

TFG

1.a: Introducción

1.b: Introduction

2. Preliminares

2.1: CAVI-ART Project

En esta seccion explicamos el proyecto CAVI-ART el cual es un proyecto actualmente en desarrollo en la UCM y del cual forma parte mi TFG.

La plataforma **CAVI-ART** consiste en un conjunto de herramientas pensadas para ayudar al programador en la validacion de programas escritos en diferentes lenguajes. Estas ayudas incluyen la extracción automática y prueba de condiciones de verificación, la prueba automática de terminación (siempre que sea decidible usando la tecnología actual), la inferencia automática de algunos invariantes y la generación automática y ejecución de casos de prueba. [1]–[3]

Un aspecto clave de la plataforma es su Representación Intermedia de los programas (de aquí en adelante IR). Programas escritos en lenguajes convencionales como C++, Java, Haskell, OCaml y otros se traducen a la IR, sobre la cual se realizan todas las actividades mencionadas anteriormente. La intencion es programar la mayor parte de la plataforma una sola vez, de manera que sea independiente del lenguaje de programación utilizado.

El diseño de la IR fue realizado con la intencion de facilitar las tareas nombradas con anterioridad tanto como fuera posible. Un diseño simple que cuenta con muy pocas construcciones primitivas. Nunca se pensó en la IR como código ejecutable sino como una sintaxis abstracta sobre la cual resultaria fácil realizar análisis estático y verificación formal. Pero en los últimos meses se decidió convertir la IR en código ejecutable, sobre la cual sería posible ejecutar pruebas independientes del lenguaje, y construir herramientas de testeo independientes del lenguaje. La mayoría del trabajo hecho en este campo y la mayoría de las herramientas de testeo existentes están ligadas a un lenguaje en concreto.

Dicho trabajo de traducir la IR a Haskell y hacer ejecutables los asertos se engloba dentro del trabajo de fin de grado de Marta Aracil Muñoz con título **Implementación de asertos ejecutables para una plataforma de verificación**.

Esquema del proyecto CAVI-ART(Fig 1)

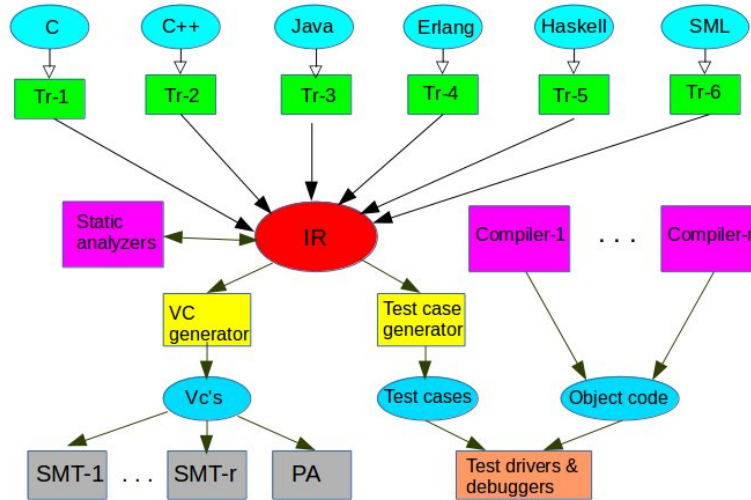


Figure 1: Esquema del proyecto CAVI-ART

2.2: QuickCheck

Quickcheck [4] es una herramienta de Haskell pensada para probar funciones escritas en dicho lenguaje sobre un conjunto de casos de prueba generados de manera aleatoria. Dicho programa resultó ser de gran ayuda pues tiene ideas similares a lo que queríamos conseguir con nuestro proyecto ya que se trata también de un sistema de prueba tipo caja negra. Aunque también cuenta con algunas diferencias sobre todo en la generación de los casos de prueba, ya que **Quickcheck** los genera de manera aleatoria mientras que nuestro proyecto los genera de manera exhaustiva.

Ejemplo de funcionamiento del programa

Vamos a trabajar en este caso con la siguiente propiedad de las listas, cierta para cualquier lista finita.

```
prop_RevApp xs ys =
  reverse (xs++ys) == reverse ys++reverse xs
```

Ahora lanzamos el programa **Quickcheck** para comprobar si pasa todos los casos de prueba.

```
Main> quickCheck prop_RevApp
OK: passed 100 tests.
```

Veamos ahora que pasa en caso de que nuestra función no esté bien definida.

```
prop_RevApp2 xs ys =
  reverse (xs++ys) == reverse xs++reverse ys
```

Al ejecutar la nueva función desde **Quickcheck**.

```
Main> quickcheck prop_RevApp2
Falsifiable, after 1 tests:
[2]
[-2,1]
```

Aquí podemos observar que en caso de fallo **Quickcheck** nos devuelve el contraejemplo de tamaño mínimo. Lo que nos dice esta vez es que nuestra definición ha fallado en el primer test y que en dicho caso las respectivas listas para las que ha sido probado falso son [2] y [-2,1].

Leyes condicionales

En algunos casos las leyes que queremos definir no pueden ser representadas mediante una simple función y solo son ciertas bajo unas precondiciones muy concretas. Para dichos casos **Quickcheck** cuenta con el operador de implicación `==>` para representar dichas leyes condicionales. Por ejemplo una ley tan simple como la siguiente:

```
x <= y ==> max x y == y
```

Puede ser representada por la siguiente definición.

```
prop_MaxLe :: Int -> Int -> Property
prop_MaxLe x y = x <= y ==> max x y == y
```

En este ejemplo podemos observar que el resultado de la función es de tipo **Property** en vez de **Bool**, lo cual es debido a que en el caso de las leyes condicionales en vez de probar la propiedad para 100 casos de prueba aleatorios, esta es probada contra 100 casos que cumplan la precondición establecida. Si uno de los candidatos no cumple la propiedad este será descartado y se considerará el siguiente. **Quickcheck** genera un máximo de 1000 casos de prueba y si entre ellos no se han encontrado al menos 100 que cumplan la precondición simplemente informa al usuario cuantos se han encontrado que la cumplan. Dicho límite está pensado para que el programa no busque indefinidamente en caso de que no existan más casos que cumplan dicha precondición.

Monitorizando los datos

Al testear propiedades debemos tener cuidado, pues quizás parezca que hemos probado una propiedad a fondo para estar seguros de su credibilidad pero esta

simplemente ser aparente. Voy a intentar ejemplificarlo usando la inserción en una lista ordenada.

```
prop_Insert :: Int -> [Int] -> Property
prop_Insert x xs =
  ordered xs ==>
    classify (null xs) "trivial" $
      ordered (insert x xs)
```

Esto nos permite saber cuantas de las pruebas se realizaron sobre una lista vacía. En cuyo caso la condición de **ordered xs** es trivial. Si ejecutamos esta nueva función con **Quickcheck** obtenemos el siguiente mensaje.

```
Ok, passed 100 tests (43% trivial)
```

Es decir que el 43% de los tests realizados son sobre una lista vacía.

Pero a su vez **Quickcheck** nos ofrece la posibilidad de un mejor análisis, más allá de etiquetar uno de los casos que nos interese. Podemos realizar una especie de histograma, utilizando la palabra reservada **collect**, que nos dará una mayor información de la distribución de los casos de prueba, por ejemplo en este caso según su longitud.

```
prop_Insert :: Int -> [Int] -> Property
prop_Insert x xs =
  ordered xs ==>
    collect (length xs) $
      ordered (insert x xs)
```

Al ejecutarlo obtendríamos un resultado como el siguiente, separado según los tamaños de las listas.

```
Ok, passed 100 tests.
49% 0.
32% 1.
12% 2.
4% 3.
2% 4.
1% 5.
```

Definir generadores

En primer lugar vamos a empezar definiendo la clase de tipos **Arbitrary** de la cual un tipo es una instancia si podemos generar casos aleatorios de él. La manera de generar los casos de prueba depende por supuesto del tipo.

```
class Arbitrary a where
  arbitrary :: Gen a
```

Gen es un tipo abstracto representando el generador para el tipo **a**, que bien puede ser el generador por defecto o uno creador por el programador para el caso específico. El tipo abstracto **Gen** se define como:

```
newtype Gen a = Gen (Rand -> a)
```

En esta definición **Rand** se trata de un número semilla aleatorio y un generador no es más que una función que puede generar una **a** de una manera pseudoaleatoria.

Ahora vamos a echarle un vistazo a las posibilidades que nos ofrece **Quickcheck** a la hora de definir los generadores de casos para los tipos de datos definidos por el usuario.

Supongamos que definimos el tipo **Colour** de la siguiente manera

```
data Colour = Red | Blue | Green
```

Un ejemplo de un generador para dicho tipo en el cual los tres colores son equiprobables sería

```
instance Arbitrary Colour where
  arbitrary = oneof [return Red | return Blue | return Green]
```

en el cual podemos observar el funcionamiento de la función **oneof** que se encarga de devolver uno de los elementos de la lista dando la misma probabilidad a todos ellos.

Vamos a observar otro ejemplo, un generador para listas de un tipo **a** arbitrario.

```
instance Arbitrary a => Arbitrary [a] where
  arbitrary = frequency
    [ (1, return [])
    , (4, liftM2 (:) arbitrary arbitrary)]
```

En ella usamos la función **frequency** la cual funciona similar a **oneof** pero dándole pesos diferentes a los diferentes casos. En este ejemplo le damos peso 1 a la lista vacía y peso 4 a la lista compuesta de otras 2 listas, con lo cual obtenemos casos de prueba de una longitud media de 4 y evitando de esta manera el problema visto antes de que la mayoría de los casos de prueba sean listas vacías.

2.3: Librería Generics de GHC

El siguiente punto a tratar en estos preliminares es la librería **Generics** del compilador GHC de Haskell[5], una librería utilizada principalmente para la generación automática de instancias de funciones correctas para cualquiera que sea el tipo de datos. En el caso de este proyecto **Generics** apareció como una librería necesaria para escribir nuestro programaz de manera que funcionaran para cualquier tipo de datos, incluidos los definidos por el usuario y de los cuales no podemos tener conocimiento en adelantado.

Dicha librería dentro de Haskell es posible por dos características del propio lenguaje:

1. En primer lugar la existencia de las clases de tipos, que actúan como una interfaz de Java definiendo el comportamiento de las operaciones sobre los tipos que pertenecen a dicha clase.
2. En segundo lugar, gracias a la existencia del polimorfismo de tipo Ad-hoc. Este nos permite abstraer una operación sobre una o más clases de tipos simplemente con la condición de que el tipo concreto tenga unas propiedades como por ejemplo que sea ordenable (pertenezca a la clase **Ord**) o que sus elementos admitan comparaciones por igualdad (que pertenezca a la clase **Eq**).

En el caso de la librería **Generics** esta permite definir funciones genéricas para cualquiera que sea el tipo al que se apliquen ya que dicha definición se realiza sobre la estructura del tipo y teniendo en cuenta que todo tipo algebraico en Haskell utiliza un número pequeño de construcciones (uniones, productos cartesianos, recursión y tipos básicos).

En el caso de esta librería, la clase de tipos principal (**Generic**) expresa la posibilidad de describir un tipo de datos en términos de un conjunto simple de combinadores. Estos combinadores son:

- En primer lugar debemos definir el comportamiento deseado para los tipos de datos vacíos (representados con **V1** en **Generics**)
- En segundo lugar debemos definir el comportamiento deseado para los tipos de datos cuyo constructor carece de parámetros (representados con **U1** en **Generics**).
- En tercer lugar se trata de definir el comportamiento para los tipos compuestos de acuerdo a como se forman. En Haskell los tipos compuestos solo pueden definirse mediante dos operaciones partiendo de los tipos básicos. Estas dos operaciones son la suma y el producto de tipos (representados como **:+:** y **:*:** respectivamente en **Generics**). Debemos definir como queremos que sea el comportamiento de las funciones de nuestra clase genérica de acuerdo a como se forma nuestro tipo a partir de los tipos básicos.
- Por último están dos tipos para representar meta-información y etiquetado de tipos (representados respectivamente por **M1** y **K1**), que nos permitirán definir el comportamiento esperado para las funciones cuando esta depende de las etiquetas o parte de la meta-información del tipo.

Una vez definidas las funciones para estos cinco diferentes combinadores es necesario definir algunas instancias para los tipos predefinidos como **Int**, **Char**, **Boolean**... de manera que si el usuario crea un tipo complejo como por ejemplo un Diccionario con valores de **Int** como clave y **Char** como valores tengamos un punto de partida para construir mediante **Generics** las instancias en nuestra clase para los nuevos tipos de datos.

2.4 Template Haskell

En este apartado trataremos sobre **Template Haskell** [6], una extensión sobre el lenguaje original que añade la posibilidad de realizar metaprogramación en Haskell, de una manera similar al sistema de templates de C++, de ahí su nombre, permitiendo a los programadores computar parte de la generación de código en tiempo de compilación dependiendo de las necesidades.

Un ejemplo de la idea básica

Imaginemos que escribir una función para imprimir un valor en Haskell siguiendo el estilo de C. Nos gustaría poder escribir algo como esto en Haskell:

```
printf "Error: %s on line %d." msg line
```

El caso es que en Haskell uno no puede definir **printf** de una manera tan sencilla pues su tipo depende del valor de su primer argumento. En **Template Haskell** en cambio podemos definir **printf** de manera que sea definido por el usuario, eficiente y garantice la seguridad de tipos de Haskell.

```
$(printf "Error: %s on line %d") msg line
```

El símbolo \$ indica “evaluar en tiempo de compilación”. La llamada a la función **printf** devuelve a Haskell una expresión que es insertada en el lugar de la llamada después de lo cual se puede realizar la compilación de la expresión. Por ejemplo el código entre parentesis:

```
$(printf "Error: %s on line %d")
```

lo traduce en la siguiente expresión lambda en Haskell

```
(\ s0 -> \ n1 -> "Error: " ++ s0 ++ " on line " ++ show n1)
```

Sobre la cual se aplicará la comprobación de tipos y se aplicará sobre **msg** y **line**

Como usar template Haskell

Lo primero que hay que resaltar es el hecho que las funciones de **Template Haskell** que son ejecutadas en tiempo de compilación están escritas en el mismo lenguaje que las funciones utilizadas en tiempo de ejecución. Una gran ventaja de esta aproximación es que todas las librerías existentes y técnicas usadas en Haskell pueden ser utilizadas directamente en Template Haskell. Por otro lado, una de las posibles desventajas de esta aproximación puede ser la necesidad de tener que utilizar notaciones como “\$” o “[|]” (conocidas como **splicing** y **quasi-quotes**) para especificar que partes del código se deben ejecutar en tiempo de ejecución y cuales en tiempo de compilación.

En los ejemplos más sencillos como el anteriormente presentado sobre como escribir una función printf en Template Haskell la notación del **splicing** o la

quasi-quotation pueden resultar de gran ayuda. El problema es que tan pronto como empezamos a hacer cosas más complejas en meta-programación esta notación deja de ser suficiente. Por ejemplo no es posible definir una función para seleccionar el *i*-ésimo elemento de una tupla de *n* elementos usando solo esas dos notaciones. Dicha función en **Template Haskell** sería así.

```

sel :: Int -> Int -> ExpQ
sel i n = [| \x -> $(caseE [| x |] [alt]) |]
    where alt :: Match
          alt = simpleM pat rhs

pat :: PatQ
pat = ptup (map pvar as)

rhs :: ExpQ
rhs = var (as !! (i-1))

as :: [String]
as = ["a" ++ show i | i <- [1..n]]

```

Para explicar un poco este código vamos a empezar de abajo a arriba, para entender las partes que usaremos después en la función principal **sel**. En primer lugar **as** lo que hace es crear una lista de nombres de *aes* desde *a1* hasta *an*. La segunda de ellas, **rhs** se encarga de coger el *i*-ésimo elemento de la lista de *aes* y devolverlo como una variable de tipo **ExpQ** que es el tipo utilizado en **Template Haskell** para las expresiones. La función **pat** transforma en primer lugar la lista de **Strings** en una lista de variables de tipo **PatQ** que es el tipo utilizado en TH para referirse a los patrones y después junta dicha lista en una tupla de tipo **PatQ**. Después al realiza un emparejamiento de la tupla tipo **PatQ** con el **rhs** mediante la función **simpleM** (simple Match). Finalmente la función **caseE** que toma como parametros una variable *x* (de tipo **ExpQ** como indica la quasi-quotation alrededor de *x*) y el emparejamiento devuelto por **alt**, realizando la sustitución de la *x* al lado izquierdo de la flecha por el patrón correspondiente y colocando al lado izquierdo de la flecha la **ExpQ** devuelta por **rhs** que es elemento de la tupla tomado.

Esta función se traduciría a una expresión lambda que por ejemplo si llamáramos a **sel 4 6** es decir el cuarto elemento de una tupla de 6 tendría esta forma

```
(\ (a1,a2,a3,a4,a5,a6) -> a4)
```

Cosificación (Reification)

La **cosificación** es la herramienta presente en **Template Haskell** para permitir al programador preguntar sobre el estado de la tabla de símbolos que guarda el compilador. Por ejemplo se puede escribir un código como el siguiente:

```
module M where
```

```

data T a = Tip a | Fork (T a) (T a)

repT :: Decl
repT = reifyDecl T

lengthType :: Type
lengthType = reifyType length

percentFixity :: Q Int
percentFixity = reifyFixity (%)

here :: Q String
here = reifyLocn

```

La primera de las funciones declaradas devuelve un resultado de tipo **Decl** (equivalente a **Q Dec**), representando la declaración del tipo **T**. El siguiente computo **reifyType length** devuelve un resultado de tipo **Type** (equivalente a **Q Typ**) representando el conocimiento del compilador sobre el tipo de la función **length**. En tercer lugar **reifyFixity** devuelve la “fixity” de los argumentos de la función lo cual es muy útil cuando se quiere deducir como imprimir algo. Finalmente **reifyLocn** devuelve un resultado de tipo **Q String** que representa la posición en el código fuente desde donde se ejecutó **reifyLocn**.

De esta manera la cosificación devuelve un resultado que puede ser analizado y utilizado en otros cálculos, pero hay que recordar que al tratarse de una herramienta del lenguaje para acceder a la tabla de símbolos y estar encapsulado dentro de la monada **Q** no puede ser usada como una función, por ejemplo con la función **map** (**map reifyType xs** sería incorrecto).

3. Nuestra propuesta: las clases **Allv**, **Sized** y **Arbitrary**

3.1: Black box testing en nuestro contexto

En cuanto al mundo del testing existen dos grandes posibilidades, sistemas de tipo caja negra o sistemas de tipo caja blanca. En primer lugar los de caja negra son aquellos sistemas de testing que no se basan en la estructura interna si no que trabajan únicamente con la entrada sobre la que aplican una precondition y la salida sobre la que comprueban si cumple las postcondiciones establecidas. En cambio los de caja blanca testean no solo las entradas y salidas del programa aplicandoles precondiciones y comprobando la postcondiciones si no que además se basan en la estructura interna del programa para realizar la generación de casos de prueba de forma que se cubra todo el texto del programa. Segun el criterio de cobertura deseado se pueden generar casos para ejercitar todas las condiciones o todas las ramas o todos los caminos.

En el caso de nuestro proyecto nos decidimos por el método de caja negra pues queríamos conseguir un sistema válido para poder probar cualquier programa sin necesidad de tener que adaptar nuestra plataforma para cada nuevo programa, es decir que funcionase fuese cual fuese el programa bajo prueba. Esa es una de las desventajas del testeo de tipo caja blanca que para poder comprobar partes de la estructura interna de un programa tienes que adaptar la plataforma para cada uno de los nuevos programas.

La idea principal detras de nuestro proyecto era principalmente la inmediatez y la comodidad del usuario, es decir que para probar un programa no necesitara escribir código extra aparte del ya existente programa si no que solo debe especificar como quiere que se generen los casos de prueba y los rangos de los dominios a usar y con eso ser ya capaz de probar su programa lo cual se ajusta mucho más a la idea de testeo de caja negra.

Las posibles maneras en las que el usuario puede especificar que se generen los casos de prueba para cada argumento son 3: - O generar n casos de prueba de manera aleatoria. - O coger n casos de prueba de tamaño menor o igual a m . - O coger los n primeros casos de prueba de la lista de todos los valores, sea cual sea su tamaño.

3.2: Sized

En la estructura del proyecto **Sized** está pensada como la clase externa que hereda de **Allv**. A su vez es la clase que se ocupa de a partir de la lista **allv** de un tipo de datos devolver la lista de los casos de prueba. Esto se realiza mediante dos funciones: - **sized** que devuelve los n primeros casos menores o iguales a un tamaño m . - **smallest** que devuelve los n primeros casos de la lista **allv** según su posición y sin importar su tamaño.

En esta clase del proyecto decidimos implementar el concepto de tamaño de un elemento mediante la librería **Generics** explicada anteriormente pues de esa manera podríamos tener una representación del tamaño independiente del tipo y no hay que definirlo para cada tipo nuevo creado por el usuario. (Fig 2)

En primer lugar debemos definir la clase externa de la parte de **Generics** que será la que nosotros usemos. En ella solo debemos definir las funciones que queremos que tenga y como se comunica con la clases internas de **Generics**. Primero definimos la funcion en si que será una lista que dada un elemento de un tipo cualquiera nos devuelva un entero que representará su tamaño.

Despues debemos definir como se comunica la función **size** externa con la versión genérica **gsize** para obtener de esta el valor a devolver. En este caso usamos la función **from** que lo que hace es transformar un valor en su representación no genérica y transformarlo a su representación genérica para que pueda ser manipulado en las diferentes funciones. En este caso es simple pues el valor del tamaño obtenido por **gsize** será el mismo devuelto por nuestra función **size**. Finalmente creamos la clase interna **GSized** y definimos la función **gsize**.

Una vez tenemos la interfaz entre las dos clases **Sized** y **GSized** lo primero que debemos definir es el constructor sin argumentos que en nuestro caso devuelve el tamaño 0. A continuacion definimos **size** para un tipo compuesto por otros dos tipos, el tamaño de dicho tipo es la suma de los tamaños de los tipos que los componen. Tras ello definimos el comportamiento cuando el tipo tiene mas de un constructor posible, en este caso si elegimos el constructor de la derecha el tamaño del tipo será el tamaño del tipo de la derecha y similar si elegimos el tipo de la izquierda. Por último tenemos la instancia utilizada para trabajar con metainformación del tipo, que en nuestro caso al no ser necesaria dicha información simplemente llamamos de nuevo a la funcion **gsize** ignorando la metainformación.

```

-- / This is the exported, visible class that inherits from Allv.
class (Allv a) => Sized a where
  -- This function returns the first n elements of size lower or equal m from the "allv" list
  sized :: Int -> Int -> [a]
  sized n m = take n (filter (\x -> (size x) <= m) allv)

  -- This function takes an integer n and returns the n first elements of the "allv" list
  smallest :: [a]
  smallest = take uutNumCases (concat $ repeat allv)

size :: a -> Int
default size :: (Generic a, GSized (Rep a)) => a -> Int
size a = gsize (from a)

-- / This is the generic, non-visible class
class GSized f where
  gsize :: f a -> Int

-- / Unit: used for constructors without arguments
instance GSized U1 where
  gsize U1 = 0

-- / Products: encode multiple arguments to constructors
instance (GSized a, GSized b) => GSized (a :*: b) where
  gsize (x :*: y) = gsize x + gsize y

-- / Sums: encode choice between constructors
instance (GSized a, GSized b) => GSized (a :+: b) where
  gsize (L1 x) = gsize x
  gsize (R1 x) = gsize x

-- / Meta-information (constructor names, etc.)
instance (GSized f) => GSized (M1 i c f) where
  gsize (M1 x) = gsize x

-- / Constants, additional parameters and recursion of kind *
instance Sized a => GSized (K1 i a) where
  gsize (K1 x) = size x

```

Figure 2: Class Sized

3.3: Allv/TemplateAllv

En primer lugar vamos a tratar la clase **Allv**, cuyas instancias cuentan unicamente con una función, **allv** la cual devuelve la lista de todos los posibles valores del tipo de datos.

Al principio esta clase estaba pensada para ser una única clase que utilizara la librería **Generics** y para contar con un método, **compose** con el cual ser capaces de generar instancias de la clase **Allv** para los tipos definidos por el usuario. Dicha función se encargaría de crear la lista de todos los valores (**allv**) para el nuevo tipo de datos a partir de las listas de los tipos predefinidos, pero encontramos un problema a la hora de integrarlo con la clase **Sized**. La idea que teníamos sobre **Sized** era darle al usuario la posibilidad de pedir los n valores mas pequeños de una clase o los n primeros valores de tamaño menor o igual a un número prefijado por él. Lo cual entraba en conflicto con la manera en la que generábamos las listas de **allv** para los tipos definidos por el usuario. Para realizar la composición de dos listas seguimos el método mostrado en la siguiente figura.

//////////IMAGEN EXPLICATIVA COMPOSE//////////

Dadas dos listas la idea es realizar el producto cartesiano de ellas siendo este el resultado de generar todas las parejas con un valor de la primera lista y otro de la segunda. Teniendo en cuenta que ambas pueden ser infinitas, dicho producto deberá ser realizado por diagonales. Dicha combinación de listas infinitas podía ser realizada sin problemas usando **Generics** pero el problema llegaba a la hora de querer devolver los n primeros valores de un tamaño menor o igual a m ya que para ello debíamos ordenar la lista infinita y encontramos el problema de que en dichas listas infinitas los elementos de un tamaño siempre eran infinitos y que siempre habría algún elemento a mayores de tamaño menor o igual a m aunque fuera despues de muchos elementos por el medio que no lo fueran. Dicho problema fue el por que tuvimos que pensar en utilizar **Template Haskell** en lugar de **Generics**.

En la versión definitiva del programa en la clase **TemplateAllv** se encuentra esta funcionalidad de crear una instancia de **Allv** para los tipos de datos definidos por el usuario utilizando para ello **TemplateAllv**, con la ayuda de la ya nombrada función **compose**(Fig 4) que tiene la siguiente forma.

Compose se encarga de concatenar todas las diagonales en una única lista final que es la que se devuelve mediante la función **allv**, por otro lado **diags** se encarga de crear una de las diagonales y mientras no sea la ultima diagonal volver a llamarse a si misma con los parametros para la siguiente. Los parámetros de la función **diags** son: - **i** se trata del ordinal de la diagonal que vamos a generar. - **xs** e **ys** se tratan de las dos listas que vamos a combinar.

Además dentro de **TemplateAllv** tres funciones se encargan de crear una instancia adecuada de la clase **Allv** adecuada para cada uno de los tipos de datos definidos

por el usuario.

La primera de ellas y la más externa en dicho proceso es **gen_allv**(Fig 3), la cual además de llamar a **TypeInfo** para extraer la información del tipo y pasarsela a las subfunciones también es donde se define como se formará exactamente la nueva función **allv** dentro de la instancia del tipo. Adjunto el código de la función **gen_allv**.

Vamos a echar un vistazo mas de cerca a dicha función **gen_body** dentro de la clausula **where** y al tipo de comprobaciones o analisis sobre el tipo que realiza. En primer lugar nombrar lo que significa cada una de las cuatro listas que recibe como parámetro dicha función: - La primera de ellas contiene los números de parámetros de cada uno de los diferentes constructores. - La segunda contiene los nombres de los diferentes constructores. - La tercera una lista de nombres de **f's** entre **f₁** y **f_n** siendo *n* el número de constructores distintos para el tipo de datos. **Gen_body** se encarga de analizar el número de parámetros de cada uno de los constructores ya que si cuenta con un único parámetro, se puede utilizar el nombre del propio constructor sin ningún problema pero en caso de tener más de un parámetro debido a que compose devuelve la lista compuesta como una lista de tuplas, es necesario utilizar una función auxiliar **f** para realizar la aplicación del constructor sobre los elementos de la tupla en lugar de sobre la tupla en si. Aparte de esto **gen_body** se encarga de utilizando **Template Haskell** conseguir juntar todas las partes que fueron en parte preprocesadas en **gen_clause**

La siguiente función a tratar, **gen_instance**(Fig 5) se encarga únicamente de crear una instancia de la clase **Allv** para el nuevo tipo de datos (parámetro **for_type**) y adjuntar a dicha instancia la definición de la función **allv** que se crea en **gen_clause**. Adjunto el código de **gen_instance**

Por último tenemos la función **gen_clause**(Fig 6) que se encarga de crear la definición de la función **allv** para el tipo de datos, usando para ello la función **gen_body** que había sido definida anteriormente en **gen_allv**. Además cuenta con una serie de funciones auxiliares que realizan parte del procesamiento: - **listOfFOut** se encarga de crear la lista de nombres de variables entre **f₁** y **f_n** para aquellos casos en los cuales los constructores tienen más de un parámetro. - **isRec** devuelve una lista de booleanos en la cual cada posición indica si el constructor en dicha posición es recursivo o no. - **reorderL** se encarga de reordenar los constructores (lo cual es equivalente a las listas con la información por cada constructor) de manera que queden en primer lugar aquellos que no son recursivo y al final los que si lo son. Esto es necesario ya que los constructores recursivos harán uso de aquellos que no lo son y por ello los no recursivos deben definirse en primer lugar. - **gen_wheres** que se encargará de definir las clausulas where necesarias para todos aquellos constructores con más de un parámetro que necesiten utilizar una función auxiliar (que son las representadas por las **f's**). - **tupleParam** crea las tuplas de parámetros para cada una de las funciones auxiliares **f**.


```

gen_allv :: Name -> Q Dec
gen_allv typName =
  do (TyConI d) <- reify typName
    --Extract all the type info of the data type
    (t_name,noSimplifiedName,cInfo,consts,typesCons) <- typeInfo (return d)
    --We call to gen_instance with a name for the class, the name of the constructor,
    --a list of info of the constructors, the constructors itself, lists containing
    --the constructors, name of the data-type without being simplified, and lastly
    --the function to generate the body of the function of the class.
    i_dec <- gen_instance (mkName "Allv") (conT t_name) cInfo consts
    typesCons noSimplifiedName (mkName "allv", gen_body)
  return i_dec -- return the instance declaration
    -- gen_body is the function that we pass as an argument to gen_instance
    --and later on is used to generate the body of the allv function
    --for a determined data-type
  where gen_body :: [Int] -> [Name] -> [Name]-> [ExpQ]
        gen_body _ [] [] = []
        gen_body (i:is) (c:cs) (f:fs) --cInfo consts listOfF
        | null cs = [appsE (mapE:constructorF:(allvFunc i))] ++
          (gen_body is cs fs rs)
        | otherwise = [appsE (varE '(++):[appsE (mapE:constructorF:
          (allvFunc i))] ++ gen_body is cs fs rs)]
        where --constructorF decided to use the data constructor
              --if having just one parameter or to use a function if
              --having more than one. This is duo to the fact that
              --if the data constructor has more than one parameter
              --we need to apply compose to them and then apply a
              --function over the result of compose.
              constructorF
                | i > 1 = varE f
                | otherwise = conE c
              --mapE, composeE and allvE are three auxiliar function
              --that serve to get the expresion equivalent to those 3
              --functions in template haskell
              mapE = varE 'map
              composeE = varE 'compose
              allvE = varE 'allv
              moveHead (x1:x2:xs) = x2:x1:xs

          allvFunc 1 = [appsE [allvE]]
          allvFunc n = [appsE (composeE:[allvE] ++ allvFunc (n-1))]

```

Figure 3: Función gen_allv

```

compose :: [a] -> [b] -> [(a,b)]
compose xs ys = (e:lattice)
  where e:lattice = concat $ diags 0 0 0 xs ys

--
-- It builds the lattice of tuples from two lists, each one may be either
-- finite or infinite

diags :: Int -> [a] -> [b] -> [(a,b)]
diags _ [] [] = [[]]
diags i xs ys
  | fullDiag      = [tup k | k <- [0..i]] : diags (i+1) xs ys
  | finiteFirst   = diags (i-1) xs  ysr
  | finiteSecond  = diags (i-1) xsr ys
  | otherwise     = diags (i-2) xsr ysr

  where xs'       = drop i xs
        ys'       = drop i ys
        xsr       = tail xs
        ysr       = tail ys
        fullDiag   = not (null xs') && not (null ys')
        finiteFirst = null xs' && not (null ys')
        finiteSecond = not (null xs') && null ys'
        tup k      = (x,y)
                      where x = xs !! k
                            y = ys !! (i-k)

```

Figure 4: Función compose

```

--Construct an instance of class class_name for type for_type
--with a corresponding function to build the method body
gen_instance :: Name -> TypeQ -> [Int] -> [Name]
              -> [[Type]] -> Name -> Func -> DecQ
gen_instance class_name for_type cInfo consts typesCons typeName_nosimp func =
  instanceD (cxt [])
    (appT (conT class_name) for_type)
    [(func_def func)]
  where func_def (func_name, gen_func) -- extracts func_name and gen_func
        = funD func_name -- method name
          -- generate function body
          [gen_clause gen_func cInfo consts typesCons typeName_nosimp]

```

Figure 5: Función gen_instance

```

-- Generate the pattern match and function body for a given method and
-- a given data-type. gen_func is the function that generates the function body
gen_clause :: Gen_func -> [Int] -> [Name] -> [[Type]] -> Name -> ClauseQ
gen_clause gen_func cInfo consts typesCons typeName_nosimp =
  (clause []
    --here we execute the gen_function to generate the body of the function
    (normalB $ head (gen_func cInfoOrd constsOrd listOffOutOrd))
    --this other one generates the where clause of the function
    (gen_where cInfoOrd constsOrd listOffOutOrd))
  where
    --listOffOut generates a fresh list of "Name" for n different f's
    --this f's are used when one of the data types has more than one
    --parameter
    listOffOut = listOff (length consts)
    listOff 0 = []
    listOff n = (mkName ("f"++ show n)):(listOff (n-1))
    --isRec checks which of the constructors of the given data-type
    --are recursive and which others are not. It returns a boolean list
    --where true means to be recursive and false to not to be recursive.
    isRec = isRecAux typesCons
    isRecAux [] = []
    isRecAux (x:xs) = (or $ map (==(ConT typeName_nosimp)) x): isRecAux xs
    --ReorderL reorders all this lists so they have all non recursive
    --type constructors first and all recursive ones at the end
    reorderL = auxFirst cInfo consts listOffOut isRec 0 False
    auxFirst is cs fs rs n foundRec
      | n > ((length rs)-1) = (is, cs, fs, rs)
      | foundRec && (not (rs!!n)) = auxFirst
        ((is!!n):(remove n is 0))
        ((cs!!n):(remove n cs 0))
        ((fs!!n):(remove n fs 0))
        ((rs!!n):(remove n rs 0)) 0 False
      | (not foundRec) && (rs!!n) = auxFirst is cs fs rs (n+1) (not foundRec)
      | otherwise = auxFirst is cs fs rs (n+1) foundRec
    --removes position n from the list (x:xs)
    remove n (x:xs) actPos
      | n==actPos = xs
      | otherwise = x:(remove n xs (actPos+1))
    --This four functions serve to take the reordered lists for those 4 lists
    cInfoOrd = (\(x,_,_,_) -> x) reorderL
    constsOrd = (\(_,x,_,_) -> x) reorderL
    listOffOutOrd = (\(_,_,x,_) -> x) reorderL
    isRecOrd = (\(_,_,_,x) -> x) reorderL
    --gen_where is the auxiliar function that generates the where "clause"
    --of the function when necessary.
    gen_where [] [] [] = []
    gen_where (n:ns) (c:cs) (f:fs) --gen_where numParam consts listOff
      | n > 1 = funD f (bodyFunc listOffVar c):gen_where ns cs fs
      | otherwise = gen_where ns cs fs
      where listOffVar = listVariab n
            listVariab 0 = []
            listVariab n = (mkName ("x"++ show n)):(listVariab (n-1))
    --generates the body for the functions in the where clause when necessary.
    bodyFunc listOffVar constructorName = [clause (tupleParam listOffVar)
      (normalB (appsE ((conE constructorName):
        (map varE listOffVar))))] []

tupleParam (v:vs) --tupleParam listVars
  | (null vs) = [varP v]
  | otherwise = [tupP ((varP v):tupleParam vs)]

```

Figure 6: Función gen_clause

3.4: Arbitrary

3.5: Instancias predefinidas

En este último apartado vamos a repasar las instancias dentro de las clases **Sized** y **Allv** para los tres tipos básicos (**Int**, **Char** **Bool**) y para los tipos que se deducen directamente de ellos como es el caso de listas de cualquier tipo ya instanciado en dichas clases o las tuplas de hasta longitud 6.

Adjunto el código donde se instancian dichos tipos en las dos clases que se encuentran en el archivo **Sized.hs**.

```
instance Sized Int where
  size x = 1

instance Allv Int where
  allv = [1..100]

instance Sized Char where
  size x = 1

instance Allv Char where
  allv = ['a'..'z']

instance Sized Bool where
  size x = 1

instance Allv Bool where
  allv = [True, False]
```

Como podemos observar en el caso de la instancia en la clase **Sized** cualquier elemento de uno de los tres tipos tendrá tamaño uno. En el caso de las instancias de los tres tipos en la clase **Allv** simplemente debemos indicar el conjunto de valores de dicha clase que serán elegibles a la hora de generar casos de prueba.

A continuación nos encontramos con las instancias derivadas de tipos ya definidos en **Allv**.

```
instance Allv a => Allv [a] where
  allv = [] : map (\(x,xs) -> x:xs) $ compose (allv::a) (allv::[a])

instance (Allv a, Allv b) => Allv (a,b) where
  allv = compose allv allv

instance (Allv a, Allv b, Allv c) => Allv (a,(b,c)) where
  allv = compose allv (compose allv allv)

instance (Allv a, Allv b, Allv c, Allv d) => Allv (a,(b,(c,d))) where
```

```

allv = compose allv (compose allv (compose allv allv))

instance (Allv a, Allv b, Allv c, Allv d, Allv e) => Allv (a,(b,(c,(d,e)))) where
  allv = compose allv (compose allv (compose allv (compose allv allv)))

instance (Allv a, Allv b, Allv c, Allv d, Allv e, Allv f) => Allv (a,(b,(c,(d,(e,f))))) where
  allv = compose allv (compose allv (compose allv (compose allv (compose allv allv))))

```

Para las cuales utilizamos la función de **compose** explicada con anterioridad.

En el caso de las instancias derivadas dentro de la clase Sized nos encontramos que estas se generan mediante generics.

Estaba también pensado incluir dentro del archivo **Arbitrary.hs** las instancias de estos tres tipos y las instancias derivadas a partir de ellos para la clase Arbitrary, pero por falta de tiempo se decidió centrarse en la parte de Sized.

4. El generador de casos

4.1: La interfaz con la UUT

La interfaz de mi programa con la unidad bajo testeo (UUT a partir de ahora) se encuentra en el archivo `UUT.hs`(Figura x), dicho archivo es diferente para cada función que vayamos a probar y contiene la información mínima necesaria para poder hacer todas las pruebas. Además dicho archivo se genera automáticamente para cada función que vayamos a probar mediante la `IR2Haskell`, que se encarga de traducir la representación de la IR a código Haskell. La información presente en la UUT es: - En primer lugar una función `uutNargs` que devuelve un entero y que indica el número de argumentos que tiene la función que vamos a probar. - En segundo lugar **`uutMethods`** que contiene los nombres de las tres funciones que tendremos que utilizar en el proceso (precondición, función y postcondición). -A continuación la precondición en este caso **`uutPrec`**, la función **`uutMethod`** y postcondición **`uutPost`**. Estas tres funciones serán las que guíen todo el proceso de prueba de la función para la lista de casos generados.

```
module UUT where

uutNargs :: Int
uutNargs = 2

uutMethods :: [String]
uutMethods = ["uutPrec", "uutMethod", "uutPost"]

uutPrec :: Int -> Int -> Bool
uutPrec x y = True

uutMethod :: Int -> Int -> Int
uutMethod x y = x+y

uutPost :: Int -> Int -> Int -> Bool
uutPost x y z = True
```

Figure 7: Clase UUT

4.2: La obtención del tipo de la UUT

Dentro del programa, una de las partes importantes y la principal por la cual Template Haskell resultó de gran utilidad para el proyecto es poder analizar los tipos de las funciones y adaptar el generador de casos a ellos, tanto si son tipos predefinidos, como si son tipos definidos por el usuario.

Dentro de **TemplateAllv** se encuentra la función **typeInfo** (Figura x) que se encarga de extraer y sintetizar la información sobre un tipo declarado por el usuario. Se trata de una función que recibe como parametro una variable del tipo **DecQ** y devuelve una tupla dentro de la monada **Q** con la siguiente información:

- En primer lugar el nombre simplificado del tipo del cual vamos a realizar la instancia, refiriendome con simplificado a quitar toda la parte del nombre que se refiere a la estructura de módulos de la cual se hereda dicho tipo. Por ejemplo si creáramos una instancia para el tipo **Integer** del módulo **Prelude** el nombre del tipo sin simplificar sería **Prelude.Integer** y una vez simplificado simplemente **Integer**. Dicho nombre se trata de una variable de tipo **Name**, que es la manera en la que se maneja el tipo **String** en **TH** para todo tipo de nombres.
- El segundo se trata del nombre del tipo sin simplificar, devuelto también como una variable de tipo **Name**.
- El tercero es una lista de enteros para cada uno de los diferentes constructores del tipo. Los enteros expresan el número de argumentos de cada uno de los constructores.
- El cuarto se trata de una lista de los diferentes nombres de los constructores de tipo. Se trata de una lista de tipo **Name**.
- El último se trata de una lista de listas. Cada una de las listas internas contiene los tipos para uno de los constructores del tipo.

El otro gran punto en el cual necesitamos analizar el tipo de las funciones es a la hora de crear los casos de prueba, y de ello se encarga la función **get_f_inp_types** la cual que dada una **String** que será el nombre de una función nos devuelve una lista con los tipos de entrada de dicha función en forma de lista de **Strings**. Esta función consta de 4 pasos o llamadas a otras funciones auxiliares (Figuras x y x+1):

- En primer lugar **lookupValueName**, que es una función de la librería **Template Haskell** y que lo que hace es dado una **String** que será el nombre de una función nos devuelve el **Name** asociado a ella dentro del namespace actual.
- La segunda función se trata de **extract_info**, la cual recibe como entrada un **InfoQ** el cual es un tipo que se usa dentro de **Template Haskell** para encapsular información como por ejemplo en este caso la información devuelta por el reify del **Name** de la función. A partir de ello **extract_info** nos devolverá el nombre de la función sin el prefijo del módulo, el nombre de la función con el prefijo y por último el tipo de la función en forma prefija.
- En tercer lugar **simplifyParsing** que recibe como entrada el tipo de una función en forma prefija y lo transforma a forma infija, que es la manera en la que indicamos por ejemplo en tipo de la función cuando lo ponemos explícitamente en **Haskell**.
- Finalmente la última función **extract_types** se encarga de transformar el tipo de la función en forma infija a una lista con los tipos de entrada de la misma, ignorando el tipo de salida.

4.3 La generación de instancias de **Allv** y **Arbitrary**

Tras obtener la lista de tipos de datos que se utilizan en la función que no están definidos por defecto (lo cual corresponde con la segunda parte del apartado anterior) deberemos crear instancias en las dos clases **Allv** y **Arbitrary** para

```

typeInfo :: DecQ -> Q (Name, Name,[Int],[Name],[[Type]])
typeInfo m =
  do d <- m
  case d of
    d@(DataD _ _ _ _) ->
      return $ (simpleName $ name d, name d , consA d, termsA d, listTypesA d)
    d@(NewtypeD _ _ _ _) ->
      return $ (simpleName $ name d, name d , consA d, termsA d, listTypesA d)
    _ -> error ("derive: not a data type declaration: " ++ show d)

  where
    consA (DataD _ _ _ cs _) = map conA cs
    consA (NewtypeD _ _ _ c _) = [ conA c ]

    conA (NormalC c xs) = length xs
    conA (RecC c xs) = length xs
    conA (InfixC _ c _) = 2

    nameFromTyVar (PlainTV a) = a
    nameFromTyVar (KindedTV a _) = a

    termsA (DataD _ _ _ cs _) = map termA cs
    termsA (NewtypeD _ _ _ c _) = [ termA c ]

    termA (NormalC c xs) = c
    termA (RecC c xs) = c
    termA (InfixC t1 c t2) = c

    name (DataD _ n _ _ _) = n
    name (NewtypeD _ n _ _ _) = n
    name d = error $ show d

    listTypesA (DataD _ _ _ cs _) = (map typesA cs)
    listTypesA (NewtypeD _ _ _ c _) = [ typesA c ]

    typesA (NormalC _ xs) = map snd xs
    typesA (RecC _ xs) = map (\(_, _, t) -> t) xs
    typesA (InfixC t1 _ t2) = [snd t1] ++ [snd t2]

simpleName :: Name -> Name
simpleName nm =
  let s = nameBase nm
  in case dropWhile (/=':') s of
    [] -> mkName s
    _:[] -> mkName s
    _:t -> mkName t

```

Figure 8: Función typeInfo


```

get_f_inp_types :: String -> Q [String]
get_f_inp_types str = do (Just name) <- lookupValueName str
  (_,_,text) <- extract_info (reify name)
  t <- return(simplifyParsing text)
  return (extract_types t [] "")

extract_info :: InfoQ -> Q(Name, Name, String)
extract_info m =
  do d <- m
  case d of
    d@(VarI _ _ _ _) ->
      return $ (funcName d, simpleName $ funcName d, parseDataTypes d)
    d@(ClassOpI _ _ _ _) ->
      return $ (funcName d, simpleName $ funcName d, parseDataTypes d)
    _ -> error ("Error in extract_info" ++ show d)
  where
    funcName (VarI n _ _ _) = n
    funcName (ClassOpI n _ _ _) = n

    parseDataTypes (VarI _ x _ _) = first_parse x
    parseDataTypes (ClassOpI _ x _ _) = first_parse x

    first_parse ((ForallIT _ _ x)) = parsing x
    first_parse x = parsing x

    parsing ((AppT x y)) = (parsing x) ++ (parsing y)
    parsing (ArrowT) = "-> "
    parsing (ListT) = "["
    parsing ((TupleT 2)) = "(,)"
    parsing ((TupleT 3)) = "(,)"
    parsing ((VarT _)) = "Int "
    parsing ((ConT x)) = (nameBase x) ++ " "
    parsing _ = "UND "

simpleName :: Name -> Name
simpleName nm =
  let s = nameBase nm
  in case dropWhile (/=':') s of
    [] -> mkName s
    _:[] -> mkName s
    _:t -> mkName t

```

Figure 9: Funcion `get_f_inp_types` y auxiliares

```

get_f_inp_types :: String -> Q [String]
get_f_inp_types str = do (Just name) <- lookupValueName str
  (_,_,text) <- extract_info (reify name)
  t <- return(simplifyParsing text)
  return (extract_types t [] "")

extract_info :: InfoQ -> Q(Name, Name, String)
extract_info m =
  do d <- m
  case d of
    d@(VarI _ _ _) ->
      return $ (funcName d, simpleName $ funcName d, parseDataTypes d)
    d@(ClassOpI _ _ _) ->
      return $ (funcName d, simpleName $ funcName d, parseDataTypes d)
    _ -> error ("Error in extract_info" ++ show d)
  where
    funcName (VarI n _ _ _) = n
    funcName (ClassOpI n _ _ _) = n

    parseDataTypes (VarI _ x _ _) = first_parse x
    parseDataTypes (ClassOpI _ x _ _) = first_parse x

    first_parse ((ForallT _ _ x)) = parsing x
    first_parse x = parsing x

    parsing ((AppT x y)) = (parsing x) ++ (parsing y)
    parsing (ArrowT) = "-> "
    parsing (ListT) = "["
    parsing ((TupleT 2)) = "(, "
    parsing ((TupleT 3)) = "(,, "
    parsing ((VarT _)) = "Int "
    parsing ((ConT x)) = (nameBase x) ++ " "
    parsing _ = "UND "

simpleName :: Name -> Name
simpleName nm =
  let s = nameBase nm
  in case dropWhile (/=':') s of
    [] -> mkName s
    _:[] -> mkName s
    _:t -> mkName t

```

Figure 10: Funcion `get_f_inp_types` y auxiliares

dichos tipos. Dicha generación de instancias se realiza mediante **Template Haskell** dentro de la clase **UUTReader** mediante el código mostrado en la Figura x.

En dicho código realizamos una llamada a las funciones **gen_allv_str_list** y **gen_arbitrary_str_listQ** de las clases **TemplateAllv** y **TemplateArbitrary** respectivamente. Ambas funciones reciben como parámetro una lista de Strings que contiene todos los nombres de los tipos definidos por el usuario y a partir de ella crean instancias para cada uno de dichos tipos en la clase a la que esta dirigida cada función.

Dicha lista de tipos definidos por el usuario se calcula en primer lugar hayando los tipos de los datos de la precondition y después sobre dicha lista de tipos de entrada aplicando la función **notDefTypesQMonad** la cual filtra cuales de ellos no son instancias predefinidas.(Figura x).

Analizando dicha función y sus auxiliares podemos observar que se tratan de una funciones relativamente simples, ya que **notDefTypesQMonad** se encarga de simplemente de lidiar con la monada Q y pasar la lista fuera de la monada a **notDefTypes**. En segundo lugar **notDefTypes** se encarga de pasarle dichos tipos uno a uno a **isUserDef**, pero se los pasa simplificados, lo cual significa tratar igual las listas de un tipo que el tipo en si, ya que si las instancias para un tipo están definidas en las instancias base también lo estarán para las listas de dicho tipo. Por último **isUserDef** simplemente se encarga de ver si el tipo simplificado es o no **Int**, **Char**, o **Bool** que son los tres tipos que cuentan con instancia predefinida y si no es ninguno de ellos devolverá **True**, ya que se trata de un tipo definido por el usuario.

```
$(gen_allv_str_listQ (notDefTypesQMonad (get_f_inp_types (head uutMethods))))
$(gen_arbitrary_str_listQ (notDefTypesQMonad (get_f_inp_types (head uutMethods))))
```

Figure 11: Call to the generator functions

4.4: La generación de casos

4.5: La ejecución de casos

```

notDefTypesQMonad :: Q [String] -> Q [String]
notDefTypesQMonad xs = do list <- xs
                        return (notDefTypes list)

notDefTypes :: [String] -> [String]
notDefTypes [] = []
notDefTypes (x:xs)
  | (isUserDef (plain x)) = (plain x):(notDefTypes xs)
  | otherwise = notDefTypes xs

isUserDef :: String -> Bool
isUserDef str
  | str == "Int" || str == "Char" || str == "Bool" = False
  | otherwise = True

plain :: String -> String
plain [] = []
plain (x:xs)
  | x == '[' || x == ']' = plain xs
  | otherwise = x:(plain xs)

```

Figure 12: Función notDefTypesQMonad y auxiliares

5.Experimentos

6. Related

6.1: Korat

La primera de las herramientas que vamos a tratar en este apartado se trata de **Korat** [7], una extensión de Java que sirve para la generación de casos complejos de prueba a partir de unas restricciones dadas.

La idea detras de **Korat** es que dado un predicado en Java y una función **finalization** en la cual definimos los dominios para cada una de las clases del input, es decir los valores válidos para cada una de ellas. **Korat** explora el espacio de estados de las posibles soluciones pero generando solo soluciones no isomorfas entre si, consiguiendo de esta manera una gran poda de las soluciones no interesantes del espacio de búsqueda.

Lo primero que hace **Korat** es reservar el espacio necesario para los objetos especificados por ejemplo en el caso de un **BinTree** reservaria espacio para él y para el número de Nodos que queramos. Por ejemplo si queremos un arbol con tres nodos el vector contendría 8 campos: * 2 para el **BinTree** (uno para la raíz y otro para el tamaño) * 2 campos por cada uno de los 3 nodos (hijo izquierdo/hijo derecho)

Cada uno de los posibles candidatos que considere **Korat** a partir de ese momento será una evaluación de esos 8 campos. Por lo tanto el espacio de estados de búsqueda del input consiste en todas las posibles combinaciones de esos campos, donde cada uno de ellos toma valores de su dominio definido en **finalization**

Para conseguir explorar de manera sistemática y completa el espacio de estados **Korat** ordena todos los elementos en los dominios de las clases y los dominios de los campos. Dicho orden de cada uno de los dominios de los campos será consistente con el orden del dominio de la clase y todos los valores que pertenezcan al mismo dominio de clase ocurriran de manera consecutiva en el dominio del campo. Tras esto representa cada candidato de la entrada como un vector de índices de sus correspondientes dominios de campos.

Tras definir los dominios de cada uno de los campos del vector la busqueda comienza con la inicialización de todos los indices del vector a 0. Tras ello para cada posible candidato fijamos los valores de los campos de acuerdo a los valores en el vector y acto seguido invoca a la funcion **repOk** que es donde el usuario ha definido la precondition de la función. Durante dicha ejecución **Korat** monitoriza en que orden son accedidos los campos del vector y construye una lista con los identificadores de los campos, ordenados por la primera vez en que **repOk** los accede.

Cuando **repOk** retorna **Korat** genera el siguiente candidato incrementando el indice del dominio de campo para el campo que se encuentra último en la lista ordenada construida previamente. Si dicho indice es mayor que el tamaño del dominio de su campo este se pone a cero y se incrementa el indice de la posición

anterior y así repetidamente. Al seguir este método para generar el siguiente candidato conseguiremos podar un gran número de los candidatos que tienen la misma evaluación parcial sin dejar fuera ninguno válido.

El algoritmo de búsqueda descrito aquí genera las entradas en orden lexicográfico. Además para los casos en los que **repOk** no es determinista este método garantiza que todos los candidatos para los que **repOk** devuelve true son generados, los casos para los que siempre devuelve false nunca son generados y los casos para los que alguna vez se devuelve true y a veces false pueden ser o no generados.

Dos candidatos se definen como isomorfos si las partes de sus grafos alcanzables desde la raíz son isomorfas. En el caso de **repOk** el objeto raíz es el objeto pasado como argumento implícito.

El isomorfismo entre candidatos divide el espacio de estados en particiones isomórficas (debido al ordenamiento lexicográfico introducido por el orden de los valores de los dominios de los campos y la ordenación de los campos realizado por **repOk**). Para cada una de dichas particiones isomórficas **Korat** genera únicamente el candidato lexicográficamente menor.

Además con el proceso explicado anteriormente para ir generando el siguiente candidato teniendo en cuenta la lista de ordenación de los campos **Korat** se asegura de no generar varios candidatos dentro de la misma partición isomórfica.

6.2: Smallcheck

La segunda herramienta a tratar en este apartado es **Smallcheck** [8] una librería para Haskell usada en el testing basado en propiedades. Esta librería parte de las ideas del **Quickcheck** y perfecciona algunos de los puntos flacos de este.

La principal diferencia de **Smallcheck** respecto a **Quickcheck** es la generación de sus casos de prueba. En este caso **Smallcheck** se apoya en la “hipótesis del ámbito pequeño” la cual dice que si un programa no cumple su especificación en alguno de sus casos casi siempre existirá un caso simple en el cual no la cumpla o lo que viene a ser lo mismo, que si un programa no falla en casos pequeños lo normal es que no falle en ninguno de sus casos.

Partiendo de esta idea cambia la generación existente en **Quickcheck**, la cual era aleatoria, por una generación exhaustiva de todos los casos de prueba pequeños ordenados por **profundidad** (que es el nombre usado para el tamaño), dejando a criterio del usuario hasta que profundidad deben considerarse como pequeños. A continuación presentamos como están definidas las profundidades más importantes:

- En el caso de los tipos de datos algebraicos como es usual la profundidad de una construcción de aridad cero es cero mientras que la profundidad de una construcción de aridad positiva es una más que la mayor profundidad de todos sus argumentos.

- En el caso de las tuplas dicha profundidad se define un poco diferente. La profundidad de una tupla de aridad cero es cero pero la profundidad de una tupla de aridad positiva es simplemente la mayor profundidad de entre todas las de sus componentes.
- En el caso de los tipos numéricos la definición de la profundidad es con respecto a una representación imaginaria como una estructura de datos. De esta manera, la profundidad de un entero i será su valor absoluto, ya que se construyó de manera algebraica como **Succⁱ Zero**. A su vez, la profundidad de un número decimal $s \times 2^e$ es la profundidad del par de enteros (s,e) .

Smallcheck define una clase **Serial** de tipos que pueden ser enumerados hasta una determinada profundidad. Para todos los tipos de datos del preludio existen instancias predefinidas de la clase **Serial**. Sin embargo definir una nueva instancia de dicha clase para un tipo de datos algebraico es muy fácil, se trata de un conjunto de combinadores **cons**, genéricos para cualquier combinación de tipos **Serial**, donde d es la aridad del constructor.

Por ejemplo supongamos un tipo de datos en Haskell **Prop** en el cual tenemos una variable, la negación de una variable y el **Or** de dos variables

```
data Prop = Var Name | Not Prop | Or Prop Prop
```

Definir una instancia de la clase **Serial** para dicho tipo de datos sería como sigue. Asumiendo una definición similar para el tipo **Name**.

```
instance Serial Prop where
  series = cons1 Var \d -> cons1 Not \d -> cons2 Or
```

Una serie simplemente es una función que dado un entero devuelve una lista finita.

```
type Series a = Int -> [a]
```

A su vez el producto y la suma sobre dos series se definen como:

```
(\/) :: Series a -> Series a -> Series a
s1 \/ s2 = \d -> s1 d ++ s2 d

(><) :: Series a -> Series b -> Series (a, b)
s1 >< s2 = \d -> [(x,y) | x <- s1 d, y <- s2 d]
```

Por último los combinadores **cons** están definidos usando $><$ decrementando y comprobando la profundidad correctamente.

```
haskell  cons0 c = \d -> [c]    cons1 c = \d -> [c a | d > 0,
a <- series (d-1)]  cons2 c = \d -> [c a b | d > 0, (a,b) <-
(series >< series) (d-1)]
```

Usar el esquema general para definir series de valores de prueba muchas veces produce que para alguna profundidad pequeña d los 10.000-100.000 casos de

prueba son rápidamente comprobados pero para la profundidad **d+1** resulte imposible completar los miles de millones de casos de prueba. Por ello resulta necesario reducir algunas dimensiones del espacio de búsqueda de manera que otras de las dimensiones puedan ser comprobadas en mayor profundidad.

El primer punto a tener en cuenta es que a pesar de que los números enteros pueden parecer una elección obvia como valores bases para las pruebas debemos tener en cuenta que los espacios de búsqueda para los tipos compuestos (especialmente funcionales) al usar bases numéricas crecen de manera muy rápida. En muchos casos el tipo booleano puede ser una elección perfectamente válida para los valores bases y con ello se conseguiría reducir en gran medida el espacio de búsqueda respecto a la utilización de enteros.

Existe otra version de **Smallcheck** llamada **Lazy Smallcheck**, que a su vez se aprovecha de la evaluación perezosa de Haskell, la cual permite que una función devuelva un valor aunque esta esté aplicada sobre una entrada definida parcialmente. Esta posibilidad de ver el resultado de una función sobre muchas entradas en una sola ejecución puede resultar de gran ayuda en el testeo basado en propiedades ya que si una función se cumple para una solución parcial, esta se cumplirá para todas las funciones totalmente definidas que partan de dicha definición parcial. En eso se centra el **Lazy Smallcheck**, en evitar generar todas esas funciones totalmente definidas que no aportan nada de información extra sobre la definición parcial. La actual versión de **Lazy Smallcheck** es capaz de testear propiedades de primer orden con o sin cuantificadores universales.

References

- [1] M. Montenegro, R. Peña, and J. Sánchez-Hernández, “A generic intermediate representation for verification condition generation,” in *Logic-based program synthesis and transformation - 25th international symposium, LOPSTR 2015, siena, italy, july 13-15, 2015. revised selected papers*, 2015, pp. 227–243.
- [2] M. Falaschi, Ed., *Logic-based program synthesis and transformation - 25th international symposium, LOPSTR 2015, siena, italy, july 13-15, 2015. revised selected papers*, vol. 9527. Springer, 2015.
- [3] M. Montenegro, S. Nieva, R. Peña, and C. Segura, “Extending liquid types to arrays,” in *PROLE 2016, salamanca, spain*, 2016, pp. 1–15.
- [4] K. Claessen and A. Hughes, “QuickCheck: A lightweight tool for random testing of haskell programs,” September-2000. [Online]. Available: <https://www.eecs.northwestern.edu/~robby/courses/395-495-2009-fall/quick.pdf>.
- [5] Magalhaes, A. Dijkstra, J. Jeuring, and A. Löb, “A generic deriving mechanism for haskell,” September-2010. [Online]. Available: <http://www.dreixel.net/>

research/pdf/gdmh_nocolor.pdf.

[6] T. Sheard and S. P. Jones, “Template meta-programming for haskell,” October-2002. [Online]. Available: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/meta-haskell.pdf>.

[7] C. Boyapati, S. Khurshid, and D. Marinov, “Korat: Automated testing based on java predicates,” July-2002. [Online]. Available: <http://web.eecs.umich.edu/~bchandra/publications/issta02.pdf>.

[8] C. Runciman, M. Naylor, and F. Lindblad, “SmallCheck and lazy smallcheck automatic exhaustive testing for small values,” September-2008. [Online]. Available: <https://pdfs.semanticscholar.org/2460/c9b40ea3c4bbaef53c5f4ad2717154cf15b5.pdf>.