

# **A Type-Changing, Equivalence-Preserving Program Transformation System**

Bram Schuur \*

December 01, 2012

\*Msc. Thesis under supervision of Johan Jeuring and Sean Leather



Program transformations play a central role in the construction of compilers. Before a source program comes out as machine readable instructions, it has gone through a lot of optimization and simplification steps, preferably without changing the behavior of the original program.

Traditionally, these transformations work by manipulating the syntactic constructs of a language, and do not alter the types of a program, or are applied to untyped sources. However, in recent years there has been an increasing interest in transformations in type-changing program transformations on typed sources: transformations in which it is possible to change the types together with the terms.

This work introduces an extensible transformation system based on the simply typed lambda calculus, which allows type-changing transformations between terms. The system ensures that a transformation preserves the semantics of the source term, independent of the concrete datatypes and evaluation strategy of the underlying lambda calculus. This statement is formally proven using logical relations and mechanically verified in the dependently typed programming language Agda. Central to the transformation system is the concept of typing functors, a construction which types the source and result of a transformation simultaneously, while allowing changes in types to occur.

# Contents

<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Related work . . . . .	7
1.2	Motivation . . . . .	8
1.3	Contributions . . . . .	9
1.4	Overview . . . . .	9
<b>2</b>	<b>Type and Transform Systems</b>	<b>11</b>
2.1	Motivating Examples . . . . .	11
2.1.1	Hughes' strings . . . . .	11
2.1.2	Stream fusion . . . . .	12
2.2	Core Transformation System . . . . .	14
2.2.1	Transformation properties . . . . .	15
2.2.2	Object Language . . . . .	16
2.2.3	A TTS for STLC . . . . .	19
2.3	A TTS for Hughes' strings . . . . .	20
2.4	Performing a transformation . . . . .	20
<b>3</b>	<b>Proof</b>	<b>22</b>
3.1	$TTS_{\lambda}$ preserves Typing . . . . .	22
3.2	$TTS_{\lambda}$ is Productive . . . . .	23
3.3	$TTS_{\lambda}$ preserves Semantics . . . . .	23
3.3.1	Logical Relations . . . . .	23
3.3.2	A Logical Relation for $TTS_{\lambda}$ . . . . .	24
3.3.3	Proof using logical relations . . . . .	24
3.4	Hughes' Strings Transformation Preserves the TTS Properties . . . . .	30
3.5	Type Abstraction . . . . .	31
3.6	The Typing Functor is an actual Functor . . . . .	31
<b>4</b>	<b>Mechanical Proof</b>	<b>35</b>
4.1	STLC object language . . . . .	35
4.1.1	Manipulating and constructing terms . . . . .	36
4.1.2	Equality . . . . .	40
4.2	Formalization of $TTS_{\lambda}$ . . . . .	41
4.3	Properties . . . . .	44
4.3.1	Typing property . . . . .	44
4.3.2	Identity transformation . . . . .	44
4.3.3	Semantic equivalence . . . . .	44

4.4	Monoid Transformation . . . . .	47
<b>5</b>	<b>Extensions to the TTS system</b>	<b>50</b>
5.1	Extending to let-polymorphism . . . . .	50
5.2	Including a fixpoint . . . . .	51
<b>6</b>	<b>Future work</b>	<b>53</b>
<b>7</b>	<b>Conclusion</b>	<b>54</b>
7.1	Acknowledgements . . . . .	54

# 1 Introduction

Program transformation is a central aspect of computer science, most importantly in the area of compiler construction. One expects from a compiler to transform human readable code into highly optimized machine code, while maintaining the expected behaviour of the program. During compilation, a compiler makes use of a wide range of program transformations to reach this goal. A program is simplified, variables are renamed and optimizations are applied while the program may be transformed into one or multiple intermediate languages.

Closely related areas in which program transformations play a role are program refactoring and program migration. Program transformations for refactoring and migration resemble those for compilation in that the behaviour of the resulting program should remain unchanged, but the intention of the transformations are different: Refactoring is done to make a program better readable for humans and migration is done to adapt a program to a changed environment.

**Program transformations** A program transformation works by inspecting and manipulating the terms of a language to generate the desired result. However, programming languages such as Haskell or Java do not only consist of terms, but of types as well. Designing program transformations for such languages leaves the designer with a choice: either throw away the typing information and apply transformations to untyped terms, or somehow leave the types of the terms in tact during transformation. Throwing away the typing information is sometimes unavoidable, for example when transforming typed Java to untyped assembler code. However, the transformations used for optimizing, refactoring and migration usually produce terms in the same language as their input language. For such transformations the choice between typed and untyped transformation is more difficult. Doing an untyped transformation gives a lot of flexibility, but can more easily result in untypeable terms. Furthermore, the types of a language are also a source of information during transformation, it would be a waste to throw that away!

For transformations on typed languages, on the other hand, the types themselves can be restrictive. One possibility is to leave the types of the source program in tact during transformation and only substitute equally typed terms. This works, but there is a class of transformations which require changes in the types next to changes in the terms. For example the following transformation, which replaces all occurrences of integral numbers by floating point numbers to reduce the rounding errors in a program:

**percent** :: Int → Int → Int  
**percent** v v' = 100 \* (v 'div' v')

**percent** :: Float → Float → Float  
**percent** v v' = 100 \* (v / v')

Such a transformation requires a transformation of both the terms and the types. The types are changed from **Ints** to **Floats**, and the 'div' operator is replaced by /. In recent years several of

these type-changing program transformations have been developed, such as the worker/wrapper transformation by Gill and Hutton [GH09] or a continuation passing style transformation by Ahmed and Blume [AB11]. They both show that their transformations are equivalence preserving and type-preserving, two crucial properties for typed program transformations.

**Transformation systems** Creating such a program transformation is time-consuming and error-prone. It is time-consuming because a transformation has to either be built into an existing compiler, which are complicated pieces of software to work in, or one has to create a custom infrastructure to process terms of the language, which means dealing with detailed implementation issues. Because modern programming languages have many constructs which interact in many subtle ways, an error is easily made. Thus it is also good practice to provide a proof of the fact that a program transformation works as expected. This is especially important because program transformations are used in the critical parts of software systems. An error in a compiler can cause a lot of trouble. However, proving a program transformation correct is not easy and again time-consuming.

To counter these issues, the natural way to go is looking for possible abstractions. Instead of developing individual program transformations, look for parts that can be generalized and develop a generic transformation system in which transformations can be constructed. This makes developing individual transformations faster and easier, resulting in less errors.

## 1.1 Related work

Several such systems for creating type-aware program transformation have already been developed and implemented in various forms.

- The Haskell GHC compiler allows user-defined transformation rules to transform terms, such as the following for map fusion:

```
{-# RULES "map/map" forall f g xs. map f (map g xs) = map (f . g) xs #-}
```

These rewrite rules are used by the compiler to simplify and optimize during compilation. The rules are type-checked using the internal type checker, which quickly catches typos and simple errors. Although the individual rules cannot change the types in a program themselves, combinations of these rules can have much the same effect. This is more thoroughly discussed in Section 2.1.2

- Cunha and Visser [CV07] [COV06] developed a framework for type-changing program transformation as an EDSL in Haskell. Their system works on a point-free representation of terms to avoid having to deal with binders.
- Recently Erwig and Ren [ER07] proposed a generic transformation system for type-changing program transformation. In their approach they define an update calculus for program updates which can deal with both type-changes and scoping changes. They show that updates performed by their generic transformation system will result in well-typed programs and that the semantics between the source and result programs are preserved.

## 1.2 Motivation

Although all these systems facilitate type changes in their own way, none of these systems are suitable for program-wide transformation of types, which is a very real use-case for both program optimization and migration. We call such transformations *type-driven*: transformations in which the ultimate goal is to replace the types in a program. In such a transformation the terms are only changed to make a program work with a new type: term substitution is not a driving factor. We already introduced the transformation of integers to floats as a use-case for a type-driven transformation, but there are many more use-cases:

**Migration** A situation when program-wide modification of types is desired is when migrating between libraries. In Haskell this could be migrating a program which uses `Text` as a representation for character data, to a representation using `ByteStrings`. This means changing the `Text` type inside the program as much as possible, and replacing the functions that work on `Text` by functions that work on `ByteStrings`. A similar migration occurs when moving between parsing libraries or when upgrading to a new version of a package.

This use-case was the primary motivation for the work of Erwig and Ren. However, their system has a rather ad-hoc way of specifying rules and type changes were very local, not in a program-wide manner.

**Optimization** Another use-case for type-changing program transformations is when the representation of a datatype is changed for optimization purposes. Hughes' strings transformation [Hug86] and the Stream fusion [CLS07] [CSL07] transformation are prominent examples of this and will be discussed in more detail in Section 2.1.

**Refactoring** Sometimes it is desired to change the representation of a datatype because this is more suitable for the programmer. For example, a point in space may be represented by its cartesian coordinates or by polar coordinates. When a user wants to switch between these representations, a transformation could be created to change the representation, and the way in which the program calculates with these representations.

Note that in most of these examples the same result could have been achieved by changing the underlying representation of a datatype instead of changing the program. However, this is not possible when the representation of a type is managed externally, for example when transforming base types or types which are part of a standard library. In these cases the only solution is to change the types in a program.

Also, when one wants to replace a type in a program, it is not always possible to find a suitable term-level replacement for all functions. In this case it is not possible to do a program-wide replacement of a type. For example in the case of the integer to floating point transformations, there is no floating point alternative for bit-shifting an `Int` representation. Thus there is no alternative but to keep the type unchanged and convert the floating point to an integer.

**magic** :: `Int` → `Int` → `Int`  
**magic** a b = a .|. xor b

**magic** :: `Float` → `Float` → `Float`  
**magic** a b = round a .|. xor (round b)



It is also possible that a type is not fully abstract and it can be inspected using pattern matching. In this case the internals of a type are exposed and one does not get around keeping the original type in tact.

Situations like these make it beneficial to have a type-changing transformation system which works directly on program representations and which tries to replace a type as much as possible, but can locally keep the original types in tact.

## 1.3 Contributions

This work introduces a generic formal system for such type-changing program transformations, which we call type-and-transform systems, *TTS* for short. This system is intended to be a basis for type-changing program-wide transformations and has the following features:

**STLC** The transformation system is designed for languages based on the simply typed lambda calculus. The core transformations are purely based on STLC, extensions are later discussed.

**Generic** The system is generic in the types and terms that are transformed. It can be parametrized with specific type and term transformations to obtain a specific program transformation. The type and transform system is also independent of the interpretation of the underlying type language.

**Proven** The system is proven to allow only transformations which yield type correct programs and which yield a semantically equivalent program after transformation. This claim is proven using logical relations and mechanically verified in the dependently type programming language Agda [Nor07], thus contributing to the POPLmark challenge [pop] of verified metatheory in programming languages.

Note that this system does not specify how the transformation system is implemented. The *TTS* system specifies the typing rules for type-changing program transformations, not how these transformations are actually performed. Section 2.4 discusses possibilities for implementation.

## 1.4 Overview

This section gives an overview of the upcoming chapters.

Chapter 2 introduces the general concepts and construction of the *TTS* system. First more extensive motivating examples of type-changing program transformations are introduced in the first two sections. Consequently the basic type and transform system for the simply typed lambda calculus is presented, followed by an example application of the Hughes' strings example in Section 2.3. The last section will briefly discuss the possibilities and problems when implementing an actual transformations system

Chapter 3 establishes the core properties of the type and transform system. Section 3.1 and Section 3.2 establish the type soundness and productivity of the type and transform system. Section 3.3 introduces logical relations and uses these to prove the semantic correctness of program transformations.

## 2 Type and Transform Systems

This chapter introduces the core concepts of type and transform systems. The first section gives two motivating examples of type-changing program transformations which will be used throughout this work.

### 2.1 Motivating Examples

#### 2.1.1 Hughes' strings

One example of a type-changing program transformation is known as Hughes' lists [Hug86]. In his work, Hughes presents a method which reduces the computational overhead induced by the naive implementation of string concatenation. Hughes' method does not only work for strings, but for lists in general, but we will use strings for simplicity. To see what problem Hughes' strings solve, consider the standard implementation of string concatenation:

```
infixr 5 ++
(++) :: String → String → String
[]      ++ ys = ys
(x:xs) ++ ys = x : (xs ++ ys)
```

The running time of this function is dependent on the size of its first argument. The problem with this definition becomes clear when analyzing necessary computations in the following examples:

```
s1, s2, s3, s4 :: [Char]
s1 = "aap" ++ ("noot" ++ "mies")
s2 = ("aap" ++ "noot") ++ "mies"
s3 = "aap" ++ "noot" ++ "mies"
s4 = (\x → x ++ "mies")("aap" ++ "noot")
```

In the first example "noot" is traversed to create "nootmies", and consecutively "aap" is traversed to create "aapnootmies". The second example is almost identical, but first "aapnoot" is constructed by traversing "aap" and then "aapnootmies" is constructed after traversing "aapnoot". Thus "aap" is traversed twice, a gross inefficiency! To partly counter this problem, (++) has been made right-associative, such that the third example produces the most optimal result. However, there are still many cases in which concatenation does not work optimal, as in the fourth example.

The Hughes' lists transformation solves this by treating string not as normal string (**String**) but as functions over strings (**String** → **String**). Strings now become continuations of strings, where the continuation represents an unfinished string, for which the tail still has to be filled in.

Strings and Hughes' strings can be transformed into each other by the functions (**rep** (ss)) and (**abs** (ss)).

```
repss :: String → (String → String)
repss ls = (ls ++ )
absss :: (String → String) → String
absss c = c ""
```

The speedup comes from the fact that, instead of normal concatenation, function composition can be used to concatenate two Hughes' strings.

```
s1 , s2 , s3 , s4 :: String
s1 = absss $ repss "aap" ∘ (repss "noot" ∘ repss "mies")
s2 = absss $ (repss "aap" ∘ repss "noot") ∘ repss "mies"
s3 = absss $ repss "aap" ∘ repss "noot" ∘ repss "mies"
s4 = absss $ (\x → x ∘ repss "mies") (repss "aap" ∘ repss "noot")
```

All examples now have the same, optimal running time because the continuation technique avoids building intermediate results: each string is only traversed at most once. Additionally, where the speed of normal concatenation depends on the size of its first argument, function composition has a constant running time.

### 2.1.2 Stream fusion

Another example of a type-changing program transformation is stream fusion, as found in Coutts et al. [CLS07, CSL07]. The goal of stream fusion is the same as Hughes' lists: optimizing operations on lists. Stream fusion does this using a technique called deforestation, which reduces the number of intermediate data structures constructed during evaluation. Consider the following example:

```
op :: (Int → Int) → [Int] → [Int]
op f = map f ∘ filter isEven ∘ map f
```

When this example is compiled without optimization, an intermediate result will be constructed at the position of each composition. Modern compilers such as GHC can partly optimize this kind of overhead away by changing the internal representation of lists to **Streams**

```
data Step s a =
  Done
| Yield a s
| Skip s
data Stream a = ∃ s. Stream { step :: s → Step s a , seed :: s }
```

Streams do not represent lists directly, but store a seed and a function. This function can be used to obtain a new item from the list and a modified seed (**Yield**). When the list is empty the

function returns **Done**. **Skip** is returned when only the seed is modified. This becomes more clear when looking at the function which converts a stream into a list:

```

absfs :: Stream a → [a]
absfs stream = extract $ seed stream
  where
    extract seed' =
      case step stream seed' of
        Done           → []
        Skip newseed   → extract newseed
        Yield x newseed → x : extract newseed

```

Conversely we can construct a stream from a list:

```

repfs :: [a] → Stream a
repfs ls = Stream next ls
  where
    next [] = Done
    next (x:xs) = Yield x xs

```

Here the list becomes the seed and the step function produces an item from the list at each step.

Many operations on lists can now be implemented by modifying the **step** function instead of traversing the entire stream. In this way intermediate constructions are avoided. An example is the map function:

```

mapS :: (a → b) → Stream a → Stream b
mapS f stream = Stream step (seed stream)
  step seed' =
    case step stream seed' of
      Done           → Done
      Skip newseed   → Skip newseed
      Yield a newseed → Yield (f a) newseed

```

Note that the **mapS** function is not recursive. It only manipulates the function that works on lists, not the lists themselves. This is what avoids the intermediate result from being constructed. We can now construct an optimized version of our example:

```

op :: (Int → Int) → [Int] → [Int]
op f = absfs ∘ mapS f ∘ filterS isEven ∘ mapS g ∘ repfs

```

The only function constructing a list is **abs<sub>fs</sub>**, all other operations are 'fused' together.

**Stream fusion in GHC** The Haskell GHC compiler incorporates a system which can be used to create such optimizations. This system is based on local, type-checked rewrite rules to rewrite terms which can be optimized. This is done for the Stream Fusion optimization by redefining the basic list functions and adding an optimizing rewrite rule in the following way:

```

map :: (a → b) → [a] → [b]
map f = absfs ∘ mapS f ∘ repfs
filter :: (a → Bool) → [a] → [a]
filter f = absfs ∘ filterS f ∘ repfs
{-# RULES "rep/abs" rep . abs = id #-}

```

The **op** example can now be optimized by the compiler, by first expanding and inlining all definitions and consecutively applying the optimization rewrite rule, getting rid of all **abs**-**rep** pairs. Thus this achieves a type-changing transformation by applying a non type-changing rewrite rule. However, this system is limited by how much the compiler can inline and replace the terms. It is primarily a syntactic method. To see where optimization may fail, consider the following example:

```

op :: (Int → Int) → [Int] → [Int]
op f = let applyMap = (\x → map f x)
      in applyMap ∘ filter isEven ∘ applyMap

```

When expanding these definitions, this yields the following term

```

op :: (Int → Int) → [Int] → [Int]
op f = let applyMap = (\x → absfs ∘ mapS f ∘ repfs $ x)
      in applyMap ∘ absfs ∘ filterS isEven ∘ repfs ∘ applyMap

```

Without proper inlining, the **rep**-**abs** rule can not fire. In this situation the inliner may solve this issue, but there are situations where inlining is not enough to make Stream Fusion work. Allowing direct type changes in the program however, yields the desired result:

```

op :: (Int → Int) → [Int] → [Int]
op f = let applyMap = (\x → mapS f x)
      in absfs ∘ applyMap ∘ filterS isEven ∘ applyMap ∘ repfs

```

## 2.2 Core Transformation System

Looking closely at the previous two examples, we can see a transformation pattern emerge. The transformations are *type-directed*: in both examples a single type is changed into another, more optimized type. The term transformations consequently follow the transformation of the types: all functions on the original type are replaced by functions on the optimized type, while maintaining the same overall semantics. In the process of transforming to a new type, the functions **rep** and **abs** have the special role of performing conversions between the original and the new type.

Type and transform systems are a formalization of this transformation pattern. In this section, the core concepts of this formalization will be introduced.

## 2.2.1 Transformation properties

Before developing a transformation system, it is useful to formalize some overall properties that we want a transformation system to uphold. Type and transform systems are intended to maintain the following properties for its transformations:

**Productive** Transformation is always possible

**Sound** The source and result program have equal types

**Equivalence** The source and result program are semantically equivalent

Note that property 2 does not exclude changes of types within a program. The complete program after transformation should have the same type as the original, but the types may have been changed with the subterms. Or in other words: the resulting types remain the same, but the *typing derivation* may differ. In the same manner property 3 requires only the complete programs to be semantically equivalent but says nothing about the semantics of its sub-terms. This is consistent with the example transformations: Locally the types and terms have been changed, but the overall type and semantics have remained the same.

Furthermore, this implies that the source program has to be well-typed to be eligible for transformation. The transformation should also provably produce a type-correct program as a result.

To get a feeling for what could be a valid TTS transformation, consider the following example transformations:

$$\text{"aap"} \rightsquigarrow \text{"aap"} \quad (2.1)$$

$$\text{"aap"} \not\rightsquigarrow 42 \quad (2.2)$$

$$\text{"aap"} \not\rightsquigarrow \text{"noot"} \quad (2.3)$$

$$\text{upper "aap"} \not\rightsquigarrow \text{rep}_{ss} (\text{abs}_{ss} \text{upper}) \text{"aap"} \quad (2.4)$$

$$\text{"app"} ++ \text{"noot"} \not\rightsquigarrow \text{rep}_{ss} \text{"aap"} \circ \text{rep}_{ss} \text{"noot"} \quad (2.5)$$

$$\text{"aap"} ++ \text{"noot"} \rightsquigarrow \text{abs}_{ss} (\text{rep}_{ss} \text{"aap"} \circ \text{rep}_{ss} \text{"noot"}) \quad (2.6)$$

$$(\lambda x. x ++ \text{"noot"}) \text{"aap"} \rightsquigarrow \text{abs}_{ss} ((\lambda x. x \circ \text{rep}_{ss} \text{"noot"}) (\text{rep}_{ss} \text{"aap"})) \quad (2.7)$$

$$(\lambda x. x ++ \text{"noot"}) \text{"aap"} \rightsquigarrow \text{abs}_{ss} ((\lambda x. \text{rep}_{ss} x \circ \text{rep}_{ss} \text{"noot"}) \text{"aap"}) \quad (2.8)$$

$$(\lambda x. x ++ \text{"noot"}) \text{"aap"} \not\rightsquigarrow \text{rep}_{ss} (\text{abs}_{ss} (\lambda x. x ++ \text{"noot"})) \text{"aap"} \quad (2.9)$$

$$\text{"aap"} \rightsquigarrow \text{abs}_{ss} (\text{rep}_{ss} \text{"aap"}) \quad (2.10)$$

Figure 2.1: Transformation examples

The  $\rightsquigarrow$  symbol is used to denote a valid transformation from some program to a resulting program,  $\not\rightsquigarrow$  represents transformations which do not adhere to the TTS transformation properties. The first two transformations are valid and invalid for obvious reasons. Example 2.3 and 2.4 show transformations in which the types of a transformation are valid, but the semantics of

the program have changed. Example 2.5 does not preserve the typing property and is thus not valid, the next example shows how this could become valid. Examples 2.7 and 2.8 show that there can be multiple valid results for the same source program. The next example shows that the wrong placement of **abs**<sub>ss</sub> and **rep**<sub>ss</sub> can result in a type-correct solution, but with the wrong semantics. In this case, "noot" and "app" will be reversed! The last example 2.10 is correct and illustrates that the **abs**<sub>ss</sub> and **rep**<sub>ss</sub> function from Hughes' string transformation have the property that **abs**  $\circ$  **rep**<sub>ss</sub>  $\equiv$  **id**. This property is key to the construction of the TTS system and will be elaborated upon in the next paragraph.

**Restricted type changes** Looking at the stream fusion and Hughes' strings examples we see that in both cases only one type is being changed. For Hughes' strings transformation, strings are changed to string continuations and with stream fusion lists are changed to streams. We will restrict the TTS system to only changing one base type in the source program to one different type in the resulting program. The type within the source program is denoted by  $\mathfrak{A}$ , the type in the result program by  $\mathfrak{R}$ . These source and result types are required to form a *retract*, written as  $\mathfrak{A} < \mathfrak{R}$ . Two types form a retract when there exists a pair of functions, **rep**  $:: \mathfrak{A} \rightarrow \mathfrak{R}$  and **abs**  $:: \mathfrak{R} \rightarrow \mathfrak{A}$ , for which **abs** is the left inverse of **rep**, meaning that **abs**  $\circ$  **rep**  $\equiv$  **id**. Both Hughes' strings and the stream fusion functions **rep** and **abs** have this property.

## 2.2.2 Object Language

A TTS can be built for many different programming languages. The language a TTS is designed for is called the object language. However, not every language is suitable as object language. TTS property 2 requires the object language to be strongly typed. Also, in order to be able to relate the semantics of the source and result of a transformation, the object language should come with an equivalence relation for the semantics of its terms.

One of the most simple languages which is suitable as a TTS object language is the simply typed lambda calculus. This language will be used to further introduce the core concepts of type and transform systems. Chapter 5 handles TTS systems for object languages with more advanced features.

The terms and types of the simply typed lambda calculus are of the following form:

$$\begin{aligned} e &::= x \mid c \mid e e \mid \lambda x. e \\ \tau &::= T \mid \tau \rightarrow \tau \\ \Gamma &::= \emptyset \mid \Gamma, x : \tau \end{aligned}$$

As expressions we have variables, constants, application and abstraction. Types can either be base types or function space. Figure 2.2 gives the well-known typing rules for the simply typed lambda calculus. The type and transform system for the simply typed lambda calculus is called  $TTS_\lambda$ .

The judgement  $\Gamma \vdash_\lambda e : \tau$  can be seen as a 3-way relation between types, terms and type environments. The elements of this relation consist of the valid stlc type assignments, and membership to this relation is determined by the typing rules. This relation is the starting point for defining a type and transform system for the simply typed lambda calculus.



Con	$\frac{c \text{ is a constant of type } T}{\Gamma \vdash_{\lambda} c : T}$
Var	$\frac{x : \tau \in \Gamma}{\Gamma \vdash_{\lambda} x : \tau}$
Lam	$\frac{\Gamma, x : \tau_a \vdash e : \tau_r}{\Gamma \vdash_{\lambda} \lambda x. e : \tau_a \rightarrow \tau_r}$
App	$\frac{\Gamma \vdash_{\lambda} f : \tau_a \rightarrow \tau_r \quad \Gamma \vdash_{\lambda} e : \tau_a}{\Gamma \vdash_{\lambda} f e : \tau_r}$
Judgement	$\boxed{\Gamma \vdash_{\lambda} e : \tau}$

Figure 2.2: Typing rules for the simply typed lambda calculus

It is not necessary to specify a complete semantics for the simply typed lambda calculus.  $TTS_{\lambda}$  is valid for all semantics which admit  $\beta\eta$ -convertibility on terms, as will be shown in chapter 3.

**The  $TTS_{\lambda}$  relation** At the heart of each type and transform system there is a TTS relation. A TTS relation contains the valid transformations between source and result terms, together with the typing information for both these terms. A TTS relation can be systematically derived from the typing relation of the underlying object language. For STLC we derive the following relation:

$$\mathring{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \mathring{\tau}$$

The resemblance with the original STLC typing judgement is obvious. Instead of one term, the relation now embodies two terms, the source and the result term. The  $\mathring{\Gamma}$  and  $\mathring{\tau}$  constructions are similar to normal types and contexts, except that they type the source and the result term simultaneously. Such a modified type is called a *typing functor* and the context is called a *functor context*. Any variation in types between the source and result terms is embodied in the typing functor and functor context.

**Typing functor** The variation in types in  $TTS_{\lambda}$  is limited to only changing one base type  $\mathfrak{A}$  from the source program into a type  $\mathfrak{R}$  in the transformation result. The typing functor allows such changes, while maintaining the invariant that both source and result terms are well-typed. The way this is achieved, is by extending the normal types of the object language with an 'hole' construction, represented by a  $\iota$ . This hole will represent the locations at which the types have changed during transformation. For STLC, the typing functor and functor context are defined as follows:

$$\begin{aligned}\dot{\tau} &::= \iota \mid \top \mid \dot{\tau} \rightarrow \dot{\tau} \\ \dot{\Gamma} &::= \emptyset \mid \dot{\Gamma}, x : \dot{\tau}\end{aligned}$$

Along with the typing functor and context we define a function which turns a functor into a base type of the object language. This is done by filling in the hole type with some type argument. This interpretation function for the typing functor and context are defined as follows:

$$\begin{aligned}\llbracket \dot{\tau} \rrbracket_{\tau} &: \tau \\ \llbracket \tau \rrbracket_{\tau} &= \tau \\ \llbracket \top \rrbracket_{\tau} &= \top \\ \llbracket (\dot{\tau}_a \rightarrow \dot{\tau}_r) \rrbracket_{\tau} &= \llbracket \dot{\tau}_a \rrbracket_{\tau} \rightarrow \llbracket \dot{\tau}_r \rrbracket_{\tau} \\ \llbracket \dot{\Gamma} \rrbracket_{\tau} &: \Gamma \\ \llbracket \emptyset \rrbracket_{\tau} &= \emptyset \\ \llbracket \dot{\Gamma}, a : \dot{\tau} \rrbracket_{\tau} &= \llbracket \dot{\Gamma} \rrbracket_{\tau}, a : \llbracket \dot{\tau} \rrbracket_{\tau}\end{aligned}$$

The typing functor and context are an extension of normal types. Thus, normal types naturally give rise to a functor, as is shown by the following lifting functions:

$$\begin{aligned}\tau \uparrow : \dot{\tau} \\ \top \uparrow &= \top \\ (\tau_a \rightarrow \tau_r) \uparrow &= \dot{\tau}_a \uparrow \rightarrow \dot{\tau}_r \uparrow \\ \Gamma \uparrow : \dot{\Gamma} \\ \Gamma \uparrow &= \emptyset \\ \Gamma, a : \tau \uparrow &= \Gamma \uparrow, a : \tau \uparrow\end{aligned}$$

If a typing functor or context contains no holes we call it *complete*. Note that when a typing functor is complete, it is actually just an ordinary type in the object language, lifted to a functor.

We can now construct some well-typed transformation examples for Hughes' strings as members of the TTS relation. The hole type is inserted at places where the type **String** in the source term is replaced by the type **String**  $\rightarrow$  **String** in the result term. Thus the hole type reflects a change in types.

$$\begin{array}{ll}\emptyset \vdash_{\lambda} \text{"aap"} \rightsquigarrow \text{"aap"} & : \mathbf{String} \\ \emptyset \vdash_{\lambda} \text{"aap"} \rightsquigarrow \mathbf{rep}_{ss} \text{"aap"} & : \iota \\ \emptyset \vdash_{\lambda} (++) \rightsquigarrow \circ & : \iota \rightarrow \iota \rightarrow \iota \\ \emptyset \vdash_{\lambda} \backslash x.x ++ \text{"hoi"} \rightsquigarrow \backslash x.x \circ \mathbf{rep}_{ss} \text{"hoi"} & : \iota \rightarrow \iota \\ \emptyset, x : \iota \vdash_{\lambda} x ++ \text{"hoi"} \rightsquigarrow x \circ \mathbf{rep}_{ss} \text{"hoi"} & : \iota \\ \emptyset \vdash_{\lambda} \text{"aap"} ++ \text{"hoi"} \rightsquigarrow \mathbf{abs}_{ss} (\mathbf{rep}_{ss} \text{"aap"} \circ \mathbf{rep}_{ss} \text{"hoi"}) & : \mathbf{String} \\ \emptyset \vdash_{\lambda} \text{"aap"} \rightsquigarrow \mathbf{abs}_{ss} (\mathbf{rep}_{ss} \text{"aap"}) & : \mathbf{String}\end{array}$$

Figure 2.3: Transformation examples

Tr-Con	$\frac{c \text{ is a constant of type } T}{\dot{\Gamma} \vdash_{\lambda} c \rightsquigarrow c : T}$	$\frac{c \text{ is a constant of type } T}{\Gamma \vdash_{\lambda} c : T}$	Con
Tr-Var	$\frac{x : \dot{\tau} \in \dot{\Gamma}}{\dot{\Gamma} \vdash_{\lambda} x \rightsquigarrow x : \dot{\tau}}$	$\frac{x : \tau \in \Gamma}{\Gamma \vdash_{\lambda} x : \tau}$	Var
Tr-Lam	$\frac{\dot{\Gamma}, x : \dot{\tau}_a \vdash_{\lambda} e \rightsquigarrow e' : \dot{\tau}_r}{\dot{\Gamma} \vdash_{\lambda} \backslash x. e \rightsquigarrow \backslash x. e' : \dot{\tau}_a \rightarrow \dot{\tau}_r}$	$\frac{\Gamma, x : \tau_a \vdash_{\lambda} e : \tau_r}{\Gamma \vdash_{\lambda} \backslash x. e : \tau_a \rightarrow \tau_r}$	Lam
Tr-App	$\frac{\dot{\Gamma} \vdash_{\lambda} f \rightsquigarrow f' : \dot{\tau}_a \rightarrow \dot{\tau}_r \quad \dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \dot{\tau}_a}{\dot{\Gamma} \vdash_{\lambda} f e \rightsquigarrow f' e' : \dot{\tau}_r}$	$\frac{\Gamma \vdash_{\lambda} f : \tau_a \rightarrow \tau_r \quad \Gamma \vdash_{\lambda} e : \tau_a}{\Gamma \vdash_{\lambda} f e : \tau_r}$	App
Tr-Rep	$\frac{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \mathfrak{A}}{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow \mathbf{rep} e' : \iota}$		
Tr-Abs	$\frac{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \iota}{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow \mathbf{abs} e' : \mathfrak{A}}$		
Judgement	$\boxed{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \dot{\tau}}$	$\boxed{\Gamma \vdash_{\lambda} e : \tau}$	

Figure 2.4: Type checking rules for the propagation relation

A member of the  $TTS_{\lambda}$  typing relation is said to be *complete* when it results in a base type and the typing context is *complete*. Because a complete functor type is just a lifted base type, we can write a complete transformation in the following form:  $\Gamma \uparrow \vdash_{\lambda} e \rightsquigarrow e' : T$ . Each complete element of the typing relation should preserve the TTS properties. This claim will be shown in chapter 3 for  $TTS_{\lambda}$ .

### 2.2.3 A TTS for STLC

The elements of a TTS relation are defined using inference rules. Figure 2.4 introduces the basic inference rules for  $TTS_{\lambda}$ . The first four rules (Tr-Con, Tr-Var, Tr-Lam and Tr-App) are modified versions of the STLC inference rules: an extra result term has been added and types have been changed to functors, just as the TTS relation. These rules do not perform any actual transformation but make sure transformation progresses over parts of the program which do not change. Consequently they are called the propagation rules. The existence of these rules makes that this transformation system adheres to the productivity property: there is always an identity transformation rule.

The rules Tr-Rep and Tr-Abs are called the introduction and elimination rules. These rules are used to convert a term of the source type to a term of the result type and back. Introduction using Tr-Rep introduces a hole in the typing functor, reflecting that the type of the term has changed at the position of this type. Note that the type  $\mathfrak{A}$ ,  $\mathfrak{R}$  and the functions **rep** and **abs** may be different for different instantiations of this basic STLC transformation system.

These rules form the basis for all STLC-based transformation systems. For specific transformations such as Hughes' strings this core is extended with extra rules to perform the required transformations.

## 2.3 A TTS for Hughes' strings

The Hughes' strings transformation constitutes of three core transformations: converting a **String** to a **String** continuation (**rep<sub>ss</sub>**), converting a **String** continuation back to a **String** (**abs<sub>ss</sub>**), and replacing **String** concatenation with function composition. For the STLC version of the Hughes' strings transformation, the  $TTS_\lambda$  base system is instantiated with the parameters specific to Hughes' strings. The source type  $\mathfrak{A}$  is instantiated to **String**,  $\mathfrak{R}$  is instantiated to **String**  $\rightarrow$  **String** and the functions **rep** and **abs** in the Tr-Rep and Tr-Abs rules are taken to be the **rep<sub>ss</sub>** and **abs<sub>ss</sub>** functions from Hughes' strings. What is left is adding a rule for transforming string concatenation to function composition. This rule looks as follows:

$$\text{Tr-Comp} \quad \frac{}{\bar{\Gamma} \vdash_\lambda (++) \rightsquigarrow (\circ) : \iota \rightarrow \iota \rightarrow \iota}$$

The rule Tr-Comp introduces the functor type  $\iota \rightarrow \iota \rightarrow \iota$ , reflecting the type changes induced by this transformation. The Hughes' strings transformation is abbreviated as  $TTS_{ss}$ .

**Example** Figure 2.5 shows an example derivation for a program transformation. This particular transformation derivation shows that the term  $(\lambda x. x ++ \text{"b"}) \text{"a"}$  can be transformed to the term **abs**  $((\lambda x. x \circ \text{rep } \text{"b"}) (\text{rep } \text{"a"}))$  using the Hughes' lists transformation system. This example illustrates how both source and result terms are constructed and typed simultaneously when deriving a transformation. The result of the transformation yields a complete element of the TTS relation, and is thus a valid TTS transformation.

## 2.4 Performing a transformation

In the previous sections a basic transformation system is presented which defines what constitutes a valid transformation for  $TTS_\lambda$ . However, this deduction system does not show how to algorithmically perform an actual transformation. For example, the deduction system allows an infinite application of the **rep** and **abs** rule, such as the following:

$$e \rightsquigarrow \text{abs} (\text{rep} (\text{abs} (\text{rep } e)))$$

This is hardly an optimizing program transformation! Even worse, the system allows endless chains of **abs** and **rep** applications, thus allowing infinite deduction trees. The reason that such endless chains can occur is because the rules of  $TTS_\lambda$  are not *syntax directed*. In a normal typing derivation for the simply typed lambda calculus, the derivation tree is uniquely determined by the term that is being typed. However, in the  $TTS_\lambda$  system this is not the case. Multiple results are possible for the same input.

Thus program transformation becomes a form of proof search: Given an input program, try to find a valid  $TTS_\lambda$  derivation. While one can always create an identity transformation (do nothing), this would not result in any improvements. One wants to find a transformation which gives as much optimization as possible, while avoiding unnecessary application of **abs** and **rep**.

How to actually do this is not part of this work, but is part of ongoing research by Sean Leather.

$$\begin{array}{c}
\text{Tr-Comp} \quad \frac{}{x : \iota, \emptyset \vdash_{\lambda} (++) \rightsquigarrow (\circ) : \iota \rightarrow \iota} \quad \text{Tr-Var} \quad \frac{}{x : \iota, \emptyset \vdash_{\lambda} x \rightsquigarrow x : \iota} \\
\text{Tr-App} \quad \frac{x : \iota, \emptyset \vdash_{\lambda} (++) \rightsquigarrow (\circ) \quad x : \iota}{x : \iota, \emptyset \vdash_{\lambda} (++) \rightsquigarrow (\circ) \quad x : \iota} \\
\quad \cdot \\
\quad \cdot \\
\text{Tr-App} \quad \frac{x : \iota, \emptyset \vdash_{\lambda} (++) \rightsquigarrow (\circ) \quad x : \iota}{x : \iota, \emptyset \vdash_{\lambda} (++) \rightsquigarrow (\circ) \quad x : \iota} \\
\text{Tr-App} \quad \frac{x : \iota, \emptyset \vdash_{\lambda} x \rightsquigarrow x \circ \text{rep } "b" : \iota}{x : \iota, \emptyset \vdash_{\lambda} x \rightsquigarrow x \circ \text{rep } "b" : \iota} \\
\text{Tr-Lam} \quad \frac{}{\emptyset \vdash_{\lambda} \lambda x. x \rightsquigarrow \lambda x. x \circ \text{rep } "b" : \iota \rightarrow \iota} \\
\quad \cdot \\
\quad \cdot \\
\text{Tr-App} \quad \frac{\emptyset \vdash_{\lambda} \lambda x. x \rightsquigarrow \lambda x. x \circ \text{rep } "b" : \iota \rightarrow \iota}{\emptyset \vdash_{\lambda} \lambda x. x \rightsquigarrow \lambda x. x \circ \text{rep } "b" : \iota} \\
\text{Tr-Con} \quad \frac{}{\emptyset \vdash_{\lambda} "a" \rightsquigarrow "a" : \text{String}} \\
\text{Tr-Rep} \quad \frac{}{\emptyset \vdash_{\lambda} "a" \rightsquigarrow \text{rep } "a" : \iota} \\
\text{Tr-Abs} \quad \frac{\emptyset \vdash_{\lambda} (\lambda x. x \rightsquigarrow "b") \quad "a" \rightsquigarrow (\lambda x. x \circ \text{rep } "b") \quad (\text{rep } "a") : \iota}{\emptyset \vdash_{\lambda} (\lambda x. x \rightsquigarrow "b") \quad "a" \rightsquigarrow \text{abs } ((\lambda x. x \circ \text{rep } "b") \quad (\text{rep } "a")) : \text{String}}
\end{array}$$

Figure 2.5: An example transformation derivation

## 3 Proof

The goal of a TTS transformation relation is to enforce the transformation properties as defined at the beginning of section 2.2.1. This chapter is dedicated to showing that this is indeed the case for the base system of  $TTS_\lambda$ . The main theorem shown here is formulated as follows:

**Theorem 1 (Complete  $TTS_\lambda$  Transformations Ensure the transformation properties)**

For all complete elements  $\Gamma \uparrow \vdash_\lambda e \rightsquigarrow e' : T$  from the relation  $TTS_\lambda$ , the transformation  $e \rightsquigarrow e'$  adheres to the transformation properties.

The first three section of this chapter show the Productivity, Soundness and Equivalence property for  $TTS_\lambda$ . The last two sections reflect on the theoretical background of the type and transform system.

### 3.1 $TTS_\lambda$ preserves Typing

A complete transformation is defined to be a transformation which is typed with a base type and for which the environment is complete (contains no holes). This means that, as long as the simultaneous typing system is sound with respect to the typing system of stlc, a complete transformation will result in two equally typed terms. This type soundness property is formalized by the following lemma:

**Lemma 1 (Soundness of  $TTS_\lambda$ )**

The  $TTS_\lambda$  relation is sound if for all elements  $\overset{\circ}{\Gamma} \vdash_\lambda e \rightsquigarrow e' : \overset{\circ}{\tau}$  of the transformation relation we have that  $\llbracket \overset{\circ}{\Gamma} \rrbracket_{\mathfrak{L}} \vdash_\lambda e : \llbracket \overset{\circ}{\tau} \rrbracket_{\mathfrak{L}}$  and  $\llbracket \overset{\circ}{\Gamma} \rrbracket_{\mathfrak{R}} \vdash_\lambda e' : \llbracket \overset{\circ}{\tau} \rrbracket_{\mathfrak{R}}$  have a valid typing derivation.

**Proof 1**

The evidence for this property follows from straightforward induction. The propagation rules of  $TTS_\lambda$  follow identical typing rules as the underlying STLC object language, and thus preserve the typing of the transformed terms. The Tr-Rep and Tr-Abs rules preserve the correctness of typing for both source and result terms. Thus, by induction all terms in the  $TTS_\lambda$  transformation relation have a typing assignment in the underlying STLC language.

It is now easy to state more formally that TTS property 2 holds in  $TTS_\lambda$ :

**Theorem 2 (Complete Transformations ensure TTS property 2)**

For all complete elements  $\Gamma \uparrow \vdash_\lambda e \rightsquigarrow e' : T$  both terms  $e$  and  $e'$  have equal type assignments  $\Gamma \vdash_\lambda e : T$  and  $\Gamma \vdash_\lambda e' : T$  in the simply typed lambda calculus.

**Proof 2 (1 and Completeness imply 2)**

From lemma 1 follows that for a complete element in the transformation relation  $\Gamma \uparrow \vdash_\lambda e \rightsquigarrow e' : T$ , we know that here exist valid typing derivations for  $\llbracket \Gamma \cdot \uparrow \rrbracket_{\mathfrak{L}} \vdash_\lambda e : T$  and  $\llbracket \Gamma \uparrow \rrbracket_{\mathfrak{R}} \vdash_\lambda e' : T$ .

$e' : T$ . From the definition of a complete environment simply follows that  $\llbracket \Gamma \uparrow \rrbracket_\tau$  for all  $\tau$ . Thus,  $\Gamma \vdash_\lambda e : T$  and  $\Gamma \vdash_\lambda e' : T$  are valid typing assignments in STLC with the same type and type environment.

### 3.2 $TTS_\lambda$ is Productive

To show that a program transformation always produces a result, it is enough to show that the transformation system admits the identity transformation: A program can always be transformed into itself. More formally, the following theorem has to be shown:

**Theorem 3 ( $TTS_\lambda$  admits the identity transformation)**

For all well-typed terms  $\Gamma \vdash_\lambda e : \tau$  an identity transformation exists with the judgement  $\overset{\circ}{\Gamma} \uparrow \vdash_\lambda e \rightsquigarrow e : \tau$ .

**Proof 3 ( $TTS_\lambda$  admits the identity transformation)**

The existence of the propagation rules makes that the identity transformation can always be constructed. Each rule in the stlc typing derivation has a matching rule in  $TTS_\lambda$  which can always be applied.

### 3.3 $TTS_\lambda$ preserves Semantics

The third TTS property states that two terms should be semantically equivalent. Semantic equivalence is proven by showing  $\beta\eta$ -convertibility of the source and result term under all closing environments, as formulated in as the following property:

**Lemma 2 (Complete  $TTS_\lambda$  transformations preserve semantics)**

For all complete elements  $\Gamma \uparrow \vdash_\lambda e \rightsquigarrow e' : T$  of the typing relation,  $e @ \theta \equiv_{\beta\eta} e' @ \theta$  for all closing substitutions  $\theta$ .

$e @ s$  represents capture-avoiding substitution of  $s$  in  $e$ . A closing substitution is a substitution which substitutes all free variables for closed terms. This is represented by the following construction:

$$\begin{aligned} \emptyset \downarrow &= \mathbf{id} \\ \theta, x \downarrow &= [x \mapsto e] \circ \theta \downarrow \end{aligned}$$

Lemma 2 is proven with the use of a logical relations.

#### 3.3.1 Logical Relations

A proof by logical relations is a proof methodology which has been very useful for proving properties about programming languages based on the simply typed lambda calculus. The fundamentals of logical relations are explained here, for further reading the reader is referred to Mitchell [Mit96], Hinze [Hin00] or Schurmann[SS08].

A logical relation represents a property over a term, or between multiple terms. Characteristic of a logical relation is that the represented property depends on the type of the term(s) over which

the property is established. For base types this is often a simple judgement formulated in some logic. At function types the relation establishes that inputs related by the logical relation result in outputs related by the logical relation. Thus a typical unary logical relation for the simply typed lambda calculus looks as follows:

$$\begin{aligned} \llbracket e \rrbracket_{\tau} &= \mathcal{J}(e) \\ \llbracket e \rrbracket_{\tau_a \rightarrow \tau_r} &= \forall a : \llbracket a \rrbracket_{\tau_a} \supset \llbracket e a \rrbracket_{\tau_r} \end{aligned}$$

Here  $\mathcal{J}(e)$  represents some property of the term  $e$ . The case for function terms states that function application should preserve this property. The logical relation may be stated in any logic, but is often represented in set-theory. Another way to look at logical relations is as an induction hypothesis indexed by types.

### 3.3.2 A Logical Relation for $TTS_{\lambda}$

$TTS_{\lambda}$  constructs a transformation between two terms  $e$  and  $e'$ , typed by a typing functor  $\hat{\tau}$ . Thus the logical relation becomes a binary logical relation over  $e$  and  $e'$ , indexed by the typing functor  $\hat{\tau}$ . To deal with free variables the relation is parametrized by closing substitutions to close the terms. This leads to the following logical relation for  $TTS_{\lambda}$ .

$$\begin{aligned} \mathcal{V}[\llbracket \iota \rrbracket] \quad \theta \theta' e e' &= \mathbf{rep} (e @ \rho) \equiv_{\beta\eta} e' @ \rho' \\ \mathcal{V}[\llbracket T \rrbracket] \quad \theta \theta' e e' &= e @ \rho \equiv_{\beta\eta} e' @ \rho' \\ \mathcal{V}[\llbracket \hat{\tau}_a \rightarrow \hat{\tau}_r \rrbracket] \theta \theta' e e' &= \forall a a' : \mathcal{V}[\llbracket \hat{\tau}_a \rrbracket] \theta \theta' a a' \supset \mathcal{V}[\llbracket \hat{\tau}_r \rrbracket] \theta \theta' (e a) (e' a') \end{aligned}$$

The basic property that is being established is  $\beta\eta$ -convertibility between the source and result term. The case for the hole type  $\iota$  represents that the source term can be transformed into the result term by applying the function **rep**. For base types we expect both terms to be convertible. The function type establishes that related transformations result in related transformations when applied.

The logical relation extends naturally from single terms to closing substitutions. Two closing substitutions are related when they substitute related terms for equal variables. Note that equal variables may have different types in the source and result terms, but are indexed by the same variable in the functor context. The relation for closing substitutions is indexed by the types in the functor context, which it closes.

$$\begin{aligned} \mathcal{E}[\llbracket \emptyset \rrbracket] \quad \mathbf{id} \quad \mathbf{id} &= \emptyset \\ \mathcal{E}[\llbracket \hat{\Gamma}, \hat{\tau} \rrbracket] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') &= \mathcal{E}[\llbracket \hat{\Gamma} \rrbracket] \theta \theta', \mathcal{V}[\llbracket \hat{\tau} \rrbracket] \theta \theta' i i' \end{aligned}$$

### 3.3.3 Proof using logical relations

When constructing a proof using logical relations, the proof is usually constructed using two key theorems, occurring in roughly the following form:

1. Fundamental theorem: the relation  $\llbracket e \rrbracket_{\tau}$  can be established for all terms  $e : \tau$



2. Extraction theorem: terms related by  $\llbracket e \rrbracket_\tau$  give rise to some property  $\mathcal{P}(e)$

It is easy to see that the combination of these two theorems can be used to prove the property  $\mathcal{P}(e)$  for all  $e : \tau$ . This same approach is taken here, leading to the following key theorems to show that a transformation in  $TTS_\lambda$  is semantics preserving.

**Theorem 4 (Fundamental Theorem for  $TTS_\lambda$ )**

For all term  $e$  and  $e'$  for which a transformation deduction  $\dot{\Gamma} \vdash_\lambda e \rightsquigarrow e' : \dot{\tau}$  exists, the logical relation  $\mathcal{V}[\llbracket \dot{\tau} \rrbracket] \theta \theta' e e'$  holds under all related environments  $\mathcal{E}[\llbracket \dot{\Gamma} \rrbracket] \theta \theta'$ .

**Theorem 5 (Extraction Theorem for  $TTS_\lambda$ )**

For all complete terms  $\Gamma \vdash_\lambda e : T$ ,  $\Gamma \vdash_\lambda e' : T$  and term closure  $\theta : \Gamma \downarrow$ , the relation  $\mathcal{V}[\llbracket T \rrbracket] \theta \theta e e'$  implies  $e @ \theta \equiv_{\beta\eta} e' @ \theta$ .

**Corollary 1 (A Substitution Environment is related to Itself)**

An important corollary of the Fundamental Theorem and Identity Transformation property, is that a substitution environment is related to itself. This follows from the fact that all terms in the environment have an identity transformation and according to the fundamental theorem each valid transformation is part of the logical relation.

**Proof 4 (Extraction Theorem)**

The proof for the extraction theorem is immediate, because the logical relation  $\mathcal{V}[\llbracket T \rrbracket] \theta \theta e e'$  on base types is defined as  $e @ \theta \equiv_{\beta\eta} e' @ \theta$ .

With these properties established it is now possible to show that  $TTS_\lambda$  is semantics preserving.

**Proof 5 (The Fundamental Theorem and Extraction Theorem imply 2)**

The Fundamental Theorem shows that all complete elements are  $\Gamma \uparrow \vdash_\lambda e \rightsquigarrow e' : T$  logically related, with aid of Corollary 1 which shows that substitution environments are always related to themselves. The Extraction Theorem shows that logical relations give rise to  $\beta\eta$ -equality for complete terms, thus  $e @ \theta \equiv_{\beta\eta} e' @ \theta$  for all  $\theta$ .

What is left is showing the fundamental theorem for  $TTS_\lambda$ .

**Fundamental theorem** Before showing the fundamental theorem, two properties among logical relations have to be established. These properties are stated as 'logical equivalences' between two logical relations, meaning that either both relations hold, or they both do not hold. They always have the same truth value.

The first lemma establishes that  $\mathcal{V}[\llbracket \dot{\tau} \rrbracket]$  is closed under  $\beta\eta$ -equivalence of the related terms. The second lemma is the Crossing Lemma, which shows that substitutions can be commuted between the closing environments and the related terms. This lemma is the key to showing the logical relation under beta reduction.

**Lemma 3 ( $\mathcal{V}[\llbracket \dot{\tau} \rrbracket]$  is Closed under  $\beta\eta$ -equality)**

Two logical relations  $\mathcal{V}[\llbracket \dot{\tau} \rrbracket] \theta \theta' e e'$  and  $\mathcal{V}[\llbracket \dot{\tau} \rrbracket] \theta \theta' f f'$  are logically equivalent when  $e \equiv_{\beta\eta} f$  and  $e' \equiv_{\beta\eta} f'$ .

**Lemma 4**

For any two terms  $i$  and  $i'$  in which  $x$  does not appear free, the relation  $\mathcal{V}[\![\dot{\tau}]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') \mathbf{e} \mathbf{e}'$  is logically equivalent to  $\mathcal{V}[\![\dot{\tau}]\!] \theta \theta' (\mathbf{e} @ [x \mapsto i]) (\mathbf{e}' @ [x \mapsto i'])$ .

Both lemmas are proven at the end of this paragraph on page 29, first the fundamental theorem is shown.

**Proof 6 (Proof of the Fundamental Theorem)**

The fundamental theorem shows that all terms  $\mathbf{e}$  and  $\mathbf{e}'$  arising from a transformation derivation  $\dot{\Gamma} \vdash_{\lambda} \mathbf{e} \rightsquigarrow \mathbf{e}' : \dot{\tau}$  give rise to an element in the logical relation  $\mathcal{V}[\![\dot{\tau}]\!] \theta \theta' \mathbf{e} \mathbf{e}'$ , under all related environments  $\mathcal{E}[\![\dot{\Gamma}]\!] \theta \theta'$ . This is shown by induction on the deduction rules of  $TTS_{\lambda}$ .

$$\text{Tr-Con} \quad \boxed{\frac{\text{c is a constant of type T}}{\dot{\Gamma} \vdash_{\lambda} \mathbf{c} \rightsquigarrow \mathbf{c} : \text{T}}}$$

Here we have to show the logical relation for base types:  $\mathbf{c} @ \theta \equiv_{\beta\eta} \mathbf{c} @ \theta'$ , which is trivially true for constants.

$$\begin{aligned} & \mathbf{c} @ \theta \\ & \equiv_{\beta\eta} \{ \text{Substitution over constants} \} \\ & \mathbf{c} \\ & \equiv_{\beta\eta} \{ \text{Substitution over constants} \} \\ & \mathbf{c} @ \theta' \end{aligned}$$

$$\text{Tr-Var} \quad \boxed{\frac{x : \dot{\tau} \in \dot{\Gamma}}{\dot{\Gamma} \vdash_{\lambda} x \rightsquigarrow x : \dot{\tau}}}$$

Relatedness of variables is shown 'under related substitution environments', which contain two related terms  $i$  and  $i'$  for each free variable:

$$\begin{aligned} & \mathcal{E}[\![\dot{\Gamma}, x]\!] (x @ [x \mapsto i]) (x @ [x \mapsto i']) \\ & \supset \{ \text{Extract related terms for variable x} \} \\ & \mathcal{V}[\![\dot{\tau}]\!] \theta \theta' i i' \\ & \supset \{ \text{Substitution} \} \\ & \mathcal{V}[\![\dot{\tau}]\!] \theta \theta' (x @ [x \mapsto i]) (x @ [x \mapsto i']) \\ & \supset \{ \text{Crossing lemma} \} \\ & \mathcal{V}[\![\dot{\tau}]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') x x \end{aligned}$$

$$\text{Tr-Lam} \quad \boxed{\frac{\dot{\Gamma}, x : \dot{\tau}_a \vdash_{\lambda} \mathbf{e} \rightsquigarrow \mathbf{e}' : \dot{\tau}_r}{\dot{\Gamma} \vdash_{\lambda} \lambda x. \mathbf{e} \rightsquigarrow \lambda x. \mathbf{e}' : \dot{\tau}_a \rightarrow \dot{\tau}_r}}$$

The lambda rule shows that related inputs result in related outputs under beta-reduction. The following statement is to be shown:  $\mathcal{V}[\![\dot{\tau}_a]\!] \theta \theta' a a' \supset \mathcal{V}[\![\dot{\tau}_r]\!] \theta \theta' ((\lambda x. \mathbf{e}) a) ((\lambda x. \mathbf{e}') a')$

- $\mathcal{V}[\![\tau_a]\!] \theta \theta' a a'$
- $\supset \{ \text{Induction hypothesis on } e \text{ and } e' \text{ with related } a \text{ and } a' \text{ in the environment} \}$
- $\mathcal{V}[\![\tau_r]\!] ([x \mapsto a] \circ \theta) ([x \mapsto a'] \circ \theta') e e'$
- $\supset \{ \text{Crossing lemma} \}$
- $\mathcal{V}[\![\tau_r]\!] \theta \theta' (e @ [x \mapsto a]) (e' @ [x \mapsto a'])$
- $\supset \{ \text{Relation is closed under beta-eta equivalence} \}$
- $\mathcal{V}[\![\tau_r]\!] \theta \theta' ((\lambda x. e) a) ((\lambda x. e') a')$

$$\text{Tr-App} \quad \frac{\begin{array}{c} \dot{\Gamma} \vdash_{\lambda} f \rightsquigarrow f' : \tau_a \rightarrow \tau_r \\ \dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \tau_a \end{array}}{\dot{\Gamma} \vdash_{\lambda} f e \rightsquigarrow f' e' : \tau_r}$$

The logical relation already establishes that related inputs result in related outputs for related terms. This makes the application rule trivial to prove. The following needs to be shown:  $\mathcal{V}[\![\tau_r]\!] \theta \theta' (f e) (f' e')$

- $\supset \{ \text{Induction on } e \text{ and } e' \}$
- $\mathcal{V}[\![\tau_a]\!] \theta \theta' e e'$
- $\supset \{ \text{Induction on } f \text{ and } f' \text{ and modus ponens} \}$
- $\mathcal{V}[\![\tau_r]\!] \theta \theta' (f e) (f' e')$

$$\text{Tr-Rep} \quad \frac{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \mathfrak{A}}{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow \mathbf{rep} e' : \iota}$$

The logical relation for the hole type  $\iota$  dictates that **rep** applied to the source term should be  $\beta\eta$ -equivalent to the result term. Thus for the rep rule we simple need to show that  $\mathbf{rep} e @ \theta \equiv_{\beta\eta} \mathbf{rep} e' @ \theta'$ .

$$\begin{aligned} & \mathbf{rep} e @ \theta \\ & \equiv_{\beta\eta} \{ \text{Induction hypothesis} \} \\ & \mathbf{rep} e' @ \theta' \end{aligned}$$

$$\text{Tr-Abs} \quad \frac{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow e' : \iota}{\dot{\Gamma} \vdash_{\lambda} e \rightsquigarrow \mathbf{abs} e' : \mathfrak{A}}$$

To prove the Tr-Abs rule, the fact that **abs** and **rep** are a retraction pair is needed. The statement to prove is  $e @ \theta \equiv_{\beta\eta} \mathbf{abs} e' @ \theta'$ .

$$\begin{aligned} & e @ \theta \\ & \equiv_{\beta\eta} \{ \text{Retraction pair } \mathbf{abs} \text{ and } \mathbf{rep} \} \\ & \mathbf{abs} (\mathbf{rep} e @ \theta) \\ & \equiv_{\beta\eta} \{ \text{Induction hypothesis} \} \\ & \mathbf{abs} e' @ \theta' \end{aligned}$$

What is left is showing the 3 and 4 used in this proof.

**Proof 7 (Proof of 4)**

Logical equivalence is proven by showing implication in both directions. In both directions the proof is carried out by induction on the typing functor  $\hat{\tau}$ . The two implications directions are proven by mutual induction: both directions of the bi-implication make use of the other direction to prove themselves. While this may seem like cyclic reasoning, it is not, because the induction hypothesis is only ever called on smaller types.

**Proof in the direction:**  $\mathcal{V}[\![\hat{\tau}]\!] \theta \theta' (e @ [x \mapsto i]) (e' @ [x \mapsto i'])$  implies  $\mathcal{V}[\![\hat{\tau}]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') e e'$ .

ld case, showing  $\mathbf{rep} e @ [x \mapsto i] @ \theta \equiv_{\beta\eta} e' @ [x \mapsto i'] @ \theta'$

$$\begin{aligned}
& \mathbf{rep} e @ [x \mapsto i] \circ \theta \\
& \equiv_{\beta\eta} \{ \text{Definition substitution and } \cdot @ \cdot \} \\
& \mathbf{rep} (e @ [x \mapsto i]) @ \theta \\
& \equiv_{\beta\eta} \{ \text{Premise} \} \\
& (e' @ [x \mapsto i']) @ \theta' \\
& \equiv_{\beta\eta} \{ \text{Definition substitution and } \cdot @ \cdot \} \\
& e' @ [x \mapsto i'] \circ \theta'
\end{aligned}$$

T case is analogous to the ld case.

$\tau_a \rightarrow \tau_r$  case, showing  $\mathcal{V}[\![\hat{\tau}_a]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') a a' \supset \mathcal{V}[\![\hat{\tau}_r]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') (e a) (e' a')$

$$\begin{aligned}
& \mathcal{V}[\![\hat{\tau}_a]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') a a' \\
& \supset \{ \text{Crossing lemma} \} \\
& \mathcal{V}[\![\hat{\tau}_a]\!] \theta \theta' (a @ [x \mapsto i]) (a' @ [x \mapsto i']) \\
& \supset \{ \text{Premise} \} \\
& \mathcal{V}[\![\hat{\tau}_r]\!] \theta \theta' (e a @ [x \mapsto i]) (e a' @ [x \mapsto i']) \\
& \supset \{ \text{Induction} \} \\
& \mathcal{V}[\![\hat{\tau}_r]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') (e a) (e' a')
\end{aligned}$$

**Proof in the direction:**  $\mathcal{V}[\![\hat{\tau}]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') e e'$  implies  $\mathcal{V}[\![\hat{\tau}]\!] \theta \theta' (e @ [x \mapsto i]) (e' @ [x \mapsto i'])$ .

ld case, showing  $\mathbf{rep} e @ [x \mapsto i] \circ \theta \equiv_{\beta\eta} e' @ [x \mapsto i'] \circ \theta'$

$$\begin{aligned}
& \mathbf{rep} (e @ [x \mapsto i]) @ \theta \\
& \equiv_{\beta\eta} \{ \text{Definition substitution and } \cdot @ \cdot \} \\
& \mathbf{rep} e @ [x \mapsto i] \circ \theta \\
& \equiv_{\beta\eta} \{ \text{Premise} \} \\
& e' @ [x \mapsto i'] \circ \theta'
\end{aligned}$$

$$\equiv_{\beta\eta} \{ \text{Definition substitution and } \cdot @ \cdot \}$$

$$(e' @ [x \mapsto i']) m @ \theta'$$

T case is analogous to the Id case.

$\tau_a \rightarrow \tau_r$  case, showing  $\mathcal{V}[\![\hat{\tau}_a]\!] \theta \theta' a a' \supset \mathcal{V}[\![\hat{\tau}_r]\!] \theta \theta' ((e @ [x \mapsto i]) a) ((e' @ [x \mapsto i']) a')$

$$\begin{aligned} & \mathcal{V}[\![\hat{\tau}_a]\!] \theta \theta' a a' \\ \supset & \{ \text{Substitution on unbound variable } x \text{ in } a \} \\ & \mathcal{V}[\![\hat{\tau}_a]\!] \theta \theta' (a @ [x \mapsto i]) (a' @ [x \mapsto i']) \\ \supset & \{ \text{Crossing lemma} \} \\ & \mathcal{V}[\![\hat{\tau}_a]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') a a' \\ \supset & \{ \text{Premise} \} \\ & \mathcal{V}[\![\hat{\tau}_r]\!] ([x \mapsto i] \circ \theta) ([x \mapsto i'] \circ \theta') (e a) (e a') \\ \supset & \{ \text{Induction} \} \\ & \mathcal{V}[\![\hat{\tau}_r]\!] \theta \theta' (e a @ [x \mapsto i]) (e a' @ [x \mapsto i']) \\ \supset & \{ x \text{ is unbound in } a \} \\ & \mathcal{V}[\![\hat{\tau}_r]\!] \theta \theta' ((e @ [x \mapsto i]) a) ((e' @ [x \mapsto i']) a') \end{aligned}$$

### Proof 8 (Proof of 3)

The proof is by induction on  $\hat{\tau}$ . Due to the symmetric nature of this statement it is only necessary to prove this property in one direction, although

Id case, proving:  $\text{rep } f @ \theta \equiv_{\beta\eta} f' @ \theta'$

$$\begin{aligned} & \text{rep } f @ \theta \\ \equiv_{\beta\eta} & \{ \text{Premise } e \equiv_{\beta\eta} f \text{ and symmetry} \} \\ & \text{rep } e @ \theta \\ \equiv_{\beta\eta} & \{ \text{Premise} \} \\ & e' @ \theta' \\ \equiv_{\beta\eta} & \{ \text{Premise} \} \\ & f' @ \theta' \end{aligned}$$

T case is analogous to the Id case.

$\tau_a \rightarrow \tau_r$  case, showing for all  $a$  and  $a'$ :  $\mathcal{V}[\![\tau_a]\!] \theta \theta' a a' \supset \mathcal{V}[\![\tau_r]\!] \theta \theta' (f a) (f' a')$  given the premises.

$$\begin{aligned} & \mathcal{V}[\![\tau_a]\!] \theta \theta' a a' \\ \equiv_{\beta\eta} & \{ \text{Premise} \} \\ & \mathcal{V}[\![\tau_r]\!] \theta \theta' (e a) (e a') \\ \equiv_{\beta\eta} & \{ \text{Induction hypothesis with extended premises: } e a \equiv_{\beta\eta} f a \text{ and } e' a' \equiv_{\beta\eta} f' a' \} \\ & \mathcal{V}[\![\tau_r]\!] \theta \theta' (f a) (f' a') \end{aligned}$$

### 3.4 Hughes' Strings Transformation Preserves the TTS Properties

We can now show that the Hughes' Strings instantiation of  $TTS_\lambda$  is a valid TTS transformation by extending the base proof for  $TTS_\lambda$ . Two additional properties have to be established:

- It needs to be shown that  $\mathbf{abs}_{ss}$  and  $\mathbf{rep}_{ss}$  form a retraction pair, because this is a premise of  $TTS_\lambda$ . A retraction pair has the property that  $\mathbf{abs}_{ss} \circ \mathbf{rep}_{ss} \equiv \mathbf{id}$ .
- An extra case has to be added to the Fundamental Theorem for the Tr-Comp rewrite rule.

A retraction is proven through straightforward equational reasoning.

#### Proof 9 ( $\mathbf{abs}_{ss}$ and $\mathbf{rep}_{ss}$ form a retraction)

$$\begin{aligned}
 & \mathbf{abs}_{ss} \circ \mathbf{rep}_{ss} \\
 \equiv_{\beta\eta} & \{ \text{Eta expansion} \} \\
 & \backslash x \rightarrow (\mathbf{abs}_{ss} \circ \mathbf{rep}_{ss}) x \\
 \equiv_{\beta\eta} & \{ \text{Definition composition} \} \\
 & \backslash x \rightarrow \mathbf{abs}_{ss} (\mathbf{rep}_{ss} x) \\
 \equiv_{\beta\eta} & \{ \text{Definition of } \mathbf{rep}_{ss} \} \\
 & \backslash x \rightarrow \mathbf{abs}_{ss} (x ++ "") \\
 \equiv_{\beta\eta} & \{ \text{Definition of } \mathbf{abs}_{ss} \} \\
 & \backslash x \rightarrow x ++ "" \\
 \equiv_{\beta\eta} & \{ \text{Definition of } (++) \} \\
 & \backslash x \rightarrow x \\
 \equiv_{\beta\eta} & \{ \text{Definition of identity} \} \\
 & \mathbf{id}
 \end{aligned}$$

The extra case for Tr-Comp for the Fundamental Theorem shows that the Tr-Comp rule adheres to the logical relation. Because the Tr-Comp rule contains only base types, this boils down to the following lemma:

#### Lemma 5 (Tr-Comp support the Fundamental Theorem)

For all environments  $s$  and  $s'$  and related terms  $\mathbf{rep}_{ss} a @ s \equiv_{\beta\eta} a' @ s'$  and  $(\mathbf{rep} (ss)) b @ s \equiv_{\beta\eta} b' @ s'$  we have that  $(\mathbf{rep}_{ss} (a ++ b)) @ s \equiv_{\beta\eta} a' ++ b' @ s'$ .

#### Proof 10 (Tr-Comp support the Fundamental Theorem)

$$\begin{aligned}
 & (\mathbf{rep}_{ss} (a ++ b)) @ s \\
 \equiv_{\beta\eta} & \{ \text{Definition } \mathbf{rep}_{ss} \} \\
 & ((a ++ b) ++ ) @ s \\
 \equiv_{\beta\eta} & \{ \text{Commutate substitution} \} \\
 & (a @ s ++ b @ s) ++ \\
 \equiv_{\beta\eta} & \{ \text{Eta expansion} \} \\
 & \backslash x. (a @ s ++ b @ s) ++ x
 \end{aligned}$$

$$\begin{aligned}
&\equiv_{\beta\eta} \{ \text{Associativity } (++) \} \\
&\quad \backslash x. a @ s ++ (b @ s ++ x) \\
&\equiv_{\beta\eta} \{ \text{Definition } (\circ) \} \\
&\quad \backslash x. (a @ s ++ ) \circ (b @ s ++ ) x \\
&\equiv_{\beta\eta} \{ \text{Eta reduction} \} \\
&\quad (a @ s ++ ) \circ (b @ s ++ ) \\
&\equiv_{\beta\eta} \{ \text{Definition } \mathbf{rep}_{ss} \} \\
&\quad \mathbf{rep}_{ss} a @ s \circ \mathbf{rep}_{ss} b @ s \\
&\equiv_{\beta\eta} \{ \text{Premises} \} \\
&\quad a' @ s' \circ b' @ s' \\
&\equiv_{\beta\eta} \{ \text{Definition substitution} \} \\
&\quad a' \circ b' @ s'
\end{aligned}$$

### 3.5 Type Abstraction

Taking back a step, we can see that the ideas of the type and transform system are firmly rooted in the idea of type abstraction, or representation independence as it is called in Mitchell [Mit96]. The idea of type abstraction is the idea that the implementation of a datatype can be freely changed, as long as this results in the same external behavior. This makes it possible for the creators of compilers to change for example the representation of integers without breaking all software, as long as all functions on integers yield comparable results.

In our transformation system, the **abs** and **rep** functions make it possible to locally change the representation of a type, making it possible to switch to a different type in limited parts of the program. The requirement of the type and transform system that the transformed types form a retraction and that each transformed term is related to another transformed term can be seen as showing that the transformed type is just a different implementation for the original type. In the case of Hughes' strings the relatedness of Tr-Comp and the left inverse of  $\mathbf{rep}_{ss}$  and  $\mathbf{abs}_{ss}$  show that **String**  $\rightarrow$  **String** can be a replacement implementation for **String** under the idea of type abstraction.

### 3.6 The Typing Functor is an actual Functor

The typing functor is the heart of the type and transform system. The use of this functor gives rise to both the type-correctness as well as the semantic correctness of  $TTS_\lambda$  through the logical relation. The fact that this works out is because the typing functor is an actual functor as known in the field category theory. It is purely out of theoretical curiosity that we show this property here. Before showing that the typing functor is a proper functor, we introduce the concept of functors and difunctors.

**Functors** A functor can be seen as a function on types. It takes as parameter a type and yields a new type based on its argument. Associated with such a type-level functor is a term-level functor which lifts functions on the type parameter to functions on the functor:

```

type F a
fmap :: (a → b) → F a → F b

```

For **fmap** to be a proper term-level functor it has to obey the functor laws:

```

fmap id = id
fmap g ∘ fmap f = fmap (g ∘ f)

```

A list is an example of a Functor in Haskell:

```

data List a = Nil | Cons a (List a)

fmaplist :: (a → b) → List a → List b
fmaplist Nil = Nil
fmaplist f (Cons a l) = Cons (f a) (fmaplist f l)

```

What makes functors special, is that an implementation for the term level function **fmap** can be unambiguously constructed from the functor type. In other words: from a given type a term can be derived which adheres to the functor properties. This is the way in which functors connect the term and type world. The rest of this section is dedicated to showing how such a term-level functor can be constructed for the typing functor  $\hat{\tau}$ .

This does not work for any type, however. For normal functors, a term-level functor can only be constructed when the argument type occurs in covariant (result) positions within the datatype. This means **fmap** can be constructed for all polynomial types (datatypes without functions), but not for all datatypes containing functions. In the following case a functor can be constructed, because the functor parameter is in a covariant position:

```

type IntF a = Int → a
fmapIntF :: (a → b) → IntF a → IntF b
fmapIntF f intf = f ∘ intf

```

When the type parameter occurs at a covariant (or argument) position, a functor can not be constructed anymore:

```

type Func a = a → a
fmapFunc :: (a → b) → Func a → Func b
fmapFunc f func = f ∘ func ∘ ?

```

At the question mark a function is needed of the type  $b \rightarrow a$  to convert the argument of type  $b$  to an argument of type  $a$ . The function argument is of type  $a \rightarrow b$ , so this does not work. The typing functor  $\hat{\tau}$  includes a function space constructor, so to construct a term-level functor for the typing functor, something more powerful than a normal functor is needed.

Meijer and Hutton[MH95] showed that it is possible to define functors for function types (exponential types) with the use of **dimaps**. A **dimap** is the same as the normal **fmap** but with an extra function argument which can be used for occurrences of the type parameter at contra-variant positions.



$$\mathbf{dimap}_F :: (b \rightarrow a) \rightarrow (a \rightarrow b) \rightarrow F a \rightarrow F b$$

The `Func` example can now be completed with the use of a **dimap**.

$$\begin{aligned} \mathbf{dimap}_{\text{Func}} &:: (b \rightarrow a) \rightarrow (a \rightarrow b) \rightarrow \text{Func } a \rightarrow \text{Func } b \\ \mathbf{dimap}_{\text{Func}} \, g \, f \, \text{func} &= f \circ \text{func} \circ g \end{aligned}$$

The functor laws also generalize to the extended functor **dimap**:

$$\begin{aligned} \mathbf{dimap}_F \, \text{id} \, \text{id} &= \text{id} \\ \mathbf{dimap}_F \, g1 \, g2 \circ \mathbf{dimap}_F \, f1 \, f2 &= \mathbf{dimap}_F \, (f1 \circ g1) \, (g2 \circ f2) \end{aligned}$$

Note how the first function is contra-variant and the second covariant in the result type when doing composition.

Based on this work, a term-level **dimap** can be defined for the typing functor  $\hat{\tau}$  using the following functor-indexed function:

$$\begin{aligned} \mathbf{dimap}_{\hat{\tau}} &:: (a \rightarrow b) \rightarrow (b \rightarrow a) \rightarrow \hat{\tau}_b \rightarrow \hat{\tau}_a \\ \mathbf{dimap}_{\hat{\tau}} \quad \text{con cov } x &= \text{cov } x \\ \mathbf{dimap}_{\hat{\tau}} \quad \text{cov cov } x &= x \\ \mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \text{con cov } f &= \mathbf{dimap}_{\hat{\tau}_r} \text{con cov } f \circ \mathbf{dimap}_{\hat{\tau}_a} \text{cov con} \end{aligned}$$

At the hole position the covariant function is applied to manipulate the hole value. For constant types `T` the **dimap** is just the identity function. Most interesting is the case for function space, which recursively transforms the argument and result of the function, but with the argument functions `con` and `cov` switched for the contra-variant call. Switching these functions 'flips' the type signature of the function from  $\hat{\tau}_b \rightarrow \hat{\tau}_a$  to  $\hat{\tau}_a \rightarrow \hat{\tau}_b$ .

**Typing Functor** Showing that the typing functor is an actual functor can now be done by showing that the **dimap** constructed for the typing functor preserves the functor laws: identity and composition. The identity law follows readily from the definition of **dimap** and induction on the typing functor. The functor law for composition also follows from induction on the typing functor, the only non-trivial case here is the function case, which can be shown using equational reasoning:

$$\begin{aligned} &\mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \, g1 \, g2 \circ \mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \, f1 \, f2 \\ \equiv_{\beta\eta} &\{ \text{Eta expansion} \} \\ &(\mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \, g1 \, g2 \circ \mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \, f1 \, f2) \, x \\ \equiv_{\beta\eta} &\{ \text{Definition composition} \} \\ &\mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \, g1 \, g2 \, (\mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} \, f1 \, f2 \, x) \\ \equiv_{\beta\eta} &\{ \text{Definition } \mathbf{dimap} \} \\ &\mathbf{dimap}_{\hat{\tau}_r} \, g1 \, g2 \circ (\mathbf{dimap}_{\hat{\tau}_r} \, f1 \, f2 \circ x \circ \mathbf{dimap}_{\hat{\tau}_a} \, f2 \, f1) \circ \mathbf{dimap}_{\hat{\tau}_a} \, g2 \, g1 \\ \equiv_{\beta\eta} &\{ \text{Associativity composition} \} \\ &(\mathbf{dimap}_{\hat{\tau}_r} \, g1 \, g2 \circ \mathbf{dimap}_{\hat{\tau}_r} \, f1 \, f2) \circ x \circ (\mathbf{dimap}_{\hat{\tau}_a} \, f2 \, f1 \circ \mathbf{dimap}_{\hat{\tau}_a} \, g2 \, g1) \\ \equiv_{\beta\eta} &\{ \text{Induction hypothesis} \} \end{aligned}$$

$$\begin{aligned}
& \mathbf{dimap}_{\hat{\tau}_r} (g2 \circ f2) (f1 \circ g1) \circ x \circ \mathbf{dimap}_{\hat{\tau}_a} (f1 \circ g1) (g2 \circ f2) \\
& \equiv_{\beta\eta} \{ \text{Definition } \mathbf{dimap} \} \\
& \mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} (f1 \circ g1) (g2 \circ f2) x \\
& \equiv_{\beta\eta} \{ \text{Eta redutcion} \} \\
& \mathbf{dimap}_{\hat{\tau}_a \rightarrow \hat{\tau}_r} (f1 \circ g1) (g2 \circ f2)
\end{aligned}$$

Thus the typing functor is a proper functor.

## 4 Mechanical Proof

### 4.1 STLC object language

Fundamental to a mechanical formalization of the TTS system is the representation of the object language, STLC. STLC can be represented in multiple ways, as described in [Keu11]. The essential choice is between a Higher Order Abstract Syntax and a de Bruijn representation. Although HOAS terms can be constructed in Agda, Agda is not strong enough to reason about semantic equivalence of HOAS terms, unlike other languages such as Twelf [SS08]. The representation chosen here is a first-order representation using well-typed de Bruijn indices as found in Keller and Altenkirch [KA10]. A first-order formulation is mandatory because it allows full inductive reasoning over terms and types in the object language and thus reasoning about the semantics. Formulating using well-typed de Bruijn indices is useful because it asserts important properties about the terms by construction.

**De Bruijn indices** is a way to represent variables in languages based on the lambda calculus. Instead of naming a variable, a variable is given an index which denotes at which lambda the variable is bound. More precisely, the index denotes the number of lambdas that occur between the variable and its binding site. *Well-typed* de Bruijn indices are an extension of this idea: each variable now has a type associated with its binding site. When a term contains free variables, a context is used to assign each free variable a type and a binding place. Types and contexts are defined in the following way:

```
data Con : Set where  
  ε      : Con  
  _ , _ : Con → Ty → Con
```

```
data Ty : Set where  
  C      : ℕ → Ty  
  _ ⇒ _ : Ty → Ty → Ty
```

Because variables are nameless in the de Bruijn representation, each item in the type context **Con** represents a consecutive binding site for free variables and the type that is associated with it. Variable indices are defined as indices into this surrounding context.

```
data _⊃_ : Con → Ty → Set where  
  vz : ∀ {Γ σ} → Γ , σ ⊃ σ  
  vs : ∀ {τ Γ σ} → Γ ⊃ σ → Γ , τ ⊃ σ
```

Using these constructions we can construct a representation for the simply typed lambda calculus.

```

data _+_ (Γ : Con) : Ty → Set where
  var : ∀ {σ} → Γ ∋ σ → Γ ⊢ σ
  Λ    : ∀ {σ τ} → Γ , σ ⊢ τ → Γ ⊢ σ ⇒ τ
  _·_  : ∀ {σ τ} → Γ ⊢ σ ⇒ τ → Γ ⊢ σ → Γ ⊢ τ

```

Terms are indexed by a context representing the free variables it may contain, along with the resulting type of the term itself. A variable is represented by an index into the context and produces a term with the type of that variable. A lambda binding binds a free variable by removing it from the context and introducing a function space. Function application combines a function and argument into a term of the result type.

This method of representing STLC terms has two very important benefits:

- The terms are well-typed *by construction*. In other words, it is impossible to construct an ill-typed stlc term using this data type.
- The terms are well-scoped *by construction*. Free variables are explicitly represented in the typing context. A term with an empty context is guaranteed to contain no free variables.

Note also that we do not specify a semantic interpretation for the simply typed lambda calculus and no typing language is specified. This is done intentionally to show that the correctness of  $TTS_\lambda$  is independent of the semantics of the simply typed lambda calculus and independent of the typing language. The only restriction on the semantics is that it allows  $\beta\eta$ -convertibility as defined in section 4.1.2.

#### 4.1.1 Manipulating and constructing terms

The simply typed lambda calculus comes equipped with a set of functions to construct, and, most importantly, evaluate terms.

**Context weakening** When constructing STLC terms the need arises to introduce fresh variables. Creating room in a typing context for a variable is simple, but the typing context of a term can not be changed at will. A function is needed which changes a term to accept an extra free variable in the context.

Extending a typing context is done with help of the converse function, removal of a variable from the context:

```

_·_ : {σ : Ty} → (Γ : Con) → Γ ∋ σ → Con
  ∈  - ()
  Γ , σ · vz = Γ
  Γ , τ · vs x = (Γ · x) , τ

```

Using this function it is possible to express how a term *without* a certain variable, can be turned into a term *with* that variable. This is done by the following two functions:

$\mathbf{wkv} : \forall \{\Gamma \sigma \tau\} \rightarrow (x : \Gamma \ni \sigma) \rightarrow \Gamma - x \ni \tau \rightarrow \Gamma \ni \tau$   
 $\mathbf{wkv} \, \mathbf{vz} \, y = \mathbf{vs} \, y$   
 $\mathbf{wkv} \, (\mathbf{vs} \, x) \, \mathbf{vz} = \mathbf{vz}$   
 $\mathbf{wkv} \, (\mathbf{vs} \, x) \, (\mathbf{vs} \, y) = \mathbf{vs} \, (\mathbf{wkv} \, x \, y)$

$\mathbf{wkTm} : \forall \{\sigma \Gamma \tau\} \rightarrow (x : \Gamma \ni \sigma) \rightarrow \Gamma - x \vdash \tau \rightarrow \Gamma \vdash \tau$   
 $\mathbf{wkTm} \, x \, (\mathbf{var} \, v) = \mathbf{var} \, (\mathbf{wkv} \, x \, v)$   
 $\mathbf{wkTm} \, x \, (\Lambda \, t) = \Lambda \, (\mathbf{wkTm} \, (\mathbf{vs} \, x) \, t)$   
 $\mathbf{wkTm} \, x \, (t_1 \cdot t_2) = \mathbf{wkTm} \, x \, t_1 \cdot \mathbf{wkTm} \, x \, t_2$   
 $\mathbf{weaken} : \forall \{\sigma \Gamma \tau\} \rightarrow \Gamma \vdash \tau \rightarrow \Gamma, \sigma \vdash \tau$   
 $\mathbf{weaken} \, t = \mathbf{wkTm} \, \mathbf{vz} \, t$

This formulation gives the flexibility to introduce a free variable at any position in the context.

**Simultaneous substitution** Reductions in the simply typed lambda calculus are based upon substitution. A variant of substitutions that goes very well with the well-typed de Bruijn formulation of the lambda calculus are simultaneous substitutions. Simultaneous substitution is an operation in which all free variables in a term are substituted, at once, with terms belonging to an entirely new context. Such a substitution is defined as follows:

$\mathbf{data} \, \_ \Rightarrow \_ : \mathbf{Con} \rightarrow \mathbf{Con} \rightarrow \mathbf{Set} \, \mathbf{where}$   
 $\mathbf{sz} : \forall \{\Delta\} \rightarrow \epsilon \Rightarrow \Delta$   
 $\mathbf{ss} : \forall \{\Gamma \Delta \tau\} \rightarrow \Gamma \Rightarrow \Delta \rightarrow \Delta \vdash \tau \rightarrow \Gamma, \tau \Rightarrow \Delta$

The substitution type is indexed by two typing contexts. The first type context represents the free variables that will be replaced and the second type context represents the new typing context after substitution. This new typing context is the typing context for all substituted terms.

Before defining the function which will perform the actual substitution on terms, it is necessary to extend to concept of term weakening (opening up a free variable) to simultaneous substitutions. This is done by the following functions:

$\mathbf{wkS} : \forall \{\tau \Gamma \Delta\} \rightarrow (x : \Delta \ni \tau) \rightarrow \Gamma \Rightarrow \Delta - x \rightarrow \Gamma \Rightarrow \Delta$   
 $\mathbf{wkS} \, \mathbf{v} \, \mathbf{sz} = \mathbf{sz}$   
 $\mathbf{wkS} \, \mathbf{v} \, (\mathbf{ss} \, y \, y') = \mathbf{ss} \, (\mathbf{wkS} \, \mathbf{v} \, y) \, (\mathbf{wkTm} \, \mathbf{v} \, y')$   
 $\mathbf{extS} : \forall \{\tau \Gamma \Delta\} \rightarrow (x : \Gamma \ni \tau) \rightarrow (t : \Delta \vdash \tau) \rightarrow \Gamma - x \Rightarrow \Delta \rightarrow \Gamma \Rightarrow \Delta$   
 $\mathbf{extS} \, \mathbf{vz} \, t \, s = \mathbf{ss} \, s \, t$   
 $\mathbf{extS} \, (\mathbf{vs} \, y) \, t \, (\mathbf{ss} \, y' \, y0) = \mathbf{ss} \, (\mathbf{extS} \, y \, t \, y') \, y0$   
 $\mathbf{wkExtS} : \{\Gamma \Delta : \mathbf{Con}\} \{\tau : \mathbf{Ty}\} \rightarrow (x : \Gamma \ni \tau) \rightarrow (y : \Delta \ni \tau) \rightarrow \Gamma - x \Rightarrow \Delta - y \rightarrow \Gamma \Rightarrow \Delta$   
 $\mathbf{wkExtS} \, x \, y \, \mathbf{v} = \mathbf{extS} \, x \, (\mathbf{var} \, y) \, (\mathbf{wkS} \, y \, \mathbf{v})$

The  $\mathbf{wkS}$  function weakens the result context of a substitution, the  $\mathbf{extS}$  function extends a substitution such that it replaces an extra free variable with a term.  $\mathbf{wkExtS}$  is defined for

convenience to create a 'gap' in a substitution. This function adds a new free variable to a substitution which will be replaced by another newly created variable.

The substitution function  $\_/\_$  can now be defined in the following way, with use of helper function **lookup**. **lookup** retrieves the term at some variable index from a substitution.

$$\begin{aligned} \mathbf{lookup} &: \forall \{\Gamma \Delta \tau\} \rightarrow (\mathbf{v} : \Gamma \ni \tau) \rightarrow \Gamma \Rightarrow \Delta \rightarrow \Delta \vdash \tau \\ \mathbf{lookup} \mathbf{vz} (\mathbf{ss} \ y \ y') &= y' \\ \mathbf{lookup} (\mathbf{vs} \ y) (\mathbf{ss} \ y' \ y0) &= \mathbf{lookup} \ y \ y' \\ \_/\_ &: \forall \{\Gamma \Delta \tau\} \rightarrow \Gamma \vdash \tau \rightarrow \Gamma \Rightarrow \Delta \rightarrow \Delta \vdash \tau \\ \_/\_ (\mathbf{var} \ y) \ s &= \mathbf{lookup} \ y \ s \\ \_/\_ (\Lambda \ y) \ s &= \Lambda (y \ / \ \mathbf{wkExtS} \ \mathbf{vz} \ \mathbf{vz} \ s) \\ \_/\_ (y \cdot y') \ s &= (y \ / \ s) \cdot (y' \ / \ s) \end{aligned}$$

Using **lookup** the variable case becomes simple to implement. The interesting case is applying substitutions over lambda abstractions. Lambda abstraction binds a variable from the free variable context of its subterm. In order to be able to apply the given substitution to this subterm, we extend the given substitution with an identity substitution for the newly bound variable. The lambda bound variable will be replaced by itself. This is the desired working of capture-avoiding substitution: shadowed variables will not be changed.

Simultaneous substitutions can not only be applied to terms, but can be applied to other simultaneous substitutions as well. This is shown by the following function.

$$\begin{aligned} \_/\Rightarrow\_ &: \forall \{\Gamma \Delta \Delta'\} \rightarrow \Gamma \Rightarrow \Delta \rightarrow \Delta \Rightarrow \Delta' \rightarrow \Gamma \Rightarrow \Delta' \\ \mathbf{sz} \_/\Rightarrow \mathbf{s}' &= \mathbf{sz} \\ \mathbf{ss} \ y \ y' /\Rightarrow \mathbf{s}' &= \mathbf{ss} (y \ /\Rightarrow \mathbf{s}') (y' \ / \ \mathbf{s}') \end{aligned}$$

**Single substitution** Single substitution can be implemented using simultaneous substitution. Single substitution is needed in order to be able to implement  $\beta$ -reduction. A single substitution is created by extending the identity substitution with a term for one variable.

$$\begin{aligned} \mathbf{I} &: \forall \{\Gamma\} \rightarrow \Gamma \Rightarrow \Gamma \\ \mathbf{I} \{\epsilon\} &= \mathbf{sz} \\ \mathbf{I} \{y, y'\} &= \mathbf{wkExtS} \ \mathbf{vz} \ \mathbf{vz} \ (\mathbf{I} \{y\}) \\ \mathbf{sub} &: \forall \{\Gamma \tau\} \rightarrow (\mathbf{v} : \Gamma \ni \tau) \rightarrow (\mathbf{x} : \Gamma - \mathbf{v} \vdash \tau) \rightarrow \Gamma \Rightarrow \Gamma - \mathbf{v} \\ \mathbf{sub} \ \mathbf{v} \ \mathbf{x} &= \mathbf{extS} \ \mathbf{v} \ \mathbf{x} \ \mathbf{I} \end{aligned}$$

The function **up** shows how a simultaneous substitution can be used to lift a closed term into an arbitrary context.

$$\begin{aligned} \mathbf{up} &: \forall \{\Gamma \tau\} \rightarrow \epsilon \vdash \tau \rightarrow \Gamma \vdash \tau \\ \mathbf{up} \ t &= t \ / \ \mathbf{sz} \end{aligned}$$

**Term closure** The semantic equivalence property of  $TTS_\lambda$  is defined on terms 'under a closing environment'. Thus the object language is equipped with a closure construction, defined as follows:

**data**  $\_ \downarrow : (\Gamma : \mathbf{Con}) \rightarrow \mathbf{Set}$  **where**  
 $\epsilon \downarrow : \epsilon \downarrow$   
 $\mathbf{cls} : \forall \{\tau \Gamma\} \rightarrow \Gamma \downarrow \rightarrow \Gamma \vdash \tau \rightarrow \Gamma, \tau \downarrow$

Such a closure carries a closing term for each variable in the environment. These terms should be substituted into a term *sequentially* to close the term. Such a closing operation can not be defined directly but a closure can be turned into an equivalent simultaneous substitution using the following function:

$\downarrow \dashv \Rightarrow : \forall \{\Gamma\} \rightarrow \Gamma \downarrow \rightarrow \Gamma \Rightarrow \epsilon$   
 $\downarrow \dashv \Rightarrow \epsilon = \mathbf{sz}$   
 $\downarrow \dashv \Rightarrow (\mathbf{cls} \ y \ y') = \mathbf{ss} (\downarrow \dashv \Rightarrow y) (y' / \downarrow \dashv \Rightarrow y)$

Defining a term closing function is now simple:

**close** :  $\forall \{\Gamma \tau\} \rightarrow \Gamma \vdash \tau \rightarrow \Gamma \downarrow \rightarrow \epsilon \vdash \tau$   
 $\mathbf{close} \ t \ s = t / \downarrow \dashv \Rightarrow s$

**Variable construction** Variable indices are constructed in the sequential way of Peano numberings. While this simple representation is useful for defining functions and reasoning with indices, it is not very convenient to write variables as sequences of constructors when constructing terms. The helper function **i** makes this process a bit simpler by injecting a natural number into a stlc variable in the free value context.

**size** :  $\mathbf{Con} \rightarrow \mathbb{N}$   
 $\mathbf{size} \ \epsilon = \mathbf{zero}$   
 $\mathbf{size} \ (y, y') = \mathbf{suc} \ (\mathbf{size} \ y)$   
**ind** :  $(\Gamma : \mathbf{Con}) \rightarrow \mathbf{Fin} \ (\mathbf{size} \ \Gamma) \rightarrow \mathbf{Ty}$   
 $\mathbf{ind} \ \epsilon ()$   
 $\mathbf{ind} \ (y, y') \ \mathbf{zero} = y'$   
 $\mathbf{ind} \ (y, y') \ (\mathbf{suc} \ i) = \mathbf{ind} \ y \ i$   
**i** :  $\forall \{\Gamma\} \rightarrow (i : \mathbf{Fin} \ (\mathbf{size} \ \Gamma)) \rightarrow \Gamma \ni \mathbf{ind} \ \Gamma \ i$   
 $\mathbf{i} \ \{\epsilon\} ()$   
 $\mathbf{i} \ \{y, y'\} \ \mathbf{zero} = \mathbf{vz}$   
 $\mathbf{i} \ \{y, y'\} \ (\mathbf{suc} \ i) = \mathbf{vs} \ (\mathbf{i} \ i)$   
 $\mathbf{i} : \forall m \{\Gamma\} \{m < n : \mathbf{True} \ (\mathbf{suc} \ m \leq \mathbf{size} \ \Gamma)\} \rightarrow \Gamma \ni \mathbf{ind} \ \Gamma \ (\#\_m \ \{\mathbf{size} \ \Gamma\} \{m < n\})$   
 $\mathbf{i} \ v = \mathbf{i} \ (\# \ v)$

This only works as long as the natural number is within the bounds of the context. This is checked by an inferred predicate in the function **i**. If this predicate holds, a bounded (finite) number can be constructed using **#**, which can then be turned into a variable index using **i**.

Term construction is facilitated by the function `v`. Variables can now be written as normal numbers:

```
v : (m : ℕ) → {Γ : Con} → {m < n : True (suc m ≤? size Γ)}
    → Γ ⊢ ind Γ (#_ m {size Γ} {m < n})
v x = var (i x)
```

Combined with Agda's mix-fix syntax, this yields a relatively clutter-free method of constructing stlc terms:

```
id : ∀ {a Γ} → Γ ⊢ a ⇒ a
id = Λ (v 0)

const : ∀ {a b Γ} → Γ ⊢ a ⇒ b ⇒ a
const = Λ (Λ (v 1))

comp : ∀ {Γ a b c} → Γ ⊢ (b ⇒ c) ⇒ (a ⇒ b) ⇒ a ⇒ c
comp = Λ (Λ (Λ (v 2 · (v 1 · v 0))))

infixl 2 _◦_
_◦_ : ∀ {a b c Γ} → Γ ⊢ b ⇒ c → Γ ⊢ a ⇒ b → Γ ⊢ a ⇒ c
t1 ◦ t2 = comp · t1 · t2
```

#### 4.1.2 Equality

The semantics of stlc terms can be related using a convertibility relation. The  $\beta\eta$ -convertibility relation used here is based on work by Keller and Altenkirch [KA10].

```
data _βη≡_ {Γ : Con} : {σ : Ty} → Γ ⊢ σ → Γ ⊢ σ → Set where
  □      : ∀ {σ} → {t : Γ ⊢ σ} → t βη≡ t
  bsym   : ∀ {σ} → {t₁ t₂ : Γ ⊢ σ} → t₁ βη≡ t₂ → t₂ βη≡ t₁
  _↔_    : ∀ {σ} → {t₁ t₂ t₃ : Γ ⊢ σ} → t₁ βη≡ t₂ → t₂ βη≡ t₃ → t₁ βη≡ t₃
  %Λ_    : ∀ {σ τ} → {t₁ t₂ : Γ , σ ⊢ τ} → t₁ βη≡ t₂ → Λ t₁ βη≡ Λ t₂
  _%·_   : ∀ {σ τ} → {t₁ t₂ : Γ ⊢ σ ⇒ τ} → {u₁ u₂ : Γ ⊢ σ}
    → t₁ βη≡ t₂ → u₁ βη≡ u₂ → t₁ · u₁ βη≡ t₂ · u₂
  β      : ∀ {σ τ} → {t : Γ , σ ⊢ τ} → {u : Γ ⊢ σ} → Λ t · u βη≡ t / sub v z u
  η      : ∀ {σ τ} → {t : Γ ⊢ σ ⇒ τ} → Λ (weaken t · v 0) βη≡ t
```

The first three constructors establish reflexivity, symmetry and transitivity of  $\beta\eta$ -equality. `%Λ_` and `_%·_` establishes that convertibility is a congruence relation.  $\beta$  and  $\eta$  represent the respective beta-reduction and eta-expansion rules. Note that because of the use of well-typed de-Brujin indices, the subject reduction property of the lambda calculus comes for free.  $\beta$ -reduction is guaranteed to preserve typing.

Because the  $\beta\eta$ -convertibility relation is reflexive, symmetric and transitive, it gives rise to a setoid. In Agda this makes the relation eligible for use with the equational reasoning module, which makes proving properties much more intuitive. As an example, the `ext` property shows that this formalization of the lambda calculus supports the extensionality lemma.



```

βηsetoid : {Γ : Con} {σ : Ty} → Setoid _ _
βηsetoid {Γ} {σ} =
  record { Carrier = Γ ⊢ σ
        ; _≈_ = _βη≡_
        ; isEquivalence =
            record { refl = □
                  ; sym = bsym
                  ; trans = _↔_
                  }
        }

ext : ∀ {Γ σ τ} → (e e' : Γ ⊢ σ ⇒ τ) → weaken e · v 0 βη≡ weaken e' · v 0
      → e βη≡ e'
ext e e' eq =
  let open Relation.Binary.EqReasoning βηsetoid
  renaming ( _≈⟨_⟩_ to _↔⟨_⟩_ )
  in begin
    e
    ↔⟨ bsym η ⟩
    Λ (weaken e · v 0)
    ↔⟨ %Λ eq ⟩
    Λ (weaken e' · v 0)
    ↔⟨ η ⟩
    e'
    ■

```

## 4.2 Formalization of $TTS_\lambda$

**Typing Functor** With the object language layed out, it is now possible to formalize the basic constructs of  $TTS_\lambda$ . Essential to the type and transform system is the typing functor. The typing functor is defined as a straightforward inductive datatype as follows:

```

data Functor : Set where
  ι      : Functor
  C      : (ℳ : ℕ) → Functor
  _→_    : (τ1 τ2 : Functor) → Functor

```

As expected, the functor datatype is the same as the stlc base type, with an extra constructor  $\iota$  representing a hole in the type. Two functions establish the relation between functor types and normal types: The interpretation function  $\llbracket \_ \rrbracket^{\circ}$  and the lifting function  $\_ \uparrow^{\circ}$ .

```

llbracket \_ \rrbracket^{\circ} : Functor → Ty → Ty
llbracket ι \rrbracket^{\circ} τ = τ

```

$$\begin{aligned}
& \llbracket \mathbf{C} \, n \rrbracket^{\circ} \tau = \mathbf{C} \, n \\
& \llbracket \tau_1 \longrightarrow \tau_2 \rrbracket^{\circ} \tau = \llbracket \tau_1 \rrbracket^{\circ} \tau \Rightarrow \llbracket \tau_2 \rrbracket^{\circ} \tau \\
& \_ \uparrow^{\circ} : \mathbf{Ty} \rightarrow \mathbf{Functor} \\
& \mathbf{C} \, n \uparrow^{\circ} = \mathbf{C} \, n \\
& \tau_1 \Rightarrow \tau_2 \uparrow^{\circ} = \tau_1 \uparrow^{\circ} \longrightarrow \tau_2 \uparrow^{\circ}
\end{aligned}$$

In the Agda world, the functor datatype can be seen as a universe, with  $\llbracket \_ \rrbracket^{\circ}$  as universe interpretation onto the base types.

**Functor Context** A functor context is basically the same as a normal context, only containing functors. The accompanying interpretation and lifting functions are equally straightforward.

```

data Ftx : Set where
   $\epsilon$       : Ftx
   $\_ , \_$  : ( $\dot{\Gamma}$  : Ftx)  $\rightarrow$  ( $\dot{\tau}$  : Functor)  $\rightarrow$  Ftx

 $\llbracket \_ \rrbracket^{\dot{\Gamma}} : \mathbf{Ftx} \rightarrow \mathbf{Ty} \rightarrow \mathbf{Con}$ 
 $\llbracket \epsilon \rrbracket^{\dot{\Gamma}} n = \epsilon$ 
 $\llbracket \dot{\Gamma} , \dot{\tau} \rrbracket^{\dot{\Gamma}} n = \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} n , \llbracket \dot{\tau} \rrbracket^{\dot{\Gamma}} n$ 

 $\_ \uparrow^{\dot{\Gamma}} : \mathbf{Con} \rightarrow \mathbf{Ftx}$ 
 $\epsilon \uparrow^{\dot{\Gamma}} = \epsilon$ 
 $y , y' \uparrow^{\dot{\Gamma}} = (y \uparrow^{\dot{\Gamma}}) , y' \uparrow^{\dot{\Gamma}}$ 

```

Also the concept of variables extends naturally to functors, with the accompanying interpretation function.

```

data  $\_ \ni^{\dot{\Gamma}} \_ : \mathbf{Ftx} \rightarrow \mathbf{Functor} \rightarrow \mathbf{Set}$  where
  vz :  $\forall \{ \dot{\Gamma} \dot{\tau} \} \rightarrow \dot{\Gamma} , \dot{\tau} \ni^{\dot{\Gamma}} \dot{\tau}$ 
  vs :  $\forall \{ \dot{\Gamma} \dot{\tau}_1 \dot{\tau}_2 \} \rightarrow \dot{\Gamma} \ni^{\dot{\Gamma}} \dot{\tau}_1 \rightarrow \dot{\Gamma} , \dot{\tau}_2 \ni^{\dot{\Gamma}} \dot{\tau}_1$ 

 $\llbracket \_ \rrbracket^{\ni} : \forall \{ \dot{\Gamma} \dot{\tau} \} \rightarrow (\mathbf{v} : \dot{\Gamma} \ni^{\dot{\Gamma}} \dot{\tau}) \rightarrow (\mathbf{a} : \mathbf{Ty}) \rightarrow \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} \mathbf{a} \ni \llbracket \dot{\tau} \rrbracket^{\dot{\Gamma}} \mathbf{a}$ 
 $\llbracket \mathbf{vz} \rrbracket^{\ni} \mathbf{t} = \mathbf{vz}$ 
 $\llbracket \mathbf{vs} \, y \rrbracket^{\ni} \mathbf{t} = \mathbf{vs} (\llbracket y \rrbracket^{\ni} \mathbf{t})$ 

```

$TTS_{\lambda}$  is intended to be a base system for type-changing transformations, independent of which types and terms are changed. In other words,  $TTS_{\lambda}$  should be parametrizable with different types and rewriting rules. In Agda this can be expressed using parametrized modules. The base system is parametrized by the source and result type  $\mathfrak{U}$  and  $\mathfrak{R}$ , together with the **abs** and **rep** functions to convert between them. Additionally a set of rules is expected which perform the actual transformations.

```

module TTS.Judgement.Base
  ( $\mathfrak{U} : \mathbb{N}$ ) ( $\mathfrak{R} : \mathbf{Ty}$ )
  (rep :  $\epsilon \vdash \mathbf{C} \, \mathfrak{U} \Rightarrow \mathfrak{R}$ ) (abs :  $\epsilon \vdash \mathfrak{R} \Rightarrow \mathbf{C} \, \mathfrak{U}$ )

```

(rules : Rules  $\mathcal{A} \mathcal{R}$ )  
 where

The inductive family representing  $TTS_{\lambda}$  now looks as follows:

```

infix 1 _:_ $\vdash$ _~_
data _:_ $\vdash$ _~_ : ( $\dot{\Gamma}$  : Ftx)  $\rightarrow$  ( $\dot{\tau}$  : Functor)  $\rightarrow$  (e :  $\llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} \mathcal{C} \mathcal{A} \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} \mathcal{C} \mathcal{A}$ )
   $\rightarrow$  (e' :  $\llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} \mathcal{R} \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} \mathcal{R}$ )  $\rightarrow$  Set where
  var :  $\forall \{ \dot{\Gamma} \dot{\tau} \} (v : \dot{\Gamma} \ni \dot{\Gamma} \dot{\tau})$ 
     $\rightarrow \dot{\Gamma} : \dot{\tau} \vdash \mathbf{var} (\llbracket v \rrbracket \ni \mathcal{C} \mathcal{A}) \sim \mathbf{var} (\llbracket v \rrbracket \ni \mathcal{R})$ 
  app :  $\forall \{ \dot{\Gamma} \dot{\tau}_1 \dot{\tau}_2 e_1 e_1' e_2 e_2' \}$ 
     $\rightarrow \dot{\Gamma} : \dot{\tau}_1 \longrightarrow \dot{\tau}_2 \vdash e_1 \sim e_1' \rightarrow \dot{\Gamma} : \dot{\tau}_1 \vdash e_2 \sim e_2'$ 
     $\rightarrow \dot{\Gamma} : \dot{\tau}_2 \vdash e_1 \cdot e_2 \sim e_1' \cdot e_2'$ 
  lam :  $\forall \{ \dot{\Gamma} \dot{\tau}_1 \dot{\tau}_2 e e' \} \rightarrow \dot{\Gamma}, \dot{\tau}_1 : \dot{\tau}_2 \vdash e \sim e' \rightarrow \dot{\Gamma} : \dot{\tau}_1 \longrightarrow \dot{\tau}_2 \vdash \Lambda e \sim \Lambda e'$ 
  i-rep :  $\forall \{ \dot{\Gamma} e e' \} \rightarrow \dot{\Gamma} : \mathcal{C} \mathcal{A} \vdash e \sim e' \rightarrow \dot{\Gamma} : \iota \vdash e \sim \mathbf{up\ rep} \cdot e'$ 
  i-abs :  $\forall \{ \dot{\Gamma} e e' \} \rightarrow \dot{\Gamma} : \iota \vdash e \sim e' \rightarrow \dot{\Gamma} : \mathcal{C} \mathcal{A} \vdash e \sim \mathbf{up\ abs} \cdot e'$ 
  rule :  $\forall \{ \dot{\Gamma} \dot{\tau} e e' \} \rightarrow \mathbf{Rule} \{ \dot{\tau} \} e e' \mathbf{rules} \rightarrow \dot{\Gamma} : \dot{\tau} \vdash \mathbf{up} e \sim \mathbf{up} e'$ 

```

The inductive family closely follows the specification from chapter 2. In the judgement the functor is moved in front of the converted terms, because scoping in Agda is from left to right.

This definition shows clearly how two terms are typed by one typing functor and functor context. The **var**, **app** and **lam** rules just propagate these type changes using the rules of the simply typed lambda calculus. The **i-rep**, **i-abs** and **rule** construction actually have the power to change the types and terms.

**Transformation rules** There is a bit of room in the design space as to how represent transformation rules. In this version of the type and transform system a simple dictionary of transformable terms is used. Chapter 5 discusses more possibilities for extension.

```

data Rules ( $\mathcal{A} : \mathbb{N}$ ) ( $\mathcal{R} : \mathbf{Ty}$ ) : Set where
   $\epsilon$  : Rules  $\mathcal{A} \mathcal{R}$ 
  replace :  $\forall \{ \dot{\tau} \} \rightarrow (r : \mathbf{Rules} \mathcal{A} \mathcal{R}) \rightarrow (e : \epsilon \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} \mathcal{C} \mathcal{A})$ 
     $\rightarrow (e' : \epsilon \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} \mathcal{R}) \rightarrow \mathbf{Rules} \mathcal{A} \mathcal{R}$ 
data Rule  $\{ \dot{\tau} \mathcal{A} \mathcal{R} \} (e : \epsilon \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} \mathcal{C} \mathcal{A}) (e' : \epsilon \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} \mathcal{R}) : \mathbf{Rules} \mathcal{A} \mathcal{R} \rightarrow \mathbf{Set} \mathbf{where}
  rule :  $\forall rs \rightarrow \mathbf{Rule} e e' (\mathbf{replace} \{ \mathcal{A} \} \{ \mathcal{R} \} \{ \dot{\tau} \} rs e e')$ 
  skip :  $\forall \{ rs \dot{\tau}' f f' \} \rightarrow (r : \mathbf{Rule} \{ \dot{\tau} \} e e' rs)$ 
     $\rightarrow \mathbf{Rule} e e' (\mathbf{replace} \{ \mathcal{A} \} \{ \mathcal{R} \} \{ \dot{\tau}' \} rs f f')$$ 
```

The **Rules** datatype is list of transformation terms. A **Rule** indexes a rule in this list. Note that only closed terms can be transformed using this formulation, this makes the transformations context-insensitive.

## 4.3 Properties

We will now mechanically show that the defined system adheres to the desired transformation properties of Section 2.2. This proof follows the same structure as the 'pen-and-paper' proof from Chapter 3 and relies on the Curry-Howard correspondence for its validity.

**Curry-Howard Correspondence** The Curry Howard correspondence is the notion that there exists a direct connection between types in a programming language and propositions in classical, predicate and intuitionistic logic. This correspondence makes it possible to construct proofs as programs: providing an implementation program for a given type corresponds to proving that same logical property. According to the Curry-Howard correspondence, implication in logic has a direct relation to function space in programming languages, and universal quantification is related to dependent function space. Sum types and product types have a direct relation to disjunction and conjunction. In this way the Curry-Howard correspondence makes it possible to mechanically prove logical properties in a programming language, a feature that is put to good use in this section.

### 4.3.1 Typing property

The TTS typing property does not need any further proving but is inherent in the construction of the whole system. Terms are type-correct by construction using the well-typed De Bruijn indices and the transformation relation is indexed by two terms which derive a valid type from the typing functor.

### 4.3.2 Identity transformation

As a bare minimum, all transformation systems should allow the identity transformation to be productive. The following function shows this by showing that a valid transformation derivation exists for any term in the simply typed lambda calculus:

$$\begin{aligned} \text{id} \rightsquigarrow &: \forall \{ \Gamma \tau \} \rightarrow (e : \Gamma \vdash \tau) \\ &\rightarrow \Gamma \uparrow \overset{\circ}{\Gamma} : \tau \uparrow \overset{\circ}{\tau} \models ! \uparrow \overset{\circ}{\Gamma} \equiv \Gamma, \uparrow \overset{\circ}{\tau} \equiv \tau \triangleright e \rightsquigarrow ! \uparrow \overset{\circ}{\Gamma} \equiv \Gamma, \uparrow \overset{\circ}{\tau} \equiv \tau \triangleright e \end{aligned}$$

The typing functor and functor context of the identity transformation are the lifted version of the base type and context. The function  $! \uparrow \overset{\circ}{\Gamma} \equiv \Gamma, \uparrow \overset{\circ}{\tau} \equiv \tau \triangleright e$  shows Agda that the interpretation of a lifted type, is equal to the base type.

This shows clearly how implication in logic is connected to function space in a programming language. The statement: the existence of a valid term implies the existence of a transformation for that term, is transformed into showing that a function exists which constructs a transformation out of a term.

### 4.3.3 Semantic equivalence

The Agda formalization of the equivalence proof strictly follows the proof structure as described in Chapter 3. The first challenge is to find a suitable Agda representation for the logical relation.

**Logical relation** To construct the logical relation we can make good use of dependent types: the relation constructs a different type for different Functor constructs. For base types it constructs a  $\beta\eta$  equivalence and for function space it constructs an implication in the form of a normal Agda function.

```

module TTS.Relation.Base (A : ℕ) (R : Ty) (rep :  $\epsilon \vdash C A \Rightarrow R$ ) where
rel :  $\forall \{ \dot{\Gamma} \dot{\tau} \} \rightarrow (e : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} C A \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} C A) \rightarrow (e' : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} R \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} R)$ 
   $\rightarrow (s : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} C A \downarrow) \rightarrow (s' : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} R \downarrow) \rightarrow \mathbf{Set}$ 
rel { $\dot{\Gamma}$ } { $\iota$ }      e e' s s' = up rep · close e s  $\beta\eta$ -≡ close e' s'
rel { $\dot{\Gamma}$ } {C n}     e e' s s' = close e s  $\beta\eta$ -≡ close e' s'
rel { $\dot{\Gamma}$ } { $\dot{\tau}_1 \rightarrow \dot{\tau}_2$ } e e' s s' =  $\forall a a' \rightarrow$  rel { $\dot{\Gamma}$ } { $\dot{\tau}_1$ } a a' s s'
   $\rightarrow$  rel { $\dot{\Gamma}$ } { $\dot{\tau}_2$ } (e · a) (e' · a') s s'
```

Before proving the fundamental Lemma we first establish the  $\beta\eta$ -closure and crossing lemma's over the logical relation. Because the type of the logical relation is dependent on the functor, there is no choice but to prove properties about by the logical relation by induction on the Typing functor.

```

rel- $\beta\eta$  :  $\forall \{ \dot{\Gamma} \dot{\tau} \} \{ e e' : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} C A \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} C A \} \{ f f' : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} R \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} R \}$ 
   $\rightarrow (s : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} C A \downarrow) \rightarrow (s' : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} R \downarrow) \rightarrow e \beta\eta$ -≡  $e' \rightarrow f \beta\eta$ -≡  $f'$ 
   $\rightarrow$  rel { $\dot{\Gamma}$ } { $\dot{\tau}$ } e f s s'  $\rightarrow$  rel { $\dot{\Gamma}$ } { $\dot{\tau}$ } e' f' s s'
rel- $\beta\eta$  { $\dot{\Gamma}$ } { $\iota$ }      s s' eq1 eq2 r = ( $\square$  %· %close s (bsym eq1))
   $\leftrightarrow$  r
   $\leftrightarrow$  %close s' eq2
rel- $\beta\eta$  { $\dot{\Gamma}$ } {C n}     s s' eq1 eq2 r = %close s (bsym eq1)
   $\leftrightarrow$  r
   $\leftrightarrow$  %close s' eq2
rel- $\beta\eta$  { $\dot{\Gamma}$ } { $\dot{\tau}_1 \rightarrow \dot{\tau}_2$ } s s' eq1 eq2 r =
   $\lambda a a' \text{ra} \rightarrow$  rel- $\beta\eta$  { $\dot{\Gamma}$ } { $\dot{\tau}_2$ } s s' (eq1 %·  $\square$ ) (eq2 %·  $\square$ ) (r a a' ra)
```

The  $\beta\eta$  closure is another good example of the Curry-Howard correspondence in action. In the proof of Chapter 3 we used sequences of implication to show the case for function space. In the Curry-Howard correspondence implication elimination becomes function application.

For the crossing Lemma's we just show the types, which give an exact formal representation of the lemma. The logical equivalence of the crossing lemma is proving by mutual induction on the two directions the implication, in Agda we can model this by using a mutual block. Agda's termination checker will tell whether we have cyclic reasoning or not: if the construction of the proof term terminates, we have no cyclic reasoning, if it is proven using infinite recursion the reasoning was cyclic.

**mutual**

```

cross-left :  $\forall \{ \dot{\Gamma} \dot{\tau} \dot{\tau}' \} \rightarrow (e : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} C A, \llbracket \dot{\tau}' \rrbracket^{\dot{\tau}'} C A \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} C A)$ 
   $\rightarrow (e' : \llbracket \dot{\Gamma} \rrbracket^{\dot{\Gamma}} R, \llbracket \dot{\tau}' \rrbracket^{\dot{\tau}'} R \vdash \llbracket \dot{\tau} \rrbracket^{\dot{\tau}} R)$ 
```

$$\begin{aligned}
& \rightarrow (s : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow) \rightarrow (s' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \Downarrow) \\
& \rightarrow (a : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} C \Downarrow) \rightarrow (a' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} \mathcal{R}) \\
& \rightarrow \mathbf{rel} \{ \overset{\circ}{\Gamma} \} \{ \overset{\circ}{\tau} \} (e / \mathbf{sub} \mathbf{vz} a) (e' / \mathbf{sub} \mathbf{vz} a') s s' \\
& \rightarrow \mathbf{rel} \{ \overset{\circ}{\Gamma}, \overset{\circ}{\tau}' \} \{ \overset{\circ}{\tau} \} e e' (\mathbf{cls} s a) (\mathbf{cls} s' a') \\
\mathbf{cross-right} : & \forall \{ \overset{\circ}{\Gamma} \overset{\circ}{\tau} \overset{\circ}{\tau}' \} \rightarrow (e : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow, \llbracket \overset{\circ}{\tau}' \rrbracket \overset{\circ}{\tau}' C \Downarrow \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} C \Downarrow) \\
& \rightarrow (e' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R}, \llbracket \overset{\circ}{\tau}' \rrbracket \overset{\circ}{\tau}' \mathcal{R} \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} \mathcal{R}) \\
& \rightarrow (s : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow) \rightarrow (s' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \Downarrow) \\
& \rightarrow (a : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow \vdash \llbracket \overset{\circ}{\tau}' \rrbracket \overset{\circ}{\tau}' C \Downarrow) \rightarrow (a' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \vdash \llbracket \overset{\circ}{\tau}' \rrbracket \overset{\circ}{\tau}' \mathcal{R}) \\
& \rightarrow \mathbf{rel} \{ \overset{\circ}{\Gamma}, \overset{\circ}{\tau}' \} \{ \overset{\circ}{\tau} \} e e' (\mathbf{cls} s a) (\mathbf{cls} s' a') \\
& \rightarrow \mathbf{rel} \{ \overset{\circ}{\Gamma} \} \{ \overset{\circ}{\tau} \} (e / \mathbf{sub} \mathbf{vz} a) (e' / \mathbf{sub} \mathbf{vz} a') s s' \\
\mathbf{rel-weak} : & \forall \{ \overset{\circ}{\Gamma} \overset{\circ}{\tau} \overset{\circ}{\tau}' \} \rightarrow (e : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} C \Downarrow) \\
& \rightarrow (e' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} \mathcal{R}) \\
& \rightarrow (s : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow) \rightarrow (s' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \Downarrow) \\
& \rightarrow (a : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow \vdash \llbracket \overset{\circ}{\tau}' \rrbracket \overset{\circ}{\tau}' C \Downarrow) \rightarrow (a' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \vdash \llbracket \overset{\circ}{\tau}' \rrbracket \overset{\circ}{\tau}' \mathcal{R}) \\
& \rightarrow \mathbf{rel} \{ \overset{\circ}{\Gamma} \} \{ \overset{\circ}{\tau} \} e e' s s' \\
& \rightarrow \mathbf{rel} \{ \overset{\circ}{\Gamma}, \overset{\circ}{\tau}' \} \{ \overset{\circ}{\tau} \} (\mathbf{wkTm} \mathbf{vz} e) (\mathbf{wkTm} \mathbf{vz} e') (\mathbf{cls} s a) (\mathbf{cls} s' a')
\end{aligned}$$

The entire proof for this lemma can be found in the sources.

**Relating environments** Semantic equivalence is proven 'under related closing environments'. The fact that two closing environments are related is expressed by the following inductive datatype.

$$\begin{aligned}
\mathbf{data} \mathbf{Rel} \downarrow : & (\overset{\circ}{\Gamma} : \mathbf{Ftx}) \rightarrow (\llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow) \rightarrow (\llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \Downarrow) \rightarrow \mathbf{Set} \mathbf{where} \\
\epsilon : & \mathbf{Rel} \downarrow \epsilon \epsilon \epsilon \\
\mathbf{cls} : & \forall \{ \overset{\circ}{\Gamma} \overset{\circ}{\tau} \} \{ e : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} C \Downarrow \} \{ e' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} \mathcal{R} \} \\
& \rightarrow \{ s : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} C \Downarrow \} \rightarrow \{ s' : \llbracket \overset{\circ}{\Gamma} \rrbracket \overset{\circ}{\Gamma} \mathcal{R} \Downarrow \} \rightarrow \mathbf{Rel} \downarrow \overset{\circ}{\Gamma} s s' \\
& \rightarrow (w : \mathbf{rel} \{ \overset{\circ}{\Gamma} \} \{ \overset{\circ}{\tau} \} e e' s s') \rightarrow \mathbf{Rel} \downarrow (\overset{\circ}{\Gamma}, \overset{\circ}{\tau}) (\mathbf{cls} s e) (\mathbf{cls} s' e')
\end{aligned}$$

$\mathbf{Rel} \downarrow$  is indexed by the closing environments it relates. For each two respective terms in the environment a witness  $w$  is evidence of the fact that both terms are related.

**Relating transformation rules** A type and transform transformation is only semantics preserving if the transformation rules preserve the equivalence between the types. This is done by showing that transformed terms are members of the logical relation, and is witnessed by the following construction:

$$\begin{aligned}
\mathbf{data} \mathbf{RuleProofs} : & \mathbf{Rules} \mathcal{A} \mathcal{R} \rightarrow \mathbf{Set} \mathbf{where} \\
\epsilon : & \mathbf{RuleProofs} \epsilon \\
\mathbf{proof} : & \forall \{ rs \overset{\circ}{\tau} \} \rightarrow \mathbf{RuleProofs} rs \rightarrow (e : \epsilon \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} C \Downarrow) \\
& \rightarrow (e' : \epsilon \vdash \llbracket \overset{\circ}{\tau} \rrbracket \overset{\circ}{\tau} \mathcal{R}) \rightarrow (r : \mathbf{rel} \{ \epsilon \} \{ \overset{\circ}{\tau} \} e e' \epsilon) \\
& \rightarrow \mathbf{RuleProofs} (\mathbf{replace} \{ \mathcal{A} \} \{ \mathcal{R} \} \{ \overset{\circ}{\tau} \} rs e e')
\end{aligned}$$

As said, a program transformation is only semantics preserving for types which form a retraction and when the transformation rules are related. This is expressed by proving within a parametrized module:

**module TransformationProof** (abs-rep : **abs**  $\circ$  **rep**  $\beta\eta \equiv \text{id}$ )  
(proofs : **RuleProofs** rules) **where**

Within this parametrized module we can now show the fundamental theorem and extraction theorem. The fundamental theorem shows that a type and transform system transformation is logically related under related environments.

**fundament** :  $\forall \{\dot{\Gamma} \dot{\tau} e e'\} \rightarrow (\mathbf{v} : \dot{\Gamma} : \dot{\tau} \models e \leadsto e') \rightarrow (\mathbf{s} : \llbracket \dot{\Gamma} \rrbracket \dot{\Gamma} \mathbf{C} \Downarrow)$   
 $\rightarrow (\mathbf{s}' : \llbracket \dot{\Gamma} \rrbracket \dot{\Gamma} \mathbf{R} \Downarrow) \rightarrow \mathbf{Rel} \downarrow \dot{\Gamma} \mathbf{s} \mathbf{s}' \rightarrow \mathbf{rel} \{\dot{\Gamma}\} \{\dot{\tau}\} e e' \mathbf{s} \mathbf{s}'$

To show the extraction theorem, we first need to show that a closing environment is related to itself. This follows from the fact that we can construct an identity transformation for each term. The fundamental theorem then shows that the transformation is related.

$\mathbf{rel} \Gamma : \forall \{\Gamma\} \rightarrow (\mathbf{s} : \Gamma \Downarrow) \rightarrow \mathbf{Rel} \downarrow (\Gamma \uparrow \dot{\Gamma}) (! \uparrow \dot{\Gamma} \equiv \Gamma > \downarrow \mathbf{s}) (! \uparrow \dot{\Gamma} \equiv \Gamma > \downarrow \mathbf{s})$   
 $\mathbf{rel} \Gamma \epsilon = \epsilon$   
 $\mathbf{rel} \Gamma (\mathbf{cls} \ y \ y') = \mathbf{cls} (\mathbf{rel} \Gamma \ y) (\mathbf{fundament} (\text{id} \leadsto y') \_ \_ (\mathbf{rel} \Gamma \ y))$

Using these two lemmas we can show the final extraction Lemma, showing that a complete transformation yields equivalent terms under any closing environment.

**extract** :  $\forall \{\Gamma \mathbf{n}\} \rightarrow (e e' : \Gamma \vdash \mathbf{C} \mathbf{n})$   
 $\rightarrow \Gamma \uparrow \dot{\Gamma} : \mathbf{C} \mathbf{n} \models ! \uparrow \dot{\Gamma} \equiv \Gamma, \equiv \tau \text{refl} > \vdash e \leadsto ! \uparrow \dot{\Gamma} \equiv \Gamma, \equiv \tau \text{refl} > \vdash e'$   
 $\rightarrow (\mathbf{s} : \Gamma \Downarrow) \rightarrow \mathbf{close} \ e \ \beta\eta \equiv \mathbf{close} \ e' \ \mathbf{s}$

The fact that the transformation is complete is enforce by the constant Functor  $\mathbf{C} \mathbf{n}$  and the fact that the functor context should be lifted from some normal context  $\Gamma$ . The  $! \uparrow \dot{\Gamma} \equiv \Gamma, \equiv \tau \text{refl} > \vdash$  term proves that the interpretation of a lifted term context is equal to the base context.

This mechanically proves that the type and transform system is semantics preserving.

## 4.4 Monoid Transformation

Because the object language used for mechanically proving  $TTS_\lambda$  is rather simple, it is not possible to express Hughes' strings transformation in this framework. However, it is possible to prove a more general transformation of which Hughes' strings is an instantiation: the monoid transformation.

A monoid is a mathematical structure consisting of a type  $\mathbf{S}$  and a binary operation  $\_ \bullet \_ :: \mathbf{S} \rightarrow \mathbf{S} \rightarrow \mathbf{S}$  and an identity  $\mathbf{zero} :: \mathbf{S}$ , which adhere to the following laws:

**Associativity**:  $\forall a \ b \ c. a \bullet (b \bullet c) \equiv_{\beta\eta} (a \bullet b) \bullet c$   
**Identity**:  $\forall a. a \bullet \mathbf{zero} \equiv_{\beta\eta} \mathbf{zero} \bullet a \equiv_{\beta\eta} a$

It is not difficult to see that  $(+)$  and  $""$  form a monoid for **Strings**. We can construct a transformation for monoids which will make sure that all applications of the monoid are *right-associative*, exactly what is being done in Hughes' string transformation.

The monoid transformation is parametrized by a monoidal structure: A type, the two operations and the accompanying laws. For this transformation we actually only need the right-identity of the  $\text{mplus}$  operation, so it is a bit more liberal than a normal monoid.

```
module TTS.Monoid ( $\mathfrak{M} : \mathbb{N}$ ) ( $\text{zero} : \epsilon \vdash \mathbf{C} \mathfrak{M}$ )
  ( $\_ \bullet \_ : \epsilon \vdash \mathbf{C} \mathfrak{M} \Rightarrow \mathbf{C} \mathfrak{M} \Rightarrow \mathbf{C} \mathfrak{M}$ )
  ( $\text{assoc} : \quad \forall \{ \Gamma \} (a_1 \ a_2 \ a_3 : \Gamma \vdash \mathbf{C} \mathfrak{M})$ 
     $\rightarrow \quad \text{up } \_ \bullet \_ \cdot (\text{up } \_ \bullet \_ \cdot a_1 \cdot a_2) \cdot a_3$ 
     $\beta\eta \equiv \text{up } \_ \bullet \_ \cdot a_1 \cdot (\text{up } \_ \bullet \_ \cdot a_2 \cdot a_3)$ )
  ( $\text{right-identity} : \quad \forall \{ \Gamma \} (e : \Gamma \vdash \mathbf{C} \mathfrak{M})$ 
     $\rightarrow \text{up } \_ \bullet \_ \cdot e \cdot \text{up } \text{zero} \beta\eta \equiv e$ ) where
```

Based on this monoid the ingredients for the transformation can be defined. The representation type  $\mathfrak{R}$  is constructed as a function over the monoidal type, analogous to Hughes' strings, the **abs** and **rep** function are constructed accordingly. The transformation has just one rule which converts the binary operator into function composition.

```
 $\mathfrak{R} : \mathbf{Ty}$ 
 $\mathfrak{R} = \mathbf{C} \mathfrak{M} \Rightarrow \mathbf{C} \mathfrak{M}$ 
abs :  $\epsilon \vdash \mathfrak{R} \Rightarrow \mathbf{C} \mathfrak{M}$ 
abs =  $\Lambda (v \ 0 \cdot \text{up } \text{zero})$ 
rep :  $\epsilon \vdash \mathbf{C} \mathfrak{M} \Rightarrow \mathfrak{R}$ 
rep =  $\Lambda (\text{up } \_ \bullet \_ \cdot v \ 0)$ 
rules : Rules  $\mathfrak{M} \ \mathfrak{R}$ 
rules = replace  $\{ \mathfrak{M} \} \{ \mathfrak{R} \} \{ \iota \longrightarrow \iota \longrightarrow \iota \} \in \_ \bullet \_ \text{comp}$ 
import TTS.Judgement.Base
open TTS.Judgement.Base  $\mathfrak{M} \ \mathfrak{R} \ \text{rep} \ \text{abs} \ \text{rules}$ 
```

This gives rise to a basic type and transform system for monoids. To show that this transformation actually preserves the semantics, we have to show that the **abs** and **rep** function form a retraction, and that the  $\_ \bullet \_$  to  $\circ$  transformation preserves the logical relation.

```
abs-rep : abs  $\circ$  rep  $\beta\eta \equiv \text{id}$ 
abs-rep =
  let open Relation.Binary.EqReasoning  $\beta\eta$  setoid
    renaming ( $\_ \approx \langle \_ \rangle \_$  to  $\_ \leftrightarrow \langle \_ \rangle \_$ )
  in begin
     $\_ \leftrightarrow \langle \text{eval-comp } \_ \_ \rangle$ 
     $\_ \leftrightarrow \langle \% \Lambda (\% \Lambda (\square \% \cdot \% \equiv \text{wk-up } (\text{vs } \text{vz}) \ \text{zero})$ 
       $\% \cdot (\% \Lambda (\% \equiv \text{wk-up } (\text{vs } \text{vz}) \ \_ \bullet \_ \% \cdot \square) \% \cdot \square)) \rangle$ 
     $\_ \leftrightarrow \langle \% \Lambda (\square \% \cdot \beta \leftrightarrow (\% \equiv \text{up-id } \_ \bullet \_ \% \cdot \square)) \rangle$ 
```



```

_ ↔ ⟨ %Λ β ⟩
_ ↔ ⟨ %Λ (□ %· %≡ up-id zero _) ⟩
_ ↔ ⟨ %Λ right-identity (var vz) ⟩
_ ■

```

The logical relation contains only base types. Proving can thus be done using equational reasoning.

```

m-rel : rel {ε} {ι → ι → ι} _ • _ comp ε ε
m-rel a a' r a0 a1 r1 =
  let open Relation.Binary.EqReasoning βηsetoid
    renaming ( _ ≈⟨ _ ⟩ _ to _ ↔⟨ _ ⟩ )
  in begin
    _ ↔⟨ %Λ (%≡ merge-/ _ • _ _ %· □) %· □ ⟩
    _ ↔⟨ β ⟩
    _ ↔⟨ %≡ merge-/ _ • _ _ %· □ ⟩
    _ ↔⟨ bsym η ↔ %Λ (%≡ wk-up vz ( _ • _ · ( _ • _ · a · a0)) %· □) ⟩
    _ ↔⟨ %Λ assoc (up a) (up a0) (v 0) ⟩
    _ ↔⟨ %Λ (%≡ split-/ _ • _ _ %· □ %· (%≡ split-/ _ • _ _ %· □ %· □)) ⟩
    _ ↔⟨ %Λ (bsym β %· (bsym β %· □)) ⟩
    _ ↔⟨ %Λ (%Λ (bsym (%≡ wk-up _ _ • _) %· □) %· bsym (%≡ wk-up _ a)
      %· (%Λ (bsym (%≡ wk-up _ _ • _) %· □) %· bsym (%≡ wk-up _ a0) %· □))
    _
    _ ↔⟨ bsym (eval-comp _ _) ⟩
    _ ↔⟨ %Λ (%≡ split-/ _ • _ _ %· □)
      %· □ %· %Λ (%≡ split-/ _ • _ _ %· □) %· □ ⟩
    _ ↔⟨ r %· r1 ⟩
    _ ■

proofs : RuleProofs rules
proofs = proof ε _ • _ comp m-rel

```

**open TransformationProof** abs-rep proofs

We can use this to show the equivalence of transformed terms.

```

trans1 : (ε , C ℳ) : C ℳ ⊢ up _ • _ · v 0 · v 0
  ~> (up abs · (up rep · v 0 ○ up rep · v 0))
trans1 = i-abs (app (app (rule (rule ε)) (i-rep (var vz))) (i-rep (var vz)))
proof1 : (s : (ε , C ℳ) ↓) → close (up _ • _ · v 0 · v 0) s
  βη≡ close (up abs · (up rep · v 0 ○ up rep · v 0)) s
proof1 = extract {ε , C ℳ} {ℳ}
  (up _ • _ · v 0 · v 0)
  (up abs · (up rep · v 0 ○ up rep · v 0))
  (≡! sym (! , ⊢-id (ε , C ℳ) (C ℳ) _), sym (! , ⊢-id (ε , C ℳ) (C ℳ) _) >~> trans1)

```

## 5 Extensions to the TTS system

Although the simply typed lambda calculus is a convenient language with which to explain ideas and prove general concepts, it is too simple to serve as a basis for real-world transformation systems. Most notably, STLC does not support recursion or polymorphism, two constructs which are present in almost all real-world functional languages.

This chapter introduces such fundamental extensions for the basic  $TTS_\lambda$  along several axis. The soundness of these extensions is not proven here but is informally shown and provability is briefly discussed.

### 5.1 Extending to let-polymorphism

One of the most common extensions to the simply typed lambda calculus is let-polymorphism with Hindley-Milner typing as found in ML and Haskell. This extension introduces the concept of type variables into the language and a way to quantify over them, as in the following definitions:

$$\begin{aligned}\tau &::= \mathbf{T} \mid \mathbf{a} \mid \tau \rightarrow \tau \\ \sigma &::= \forall \mathbf{a}. \sigma \mid \tau \\ \Gamma &::= \Gamma, \sigma \mid \emptyset \\ \theta &::= [\mathbf{a} \mapsto \tau] \circ \theta \mid \mathbf{id}\end{aligned}$$

The typing functor of  $TTS_\lambda$  is essentially an extension of the base types, and thus works equally well in the presence of type variables:

$$\begin{aligned}\dot{\tau} &::= \mathbf{T} \mid \iota \mid \mathbf{a} \mid \dot{\tau} \rightarrow \dot{\tau} \\ \dot{\sigma} &::= \forall \mathbf{a}. \dot{\sigma} \mid \dot{\tau} \\ \dot{\Gamma} &::= \dot{\Gamma}, \dot{\sigma} \mid \emptyset \\ \dot{\theta} &::= [\mathbf{a} \mapsto \dot{\tau}] \circ \dot{\theta} \mid \mathbf{id}\end{aligned}$$

Hindley-Milner typing prescribes two functions which can be used to introduce and eliminate quantification,  $\text{gen} :: \Gamma \rightarrow \tau \rightarrow \sigma$  and  $\text{inst} :: \sigma \rightarrow \theta \rightarrow \tau$ . Generalize quantifies over all type variables in  $\tau$  except the variables which occur free in the environment  $\Gamma$ .  $\text{inst}$  creates a normal type from a schema and a substitution  $\theta$  for all quantified variables. These function can be straightforwardly extended to typing functors by treating the  $\iota$  construct as a normal base type in both functions.

Figure 5.1 shows the typing rules for the let-polymorphic lambda calculus and the corresponding transformation rules for  $TTS_{\text{let}}$ , the core transformation system. The extension is again a straightforward extension of the basic Hindley-Milner typing rules. Proving this transformation correct however is more difficult.

<b>Tr-Con</b>	$\frac{\text{c is a constant of type } \mathbf{T}}{\dot{\Gamma} \vdash_{let} c \rightsquigarrow c : \mathbf{T}}$	$\frac{\text{c is a constant of type } \mathbf{T}}{\Gamma \vdash_{let} c : \mathbf{T}}$	<b>Con</b>
<b>Tr-Var</b>	$\frac{x : \dot{\sigma} \in \dot{\Gamma}}{\dot{\Gamma} \vdash_{let} x \rightsquigarrow x : inst(\dot{\sigma}, \mathbf{sub})}$	$\frac{x : \sigma \in \Gamma}{\Gamma \vdash_{let} x : inst(\sigma, \theta)}$	<b>Var</b>
<b>Tr-Lam</b>	$\frac{\dot{\Gamma}, x : \dot{\tau}_a \vdash_{let} e \rightsquigarrow e' : \dot{\tau}_r}{\dot{\Gamma} \vdash_{let} \lambda x. e \rightsquigarrow \lambda x. e' : \dot{\tau}_a \rightarrow \dot{\tau}_r}$	$\frac{\Gamma, x : \tau_a \vdash_{let} e : \tau_r}{\Gamma \vdash_{let} \lambda x. e : \tau_a \rightarrow \tau_r}$	<b>Lam</b>
<b>Tr-App</b>	$\frac{\dot{\Gamma} \vdash_{let} f \rightsquigarrow f' : \dot{\tau}_a \quad \dot{\Gamma} \vdash_{let} e \rightsquigarrow e' : \dot{\tau}_a}{\dot{\Gamma} \vdash_{let} f e \rightsquigarrow f' e' : \dot{\tau}_r}$	$\frac{\Gamma \vdash_{let} f : \tau_a \quad \Gamma \vdash_{let} e : \tau_a}{\Gamma \vdash_{let} f e : \tau_r}$	<b>App</b>
<b>Tr-Let</b>	$\frac{\dot{\Gamma} \vdash_{let} f \rightsquigarrow f' : \dot{\tau}_a \quad \dot{\Gamma}, x : gen(\dot{\Gamma}, \dot{\tau}_a) \vdash_{let} e \rightsquigarrow e' : \dot{\tau}_r}{\dot{\Gamma} \vdash_{let} \mathbf{let } x = f \mathbf{ in } e \rightsquigarrow \mathbf{let } x = f' \mathbf{ in } e' : \dot{\tau}_r}$	$\frac{\Gamma \vdash_{let} f : \tau_a \quad \Gamma, x : gen(\Gamma, \tau_a) \vdash_{let} e : \tau_r}{\Gamma \vdash_{let} \mathbf{let } x = f \mathbf{ in } e : \tau_r}$	<b>Let</b>
<b>Tr-Rep</b>	$\frac{\dot{\Gamma} \vdash_{let} e \rightsquigarrow \mathbf{rep } e' : \iota}{\dot{\Gamma} \vdash_{let} e \rightsquigarrow e' : \mathfrak{A}}$		
<b>Tr-Abs</b>	$\frac{\dot{\Gamma} \vdash_{let} e \rightsquigarrow e' : \iota}{\dot{\Gamma} \vdash_{let} e \rightsquigarrow \mathbf{abs } e' : \mathfrak{A}}$		
<b>Judgement</b>	$\boxed{\dot{\Gamma} \vdash_{let} e \rightsquigarrow e' : \dot{\tau}}$	$\boxed{\Gamma \vdash_{let} e : \tau}$	

Figure 5.1: Type checking rules for the propagation relation of  $TTS_{let}$

## 5.2 Including a fixpoint

Although the simply typed lambda calculus serves well as a foundation for a typed program transformation system, it has one important shortcoming: it is not Turing complete. A language needs some form of unbridled recursion to become Turing complete. A well-known construct for recursion is the fixpoint. A fixpoint works by taking a function and turning it into a possibly infinite self-application. An example of a fixpoint is the Y combinator, but other variants exist as well.

**fix** :: (a → a) → a  
**fix** f = (λx → f (x x)) (λx → f (x x))

Note that this expression does not type-check in Haskell. There are ways to make such a primitive recursion operator type-check but usually the fixpoint is an internal part of a language. Programs containing general recursive functions are compiled into a version containing only fixpoints as recursion primitive. A typing rule and propagation rule for a primitive **fix** can be constructed as follows:

$$\text{Tr-Fix} \quad \frac{\dot{\Gamma} \vdash_{\lambda} f \rightsquigarrow f' : \mathbf{T} \rightarrow \mathbf{T}}{\dot{\Gamma} \vdash_{\lambda} \mathbf{fix } f \rightsquigarrow \mathbf{fix } f' : \mathbf{T}} \quad \frac{\Gamma \vdash_{\lambda} f : \mathbf{T} \rightarrow \mathbf{T}}{\Gamma \vdash_{\lambda} \mathbf{fix } f : \mathbf{T}} \quad \mathbf{Fix}$$

Because **fix** is a primitive function, it has a separate convertibility rule,  $\mu$ , which states that one of the function applications can be peeled off the infinite chain of self-applications.

$$\begin{aligned}\mu & : \forall \{\tau\} \rightarrow \{f : \Gamma \vdash \tau \Rightarrow \tau\} \rightarrow \mathbf{fix} \ f \ \beta\eta \equiv f \cdot \mathbf{fix} \ f \\ \%fix & : \forall \{\tau\} \rightarrow \{f f' : \Gamma \vdash \tau \Rightarrow \tau\} \rightarrow f \ \beta\eta \equiv f' \rightarrow \mathbf{fix} \ f \ \beta\eta \equiv \mathbf{fix} \ f'\end{aligned}$$

While this seems like a straightforward enough extension to the basic  $TTS_\lambda$  system, the fixpoint has some implications on the semantics of a language, and thus on the way proofs are conducted for that language.

**Impact on evaluation** The main problem is that a fixpoint introduces possibly infinite recursion: divergent terms. This means that, next to the normal values which a term can produce, a term can also produce  $\perp$ : no value at all! In such a language, the order of evaluation becomes important.

The lambda calculus without fixpoint is *strongly normalizing*, meaning that however evaluation is performed, the answer will always be the same. However, with the presence of  $\perp$ , the order of evaluation can have an impact on the result of evaluation. This is best illustrated with an example:

`v = take 10 (fix (1 :))`

**fix** (1 :) produces an infinite list of 1's. The outcome of this function now really depends on what is evaluated first. If the arguments to a function are evaluated before a function is called, this program will loop forever. If, however, functions are being reduced before their arguments, this program will produce a list of 10 1's. The first type of evaluation is called call-by-value or strict evaluation, the second is called call-by-need or lazy evaluation.

This example shows that lazy evaluation can sometimes produce an answer when strict evaluation can not. This is because lazy evaluation has a very nice property which strict evaluation lacks: if a term can produce a value (has a *normal form*), lazy evaluation will compute this value.

**Convertibility** The fact that the evaluation order impacts the final outcome of an expression also impacts equational reasoning and the convertibility relation. Take for example the following equality:

$$\mathbf{const} \ 1 \ (\mathbf{fix} \ (:\mathbf{1})) \equiv_{\beta\eta} 1$$

In a lazy semantics this would be a valid equality. In a strict semantics this is unequal: **fix** (:1) has to be evaluated before **const** and will thus result in  $\perp$  instead of 1. In general, the convertibility relation is only sound for semantics which use *lazy evaluation*. This also means that the proofs in the type and transform system are only valid for a language with lazy semantics.

**Totality** Convertibility can be made sound in a strict language by restricting the **fix** function to functions which provably never produce  $\perp$ : they never loop. A provably finite recursive function is called a *total* function. Agda is an example of a language which allows equational reasoning because, although it has strict semantics, it requires totality on its functions. Note that limitation again removes the turing completeness from a language.

## **6 Future work**

## **7 Conclusion**

### **7.1 Acknowledgements**

# Bibliography

- [AB11] Amal Ahmed and Matthias Blume. An equivalence-preserving cps translation via multi-language semantics. In *ICFP*, pages 431–444, 2011.
- [CH07] Karl Crary and Robert Harper. Syntactic logical relations for polymorphic and recursive types. *Electron. Notes Theor. Comput. Sci.*, 172:259–299, April 2007.
- [CLS07] Duncan Coutts, Roman Leshchinskiy, and Don Stewart. Stream fusion. from lists to streams to nothing at all. In *ICFP’07*, 2007.
- [COV06] Alcino Cunha, José Nuno Oliveira, and Joost Visser. Type-safe two-level data transformation. In *Proceedings of the 14th international conference on Formal Methods, FM’06*, pages 284–299, Berlin, Heidelberg, 2006. Springer-Verlag.
- [CSL07] Duncan Coutts, Don Stewart, and Roman Leshchinskiy. Rewriting haskell strings. In *In Practical Aspects of Declarative Languages 8th International Symposium, PADL 2007*, pages 50–64. Springer-Verlag, 2007.
- [CV07] Alcino Cunha and Joost Visser. Strongly typed rewriting for coupled software transformation. *Electron. Notes Theor. Comput. Sci.*, 174(1):17–34, April 2007.
- [ER07] Martin Erwig and Deling Ren. An update calculus for expressing type-safe program updates, 2007.
- [GH09] Andy Gill and Graham Hutton. The Worker/Wrapper Transformation. *Journal of Functional Programming*, 19(2):227–251, March 2009.
- [HHS02] Bastiaan Heeren, Jurriaan Hage, and Doaitse Swierstra. Generalizing hindley-milner type inference algorithms. Technical report, 2002.
- [Hin00] Ralph Hinze. Generic programs and proofs, 2000.
- [HS99] Furio Honsell and Donald Sannella. Pre-logical relations. In *PROC. COMPUTER SCIENCE LOGIC, CSL’99*, pages 546–561. Springer, 1999.
- [Hug86] R J M Hughes. A novel representation of lists and its application to the function "reverse". *Information Processing Letters*, 22(3):141–144, 1986.
- [JV04] Patricia Johann and Janis Voigtländer. Free theorems in the presence of seq, 2004.
- [JV09] Patricia Johann and Janis Voigtländer. A family of syntactic logical relations for the semantics of haskell-like languages. *INFORMATION AND COMPUTATION*, 2009.

- [KA10] Chantal Keller and Thorsten Altenkirch. Normalization by hereditary substitutions. 2010.
- [Keu11] Steven Keuchel. Generic programming with binders and scope, 2011.
- [Kuc97] Jakov Kucan. Metatheorems about convertibility in typed lambda calculi: Applications to cps transform and "free theorems". Technical report, 1997.
- [MH95] Erik Meijer and Graham Hutton. Bananas in space: extending fold and unfold to exponential types. In *Proceedings of the seventh international conference on Functional programming languages and computer architecture*, FPCA '95, pages 324–333, New York, NY, USA, 1995. ACM.
- [Mit96] John C. Mitchell. *Foundations for programming languages*. Foundation of computing series. MIT Press, 1996.
- [MW85] Albert R. Meyer and Mitchell Wand. Continuation semantics in typed lambda-calculi. In *Logics of Programs*, pages 219–224. Springer-Verlag, 1985.
- [Nor07] Ulf Norell. *Towards a practical programming language based on dependent type theory*. PhD thesis, Department of Computer Science and Engineering, Chalmers University of Technology, SE-412 96 Göteborg, Sweden, September 2007.
- [pop] The poplmark challenge. <http://www.seas.upenn.edu/~plclub/poplmark/>.
- [pro] Program-transformation.org. <http://http://www.program-transformation.org/>.
- [Rey83] John C. Reynolds. Types, abstraction and parametric polymorphism. In *IFIP Congress*, pages 513–523, 1983.
- [SS08] Carsten Schürmann and Jeffrey Sarnat. Structural logical relations \*, 2008.
- [str] Stratego/xt. <http://strategoxt.org/>.
- [Wad89] Philip Wadler. Theorems for free! In *Proceedings of the fourth international conference on Functional programming languages and computer architecture*, FPCA '89, pages 347–359, New York, NY, USA, 1989. ACM.