possible* for me to accidentally write addition on Boolean expressions.
- Idea - create your data structures in such away that they enforce correctness?.

Moving Away from Haskell

- Extensions overload: PolyKinds, DataKinds, KindSignatures, KindAsType, etc.
- Reification and Reflection: Haskell has two languages!
- Just to get more expressivity and functionality for GADTS?

Stephanie Weirich's Dependent Haskell...

Haskell looks different with just *one* extension...

```
{-# LANGUAGE DataKinds, TypeFamilies, PolyKinds,
    TypeInType, GADTs, RankNTypes, ScopedTypeVariables,
    TypeApplications, TemplateHaskell,
    UndecidableInstances, InstanceSigs,
    MultiParamTypeClasses, TypeOperators,
    KindSignatures, TypeFamiliyDependencies,
    AllowAmbiguousTypes, FlexibleContexts,
    FlexibleInstances #-}
```

To Idris!

- Full Support for Dependent Types.
- Pure Functional Language.
- Syntactically Similar to Haskell.
- Term and Type Languages are Identical.
- It has a book [Brady, 2017].
- My Favourite.

Installation (on Linux)

The README on the repo has good installation instructions.

1. `$ sudo apt-get install chezscheme9,5`
2. `$ git clone https://github.com/idris-lang/idris2`
3. `$ cd idris2`
4. `$ make bootstrap SCHEME=chezscheme9.5`
5. `$ make install`
6. `$ make clean`
7. `$ make all`
8. `$ make install`
9. `add  /.idris2/bin to your system path`

DDTS (GADTS) in Idris

Strictness, loss of type inference.

```
data Expr : (a : Type) -> Type where
  EVal : a -> Expr a
  EAdd : Num a => Expr a -> Expr a -> Expr a
  EAnd : Expr Bool -> Lazy (Expr Bool) -> Expr Bool

eval : Expr a -> a
eval (Eval x) = x
eval (EAdd x y) = (eval x) + (eval y)
eval (EAnd p q) = (eval p) && (eval q)
```

Slim instead of Thick. Fat instead of Thin. Full of holes.

- `:` not `::`
- `(x :: xs)` not `(x : xs)`
- `=>` not `->`
- `?what`

```
f : Nat -> Nat
f x =
  case x of
   Z     => ?baseCaseHole
   (S k) => ?stepCaseHole
```

Gentle Dependent Types 1

- We can *index* our data types as well as *parameterise* them.
- The index may have a specific element in the return type, the parameter may not.
- in `List`, a is a parameter. In `Expr`, a is an index.

Gentle Dependent Types 2

We can be *precise* about head and tail.

```
data Vect : Nat -> Type -> Type
  Nil  : Vect Z a
  (::) : a -> Vect k a -> Vect (S k) a

hd : Vect (S k) a -> a
hd (x :: _) = x

tail : Vect (S k) a -> Vect k a
tail (_ :: xs) = xs
```

Scary Dependent Types 1

```
data (=) : a -> b -> Type where
  Refl : a = a
```

We can state equality between any two types. However we can only construct an element of the equality type if `a` and `b` are the same thing.

This happens by beta reduction.

Scary Dependent Types 2

Interactive Demo on defining $(++)$

- What is rewrite? Goal changing?
- Also implicits?
- More proofs like this, more practice? Port from Coq!
- Read logical foundations and skip the tactics!

Okay...but that's not a proof!

- A proof based on intuitionistic higher order logic.
- Thanks to the curry-howard isomorphism.
- Commonly known as 'Propositions as Types' [Wadler, 2015].
- As Phillip Wadler speaks about.

Other Invariants

- Sorted Lists
- Ordered Binary Trees
- What about Balanced BSTs?
- let's see the demo.

Who to talk to if I want more?

- Lots of academics in SOC Foundations Cluster care about FP and Formal Methods.
- Offhand: Dirk Pattinson, Ranald Clouston, Michael Norrish.
- likely others!

References

E. Brady. *Type-driven development with Idris*. Simon and Schuster, 2017.

P. Wadler. Propositions as types. *Communications of the ACM*, 58 (12):75–84, 2015.