Chalmers | Göteborgs Universitet
Alejandro Russo, Computer Science and Engineering

Advanced Functional Programming TDA342/DIT260

Tuesday 14th March, 2017, Samhällsbyggnad, 8:30.

(including example solutions to programming problems)

Alejandro Russo (Anton Ekblad, tel. 0707 579 070)

- The maximum amount of points you can score on the exam: 60 points. The grade for the exam is as follows:

  Chalmers: **3**: 24 - 35 points, **4**: 36 - 47 points, **5**: 48 - 60 points.
  GU: Godkänd 24-47 points, Väl godkänd 48-60 points
  PhD student: 36 points to pass.

- Results: within 21 days.

- **Permitted materials (Hjälpmedel):** Dictionary (Ordlista/ordbok).

  You may bring up to two pages (on one A4 sheet of paper) of pre-written notes – a "summary sheet". These notes may be typed or handwritten. They may be from any source. If this summary sheet is brought to the exam it must also be handed in with the exam (so make a copy if you want to keep it).

- **Notes:**
  - Read through the paper first and plan your time.
  - Answers preferably in English, some assistants might not read Swedish.
  - If a question does not give you all the details you need, you may make reasonable assumptions. Your assumptions must be clearly stated. If your solution only works under certain conditions, state them.
  - Start each of the questions on a new page.
  - The exact syntax of Haskell is not so important as long as the graders can understand the intended meaning. If you are unsure just put in an explanation of your notation.
  - Hand in the summary sheet (if you brought one) with the exam solutions.
  - As a recommendation, consider spending around 1h for exercise 1, 1.20h for exercise 2, and 2hs for exercise 3. However, this is only a recommendation.
  - To see your exam: *by appointment (send email to Alejandro Russo)*

Problem 1: (Applicative Functors)

In the lectures, we saw an example of an applicative functor which was not a monad. The example consisted on the data type definition:

$$\textbf{data}\ \mathit{Phantom}\ o\ a = \mathit{Phantom}\ o$$

It is called *Phantom* since it contains no value of type a—it is like an empty body, a spirit, a phantom.

We saw that we can define the instances *Functor* and *Applicative* as follows.

$$\begin{array}{l} \textbf{instance}\ \mathit{Functor}\ (\mathit{Phantom}\ o)\ \textbf{where} \\ \quad \mathit{fmap}\ \_\ (\mathit{Phantom}\ o) = \mathit{Phantom}\ o \\ \textbf{instance}\ \mathit{Monoid}\ o \Rightarrow \mathit{Applicative}\ (\mathit{Phantom}\ o)\ \textbf{where} \\ \quad \mathit{pure}\ \_ \qquad\qquad\qquad\qquad\quad = \mathit{Phantom}\ 1 \\ \quad \mathit{Phantom}\ o_1 \circledast \mathit{Phantom}\ o_2 = \mathit{Phantom}\ (o_1 \cdot o_2) \end{array}$$

In these definitions, we assume a monoid structure for elements of type o, i.e. it contains an identity element 1 and a associative binary operation $(\cdot)$.

In the lectures, we showed that when o is of type *Int*, any implementation of bind, i.e.

$$(\gg=) :: \mathit{Phantom}\ \mathit{Int}\ a \rightarrow (a \rightarrow \mathit{Phantom}\ \mathit{Int}\ b) \rightarrow \mathit{Phantom}\ \mathit{Int}\ b$$

violates the left identity law.

i) (**Task**) Come up with a type o' and an implementation of **instance** *Monad* (*Phantom* o'), where *Phantom* o' is indeed a monad, i.e. it respects the monadic laws (see Figure 4). *(4p)*

Solution:

$$\begin{array}{l} \textbf{data}\ \mathit{Unit} = \mathit{Unit} \quad \texttt{-- o'} \\ \textbf{instance}\ \mathit{Monoid}\ \mathit{Unit}\ \textbf{where} \\ \quad 1 \qquad\qquad\quad = \mathit{Unit} \\ \quad (\cdot)\ \mathit{Unit}\ \mathit{Unit} = \mathit{Unit} \\ \textbf{instance}\ \mathit{Monad}\ (\mathit{Phantom}\ \mathit{Unit})\ \textbf{where} \\ \quad \mathit{return}\ \_ \qquad\qquad = \mathit{Phantom}\ \mathit{Unit} \\ \quad \mathit{Phantom}\ \mathit{Unit} \gg= \_ = \mathit{Phantom}\ \mathit{Unit} \end{array}$$

$$\begin{array}{l} \quad \mathit{return}\ a \gg= k \\ \equiv \mathit{Unit} \\ \equiv k\ a \end{array}$$

$$\begin{array}{l} \quad \mathit{ma} \gg= \mathit{return} \\ \equiv \mathit{Unit} \\ \equiv \mathit{ma} \end{array}$$

$$\begin{array}{l} \quad \mathit{ma} \gg= k \gg= l \\ \equiv \mathit{Unit} \gg= l \\ \equiv \mathit{Unit} \\ \equiv \mathit{ma} \gg= (\lambda a \rightarrow k\ a \gg= l) \end{array}$$

ii) The *composition* of two functors f and g is defined by the following data type:

$$\textbf{data}\ Comp\ c\ d\ a = Comp\ (c\ (d\ a))$$

$$\textbf{instance}\ (Functor\ c, Functor\ d) \Rightarrow Functor\ (Comp\ c\ d)\ \textbf{where}$$
$$\quad fmap\ f\ (Comp\ cda) = Comp\ (fmap\ (fmap\ f)\ cda)$$

(**Task**) Show that $Comp\ f\ g\ a$ is also a functor, so it fulfills the *identity* and *map fusion* laws (see Figure 5). In other words, you will show that the composition of functors results in a functor. *(8p)*

{-Identity -}
$id\ (Comp\ cda)$
{-by def. of id -}
$\equiv Comp\ cda$
{-by def. of id -}
$\equiv Comp\ (id\ cda)$
{-by Identity on functor c -}
$\equiv Comp\ (fmap\ id\ cda)$
{-id has type (d a) to (d a), so by Identity on functor d -}
$\equiv Comp\ (fmap\ (fmap\ id)\ cda)$
{-By def. of fmap on Comp -}
$\equiv fmap\ id\ (Comp\ cda)$

{-Map fusion -}
$fmap\ (f \circ g)\ (Comp\ cda)$
$\equiv$ {-by def. of fmap on Comp -}
$Comp\ (fmap\ (fmap\ (f \circ g))\ cda)$
{-By map fusion on d -}
$\equiv Comp\ (fmap\ (fmap\ f \circ fmap\ g)\ cda)$
{-By map fusion on c -}
$\equiv Comp\ ((fmap\ (fmap\ f) \circ fmap\ (fmap\ g))\ cda)$
{-By def. of (.) -}
$\equiv Comp\ (fmap\ (fmap\ f)\ (fmap\ (fmap\ g)\ cda))$
{-By def. fmap on Comp -}
$\equiv fmap\ f\ (Comp\ (fmap\ (fmap\ g)\ cda))$
{-By def. of fmap on Comp -}
$\equiv fmap\ f\ (fmap\ g\ (Comp\ cda))$
{-By def. of (.) -}
$\equiv (fmap\ f \circ fmap\ g)\ (Comp\ cda)$

iii) (**Task**) Applicatives are closed under functor composition, too! Define the applicative instance for the composition of two applicatives.

$$\textbf{instance}\ (Applicative\ f, Applicative\ g) \Rightarrow Applicative\ (Comp\ f\ g)\ \textbf{where}$$
$$\quad ...$$

Solution:

$$pure\ a = Comp\ \$\ pure\ (pure\ a)$$
$$Comp\ fgf \circledast Comp\ fga = Comp\ \$\ (\circledast) <\$> fgf \circledast fga$$

Show that your definitions of $pure$ and $(\circledast)$ satisfy the applicative laws (see Figure 6).

Solution: *Identity*

$pure\ id \circledast Comp\ vv$
$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}
$Comp\ (pure\ (pure\ id)) \circledast Comp\ vv$
$\equiv$ {-def. of $(\circledast)$ for $Comp\ f\ g$ -}
$Comp\ ((pure\ (\circledast) \circledast pure\ (pure\ id)) \circledast vv)$
$\equiv$ {-homomorphism for f -}
$Comp\ (pure\ (pure\ id \circledast) \circledast vv)$
$\equiv$ {-identity for g -}
$Comp\ (pure\ id \circledast vv)$
$\equiv$ {-identity for f -}
$Comp\ vv$

Composition

$pure\ f \circledast (pure\ g \circledast x)$
$\equiv$ {-composition -}
$pure\ (\circ) \circledast pure\ f \circledast pure\ g \circledast x$
$\equiv$ {-homomorphism -}
$pure\ (f\circ) \circledast pure\ g \circledast x$
$\equiv$ {-homomorphism -}
$pure\ (f \circ g) \circledast x$

$pure\ f \circledast (pure\ g \circledast x \circledast y)$
$\equiv$ {-composition -}
$pure\ (\circ) \circledast pure\ f \circledast (pure\ g \circledast x) \circledast y$
$\equiv$ {-homomorphism -}
$pure\ (f\circ) \circledast (pure\ g \circledast x) \circledast y$
$\equiv$ {-lemma -}
$pure\ ((f\circ) \circ g) \circledast x \circledast y$

$pure\ (\circ) \circledast Comp\ ff \circledast Comp\ gg \circledast Comp\ zz$
$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}
$Comp\ (pure\ (pure\ (\circ))) \circledast Comp\ ff \circledast Comp\ gg \circledast Comp\ zz$
$\equiv$ {-def. of $(\circledast)$ for $Comp\ f\ g$ -}
$Comp\ (pure\ (\circledast) \circledast pure\ (pure\ (\circ)) \circledast ff) \circledast Comp\ gg \circledast Comp\ zz$
$\equiv$ {-homomorphism for f -}
$Comp\ (pure\ (pure\ (\circ) \circledast) \circledast ff) \circledast Comp\ gg \circledast Comp\ zz$

$\equiv$ {-def. of $(<*>)$ for $Comp\ f\ g$ -}
$Comp\ (pure\ (<*>) <*> (pure\ (pure\ (\circ) <*>) <*> ff) <*> gg) <*> Comp\ zz$
$\equiv$ {-lemma for f -}
$Comp\ (pure\ ((<*>) \circ (pure\ (\circ) <*>)) <*> ff <*> gg) <*> Comp\ zz$
$\equiv$ {-def. of $(<*>)$ for $Comp\ f\ g$ -}
$Comp\ (pure\ (<*>) <*> (pure\ ((<*>) \circ (pure\ (\circ) <*>)) <*> ff <*> gg) <*> zz)$
$\equiv$ {-lemma for f -}
$Comp\ (pure\ (((<*>)\circ) \circ ((<*>) \circ (pure\ (\circ) <*>))) <*> ff <*> gg <*> zz)$
$\equiv$ {-def. of $(\circ)$ -}
$Comp\ (pure\ (\lambda x\ y\ z \to pure\ (\circ) <*> x <*> y <*> z) <*> ff <*> gg <*> zz)$
$\equiv$ {-composition for g -}
$Comp\ (pure\ (\lambda x\ y\ z \to x <*> (y <*> z)) <*> ff <*> gg <*> zz)$
$\equiv$ {-def. of $(\circ)$ and $(\$)$ -}
$Comp\ (pure\ ((\$(<*>)) \circ ((\circ) \circ ((\circ) \circ (<*>)))) <*> ff <*> gg <*> zz)$
$\equiv$ {-lemma for f -}
$Comp\ (pure\ (\$(<*>)) <*> (pure\ ((\circ) \circ ((\circ) \circ (<*>))) <*> ff) <*> gg <*> zz)$
$\equiv$ {-interchange for f -}
$Comp\ (pure\ ((\circ) \circ ((\circ) \circ (<*>))) <*> ff <*> pure\ (<*>) <*> gg <*> zz)$
$\equiv$ {-lemma for f -}
$Comp\ (pure\ (\circ) <*> (pure\ ((\circ) \circ (<*>)) <*> ff) <*> pure\ (<*>) <*> gg <*> zz)$
$\equiv$ {-composition for f -}
$Comp\ (pure\ ((\circ) \circ (<*>)) <*> ff <*> (pure\ (<*>) <*> gg) <*> zz)$
$\equiv$ {-lemma for f -}
$Comp\ (pure\ (\circ) <*> (pure\ (<*>) <*> ff) <*> (pure\ (<*>) <*> gg) <*> zz)$
$\equiv$ {-composition for f -}
$Comp\ (pure\ (<*>) <*> ff <*> (pure\ (<*>) <*> gg <*> zz))$
$\equiv$ {-def. of $(<*>)$ for $Comp\ f\ g$ -}
$Comp\ ff <*> Comp\ (pure\ (<*>) <*> gg <*> zz)$
$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}
$Comp\ ff <*> (Comp\ gg <*> Comp\ zz)$

Homomorphism

$pure\ f <*> pure\ v$
$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}
$Comp\ (pure\ (pure\ f)) <*> Comp\ (pure\ (pure\ v))$
$\equiv$ {-def. of $(<*>)$ for $Comp\ f\ g$ -}
$Comp\ ((<*>) <\$> pure\ (pure\ f) <*> pure\ (pure\ v))$
$\equiv$ {-homomorphism for f -}
$Comp\ ((pure\ f <*>) <\$> pure\ (pure\ v))$
$\equiv$ {-homomorphism for f -}
$Comp\ (pure\ (pure\ f <*> pure\ v))$
$\equiv$ {-homomorphism for g -}
$Comp\ (pure\ (pure\ (f\ v)))$
$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}
$pure\ (f\ v)$

Interchange

$Comp\ ff <*> pure\ v$

$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}

$Comp\ ff <*> Comp\ (pure\ (pure\ v))$

$\equiv$ {-def. of $(<*>)$ for $Comp\ f\ g$ -}

$Comp\ ((<*>) <\$> ff <*> pure\ (pure\ v))$

$\equiv$ {-interchange for f -}

$Comp\ ((\$pure\ v) <\$> ((<*>) <\$> ff))$

$\equiv$ {-composition for f -}

$Comp\ ((\circ) <\$> (\$pure\ v) <\$> (<*>) <\$> ff)$

$\equiv$ {-homomorphism for f -}

$Comp\ ((<*> pure\ v) <\$> ff)$

$\equiv$ {-interchange for g -}

$Comp\ ((pure\ (\$v) <*>) <\$> ff)$

$\equiv$ {-homomorphism for f -}

$Comp\ ((<*>) <\$> pure\ (pure\ (\$v)) <*> ff)$

$\equiv$ {-def. of $(<*>)$ for $Comp\ f\ g$ -}

$Comp\ (pure\ (pure\ (\$v))) <*> Comp\ ff$

$\equiv$ {-def. of $pure$ for $Comp\ f\ g$ -}

$pure\ (\$v) <*> Comp\ ff$

(8p)

Problem 2: (**Type families**)

i) Consider the following EDSL, which lets users perform basic arithmetic without having to worry about dividing by zero:

```haskell
data Exp a where
  Int  ::            Int    -> Exp Int
  Doub ::            Double -> Exp Double
  Div  :: Divide a => Exp a -> Exp a -> Exp a
  Add  :: Num a    => Exp a -> Exp a -> Exp a

class (Eq a, Num a) => Divide a where
  divide :: a -> a -> a

instance Divide Int where
  divide = div

instance Divide Double where
  divide = (/)

eval :: Exp a -> Maybe a
eval (Int x)   = Just x
eval (Doub x)  = Just x
eval (Div a b) = do
  a' <- eval a
  b' <- eval b
  if b' == 0
    then Nothing
    else Just (a' `divide` b')
eval (Add a b) = do
  a' <- eval a
  b' <- eval b
  Just (a' + b')
```

(**Task**) By using type families, you should modify the EDSL so that the *Div* constructor can divide any combination of *Int*s and *Double*s. For instance, it is possible to compute *Div* (*Int* 10) (*Doub* 2.5) and *Div* (*Doub* 2) (*Doub* 2) in your language.

For the whole exercise, you can assume the function *fromIntegral* :: (*Integral a*, *Num b*) ⇒ *a* → *b*, which takes numbers with whole-number division and remainder operations (e.g., *Integer* and *Int*), and transformed them into numbers with basic operations (e.g., *Word*, *Integer*, *Int*, *Float*, and *Double*). *(7p)*

Solution

```haskell
data Exp a where
  Int  :: Int                                  -> Exp Int
  Doub :: Double                               -> Exp Double
  Div  :: Divide a b => Exp a -> Exp b -> Exp (DivRes a b)
  Add  :: Num a      => Exp a -> Exp a -> Exp a

type family DivRes a b where
```

```
  DivRes Double a = Double
  DivRes a Double = Double
  DivRes a a      = a
class (Eq b, Num b) => Divide a b where
  divide :: a -> b -> DivRes a b
instance Divide Double Int where
  divide a b = a / fromIntegral b
instance Divide Int Double where
  divide a b = fromIntegral a / b
instance Divide Int Int where
  divide a b = a `div` b
instance Divide Double Double where
  divide a b = a / b
```

ii) The following code implements a type family (*Serialized*) and a type class (*Serialize*) which in combination are used for serializing data into tuples of words of a user-specified size. Observe that the type family works on two types.

```
type family Serialized t a where
  Serialized Word16 Int  = (Word16, Word16)
  Serialized Word16 Word = (Word16, Word16)
  Serialized Word8  Int  = (Word8, Word8, Word8, Word8)
  Serialized Word8  Word = (Word8, Word8, Word8, Word8)
    -- more cases (not relevant for the rest of the exercise)
class Serialize t a where
  serialize :: a -> Serialized t a
instance Serialize Word16 Int where
  serialize i = (fromIntegral i, fromIntegral (i `shiftR` 16))
instance Serialize Word16 Word where
  serialize w = (fromIntegral w, fromIntegral (w `shiftR` 16))
  -- more instances (not relevant for the rest of the exercise)
```

Function *shiftR* shifts the first argument right by the specified number of bits.

The type family, type class and instances are all type-correct on their own. However, attempting to apply *serialize* to any value will cause a type error:

```
main = putStrLn ("High word: " ++ show hi)
  where
    lo, hi   :: Word16
    (lo, hi) = serialize (0xDEADBEEF :: Word)
```

This happens because *serialize* returns a type family application. In this case, the type of *serialize* is of the form *Word* → *Serialized t Word*. This makes the type checker unable to infer t, even though it is obvious that the t must be *Word16* in this case.

(**Task**) Explain *why* it is in general impossible to infer a type t even if we know what the type family application $F\ t$ computes to. Think in the example above: why Haskell's type system does not choose t to be *Word16* when it sees that (*lo*, *hi*) has type (*Word16*, *Word16*)? The type error is as follows:

```
Couldn't match expected type (Word16, Word16)
                with actual type Serialized t0 Word
    The type variable t0 is ambiguous
    In the expression: serialize (3735928559 :: Word)
    In a pattern binding: (lo, hi) = serialize (3735928559 :: Word)
Failed, modules loaded: none.
```

(3735928559 is 0xDEADBEEF in the message above.) You should also describe *which additional properties* a type family definition would need to make the example above to type check, i.e. when Haskell sees *Serialized t Word*, it can infer that t must be *Word16*. *(7p)*

Solution

t can not be inferred from $F\ t$ because type families are not injective. Just like we can not infer the value of x from $f(x)$ without explicit knowledge of the inverse of f, we can not deduce t from $F\ t$.

Type families would need *injectivity* to make the example type check. That is, the property that $a\ b <=> T\ a\ T\ b$.

iii) To resolve problems like this, where the type checker does not have enough information to figure out what we want, it is common to use *proxy types*:

$$\textbf{data}\ \mathit{Proxy}\ a = \mathit{Proxy}$$

Proxies allow us to pass a type directly to a function, without having to come up with a concrete value of that type—we have the constructor *Proxy*! One instance where this is useful is when composing polymorphic functions, and we need to keep track of some intermediate result.

The following example will produce a type error, since there is no way for the compiler to infer the concrete return type of *read*, which makes impossible to choose a suitable parser from the dictionary *Read a*. More concretely, let us assume the following functions and definitions.

$$\begin{aligned}
&\mathit{read}\ \ :: \mathit{Read}\ a \Rightarrow \mathit{String} \to a \\
&\mathit{print} :: \mathit{Show}\ a \Rightarrow a \to \mathit{IO}\ () \\
&\mathit{readAndPrint} :: \mathit{String} \to \mathit{IO}\ () \\
&\mathit{readAndPrint} = \mathit{print} \circ \mathit{read}
\end{aligned}$$

We get the following type error:

```
No instance for (Read a0) arising from a use of read
    The type variable a0 is ambiguous
     In the second argument of (.), namely read
    In the expression: print . read
    In an equation for readAndPrint: readAndPrint = print . read
Failed, modules loaded: none.
```

By allowing the caller to explicitly provide a proxy with the return type of *read*, we can help the compiler to select the appropriated parser for *read*.

$$\begin{aligned}
&\mathit{read}' :: \mathit{Read}\ a \Rightarrow \mathit{Proxy}\ a \to \mathit{String} \to a \\
&\mathit{read}'\ p = \mathit{read} \\
&\mathit{readAndPrint}' :: (\mathit{Read}\ a, \mathit{Show}\ a) \Rightarrow \mathit{Proxy}\ a \to \mathit{String} \to \mathit{IO}\ () \\
&\mathit{readAndPrint}'\ p = \mathit{print} \circ (\mathit{read}'\ p)
\end{aligned}$$

Observe that proxy $p :: \mathit{Proxy}\ a$ above is not used in the body of read'. It is there merely for having an argument which involves the returning type a. By instantiating a in $\mathit{Proxy}\ a$, we can indicate which parser must be used.

```
> readAndPrint' (Proxy :: Proxy Int) "42"
42
> readAndPrint' (Proxy :: Proxy Double) "1.42"
1.42
```

(**Task**) Use proxies to fix the *serialize* function from *ii)*. Then, write an example demonstrating how to use your fixed *serialize*. *(6p)*

Solution

```
class Serialize t a where
  serialize :: Proxy t -> a -> Serialized t a
instance Serialize Word16 Int where
  serialize _ i = (fromIntegral i, fromIntegral (a `shiftR` 16))
instance Serialize Word16 Word where
  serialize _ w = (fromIntegral w, fromIntegral (a `shiftR` 16))
main = print hi
  where (lo, hi) = serialize (Proxy :: Proxy Word16) (0xDEADBEEF :: Word)
```

Problem 3: (**EDSL**) *Information-flow control* (IFC) is a promising technology to guarantee confidentiality of data when manipulated by untrusted code, i.e. code written by someone else. In IFC, data gets classified either as *public* (low) or *secret* (high), where public information can flow into secret entities but not vice versa. We encode the sensitivity of data as abstract data types, and the allowed flows of information in the type-class *CanFlowTo* – see Figure 1.

```
  -- Security level for public data
data L
  -- Security level for secret data
data H
  -- allowed flows of information
class l `CanFlowTo` l' where
  -- Public data can flow into public entities
instance L `CanFlowTo` L where
  -- Public data can flow into secret entities
instance L `CanFlowTo` H where
  -- Secret data can flow into secret entities
instance H `CanFlowTo` H where
```

Figure 1: Allowed flows of information

To build secure programs which do not leak secrets, we build a small EDSL in Haskell with two core concepts: *labeled values* and *secure computations*. Labeled values are simply data tagged with a security level indicating its sensitivity. For example, a weather report is a public piece of data, so we can model it as a public labeled string *weather_report* :: *Labeled L String*. Similarly, a credit card number is sensitive, so we model it as a secret integer *cc_number* :: *Labeled H Integer*.

A secure computation is an entity of type *MAC l a*, which denotes a computation that handles data at sensitivity level *l* and produces a result (of type *a*) of this level. In order to remain secure, secure computations can only observe data that "can flow to" the computation (see primitive *unlabel* below), and can only create labeled values provided that information from the computation "can flow to" the newly created labeled value (see primitive *label* below). We describe the API for the EDSL in Figure 2, and provide a *shallow-embedded* implementation for the API in Figure 3.

With our EDSL now, you can write functions which keep secrets! For instance, imagine a function which takes the salary of a employee in a certain position (sensitive information[1]) and determines if it is above the average.

```
isAbove :: Labeled H Salary → Labeled L Salary → MAC H Bool
```

Function *isAbove* takes the employee's salary (see argument of type *Labeled H Salary*) and the average (see argument of type *Labeled L Salary*) and returns a *MAC H*-computation indicating that the resulting boolean is sensitive—after all, it depends on the employee's salary! If the returning computation were *MAC L Bool*, then *isAbove* will not type-check: it would be impossible to unwrap the employee's salary using *unlabel*.

i) (**Task**) Take the EDSL and create a monad transformer for it, which we call *MACT*.

```
data MACT l m a
```

The idea is that when applying *MACT* to a monad *m*, then we obtain a monad capable to perform the effects of *m* as well as keeping sensitive information secret. For instance, *MACT l* (*State s*) *a* is a secure state monad with state *s*.

[1] In Sweden, salaries are public information but that is not the case in other countries.

```
-- Types
newtype Labeled l a
newtype MAC l a
-- Labeled values
label    :: (l `CanFlowTo` h) => a -> MAC l (Labeled h a)
unlabel  :: (l `CanFlowTo` h) => Labeled l a -> MAC h a
-- MAC monad
return   :: a -> MAC l a
(>>=)    :: MAC l a -> (a -> MAC l b) -> MAC l b
joinMAC  :: (l `CanFlowTo` h) => MAC h a -> MAC l (Labeled h a)
-- Run function
runMAC   :: MAC l a -> a
```

Figure 2: EDSL API

```
-- Types
newtype Labeled l a = MkLabeled a
newtype MAC l a     = MkMAC a
-- Labeled values
label                 = MkMAC ∘ MkLabeled
unlabel (MkLabeled v) = MkMAC v
-- MAC operations
joinMAC (MkMAC t) = MkMAC (MkLabeled t)
runMAC (MkMAC a) = a
instance Monad (MAC l) where
  return = MkMAC
  MkMAC a >>= f = f a
```

Figure 3: Shallow-embedded implemention

Define an implementation for $MACT\ l\ m\ a$ and give the type-signature and implementation of the following operations on transformed monads.

$$
\begin{array}{ll}
return & :: \ldots \\
(\gg\!=) & :: \ldots \\
t\_label & :: \ldots \\
t\_unlabel & :: \ldots \\
t\_joinMAC & :: \ldots \\
t\_runMAC & :: \ldots
\end{array}
$$

Help: We provide the type-signature of t_label and t_runMAC.

$$
\begin{array}{ll}
t\_label & :: (Monad\ m, l\ \text{`}CanFlowTo\text{`}\ h) \Rightarrow a \rightarrow MACT\ l\ m\ (Labeled\ h\ a) \\
t\_runMAC & :: MACT\ l\ m\ a \rightarrow m\ a
\end{array}
$$

Observe that the type-signature looks almost similar to those in MAC where $MACT$ is used instead.

Hint: In the definition of $(\gg\!=)$, reuse as much as possible the monadic operators from monads m and MAC.

(10p)

Solution:

$$
\begin{array}{l}
\textbf{data}\ MACT\ l\ m\ a = MkMACT\ (MAC\ l\ (m\ a)) \\
\textbf{instance}\ Monad\ m \Rightarrow Monad\ (MACT\ l\ m)\ \textbf{where} \\
\quad return = MkMACT \circ return \circ return \\
\quad (MkMACT\ mac) \gg\!= f = MkMACT\ (mac \gg\!= \lambda ma \rightarrow return\ (ma \gg\!= t\_runMAC \circ f)) \\
t\_label :: \quad (Monad\ m, CanFlowTo\ l\ h) \Rightarrow a \rightarrow MACT\ l\ m\ (Labeled\ h\ a) \\
t\_label\ a = return\ (MkLabeled\ a) \\
t\_unlabel :: (Monad\ m, CanFlowTo\ l\ h) \Rightarrow Labeled\ l\ a \rightarrow MACT\ h\ m\ a \\
t\_unlabel\ (MkLabeled\ v) = return\ v \\
t\_joinMAC :: (Monad\ m, CanFlowTo\ l\ h) \Rightarrow MACT\ h\ m\ a \rightarrow MACT\ l\ m\ (Labeled\ h\ a) \\
t\_joinMAC\ (MkMACT\ (MkMAC\ ma)) = (MkMACT \circ return)\ (ma \gg\!= return \circ MkLabeled) \\
t\_runMAC\ :: MACT\ l\ m\ a \rightarrow m\ a \\
t\_runMAC\ (MkMACT\ mac) = runMAC\ mac
\end{array}
$$

ii) Assuming that m and MAC are monads, you need to prove that $MACT\ l\ m\ a$ is also a monad, i.e. you should show that your monad transformer generates monads! The monad laws are shown in Figure 4. In the proofs, you are likely to write the monadic operators *return* and $(\gg\!=)$. Since you would be dealing with more than one monad, it might get confusing to determine which monad you are referring to. Therefore, you must indicate as a subindex the name of the monad that operations refers to. For example, $return_m$, $return_{MAC}$, or $return_{MACT}$ refers to the *return* operation for monad m, MAC, and $MACT$, respectively. Finally, if you need auxiliary properties, you should provide a proof for them, too!

a) Prove left identity. *(2p)*

b) Prove right identity. *(2p)*

c) Prove associativity. *(6p)*

Hint: You might need to prove an auxiliary property about t_runMAC, $\gg\!=_m$, and $\gg\!=_{MACT}$.

Left identity:

-- Auxiliary property
$t\_runMAC \circ return_{MACT} \equiv return_m$

$(t\_runMAC \circ return_{MACT})\ x \equiv$
-- Composition of functions
$t\_runMAC\ (return_{MACT}\ x) \quad \equiv$
-- Definition of return
$t\_runMAC\ ((MkMACT \circ return_{MAC} \circ return_m)\ x)) \equiv$
-- By composition of functions
$t\_runMAC\ (MkMACT\ (return_{MAC} \circ return_m)\ x) \quad \equiv$
-- By definition of t_runMAC
$runMAC\ ((return_{MAC} \circ return_m)\ x) \quad \equiv$
-- By composition of functions
$runMAC\ (return_{MAC}\ (return_m\ x)) \quad \equiv$
-- Definition of return
$runMAC\ (MkMAC\ (return_m\ x)) \quad \equiv$
-- Definition of runMAC
$return_m\ x$

-- Left identity
$tmac\ \gg\!=_{MACT}\ f \equiv$
-- By pattern matching tmac is of the form (MkMACT mac)
$(MkMACT\ mac)\ \gg\!=_{MACT}\ f \equiv$
-- Def bind
$MkMACT\ (mac\ \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}\ (ma\ \gg\!=_m\ (t\_runMAC \circ return_{MACT}))$
-- By auxiliary property
$MkMACT\ (mac\ \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}\ (ma\ \gg\!=_m\ return_m))$
-- Left identity of m
$MkMACT\ (mac\ \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}\ ma)$
-- Eta-contraction
$MkMACT\ (mac\ \gg\!=_{MAC}\ return_{MAC})$
-- Left identity MAC
$MkMACT\ mac$
-- By definition of tmac
$tmac$

Right identity:

-- Auxiliary property
$MkMACT \circ MkMAC \circ t\_runMAC \equiv id$

-- Auxiliary property

$$MkMACT\ (MkMAC\ (t\_runMAC\ tmac)) \equiv$$

-- By pattern matching, tmac is of the form MkMACT mac

$$MkMACT\ (MkMAC\ (t\_runMAC\ (MkACT\ mac))) \equiv$$

-- Definition of t_runMAC

$$MkMACT\ (MkMAC\ (runMAC\ mac)) \equiv$$

-- By pattern matching mac is of the form MkMAC m

$$MkMACT\ (MkMAC\ (runMAC\ (MkMAC\ m))) \equiv$$

-- By definition of runMAC

$$MkMACT\ (MkMAC\ m) \equiv$$

-- By definition of mac

$$MkMACT\ mac \equiv$$

-- By definition of tmac

$$tmac \equiv$$

-- By definition of id

$$id\ tmac$$

-- Right identify

$$return_{MACT}\ x \ \gg\!=_{MACT}\ f \equiv$$

-- By definition of return

$$(MkMACT \circ return_{MAC} \circ return_{m})\ x \ \gg\!=_{MACT}\ f \equiv$$

-- By function composition

$$MkMACT\ (return_{MAC}\ (return_{m}\ x)) \ \gg\!=_{MACT}\ f \equiv$$

-- By definition of bind

$$MkMACT\ (return_{MAC}\ (return_{m}\ x) \ \gg\!=_{MAC} \ \lambda ma \rightarrow return_{MAC}\ (ma \ \gg\!=_{m}\ (t\_runMAC \circ f))) \equiv$$

-- By right identity of return in MAC

$$MkMACT\ (return_{MAC}\ (return_{m}\ x \ \gg\!=_{m}\ (t\_runMAC \circ f))) \equiv$$

-- By right identity of return in m

$$MkMACT\ (return_{MAC}\ ((t\_runMAC \circ f)\ x)) \equiv$$

-- By definition of return

$$MkMACT\ (MkMAC\ ((t\_runMAC \circ f)\ x)) \equiv$$

-- By function composition

$$MkMACT\ (MkMAC\ (t\_runMAC\ (f\ x))) \equiv$$

-- By auxiliary property

$$MkMACT\ (MkMAC\ (t\_runMAC\ (f\ x))) \equiv$$

--

$$f\ x$$

Associativity:

-- Auxiliary property

$$\lambda x \rightarrow t\_runMAC\ (f_1\ x \ \gg\!=_{MACT}\ f_2) \equiv \lambda x \rightarrow (t\_runMAC \circ f_1)\ x \ \gg\!=_{m}\ (t\_runMAC \circ f_2)$$

-- Extensionality, we apply functions to an argument a and prove

$$t\_runMAC\ (f_1\ a \ \gg\!=_{MACT}\ f_2) \equiv$$

-- f1 a is of the form MkMACT mac

$t\_runMAC\ (MkMACT\ mac \gg\!=_{MACT} f_2) \equiv$

-- Definition of bind

$t\_runMAC\ (MkMACT\ (mac \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}$
$(ma \gg\!=_m (t\_runMAC \circ f_2)))) \equiv$

-- Definition of t_runMAC

$runMAC\ (mac \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}$
$(ma \gg\!=_m (t\_runMAC \circ f_2))) \equiv$

-- By pattern matching of bind mac is of the form MkMAC m

$runMAC\ (MkMAC\ m \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}$
$(ma \gg\!=_m (t\_runMAC \circ f_2))) \equiv$

-- By definition of bind

$runMAC\ (return_{MAC}\ (m \gg\!=_m (t\_runMAC \circ f_2))) \equiv$

-- Definition of return

$runMAC\ (MkMAC\ (m \gg\!=_m (t\_runMAC \circ f_2))) \equiv$

-- By definition of runMAC

$m \gg\!=_m (t\_runMAC \circ f_2) \equiv$

-- By definition of runMAC

$(runMAC\ (MkMAC\ m)) \gg\!=_m (t\_runMAC \circ f_2) \equiv$

-- By definition of MkMAC m

$runMAC\ mac \gg\!=_m (t\_runMAC \circ f_2) \equiv$

-- By definition of t_runMAC

$t\_runMAC\ (MkMACT\ mac) \gg\!=_m (t\_runMAC \circ f_2) \equiv$

-- By definition of MkMACT mac

$t\_runMAC\ (f\ a) \gg\!=_m (t\_runMAC \circ f_2) \equiv$

-- By function composition

$(t\_runMAC \circ f)\ a \gg\!=_m (t\_runMAC \circ f_2)$

$tmac \gg\!=_{MACT} (\lambda x \rightarrow f_1\ x \gg\!=_{MACT} f_2) \equiv$

-- By pattern matching, tmac is of the form MkMACT mac

$(MkMACT\ mac) \gg\!=_{MACT} (\lambda x \rightarrow f_1\ x \gg\!=_{MACT} f_2) \equiv$

-- By definition of bind

$MkMACT\ (mac \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}$
$(ma \gg\!=_m (t\_runMAC \circ (\lambda x \rightarrow f_1\ x \gg\!=_{MACT} f_2)))) \equiv$

-- By auxiliary property

$MkMACT\ (mac \gg\!=_{MAC} \lambda ma \rightarrow$
$return_{MAC}$
$(ma \gg\!=_m (\lambda x \rightarrow (t\_runMAC \circ f_1)\ x \gg\!=_m (t\_runMAC \circ f_2)))) \equiv$

-- By pattern matching, mac is of the form MkMAC m

$MkMACT\ (MkMAC\ m \gg\!=_{MAC} \lambda ma \rightarrow$
$return_{MAC}$
$(ma \gg\!=_m (\lambda x \rightarrow (t\_runMAC \circ f_1)\ x \gg\!=_m (t\_runMAC \circ f_2)))) \equiv$

-- By definition of bind

$MkMACT\ (return_{MAC}\ (m \gg\!=_m (\lambda x \rightarrow (t\_runMAC \circ f_1)\ x \gg\!=_m (t\_runMAC \circ f_2)))) \equiv$

-- By associativity of m

$$MkMACT\ (return_{MAC}\ ((m \gg\!=_m (t\_runMAC \circ f_1)) \gg\!=_m (t\_runMAC \circ f_2))) \equiv$$
-- Left identity of MAC

$$MkMACT\ (return_{MAC}\ (m \gg\!=_m (t\_runMAC \circ f_1))$$
$$\gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}\ (ma \gg\!=_m (t\_runMAC \circ f_2))) \equiv$$
-- Definition of bind

$$(MkMACT\ (return_{MAC}\ (m \gg\!=_m (t\_runMAC \circ f_1))))$$
$$\gg\!=_{MACT} f_2 \equiv$$
-- By definition of bind

$$(MkMACT\ (MkMAC\ m \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}\ (ma \gg\!=_m (t\_runMAC \circ f_1))))$$
$$\gg\!=_{MACT} f_2 \equiv$$
-- By definition of mac

$$(MkMACT\ (mac \gg\!=_{MAC} \lambda ma \rightarrow return_{MAC}\ (ma \gg\!=_m (t\_runMAC \circ f_1))))$$
$$\gg\!=_{MACT} f_2 \equiv$$
-- Definition of bind

$$(MkMACT\ mac \gg\!=_{MACT} f_1) \gg\!=_{MACT} f_2 \equiv$$
-- tmac is of the form MkMACT mac

$$(tmac \gg\!=_{MACT} f_1) \gg\!=_{MACT} f_2$$

Appendix

$$\textbf{class}\ \mathit{Monad}\ m\ a\ \textbf{where}$$
$$\mathit{return} :: a \rightarrow m\ a$$
$$(\gg\!=) :: m\ a \rightarrow (a \rightarrow m\ b) \rightarrow m\ b$$

Left Identity
$$\mathit{return}\ x \gg\!= f \equiv f\ x$$

Right Identity
$$m \gg\!= \mathit{return} \equiv m$$

Associativity (x does not appear in m_2 and m_3)
$$(m \gg\!= k_1) \gg\!= k_2 \equiv m \gg\!= (\lambda x \rightarrow k_1\ x \gg\!= k_2)$$

Figure 4: Monads

Functor type-class
$$\textbf{class}\ \mathit{Functor}\ c\ \textbf{where}\ \mathit{fmap} :: (a \rightarrow b) \rightarrow c\ a \rightarrow c\ b$$

Identity
$$\mathit{fmap}\ \mathit{id} \equiv \mathit{id}\ \textbf{where}\ \mathit{id} = \lambda x \rightarrow x$$

Map fusion
$$\mathit{fmap}\ (f \circ g) \equiv \mathit{fmap}\ f \circ \mathit{fmap}\ g$$

Figure 5: Functors

Applicative type-class
$$\textbf{class}\ \mathit{Applicative}\ c\ \textbf{where}\ \mathit{pure} :: a \rightarrow c\ a \qquad (\circledast) :: c\ (a \rightarrow b) \rightarrow c\ a \rightarrow c\ b$$

Identity
$$\mathit{pure}\ \mathit{id} \circledast \mathit{vv} \equiv \mathit{vv}\ \textbf{where}\ \mathit{id} = \lambda x \rightarrow x$$

Composition
$$\mathit{pure}\ (\circ) \circledast \mathit{ff} \circledast \mathit{gg} \circledast \mathit{zz} \equiv \mathit{ff} \circledast (\mathit{gg} \circledast \mathit{zz})$$

Homomorphism
$$\mathit{pure}\ f \circledast \mathit{pure}\ v \equiv \mathit{pure}\ (f\ v)$$

Interchange
$$\mathit{ff} \circledast \mathit{pure}\ v \equiv \mathit{pure}\ (\$v) \circledast \mathit{ff}$$

Figure 6: Applicative functors